

**NETWORK FIREWALL AGREEMENT
BETWEEN DIRSEC, LLC
AND POUDRE SCHOOL DISTRICT R-1**

This Network Firewall Agreement (“Agreement”) is entered into as of the 8th day of March 2024, by and between Poudre School District R-1, a school district organized and existing under the laws of the state of Colorado (the “District”), and DirSec, LLC (“Contractor”), collectively referenced herein as the “parties.” In consideration of the mutual covenants and promises contained in this Agreement, the sufficiency of which is hereby acknowledged, the parties agree as follows:

1. Term of Agreement.

1.1. This Agreement shall commence on August 1, 2024, and continue through and including July 31, 2025, unless earlier terminated as provided herein.

1.2. Notwithstanding any other term or provision of this Agreement, the District’s obligations hereunder are expressly subject to its budgeting and appropriation of sufficient funds for each fiscal year (July 1 - June 30) an Agreement is in effect. In no event, shall the District’s obligations in an Agreement constitute a multiple-fiscal year direct or indirect debt or other financial obligation under Article X, Section 20(4)(b) of the Colorado Constitution.

1.3. Notwithstanding the planned term of an Agreement and/or any extensions thereof as provided in section 1.1 and 1.2 above, the District may terminate an Agreement at any time in its sole discretion for any reason, with or without cause, upon written notice served on the Contractor no less than thirty (30) days prior to the date of termination. In the event of such early termination by the District, the Contractor shall be paid up to the date of termination for services performed under and in accordance with this Agreement.

2. Deliverables and Purchase Price.

2.1. The Contractor’s responsibility under this Agreement is to provide its Palo Alto Network (“PAN”) firewall equipment, licensing, and any other defined services as per the scope outlined in IFB 24-680-006 – E-Rate Palo Alto Firewall or Equivalent. The parties agree to all the terms and conditions of this Agreement and within the following as specified in the:

2.1.1. Invitation for Bid (“IFB”) 24-680-006, which is part of this agreement and attached hereto as Exhibit A.

2.1.2. Contractor’s Response to IFB 24-680-006, which is part of this agreement and attached hereto as Exhibit B.

2.1.3. Contractor’s Final Quote to IFB 24-680-006, which is part of this agreement and attached hereto as Exhibit C.

All documents which are made a part of this Agreement (hereinafter the “Services”) and incorporated herein by reference.

2.2. The total cost for the Services, as set forth on the attached Exhibit C, is Two Hundred and Three Thousand, Four Hundred and Forty-Six Dollars and Forty-Five Cents (\$203,446.45), due and payable by the District thirty (30) days from the receipt of Contractor's invoice.

2.3. **Warranties**

2.3.1. Notwithstanding prior acceptance of Services by the District, the Contractor shall expressly warrant all delivered Services provided, as properly functioning at the start of operations and compliant with the terms of the Agreement and industry standards thereafter. The warranty period will begin at the time the Services have been formally accepted in writing by the District.

2.3.2. During the warranty period, the Contractor shall be responsible and bear all costs to correct any problems, defects and/or deficiencies reported which do not meet the specifications set forth in the Agreement.

2.3.3. The Contractor will correct all defects and/or deficiencies associated with this Agreement and replace incorrect or defective Services within five (5) business days of written notification from the District to the Contractor. If, within five (5) business days after written notice by the District to the Contractor, the Contractor has not corrected all defects and/or deficiencies, the District may correct all defects and/or deficiencies at the Contractor's expense.

2.3.4. Contractor warrants that all Services furnished under the Agreement shall be merchantable and shall be safe and appropriate for the purpose for which Services of like kind are normally used. If Contractor knows or has reason to know the particular purpose for which the District intends to use the Service, Contractor warrants that such Services shall be fit for that particular purpose. Contractor warrants that all Services furnished under the Agreement shall be new unless otherwise specified by the District, and that the title conveyed regarding such Services shall be complete and its transfer rightful. Contractor agrees to promptly replace or correct all defects and/or deficiencies in any Service not conforming to the foregoing warranties, without expense to the District, provided the District elects to allow Contractor the opportunity to do so.

2.3.5. Defects and/or deficiencies properly noted in writing to the Contractor before expiration of the warranty period will be fully covered regardless of such expiration.

2.3.6. In the case of emergency, repairs and/or replacement may be made without notice being given to the Contractor, if determined by the District that delay would cause certain loss or damage. The Contractor shall pay the cost of these emergency repairs and/or replacements. Contractor shall, upon District request, provide proof as to the kind and quality of materials and equipment. Contracted work shall, likewise, be free of defects and in conformance with industry standards. Contractor also warrants that its workers will be sufficiently skilled to produce high quality work, free of faults and defects. Work not conforming to these requirements, including unauthorized substitutions, may be considered defective. Contractor

further warrants that the construction processes and methods employed to perform the work shall be suitable for the results required and expected. If the Contractor proposes to use an unproved and untried method, process or product, the District must be advised of the proposal in writing and give approval. The District may permit experimentation but may require special guarantees by the Contractor to cover the experimental work.

2.4. **Review of Product.** Payment for Services furnished under the Contract shall not constitute acceptance thereof. The Project Coordinator shall have the right to confirm the completion of the Services provided, the product of such Services, and to reject any or all of which are in the District's judgment defective or nonconforming. In addition to the District's other rights, and Services which had been rejected. The District will not be charged for Services to correct Contractor's errors for correcting such Services.

2.5. **Materials.** All labor, licenses, materials, supplies, equipment, and all other items necessary to complete the Services required to be furnished by the Contractor (the "Materials") shall be part of and not in addition to the Agreement price. The Contractor shall be responsible and liable for any damage or destruction to any Materials resulting from any cause other than the deliberate or negligent acts of the District for which it could be held liable under the Colorado Governmental Immunity Act.

2.6. **Primary Contractor and Subcontractors.** The Contractor shall assume all responsibility for performance of all Services in this Agreement, whether or not the Contractor uses subcontractors. Any consequences resulting from non-performance under the terms of this Agreement are the sole responsibility and liability of the Contractor. The Contractor shall be the sole point of contact with the District with regard to all matters covered by this Agreement. The District shall not initiate or maintain contact with any subcontractor unless such contact becomes necessary to mitigate the District's damage in the event the Contractor is in default or breach of any term or obligation of this Agreement.

2.7. **Press Contacts/News Releases.** The Contractor shall not initiate any press, media, or social media, contact nor respond to press, media or social media requests regarding this Agreement and/or any related matters concerning the District without the prior written approval of the District.

2.8. **Non-Disclosure of Confidential Information.** Contractor understands that while performing Services under this Agreement, it may be provided access to student records or personally identifiable information protected from disclosure to third parties and subject to the Individuals with Disabilities Education Act (20 U.S.C. §§ 1400 et seq.), the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) ("FERPA") and the Colorado Open Records Act (C.R.S. §§ 24-72-201 et seq.). Such records and information are considered confidential and protected. Accordingly, Contractor hereby agrees that it shall keep confidential and shall not disclose any information, including but not limited to information regarding any District student, student family, student health/medical condition, student disability, student IEP and/or student accommodation, to which it gains access in connection with its provision of the Services. To the extent Contractor has access to such records and information, Contractor shall be deemed a "school official" as such term is defined under FERPA. Contractor agrees that it or

its employees, volunteers and subcontractors shall not use education records or personally identifiable student information for any purpose other than in performance of this Agreement.

2.8.1. At the termination of this Agreement or earlier, if requested by the District, Contractor shall promptly return all such information, and/or shall at the request of the District destroy or delete any and all copies or duplicates of said information, whether the information is in hard copy or electronic form. If Contractor violates the terms of this section 3.7.4, Contractor agrees to indemnify, defend and hold harmless the District, and/or its employees and agents, from any and all claims, liabilities, or causes of action, including attorney fees and costs, asserted against the District and/or its employees or agents as a result of the violation. Contractor also agrees to indemnify the District, and/or its employees and agents, from the costs of complying with and/or resolving any regulatory investigation caused by the violation, including costs and attorney fees.

2.8.2. **Obligations and Return of Confidential Information.** The receiving parties obligation hereunder shall survive for a period of five (5) years following termination of this Agreement; provided however, any confidential obligations with respect to protected District information shall survive indefinitely to the extent required to comply with applicable law. All confidential information shall remain the sole property of the disclosing party, and all materials containing any such confidential information, including all copies made by the receiving party, shall be returned to the disclosing party or destroyed immediately upon termination or expiration of this Agreement, or upon the receiving party's determination that it no longer has a need for such confidential information. Upon the request of the disclosing party, the receiving party shall certify in writing that all materials containing such confidential information, including all copies thereof, have been returned to the disclosing party or have been destroyed.

2.9. **Colorado Open Records Act.** Information and materials submitted under this Agreement may be considered public records subject to disclosure under the Colorado Open Records Act, (C.R.S. §§ 24-72-200.1 to -205.5) ("CORA"). Information and materials that the Contractor believes are confidential and not subject to disclosure under CORA must be submitted separately with a citation to the section of CORA and any other relevant law under which the Contractor believes they are confidential. The District, not the Contractor, shall determine whether information and materials so identified will be withheld as confidential, but will inform the Contractor in advance of disclosure to give it an opportunity to take legal action to protect its interests vis-à-vis the party making the CORA request.

3. **Independent Contractor.**

3.1. Contractor shall provide the Services under this Agreement as an independent contractor of the District. As such, Contractor shall have the right to determine how and by whom the Services will be provided and the right to provide the Services free from the direction and control of the District, subject to and consistent with the terms and conditions of this Agreement.

3.2. Contractor shall be exclusively responsible for: (a) all compensation, employment tax withholdings and payments, and all fringe benefits for its employees (if any) in full compliance with all applicable federal, state and local laws; (b) all insurance coverages and benefits for its employees (if any) in full compliance with all applicable federal, state and local laws, including but not limited to pension or retirement benefits, workers' compensation, unemployment compensation, and Social Security benefits; and (c) all payments to its contractors and subcontractors for goods and/or services directly or indirectly related to this Agreement.

3.3. Nothing in this Agreement shall be construed as creating a single enterprise, partnership, joint venture or employer-employee relationship between Contractor and the District. Contractor is not a partner, agent or representative of the District and shall not represent itself to be a partner, agent or representative of the District. The District is not a partner, agent or representative of Contractor and shall not represent itself to be a partner, agent or representative of Contractor.

3.4. Contractor shall not attempt or purport to extend the faith and credit of the District to any third party, person or entity. Contractor acknowledges and agrees that it has no authority to enter into any contract with a third party that would bind or in any way obligate the District. The District shall not attempt or purport to extend the faith and credit of Contractor to any third party, person or entity. The District acknowledges and agrees that it has no authority to enter into any contract with a third party that would bind or in any way obligate Contractor.

4. **Equal Opportunity.** It is agreed that no otherwise qualified Contractor shall be excluded from participating in, be denied the benefits of, or be subject to discrimination, including harassment, under any provision of this Agreement on the basis of race; creed; color; national origin; age; sex; pregnancy; physical recovery from childbirth or a related condition; sexual orientation; marital status; veteran status; religion; genetic information; gender expression; gender identity; ancestry; or disability.

5. **Health and Safety Standards.** The Contractor shall have and maintain a set of protocols and guidelines to meet evolving health and safety requirements and implement any applicable communicable disease protocols, which must follow guidance and orders from state and/or local public health officials and be no less strict than the District's protocols.

5.1. Contractor shall ensure all individuals providing Services under this agreement for the Contractor wear appropriate personal protective equipment as designated in this section 2.13, at all times while on District property.

5.2. If the District is directed, or the District determines to limit or restrict access to any or all of its facilities or District Location due to a public health or safety concern, the District may, at its discretion, temporarily delay or stop Contractor's services, with or without prior notice.

6. **Individuals Providing Services for Contractor Under this Agreement.** The Contractor shall not utilize any laborer or employee who has been convicted of

a violent crime or a crime of such nature (e.g., child-related offenses) as to categorize the person as being unsuitable for working around school children, or has engaged in such conduct as to be similarly categorized. In the event the District has reasonable grounds to believe that any individual assigned to perform work under this Agreement has a criminal record, is a registered sex offender, has exhibited violent behavior or is under the influence of alcohol or an illegal substance, including marijuana, while performing the Services or based upon other information the District deems reliable, the District may exclude such individual from any District property or impose reasonable conditions upon such individual's presence at any District Location unless the Contractor submits a copy of a completed security/background check on the employee. In the judgement of the District, if the Services cannot be performed as a result of such action, the Agreement may be terminated in accordance with section 1.3 of this Agreement. Removal of a specific person(s) will not relieve the Contractor from timely performance of work completion and will not be considered grounds for a request for additional funds or time extension to complete the Services.

6.1. The Contractor, its laborers and employees shall not fraternize or otherwise communicate with any District students except in cases of safety and like necessities.

7. **Conflict of Interest.** Contractor avers to their knowledge of no employee of the District having any personal or beneficial interest whatsoever in the service or property described in this Agreement. Contractor has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of the Contractor's Services and Contractor shall not employ any person having such known interest.

8. **Access to District Server.** If access to any District server is necessary for the functionality of the Contractor's services. Upon written approval by the Executive Director of Information Technology or designee, the District grants the Contractor limited access to the District server for the sole purpose of providing Services.

8.1. The Contractor agrees to protect the confidentiality, integrity and availability of all electronic District or student information at all times.

8.2. The Contractor agrees to take proper steps to ensure the security of the device in which they connect to the District's systems remotely. The Contractor agrees not to copy information accessed remotely to local devices and or portable devices. Printing information is not permitted unless specific authorization has been granted.

8.3. The Contractor shall not share passwords, codes, credentials or user accounts with others.

8.4. The Contractor shall have a valid and up-to-date antivirus agent installed to ensure protection against malware and viruses upon connection to the District network.

8.5. The Contractor acknowledges that if the District determines in its discretion that remote access has been compromised by unauthorized parties, or that remote access has been misused, the Contractor's access will be disabled or terminated immediately.

9. **Indemnification.** The Contractor shall indemnify and hold harmless the District and the District's Board members, employees, representatives and agents from and against any and all liability arising from any suit, action, third party claims, grievance, or proceeding, including all attorneys' fees, costs and expenses, incurred as a result of any negligent or intentional act or omission by Contractor, or its employees, agents, Subcontractors, or assignees related to the terms of this Agreement and any Services provided under this Agreement.

10. **Governmental Immunity.** It is specifically understood and agreed that nothing contained in this Agreement shall be construed as an express or implied waiver by the District of any of the immunities, rights, benefits, protections, or other provisions of the Colorado Governmental Immunity Act, C.R.S. §§ 24-10-101 *et seq.*, as now or hereafter amended.

11. **Insurance.** Vendor shall procure and maintain the required insurance specified below for the duration of this Agreement, which insurance shall be written for not less than the amounts specified or greater if required by law. The District's receipt of a Certificate of Insurance from the Vendor with limits and or coverages that do not meet the requirements does not waive the requirements and the Vendor shall still be responsible for the limits and coverages stated in this Agreement. Specified coverages and amounts may be provided by a combination of a primary policy plus an umbrella or following form excess policy. All insurance shall be with a carrier licensed in the state of Colorado and shall have a minimum A.M. Best rating of A- VII. Vendor shall furnish the District's Director of Records and Risk Management with certificates of the required insurance prior to the District's approval and signing of this Agreement, and with renewal certificates prior to the expiration of any required insurance that expires during the term of this Agreement. Memorandums of Insurance will not be accepted. Certificates of Insurance and all communication regarding insurance shall be sent to:

Poudre School District
Attention: Risk Management
2407 Laporte Ave
Ft. Collins, CO 80521
Email Certificate to: risk@psdschools.org

Any insurance and/or self-insurance carried by the District is excess of the coverage extended to the District by Vendor. Vendor shall provide at least thirty (30) days' advance written notice to the District prior to cancellation, change of coverage, or non-renewal. The insurance requirements specified in this section 10 shall not reduce the indemnification liability that Vendor has assumed herein.

Commercial General Liability

Minimum Limits

- | | |
|---|-------------|
| ● Each Occurrence Bodily Injury & Property Damage | \$1,000,000 |
| ● General Aggregate | \$2,000,000 |
| ● Products/Completed Operations Aggregate | \$2,000,000 |

- Personal/Advertising Injury \$2,000,000
- Product Recall Expense \$500,000
- Coverage must be written on an “occurrence” basis.
- Poudre School District R-1 and its elected officials, employees, agents, and volunteers shall be named as an additional insured or covered as an additional insured by way of a blanket endorsement and shall be insured to the full limits of liability purchased by the Vendor even if those limits of liability are in excess of those required by this Agreement.

Professional Liability

Minimum Limits

- a. Each Occurrence or Wrongful Act Limit \$1,000,000
- b. Annual Aggregate Limit \$3,000,000
- c. In the event that the Professional Liability insurance required by this Agreement is written on a claims-made basis Provider warrants that any retroactive date under the policy shall precede the effective date of this Agreement and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of three (3) years beginning at the time work under this Agreement is completed.
- d. Provider must provide evidence of the extended reporting period coverage at the end of the project and before all final payments to the Provider is made.

Technology Errors and Omissions Liability (Professional Liability, including Network Security and Privacy Liability)

Minimum Limits

- Per Loss \$1,000,000
- Aggregate \$3,000,000
- Liability extends for a period of three (3) years beginning at the time work under this Agreement is completed. Provider shall maintain continuous coverage, as required by the Agreement, for this period.

The insurance shall provide coverage for:

- Liability arising from theft, dissemination and/or use of confidential information (defined term including but not limited to bank account, credit card account, personal information such as name, address, social security numbers, etc. information) stored or transmitted in electronic form.
- Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party to gain access to Provider’s services including denial of service, unless caused by a mechanical or electrical failure.

- Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a District or third person's computer, computer system, network, or similar computer related property and the data, software, and programs thereon.

Crime Coverage

Minimum Limits

Per Loss

\$1,000,000

The policy shall include:

- Coverage for all directors, officers, agents, and employees of the Supplier.
- Employee dishonesty, forgery and alteration, monies and securities, and computer (cyber) crime.
- Extended theft and mysterious disappearance.
- The policy shall not contain a condition requiring an arrest and conviction.
- Policy must be endorsed to cover Third Party Fidelity and include Poudre School District R-1 as a Loss Payee.

Workers' Compensation and Employers' Liability

If Provider is exempt under the Colorado Workers' Compensation Act, this requirement will be waived if proof a current Workers' Compensation Coverage Rejection is on file with the Colorado Department of Labor and Employment, Division of Worker's Compensation and a copy is submitted to the District.

Minimum Limits

- State of Colorado Statutory
- Employer's Liability

\$100,000 Each Accident
\$500,000 Disease – Policy Limit
\$100,000 Disease – Each Employee

Waiver of subrogation in favor of Poudre School District R-1.

The Vendor shall indemnify and hold harmless the District and the District's Board members, employees, representatives and agents from and against any and all liability arising from any suit, action, third party claims, grievance, or proceeding, including all attorneys' fees, costs and expenses, incurred as a result of any negligent or intentional act or omission by Vendor, or its employees, agents, Subcontractors, or assignees related to the terms of this Agreement and any Services provided under this Agreement.

It is specifically understood and agreed that nothing contained in this Agreement shall be construed as an express or implied waiver by the District of any of the immunities, rights, benefits, protections, or other provisions of the Colorado Constitution or Governmental Immunity Act, C.R.S. §§ 24-10-101 et seq, as now or hereafter amended.

12. **Remedies.** If Contractor fails to comply with any of the foregoing requirements at any time during or after the term of the Contract the District may, as applicable, terminate the Contract and/or disqualify Contractor from future contracts and subcontracts with the District.

12.1. Upon failure of the Contractor to deliver the service(s) and/or deliverables in accordance with the specifications and to the satisfaction of the District within the time stated, the Contractor shall be subject to charges for liquidated damages in the amount of five (5) percent of the total contract value per day for each and every calendar day that the service(s) and/or deliverables are not delivered to, and accepted by, the District. As compensation due to the District for loss of use and for additional costs incurred by the District due to such noncompletion of work, the District shall have the right to deduct said liquidated damages from any amount due or that may become due to the Contractor under this agreement or to invoice the Contractor for such damages if the costs incurred exceed the amount due to the Contractor.

12.2. In the event the awarded Contractor defaults on its Contract or the Contract is terminated for cause due to performance, the District reserves the right to re-procure the Services from the next lowest Contractor or from other sources during the remaining term of the terminated/defaulted Contract. Under this arrangement, the District shall charge the awarded Contractor any differences between its price and the price to be paid to the next lowest Contractor, as well as, any costs associated with the re-solicitation effort which resulted from such default or termination.

13. **Notices and Communications.** All notices and communications required or permitted under this Agreement shall be in writing and shall be: (a) sent via certified mail, return receipt requested and postage prepaid, to the address of the other party set forth below; or (b) sent via e-mail to the other party via the e-mail address set forth below.

Poudre School District R-1
Attn: Contracts Administrator
2407 LaPorte Avenue
Fort Collins, CO 80521
E-mail: contracts@psdschools.org

DirSec, LLC
Attn: Dade Myres
357 McCaslin Blvd, Suite 200
Louisville, CO 80027
E-mail: dmyres@dirsec.com

14. **General Provisions.**

14.1. **No Assignment.** The Contractor shall not assign this Agreement or any of its rights, interests or obligations under this Agreement without the prior written consent of the District, which consent may be withheld for any reason or no reason as determined by the District in its sole discretion.

14.2. **No Waiver.** The parties agree that no assent or waiver, express or implied, to any breach of any one or more of the covenants of this Agreement shall be construed as or deemed to be an assent to or a waiver of any subsequent breach.

14.3. **Press Contacts/News Releases.** The Contractor shall not initiate any press, media, or social media contact nor respond to press, media or social media requests

regarding this Agreement and/or any related matters concerning the District without the prior written approval of the District's Chief Information Officer or designee.

14.4. **Survival of Certain Contract Terms.** Notwithstanding anything herein to the contrary, the parties understand and agree that all terms and conditions of this Agreement and the exhibits and/or attachments hereto which may require continued performance, compliance, or effect beyond the termination date of the Agreement- shall survive such termination date and shall be enforceable by the District as provided herein in the event of such failure to perform or to comply by the Contractor.

14.5. **Amendment or Modification.** No amendment or modification of this Agreement shall be valid unless set forth in writing and executed by the District and the Contractor in the same manner and with the same formality as was done for this Agreement.

14.6. **Governing Law and Venue.** All issues regarding the formation, performance and/or legal enforcement of the Contract shall be governed by and construed in accordance with the laws of the State of Colorado. Venue for the resolution of any disputes arising out of or relating to the Contract shall be in Larimer County, Colorado.

14.7. **No Third-Party Beneficiary.** Enforcement of the terms and conditions of this Agreement, and all rights of action relating to such enforcement, shall be strictly reserved to the District and the Contractor. Nothing contained in this Agreement shall give or allow any claim or right of action whatsoever by any third person other than the District or the Contractor. It is the express intent of the parties that any third person receiving services or benefits pursuant to this Agreement shall be deemed an incidental beneficiary only.

14.8. **Attorney Fees and Costs.** In the event it becomes necessary for either party to institute litigation or mutually agreed-upon arbitration proceedings to enforce any provision of this Agreement, the substantially prevailing party in such litigation or arbitration shall receive, as part of any judgment or award entered, its reasonable attorney fees and costs, including expert witness fees.

14.9. **Binding Effect.** This Agreement shall be binding upon and inure to the benefit of the parties and their respective heirs, legal representatives, successors and permitted assigns.

14.10. **Headings.** The headings used in this Agreement are for convenience only and shall have no effect upon the construction or interpretation of this Agreement.

1.1. **Conflict of Terms.** In the event of any conflict of terms found between this Agreement or any other terms and conditions, end user license agreements or privacy policies, the terms of this Agreement shall prevail.

14.11. **Entire Agreement.** This Agreement constitutes the entire Agreement of the parties regarding the subject matter addressed herein and supersedes all prior Agreements, whether oral or written, pertaining to said subject matter.

14.12. **Signatures.** This Agreement may be executed and delivered via portable document format (pdf), and the pdf signature of any party shall be considered valid, binding, effective and an original for all purposes.

14.13. **Warranty of Authority.** The individuals signing below represent and warrant that they have the authority to execute this Agreement on behalf of their respective organizations and bind their respective organizations to the terms of this Agreement.

IN WITNESS WHEREOF, the District and the Contractor have signed this Agreement as of the date first set forth above.

DIRSEC, LLC

POUDRE SCHOOL DISTRICT R-1

By: _____

Name: Matthew Eubanks
Title: President

By: R David Montoya
R David Montoya (Mar 14, 2024 11:37 MDT)_____

Dave Montoya
Chief Finance Officer

By: _____

Bud Hunt
Chief Technology Officer

Exhibit A



POUDRE SCHOOL DISTRICT R-1

INVITATION FOR BID

E-RATE PALO ALTO FIREWALL OR EQUIVALENT

IFB# 24-680-006

IFB SCHEDULE

IFB Issued

December 12, 2023

Questions Due

December 19, 2023 @ 2 p.m. MT

IFB Closing Date

January 9, 2023 @ 2 p.m. MT

TABLE OF CONTENTS

INTRODUCTION AND PURPOSE

- 1.0 BACKGROUND AND CONTEXT**
- 2.0 PROJECT SCOPE AND SPECIFICATIONS**
- 3.0 EVALUATIONS AND AWARD**
- 4.0 BID PRICING**
- 5.0 SUBMITTAL REQUIREMENTS**
- 6.0 GENERAL TERMS AND CONDITIONS**
- 7.0 INSURANCE REQUIREMENTS**
- 8.0 COOPERATIVE PURCHASING EFFORTS**
- 9.0 REFERENCES**
- 10.0 BID SUBMISSION RESPONSE FORM**
- 11.0 BID CERTIFICATION FORM**

INVITATION FOR BID
E-Rate Palo Alto Firewall or Equivalent

IFB# 24-680-006

Poudre School District R-1 (the “District”) is requesting electronic sealed bids from professional and qualified vendors (“Vendor”) who can provide a Palo Alto Firewall or equivalent and licensure. These services are to meet the District’s needs as described in this Invitation for Bid (“IFB”). All interested vendors are invited to submit a Bid in accordance with the policies, procedures and dates set forth herein.

The District shall provide copies of this IFB to vendors through the electronic solicitation platform www.bidnetdirect.com (“BidNet”) where registered vendors are required to submit their electronic IFB response along with the first and last name, telephone number and e-mail address of the employee within their organization who will be designated as the District’s primary contact with respect to this IFB and the vendor’s response thereto. The District may provide copies of this IFB to other vendors upon request, who are also requested to provide the first and last name, telephone number and e-mail address of the employee within their organization who will be designated as the District’s primary contact with respect to this IFB and their response thereto.

Questions regarding this IFB must be in writing and may only be directed to the District via BidNet any time after the issuance of this IFB through and including **2:00 p.m. MT on December 19, 2023**. Questions received after the date/time and/or not submitted electronically through BidNet may not be addressed.

Each question submitted, as well as the District’s response thereto, shall be provided in a questions and answers document/addendum via BidNet.

Note: Each question must be submitted individually. Multiple questions per entry may not be answered.

The District will only accept and consider electronically submitted Bids from vendors, which must be submitted and received in BidNet on or before **2:00 p.m. MST on January 9, 2023**, at which time the submission portal will close, and no further submissions will be allowed or considered. It is the sole responsibility of the service provider to see that the bids are submitted through BidNet by the submission deadline.

At no time during the solicitation process will communication regarding this IFB be permitted with any District employee other than the Procurement Agent named below until an award has been announced. Communication with a District employee other than the Procurement Agent named below may disqualify your Bid from consideration.

Sales Prohibited/Conflict of Interest: No officer, employee, or member of the School Board, shall have a financial interest in the sale to the District of any real or personal property, equipment,

material, supplies or services where such officer or employee exercises directly or indirectly any decision-making authority concerning such sale or any supervisory authority over the services to be rendered. This rule also applies to subcontracts with the District.

Soliciting or accepting any gift, gratuity favor, entertainment, kickback, or any items of monetary value from any person who has or is seeking to do business with the District is prohibited.

Collusive or sham proposals: Any proposal deemed to be collusive, or a sham proposal will be rejected and reported to authorities as such. Your authorized signature on this proposal assures that such proposal is genuine and is not a collusive or sham proposal.

The District reserves the right to reject any and all proposals and to waive any irregularities or informalities.

Sincerely,

Kristin Thetford
Purchasing and Contract Manager
Strategic Sourcing Department
kthetford@psdschools.org

1.0 BACKGROUND AND CONTEXT

Poudre School District is looking for a Vendor or Vendors who can provide a Palo Alto Firewall or equivalent and licensure.

Poudre School District is a high-performing district, covering more than 1,800 square miles in northern Colorado with diverse school settings. The District's instructional program is centered around District Ends, under the Policy Governance model, developed to support a comprehensive curriculum.

While more than 70% of the District's families choose to send their children to their neighborhood school, the District does support school choice and offers a wide spectrum of educational programs to fit any child's needs. Program options include International Baccalaureate, Core Knowledge, Bilingual/Dual Language Immersion, Hybrid/Online, Expeditionary Learning, Science, Technology, Engineering and Math (STEM) along with extra-curriculars and athletics. The District has two (2) Leadership in Energy and Environmental Design (LEED) certified school buildings and over 30 Energy Star awards and supports operational sustainability in all areas of work.

Our Schools:

- 32 elementary schools
- 10 middle schools
- 4 comprehensive high schools
- 2 combined middle/high schools
- 6 option (100% choice) schools
- 3 alternative high schools
- 5 charter schools
- 1 online school

2.0 PROJECT SCOPE AND SPECIFICATIONS

- 2.1 The District intends to award this solicitation to a single submitter.
- 2.2 Supplier shall submit the following information with its bid response for each device.
 - 2.2.1 Brand and model
 - 2.2.2 Supplier part number
 - 2.2.3 Technical details / build sheet
 - 2.2.4 Current lead time
 - 2.2.5 Warranty information
- 2.3 All pricing shall include shipping, handling, freight charges, and inside delivery.
- 2.4 Manufacturers shall either use the “direct distribution channel” to sell directly to the District or distribute its products through VARs. Any VAR or Partner that the manufacturer chooses to work with MUST have local sales and local support personnel within the State of Colorado.
- 2.5 Quantities listed are the District’s best estimate and do not obligate the District to order or accept more than its actual requirements as determined by actual needs and availability of appropriated funds. The District reserves the right to adjust the quantities ordered in conjunction with this IFB.
- 2.6 All equipment covered by this solicitation must meet both current and proposed future technical specifications for Statewide online assessments. Details are available from Colorado Department of Education (CDE) assessments website at:

<http://www.cde.state.co.us/assessment/newassess-dtc>
- 2.7 Product changes must be submitted to and approved by the District’s Information Technology Department in writing prior to implementing any changes.
- 2.8 Delivery
 - 2.8.1 With Poudre School District Board of Education approval, the District anticipates beginning to issue purchase orders resulting from this IFB for desired devices no earlier than April 1st, 2024.

- 2.8.2 For all deliveries, forty-eight (48) hour advanced delivery notification prior to delivery must be given to the designated District point of contact. Notification must include day(s) of delivery as well as delivery window and approximate time to offload the delivery.
- 2.8.2.1 Deliveries shall be made Monday through Friday, 8 a.m. – 3 p.m. MST excluding holidays. Deliveries made outside of this window will not be accepted. Any costs associated with deliveries that are not accepted will be the sole responsibility of the Supplier.
- 2.8.3 Pricing and deliveries are to be FOB destination freight prepaid and shall require inside delivery unless otherwise specified in this solicitation. Title and risk of loss shall pass to the District upon inspection and written acceptance. Accordingly, the total unit cost of each item bid, shall include all handling, shipping, and freight charges.
- 2.8.4 If the Supplier experiences a back order of items from its Distributor or Manufacturer, the Supplier shall ensure that such back orders are filled within a reasonable period of time. The Supplier shall not invoice the District for back ordered items until items are delivered and accepted by an authorized District representative. The District shall determine what constitutes a reasonable period of time and may verbally cancel back orders, seek the items from another Supplier, and charge the original Supplier for any re- procurement costs.
- 2.8.5 The District shall not incur demurrage charges from the awarded Supplier who may choose to store product on an interim basis until delivery can take place. Any rental, storage, or demurrage charges are the responsibility of the awarded Supplier.
- 2.8.6 Supplier shall enclose a complete packing slip or delivery ticket with any items to be delivered in conjunction with this solicitation. The packing slip shall be attached to the shipping carton(s) which contain the items and shall be made available to the District's authorized representative during delivery.
- 2.8.6.1 The packing slip or delivery ticket shall include, at a minimum, the purchase order number, date of order, total number of boxes contained in the order (e.g., Box 5 of 10), a complete listing of items being delivered and corresponding

quantities, back-ordered quantities, and estimated delivery date of the backorders, if applicable and allowed.

2.8.6.2 Packing slip which includes the order number must be attached to the sides of the boxes contained on pallets, so they are easily accessible and are not hidden when boxes and/or pallets are stacked.

3.0 EVALUATIONS AND AWARD

- 3.1 Award shall be made to the most responsive and responsible Suppliers meeting the specifications and deemed to be in the best interest of the District.
 - 3.1.1 Final evaluation may be based on, but not limited to price, delivery time, warranty, adherence to specifications, and previous experience with similar projects.
 - 3.1.2 Those bids that are clearly non-responsive or incomplete to the stated requirements may be eliminated prior to evaluation.
- 3.2 All changes in bid documents shall be through written addenda and shall be posted to BidNet.
 - 3.2.1 Amendments or clarifications to the submitted bids not requested by the District will not be accepted, nor considered in awarding the agreement.
- 3.3 During the evaluation process, the District reserves the right, where it may serve the District's best interest, to request additional information, or clarifications from bidders, or to allow corrections of errors or omissions. Amendments or clarifications to submitted response not requested by the District will not be accepted, nor considered following the opening of the response.
- 3.4 Responses to this solicitation will be independently evaluated by an evaluation committee to be established for such purpose.
- 3.5 Responses submitted will be evaluated using pre-determined rating criteria. Those responses that are clearly non-responsive to the stated requirements may be eliminated prior to the evaluation. Prior to response submission, bidders are encouraged to review the requirements stated in this solicitation document and BidNet for any related addenda to ensure requirements are incorporated in their responses.
- 3.6 The District reserves the right to negotiate further, request additional information or enter into an agreement with one (1) or more Vendors. The District may make such inquiries and conduct such investigations as it deems necessary to determine the qualifications and ability of the Vendor(s) to provide the services or products called

for under the Solicitation and/or represented in the Vendor(s)'s response. Vendor(s) shall provide information in a timely manner to the District in connection with such inquiries and investigations.

- 3.7 Should the District determine in its sole discretion that only one (1) Vendor is fully qualified or that one (1) Vendor is clearly more highly qualified than the others under consideration, an agreement may be negotiated and awarded to that Vendor.
- 3.8 For the purposes of solicitation evaluation, bidders must indicate any variances to the specifications and terms and conditions, no matter how slight. If variations are not stated in the bidder's response, it shall be construed that the proposal fully complies with the specifications and terms and conditions. Notwithstanding the above, it is hereby agreed and understood that the District reserves the right to reject these variations if they individually or, as a whole, do not meet the standards established in the specifications.
- 3.9 Modification to this document, exhibits or addenda will be considered invalid will not accepted in any format by the District, and may be cause for disqualification. Proposed modifications may be submitted through BidNet with the submission of a Bid response. Proposed modifications are not considered as accepted unless formally accepted in writing by the procurement agent prior to the intent to award. Submission of a modification, and an intent to award from a solicitation shall not be considered in any way, an acceptance of any proposed modifications by the Vendor.
- 3.10 Award of contract shall be made to the responsive and responsible Vendor meeting the specifications and as deemed to be in the best interests of the District. Interviews may be requested with one or more respondents. Final evaluation may be based on, but not limited to, any or all of the following: price, adherence to specifications, performance, previous experience with similar projects, references, product availability and delivery time. Those Bids that are clearly non-responsive to the stated requirements may be eliminated prior to this evaluation.
- 3.11 This solicitation, or submitted agreement from Vendor, does not commit the District to award a contract or to pay any costs incurred in the preparation of a proposal or to procure a contract for the services. The District reserves the right to accept or reject any or all proposals received as a result of this request or to cancel in part or in its entirety this solicitation if it is deemed to be in the best interest of the District. The District reserves the right to accept any portion of the proposal, or the entire proposal as deemed in the best interest of the District.
- 3.12 The successful Vendor(s) will be required to enter into a negotiated agreement with the District prior to the start of work.
- 3.13 The agreement language will control over any language contained within with the IFB that conflicts with the signed and fully executed agreement.

4.0 BID PRICING

- 4.1 Supplier shall complete and submit the table below. Technical details / build sheet pages shall be submitted with bid form. All lines must be completed (this table is provided in section 10.0).

Asset	Product/Model #	Description	Quantity	Price
Next Generation Firewall	PAN-PA-5410-AC or equivalent	Palo Alto Networks PA-5410 with redundant AC power supplies or equivalent	2	
License	PAN-PA-5410-GP-HA2 or equivalent	PA-5410, GlobalProtect subscription 1 year or equivalent	2	
License	PAN-PA-5410-WF-HA2 or equivalent	PA-5410, WildFire subscription 1 year or equivalent	2	
License	PAN-PA-5410-ADVURL-HA2 or equivalent	PA-5410, Advanced URL Filtering subscription 1 year or equivalent	2	
License	PAN-PA-5410-ATP-HA2 or equivalent	PA-5410, Advanced Threat Prevention subscription 1 year or equivalent	2	
License	PA-SVC-PREM-5410 or equivalent	PA-5410, Premium Support 1 year or equivalent	2	

5.0 SUBMITTAL REQUIREMENTS

As set forth in more detail below, the District is requiring the following information from all potential Vendors as part of their response as it relates to the content of this IFB:

- 5.1 All successful bid submissions must describe how they will address each of the items the Project Scope and Specifications in Section 2.0.
- 5.2 All Vendors must fill out and submit the included Reference form in Section 9.0, highlighting any K-12 experience.
- 5.3 All Vendors must fill out and submit the included Bid Submission Response Form in Section 10.0.
- 5.4 By signature of the Bid Certification Form in Section 11.0, contained within this IFB, and accepted submission through BidNet to this solicitation, the Vendor certifies that submission of this IFB is made without any previous understanding, agreement, or connection either with any persons, firms or corporations offering a IFB for the same items or with the District.
- 5.5 Bid responses shall contain a signature of an authorized representative in the space provided on the Bid Certification Form.
- 5.6 The Vendor through submission of the Bid Certification Form certifies that this solicitation is in all respects fair, without outside control, collusion, fraud, or otherwise illegal action.

- 5.7 Submission of a bid response is deemed as acceptance of all terms, conditions and specifications contained in the solicitation package initially provided to the Vendor.
- 5.8 It shall be the sole responsibility of the Vendor to ensure their Bid is submitted through BidNet by the submission deadline. Late responses will not be accepted.

6.0 GENERAL TERMS AND CONDITIONS

- 6.1 Information and materials submitted in response to this solicitation may be considered public records subject to disclosure under the Colorado Open Records Act ("CORA"), C.R.S. §§ 24-72-200.1 to -205.5. Information and materials that the vendor believes are confidential and not subject to disclosure under CORA must be submitted separately with a citation to the section of CORA and any other relevant law under which the vendor believes they are confidential. The District, not vendor, shall determine whether information and materials so identified will be withheld as confidential, but will inform the vendor in advance of disclosure to give it an opportunity to take legal action to protect its interests vis-à-vis the party making the CORA request.
- 6.2 Each Vendor, its employees, representatives and subcontractors agree to abide by all applicable Federal, State and Local codes, laws, rules and regulations.
- 6.3 All issues regarding the formation, performance and/or legal enforcement of the contract shall be governed by and construed in accordance with the laws of the State of Colorado. Venue for the resolution of any disputes arising out of or relating to the contract shall be in Larimer County, Colorado.
- 6.4 The District shall issue a written addendum if substantial changes, which impact the technical submission of Bids, are required. A copy of such addenda will be distributed via BidNet. In the event of conflict with the original contract documents, addenda shall govern all other contract documents to the extent specified. Subsequent addenda shall govern over prior addenda only to the extent specified.
 - 6.4.1 The Vendor shall be solely responsible for confirming receipt of all addenda prior to Bid submittal.
 - 6.4.2 Amendments or clarifications to the submitted bids not requested by the District evaluation committee will not be accepted, nor considered in awarding of the contract.
- 6.5 The District confirms and the Vendor agrees that there is no expressed or implied obligation for the District to reimburse Vendors for any expenses incurred in preparing the Vendor's response to this IFB.

- 6.6 This solicitation does not commit the District to select or contract with any bidder that provides a response, or to pay any costs incurred by bidders in responding to the solicitation or negotiating a contract.
- 6.7 The District reserves the right to reject any and all responses to this solicitation at any point in the process, to waive any irregularities and/or informalities with respect to the solicitation procedures and deadlines, and to select the bidder whose response it deems in its sole discretion to be in the best interest of the District.
- 6.8 Vendor must provide all requested information. Failure to do so may result in rejection of the response at the option of the District.
- 6.9 Bid responses must meet or exceed specifications contained in the solicitation document.
- 6.10 Vendor agrees to furnish the products or services covered as a result of this solicitation in strict accordance with the District's specifications.
- 6.11 All information and supplemental documentation required in conjunction with this solicitation shall be furnished by the Vendor with their bid responses. If the Vendor fails to supply any required information or documents, their bid response may be considered non-responsive and ineligible for award.
- 6.12 The accuracy of the bid responses is the sole responsibility of the Vendor. No changes in the bid response shall be allowed after the submission deadline, except when the Vendor can show clear and convincing evidence that an unintentional factual mistake was made, including the nature of the mistake and the price actually intended.
- 6.13 The apparent silence or omissions within this solicitation regarding a detailed description of the materials and services to be provided shall be interpreted to mean that only the best commercial practices are to prevail and that only materials and workmanship of first quality are to be used.
- 6.14 The award of this solicitation to a selected bidder is contingent upon the execution of a mutually acceptable agreement. If a mutually acceptable agreement is not executed, the District reserves the right, at its sole discretion, to negotiate with a subsequent bidder(s) who submitted a responsive and responsible response to this solicitation per the specified terms herein.
- 6.15 The District may, at its sole and absolute discretion:
 - 6.15.1 Reject any and all or parts of any or all bid responses submitted by prospective Vendors;
 - 6.15.2 Re-advertise this solicitation;

- 6.15.3 Postpone or cancel the solicitation process for this solicitation;
 - 6.15.4 Waive any irregularities or technicalities that are not qualified as a requirement for responsiveness in this solicitation or in bid responses received in conjunction with this solicitation; and/or
 - 6.15.5 Determine the criteria and process whereby bid responses are evaluated and awarded.
- 6.16 The District shall be the sole judge in determining equals in regard to quality, price and performance.
- 6.17 Vendor shall provide the services under this IFB as an independent contractor of the District. As such, Vendor shall have the right to determine how and by whom the Services will be provided and the right to provide the Services free from the direction and control of the District, subject to and consistent with the terms and conditions of a District issued purchase order or agreement.
- 6.17.1 Vendor shall be exclusively responsible for: (a) all compensation, employment tax withholdings and payments, and all fringe benefits for its employees (if any) in full compliance with all applicable federal, state and local laws; (b) all insurance coverages and benefits for its employees (if any) in full compliance with all applicable federal, state and local laws, including but not limited to pension or retirement benefits, workers' compensation, unemployment compensation, and Social Security benefits; and (c) all payments to its contractors and subcontractors for goods and/or services directly or indirectly related to this IFB.
 - 6.17.2 Nothing in this Solicitation shall be construed as creating a single enterprise, partnership, joint venture or employer-employee relationship between Vendor and the District. Vendor is not a partner, agent or representative of the District and shall not represent itself to be a partner, agent or representative of the District. The District is not a partner, agent or representative of Vendor and shall not represent itself to be a partner, agent or representative of Vendor.
 - 6.17.3 Vendor shall not attempt or purport to extend the faith and credit of the District to any third party, person or entity. Vendor acknowledges and agrees that it has no authority to enter into any contract with a third party that would bind or in any way obligate the District. The District shall not attempt or purport to extend the faith and credit of Vendor to any third party, person or entity. The District acknowledges and agrees that it has no authority to enter into any contract with a third party that would bind or in any way obligate Vendor.

- 6.18 The Vendor shall not assign an agreement, as a result of this solicitation, or any of its rights, interests or obligations without the prior written consent of the District. The consent may be withheld for any reason or no reason as determined by the District in its sole discretion.
- 6.19 It is agreed that no otherwise qualified vendor shall be excluded from participating in, be denied the benefits of, or be subject to discrimination, including harassment, under any provision of this IFB on the basis of race; creed; color; national origin; age; sex; pregnancy; physical recovery from childbirth or a related condition; sexual orientation; marital status; veteran status; religion; genetic information; gender expression; gender identity; ancestry; or disability.
- 6.20 Vendors may offer a cash discount for prompt payment; however, such discounts shall not be considered in determining the lowest net cost for the Bid evaluation purposes.
- 6.21 **Invoicing.** The District utilizes an online vendor portal to collect, validate, and manage vendor information, including but not limited to tax identification verification, sanction monitoring, receipt of W9 and other required forms. Prior to the issuance of a purchase order or payment, the Contractor will be required to complete the online registration process through the online vendor portal, which shall include the Contractor providing all required documentation, and receiving approval of the submission of all documentation, including but not limited to, taxpayer identification number and bank account verification.
- 6.21.1 Invoices for Services provided shall be submitted directly to the District's accounts payable department within thirty (30) days of completion of Services. Invoices for such Services shall include (a) date on which Services were provided, (b) the District Location for which the Service were provided, (c) details of Products delivered, (d) and purchase order number. All invoices must be submitted within 30 days of fiscal year end June 30 and may not include items received by the District outside of the fiscal year July 1 – June 30.
- 6.21.2 Invoices received from the Contractor pursuant to this Agreement will be reviewed and approved by the District's representative, indicating that services have been rendered in conformity with the Agreement and then will be sent to the Finance Department for payment. Payment for Services not approved by the District in writing, shall not be considered valid and the District will not be responsible for covering associated costs. Invoices will generally be paid within thirty (30) days following the District representative's approval.
- 6.21.3 Invoices which do not conform with the agreement will be paid thirty (30) days from receipt of a revised and corrected invoice.

6.21.4 Invoices shall be sent to ap@psdschools.org.

6.21.5 The District is a political subdivision of the State of Colorado and considered a governmental entity for tax classification purposes. The District is exempt from city, county, and state sales tax. The District's state tax exempt number is 98-03335 and the District's Federal Tax Identification Number (TIN) is 84-6013733.

6.21.6 If the contract results in the right to use an asset, the Contractor shall provide the District, if requested, documentation necessary to facilitate the District's compliance with the Governmental Accounting Standards Board ("GASB") issued GASB Statement No. 87, Leases.

6.22 **Governing Law.** All issues regarding the formation, performance and/or legal enforcement of the Contract shall be governed by and construed in accordance with the laws of the State of Colorado. Venue for the resolution of any disputes arising out of or relating to the Contract shall be in Larimer County, Colorado.

6.23 **Equal Opportunity.** It is agreed that no otherwise qualified Contractor shall be excluded from participating in, be denied the benefits of, or be subject to discrimination, including harassment, under any provision of this Agreement on the basis of race; creed; color; national origin; age; sex; pregnancy; physical recovery from childbirth or a related condition; sexual orientation; marital status; veteran status; religion; genetic information; gender expression; gender identity; ancestry; or disability.

7.0 INSURANCE REQUIREMENTS

Vendor shall procure and maintain the required insurance specified below for the duration of this Agreement, which insurance shall be written for not less than the amounts specified or greater if required by law. The District's receipt of a Certificate of Insurance from the Vendor with limits and or coverages that do not meet the requirements does not waive the requirements and the Vendor shall still be responsible for the limits and coverages stated in this Agreement. Specified coverages and amounts may be provided by a combination of a primary policy plus an umbrella or following form excess policy. All insurance shall be with a carrier licensed in the state of Colorado and shall have a minimum A.M. Best rating of A- VII. Vendor shall furnish the District's Director of Records and Risk Management with certificates of the required insurance prior to the District's approval and signing of this Agreement, and with renewal certificates prior to the expiration of any required insurance that expires during the term of this Agreement. Memorandums of Insurance will not be accepted. Certificates of Insurance and all communication regarding insurance shall be sent to:

Poudre School District
Attention: Risk Management
2407 Laporte Ave
Ft. Collins, CO 80521

Email Certificate to: COI@psdschools.org

Any insurance and/or self-insurance carried by the District is excess of the coverage extended to the District by Vendor. Vendor shall provide at least thirty (30) days' advance written notice to the District prior to cancellation, change of coverage, or non-renewal. The insurance requirements specified in this section 10 shall not reduce the indemnification liability that Vendor has assumed herein.

Commercial General Liability

Minimum Limits

- Each Occurrence Bodily Injury & Property Damage \$1,000,000
- General Aggregate \$2,000,000
- Products/Completed Operations Aggregate \$2,000,000
- Personal/Advertising Injury \$2,000,000
- Product Recall Expense \$500,000
- Coverage must be written on an "occurrence" basis.
- Poudre School District R-1 and its elected officials, employees, agents, and volunteers shall be named as an additional insured or covered as an additional insured by way of a blanket endorsement and shall be insured to the full limits of liability purchased by the Vendor even if those limits of liability are in excess of those required by this Agreement.

Professional Liability

Minimum Limits

- a. Each Occurrence or Wrongful Act Limit \$1,000,000
- b. Annual Aggregate Limit \$3,000,000
- c. In the event that the Professional Liability insurance required by this Agreement is written on a claims-made basis Provider warrants that any retroactive date under the policy shall precede the effective date of this Agreement and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of three (3) years beginning at the time work under this Agreement is completed.
- d. Provider must provide evidence of the extended reporting period coverage at the end of the project and before all final payments to the Provider is made.

Technology Errors and Omissions Liability (Professional Liability, including Network Security and Privacy Liability)

Minimum Limits

- Per Loss \$1,000,000
- Aggregate \$3,000,000

- Liability extends for a period of three (3) years beginning at the time work under this Agreement is completed. Provider shall maintain continuous coverage, as required by the Agreement, for this period.

The insurance shall provide coverage for:

- Liability arising from theft, dissemination and/or use of confidential information (defined term including but not limited to bank account, credit card account, personal information such as name, address, social security numbers, etc. information) stored or transmitted in electronic form.
- Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party to gain access to Provider's services including denial of service, unless caused by a mechanical or electrical failure.
- Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a District or third person's computer, computer system, network, or similar computer related property and the data, software, and programs thereon.

Crime Coverage

Minimum Limits

Per Loss

\$1,000,000

The policy shall include:

- Coverage for all directors, officers, agents, and employees of the Supplier.
- Employee dishonesty, forgery and alteration, monies and securities, and computer (cyber) crime.
- Extended theft and mysterious disappearance.
- The policy shall not contain a condition requiring an arrest and conviction.
- Policy must be endorsed to cover Third Party Fidelity and include Poudre School District R-1 as a Loss Payee.

Workers' Compensation and Employers' Liability

If Provider is exempt under the Colorado Workers' Compensation Act, this requirement will be waived if proof a current Workers' Compensation Coverage Rejection is on file with the Colorado Department of Labor and Employment, Division of Worker's Compensation and a copy is submitted to the District.

Minimum Limits

- State of Colorado Statutory
 - Employer's Liability
- \$100,000 Each Accident
\$500,000 Disease – Policy Limit

\$100,000 Disease – Each Employee

Waiver of subrogation in favor of Poudre School District R-1.

The Vendor shall indemnify and hold harmless the District and the District's Board members, employees, representatives and agents from and against any and all liability arising from any suit, action, third party claims, grievance, or proceeding, including all attorneys' fees, costs and expenses, incurred as a result of any negligent or intentional act or omission by Vendor, or its employees, agents, Subcontractors, or assignees related to the terms of this Agreement and any Services provided under this Agreement.

It is specifically understood and agreed that nothing contained in this Agreement shall be construed as an express or implied waiver by the District of any of the immunities, rights, benefits, protections, or other provisions of the Colorado Constitution or Governmental Immunity Act, C.R.S. §§ 24-10-101 et seq, as now or hereafter amended.

8.0 COOPERATIVE PURCHASING EFFORTS

The District is a member of, or affiliated with, several regional professional procurement organizations within Colorado and Wyoming. These organizations are comprised of governmental purchasing agents, or agency representatives responsible for the purchasing function. These organizations include:

- 8.1 Colorado Educational Purchasing Council (CEPC) - A cooperative purchasing organization comprised of purchasing agents/buyers representing all Colorado public school districts.
- 8.2 Multiple Assembly of Procurement Officials (MAPO) - A cooperative purchasing organization comprised of procurement representatives from state, county, municipal, governments, special districts, or school districts along the front range of the Rocky Mountains in Colorado.
- 8.3 Rocky Mountain Governmental Purchasing Association (RMGPA) - A chapter member of the National Institute of Governmental Purchasing (NIGP), consisting of public procurement professionals and their representative agencies which include approximately 100 state, county, and municipal governments; school districts and higher education; and other special districts.
- 8.4 Members of these organizations, at their discretion, may request use of the contracts or awards that result from this solicitation. Each governmental entity which uses a contract resulting from this solicitation would establish its own contract, issue its own orders, schedule deliveries, be invoiced individually, make its own payments, and issue its own exemption certificates as required by the Vendor. It is understood and agreed that the Poudre School District R-1 is not a legally binding party to any contractual agreement made between another governmental entity and the Vendor as a result of this solicitation. The District shall not be liable for any costs or damages

incurred by any other entity. Usage by any other entity shall not have a negative impact on the District in the current term or in any future terms.

-Intentionally Left Blank-

9.0 **REFERENCES**

References – List three (3) references for which your company has completed similar services for projects of similar scope. Colorado K-12 public school references are preferred, if available.

Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

10.0 **BID SUBMISSION RESPONSE FORM**

Vendors must complete and submit all lines of the following table as part of the bid submission packet and equivalent submissions must be specified with OEM and model information:

Asset	Product/Model #	Description	Quantity	Price
Next Generation Firewall	PAN-PA-5410-AC or equivalent	Palo Alto Networks PA-5410 with redundant AC power supplies or equivalent	2	
License	PAN-PA-5410-GP-HA2 or equivalent	PA-5410, GlobalProtect subscription 1 year or equivalent	2	
License	PAN-PA-5410-WF-HA2 or equivalent	PA-5410, WildFire subscription 1 year or equivalent	2	
License	PAN-PA-5410-ADVURL-HA2 or equivalent	PA-5410, Advanced URL Filtering subscription 1 year or equivalent	2	
License	PAN-PA-5410-ATP-HA2 or equivalent	PA-5410, Advanced Threat Prevention subscription 1 year or equivalent	2	
License	PA-SVC-PREM-5410 or equivalent	PA-5410, Premium Support 1 year or equivalent	2	

11.0 CERTIFICATION FORM

E-Rate Palo Alto Firewall or Equivalent IFB #24-680-006

The District will only accept and consider electronically submitted proposals from Vendors, which must be submitted and received in the www.bidnetdirect.com electronic solicitation portal on or before **January 9, 2023, 2:00 p.m. MT.**

The undersigned hereby affirms that:

- Vendor is a duly authorized agent of the company issuing this response and that all information provided in the response is true and accurate.
- Vendor has read the conditions and technical specifications, which were made available to the company in conjunction with this IFB, and fully understands and accepts these terms unless specific variations have been expressly listed in the response.
- Vendor will adhere to all terms and conditions and provide, at a minimum, all services as expressed in the IFB and/or the company's response to the IFB.
- Vendor meets or exceeds all of the required criteria as specified by this IFB, or if not, has submitted a Justification for Consideration addressing any failure to meet the criteria.
- Vendor's response is being offered independently of any other Vendor and in full compliance with the terms specified in the IFB.

Company Name: _____

Signature of Agent: _____

Printed Name: _____

Title: _____

E-mail address: _____

Mailing address: _____

Phone Number: _____

Contact Person: _____

(If different from Agent – include e-mail address and phone number)

NOTE: Responses submitted without the signature of an authorized agent of the company may be considered non-responsive and ineligible for the award.

-Intentionally Left Blank-

Exhibit B



**POUDRE SCHOOL DISTRICT R-1
PROCUREMENT SERVICES
ATTN: KRISTIN THETFORD
2407 LAPORTE AVE
FT. COLLINS, CO 80521**

**INVITATION FOR BID (IFB) #24-680-006
E-RATE PALO ALTO FIREWALL OR EQUIVALENT
RESPONSE FROM DIRSEC, INC. AND PALO ALTO NETWORKS**

ORIGINAL BID

**PREPARED BY:
DADE MYRES – DIRSEC, LLC
ART WALKER – DIRSEC, LLC
DEAN JANSEN – PALO ALTO NETWORKS
JASON WELTON – PALO ALTO NETWORKS**

JANUARY 9, 2024

**DIRSEC, LLC
357 MCCASLIN BLVD., SUITE 200
LOUISVILLE, CO 80027
(800) 741-0354
WWW.DIRSEC.COM**

TABLE OF CONTENTS

1.	PROJECT SCOPE AND SPECIFICATIONS	1
2.	REFERENCE FORM	5
3.	BID SUBMISSION RESPONSE FORM	6
3.1	BID SUBMISSION RESPONSE FORM	6
3.2	PRICING DETAIL – ONE YEAR PRICING OPTION	7
3.3	PRICING DETAIL – THREE YEAR PRICING OPTION	8
4.	BID CERTIFICATION FORM.....	9
	APPENDIX A – PRODUCT DATA SHEETS AND INFORMATION	10



January 9, 2024

Kristin Thetford
Purchasing and Contract Manager
Poudre School District R-1
2407 Laporte Ave
Fort Collins, CO 80521

Thank you for allowing DirSec, Inc. the opportunity to respond to your Invitation for Bid **IFB #24-680-006** for **E-Rate Palo Alto Firewall or Equivalent**. Enclosed is DirSec's submission featuring firewalls from Palo Alto Networks. DirSec, Inc. is an authorized Palo Alto Networks Innovator partner.

Company Information: Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

Company Information: DirSec, LLC

DirSec, Inc. is a reseller and integrator of IT security solutions for the Enterprise, Small to Medium Business, Education and Government. The company has been in business since 2001 and offers decades of industry expertise to its clients throughout the United States. By focusing on long-term relationships, DirSec provides critical security technologies and services that protect vital information.

We look forward to working with you and your staff on this project.

Best regards,

A handwritten signature in black ink that reads 'Dade Myres'.

Dade Myres
Director, SLED Sales
DirSec, LLC
303-581-7915
dmyres@dirsec.com

1. PROJECT SCOPE AND SPECIFICATIONS

Section	Requirement	Response
2.1	The District intends to award this solicitation to a single submitter.	DirSec, LLC and Palo Alto Networks have read and acknowledge this section.
2.2	Supplier shall submit the following information with its bid response for each device.	See below for details
2.2.1	Brand and model	Brand and model information is included in Section 3, "Bid Submission Response Form"
2.2.2	Supplier part number	Supplier part number information is included in Section 3, "Bid Submission Response Form"
2.2.3	Technical details / build sheet	Technical details and build sheets are included in Appendix A, "Product Data Sheets and Information"
2.2.4	Current lead time	Current lead time for Palo Alto Networks PA-5410 is two weeks.
2.2.5	Warranty information	Current Palo Alto Networks Product Warranty and Product Service Model may be found at: https://www.paloaltonetworks.com/services/support/product-warranty Palo Alto Networks Product Warranty and Hardware Service Model All Palo Alto Networks products are covered by a 90 day software and 12 month hardware warranty. To take advantage of our warranty related information and updates, we encourage you to register your products through our Palo Alto Networks Support Portal (https://support.paloaltonetworks.com). Other details about your software and hardware warranty are outlined below. Your Software Warranty The standard warranty for software is 90 days. During the 90 day warranty period, you are entitled to all software updates (bug fixes, maintenance releases, and feature upgrades) for your particular software product. You can download the software updates through our software update portal embedded in your device web interface, or through our password-protected Palo Alto Networks support web site. You must create an account and register your device for access into the support portal. Hardware Warranty The standard warranty for our hardware is 12 months from the date of shipment. This is a 'return

Section	Requirement	Response
		and repair' hardware service model. If a Return Merchandise Authorization ("RMA") is required during the 12 month period, we will work with you to confirm the hardware problem and issue an RMA number to be used when you ship the product to Palo Alto Networks. Hardware Return Procedures You should obtain a RMA number for the product that you wish to return to us, Palo Alto Networks by contacting Support via telephone or by opening a case with Palo Alto Networks Support. You must ship the product in the original packaging (shipping damage that occurs from insufficient packaging is not covered), record the RMA number on the shipping label, and send the product to the specified Palo Alto Networks location. You will be responsible for all shipping costs incurred in returning the defective product. Products will be repaired (or replaced) and shipped within 10 business days from receipt of the defective product by us. We will pay all costs incurred in shipping the repaired or replacement product to you, except that if you are located outside the United States, you will be responsible for any taxes, duties, fees or other charges assessed in connection with importing the repaired or replaced product into your country of destination. Warranty and Service Model Restrictions The applicable warranties and Service Model do not apply if the product: • Has been altered, except by an authorized Palo Alto Networks, Inc. • Has not been installed, operated, repaired, or maintained in accordance with the instructions supplied by Palo Alto Networks, Inc. • Has been subjected to unreasonable physical or electrical stress, misuse, negligence, accidental damage, or damage caused by an Act of God. • Is being used in a different country than where the original purchase or activation occurred.
2.3	All pricing shall include shipping, handling, freight charges, and inside delivery.	Shipping, handling, freight charges and inside delivery is included in the pricing contained in Section 3, "Bid Submission Response Form".
2.4	Manufacturers shall either use the "direct distribution channel" to sell directly to the District or distribute its products through VARs. Any VAR or Partner that the	DirSec, LLC is an Innovator-level Value Added Reseller (VAR) of Palo Alto Networks.

Section	Requirement	Response
	manufacturer chooses to work with MUST have local sales and local support personnel within the State of Colorado.	DirSec, LLC is headquartered in Louisville, CO and has local sales and local support personnel within the State of Colorado.
2.5	Quantities listed are the District's best estimate and do not obligate the District to order or accept more than its actual requirements as determined by actual needs and availability of appropriated funds. The District reserves the right to adjust the quantities ordered in conjunction with this IFB.	DirSec, LLC and Palo Alto Networks have read and acknowledge this section.
2.6	All equipment covered by this solicitation must meet both current and proposed future technical specifications for Statewide online assessments. Details are available from Colorado Department of Education (CDE) assessments website at: http://www.cde.state.co.us/assessment/newassess-dtc	Palo Alto Networks firewalls and associated Cloud Delivered Security Services (GlobalProtect, WildFire, Advanced URL Filtering, Advanced Threat Protection, etc.) are used in school districts throughout Colorado. Details regarding other DirSec/Palo Alto Networks customers can be found in Section 2, "References"
2.7	Product changes must be submitted to and approved by the District's Information Technology Department in writing prior to implementing any changes.	DirSec, LLC and Palo Alto Networks have read and acknowledge this section.
2.8	Delivery	See below for details
2.8.1	With Poudre School District Board of Education approval, the District anticipates beginning to issue purchase orders resulting from this IFB for desired devices no earlier than April 1st, 2024.	DirSec, LLC and Palo Alto Networks have read and acknowledge this section.
2.8.2	For all deliveries, forty-eight (48) hour advanced delivery notification prior to delivery must be given to the designated District point of contact. Notification must include day(s) of delivery as well as delivery window and approximate time to offload the delivery.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.
2.8.2.1	Deliveries shall be made Monday through Friday, 8 a.m. – 3 p.m. MST excluding holidays. Deliveries made outside of this window will not be accepted. Any costs associated with deliveries that are not accepted will be the sole responsibility of the Supplier.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.
2.8.3	Pricing and deliveries are to be FOB destination freight prepaid and shall require inside delivery unless otherwise specified in this solicitation. Title and risk of loss shall pass to the District upon inspection and written acceptance. Accordingly, the total unit cost of each item bid, shall include all handling, shipping, and freight charges.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.

Section	Requirement	Response
2.8.4	If the Supplier experiences a back order of items from its Distributor or Manufacturer, the Supplier shall ensure that such back orders are filled within a reasonable period of time. The Supplier shall not invoice the District for back ordered items until items are delivered and accepted by an authorized District representative. The District shall determine what constitutes a reasonable period of time and may verbally cancel back orders, seek the items from another Supplier, and charge the original Supplier for any re- procurement costs.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.
2.8.5	The District shall not incur demurrage charges from the awarded Supplier who may choose to store product on an interim basis until delivery can take place. Any rental, storage, or demurrage charges are the responsibility of the awarded Supplier.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.
2.8.6	Supplier shall enclose a complete packing slip or delivery ticket with any items to be delivered in conjunction with this solicitation. The packing slip shall be attached to the shipping carton(s) which contain the items and shall be made available to the District's authorized representative during delivery.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.
2.8.6.1	The packing slip or delivery ticket shall include, at a minimum, the purchase order number, date of order, total number of boxes contained in the order (e.g., Box 5 of 10), a complete listing of items being delivered and corresponding quantities, back-ordered quantities, and estimated delivery date of the backorders, if applicable and allowed.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.
2.8.6.2	Packing slip which includes the order number must be attached to the sides of the boxes contained on pallets, so they are easily accessible and are not hidden when boxes and/or pallets are stacked.	DirSec, LLC and Palo Alto Networks have read, acknowledge, and will comply with this requirement.

2. REFERENCE FORM

9.0 REFERENCES

References – List three (3) references for which your company has completed similar services for projects of similar scope. Colorado K-12 public school references are preferred, if available.

Company Name Academy School District 20

Address 1110 Chapel Hills Dr, Colorado Springs, CO 80920

Contact Person Shelley Kooser - CIO

Telephone (719) 234-1200

Email shelley.kooser@asd20.org

Describe type of work/service performed or items supplied Palo Alto Networks

PA-5410 firewalls with Threat Protection, URL Filtering and Panorama

Company Name Boulder Valley School District

Address 6500 Arapahoe Rd, Boulder, CO 80303

Contact Person Chris Paschke - Director, Information Security

Telephone (303) 884-4700

Email christopher.paschke@bvdsd.org

Describe type of work/service performed or items supplied Palo Alto Networks

PA-5260 firewalls with Threat Prevention and URL Filtering

Company Name Jefferson County Schools

Address 1829 Denver West Dr, Golden, CO 80401

Contact Person Daniel Clements - Manager, Infosec

Telephone

Email daniel.clements@jeffco.k12.co.us

Describe type of work/service performed or items supplied Palo Alto Networks

5450 firewalls with Threat Prevention, URL Filtering, Panorama and Cortex XDR.

3. BID SUBMISSION RESPONSE FORM

NOTE: As part of the Invitation For Bid, DirSec, LLC has also included a three-year pricing option, detailed in Section 3.3 below.

3.1 Bid Submission Response Form

10.0 BID SUBMISSION RESPONSE FORM

Vendors must complete and submit all lines of the following table as part of the bid submission packet and equivalent submissions must be specified with OEM and model information:

Asset	Product/Model #	Description	Quantity	Price
Next Generation Firewall	PAN-PA-5410-AC or equivalent	Palo Alto Networks PA-5410 with redundant AC power supplies or equivalent	2	\$78,930.56
License	PAN-PA-5410-GP-HA2 or equivalent	PA-5410, GlobalProtect subscription 1 year or equivalent	2	\$19,358.14
License	PAN-PA-5410-WF-HA2 or equivalent	PA-5410, WildFire subscription 1 year or equivalent	2	\$29,399.94
License	PAN-PA-5410-ADVURL-HA2 or equivalent	PA-5410, Advanced URL Filtering subscription 1 year or equivalent	2	\$26,554.25
License	PAN-PA-5410-ATP-HA2 or equivalent	PA-5410, Advanced Threat Prevention subscription 1 year or equivalent	2	\$26,554.25
License	PA-SVC-PREM-5410 or equivalent	PA-5410, Premium Support 1 year or equivalent	2	\$22,649.33

3.2 Pricing Detail – One Year Pricing Option

DirSec Corporate Office
357 McCaslin Blvd. Suite 200
Louisville, CO 80027

WWW.DIRSEC.COM
Est. 2001





Quote - One Year

Quote #: Poudre_PaloAlto_122023

Date: December 20, 2023

Prepared for: *Poudre School District*

Attention:

Email:

Terms: Net 30

Quoted by: Dade Myres

E-mail: dmyres@dirsec.com

Phone: 303.588.6938

Line #	Qty	Product/ Model #	Product Description	List Unit Price	Total Retail Price	Total with Discount
1	2	PAN-PA-5410-AC	Palo Alto Networks PA-5410 with redundant	\$ 72,660.00	\$ 145,320.00	\$ 78,930.56
2	2	PAN-PA-5410-GP-1YR-HA2	PA-5410, GlobalProtect subscription	\$ 13,230.00	\$ 26,460.00	\$ 19,358.14
3	2	PAN-PA-5410-AWF-1YR-HA2	PA-5410, Advanced WildFire subscription	\$ 18,320.00	\$ 36,640.00	\$ 29,399.94
4	2	PAN-PA-5410-ADVURL-1YR-HA2	PA-5410, Advanced URL Filtering subscription	\$ 19,740.00	\$ 39,480.00	\$ 26,554.25
5	2	PAN-PA-5410-ATP-1YR-HA2	Advanced Threat Prevention subscription	\$ 19,740.00	\$ 39,480.00	\$ 26,554.25
6	2	PAN-SVC-PREM-5410-1YR	Premium support 1-year prepaid, PA-5410	\$ 13,080.00	\$ 26,160.00	\$ 22,649.33
			TERMS OF COVERAGE: 1 YEAR			
				Total	\$ 313,540.00	\$ 203,446.45

Quoted prices valid for 30 days. Quote is subject to revision or cancellation prior to acceptance by the customer. Prices quoted do not include applicable sales tax.

DirSec will only accept credit card payments for transactions that are less than \$10,000.

Representing the Best of Breed Vendors:

Cloud Data Security (Including SASE, SWG, CASB, CSPM, DLP), Next Generation Endpoint Protection and Remediation, Structured Data Security, Web Application Security, User & Entity Behavioral Analytics, Next Generation SIEM , PIM/PAM, Vulnerability Management, Security/Risk/Compliance Optimization/ Enforcement

Services include: Managed Services, Architectural Review and Design, Implementation, Upgrades

3.3 Pricing Detail – Three Year Pricing Option

DirSec Corporate Office

357 McCaslin Blvd. Suite 200

Louisville, CO 80027

WWW.DIRSEC.COM

Est. 2001

paloalto

NETWORKS

DIRSEC

Quote - Three Year

Quote #: Poudre_PaloAlto_122023

Date: December 20, 2023

Prepared for: Poudre School District

Attention:

Email:

Terms: Net 30

Quoted by: Dade Myres

E-mail: dmyres@dirsec.com

Phone: 303.588.6938

Line #	Qty	Product/ Model #	Product Description	List Unit Price	Total Retail Price	Total with Discount
1	2	PAN-PA-5410-AC	Palo Alto Networks PA-5410 with redundant	\$ 72,660.00	\$ 145,320.00	\$ 78,930.56
5	2	PAN-PA-5410-GP-3YR-HA2	PA-5410, GlobalProtect subscription	\$ 37,070.00	\$ 74,140.00	\$ 54,332.76
4	2	PAN-PA-5410-AWF-3YR-HA2	PA-5410, Advanced WildFire subscription	\$ 54,940.00	\$ 109,880.00	\$ 88,317.15
2	2	PAN-PA-5410-ADVURL-3YR-HA2	PA-5410, Advanced URL Filtering subscription	\$ 55,440.00	\$ 110,880.00	\$ 74,704.29
3	2	PAN-PA-5410-ATP-3YR-HA2	Advanced Threat Prevention subscription	\$ 55,440.00	\$ 110,880.00	\$ 74,704.29
6	2	PAN-SVC-PREM-5410-3YR	Premium support 3-year prepaid, PA-5410	\$ 39,240.00	\$ 78,480.00	\$ 67,764.34
			TERMS OF COVERAGE: 3 YEARS			
				Total	\$ 629,580.00	\$ 438,753.39

Quoted prices valid for 30 days. Quote is subject to revision or cancellation prior to acceptance by the customer. Prices quoted do not include applicable sales tax.

DirSec will only accept credit card payments for transactions that are less than \$10,000.

Representing the Best of Breed Vendors:

Cloud Data Security (Including SASE, SWG, CASB, CSPM, DLP), Next Generation Endpoint Protection and Remediation, Structured Data Security, Web Application Security, User & Entity Behavioral Analytics, Next Generation SIEM , PIM/PAM, Vulnerability Management, Security/Risk/Compliance Optimization/ Enforcement

Services include: Managed Services, Architectural Review and Design, Implementation, Upgrades

4. BID CERTIFICATION FORM

11.0 CERTIFICATION FORM

E-Rate Palo Alto Firewall or Equivalent IFB #24-680-006

The District will only accept and consider electronically submitted proposals from Vendors, which must be submitted and received in the www.bidnetdirect.com electronic solicitation portal on or before **January 9, 2023, 2:00 p.m. MT.**

The undersigned hereby affirms that:

- Vendor is a duly authorized agent of the company issuing this response and that all information provided in the response is true and accurate.
- Vendor has read the conditions and technical specifications, which were made available to the company in conjunction with this IFB, and fully understands and accepts these terms unless specific variations have been expressly listed in the response.
- Vendor will adhere to all terms and conditions and provide, at a minimum, all services as expressed in the IFB and/or the company's response to the IFB.
- Vendor meets or exceeds all of the required criteria as specified by this IFB, or if not, has submitted a Justification for Consideration addressing any failure to meet the criteria.
- Vendor's response is being offered independently of any other Vendor and in full compliance with the terms specified in the IFB.

Company Name: DirSec, LLC

Signature of Agent: *Dade Myres*

Printed Name: Dade Myres

Title: Director, SLED Sales

E-mail address: dmyres@dirsec.com

Mailing address: 357 McCaslin Blvd, Suite 200, Louisville CO 80027

Phone Number: (303) 581-7915

Contact Person: _____

(If different from Agent – include e-mail address and phone number)

NOTE: Responses submitted without the signature of an authorized agent of the company may be considered non-responsive and ineligible for the award.

-Intentionally Left Blank-

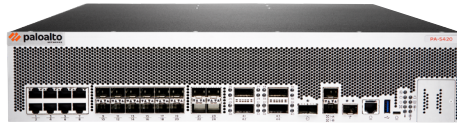
APPENDIX A – PRODUCT DATA SHEETS AND INFORMATION

This section contains the following Vendor data sheets and vendor information:

- Palo Alto Networks PA-5400 Series Firewall Data Sheet
- Palo Alto Networks GlobalProtect Data Sheet
- Palo Alto Networks WildFire Data Sheet
- Palo Alto Networks Advanced URL Filtering Data Sheet
- Palo Alto Networks Advanced Threat Protection Data Sheet
- Palo Alto Networks Premium Support Data Sheet



PA-5410



PA-5420



PA-5430



PA-5440



PA-5445

PA-5400 Series

Palo Alto Networks PA-5400 Series ML-Powered Next-Generation Firewalls—comprising the PA-5445, PA-5440, PA-5430, PA-5420, and PA-5410—are ideal for high-speed data center, internet gateway, and service provider deployments. The PA-5400 Series appliances secure all traffic, including encrypted traffic.

Highlights

- World's first ML-Powered NGFW
- Eleven-time Leader in the Gartner Magic Quadrant for Network Firewalls
- Leader in The Forrester Wave: Enterprise Firewalls, Q4 2022
- Delivers 5G-Native Security built to safeguard service provider and enterprise 5G transformation and multi-access edge computing (MEC)
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors
- Supports high availability with active/active and active/passive modes
- Delivers predictable performance with security services
- Supports centralized administration with Panorama network security management
- Maximizes security investments and prevents business disruptions with AIOps

The world's first ML-Powered Next-Generation Firewall enables you to prevent unknown threats, see, and secure everything—including the internet of things (IoT)—and reduce errors with automatic policy recommendations.

The controlling element of the PA-5400 Series is PAN-OS®, the same software that runs all Palo Alto Networks NGFWs. PAN-OS natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user regardless of location or device type. The application, content, and user—in other words, the elements that run your business—then serve as the basis of your security policies, resulting in improved security posture and reduced incident response time.

Key Security and Connectivity Features

ML-Powered Next-Generation Firewall

- Embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.
- Leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
- Uses behavioral analysis to detect IoT devices and make policy recommendations; cloud-delivered and natively integrated service on the NGFW.
- Automates policy recommendations that save time and reduce the chance of human error.

Identifies and Categorizes All Applications, on All Ports, All the Time, with Full Layer 7 Inspection

- Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (TLS/SSL). In addition, it automatically discovers and controls new applications to keep pace with the SaaS explosion with SaaS Security subscription.
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- Offers the ability to create custom App-ID™ tags for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application (e.g., files and data patterns) to block malicious files and thwart data exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all sanctioned and unsanctioned SaaS traffic on your network.
- Enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, giving you a rule set that is more secure and easier to manage.

Check out the [App-ID tech brief](#) for more information.

Enforces Security for Users at Any Location, on Any Device, While Adapting Policy Based on User Activity

- Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android mobile devices; macOS, Windows, and Linux desktops and laptops; Citrix and Microsoft VDI; and terminal servers).
- Prevents corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without any application changes.
- Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.
- Consistently authenticates and authorizes your users, regardless of location and where user identity stores live, to move quickly toward a Zero Trust security posture with Cloud Identity Engine—an entirely new cloud-based architecture for identity-based security.

Check out the [Cloud Identity Engine solution brief](#) for more information.

Prevents Malicious Activity Concealed in Encrypted Traffic

- Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, without decrypting.
- Enables control over use of legacy TLS protocols, insecure ciphers, and misconfigured certificates to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- Lets you enable or disable decryption flexibly based on URL category, source and destination zone, address, user, user group, device, and port, for privacy and regulatory compliance purposes.
- Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).
- Allows you to intelligently forward all traffic (decrypted TLS, undecrypted TLS, and non-TLS) to third-party security tools with network packet broker and optimize your network performance and reduce operating expenses.

Refer to this [decryption whitepaper](#) to learn where, when, and how to decrypt to prevent threats and secure your business.

Offers Centralized Management and Visibility

- Benefits from centralized management, configuration, and visibility for multiple distributed Palo Alto Networks NGFWs (irrespective of location or scale) through Panorama™ network security management in one unified user interface.
- Streamlines configuration sharing through Panorama with templates and device groups and scales log collection as logging needs increase.
- Enables users, through the Application Command Center (ACC), to obtain deep visibility and comprehensive insights into network traffic and threats.

Maximize Your Security Investment and Prevent Business Disruption with AIOps

- AIOps for NGFW delivers continuous best practice recommendations customized to your unique deployment to strengthen your security posture and get the most out of your security investment.
- Intelligently predicts firewall health, performance, and capacity problems based on ML powered by advanced telemetry data. It also provides actionable insights to resolve the predicted disruptions.

Detects and Prevents Advanced Threats with Cloud-Delivered Security Services

Today's sophisticated cyberattacks can spawn 45,000 variants in 30 minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams, and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of 80,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats.

Services include:

- **Advanced Threat Prevention:** Stop known exploits, malware, spyware, and command-and-control (C2) threats, while utilizing industry-first prevention of zero-day attacks—prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire®:** Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60X faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering:** Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security:** Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.

- **Enterprise DLP:** Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise with 2X greater coverage of any cloud-delivered enterprise DLP.
- **SaaS Security:** Stay ahead of the SaaS explosion with the industry's only Next-Generation CASB to automatically see and secure all apps across all protocols.
- **IoT Security:** Safeguard every "thing" and implement Zero Trust device security 20X faster with the industry's smartest security for smart devices.

Delivers a Unique Approach to Packet Processing with Single-Pass Architecture

- Performs networking, policy lookup, application and decoding, and signature matching—for all threats and content—in a single pass. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Enables consistent and predictable performance when security subscriptions are enabled. (In table 1, "Threat Prevention throughput" is measured with multiple subscriptions enabled.)

Enables SD-WAN Functionality

- Allows you to easily adopt SD-WAN by simply enabling it on your existing firewalls.
- Enables you to safely implement SD-WAN, which is natively integrated with our industry-leading security.
- Delivers an exceptional end-user experience by minimizing latency, jitter, and packet loss.

Table 1: PA-5400 Series Performance and Capacities

	PA-5410	PA-5420	PA-5430	PA-5440	PA-5445
Firewall throughput (HTTP/appmix)*	52.4/43.5 Gbps	68.0/56 Gbps	79/61 Gbps	93.5/72 Gbps	93.5/90 Gbps
Threat Prevention throughput (HTTP/appmix)†	26/26.7 Gbps	33/32 Gbps	43/40 Gbps	61.5/52 Gbps	71.5/72 Gbps
IPsec VPN throughput‡	21 Gbps	28.7 Gbps	42 Gbps	58 Gbps	64 Gbps
Max concurrent sessions§	3.6M	5M	7.2M	20M	48M
New sessions per second	270,000	370,000	380,000	390,000	449,000
Virtual systems (base/max)¶	10/20	15/65	25/125	25/225	25/225

Note: Results for PA-5445 were measured on PAN-OS 11.1. Results for PA-5410, PA-5420, PA-5430, and PA-5440 were measured on PAN-OS 11.0.

* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispayware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions.

‡ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.

§ Max concurrent sessions are measured utilizing HTTP transactions.

|| New sessions per second is measured with application override, utilizing 1 byte HTTP transactions.

¶ Adding virtual systems over base quantity requires a separately purchased license.

Table 2: PA-5400 Series Networking Features

Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-Point Protocol over Ethernet (PPPoE) and DHCP supported for dynamic address assignment
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)

Table 2: PA-5400 Series Networking Features (continued)

SD-WAN
Path quality measurement (jitter, packet loss, latency)
Initial path selection (PBF)
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
IPv6
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire, and SSL Decryption
SLAAC
IPsec and SSL VPN
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
Encryption: 3des, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
GlobalProtect Large Scale VPN for simplified configuration and management*
Secure access over IPsec and SSL VPN tunnels using GlobalProtect gateway and portals*
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
Network Address Translation
NAT modes (IPv4): static IP, Dynamic IP, Dynamic IP and Port (port address translation)
NAT64, NPTv6
Additional NAT features: Dynamic IP reservation, tunable Dynamic IP and Port oversubscription
High Availability
Modes: active/active, active/passive, HA clustering
Failure detection: path monitoring, interface monitoring
Mobile Network Infrastructure†
5G Security
GTP Security
SCTP Security

* Requires GlobalProtect license.

† For additional information, refer to our [ML-Powered NGFWs for 5G datasheet](#).

Table 3: PA-5400 Series Hardware Specifications

I/O
1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 1G/10G/25G SFP/SFP+/SFP28 (4), 40G/100G QSFP+/QSFP28 (4)
Management I/O
1G/10G SFP/SFP+ out-of-band management port (1), 1G/10G SFP/SFP+ high availability (2), 40G QSFP+ high availability (1), RJ-45 console port (1), Micro USB
Storage Capacity
480 GB SSD pair, system storage
Power Supply (Avg/Max Power Consumption)
630/760 W

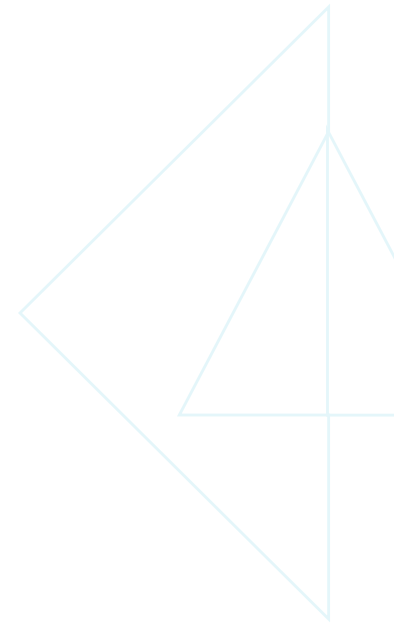
Table 3: PA-5400 Series Hardware Specifications (continued)

Max BTU/hr
1638
Power Supplies (Base/Max)
1:1 fully redundant (2/2)
AC Input Voltage (Input Hz)
100–240 VAC (50–60 Hz)
AC Power Supply Output
1,200 watts/power supply
Max Current Consumption
AC: 7 A @ 100 VAC, 3 A @ 240 VAC
DC: 15 A @ -48 VDC, 12 A @ -60 VDC
Max Inrush Current
AC: 50 A @ 230 VAC, 50 A @ 120 VAC
DC: 200 A @ 72 VDC
Mean Time Between Failure (MTBF)
22 years
Rack Mount Dimensions
2U, 19" standard rack (3.45" H x 22.5" D x 17.34" W)
Weight (Standalone Device/As Shipped)
35.2 lbs/48.8 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See paloaltonetworks.com/company/certifications.html
Environment
Operating temperature: 32°F to 122°F, 0°C to 50°C
Nonoperating temperature: -4°F to 158°F, -20°C to 70°C
Humidity tolerance: 10% to 90%
Maximum altitude: 10,000 ft/3,048 m
Airflow: front to back



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. strata_ds_pa-5400-series_interim_110723



GlobalProtect

GlobalProtect consistently extends the protection of Palo Alto Networks next-generation cybersecurity to the members of your mobile workforce, no matter where they go.

The world you need to secure continues to expand as users and applications shift to locations outside the traditional network perimeter. Security teams face challenges with maintaining visibility into network traffic and enforcing security policies to stop threats. Traditional technologies used to protect mobile endpoints, such as host endpoint antivirus software and remote access virtual private networks (VPNs), cannot stop the advanced techniques employed by today's sophisticated attackers.

GlobalProtect™ enables you to protect your mobile workforce by extending the consistent protections of Palo Alto Networks Prisma® Access and Next-Generation Firewalls to all users, regardless of location. It secures traffic by applying the platform's capabilities to understand application use, associate the traffic with users and devices, and enforce security policies with next-generation technologies.

Key Usage Scenarios and Benefits

Secure Remote Access

- Provides secure access to internal and cloud-based business applications

Advanced Threat Prevention

- Secures internet traffic
- Stops threats from reaching the endpoint
- Protects against phishing and credential theft
- Quarantines compromised devices by leveraging immutable characteristics

URL Filtering

- Enforces acceptable use policies
- Filters access to malicious domains and adult content
- Prevents the use of avoidance and evasion tools
- Secures access to SaaS applications

- Controls access and enforces policies for SaaS applications while blocking unsanctioned applications

Bring-Your-Own-Device Policies

- Supports app-level VPN for user privacy
- Enables secure, clientless access for partners, business associates, and contractors
- Supports automated identification of unmanaged devices
- Supports customized authentication mechanisms for managed and unmanaged devices

Zero Trust Implementation

- Delivers reliable user identification
- Delivers immediate and accurate host information for visibility and policy enforcement
- Enforces step-up multi-factor authentication to access sensitive resources

Extending the Platform Protection Externally

GlobalProtect safeguards your mobile workforce by inspecting all traffic using your next-generation cybersecurity deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud. Laptops, smartphones, and tablets with the GlobalProtect app automatically establish a secure IPsec/SSL VPN connection to Prisma Access or a Next-Generation Firewall using the best gateway, thus providing full visibility of all network traffic, applications, ports, and protocols. By eliminating the blind spots in mobile workforce traffic, your organization can maintain a consistent view into applications.

Implementing Zero Trust in Your Network

Not all users need access to all assets inside your corporate network. Security teams are adopting Zero Trust principles to segment their networks and enforce precise controls for access to internal resources. GlobalProtect provides the fastest, most authoritative user identification for the platform, enabling you to write precise policies that allow or restrict access based on business need. Furthermore, GlobalProtect provides host information that establishes device compliance criteria associated with security policies. These measures allow you to take preventive steps to secure your internal networks, adopt Zero Trust network controls, and reduce the risk of attack.

When GlobalProtect is deployed in this manner, the internal network gateways may be configured with or without a VPN tunnel.

In addition, GlobalProtect enables you to quarantine compromised devices by utilizing an endpoint's immutable characteristics. This will allow administrators to restrict network access as well as prevent the compromised endpoint from infecting other users and devices. Quarantine restrictions can apply whether the compromised device is external or on the internal network.

Inspection of Traffic and Enforcement of Security Policies

GlobalProtect enables security teams to build policies that are consistently enforced whether the user is internal or remote. Security teams can prevent successful cyberattacks by bringing all of the platform's capabilities to bear:

- **App-ID™** technology identifies application traffic, regardless of port number, and enables organizations to establish policies to manage application usage based on users and devices.
- **User-ID™** technology identifies users and group memberships for visibility as well as the enforcement of role-based network security policies.
- **SSL decryption** inspects and controls applications that are encrypted with SSL/TLS/SSH traffic and stops threats within the encrypted traffic.

- **WildFire® malware prevention service** automates the analysis of content to identify new, previously unknown, and highly targeted malware by its behavior and generates the threat intelligence to stop it in near-real time.
- **Threat Prevention** for IPS and antivirus blocks network-based exploits targeting vulnerable applications and operating systems, denial-of-service (DoS) attacks, and port scans. Antivirus profiles stop malware and spyware from reaching the endpoint using a stream-based engine.
- **URL Filtering with PAN-DB** categorizes URLs based on their content at the domain, file, and page level, and receives updates from WildFire so that when web content changes, so do categorizations.
- **File blocking** stops the transfer of unwanted and dangerous files while further scrutinizing allowed files with WildFire.
- **Data filtering** enables administrators to implement policies that can be used to stop the unauthorized movement of data, such as the transfer of customer information or other confidential content.

Secure Access Control

User Authentication

GlobalProtect supports all existing PAN-OS® authentication methods, including Kerberos, RADIUS, LDAP, SAML 2.0, client certificates, biometric sign-in, and a local user database. Once GlobalProtect authenticates the user, it immediately provides Prisma Access or a Next-Generation Firewall with a user-to-IP-address mapping for User-ID.

Strong Authentication Options

GlobalProtect supports a range of third-party multi-factor authentication (MFA) methods, including one-time password tokens, certificates, and smart cards, through RADIUS and SAML integration.

These options help organizations strengthen the proof of identity for access to internal data center or software-as-a-service (SaaS) applications.

GlobalProtect has options to make strong authentication even easier to use and deploy:

- **Cookie-based authentication:** After authentication, you may choose to use an encrypted cookie for subsequent access to a portal or gateway for the lifetime of that cookie.
- **Simplified certificate enrollment protocol support:** GlobalProtect can automate the interaction with an enterprise public key infrastructure (PKI) for managing, issuing, and distributing certificates to GlobalProtect clients.
- **MFA:** Before a user can access an application, he or she can be required to present an additional form of authentication.

Host Information Profile

GlobalProtect checks the endpoint to get an inventory of how it's configured and builds a host information profile (HIP) that's shared with Prisma Access and Next-Generation Firewalls. They use the HIP to enforce application policies that only permit access when the endpoint is properly configured and secured. These principles help enforce compliance with policies that govern the amount of access a given user should have with a particular device.

HIP policies can be based on a number of attributes, including:

- Managed/Unmanaged device identification
- Machine certificates present on device
- Device information received from mobile device manager
- Operating system and application patch level
- Host antimalware version and state
- Host firewall version and state
- Disk encryption configuration
- Data backup product configuration
- Customized host conditions (e.g., registry entries, running software)

Control Access to Applications and Data

Security teams can establish policies based on application, user, content, and host information to maintain granular control over access to a given application. These policies may be associated with specific users or groups defined in a directory to ensure that organizations provide the correct levels of access based on business need. The security team can further establish policies for step-up MFA to provide additional proof of identity before accessing particularly sensitive resources and applications.

Enhanced Troubleshooting and Visibility

GlobalProtect Application Command Center (ACC) widgets, reports, and the new GlobalProtect log provide full visibility into GlobalProtect usage in your deployment. Detailed logging of the connection workflow in stages greatly simplifies troubleshooting of user connection issues. This logging allows administrators to easily identify the stage/event in the connection process where a given user has an issue.

Secure and Enabled BYOD

The effects of bring-your-own-device (BYOD) policies are changing the number of use case permutations that security teams need to support. It is necessary to provide application access to a broader spectrum of employees and contractors using a wide range of mobile devices.

Integration with mobile device management offerings, such as AirWatch® and MobileIron®, can help you deploy GlobalProtect as well as provide additional security measures through the exchange of intelligence and host configuration. Using these in conjunction with GlobalProtect, your organization can maintain visibility and the enforcement of security policy on a per-app basis while maintaining data separation from personal activities to honor the user's expectations of privacy in BYOD scenarios.

GlobalProtect supports clientless SSL VPN for secure access to applications in the data center and the cloud from unmanaged devices. This approach allows customers to enable secure access for third-party users and employees connecting from BYOD devices by providing access to specific applications through a web interface, both without requiring users to install a client and without setting up a VPN tunnel.

Architecture Matters

The flexible architecture for GlobalProtect provides many capabilities that can help you solve an array of security challenges. At the most basic level, you can use GlobalProtect as a replacement for the traditional VPN, eliminating the complexity and headaches of administering a standalone, third-party VPN gateway.

Options for manual connections and gateway selection enable you to tailor the configuration to support business requirements as needed.

In a more comprehensive deployment for securing traffic, GlobalProtect can be deployed with an always-on secure connection with a full tunnel, ensuring that protection is always present and transparent to the user experience. Exceptions can be defined for latency-sensitive traffic by application, domain names and routes, or video traffic.

Cloud-Based Gateways

Workforces shift from one location to another, creating changes in traffic load. This is especially true when considering how companies evolve, whether on a temporary basis (e.g., following a natural disaster) or a permanent one (e.g., when entering new markets).

Prisma® Access by Palo Alto Networks provides a co-managed option for deploying coverage in the locations organizations need, using your security policies. It can be used in conjunction with your existing firewalls, making your architecture adaptable to changing conditions.

Prisma Access supports auto scaling, which dynamically allocates new firewalls based on load and demand in a given region.

Conclusion

Palo Alto Networks next-generation cybersecurity plays a critical role in preventing breaches. Use GlobalProtect to extend the protection of the platform to users wherever they go. By using GlobalProtect, you can get consistent enforcement of security policy so that even when users leave the building, their protection from cyberattacks remains in place.

Table 1: GlobalProtect Features	
Category	Specification
VPN Connection	IPsec
	SSL
	Clientless VPN
	Per-app VPN on Android, iOS
Gateway Selection	Automatic selection
	Manual selection
	Preferred gateway selection
	External gateway selection by source location
	Internal gateway selection by source IP
Connection Methods	User logon (always-on)
	On-demand
	Pre-logon (always-on)
	Pre-logon, then on-demand
	User-initiated pre-logon
Connection Mode	Internal mode
	External mode
Layer 3 Protocols	IPv4
	IPv6
Single Sign-On	SSO (Windows credential provider)
	Kerberos SSO
	SSO for macOS
Split Tunneling	Include routes, domains, applications
	Exclude routes, domains, applications
Authentication Methods	SAML 2.0
	LDAP
	Client certificates
	Kerberos
	RADIUS
	Two-factor authentication
	Authentication method selection based on operating system or device ownership
HIP Reporting, Policy Enforcement, and Notifications	Patch management
	Host antispware
	Host antimalware
	Host firewall
	Disk encryption
	Disk backup
	Data loss prevention
	Customized HIP conditions (e.g., registry entries, running software)
Managed Device Identification	By machine certificates
	By hardware serial number
MFA	At connect time and resource access time

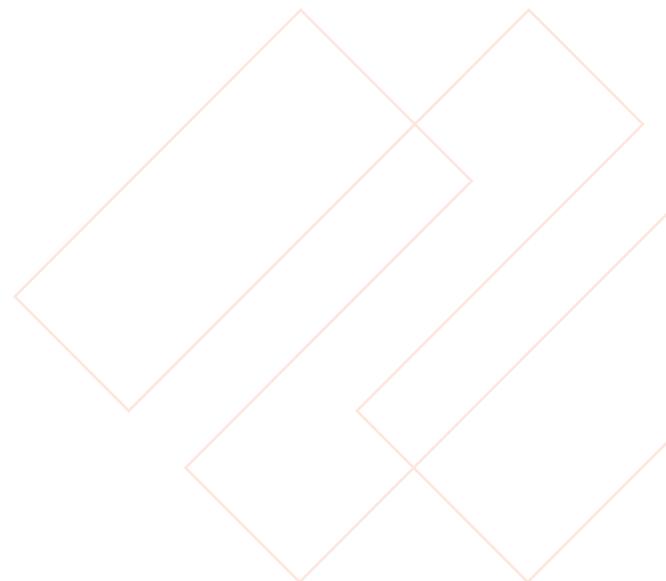
Table 1: GlobalProtect Features (continued)

Other Features	User-ID
	IPsec to SSL VPN fallback
	Enforce GlobalProtect connection for network access
	Tunnel configuration based on user location
	HIP report redistribution
	Certificate checks in HIP
	SCEP-based automatic user certificate management
	Script actions that run before and after sessions
	Dynamic GlobalProtect app customization
	App configuration based on users, groups, and/or operating systems
	Automatic internal/external detection
	Manual/automatic upgrade of GlobalProtect app
	Certificate selection by OID
	Blocking of access by lost, stolen, or unknown devices
	Smart card support for connection/disconnection
	Transparent distribution of trusted root CAs for SSL decryption
	Disabling of direct access to local networks
	Customizable welcome and help pages
	RDP connection to a remote client
	Operating system-native notifications
	User sign-out restriction
	Proxy support
	Enforcement of GlobalProtect exclusions
	Connection with SSL only
	RSA software token integration
MDM/EMM Integration	Device Quarantine
	AirWatch
	MobileIron
Management Tools and APIs	Microsoft Intune
	Palo Alto Networks Next-Generation Firewalls, including physical and virtual appliances
	Prisma Access
GlobalProtect App Supported Platforms	Panorama network security management
	Microsoft Windows and Windows UWP
	Apple macOS
	Apple iOS and iPadOS
	Google Chrome OS
	Android OS
	Linux OS (Red Hat, CentOS, Ubuntu)
IPsec XAuth	IoT devices
	Apple iOS IPsec client
	Android OS IPsec client
	Third-party VPNC and strongSwan client
GlobalProtect App Localization	Chinese, English, French, German, Japanese, Spanish



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
prisma_ds_globalprotect_070622



Advanced WildFire

Stop Highly Evasive Malware at Scale

Modern threat actors have two main advantages over organizations today: opportunity and accessibility. With the adoption of hybrid work, the shift to the cloud, and rapid growth in IoT and SaaS applications, the attack surface has expanded, providing greater opportunity for threat actors to find ways to infiltrate an organization. In addition, ransomware-as-a-service and automation offerings have lowered the technical bar for deploying sophisticated malware campaigns, providing threat actors access to the tools they need to increase the volume, severity, and scope of attacks.

Modern malware has been shown to be highly evasive, using techniques such as packing, encryption, and fileless or memory-only presence to bypass traditional security defenses. These advanced evasion methods have added complexity in detecting new and sophisticated malware, rendering AV scanning and traditional sandboxing solutions useless.

Business Benefits

The Advanced WildFire security service enables you to:

- **Reduce the risk of patient zero.** Prevent 26% more highly evasive malware that bypasses traditional sandboxes, in addition to stopping over 99% of known and unknown malware.¹
- **Take advantage of an “infinite” signature repository.** Access all known AV signatures, whether the threat was seen yesterday or 10 years ago, with real-time signature lookup provided on the NGFW.
- **Achieve comprehensive protection while meeting compliance requirements.** Join a global network of 85K+ customers with access to 10 regional clouds and 17 international certifications.
- **Eliminate dwell time risk.** Cut threat response time to seconds with automated delivery of coordinated protection across network, endpoint, and cloud, with 60x faster signature delivery than the nearest competitor.
- **Reduce actionable events and workload for the SOC.** Stop the initial threat, delivering fewer detection events to investigate and contain.
- **Avoid manual integrations.** Threat intel automatically flows into the Palo Alto Networks ecosystem, eliminating manual tooling or integration.

1. “Palo Alto Networks WildFire Detection Efficacy: Public Statement,” AV-Test, June 2022.

The Pitfalls of Traditional Sandboxing Solutions

To mitigate risks associated with attacks using evasive attacks, organizations turn to network sandboxing solutions for malware analysis. Unfortunately, traditional sandboxing solutions can suffer from the following pitfalls that render them useless against advanced threats:

- **Traditional sandboxing solutions cannot stay hidden from malware.** Highly evasive malware checks for instrumentation or “hooks,” which are used by sandboxes to log the activity of a sample when it is under analysis. Since analysis engines reside in the same environment as where the malware would execute, if malware observes the presence of these hooks, it will choose not to execute or, in cases of sophisticated malware, to evade the hooks. This tricks the sandbox into thinking the sample is benign.
- **Traditional sandboxing solutions may be tricked by latent behavior.** Some sandboxes can time out and miss a detection because of “sleeping” malware. Traditional sandboxes cannot simply reduce the timer to a low number because it might break the execution of other software.
- **Traditional sandboxing solutions cannot detect memory-resident malware.** Machine learning models trained on file structure alone are ineffective at detecting samples that employ evasion techniques such as obfuscation, packing, and execution of dynamically injected shellcode in process memory. Additionally, significant storage, compute, and infrastructure are required to look into memory samples, which most vendors do not invest in.
- **Traditional inline sandboxing solutions affect user productivity.** When a vendor chooses to hold files for analysis, they will, in turn, interrupt user workflows and productivity.
- **Traditional sandboxing solutions are slow to deliver verdicts.** Without a connected security ecosystem, signature updates can take anywhere from hours to days to provide updates.

Go Beyond Traditional Sandboxing

Palo Alto Networks Advanced WildFire is the industry’s largest cloud-based malware prevention engine that protects organizations from highly evasive threats using patented machine learning detection engines, enabling automated protections across network, cloud, and endpoints. Advanced WildFire analyzes every unknown file for malicious intent and then distributes prevention in record time—60 times faster than the nearest competitor—to reduce the risk of patient zero.

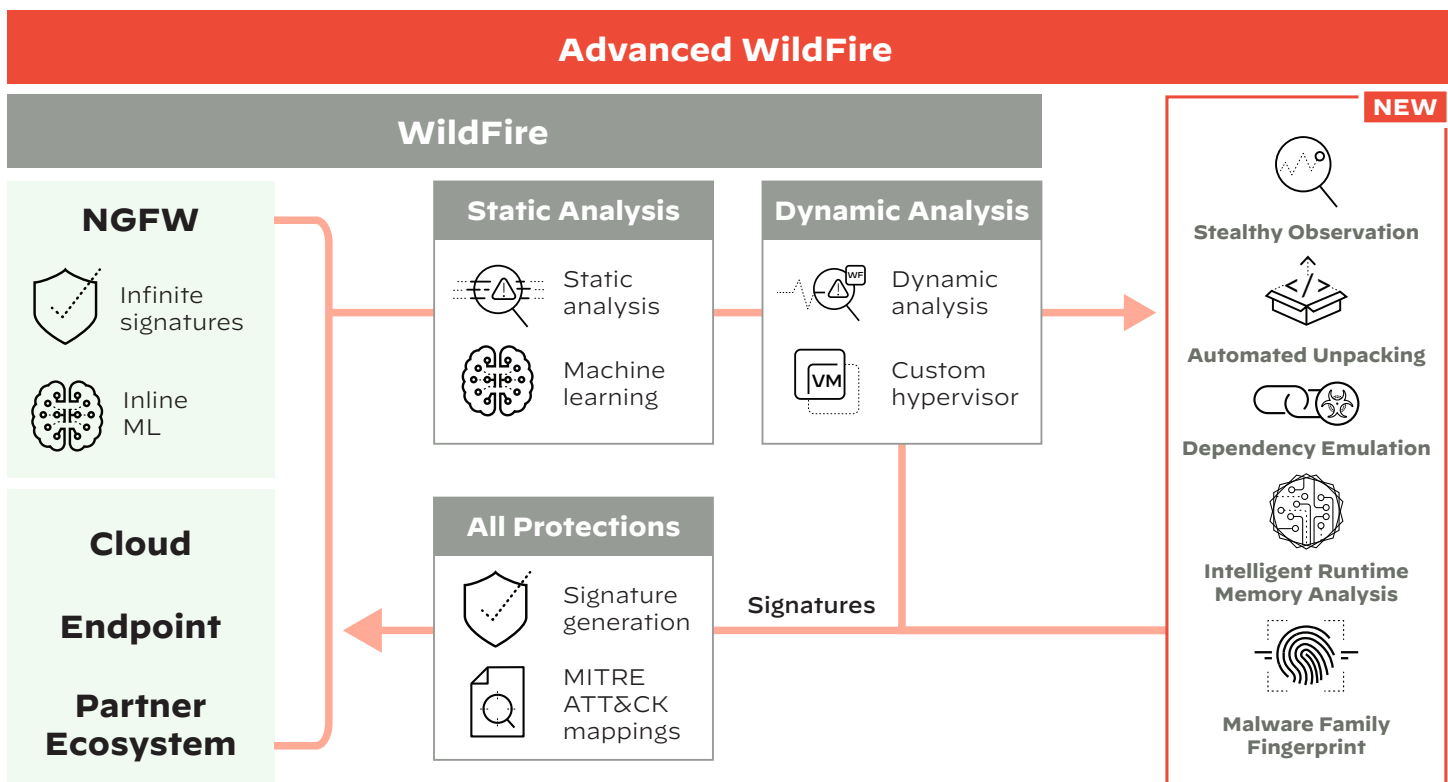


Figure 1: Advanced WildFire detection engines

Advanced WildFire is the industry's only malware prevention engine to defeat an additional 26% of highly evasive modern malware at scale with a brand-new infrastructure and patented analysis techniques, including intelligent runtime memory analysis, dependency emulation, malware family fingerprinting, and more. Unlike traditional solutions that depend solely on offline or delayed analysis of unknown malware, Advanced WildFire analysis and threat intelligence flow directly into machine learning models that act both locally at the firewall level and in the cloud—stopping over 99% of known and unknown malware.² After analysis, automated prevention is where Advanced WildFire shines: it applies rapid and consistent protection at the edge, in your data center, in the cloud, within software-as-a-service (SaaS) applications, and on endpoints.

Advanced WildFire goes beyond traditional sandboxing approaches to prevent unknown and highly evasive malware in a cloud environment. Over 25 patented detection techniques enable advanced malware analysis while maintaining high detection efficacy and near-zero false positives. As a sample gets analyzed by Advanced WildFire, it will pass through a combination of the following analysis engines:

- **Lightweight inline machine learning** models on the next-generation firewall provide real-time prevention of known malware and unknown variants.
- **Static analysis** looks at the characteristics of a file while leveraging dynamic unpacking to analyze threats attempting to evade detection through the use of packing tool sets.
- **Cloud-based machine learning** models extract thousands of unique features from each file which is not possible with static or dynamic analysis alone. Information gathered is then used to further train the predictive machine learning models to identify new malware.
- **Dynamic analysis** observes files as they execute in a purpose-built, evasion-resistant virtual environment, enabling the detection of previously unknown malware using hundreds of behavioral characteristics.
- **Intelligent runtime memory analysis** captures snapshots of malicious activity in memory and conducts real-time analysis to identify malicious behavior, detecting highly evasive malware that would not have otherwise gone undetected.

Key Capabilities

Root Out Malicious Behavior in All Traffic

Advanced WildFire identifies files with potential malicious behaviors and then delivers verdicts based on their actions by applying threat intelligence, analytics, and correlation alongside advanced capabilities:

- **Complete malicious behavior visibility** identifies threats in all traffic across hundreds of applications, including web traffic; email protocols like SMTP, IMAP, and POP; and file-sharing protocols like SMB and FTP, regardless of ports or encryption.
- **Suspicious network traffic analysis** monitors all network activity produced by a suspicious file, including backdoor creation, downloading of next-stage malware, visiting low-reputation domains, network reconnaissance, and much more.
- **Fileless attack/script detection** identifies when potentially malicious scripts, such as JScript and PowerShell, traverse the network and forwards them to Advanced WildFire for analysis and execution.

The powerful discovery and analysis capabilities of Advanced WildFire are seamlessly integrated with numerous products across the Palo Alto Networks portfolio as well as within leading partner solutions across email and cloud platforms.

Stop Unknown Threats at the Firewall Level with Inline Machine Learning

Powered by threat models continually homed in the cloud, Advanced WildFire includes an inline machine learning-based engine delivered within our hardware and virtual ML-Powered NGFWs. This innovative, signatureless capability prevents malicious content in common file types—such as portable executable files and fileless attacks stemming from PowerShell—completely inline, with no required cloud analysis, no damage to content, and no loss of user productivity. Whether an unknown file matches an existing signature or is classified by an ML-Powered NGFW, Advanced WildFire always performs full analysis, extracting valuable intelligence and data to provide context for security analysts, generate training updates for the machine learning models, and share intelligence with other subscriptions to prevent other attack vectors.

2. "Palo Alto Networks WildFire Detection Efficacy: Public Statement," AV-Test, June 2022.

Prevent Highly Evasive Malware

Defeat modern malware evasion techniques using the following key features:

Stealthy Observation

Malware conducts environmental checks and withholds detonation if it believes it is in a sandbox environment. By using a custom hardened hypervisor where analysis components exist entirely outside of the guest VM, Advanced WildFire conducts stealthy observation to uncover malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis.

Automated Unpacking

It is common for malicious actors to obfuscate their payloads using tools like encoding, encryption, and packing. Packing inhibits static or dynamic data from being useful for accurate detection. With automated unpacking, Advanced WildFire gains full visibility into file contents during analysis. Advanced WildFire also now generates signatures on packed payloads.

Dependency Emulation

One of the most malicious file types, portable executables, often require external dependencies to be satisfied to execute. With new dependency emulation capabilities, the sandbox environment will satisfy all external dependencies required for malware to execute, allowing the analysis engines to observe malicious behavior.

Intelligent Runtime Memory Analysis

Advanced WildFire introduces a brand-new detection infrastructure to support intelligent runtime memory analysis, enabling snapshots to be taken at critical points in memory when malicious behavior is observed. This not only provides the most relevant information for post-execution analysis but also efficiently allocates storage and compute resources.

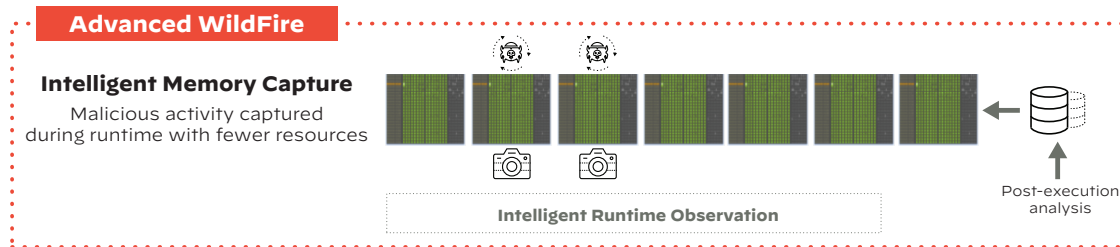


Figure 2: Intelligent runtime memory analysis

Malware Family Fingerprinting

Advanced WildFire extracts packed executables, commonly used to evade static signatures and generic pattern matching, and uses patented malware family fingerprinting detection to correlate new threats to known malware families, generating preventions for evasive malware at scale.

Get Global Prevention Across the Advanced WildFire Ecosystem, Delivered in Seconds

For highly customized threats that inline machine learning-powered prevention cannot stop, Advanced WildFire applies powerful cloud-based analysis to deliver prevention across networks, clouds, endpoints, or wherever Advanced WildFire-enabled sensors are deployed. Working in tandem with the capabilities of PAN-OS, Advanced WildFire generates and delivers prevention globally within seconds of initial analysis for most new threats. This innovative, cloud-scale delivery of evasion-resistant signatures closes the window for adversaries to successfully deploy malicious content.

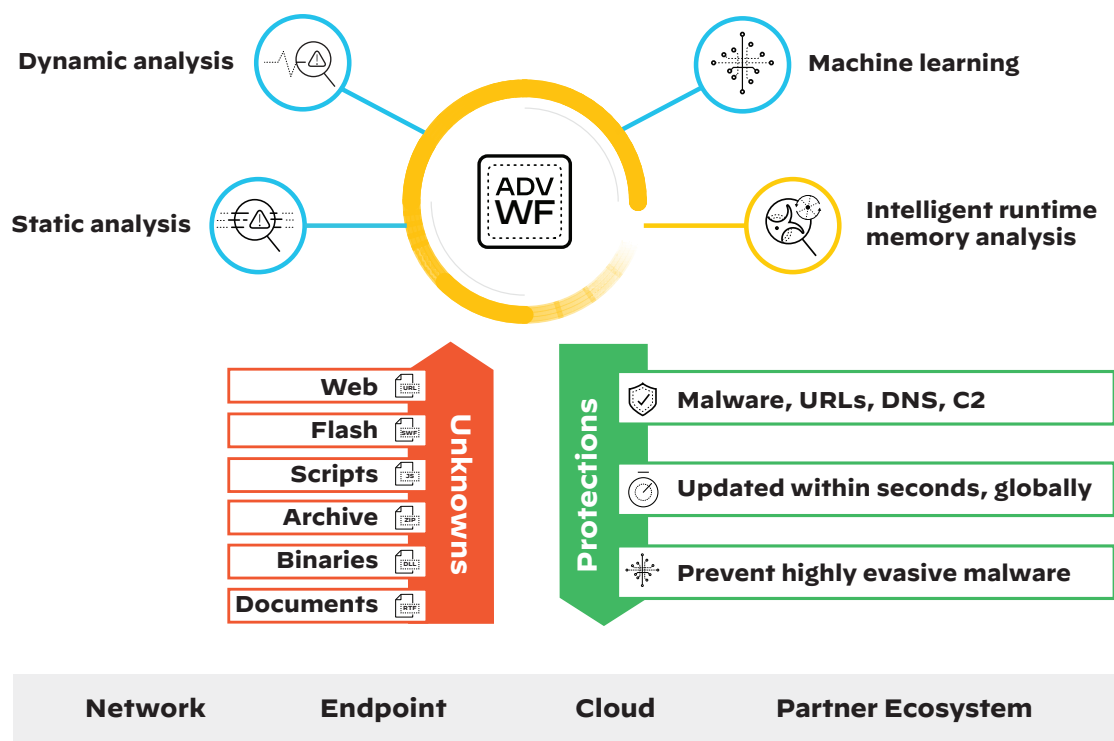


Figure 3: Integrated security for protection across your organization

How Advanced Threat Prevention and Advanced WildFire Work Together

The primary function of Advanced WildFire is to determine whether a given file is malware, greyware, or benign. When Advanced WildFire determines a file is malicious, that file is sent through the AV pipeline to have a signature generated. This new signature is then distributed to Advanced WildFire customers in the next five-minute update and to Advanced Threat Prevention customers in the next daily AV content package.

When a file passes through the firewall, there are several mechanisms used to block malware. The following describes the process for a firewall that has both the Advanced WildFire and Advanced Threat Prevention subscriptions and is configured according to best practices:

1. There are file-type-specific machine learning models that run on the data plane of the firewall. These models provide a measure of protection against zero-day malware.
2. The firewall checks against the signatures in its local cache to see if there is a match for the file. The local cache on the firewall is primarily populated by the AV content package provided by Advanced Threat Prevention and the Advanced WildFire five-minute signature update. The AV content package contains ~1.2 million signatures, and the five-minute update will contain new malware that Advanced WildFire has detected.
3. If there is no match in the local cache, the firewall will query the real-time signature service provided by Advanced WildFire to search the complete database of historical signatures to see if there is a match. With PAN-OS Nova, you can hold the transfer of the file while this query is taking place. If there is a match, a signature is:
 - a. Installed into the local cache of the firewall.
 - b. Included in the next five-minute update to all Advanced WildFire customers.
 - c. Re-included in the Advanced Threat Prevention AV content package for the next day.
4. If there is no match from the real-time signature service and Advanced WildFire has not seen the file before, it will be sent to the Advanced WildFire cloud for analysis.

Without Advanced WildFire, customers have no way of determining if a new, never-before-seen file is malicious or not. In addition to being limited to the 1.2 million malware signatures in the AV package, customers will miss out on real-time signature lookup and the five-minute update post-Advanced WildFire cloud analysis. In practice, this means that they will not get coverage for new malware until the next day, as opposed to within five minutes of discovery.

Use Signatures, Not Hashes

Advanced WildFire uses content signatures for prevention instead of hashes so it can identify more malware with a single signature. As a result, compared to the mostly hash-based systems that require 1:1 ratios, Advanced WildFire protects against more attacks with the same resources. A single Advanced WildFire signature can protect against up to millions of polymorphic variants of a single malware.

Operational Benefits

- **Automate reprogramming of security controls to block unknown threats.** Shared real-time intelligence from a network of over 85,000 customers automatically updates and prevents threats across networks, endpoints, and clouds.
- **Gain detailed context on analyzed threats.** Get thorough visualization of every malicious file sent to Advanced WildFire across multiple operating system environments and application versions with AIOps.
- **Integrate seamlessly to enrich custom applications and existing security tools.** Leverage open API integration with SIEM, TIP, ticketing, SOAR, XDR tools, or custom use cases to process indicators of compromise (IOCs).

Deploy in a Compliant and Secure Cloud-Based Architecture

Files are submitted to the Advanced WildFire global cloud, delivering speed and scale, and any Palo Alto Networks customer can quickly turn on the service—including users of hardware and virtual ML-Powered NGFWs, public cloud offerings, Prisma SaaS, and Cortex XDR agents. Palo Alto Networks directly manages the Advanced WildFire infrastructure, following industry-standard best practices for security and confidentiality, with regular SOC 2 compliance audits. See the [Advanced WildFire privacy datasheet](#) and [certifications webpage](#) for more information.

To enable you to better address data sovereignty and privacy concerns, we maintain distributed regional Advanced WildFire clouds that give you more control over the location of your data. Providing the same detection and prevention capabilities as the Advanced WildFire public cloud, these clouds allow you to adjust submissions to address localized data privacy concerns.



Figure 4: Advanced WildFire regional clouds

Integrate Seamlessly with Existing Security Tools and Custom Applications

The rapid move to the cloud and digital transformation efforts are surfacing security challenges that require rapid, effective, and on-demand malware analysis performed outside of the next-generation firewall or traditional control points. The Advanced WildFire API enables customers to make queries to Advanced WildFire for information about potentially malicious content and submit files for analysis using the advanced threat analysis capabilities of Advanced WildFire. Using this RESTful API, customers can leverage the industry-leading malware analysis capabilities of Advanced WildFire to integrate with existing SOAR tools to secure custom applications (such as business-to-consumer web portals), scan file share and storage locations for malicious content prior to cloud migration, and more. An Advanced WildFire subscription unlocks API access for a fixed number of submissions and queries. A separate stand-alone Advanced WildFire subscription, which does not require the purchase of a next-generation firewall, enables customers to purchase flexible submission and query volumes to access Advanced WildFire malware analysis via an API wherever needed.

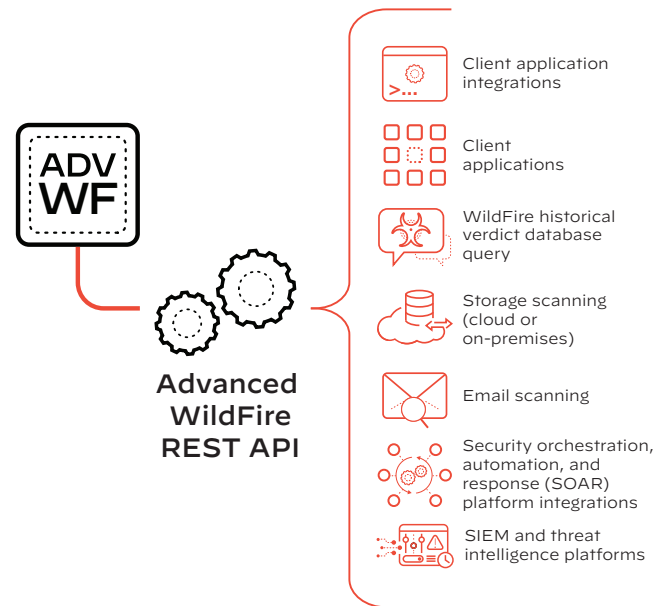


Figure 5: Advanced WildFire API

Integrated Logging, Reporting, and Forensics

Advanced WildFire users receive integrated logs, analysis, and visibility into malicious events through the PAN-OS management interface, Panorama network security management, Cortex XDR, or Cortex XSOAR, enabling teams to quickly investigate and correlate events observed in their networks. With this information, security teams can rapidly locate and take action on the data needed for timely investigations and incident response, regardless of the application they use.

The Power of Palo Alto Networks Security Subscriptions

Today's threat actors benefit from the ever-growing opportunities to take advantage of insecure networks while leveraging sophisticated cloud-based tool sets to deploy threat campaigns. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams, and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of over 85,000 customers to instantly coordinate intelligence and protect against threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats:

- **Advanced Threat Prevention:** Stop known exploits, malware, spyware, and command-and-control (C2) threats while utilizing industry-first prevention of zero-day attacks. Prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire malware prevention:** Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60x faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering:** Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security:** Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.
- **Enterprise DLP:** Minimize the risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2x greater coverage of any cloud-delivered enterprise DLP.

- **SaaS Security:** The industry's only Next-Generation CASB natively integrated into Palo Alto Networks SASE offers proactive SaaS visibility, comprehensive protection against misconfigurations, real-time data protection, and best-in-class security.
- **IoT Security:** Safeguard every "thing" and implement Zero Trust device security 20x faster with the industry's smartest security for smart devices.
- **AIOps:** AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions.

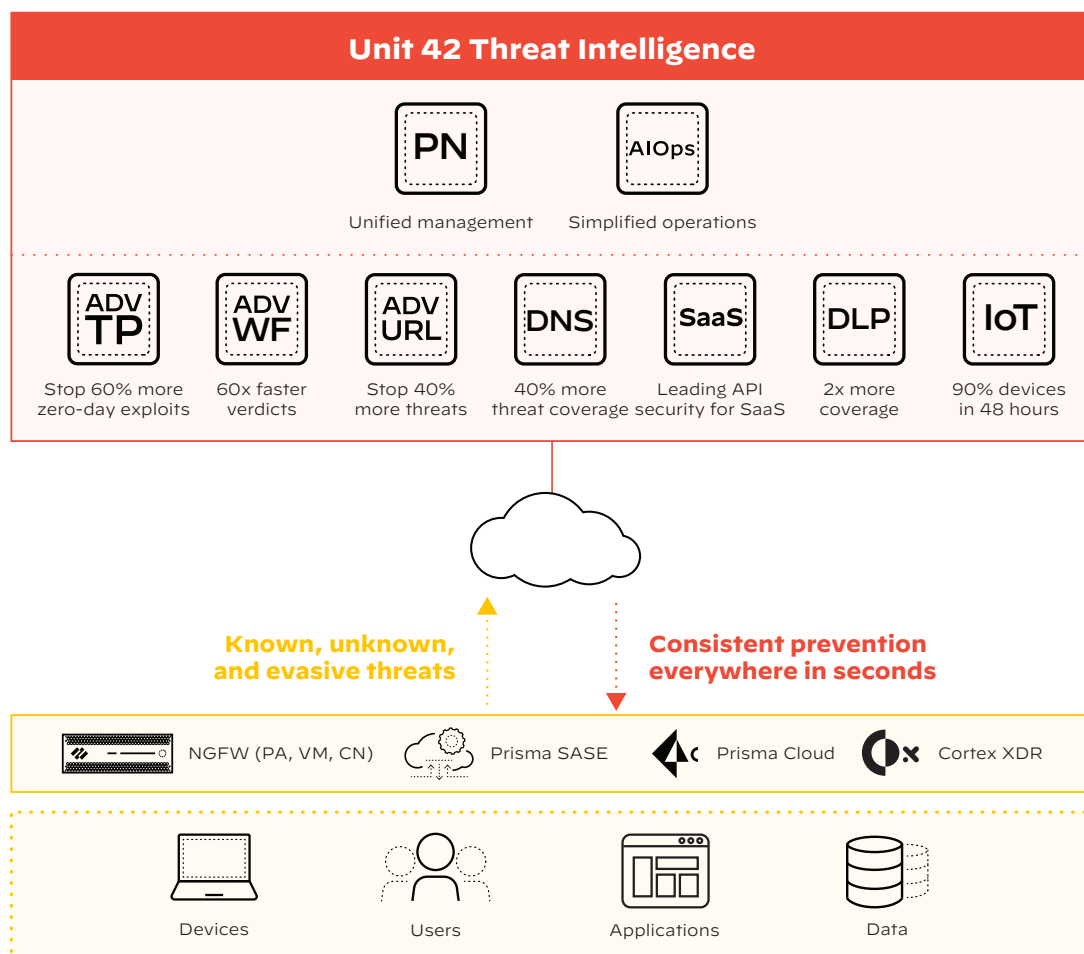


Figure 6: Palo Alto Networks Cloud-Delivered Security Services

Table 1: Features and Licensing Summary	
Capabilities Activated with the Advanced WildFire Subscription Attached to NGFW	
Advanced Analysis, Prevention, and Anti-Evasion Techniques	Static analysis combines static analysis, machine learning, and analysis of file anomalies, malicious patterns, and known malicious code. Inline ML-based prevention (on firewall) blocks unknown malicious executables and PowerShell attacks. Dynamic analysis includes custom hardened hypervisor, behavioral scoring, network profiling, and multistage recursive analysis. Intelligent runtime memory analysis captures snapshots of malicious activity in memory and conducts runtime analysis to identify malicious behavior.
OS Support	macOS, Android, Windows 7/10, and Linux

Table 1: Features and Licensing Summary (continued)

Capabilities Activated with the Advanced WildFire Subscription Attached to NGFW		
File Support	PE files (EXE, DLL, and others), all Microsoft Office file types, Mac OS X files, Linux (ELF) files, Android Package Kit (APK) files, Adobe Flash and PDF files, archive (RAR and 7-Zip) files, script (BAT, JS, VBS, PS1, Shell script, and HTA) files, analysis of links within email messages, and encrypted (TLS/SSL) files	
Protocol Support	SMTP, POP3, SMB, FTP, IMAP, HTTP, and HTTPS	
File Analysis per Day	80 million+ unique files analyzed per day	
Signature Type	- Based on new/zero-day malware discovered in web traffic (HTTP/HTTPS), email protocols (SMTP, IMAP, and POP), and FTP traffic - Generated on the malware payload of the sample and tested for accuracy and safety	
Protection Updates for Unknown Malware	Seconds, with zero-delay signatures to connected NGFW*	
Regional Cloud Locations	Australia, Canada, Germany, India, Japan, the Netherlands (EU Regional Cloud), Singapore (APAC Regional Cloud), United Kingdom, United States (Global Cloud and US Government Cloud)	
WildFire API Key	The Advanced WildFire subscription on the NGFW includes access to the Advanced WildFire API, enabling integrating Advanced WildFire into other applications. This API has daily limits for file submissions and hash queries.	
Integrations	With Palo Alto Networks, including all cloud-delivered security subscriptions, Cortex XDR, Cortex XSOAR, Prisma Access, Prisma Cloud, and SaaS Security	
	With technology partners for verdict determination on third-party services with the Advanced WildFire API	
Management and Reporting	Palo Alto Networks Panorama and WebUI, API, and AIOps	
Forensics	- Detailed analysis of every malicious file sent to Advanced WildFire across multiple operating system environments, including both host- and network-based activity - Access to the original malware sample for reverse engineering, with full PCAPs of dynamic analysis sessions - Open API for integration with third-party security tools, such as security information and event management (SIEM) systems	
Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.	
Requirements†	To use the features of the Palo Alto Networks Advanced WildFire subscription, you will need to meet the following PAN-OS requirements:	
	Feature	PAN-OS Requirement
	WildFire Cloud-based File Analysis	Any supported PAN-OS
	Advanced WildFire Cloud-based File Analysis	Any supported PAN-OS
	NGFW Inline Machine Learning (PE, ELF, PS1, PS2, Office)	10.1+
	Advanced WildFire Real-Time Signature Delivery	10.1+
Recommended Environment	Palo Alto Networks Next-Generation Firewalls deployed in any location, as both internal and external sources, may introduce file-based threats into the network.	

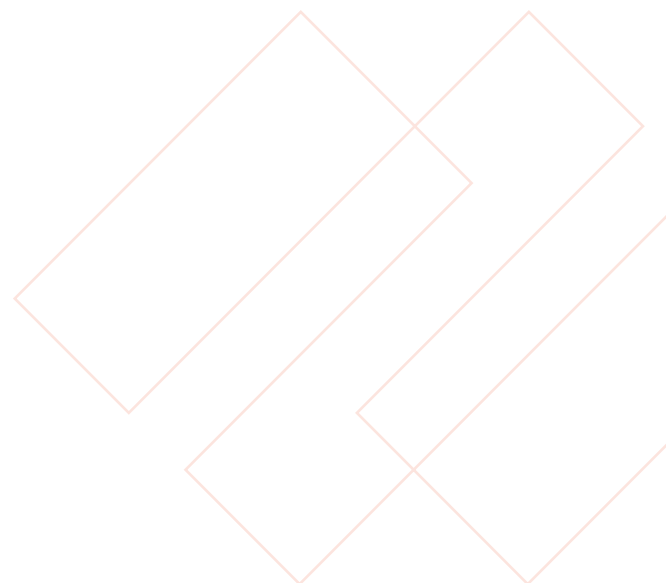
* Requires PAN-OS 10.0 and above.

† Customers can purchase Advanced WildFire with any PAN-OS version and will receive additional features upon upgrade.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks, Inc. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
parent_ds_advanced-wildfire_030223



Advanced URL Filtering

Best-in-Class Web Protection

Safeguarding the Web in Real Time

As applications move to the cloud and people work from anywhere, it's becoming more important—and more difficult—to secure the web. Web-based attacks like phishing and fileless attacks are coming at higher volume, greater speed, and increased sophistication, yet many web security solutions only depend on databases of known malicious webpages that are quickly overrun by the hundreds of thousands of new threats created every day.

Palo Alto Networks Advanced URL Filtering provides best-in-class web protection for the modern enterprise. Bringing together the best of both worlds, Advanced URL Filtering combines our renowned malicious URL database capabilities with the industry's first real-time web protection engine powered by deep learning. Now, you can automatically detect and prevent new malicious and targeted web-based threats instantly. Welcome to real-time protection.

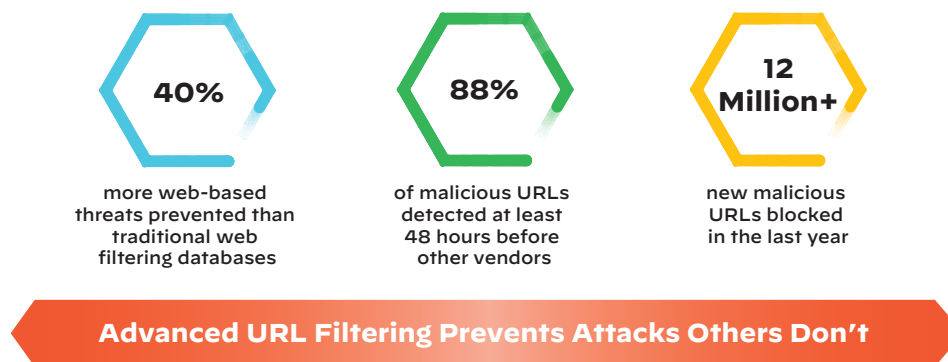


Figure 1: Advanced URL Filtering detects the most damaging web-based attacks aimed at enterprise networks today

The Advanced URL Filtering Difference

Built in the cloud, Advanced URL Filtering is a subscription service that works natively with your Palo Alto Networks Next-Generation Firewall (NGFW) to secure your network against web-based threats such as phishing, malware, ransomware, and command and control (C2).

Advanced URL Filtering uses Palo Alto Networks patent-pending inline deep learning technology to analyze URLs in real time and classify them into benign or malicious categories, which you can easily build into your NGFW policy for total control of web traffic. These categories trigger complementary capabilities across the NGFW platform, enabling additional layers of protection, such as targeted SSL decryption and advanced logging. Alongside its own analysis, Advanced URL Filtering uses shared threat information from Palo Alto Networks industry-leading malware prevention service, Advanced WildFire and other sources to automatically update protections against malicious sites. Advanced URL Filtering delivers:

- **Superior protection against web-based attacks** with the combined power of our URL database stopping known threats and a cloud-delivered web security engine powered by machine learning that categorizes and blocks new malicious URLs in real time, even when content is cloaked from crawlers. Advanced URL Filtering prevents 40% more threats than traditional web filtering databases.
- **Industry-leading phishing protections** that tackle the most common causes of breaches.
- **Total control of your web traffic** through fine-grained controls and policy settings that enable you to automate security actions based on users, risk ratings, and content categories.
- **Maximum operational efficiency** by enabling web protection through the Palo Alto Networks platform.

Business Benefits

- **Inline protection.** Protection from new and unknown web-based attacks in less than 100 milliseconds to prevent patient zero.
- **Detect evasive and targeted attacks.** Increase detection of evasive and targeted attacks by detecting real web traffic and not web crawler data.
- **Cloud-native service.** Designed to expand and scale capabilities over time.
- **Leverage consistent security policies and capabilities.** Deploy Advanced URL Filtering with hardware appliances, on virtual environments, or in the cloud with the same set of policies and security consistently applied.
- **Eliminate security silos and keep users safe.** We can help you attain proper security posture 30% faster compared to point solutions.
- **Minimize operational expenditure.** Palo Alto Networks Cloud-Delivered Security Services reduce the need for standalone solutions, saving US\$9.9 million over three years.¹
- **Safeguard against phishing.** Layers of prevention protect your organization from known and brand-new phishing sites by stopping credential phishing in real time.
- **Support regulatory compliance and acceptable use.** Ensure your organization stays compliant with internal, industry, and government regulatory policies.

Key Capabilities

Inline Protection from New Malicious Webpages

At Palo Alto Networks, we saw a 127% increase in malicious webpages from 2019 to 2021.² With so many new threats, practically every one of them has never been seen before when it hits your network.

In addition, 40% of malicious URLs come from legitimate domains,³ as adversaries look to embed threats in websites that have largely been deemed trustworthy. URLs change from benign to malicious frequently, and unless your solution is constantly analyzing them, that leaves you exposed. Modern organizations can no longer depend solely on static or slow-to-update databases to keep pace. A new approach is necessary.

Advanced URL Filtering takes web protection to the next level with the ability to detect and block new threats in real time, preventing patient zero. Cloud-based inline ML performs real-time web analysis of real web traffic instead of web crawler data, categorizing and blocking malicious URLs in milliseconds—before they have a chance to infect your organization. Our ML models are retrained frequently, ensuring the most up-to-date detection intelligence against new web-based threats. Meanwhile, our extensible cloud-based architecture ensures you can take advantage of the latest innovative detection modules on the fly without going through a painful update process.

It's time to move beyond the overreliance on offline crawling and databases that take too long to update. Advanced URL Filtering takes that step, delivering the industry's first inline web protection engine capable of detecting never-before-seen web-based threats and preventing them in real time.

Anti-Evasion

Modern adversaries have evolved to avoid security measures, and now 90% of phishing kits sold on the dark web include at least one type of evasive technique.⁴ The most common of these techniques, called cloaking, capitalizes on the fact that many web security solutions rely solely on offline crawling of webpage content to determine whether a threat exists. Attackers may actively block connections from specific IP addresses and hosts they know to be security companies or reroute them to benign content.

Advanced URL Filtering goes beyond webpage crawling to analyze live web content, disrupting attackers and identifying the true nature of malicious sites hiding behind evasive techniques.

1. *The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN*, Forrester, January 2021, <https://start.paloaltonetworks.com/2021-forrester-tei-report-network-security.html>.

2. Observed by Palo Alto Networks systems, 2019–2021.

3. *2019 Webroot Threat Report*, Webroot, February 22, 2019, https://www-cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf.

4. “6 Phishing Techniques Driven by the Phishing-as-a-Service Industry,” Cyren Security Blog, July 1, 2019, <https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service>.

Phishing Protection

One of the oldest tricks in the book, phishing continues to pose a challenge for enterprise organizations. A new phishing site launches every 20 seconds,⁵ and phishing constitutes more than 80% of reported security incidents⁶ as well as 22% of successful breaches.⁷

Phishing is a constant threat, with new phishing sites able to be set up and taken down in seconds. With Advanced URL Filtering, you're protected from millions of known phishing pages, but it's also critical to detect new phishing pages instantly and accurately before they can claim their first victim. We incorporate layers of innovative detection capabilities to provide the most comprehensive phishing protection available, including:

- Inline ML-based web content analysis for real-time detection of never-before-seen and highly evasive phishing attacks
- The industry's only real-time credential theft prevention
- ML-based image analysis
- Static and dynamic analysis
- Deep recursive analysis
- Deep learning convolutional neural networks (CNN) model
- Append attack detection
- ML-powered domain analysis
- Deobfuscating JavaScript engine
- Phishing redirection chain analysis
- Fake CAPTCHA interaction analysis

Total Control of Web Traffic

Web policy is simply an extension of your firewall policy. Your Palo Alto Networks NGFW uses Advanced URL Filtering to identify URL categories, assign risk ratings, and apply consistent policy. Multiple URL categories and risk ratings can be combined in nuanced policies, allowing for precise exception-based enforcement, simplified management, and granular control of web traffic through a single policy set. You can block dangerous sites that may be used in phishing attacks, exploit kit delivery, or C2 while still allowing employees the freedom to access web resources they need for business purposes.

Operational Efficiency

Reduce the total cost of your security stack and maximize operational efficiency by enabling web protection through the Palo Alto Networks platform. Because of its cloud architecture, Advanced URL Filtering eliminates the need to deploy and manage additional appliances for web protection—you simply turn it on through the NGFW. Our Cloud-Delivered Security Services reduce the need for standalone solutions, saving US\$9.9 million over three years and reducing risk by 45%.⁸ Using a platform where each security capability enhances the next, you can achieve proper security posture 30% faster compared to point solutions.⁹

The Power of Palo Alto Networks Security Subscriptions

Today, cyberattacks have increased in volume and sophistication, using advanced techniques to bypass network security devices and tools. This challenges organizations to protect their networks without increasing workloads for security teams or hindering business productivity. Seamlessly integrated with our industry-leading NGFW platform, our cloud-delivered security subscriptions coordinate intelligence and provide protections across all attack vectors, providing best-in-class functionality while eliminating the coverage gaps disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform and secure your organization against even the most advanced and evasive threats. Benefit from Advanced URL Filtering or any of our security subscriptions.

Operational Benefits

The Advanced URL Filtering subscription enables you to:

- **Benefit from shared intelligence.** Take advantage of best-in-class web security with easy-to-use application- and user-based policies, alongside tight integration with Advanced Threat Prevention and Advanced WildFire .
- **Maintain total control over web traffic.** Use URL categories to automatically trigger advanced security actions, such as selective TLS/SSL decryption for suspicious sites.
- **Automate your security.** Save time as policy is applied to URL categories automatically, requiring no analyst intervention.
- **Gain insight into user and URL activity.** Enable your IT department to gain visibility into URL filtering and related web activity through a set of predefined or fully customized reports.

5. *Mobile Threat Landscape Report 2020*, Wandera, accessed May 6, 2021, <https://www.wandera.com/mobile-threat-landscape>.

6. "Top cybersecurity facts, figures and statistics," CSO from IDG, March 9, 2020, <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>.

7. *2020 Data Breach Investigations Report*, Verizon, accessed May 3, 2021, <https://enterprise.verizon.com/resources/reports/dbir>.

8. Forrester *Total Economic Impact* study.

9. Andy Elder, "Managing Risks and Resources to Lower Your Cybersecurity TCO," accessed January 26, 2022, <https://www.paloaltonetworks.com/cxo-perspectives/managing-cybersecurity-TCO>.

Table 1: Palo Alto Networks Cloud-Delivered Security Services	
Service	Description
Advanced Threat Prevention	Stop known exploits, malware, spyware, and command-and-control (C2) threat, while utilizing industry-first prevention of zero-day attacks. Prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
Advanced WildFire	Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60x faster with the industry-largest threat intelligence and malware prevention engine.
Advanced URL Filtering	Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
DNS Security	Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft, without requiring changes to your infrastructure.
Enterprise DLP	Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise with 2x greater coverage of any cloud-delivered enterprise DLP.
SaaS Security	The industry's only Next-Generation CASB natively integrated into Palo Alto Networks SASE offers proactive SaaS visibility, comprehensive protection against misconfigurations, real-time data protection, and best-in-class security.
IoT Security	Safeguard every "thing" and implement Zero Trust device security 20x faster with the industry's smartest security for smart devices.
AIOps	AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions.

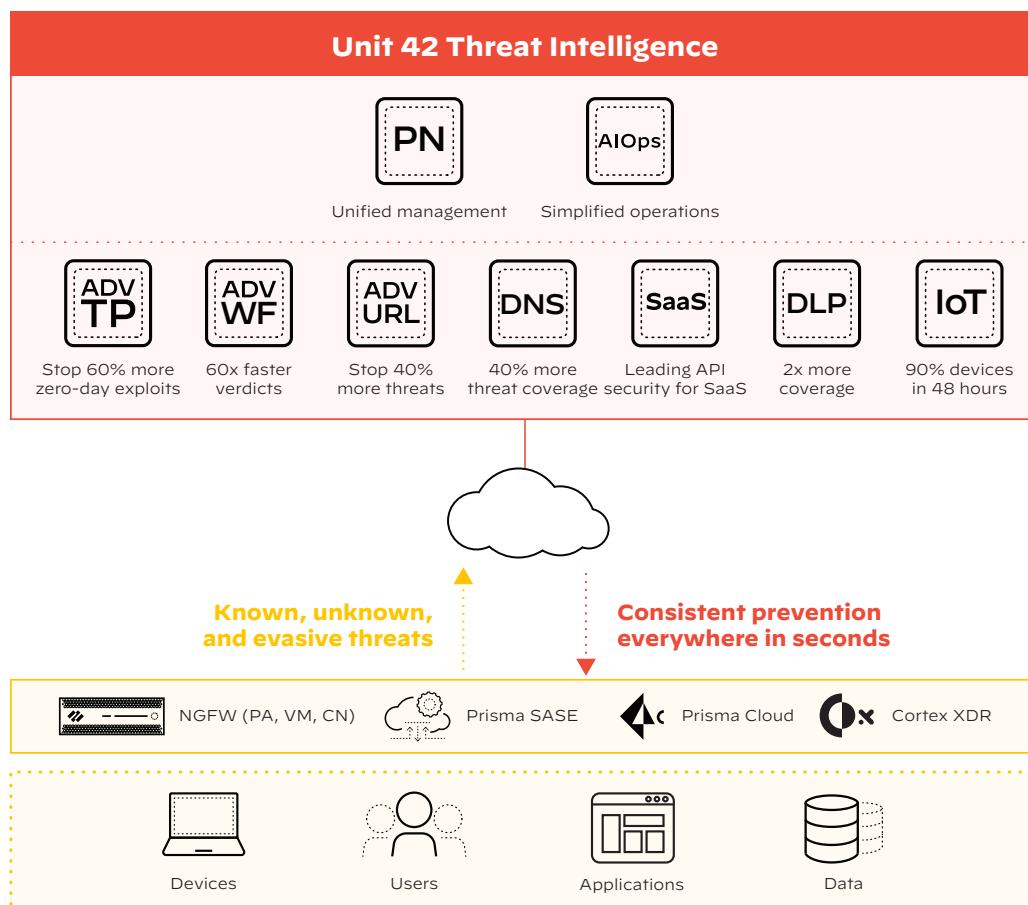


Figure 2: Palo Alto Networks Cloud-Delivered Security Services

Table 2: Advanced URL Filtering Features

Feature	Description
Inline Real-Time Web Threat Prevention	Uses cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time. ML models are retrained frequently, ensuring protection against new and evolving never-before-seen threats (e.g., phishing, exploits, fraud, C2).
Anti-Evasion Measures	Protects against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding.
URL Database	Maintains hundreds of millions of known malicious and benign URLs categorized through a combination of static, dynamic, machine learning, and human analysis.
Content Categories	Classifies websites based on site content, features, safety, and includes more than 70 benign and malicious content categories.
Risk Ratings	Scores URLs on a variety of factors to determine risk. These security-focused URL categories can help you reduce your attack surface by providing targeted decryption and enforcement for sites that pose varying levels of risk but are not confirmed malicious.
Multicategory Support	Categorizes a URL with up to four categories, allowing for flexible policy and the creation of custom categories.
Custom Categories	Lets you tailor categories and policies to your organization's needs. Although Advanced URL Filtering utilizes a defined set of categories, different organizations may have different needs around risk tolerance, compliance, regulation, or acceptable use. To meet your requirements and fine-tune policies, administrators can create new custom categories by combining multiple existing categories.
Real-Time Credential Theft Protection	Detects and prevents credential theft by controlling sites to which users can submit corporate credentials based on the site's URL category. This allows you to block users from submitting credentials to untrusted sites in real time while still allowing users to only submit credentials to corporate and sanctioned sites with zero false positives.
Phishing Image Detection	Uses ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.
Criteria Matching	Allows you to designate multiple policy action types based on URL categories or criteria. Beyond simply blocking or allowing sites, policy examples may include selective SSL decryption, advanced logging, blocking downloads, or preventing credential submission.
Selective SSL Decryption	Helps you further reduce risk with targeted decryption. Policies can be established to selectively decrypt TLS/SSL-encrypted web traffic, maximizing visibility into potential threats while keeping you compliant with data privacy regulations. Specific URL categories (e.g., social networking, web-based email, content delivery networks) can be designated for decryption while transactions to and from other types of sites (e.g., those of governments, banking institutions, healthcare providers) can be designated to remain encrypted. You can implement simple policies that enable decryption for applicable content categories with high or medium risk ratings. Selective decryption enables optimal security posture while respecting confidential traffic parameters set by company policies or external regulations.
Translation Site Filtering	Applies Advanced URL Filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.
Search Engine Cached Results Prevention	Applies Advanced URL Filtering policies when end users attempt to view the cached results of web searches and internet archives.
Safe Search Enforcement	Allows you to prevent inappropriate content from appearing in users' search results. With this feature enabled, only Google, Yandex, Yahoo, or Bing searches with the strictest safe search options set will be allowed, and all other searches can be blocked.
Customizable End-User Notifications	Enables administrators to notify users of a violation using a custom block page. These pages may include options to present a warning and allow the user to continue or require a configurable password that creates a policy exception.
Multilingual Support	Supports crawling and analysis in 41 languages.
Reporting	Provides visibility into Advanced URL Filtering and related web activity through a set of predefined or fully customized Advanced URL Filtering reports.

Table 3: Privacy and Licensing Summary**Privacy with Advanced URL Filtering Subscription****Trust and Privacy**

Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our [privacy datasheets](#).

Licensing and Requirements**Requirements**

To use the Palo Alto Networks Advanced URL Filtering subscription, you will need Palo Alto Networks Next-Generation Firewalls running PAN-OS 9.0 or later. Real-time web analysis is only supported on PAN-OS 10.2 Nebula and later.

Recommended Environment

Use Advanced URL Filtering with Palo Alto Networks Next-Generation Firewalls deployed in any internet-facing location, as ransomware, malware, grayware, phishing, credential theft, and C2 require external connectivity.

Advanced URL Filtering License

Advanced URL Filtering requires a standalone license, delivered as an integrated, cloud-based subscription for Palo Alto Networks Next-Generation Firewalls. It can also be available as part of an Enterprise Licensing Agreement or Software NGFW Credits.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
parent_ds_advanced-url-filtering_110922

Advanced Threat Prevention

Reimagine IPS: Prevent Zero-Day Threats in Real Time

One of the leading problems for network defenders today involves the rise of highly evasive and automated attacks. With access to sophisticated tool sets, adversarial as-a-service offerings, and versions of popular red team tools, bad actors have dramatically improved the speed and success of covert attacks. It has also become easy and inexpensive for malicious actors to find any vulnerabilities, exposures, and other unknown open doors that offer the least barrier to entry for a cyberthreat. We see that attackers are increasingly taking advantage of the windows of exposure—before vendors can patch vulnerable software—with zero-day exploits doubling year over year.¹ In addition, the 73% year-over-year rise in attacks using the highly customizable Cobalt Strike tool is just the start of this new wave of highly evasive attacks plaguing organizations today.² Encryption is another method attackers are leveraging to bypass traditional security controls, with reports showing that the vast majority of malware is now delivered through encrypted connections.³ Network security must evolve to stop highly evasive and unknown threats.

1. Patrick Howell O'Neill, "2021 has broken the record for zero-day attacks," MIT Technology Review, September 23, 2021.

2. Selena Larson and Daniel Blackford, "Cobalt Strike: Favorite Tool from APT to Crimeware," Proofpoint, June 29, 2021.

3. *Internet Security Report – Q2 2021*, WatchGuard Technologies, September 30, 2021.

Intrusion prevention or detection systems (IPS/IDS) are considered the foundation for network security to detect and deter the latest known threats. However, attackers are employing new techniques that make it easier to evade even today's "next-generation" IPS solutions. Traffic is typically only inspected on certain ports, and while adding single-function devices to the defensive stack may alleviate certain problems, it results in poor performance and a lack of overall visibility. Furthermore, the basics are often left uncovered, putting the onus on security teams who are not properly resourced to identify and patch vulnerabilities to confidently avoid data breaches. Most importantly, modern IPS solutions have not provided an answer for real-time prevention of unknown threats in critical phases of the attack lifecycle.

The Intrusion Prevention System Reimagined

Go beyond traditional IPS capabilities with Palo Alto Networks Advanced Threat Prevention, extending industry-leading protection against known threats to the prevention of the unknown. Advanced Threat Prevention is the industry's first IPS to stop zero-day attacks completely inline. Reduce your organization's window of exposure by stopping 90% of injection attacks and preventing 60% more zero-day exploits targeting software and web application vulnerabilities. If a threat actor is somehow able to infiltrate your network, receive protection at the last opportunity to stop an in-flight attack before a communication channel with the malicious actor is established. Advanced Threat Prevention prevents 96% of web-based hack tools such as Cobalt Strike and detects 48% more evasive command and control compared to our industry-leading Threat Prevention solution. Providing the widest visibility, Advanced Threat Prevention detects and blocks threats on any and all ports instead of invoking signatures based on a limited set of predefined ports. Our worldwide community of customers shares collective global threat intelligence, significantly reducing the success rate of advanced attacks by stopping them as they are encountered.

Business Benefits

The Advanced Threat Prevention security service enables you to:

- **Reduce business risk by preventing zero-day threats inline.** Prevent 96% of web-based Cobalt Strike, and detect 48% more evasive and unknown command and control compared to our industry-leading Threat Prevention solution. Prevent 90% of unknown injection attacks, and detect 60% more zero-day exploits compared to our industry-leading Threat Prevention solution.
- **Eliminate cost and management for stand-alone IPS.** Benefit from 45% breach reduction⁴ and leverage Snort and other powerful IPS capabilities integrated with our NGFW for a single security policy rule base.
- **Gain visibility into attacks, assuring your organization is protected.** Inspect all traffic for threats, regardless of port, protocol, or encryption.
- **Reduce the resources needed to manage vulnerabilities and patches.** Automatically block known malware, vulnerability exploits, and C2 with 100% effectiveness.⁵
- **Take advantage of full threat detection and enforcement of prevention controls** without sacrificing performance.

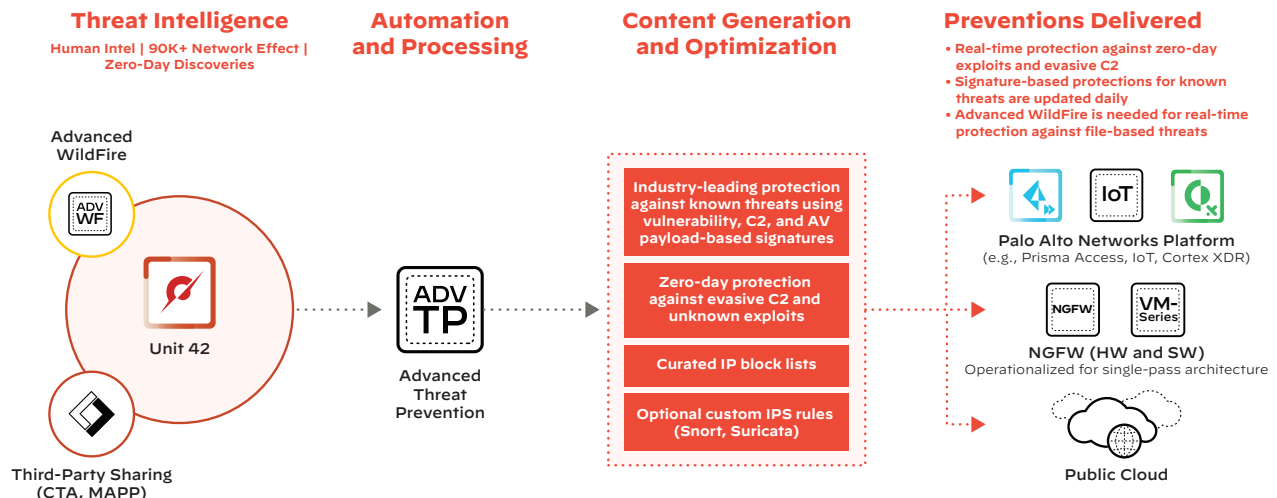


Figure 1: Palo Alto Networks Advanced Threat Prevention

4. Palo Alto Networks Cloud-Delivered Security Services Enhance Security And Compound Benefits Of Other Network Security Investments, a Forrester Consulting Total Economic Impact™ Spotlight commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, January 2021.

5. Next Generation Firewall Comparative Report, NSS Labs, July 17, 2019.

Advanced Threat Prevention benefits from our other cloud-delivered security subscriptions with daily updates that stop exploits, malware, C2, spyware, etc. A necessity for every Palo Alto Networks Next-Generation Firewall, Advanced Threat Prevention can speed the prevention of new unknown threats to real time when paired with other Palo Alto Networks subscriptions, including the Advanced WildFire malware prevention service for file-based threats, Advanced URL Filtering for web-borne attacks, DNS Security for attacks using the Domain Name Service, and IoT Security for unmanaged device visibility and context, to provide comprehensive protection across the entire attack lifecycle.

Key Capabilities

Leverage Industry-Leading Intrusion Prevention

Threat-based protections detect and block exploit attempts and evasive techniques at both the network and application layers, including port scans, buffer overflows, remote code execution, protocol fragmentation, and obfuscation. Protections are based on signature matching and anomaly detection, which decode and analyze protocols and use the information learned to send alerts and block malicious traffic patterns. Stateful pattern matching detects attacks across multiple packets, taking into account arrival order and sequence, ensuring all allowed traffic is well-intentioned and devoid of evasion techniques. Within our intrusion prevention technology, we offer:

- **Heuristic-based analysis** that detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.
- **Protocol decoder-based analysis** that statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits.
- **Protocol anomaly based protection** that detects non-RFC-compliant protocol usage, such as an overlong URI or FTP login.
- **Easy-to-configure, custom vulnerability signatures** that allow us to tailor intrusion prevention capabilities to your network's unique needs.

Because there are many ways to exploit a single vulnerability, our intrusion prevention signatures are built based on the vulnerability itself, providing more thorough protection against a wide variety of exploits. A single signature can stop multiple exploit attempts on a known system or application vulnerability.

Protect Against Malware

Inline malware protection—through signatures based on payload, not hash—blocks malware before it ever reaches the target host. This includes known malware, highly evasive malware, and future variants—even those not yet seen in the wild. Our stream-based scanning engine protects your network without introducing significant latency, which is a serious drawback of network antivirus offerings that rely on proxy-based scanning engines. Stream-based scanning inspects traffic as soon as the first packets of the file are received, eliminating threats as well as the performance issues associated with traditional standalone solutions. Key antimalware capabilities include:

- **Inline, stream-based detection and prevention** of malware hidden within compressed files and web content.
- **Protection against payloads** hidden within common file types, such as Microsoft 365 documents and PDFs.
- **Updates from Advanced WildFire to ensure protection against zero-day malware.** Signatures for all types of malware are generated directly from billions of samples collected by Palo Alto Networks, including previously unknown highly evasive malware sent to Advanced WildFire, our Unit 42 Threat Research team, and third-party research and technology partners worldwide.

Integrate with Advanced WildFire

Extend your protection against malware and C2 attacks with the Advanced WildFire service, the industry's largest malware prevention engine that uses machine learning and crowdsourced intelligence to protect organizations from the hardest-to-detect threats. The cloud-based service employs a unique multitechnique approach that combines static and dynamic analysis, custom hypervisors, and innovative machine learning techniques to detect and prevent known, unknown, and highly evasive malware. Once identified, Advanced Threat Prevention applies verdicts in real time to all ML-Powered NGFW form factors, instantly stopping threat proliferation across your enterprise.

Scan All Threats in a Single Pass

The Advanced Threat Prevention engine inspects and classifies traffic and detects and blocks both malware and vulnerability exploits in a single pass. Traditional threat prevention technologies require two or more scanning engines and multiple rule bases that need to be managed separately, adding significant latency and management overhead while dramatically slowing throughput performance. We use a uniform signature format for all threats to ensure rapid processing by performing all analyses in a single, integrated scan, eliminating redundant processes common to traditional solutions. Our Advanced Threat Prevention technology combs each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload. From this analysis, important details about a packet are identified, such as the application used, its source and destination, whether the protocol is RFC-compliant, and whether the payload contains an exploit or malicious code. Beyond individual packets, the context provided by the arrival order and sequence of multiple packets is also analyzed to catch and prevent evasion techniques. All of this happens within one scan, so your network traffic remains as fast as you need it to be.

Achieve 6X higher throughput with all security functions active using a single-pass architecture.⁶

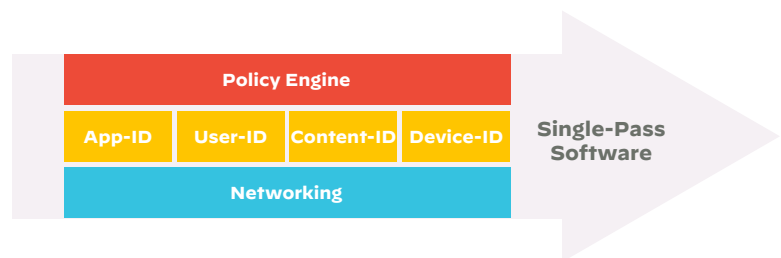


Figure 2: Palo Alto Networks NGFW Single-Pass Architecture

Zero-Day Prevention Inline

Advanced Threat Prevention introduces industry-first real-time prevention of zero-day threats, such as unknown exploit attempts and evasive command and control. Hackers are constantly monitoring software vendor bulletin boards for new vulnerability announcements they can leverage for initial access to a corporate network or to perform remote code execution. In fact, threat actors can begin to exploit a new CVE within 15 minutes of disclosure.⁷ Traditional approaches struggle to detect these unknown exploits, leaving the door open for bad actors to enter an organization's network and establish a command-and-control channel. Since malware communications must be observed in the wild first before protections can be released, organizations may suffer from being patient zero of an attack.

Advanced Threat Prevention addresses this challenge by providing multiple deep learning and machine learning models to detect common OWASP Top 10 security risk techniques, such as SQL and command injection. These models also detect evasive C2 inline and in real time. This is done by leveraging a combination of the high-fidelity dataset from Advanced WildFire, signals from soak sites, and intelligence from our Unit 42 Threat Research team. As traffic traverses the firewall, a prefiltered portion of traffic goes to the cloud for analysis, with a response sent back to the firewall to determine if the traffic should proceed. Based on these tuned models and integration with the NGFW, Advanced Threat Prevention provides real-time inline prevention of previously unknown exploit attempts and command and control. Specific models also identify C2 traffic from tools such as Cobalt Strike over key protocols such as HTTP, SSL, Unknown UDP, and Unknown TCP.

Utilize Custom Signature Compatibility

Advanced Threat Prevention also provides flexible support for Snort and Suricata rule conversion, providing easy-to-configure custom signatures. This support completely eliminates the need for standalone IPS or IDS solutions. With the conversion support, you can automatically convert, sanitize, upload, and manage Snort and Suricata rules, allowing you to take advantage of intelligence feeds while saving time and effort imposed by traditional signature-based IPS technologies. You can leverage exposed APIs to automate the process of applying new Snort rule coverage across your environment.



90%

prevention of injection attacks such as SQLi.

In addition, **60%** more detection of zero-day injection attacks.



96%

prevention of web-based Cobalt Strike C2.

In addition, **48%** more detection of evasive C2 traffic.

6. <https://start.paloaltonetworks.com/security-without-compromise.html>

7. Unit 42 Incident Response Report, Palo Alto Networks, July 26, 2022.

Succeeded (6/17) Succeeded with Warnings (6/17) Failed (3/17) Duplicates (2/17)			
LINE #	NAME	WARNINGS	DETAILS
2	Converted_ET_SHELLCODE Possible 0x0c0c0c Heap Spray Attempt_2012964	[performance_impact] use of tcp-context-free (0x0c0c0c0c)	Show
3	Converted_ET_SCAN_DCERPC pcgmctf ifds Unauthenticated BIND_2009832	[performance_impact] use of tcp-context-free (x051x)	Show
9	Converted_MALWARE-CNC Win.Trojan.Kuluoz outbound connection_29865	[performance_impact] use of tcp-context-free (HTTP/1.1.1x0D 0A)xAccept: /\^/\x0D 0A\xContent-Type: application/x-www-form-urlencodedx0D 0A\xUser-Agent: Mozilla/5.0 \Win	Show
10	Converted_MALWARE-CNC Dcc.Dropper.Agent variant outbound connection_40445	[performance_impact] bad PCRE - \x2fximages(0-9)+\x2e\xpHp (\x2fximages(0-9)+\x2e\xpHp	Show
11	IOC List 1	[wrong_rule] IP is not supported. You may need to replace with an IP address (\$HOME_NET)	Show
12	IOC List 2	[wrong_rule] IP is not supported. You may need to replace with an IP address (\$HOME_NET)	Show

Figure 3: Snort support on PAN-OS

Gain Additional Context on Threats in Your Environment

Leverage threat analytics data and threat intelligence from the [Threat Vault API](#) to improve your incident response processes. Through a programmatic RESTful API, access threat signature metadata and pertinent information to determine existing threat coverage, assist in threat alert investigation, and enrich incident response tickets.

Reduce the Attack Surface

Working seamlessly with the built-in, prevention-focused features of the ML-Powered NGFW, Advanced Threat Prevention, and the added capabilities from Palo Alto Networks Cloud-Delivered Security Services enables you to significantly reduce your organization's attack surface and associated business risk. This section provides some examples of complementary technologies.

SSL Decryption

The vast majority of enterprise network traffic is encrypted. This leaves a potential gap in network defenses if that traffic is not decrypted and scanned for threats. Our platform's built-in SSL Decryption service can selectively decrypt inbound and outbound SSL traffic. After decryption, all traffic is fully inspected and—if confirmed to be safe—re-encrypted before being allowed through to its destination.

File Blocking

Reduce the likelihood of a malware infection by preventing dangerous file types known to hide malware from entering your network. Executable files constitute a massive share of the malicious files used in spear phishing attacks. These files, combined with employee negligence, constitute a major security risk. File blocking functionality can be combined with User-ID, a standard feature on the Palo Alto Networks NGFW, to block unnecessary files based on users' job roles, making sure all users have access to the files they need and providing you with a granular way to reduce your exposure based on your organization's requirements. You can further decrease the number of attack opportunities by sending all allowed files to Advanced WildFire for analysis to determine if they contain zero-day malware.

Drive-by Download Protection

Unsuspecting users can inadvertently download malware merely by visiting a favorite website. Even a site's owners may not know when their site has been compromised. Our Advanced Threat Prevention technology identifies potentially dangerous downloads and sends a warning to the user to ensure that the download is intended and approved. Within Advanced Threat Prevention, the detection of such "phishing kit" landing pages, as well as the detection of web shell files (which aim to enable remote administration of web servers to target other internal systems), are packaged and delivered as spyware signatures. You can extend these capabilities and prevent attacks from new and rapidly changing domains by tying this feature to Advanced URL Filtering and file-blocking policies.

The Power of Palo Alto Networks Security Subscriptions

Today, cyberattacks have increased in volume and sophistication, using advanced techniques to bypass network security devices and tools. This challenges organizations to protect their networks without increasing workloads for security teams or hindering business productivity. Seamlessly integrated with the industry's first ML-Powered NGFW platform, our Cloud-Delivered Security Services coordinate intelligence and provide protections across all attack vectors, providing best-in-class functionality while eliminating the coverage gaps disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform, and secure your organization against even the most advanced and evasive threats. Benefit from Advanced Threat Prevention or any of the following security subscriptions:

- **Advanced Threat Prevention:** Stop known exploits, malware, spyware, and command-and-control (C2) threats while utilizing industry-first prevention of zero-day attacks. Prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire malware prevention:** Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60X faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering:** Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security:** Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.
- **Enterprise DLP:** Minimize the risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2X greater coverage than any cloud-delivered enterprise DLP.
- **SaaS Security:** The industry's only Next-Generation CASB natively integrated into the Palo Alto Networks SASE offers proactive SaaS visibility, comprehensive protection against misconfigurations, real-time data protection, and best-in-class security.
- **IoT Security:** Safeguard every "thing" and implement Zero Trust device security 20X faster with the industry's smartest security for smart devices.
- **AIOps:** AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions.

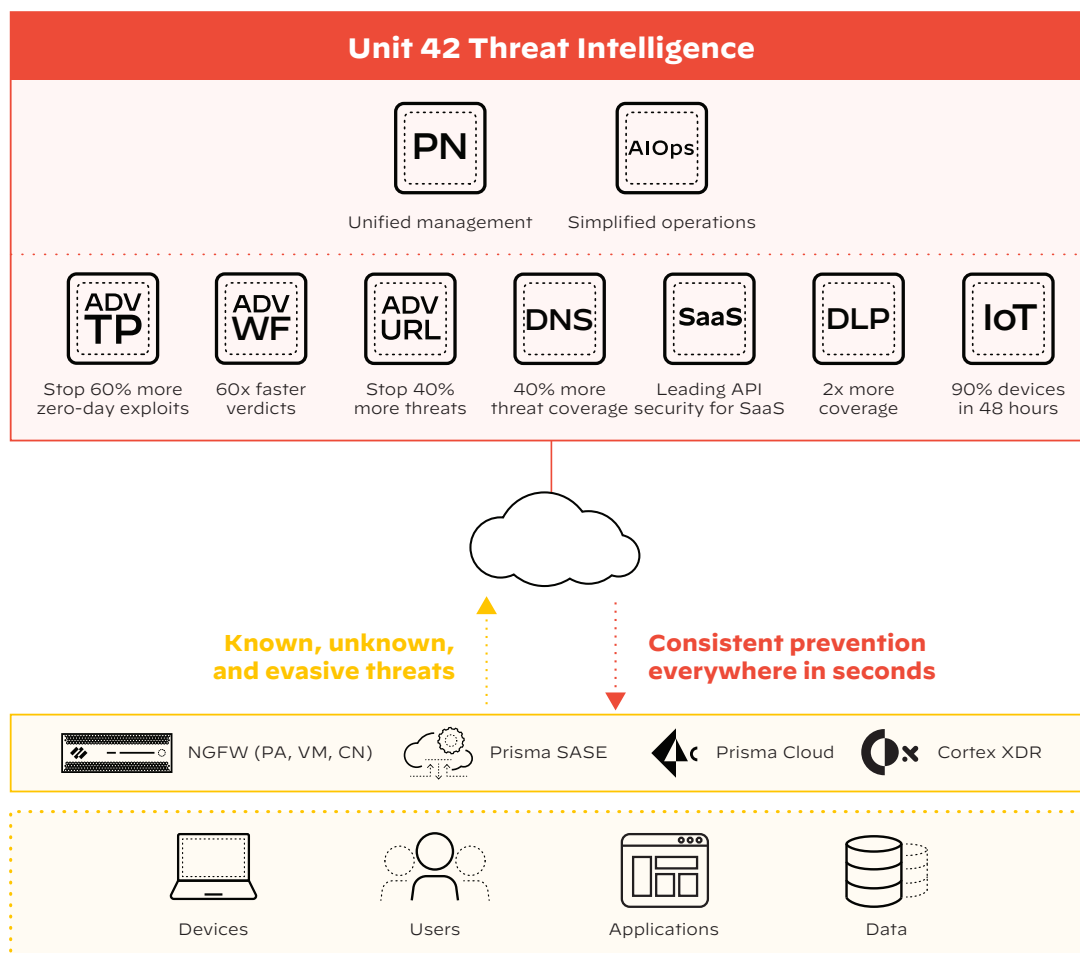


Figure 4: Palo Alto Networks Cloud-Delivered Security Services

Operational Benefits

The Advanced Threat Prevention subscription enables you to:

- **Lock down zero-day risk.** Automatically prevent unknown exploits and evasive C2 attacks inline.
- **Reduce actionable events and workload for the SOC.** Inline blocking of threats in real time saves time and resources spent on investigation post-execution.
- **Gain comprehensive security for all data, applications, and users.** Scan all traffic with full context around applications and users.
- **Deploy Snort signatures.** Automatically convert, sanitize, upload, and manage custom Snort and Suricata rules.
- **Gain additional context on threats in your environment.** Obtain threat metadata, indicators, signature release history, changelists, reports, and PCAPs via the Threat Vault API, and automate your incident response processes.
- **Leverage cloud scale to automate security.** Receive automatic updates and new capabilities over time to stay ahead of the changing threat landscape.
- **Keep your network secure with granular, policy-based controls.** Go beyond simply blocking malicious content to controlling specific file types, reducing the risk to your entire organization.

Table 1: Privacy and Licensing Summary

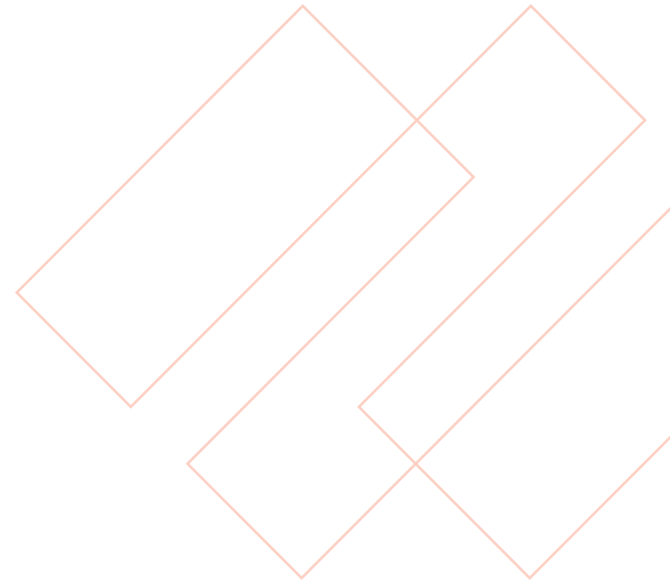
Privacy with the Advanced Threat Prevention Subscription

Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets .
Licensing and Requirements	To use the Advanced Threat Prevention subscription, you will need Palo Alto Networks Next-Generation Firewalls running PAN-OS 10.2 or later for the prevention of unknown C2 and PAN-OS 11.0 or later for the prevention of unknown exploits.
Recommended Environment	Palo Alto Networks Next-Generation Firewalls deployed in any location, as both internal and external sources may introduce network-based threats involving exploits, malware, spyware, C2, URLs, and more into your network.
Advanced Threat Prevention License	Advanced Threat Prevention requires a standalone license, delivered as an integrated, cloud-based subscription for Palo Alto Networks Next-Generation Firewalls. It is also available as part of the Palo Alto Networks Subscription ELA, Bundles, Firewall Flex, or Prisma Access.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
parent_ds_advanced-threat-prevention_111022



Premium Support

Maintaining your security infrastructure is a mission-critical task. Our Customer Support and Maintenance programs are designed to ensure that traffic flows smoothly and securely across your network. When problems arise, our dedicated Support Services team will quickly and proficiently resolve any questions or challenges.

As an industry leader, our comprehensive set of Support Services underscores our commitment to the ongoing success of your Palo Alto Networks infrastructure. With business-critical Customer Support options, 24/7 availability, and a global network of support centers and parts-replacement depots, organizations of all sizes and complexities around the world can rely on Palo Alto Networks Customer Support Services for fast and dependable service.

Benefits

- Improved system availability with continual software enhancements and outstanding responsiveness.
- Increased uptime and expedited issue resolution with Palo Alto Networks specialists augmenting your internal technical resources.
- Optimized security architecture to reduce and prevent security events.
- Improved operational efficiency.
- Enhance your investment in your internal IT resources with access to technical support by phone and online.

Premium Support: Service Overview

The Palo Alto Networks Premium Support offering enhances your in-house resources with technical experts available to support your Palo Alto Networks security infrastructure. This support level also gives you access to Security Assurance to assist when security incidents occur and you need to augment your staff with security experts.

Premium Support is ideal for organizations that want to work directly with Palo Alto Networks to address their support needs with 24/7, year-round assistance as well as keep up to date with the latest upgrades and updates.

Features

Premium Support provides access to:

- **Feature releases and software updates:** Stay current with the latest features and software updates.
- **Subscription services updates:** To ensure your Palo Alto Networks deployment stays up to date, you can configure devices to automatically download App-ID technology, URL Filtering, DNS Security, Threat Prevention, and WildFire service updates. Alternatively, these updates can be downloaded and manually applied.
- **Security Assurance:** In the event you detect suspicious activity in your network, Security Assurance gives you access to our security experts with unique threat intelligence tools and practices for your Palo Alto Networks footprint. Our team will help orient initial investigations, facilitate the collection of logs and indicators of compromise (IoCs), while expediting hand-off to your preferred incident response (IR) vendor. See our [End User Support Agreement](#) for the latest details.
- **Direct access to product experts:** Interact with a support engineer trained to quickly understand and resolve your unique challenges.
- **Premium Support availability:** Enjoy 24/7 support for issues of all severities with Platinum senior engineers available around the clock to assist.
- **Online Customer Support Portal:** A feature-rich platform provides access to product documentation, problem resolution databases, peer-to-peer interaction, and support case management.

Table 1: Palo Alto Networks Support Offering Summary

Support Comparison	Premium	Platinum*
1. Technical Support		
Telephone Support	24/7	24/7
Call Response Time		
Severity 1: Critical Product is down, and customer production environment is critically affected. No workaround available yet.	< 1 hour	< 15 minutes
Severity 2: High Product is impaired, and customer production is up but impacted. No workaround available yet.	2 hours	< 30 minutes
Severity 3: Medium A product function has failed; customer production is not affected. Support is aware of the issue, and a workaround is available.	4 hours	< 2 hours
Severity 4: Low Noncritical issue. Does not impact customer business. Feature, information, documentation, how-to, and enhancement requests from customer.	8 hours	< 4 hours
Support Specialist Type	Support Engineer	Senior Engineer
RMA (NBD included, 4-hour service optional)	NBD 4 Hr.	NBD 4 Hr.

Table 1: Palo Alto Networks Support Offering Summary (continued)

Support Comparison	Premium	Platinum*
2. Security Assurance Incident Support		
Assisted security investigations	•†	•
Advanced log and IoC analysis	•†	•
Next steps recommendations	•†	•
3. Expert Assistance		
Prescheduled event support	—	•
On-site assistance for critical issues (after remote troubleshooting)	—	•
Failure analysis (HW)	—	•

* Investment minimum required.

† Other restrictions may apply. Please see our [EUSA](#) for details.

- **Case management:** Submit, update, check status, and manage support cases for all your supported Palo Alto Networks products via the online Customer Support Portal.
- **Documentation and FAQ:** Access product manuals, technical guides, software release notes, and frequently asked questions (FAQ) to streamline operations and incident resolution.
- **Next-business-day delivery for parts and hardware replacement:** Get fast turnaround for hardware replacement. Note: The Next-Business-Day Delivery Service is subject to certain limitations. Please see the [Return Materials Authorization \(RMA\) Process Policy](#) for details.
- **(Optional) 4-hour RMA service for parts and hardware replacement:** For an additional fee, hardware replacement services can be upgraded to a 4-hour shipment for a rapid RMA turnaround. 4-Hour Premium Support RMA is an optional upgrade to Premium Support for customers and data centers requiring mission-critical response times that are located within a specified range of a Palo Alto Networks service location. With the optional upgrade to 4-Hour Premium or 4-Hour Partner Premium Support, Palo Alto Networks will make commercially reasonable best efforts to deliver replacement component hardware to you within four hours from issuance of an RMA, 24/7, year-round.

Customer Support Services Program

Palo Alto Networks provides you with a range of several customer support and maintenance options designed to meet the unique needs of your business:

- Standard Support (US only)
- Premium Support
- Platinum Support
- Focused Services
- On-Site Spares Hardware Program

Whichever support and maintenance plan you choose, you will experience our commitment to delivering the highest level of customer service. The goal of our program is to minimize business disruption, maximize protection, and increase the value of your investment.

Partner Enabled Premium Support

In addition to Standard or Premium Support delivered directly by Palo Alto Networks, you may choose a technical support offering from a Palo Alto Networks Authorized Support Center (ASC). ASC-designated partners provide Level 1 and 2 support with the added value of local language, multivendor, or customized support that complements Palo Alto Networks offerings.

When you choose support from an ASC, Palo Alto Networks will provide the partner with Partner Enabled Premium Support to enable them to better support you. This gives the ASC advanced support, 24/7, year-round coverage, and next-business-day shipment or 4-hour advanced replacement services.

More Information

To learn more about Palo Alto Networks Support offerings, visit paloaltonetworks.com/support or contact your local account manager. For product information, visit <https://www.paloaltonetworks.com/products/products-a-z>.

Why Palo Alto Networks?

Palo Alto Networks is committed to your success in preventing successful cyberattacks. Our award-winning services organization gives you timely access to technical experts and online resources to ensure your business is protected. We take our responsibility for your success seriously and continuously strive to deliver an exceptional customer experience. Our entire services organization and Authorized Support Centers are there to ensure maximum uptime and streamlined operations.



2015–2021: Palo Alto Networks, Inc. has been recognized by J.D. Power for seven consecutive years for providing “An Outstanding Customer Service Experience” for its Assisted Technical Support.



2015–2021: TSIA certification recognizes that Palo Alto Networks meets the highest industry support standards and has achieved Global Rated Outstanding Assisted Support for a seventh consecutive year.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. parent_ds_premium-support_071823

Exhibit C

3.2 Pricing Detail – One Year Pricing Option

DirSec Corporate Office 357 McCaslin Blvd. Suite 200 Louisville, CO 80027						
WWW.DIRSEC.COM Est. 2001						
Quote - One Year						
Quote #: Poudre_PaloAlto_122023						
Date: December 20, 2023						
Prepared for: <i>Poudre School District</i>						
Attention:						
Email:						
Terms: Net 30						
Quoted by: Dade Myres						
E-mail: dmyres@dirsec.com						
Phone: 303.588.6938						
Line #	Qty	Product/ Model #	Product Description	List Unit Price	Total Retail Price	Total with Discount
1	2	PAN-PA-5410-AC	Palo Alto Networks PA-5410 with redundant	\$ 72,660.00	\$ 145,320.00	\$ 78,930.56
2	2	PAN-PA-5410-GP-1YR-HA2	PA-5410, GlobalProtect subscription	\$ 13,230.00	\$ 26,460.00	\$ 19,358.14
3	2	PAN-PA-5410-AWF-1YR-HA2	PA-5410, Advanced WildFire subscription	\$ 18,320.00	\$ 36,640.00	\$ 29,399.94
4	2	PAN-PA-5410-ADVURL-1YR-HA2	PA-5410, Advanced URL Filtering subscription	\$ 19,740.00	\$ 39,480.00	\$ 26,554.25
5	2	PAN-PA-5410-ATP-1YR-HA2	Advanced Threat Prevention subscription	\$ 19,740.00	\$ 39,480.00	\$ 26,554.25
6	2	PAN-SVC-PREM-5410-1YR	Premium support 1-year prepaid, PA-5410	\$ 13,080.00	\$ 26,160.00	\$ 22,649.33
			TERMS OF COVERAGE: 1 YEAR			
				Total	\$ 313,540.00	\$ 203,446.45
Quoted prices valid for 30 days. Quote is subject to revision or cancellation prior to acceptance by the customer. Prices quoted do not include applicable sales tax.						
DirSec will only accept credit card payments for transactions that are less than \$10,000.						
Representing the Best of Breed Vendors:						
Cloud Data Security (Including SASE, SWG, CASB, CSPM, DLP), Next Generation Endpoint Protection and Remediation, Structured Data Security, Web Application Security, User & Entity Behavioral Analytics, Next Generation SIEM , PIM/PAM, Vulnerability Management, Security/Risk/Compliance Optimization/ Enforcement						
Services include: Managed Services, Architectural Review and Design, Implementation, Upgrades						