TRANSITION TO A CYBERSECURITY PLATFORM TO IMPROVE EFFECTIVENESS AND EFFICIENCY

SPOTLIGHTS

Industry
Local Government

Use Case
Reduce security complexity as well as improve efficiency and effectiveness with a platform approach

Business Benefits
- Reduces risk of business interruption or data breaches with automated threat identification and prevention across clouds, networks and endpoints.
- Decreases security costs and demand on security resources with unified security data, automation and fewer devices.
- Enables productivity with granular security policies that meet the needs of different departments.

Operational Benefits
- Unifies security visibility across your endpoints, networks and cloud resources.
- Leverages existing security investments while expanding security capabilities as needed.
- Reduces manual work of correlating threats and logs across multiple security products.
- Reduces manual work of creating and maintaining security policy rules for each product.
- Improves visibility and simplifies compliance with a consolidated set of screens, dashboards, logs and reports on various security threats, including data exfiltration attempts.

Security Benefits
- Automatically correlates threat intelligence feeds and insights across cloud, network, servers and endpoints.
- Continually updates threat prevention to every platform sensor – endpoint, network or cloud.
- Eliminates shadow IT with granular policies and application visibility across network, SaaS and cloud.
- Uses network segmentation to limit users, applications or content in critical environments.
- Reduces the chances of issues with outdated or misconfigured security policies.

Business Drivers

City, county and municipal governments seek to provide more services for less. Managing resources and budgets to achieve this goal extends to IT and Operational Technology, or OT, networks, even as local governments adopt a range of digital technologies to better serve citizens and improve efficiency. Digital government initiatives offer easier access to services for citizens and businesses. For employees, laptops and mobile devices enable valuable work outside government offices. Remote sensors and devices automate services, gather data and monitor equipment for smart cities and SCADA networks. These networks, devices and data need protection, and local governments want to use security resources efficiently – particularly since the demand for cybersecurity professionals outstrips supply.[1]

Local governments must regularly demonstrate compliance with applicable data protection, privacy, accounting and other regulations.

Business Problem

Every expansion into digital technologies introduces potential vulnerabilities and points where the network can be infiltrated. Government data breaches usually involve the loss of valuable personal information or confidential data while nation-state attacks and hacktivism threaten critical infrastructure. As hackers and their techniques become more sophisticated, it's difficult for employees to discern legitimate links and files from targeted attacks designed to steal credentials or sensitive information. To complicate matters, experts say local governments are disproportionately targeted by ransomware.[2]

High-profile data breaches have elevated the importance of cybersecurity in senior government positions. Management now wants regular reports on cybersecurity statistics and effectiveness. These are proving difficult and time-consuming to pull together as security products proliferate.

1. http://blog.indeed.com/2017/01Ad/17/cybersecurity-skills-gap-report/
2. thehill.com, December 2017: Local governments grapple with ransomware threat

As cyberattacks increase in volume and sophistication, governments are finding it more difficult to keep pace with thwarting them. Since 98 percent of network compromises take only minutes to execute,[3] the focus must be on prevention rather than detection. Preventing the spread of new or multi-method threats requires correlation and coordination, which are two areas where discrete security functions – such as within a UTM – and products fall short. Correlation and coordination become even more difficult to execute as the number of vendors and products increases.

Finally, local governments must regularly demonstrate compliance with applicable data protection, privacy, accounting and other regulations. Data aggregation and correlation between multiple security products to support these initiatives are time-consuming for security teams.

Traditional Approaches

As new digital technologies or threats have emerged, the traditional approach has been to add new, discrete security appliances and products to the network and its elements. For example, security vendors countered application-level attacks with intrusion prevention systems. Phishing emails increased the popularity of content filtering. As governments move into SaaS and cloud, separate cloud-based security products are attempting to gain momentum.

This approach results in an explosion of separate cybersecurity appliances and products, including:

- Firewalls
- Web proxy servers
- Network intrusion detection/prevention
- Gateway antivirus/anti-spam
- Email security appliances
- Virtual private network clients and appliances
- Content filtering
- Web content filtering
- Zero-day exploit prevention
- Cloud Access Security Broker products
- Security for individual SaaS applications
- SSL decryption devices
- Endpoint security
- Antivirus

Local government business remains at risk when disparate security capabilities cannot correlate attacks across multiple vectors or are slow to prevent never-before-seen threats. Among the reasons:

- **Lack of visibility:** With disparate point products, it's difficult to get a correlated view of traffic and potential threats across endpoints, networks and cloud environments.
- **Operational complexity:** Each point product is separately managed by its own management interface and requires time and training to manage, resulting in greater overhead for security teams that must manually update security appliances, correlate insights, amalgamate logs and events, and trawl through logs.
- **Higher costs:** More security devices cost more to purchase, support and manage.

It's becoming more common to link many separate security products together using a security information and event management product. SIEMs are useful for forensic analysis, incident response, operational intelligence and remediation; however, they are not fast enough to prevent today's cyberattacks from successfully penetrating governments. SIEM systems are typically customized, so they cost more to maintain and change as government requirements and networks evolve.

Some security vendors attempt to consolidate multiple security functions into a single physical appliance, sharing power, cooling and rack space. However, their software technologies remain unintegrated, and they cannot share context and correlate between security functions. Many vendors have separate management interfaces for different security functions. For example, their email security scanning may be separate from their firewall security scanning, which may be different from their antivirus and endpoint security. These separate functions still require security teams to manually correlate logs and events.

3. Verizon 2017 Data Breach Investigations Report

Palo Alto Networks Approach

In stark contrast to other approaches, Palo Alto Networks® consolidates multiple security functions above into a single, natively integrated platform (see Figure 1), safely enabling users, applications and traffic across endpoints, servers, networks, cloud and SaaS environments.

The key advantages of this platform approach include:

- **Faster, better threat prevention:** Automatic correlation of insights between security functions and automatic distribution of signatures to sensors quickly repel the newest threats – including exploits, ransomware and other malware, as well as fileless attacks – in all locations. This means security teams can easily adopt security best practices using app-, user- and content-based policies with a Zero Trust approach.
- **A focus on what matters:** Automate security controls with policies that dynamically change to match your application, users and content. A single pane of glass provides complete visibility into users, applications and traffic across all locations, simplifying management for network and security teams. No more logging into individual management interfaces and attempting to correlate incidents or track them as they move through different appliances.
- **Faster consumption of security innovations:** To keep up with the latest threats, you want to continually improve security effectiveness and efficiency. Add tightly integrated security functions over time without additional training or management overhead. The platform works in tandem with other security devices, such as data loss prevention appliances, and can ingest third-party threat intelligence feeds. Easily add custom or third-party security apps tuned to your business, without deploying new infrastructure, while making use of a unified security data set, sensors and enforcement points.

To better understand how Palo Alto Networks government customers have leveraged the Security Operating Platform to prevent successful cyberattacks, focus on what matters and achieve even more benefits, read the following about a local city government's deployment.

Figure 1: Palo Alto Networks Security Operating Platform

Real-World Local Government Customer Deployment

This example profiles a large U.S. city with a centralized IT department that provides several services for many agencies. Several years ago, the IT department began to refresh and strengthen network security for its mission-critical Enhanced 911 call center environments. As the city's security strategy matured, it amalgamated and centralized its security teams and stood up its first Security Operations Center, or SOC. Over time, the city centralized security and took on the role of managing and securing internet access for all its many agencies, even though each had different security policies and access requirements. Beginning with a modest deployment of the Palo Alto Networks Security Operating Platform, the city expanded the volume and breadth of the platform over several years and stages, increasing its traffic and threat visibility while simplifying security operations. Visibility and control of all applications – including SaaS applications – combined with new zero-day threat prevention and SSL decryption capabilities, mean the city now stops 1 million threats per month on average, without any increase in security resources.

Benefits Customer Realized With a Platform Approach to Cybersecurity

The city enjoys the following business, operational and security benefits with its expanded use of the Security Operating Platform.

Business Benefits

- Decreases capital and operations costs with fewer devices to deploy and manage.
- Enables productivity while reducing risk via granular security policies that meet the business needs of different departments.

Operational Benefits

- Reduces manual work of correlating threats across many devices and point products.
- Meets departmental needs for different security policies while cybersecurity group maintains overall visibility of policies, traffic and threats.
- Achieves better performance with a single-pass architecture.
- Minimizes operations disruption and IT/security team training costs with the ability to add new security functions as needed on a single platform.

- Supports compliance requirements for SSL decryption as part of a platform.
- Reduces the number of security policies and rules.

Security Benefits

- Stops ransomware, credential theft, everyday attacks and other zero-day threats – 1 million threats per month on average.
- Achieves better visibility into threats through a single pane of glass, with context and analysis.
- Reduces the attack surface by eliminating unknown or unsanctioned applications, including SaaS applications.
- Protects legacy endpoints in air-gapped or SCADA environments.
- Prevents data exfiltration through SaaS applications, email or other means.

Stage 1: Initially, the city aimed to secure outbound internet traffic for its mission-critical E911 network. Its perimeter locations had Cisco® ASA firewalls, another appliance for IPS/IDS, and Blue Coat® web filtering. One goal was to achieve granular control over allowed applications while blocking all others, so application awareness was a must. Another was to simplify the security infrastructure at the perimeter. After some evaluation, the security team realized they could do both, with less overhead and fewer products, with Palo Alto Networks Security Operating Platform. Later in this stage, they also purchased more than two dozen next-generation security appliances to secure inbound internet traffic.

Stage 2: The city was in the process of moving its applications to the cloud and wanted to ensure both that threats did not infiltrate the network from SaaS applications and that data was not exfiltrated. One issue was employees downloading and using their own versions of SaaS applications, such as Box, rather than enterprise-licensed versions. The city had no visibility into these applications or what entered or exited through them. At this stage, the city turned on Palo Alto Networks Aperture™ SaaS security service, part of the Security Operating Platform. It now gives the security team visibility into SaaS applications in use on the network from the same management interface as the applications in the data center. They have the flexibility to block unsanctioned SaaS applications – such as personal Box accounts – for some users. Now, most employees can only access their corporate SaaS applications, and data filtering policies reduce the possibility of accidental exfiltration of sensitive data.

Stage 3: The city had recently purchased an endpoint security product, but it was not suitable for air-gapped environments, such as the E911 network, or SCADA environments where the city could not update the operating systems of old servers. To protect these critical operational assets, the team deployed Palo Alto Networks Traps™ advanced endpoint protection. At the same time, they amalgamated all cybersecurity for the entire city – including several stand-alone agencies – into one organization. The city refreshed its second call center environment and replaced numerous point products with Palo Alto Networks next-generation firewalls.

Stage 4: The amalgamated cybersecurity organization now offers free internet access to most city agencies. Previously, city agencies had to pay for this service or manage their own internet access. With demand for internet access expected to snowball, the cybersecurity group had to scale its capacity, roughly 5 to 10 Gbps, up to 40 Gbps. The team projects the demand might reach 100 Gbps throughput eventually, and they know Palo Alto Networks appliances will help them reach this goal while also handling the necessary SSL decryption for the environment.

Next steps: Moving to the cloud is a city-wide initiative. The city is currently evaluating Palo Alto Networks virtualized appliances to secure its Microsoft® Azure® and Amazon® Web Services environments. The city will be able to use the same tools to create application whitelisting policies that reduce the possibility of threats breaking through.

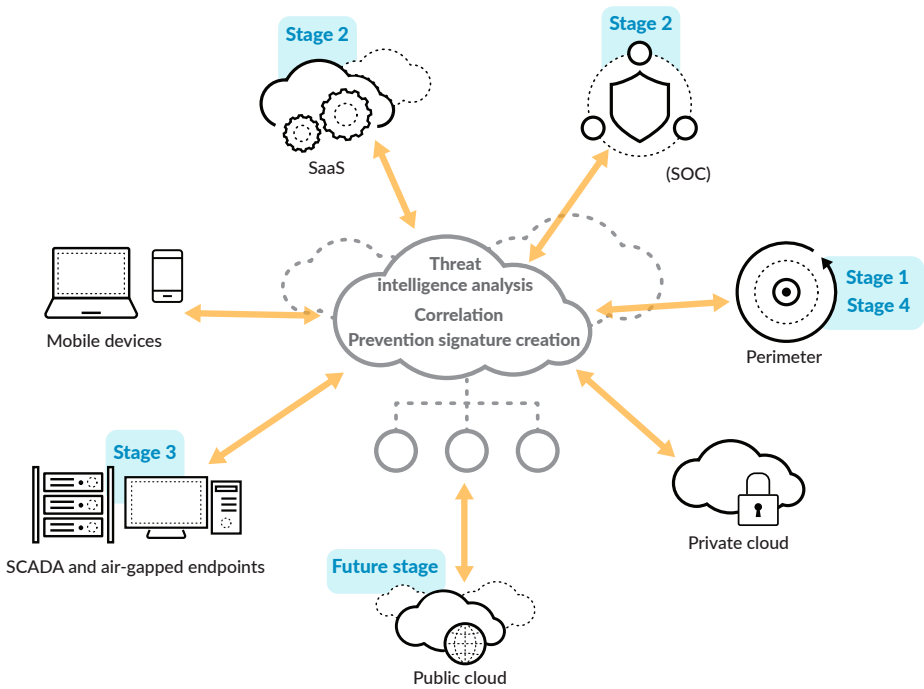

Figure 2: Automatically preventing successful cyberattacks and expanding platform use over time

Implementation Overview

Products deployed:

Stage 1:

- Palo Alto Networks PA-5050 next-generation firewall with subscriptions to Threat Prevention, URL Filtering and WildFire® cloud-based threat analysis service
- PA-5060 next-generation firewalls with Threat Prevention, URL Filtering and WildFire
- Panorama™ network security management
- WildFire private cloud appliances – WF-500

Stage 2:

- Aperture SaaS security service

Stage 3:

- Traps advanced endpoint protection
- (24) PA-5060 next-generation firewalls with Threat Prevention, URL Filtering and WildFire

Stage 4:

- PA-7080 next-generation firewalls with Threat Prevention, URL Filtering and WildFire

How the customer implemented a platform approach to cybersecurity (high level):

At the internet edge and protecting the E911 network:

- **Point product consolidation:** Each next-generation security appliance serves as an application-aware firewall and intrusion prevention system; performs network anti-malware and DNS sinkhole functions; and conducts web filtering, SSL decryption and zero-day threat prevention; eliminating multiple stand-alone point products and dramatically reducing the management complexity of perimeter security.
- **Private sandbox environment:** WF-500 appliances provide a private malware analysis sandbox so the security team can analyze suspicious files in the network without having to send them to the cloud. Next-generation security appliances automatically forward suspicious files to the WF-500, which analyzes them and automatically sends confirmed malware to WildFire for signature generation. Generated signatures are automatically distributed to all WildFire customers.
- **Granular application control:** Application-aware endpoints, appliances and SaaS offerings enable the security team to maintain exacting control over users' permissions. For example, employees can access Facebook® at work but can't use the chat feature. Employees in some agencies can use personal Box folders but cannot upload to them, and any content downloaded from personal Box folders is scanned for potential threats.
- **Granular policy control:** Different users and agencies have different work needs, enforceable by policy. For example, the police investigations unit can access adult websites, while others cannot.
- **Native SSL decryption:** This capability of the next-generation firewalls enables the security team to define what traffic to decrypt and ensures compliance with security regulations.

In air-gapped and SCADA environments:

- **Advanced endpoint protection:** Traps protects more than 1,000+ Windows® endpoints and servers, particularly legacy systems that can no longer update their operating systems and/or custom applications. Rather than relying on signatures that try to keep up with the ever-growing list of threats, Traps uses exploit and malware prevention techniques, policy-based restrictions and other roadblocks that prevent attacks at initial entry points.
- **Application whitelisting:** This feature enables the city to secure particularly sensitive environments by enabling the passage of only the applications they expressly allow.

In the SOC:

- **SaaS visibility and control:** Aperture ensures most employees use only corporate SaaS applications, restricts uploads to the few employees using personal SaaS applications and eliminates threats, such as malware, attempting to infiltrate the network through Office 365®, Box or other SaaS applications.

- **Security management consolidation:** Panorama network security management provides a single pane of glass through which to manage all applications and traffic traversing the networks, clouds and endpoints. From a single console, security teams enjoy real-time views, logs and reports across all security functions. They can see which URLs have been recently blocked, which known threats have been detected and blocked, and which suspicious files have been sandboxed by WildFire. Furthermore, they can generate quality reports on traffic and threats in minutes, instead of the many hours it took previously.

Best Practices and Deployment Considerations

Palo Alto Networks appliances are available in a range of physical and virtualized form factors for all popular virtual environments, serving remote offices, ruggedized locations, headquarters and data centers. With Palo Alto Networks virtualized appliances, governments can extend security and network policies to Amazon Web Services, Microsoft Azure and Google® Cloud Platform environments as well as hybrid and private clouds.

Some government agencies may not wish to send files to a cloud-based malware analysis environment for inspection or have their appliances communicate with a vendor's network outside their organization. These agencies can implement their own private malware analysis environments and optionally configure them to receive signature updates and other preventions from the Palo Alto Networks threat intelligence cloud, either automatically or via manual updates.

Additional Resources

The following links offer additional information on protecting city, county and municipal networks, endpoints and cloud resources with a platform approach.

- **Provincial/State/Local government resources:** https://www.paloaltonetworks.com/solutions/industries/government/government-state-local
- **ICS/SCADA Use Case: Windows-based Endpoint Security:** https://www.paloaltonetworks.com/resources/whitepapers/ics-scada-use-case-windows-based-endpoint-security.html
- **Use Case: Secure the Network through Application Visibility:** https://www.paloaltonetworks.com/resources/whitepapers/secure-the-network-through-application-visibility
- **Government Use Case: Network Security Consolidation:** https://www.paloaltonetworks.com/resources/whitepapers/network-consolidation-usecase
- **Build a Next-Generation SOC:** https://www.paloaltonetworks.com/resources/techbriefs/build-next-generation-soc
- **Aperture for SaaS Applications:** https://www.paloaltonetworks.com/products/secure-the-cloud/aperture-for-saas

Services to Help You

Support

Palo Alto Networks Customer Support automates the discovery of related cases to increase productivity and get you to a resolution more quickly. We offer multiple support packages: Standard, Premium and Premium Plus. You can also opt for your own technical account manager as a subscription-based extension of Premium Support. Premium Plus provides both a designated technical support engineer and technical account manager who will learn and understand your deployment at both technical and business levels, accelerating incident resolution.

Consulting

Palo Alto Networks Consulting Services provides access to specialized talent knowledgeable in ensuring the safe enablement of applications. By matching talent to task, we deliver the right expertise at the right time, dedicated to your success. Resident engineers, for example, provide on-site product expertise and are uniquely qualified to advise you on getting the most out of your Security Operating Platform deployment.

Education

Training from a Palo Alto Networks Authorized Training Center delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications provide the necessary Security Operating Platform knowledge to prevent successful cyberattacks and safely enable applications.

Participate in a Cyber Range to get the latest interactive cyber defense training to keep your teams razor-sharp. Cyber Range arms network and security professionals with the skill sets and insight to use the most advanced technology to thwart the most advanced attacks hitting networks today. A cross-disciplinary training tool and a highly immersive team-building experience, Cyber Range is an exciting and fun way to effectively train all your front-line people.

Conclusion

As local governments embrace more digital technologies, they must find ways to efficiently protect the data entrusted to them, maintain critical and everyday operations, and serve citizens efficiently. Network and security teams have enough to manage without constant manual security updates, log aggregation, event correlation and security actions from multiple management interfaces. A survey of almost 150 of our customers showed that consolidating multiple security functions on a single platform resulted in Opex savings and, moreover, improved attack analysis.[4] These customers deployed an average of 3.2 subscriptions on their next-generation appliances and reported average reductions of:

- 26 percent in the amount of time required to add new rules to manage their firewalls.
- 25 percent in the number of security alerts requiring human intervention.
- 30 percent in the time it takes an analyst to investigate an event in order to drive a technical action to prevent or block an incident.

These savings could be yours. For more information on how security network consolidation with Palo Alto Networks could reduce your total cost of ownership, reach out to your Palo Alto Networks account team and sign up for a free TCO calculator session.

4. The Value of the Next-Generation Security Platform: https://www.paloaltonetworks.com/resources/techbriefs/value-of-next-generation-security-platform

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