NEXT-GENERATION SECURITY PLATFORM FOR GOVERNMENT

A strong cyber defense, agile to the needs of governments globally as well as to adversaries' tactics and tool changes, is germane to the future. Palo Alto Networks meets the cybersecurity needs of its government customers by providing a future-proof platform with visibility, prevention and resilience – from the endpoint to the heart of the network, data center and cloud – and for all threat types for IT and OT networks.

Government digital transformation and IT modernization initiatives that 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 in and the speed at which they communicate with their citizens. They are doing so cautiously. As some of the most targeted organizations in the world, they know nation-states and other adversaries will continue to threaten sensitive information, military networks, and communications with ever-more advanced tactics.

From ICT/IT systems to SCADA, government services and systems need security solutions that can understand their environments and block both traditional ICT applications and unauthorized users from these critical networks. Modern military personnel and mobile civilian workers are increasingly untethered from their government networks, using mobile devices as well as advanced tactical mobile gear. They are more frequently in adversary territory and must maintain critical communications. As such, cyber defense is an all-time high priority and must not only focus on prevention but resilience in the face of an attack. It must defend the critical endpoint – however defined by the strategic, tactic, military or civilian entity – that is key to resilient communications flow.

Cyberattack Lifecycle

In numerous successful attacks against governments worldwide, adversaries have used each stage of the cyberattack lifecycle to successfully gain access to the government's network. In analysis of these attacks, best practices, such as the timely patching of vulnerable operating systems and applications, and a technology approach to security that is platform-based, could have prevented their success. To effectively protect today's government networks, a modern cyber defense is necessary. The steps to a modern 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 the approach to defense in depth to mean vendor in depth. This error has been costly – in manpower, in training and in complexity. It has also been costly in its ineffectiveness to thwart attacks to government networks. Because there is no correlation among the numerous flavors of security sensors, nor network to endpoint, attackers have an immediate time advantage over the governments they seek to attack. They can get in, move laterally, and exfiltrate the data they seek – all while government security teams are pouring through irrelevant logs, fighting tactical battles at each security sensor, oblivious to the unfolding puzzle of an advanced attack.

Threat Intelligence for Academic Analysis or True Threat Prevention?

Another challenge attackers can take advantage of is the overload of threat intelligence an agency tries to process – through free or paid subscriptions, open source intelligence sources, and/or from its own internal teams. The de-duplication, deprecation and other activities that must happen to expedite the analysis is manual and time-consuming. Even worse, often an attack hits a government network, and the threat is sent to an entirely separate government agency to analyze and, ultimately, write threat signatures to then prevent future threats from the same adversary. By the time this chain of events occurs, the attackers have likely moved through the network, accessed what they needed, and changed their attack malware to successfully attack you or your peers again.

The threat intelligence you receive should be actionable. What does that mean? It must be immediately usable by your security sensors for threat prevention at each area of your network that is potentially vulnerable to the cyberattack lifecycle: at your endpoints, your perimeter, your data center edge, between your VMs in your virtualized data center, and in your public cloud. Anything less becomes more of an academic exercise of intelligence analysis. Without the ability to use the threat intelligence to immediately create protections and push them to your sensors, your network remains vulnerable.

Platform Approach to Cyberattack Lifecycle Prevention

Given the above challenges, if you knew there was a security approach that did all of the following, and ultimately prevented the threats against your network rather than just detecting them, wouldn't you want to immediately leverage it?

- Automate correlation across the security sensors in your network and at your endpoints, responding with prevention to unknown threats within five minutes of being seen anywhere in the world.
- Prevent phishing credential theft and the use of stolen credentials. Enterprise credentials passing to an external website are detected and stopped. Attempts to use stolen credentials are stopped by enforcing policy-driven, multi-factor authentication directly from the appliance (virtual or physical) to all sensitive applications.
- Reduce your analyst hours by reducing your overall threat posture, and thus incidents, down to the most critical events.
- Prevent threats at every stage of the cyberattack lifecycle – from initial endpoint access to the perimeter to lateral movement and exfiltration.
- Protect the totality of your enterprise network from mobile to static endpoints, ICS/SCADA assets, traditional or virtualized data center with VMs, to public cloud and SaaS applications.
- Reduce operational expenses (OPEX) and Total Cost of Ownership (TCO).

These benefits of the Palo Alto Networks® Next-Generation Security Platform are what government organizations around the world have immediately reaped the rewards of, resulting in dramatically improved security. This approach is a modern cyber defense.

The Palo Alto Networks Next-Generation Security Platform, with its single-pass architecture (Figure 1), is a natively integrated platform that brings network, cloud and endpoint security into a common architecture, with complete visibility and control. This platform approach ensures your organization – IT and OT – can detect and prevent attacks and streamline day-to-day operations while boosting security efficacy and preventing threats at each stage of the attack lifecycle. https://www.paloaltonetworks.com/products/platforms.html

Attack prevention, automatically correlated – across the network and endpoint:

- Security capabilities (e.g., decryption, URL filtering, unknown threat detection, network antivirus, IPS, firewall) on the platform are seamlessly integrated to add protection from both known and unknown threats, classification and filtering of URLs, IPs, domains, and the ability to build logical policies based on the specific security posture of a user's device. https://www.paloaltonetworks.com/products/platforms/subscriptions.html

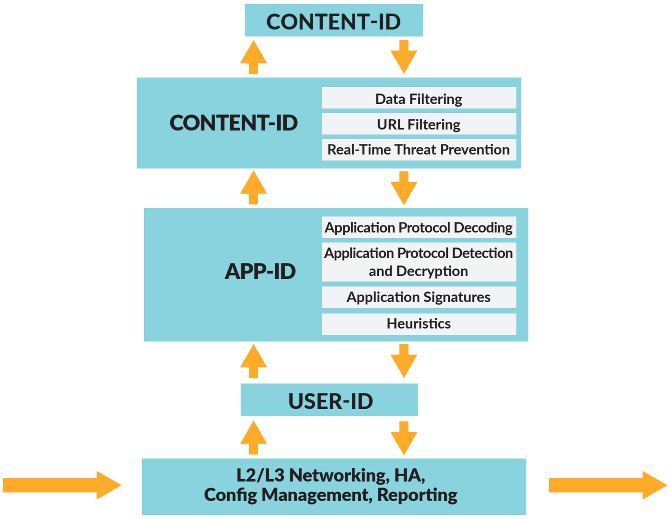
CONTENT-ID
CONTENT-ID
Data Filtering
URL Filtering
Real-Time Threat Prevention
APP-ID
Application Protocol Decoding
Application Protocol Detection and Decryption
Application Signatures
Heuristics
USER-ID
L2/L3 Networking, HA, Config Management, Reporting

Figure 1: Single-pass architecture traffic flow

- Unknown threat analysis, featuring Palo Alto Networks WildFire™ threat analysis environment conducts dynamic analysis of suspicious content in a virtual environment to discover unknown threats. It then automatically creates and enforces content-based malware protections in five minutes. It also detects malicious links in email, proactively blocking access to malicious websites. For governments desiring their own private threat intelligence cloud, the on-premise WF-500 WildFire appliance can be deployed in any government network for this function.
- Endpoint exploit and malware detection and prevention can be stopped in their tracks.

- Onboard TLS/SSL/SSH decryption provides visibility and immediate threat prevention for otherwise hidden attacks obfuscated with encryption.

Cloud support – private to public and hybrid:

- With the same complete visibility and protection as the appliances, the Palo Alto Networks VM-Series supports AWS® and Microsoft® Azure™ public cloud offerings, KVM/OpenStack® and VMware®, with the VM-Series for NSX™ for private clouds and provides granular access controls and threat prevention in SaaS environments.
- Without impact to speed or efficiency, the platform examines 100 percent of the traffic flowing in and out of the data center and between all applications.
- Segmenting north-south (physical) and east-west (virtual) traffic, the platform tracks virtual application provisioning and changes via dynamic address groups and automation and orchestration support via REST API.
- Scaling to support more data with fewer entry points, the platform supports government data consolidation and cost reduction efforts.

Threat intelligence for true threat prevention:

- Security teams can devote their limited time hunting for the small number of truly advanced, targeted attacks using AutoFocus™ contextual threat intelligence service. This accelerates analysis, hunting and response workflows and automatically prioritizes unique, targeted attacks with full context. Security teams can then respond to critical attacks faster, without additional IT security resources.
- Receiving ISAC and other threat feeds? These organizational intelligence feeds, such as those from government or industry CERTs, can now be *automatically consumed* via STIX and TAXII by the platform through the MineMeld service, ultimately creating new prevention mechanisms for security devices. Through MineMeld – as an open source tool or as part of AutoFocus – you can *automate* the enforcement of IP address, URL and domain block lists, making *instant* use of your new intelligence from an ecosystem of third-party services.

Strategic partnerships with some of the world's leading vendors including Splunk®, VMware®, Proofpoint™, Aruba, and Tanium™ for our products to work seamlessly provides added value to our mutual customers, allowing them to be more mobile, nimble and collaborative.

Getting Started

When you are ready to realize the threat prevention benefits of the Palo Alto Networks Next-Generation Security Platform, there are several tools that will be at your disposal:

- Application Control Center depicts the top applications and sources that you can use in establishing visibility to understand the needs of your particular organization while making decisions on how best to reduce risk.
- Migration Tool makes it easy to migrate from IP/port-based firewall rules in legacy firewalls to application-based rules in the Next-Generation Security Platform.
- NextWave Partners and our own industry-recognized Professional Services – including specialized U.S. Government Support Services that are designed to meet the unique security needs of the U.S. federal government – are at your disposal when you need further assistance.

A strong cyber defense, agile to the needs of governments globally as well as to adversaries' tactics and tool changes, is germane to the future. Palo Alto Networks meets the cybersecurity needs of its government customers by providing a future-proof platform with visibility, prevention and resilience – from the endpoint to the heart of the network and data center cloud – and for all threat types. Customers across all continents and numerous industries, the Fortune 100, and the most advanced governments and militaries rely on Palo Alto Networks to improve their cybersecurity posture. Schedule an Ultimate Test Drive (UTD) for hands-on experience with the platform. Find out how you can quickly discover which protocols, applications and risks exist on your own network and embark on a true prevention-focused approach to your network today.

The Palo Alto Networks Next-Generation Firewall is the core of the Next-Generation Security Platform – and this firewall is a Gartner Magic Quadrant leader for the fifth year in a row. See for yourself in the 2016 Gartner Magic Quadrant report. For more information on our support to government networks worldwide, please visit www.paloaltonetworks.com/government.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com