CYBERSECURITY FOR GOVERNMENTS

A Platform Approach

As governments modernize their IT infrastructures, their cybersecurity must keep pace. Palo Alto Networks® meets the cybersecurity needs of its government customers by automatically preventing the latest cyberthreats, enabling granular control of sensitive data and dramatically improving security visibility. Security sensors automatically coordinate threat prevention across endpoints, networks, data center and cloud environments, and IT and OT networks.

Government Digital Transformation and IT Modernization Initiatives Must Be Secure:

- Cloud-first policy
  - Public cloud
  - SaaS
- Shared services
- Enterprise platforms
- Smart nations
- Enterprise consolidation
- Continuous monitoring and threat mitigation

Governments are modernizing their networks to take advantage of digital innovations and improve the way they communicate with citizens. They are doing so cautiously as nation-states and other adversaries continue to threaten sensitive information, military networks and communications with evermore advanced tactics.

Thwarting the Cyberattack Lifecycle

In numerous successful attacks against governments worldwide, adversaries have used each stage of the cyberattack lifecycle – from reconnaissance and delivery to exploitation, command and control, and exfiltration – often within minutes. Successful cyber defense must start with addressing two systemic problems: the misinterpretation of defense in depth and an ineffective approach to threat intelligence.

Defense in Depth Misinterpreted

Traditionally, some governments have taken defense in depth to mean a deep bench of security vendors or point products. This error has been costly in manpower, training and complexity. It has also been ineffective in thwarting attacks since there is no correlation among the numerous flavors of security sensors, nor between networks, endpoints, or – if used – SaaS or cloud sensors. As a result, attackers have an immediate time advantage. They can get in, move laterally and exfiltrate the data they seek while government security teams are poring over irrelevant logs and fighting tactical battles at each security sensor, oblivious to the unfolding puzzle of an advanced attack.

Threat Intelligence Only Works If It's Actionable and Fast

Another challenge attackers take advantage of is the overload of threat intelligence an agency tries to process – free or paid subscriptions, open source intelligence, and its own internal teams. Deduplication, deprecation and other activities that expedite analysis are manual and time-consuming. Even worse, an attack often hits one government network, prompting a separate government agency to analyze and write threat signatures to repel future threats from the same adversary. By this time, the attackers have moved through the network, accessed what they needed, and changed their attack vectors or mutated their malware, allowing them to successfully attack that organization or its peers again.

Prevent Successful Cyberattacks With a Platform Approach

Palo Alto Networks Security Operating Platform automatically correlates insights on emerging threats across endpoints, data centers, SaaS and cloud resources, ensuring fast response to any threat with little or no manual intervention. Governments around the world rely on the Palo Alto Networks platform to:

- Automate correlation across network, endpoint and cloud security sensors, preventing unknown threats in as few as five minutes after they are first encountered, anywhere in the world.
- Detect and prevent phishing, credential theft and the use of stolen credentials.
- Reduce analyst hours by reducing the attack surface, and thus incidents, down to the most critical events.
- Prevent ransomware and other threats at every stage of the cyberattack lifecycle.
- Protect enterprise networks from mobile to static endpoints, ICS/SCADA assets, traditional or virtualized data centers, public cloud and SaaS applications.
- Reduce operational expenses, or opex, and total cost of ownership, or TCO.

Automatically Prevent Known and Unknown Threats From Affecting Networks, Users and Data

Government employees may unwittingly or deliberately put the network or sensitive data at risk by clicking a link or downloading a file. With new malware created every minute, IT teams must constantly update security posture to be effective. Palo Alto Networks offers coordinated and automated threat prevention, starting with the endpoints that are typically targeted for attack. Palo Alto Networks advanced endpoint protection detects and prevents exploits and malware, including ransomware, before it can gain a foothold.

For brand-new threats, Palo Alto Networks malware analysis service conducts dynamic analysis of suspicious content – even encrypted content – in a virtual environment to discover brand-new threats anywhere in the world. It then triggers the creation of new protections, which are delivered to the platform's intrusion prevention system sensors in the network, or in virtualized or cloud environments, in as few as five minutes. Security Operating Platform deployments are continuously updated with protections against new phishing and malware sites, ransomware, malicious links in emails, and command-and-control infrastructure, blocking any part of an attack. This automation vastly reduces the operational burden on IT teams, which would normally have to manually update multiple security devices across the network to block even one part of such attacks.

Prevent Advanced, Targeted Attacks

With automation taking care of known threats, security teams can devote their valuable time to the unknown by hunting for advanced, targeted attacks. The platform's contextual threat intelligence service accelerates analysis, hunting and response workflows, and automatically prioritizes unique, targeted attacks with full context. Security teams can then respond to critical attacks more quickly without additional IT security resources.

Governments can also automatically integrate threat intelligence TAXII™ feeds, enforcing IP address, URL and domain block lists as well as making instant use of intelligence from an ecosystem of third-party services.

Block Phishing and Credential Theft

Stealing and using passwords is one of the oldest tricks in the book, yet it remains very effective. The Security Operating Platform detects and stops enterprise credentials from passing to external websites. Attempts to use stolen credentials are stopped by enforcing policy-driven, multi-factor authentication from virtual or physical platform deployments to all sensitive applications.

Safely Enable Cloud Use and SaaS Applications

SaaS applications are traditionally invisible to IT. The Security Operating Platform provides full visibility into the day-today activities of employees using SaaS applications, such as Microsoft® Office 365®, Dropbox® and more. Granular security policies help eliminate data exposure and threat risks.

Palo Alto Networks virtualized appliances bring the security of the on-premise network to public and private clouds. Protect AWS®, Microsoft Azure®, Google® Cloud Platform environments and private clouds from advanced cyberattacks while providing application-level control between workloads, policy consistency from the network to the cloud, fast deployment and dynamic security policy updates as workloads change.

Secure Government-Owned Devices Inside and Outside the Firewall

To establish a foothold in government IT systems, many cyberattacks first compromise an endpoint. Advanced endpoint protection from Palo Alto Networks coordinates with threat intelligence to pre-emptively block known and unknown malware, exploits, and zero-day threats, empowering personnel to use web-, mobile- and cloud-based applications safely.

IT teams should have complete visibility and precise control over government-issued devices regardless of their physical locations. The Palo Alto Networks platform extends both a VPN and granular security out to remote vendors, staff and third-party devices – computers, tablets and smartphones – no matter where they travel. Remote devices maintain the same security posture and access capabilities as those inside the network perimeter.

Gain Granular Visibility and Control Over Network Users, Applications and Content

Most government IT and security teams have little visibility into users and their network activity, which can leave them vulnerable to serious security breaches or misuse of applications or data.

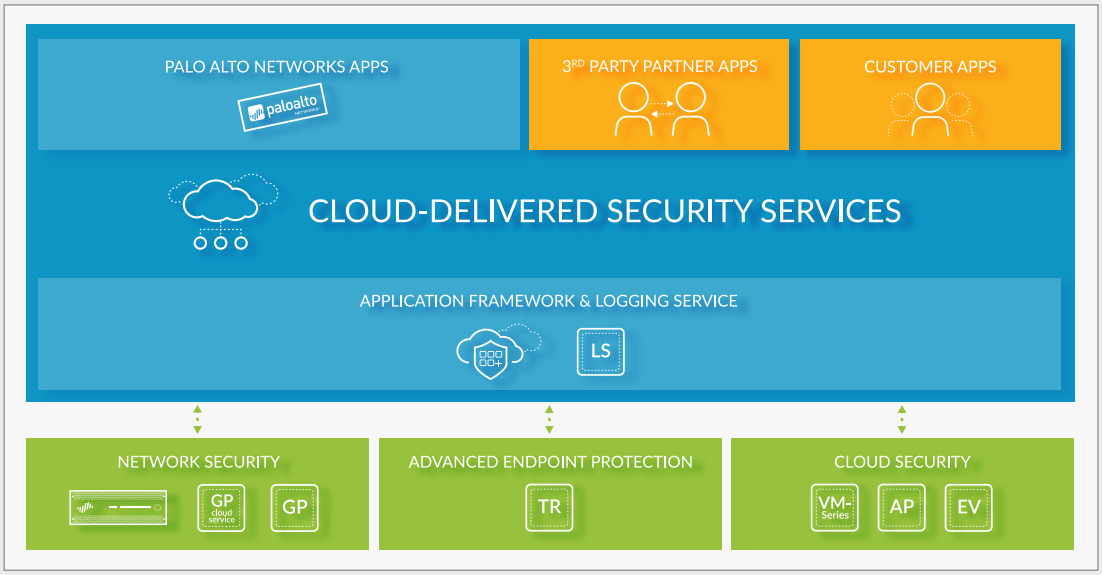

Figure 1: Palo Alto Networks Security Operating Platform

Security Operating Platform

The Security Operating Platform offers governments automated threat prevention across network, endpoint and cloud environments, enabled by real-time traffic visibility and consistent security policies for users, applications and content. The platform comprises enforcement points and shared intelligence that work together at network speed to automatically prevent ever-changing threats from affecting government services, employees or data. Accurate analytics allow you to streamline routine tasks and focus on government priorities. Tight integration across the platform and with ecosystem partners delivers consistent security across cloud, network and mobile devices. Among the core elements:

- **Network security** employs next-generation firewalls to protect networked services ranging from branch offices of all sizes to harsh environments, perimeters and data centers. Integrated network security clients extend security policies and protections to remote users and locations.
- **Advanced endpoint protection** safeguards servers, clients and mobile devices against the latest vulnerability exploits, ransomware and other malware delivered via any method, including email, USB drives or other attached devices, and other channels.
- **Cloud security** provides the same protections as the network security components for private, public and hybrid cloud environments as well as SaaS applications. Deep integration with native cloud services and automation tools speeds up multi-cloud deployments.
- **Cloud-delivered security services**, available in several deployment options to comply with government regulations, employ global intelligence to filter content as well as detect threats and attackers. These services automatically create protections against new threats and attacks as well as continuously update endpoint, network and cloud sensors.

This platform approach reduces silos of information, unifies visibility, policies and reporting, and shares threat intelligence across security functions, reducing the risk of threats or attacks, misconfigurations, or operating with outdated policies. Governments can start with any platform element and extend over time as requirements change.

Palo Alto Networks is committed to meeting the security regulatory needs of government environments on-premise and in the cloud.

For more information on our in-progress certifications, contact your account team. For completed certifications, visit https://www.paloaltonetworks.com/company/certifications.html

Palo Alto Networks has recently opened up the platform, enabling you to swiftly take advantage of security innovations that meet the particular needs of your government environment.

- **Application Framework** enables rapid development of custom and third-party applications that make use of data from the Logging Service and other cloud-delivered security services.
- **Logging Service** provides a secure, cloud-based repository for all application and data logs, collecting data from various sources while eliminating the burden of scaling and maintaining on-premise compute and storage.

Palo Alto Networks apps on the Application Framework include:

- **Behavioral analytics** to help discover anomalous and malicious user or application activity inside the network.
- **Contextual threat intelligence service** for malware analytics and hunting tools for security operations center teams.

For more information on the Palo Alto Networks Security Operating Platform, please visit https://www.paloaltonetworks.com/products/security-operating-platform.

The Security Operating Platform allows granular visibility and control of users, applications and content on the network, enabling governments to monitor usage, reduce risk and improve productivity. The platform can:

- Identify individual users, not just IP addresses, making it easy to quickly identify unauthorized network access by bad actors.
- Employ user identification to create role-based permission policies, ensuring all users have access to the network resources they need while denying access to systems they don't.
- Decrypt TLS/SSL/SSH traffic inline to detect and prevent hidden attacks, and/or work with existing third-party appliances to perform additional inspection and validation.
- Identify thousands of applications traversing the network, including those that may pose risks to operations or reputation.
- Combine application visibility with constantly updated URL Filtering so IT teams can easily identify or block applications or web content that may pose risks.
- Allow, deny or bandwidth-limit certain applications by user, location and even time of day, maintaining performance for critical applications.
- Provide better visibility and more precise control over sensitive data by blocking valid users from performing certain actions, such as outbound file transfers, or by scanning information leaving the network for certain patterns, such as credit card or Social Security numbers.
- Track how policies are working with real-time reports organized by users and applications so administrators can adjust if needed.

Getting Started

We offer multiple services and tools to help you understand and take full advantage of the threat prevention benefits of the Palo Alto Networks Security Operating Platform:

- Start by gaining visibility into the users, applications and content in your network. Contact your account team for a free **Security Lifecycle Review**. This non-disruptive process will define top risks due to usage, unknown applications, malware and more.
- Schedule an **Ultimate Test Drive** to get hands-on experience with the platform. Find out how you can quickly discover which protocols, applications and risks exist on your own network.
- Take advantage of Palo Alto Networks **Cyber Range**, an interactive cyber defense training tool that helps keep your IT network, infrastructure, OT, DevOps and SecOps teams razor-sharp.
- **NextWave Partners** and our own industry-recognized **Professional Services**, including specialized U.S. Government Support Services that meet the unique security needs of the U.S. federal government, are at your disposal.

For more information on our support for government networks worldwide, please visit **www.paloaltonetworks.com/cybersecurity-for-federal-government**.

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

cybersecurity-for-governments-b-081018