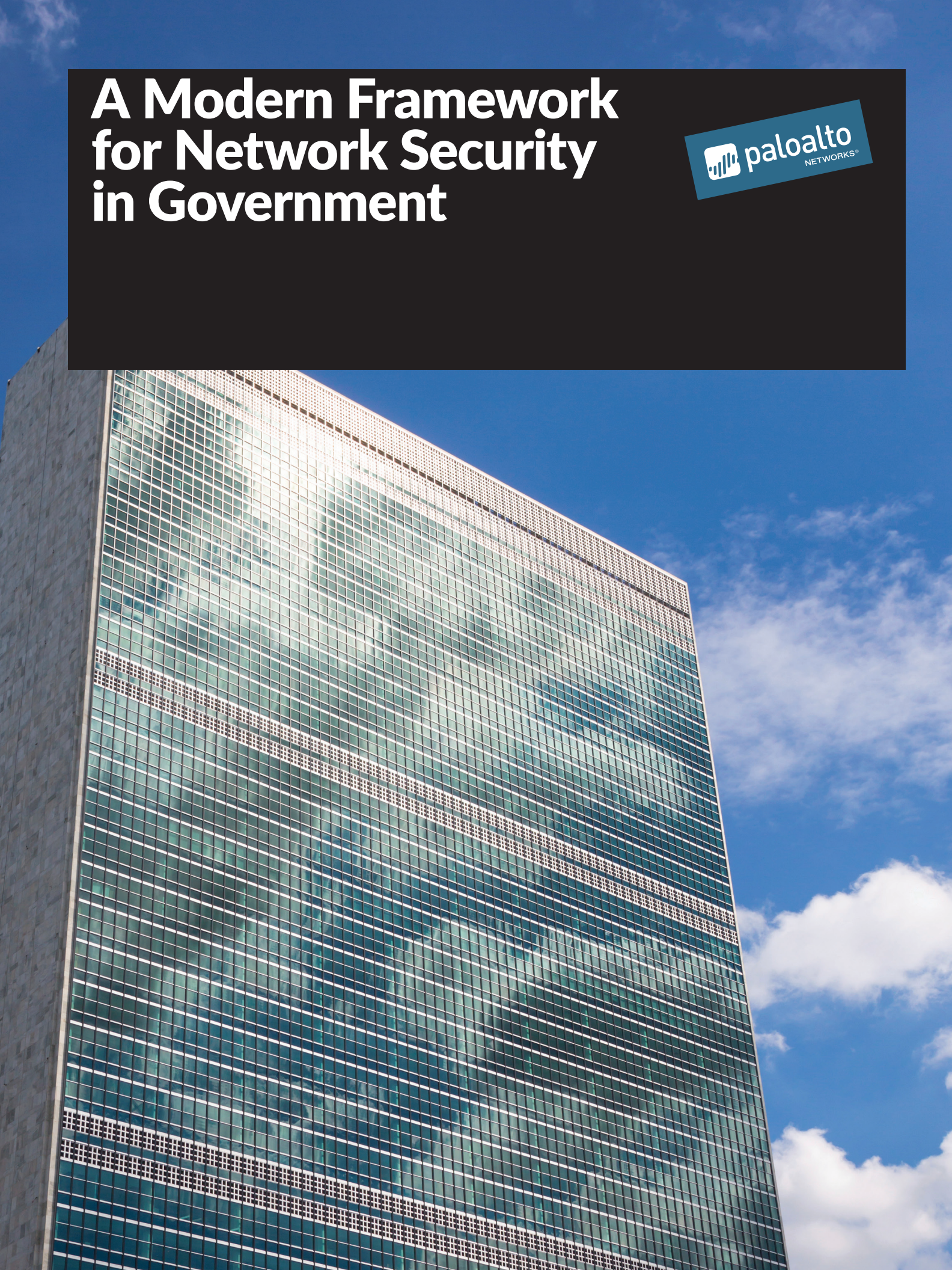
A Modern Framework for Network Security in Government



Government: Securing Your Data, However and Wherever Accessed

Governments around the world are exchanging more data with all of their constituents: citizens, civilians and warriors, patients, students, and partners in more ways than ever. This exchange of information – further and faster, across both IT and control systems networks – means the security of the networks housing and serving that data requires change in parallel. This ensures the confidentiality, integrity and availability of that data whenever it is needed.

The adversary wants access to that same data – to steal it, disrupt it, or possibly even change it. To reduce advanced attacks, governments must create agility to prevent attacks across their networks, from the perimeter edge and endpoints to the heart of their data centers. Security operations centers (SOCs) and intelligence analysts must have less noise and more relevant data to act upon. They must move beyond mere detection and response, to prevention that allows the security functions to prevent, automatically, in cooperation with one another.

Cyber Attack Chain and Zero Trust

It's no secret that government networks are among the most targeted of virtually any industry. The stakes are high, and attackers know they must use more evasive tactics to penetrate these networks. Some of the latest attacks show a concerted effort to study victims with appropriate access, identify their patterns, and develop spear phishing and waterhole attacks, among other approaches, to gain access through the unwitting victim to the target network. Many attackers are able to, not only penetrate their target network, but often successfully establish a beachhead and remain undetected for a significant period of time while continuing evasive and damaging action. This can lead to tremendous loss, whether of strategic, political, monetary or intelligence value.

The Gartner Cyber Attack Chain reveals six stages of an attack from delivery and exploitation and installation to exfiltration of information from the target network. Fundamentally, the approach to the threat must move beyond mere detection and remediation of latter points in the attack chain to a preventative approach throughout. With the technology available today, governments can defeat attackers before they can exploit a vulnerability. But they can also thwart other steps in the attack chain by controlling applications, users and content everywhere across the network.

The Zero Trust approach, first coined by Forrester, enables an organization to establish the verification of all users, devices and applications traversing the network, within the context of user or group functions, device and/or location. By establishing Zero Trust boundaries that effectively compartmentalize different segments of the network, governments can protect critical information from unauthorized applications or users, reduce the exposure of vulnerable systems, and prevent the lateral movement of malware throughout the network. A Zero Trust model incorporates virtual segmentation with the enforcement controls and threat prevention necessary to defeat the lateral movement of adversaries through the target network and thwart the attack.

THWART THE ATTACK CHAIN

1. Adopt a Zero Trust approach.
2. Automatically control and block unwanted applications and activity everywhere on the network and endpoint.
3. Protect and defend systems at all places in the network, across all network traffic on endpoints, in data centers, in remote locations and at major Internet gateways.
4. Protect and defend the endpoints that are off-network, regardless of location or device.
5. Prevent new attacks and automatically block follow-on attacks.
6. Create cohesion between IT, cybersecurity and intelligence professionals to coordinate actions.
7. Ensure the immediate and automatic sharing and distribution of intelligence signatures around the world.

Securing the Host and Network from Low Level to Advanced Threats

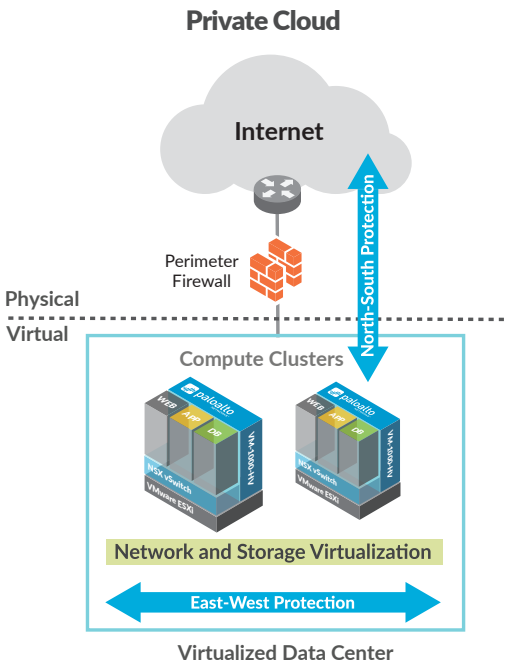
To secure their networks and endpoints, here are several key steps governments should consider:

- **Establish visibility into all network** traffic and define which applications do and do not belong on the mission network.
- **Whitelist the applications** by user or user group and enforce the controls.
- **Decrypt SSL communications**, where attackers often hide their tracks.
- **Incorporate malware analysis.** Decrypt SSL communications, where attackers often hide their tracks.
- **Incorporate advanced attack detection and prevention** across all communications – not just web and email. Any deviations from the whitelist are stopped; newly discovered legitimate applications are supported with new classifiers; and any suspicious files are automatically and immediately analyzed, identified threats are detected, malicious URLs and IP addresses involved in the attack are identified, signatures *automatically* generated, and appliances (virtual and physical) are *automatically* reprogrammed with the protections – for malware, URLs and IP addresses – in as little as five minutes, all without human intervention.
- **Thwart both exploits and malware on all endpoints**. Adopt lightweight, scalable advanced endpoint protection that prevents all exploits and prevents all malicious executables, without requiring any prior knowledge. The defenses across the cyberattack chain, from network to endpoint, should be fully integrated and should learn from one another.
- **For mobile endpoints and their access to your data**: Apply mobile threat prevention and policy enforcement at all mobile endpoints, based on applications, user, content, device and device state. Extend a VPN tunnel to mobile devices. Integrate the mobile device security with advanced attack prevention to prevent new malware from affecting the mobile devices. Use device management to configure the mobile devices, provide device state information, and establish secure connectivity to access applications and data in accordance with security policies. Identify devices with infected applications. Host a government application store for managing government-vetted or custom government applications. Isolate government data by controlling lateral data movement between government and personal applications on the same device.
- **Within the security operations** and/or the security operations center (SOC), make the broadest visibility and threat prevention a reality:
  - Across the breadth of the network from the mobile and fixed endpoints into the core of the data center and/or cloud.
  - From individual malware behaviors and attack tactics all the way up to a global campaign.
  - With correlation and automatic threat prevention at a platform level to reduce the volume of threats that must be reviewed. This can be achieved with an application whitelisting approach coupled with on-board correlation of security information.
  - With automation, de-duplication, correlation of threat intelligence feeds and automated blocklists from the results, resulting in drastically reduced events per analyst hour, which leads to much more effective use of security operations or SOC personnel.

Securing the Data Center and Cloud

Numerous data uses and many more data users connecting through numerous devices represent complexity and risk. Regardless of how you have architected your data center – consolidation, private, hybrid cloud and/or public cloud – security of the data must remain the highest priority. There are several key considerations:

- As noted previously, **establish a benchmark of which applications reside within your data center**. Though these are critical applications, they are often the very ones with vulnerabilities and active exploits available. Understand your data center applications and their current risk profiles. Establish a dynamic whitelist of all approved applications to ensure normal operations.
- **Ensure your security strategy considers both east-west and north-south traffic** by decoding all ingress and egress data, and apply granular control for all applications, users and network traffic based on the steps above down to the virtual machine (VM), as users, applications and content move from VM to VM. Choose a cybersecurity solution that makes VM seamless while the security policies remain intact with them.
- **Credential theft** is a frequent tactic for those targeting government data globally. Establish a Zero Trust model to protect the mission and ensure the confidentiality and integrity of government data. Thwart attempted outbound leaks of credentials as part of a phishing attack, and thwart attempted use of stolen credentials for access from outside the network perimeter. Using the pre-established whitelist of applications, establish zones of users and access to those applications and data. Strictly control the flow between security zones of trust. Thwart any attacker who attempts to compromise a host and move laterally by suppressing their movement and access.
- For Amazon® Web Services and Microsoft® Azure® public cloud environments, **integrate the same level of security at the VM level for visibility and threat prevention as on-premise services or data-center operations.**



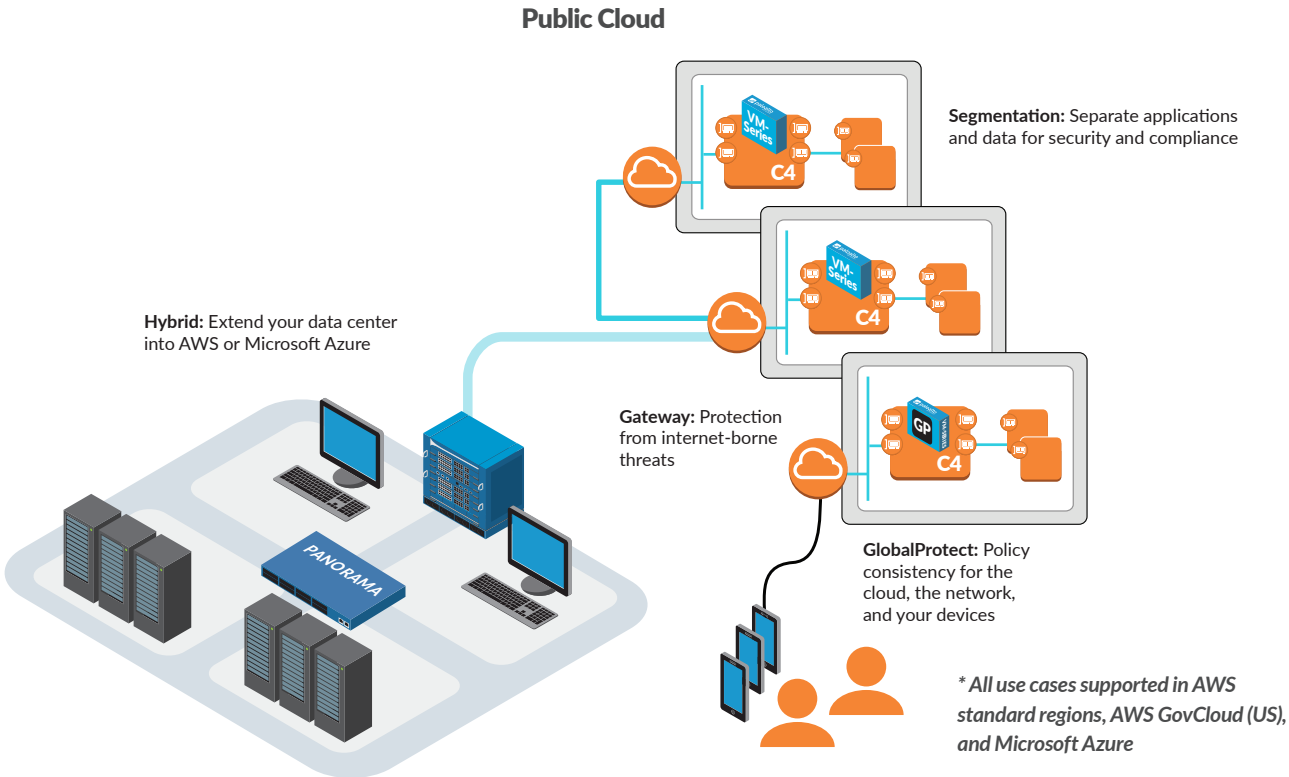
– **For SaaS, maintain granular visibility and control of use at the application and individual application function level,** for example approving the use of a specific videoconferencing service, but not the file transfer capability within it. Extend visibility and control down to the individual file, folder and user operating within the SaaS application. Apply advanced threat prevention to block known malware and identify and block new malware in these environments. Apply deep analytics into the day-to-day usage to quickly determine if there are any data losses or compliance-related policy violations. Incorporate advanced attack detection and prevention across all communications in and out of each zone. Don't settle for manual, manpower-intensive efforts to thwart advanced attacks.

– **Incorporate advanced attack detection and prevention** across all communications in and out of each zone. Don't settle for manual, manpower-intensive efforts to thwart advanced attacks.

– **Any deviations from the whitelist are stopped;** newly discovered legitimate applications are supported with new classifiers; and any suspicious files are *automatically* and immediately analyzed; identified threats are detected; malicious URLs and IP addresses involved in the attack are identified; signatures are *automatically* generated and attacks are thwarted; and sensors are reprogrammed with the protections – for malware, URLs and IP addresses – in as little as five minutes, all without human intervention.

Control Systems Security

Control systems and machine-to-machine operations manage critical functions for government – from civilian to military operations. These critical operations perform fuel and weapons storage; transport and onboard ship, aircraft and tank operations; navigation; operation of rivers and dams; building automation; and other functions.



To ensure the protection of these critical systems – often running unpatchable systems – governments should:

- **Evaluate any third-party people, processes and technologies** operating these systems on behalf of government and ensure they have the same level of security controls as those the government itself operates.
- **Apply the appropriate security and best practices** to the operations or automation networks as you would the IT network.
- **Make visibility of the network traffic into and out of the operational network a priority**. Secure the operational network boundary, both to the IT network and within the operational network between functions, by user and application.
- **Recognize that unpatchable systems with antiquated operating systems, or those which simply cannot be patched** due to operational downtime, pose a very high risk and must be a priority for advanced endpoint protection.

Palo Alto Networks Next-Generation Security for Government

Palo Alto Networks serves governments in over 70 countries today, which are demanding more from their security solutions. With the most advanced and flexible next-generation security platform, and as a five-time Gartner Magic Quadrant Leader, we provide an innovative threat prevention approach.

Prevent Threats at Every Step of the Cyber Attack Chain

Focused on preventing exploits and both known and unknown malware, Palo Alto Networks Next-Generation Security Platform provides threat prevention across the Cyber Attack Chain, delivering threat prevention for unknown threats in as little as 5 minutes. With full visibility into all network traffic, including stealthy attempts to evade detection, such as SSL encryption, the platform's unique, closed-loop approach controls cyberthreats, beginning with positive security controls to reduce the attack surface.

- **Application visibility and positive enforcement:** Visibility of all users, applications, and content enables an organization to understand the most-used applications, users' application needs, high-risk applications, encrypted communications, and potential security impact. Armed with this information, organizations can make fully informed decisions for application whitelisting, and create security policies appropriate for their own environment, thereby reducing the overall threat footprint.
- **Unknown or zero-day malware prevention:** Analysis of unknown files in an advanced, virtual malware analysis environment available for your own private network, purpose-built for high fidelity hardware emulation, analyzing suspicious samples as they execute. This capability detects and blocks targeted and unknown malware, exploits, and outbound command and control (C2) activity by observing their actual behavior, rather than relying on pre-existing signatures. In addition to quickly turning unknown threats into known, the environment generates protections that are shared globally in about 5 minutes.
- **Known malware prevention:** Proactive blocking of known threats with Threat Prevention and URL Filtering services, providing baseline defenses against known exploits, malware, malicious URLs, and command and control activity.
- **Endpoint exploit, malware, and policy violation prevention**: Prevention of advanced endpoint attacks by thwarting exploits, including those utilizing unknown zero-day vulnerabilities, and all malicious executables, without requiring any prior knowledge. Beyond immediate malware detection, additional protections are afforded at the endpoint through policy restrictions. Examples of policy restrictions include:
  - Block unsigned executables
  - Block executables launched from specific network locations or devices.

The Palo Alto Networks Next- Generation Security Platform is a natively integrated platform that brings network, cloud, SaaS, mobile, and endpoint security into a common architecture, with complete visibility and threat prevention. This platform approach ensures your organization can detect and prevent swiftly evolving attacks, streamlines day-to-day operations and boosts security efficacy, and prevents threats at each stage of the attack lifecycle. https://www.paloaltonetworks.com/products/platforms.html

Security subscriptions on the platform are seamlessly integrated to add protection from both known and brand new threats, malicious infrastructure such as malicious domains and DNS activity, and command-and-control infrastructure, classification and filtering of URLs, 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. Palo Alto Networks cloud-based or on-premises malware analysis environment, WildFire™, provides dynamic and static analysis of suspicious content, coupled with machine learning for swift learning of attack behavior – from malicious content up to a global campaign of activities – in a virtual environment to discover new threats. It then automatically creates and enforces content-based malware protections. It also detects malicious links in email and malicious infrastructure, proactively blocking access to malicious websites and other attacker resources.

Protect Your Entire Extended Network: Private and Public Cloud to Mobile Devices

Focused on securing every stage of the data center – from consolidation to private cloud, public cloud and hybrid cloud – Palo Alto Networks security platform secures the edge and heart of the data center:

- **Private, public, and hybrid cloud security:** Extension of the aforementioned security capabilities for private, public, and hybrid cloud environments. The VM-Series of virtualized Next-Generation Firewalls supports the same security features available in the physical form- factor appliances, allowing for the safe enablement of applications flowing into and across your private, public, and hybrid cloud computing environments. The VM-Series supports VMware® ESXi™, NSX™ and vCloud® Air™, Microsoft Azure, Amazon Web Services, including AWS®, GovCloud, KVM/OpenStack® for open source implementations and Citrix® Netscaler SDX™.
- **SaaS control and threat prevention:** Added security of sanctioned SaaS applications with complete visibility across all user, folder and file activity, deep analytics into day-to-day usage to quickly determine if there are any data loss protection or compliance-related policy violations, and granular, context-aware policy control to drive real-time enforcement and quarantine of users and data as soon as a violation occurs

Create Actionable Intelligence

- Security practitioners receive an overwhelming volume of security data and alerts daily from a variety of tools, vendor feeds, and devices deployed across their organization. With Palo Alto Networks AutoFocus™ service, security practitioners gain instant access to actionable intelligence derived from billions of file analysis artifacts based on the files collected from over 5,000 global enterprises. Stand-alone or as part of AutoFocus™ contextual threat analysis service, MineMeld automates de-duplication and correlation of threat intelligence feeds and automates blocklists for the platform from the results.

Improve Efficiency of Security Operations and/or SOCs

Visibility and threat prevention across the breadth of the network – from mobile to the core of the data center and/or cloud, from individual malware behaviors to a global campaign, from internal to external threat feeds – the platform drastically reduces events-per-analyst-hour, resulting in much more effective use of security operations or SOC personnel.

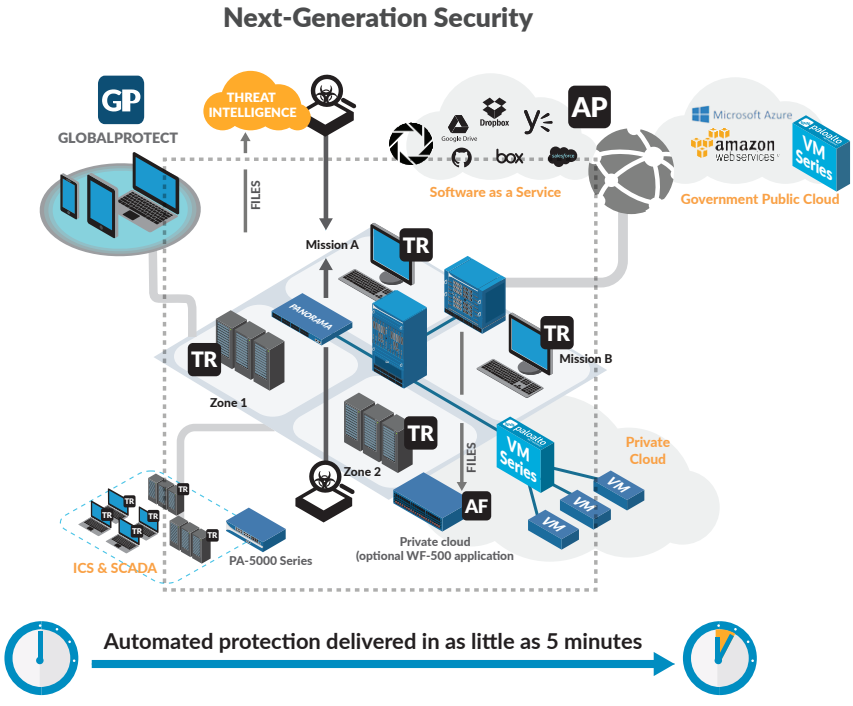
Provide a Safe Environment for Applications and Data from Any Device

Palo Alto Networks security platform combines technology, global intelligence, and policy enforcement over mobile applications and threats to ensure a safe network environment while connecting mobile users to your infrastructure.

Mobile threat prevention and policy enforcement at all mobile endpoints are based on applications, user, content, device and device state; integration of mobile device security with advanced attack prevention prevents new malware from affecting mobile devices. Device management configures mobile devices, provides device state information – including infected devices – and establishes secure connectivity to access applications and data, according to security policies.

Reduce Noise, Increase Focus on Actionable Intelligence

Security practitioners receive an overwhelming volume of security data and alerts daily from a variety of tools, vendor feeds and devices deployed across their organization. With Palo Alto Networks AutoFocus™ service, security practitioners gain instant access to actionable intelligence derived from billions of file analysis artifacts based on the files collected from over 5,000 global enterprises.



Multi-Faceted Government Support

Palo Alto Networks serves government customers in every spectrum, and at all levels and functions, and meets the certification requirements and standards required of governments, including Common Criteria, ANSSI, FIPS-140, Suite B, NIST SP 800-63-2 Levels 3 and 4, and DISA UC APL. Our U.S. Government Support Services provide technical support provided by U.S. citizen engineers located in U.S.-based support centers for all aspects of support, technical and administrative cases.

Summary

Governments need a plan that addresses their current needs without compromising access or security. Palo Alto Networks differentiated approach to security offers a model of positive enforcement and prwevention – throughout your network and out to your mobile workers. Providing an innovative next-generation security platform, we protect government networks across the entire attack lifecycle and across government assets: fixed to mobile, IT to automation and operational environments, and edge to heart of the data center and cloud.

Take a Test Drive

Take advantage of the benefits of the Palo Alto Networks platform with an Ultimate Test Drive. These demonstrations arm government network and cybersecurity experts with hands-on experience with the Palo Alto Networks Next-Generation Security Platform.

See the Palo Alto Networks difference for yourself at **https://www.paloaltonetworks.com/events/test-drive.html.**

Request a demonstration with our team in your country:
https://www.paloaltonetworks.com/events/test-drive.html

Web:	https://www.paloaltonetworks.com/government
Twitter:	https://twitter.com/NGS_Gov
Youtube:	https://www.youtube.com/playlist?list=PLqATPiC_Bcl-iFpziDZ4sIppcKz_u8bLL
Government Blog:	http://researchcenter.paloaltonetworks.com/government/

Palo Alto Networks
4401 Great America Parkway
Santa Clara, California, 95054

+1-408-753-4000 main
+1-866-320-4788 sales
+1-866-898-9087 support
www.paloaltonetworks.com