LEVERAGING CDM TO IMPROVE CYBERSECURITY

Palo Alto Networks CDM Integration Framework

In 2012, the U.S. Office of Management and Budget identified continuous monitoring of federal IT networks as one of 14 Cross-Agency Priority Goals. Subsequently, the Department of Homeland Security established the Continuous Diagnostics and Mitigation program to "support … government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity."

The CDM program is designed to roll out in phases. This white paper describes how Palo Alto Networks Next-Generation Security Platform, in combination with select technology and delivery partners, supports CDM phases and enables agencies to achieve the security objectives of the program.

Table of Contents

Executive Summary

In 2012, the Office of Management and Budget identified continuous monitoring of federal IT networks as one of 14 Cross-Agency Priority Goals, established in accordance with the Government Performance and Results Modernization Act.

Subsequently, the Department of Homeland Security established the Continuous Diagnostics and Mitigation program to "support … government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity."[1] The $6 billion program, which was announced in 2013, is targeting the ability to deploy a federal CDM dashboard with a government-wide view of agency security status by the end of the 2017 fiscal year.[2]

The goals and objectives of the program are:

- Enable network administrators to know the state of their respective networks at any given time.
- Inform them about the relative risks of threats.
- Make it possible for system personnel to rapidly identify and mitigate flaws.

The CDM program is designed to roll out in phases. Each phase consists of a number of capabilities, with the goal of establishing a system that will continually monitor an IT environment, identify and remediate threats, and roll up data to agency and government-wide management dashboards.

This white paper gives an overview of the Palo Alto Networks® Next-Generation Security Platform and describes in detail how the platform, in combination with select technology and delivery partners, supports all CDM phases and enables agencies to achieve the security objectives of the program.

CDM Program Overview

The Continuous Diagnostics and Mitigation program is available to U.S. government civilian agencies, as well as state, local, tribal and territorial departments and agencies, and currently consists of 15 continuous diagnostic capabilities rolled out in three phases. Phase 1 focuses on Endpoint Integrity; Phase 2 covers Least Privilege and Infrastructure Integrity; and Phase 3 is concerned with Boundary Protection and Event Management. Phase 4, currently being defined by the Department of Homeland Security, is focused on Protecting the Data on the network.[3]

The CDM program uses commercial off-the-shelf tools to automate the process of continually scanning an IT environment to discover, report and manage security flaws.

Overall, the CDM program improves government network protection using an approach designed to:

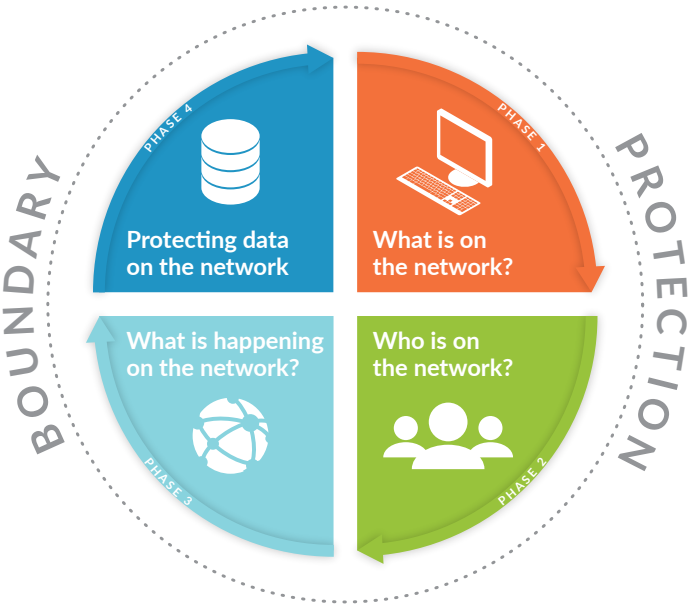


Figure 1: How CDM Works[4]

- Provide services to implement sensors and dashboards.
- Deliver near-real-time results.
- Prioritize the worst problems within minutes, rather than quarterly or annually.
- Enable defenders to identify and mitigate flaws at network speed.
- Lower operational risk and exploitation of government IT systems and networks.

[1] https://www.us-cert.gov/sites/default/files/cdm_files/CDM_ProgramOverview.pdf
[2] https://fcw.com/microsites/2015/contract-guide-carahsoft-cdm/05-how-cdm-is-rolling-out.aspx
[3] http://thecgp.org/images/CDM-DEFEND-Industry-Day_PPT_FINAL_15MAY17-1.pdf
[4] https://www.us-cert.gov/cdm/home

How Palo Alto Networks Supports the CDM Program

Palo Alto Networks provides support for the CDM program through:

- Natively integrated capabilities in Palo Alto Networks Next-Generation Security Platform that identify, prevent and report on key cybersecurity threats.
- Integration with key CDM technologies for security automation and improved detection and correlation.
- Working with approved system integrators authorized to sell CDM program components and systems under the auspices of a General Services Administration (GSA) Blanket Purchase Agreement (BPA).

Palo Alto Networks Next-Generation Security Platform includes:

Product	Description
Next-Generation Firewall	**Classify all traffic, across all ports, all the time:** Today, applications and associated content can easily bypass a port-based firewall using a variety of techniques. Palo Alto Networks Next-Generation Security Platform addresses the traffic visibility limitations that plague port-based security by applying multiple classification mechanisms to the traffic stream to determine the identities of applications traversing a network and whether they are carrying any threats or malware. All traffic is classified regardless of port, encryption (SSL/SSH) or evasive techniques employed. Unidentified applications – typically a small percentage of traffic, yet high in potential risk – are automatically categorized for systematic management. **Reduce the threat footprint, prevent known threats:** Once traffic is fully classified, an organization can protect its network from a range of cyberattacks by allowing only the applications required for business operations and inspecting the content for exploits, malware, dangerous files or content. Intrusion Prevention System (IPS) capabilities block network and application-layer vulnerability exploits, buffer overflows, DoS (denial-of-service) attacks and port scans. Antivirus/anti-spyware protection blocks millions of malware variants, including those hidden in compressed files, PDF files or web traffic. Policy-based decryption can be selectively applied to traffic encrypted with SSL and the traffic inspected for threats, regardless of port. Threat prevention capabilities go beyond blocking malicious content to include control of specific file types by policy, as well as inspecting traffic for specific content to prevent data loss. The following unique traffic identification features are included in every Palo Alto Networks Next-Generation Firewall: • **User-ID™** technology verifies the user's identity, rather than a device IP address, obtained from enterprise directories, terminal servers or Microsoft® Exchange. It is used to analyze the application, threat and web surfing activity of individual users and user groups. User-ID also supports third-party solutions, such as ForeScout CounterACT®. • **App-ID™** technology natively recognizes and categorizes more than 2,000 enterprise, web and SaaS (software as a service) applications. • **Content-ID™** technology combines real-time threat prevention, a comprehensive URL database and elements of application identification to limit unauthorized data and file transfers, as well as detect and block a wide range of exploits, malware, dangerous or unauthorized web surfing, and targeted and unknown threats.
WildFire™ cloud-based threat analysis service	**Prevent unknown threats:** Previously unknown threats, such as custom or polymorphic malware, are increasingly used in modern cyberattacks. Unknown threats are analyzed and identified via WildFire across thousands of applications and protocols, regardless of ports or encryption, via direct observation of the malicious behavior of unknown files in an isolated malware analysis environment. If new malware is discovered, WildFire automatically generates a signature for the file and related traffic, and shares it globally to all subscribers in as few as five minutes. WildFire supports all major file types, including PE files; Microsoft Office documents; Adobe® PDF; Java® Applet (JAR and class); and Android® APK (Application Package). WildFire is available on-premise, in the cloud, or using a hybrid architecture.

Product	Description
Traps™ advanced endpoint protection	Protect the endpoint: Traps persistently enforces the Zero Trust model on any supported Microsoft Windows® endpoint. Rather than rely on inadequate signature detection technology, Traps employs a series of exploit-prevention modules aimed at blocking techniques that attackers must use to be successful. Traps can send an unknown malware file to WildFire for further analysis. Advanced endpoint protection delivers on the following: • Prevents all exploits, including malicious executables, that use unknown or "zero-day" vulnerabilities. • Provides detailed forensics against prevented attacks. • Highly scalable, lightweight and seamless, with minimal to no disruption.
GlobalProtect™ network security for endpoints	Mobile device protection: GlobalProtect is an integrated solution that safely enables mobile devices for business use. Capabilities include: • **Device management – Enables** agencies to manage mobile device configuration, provision apps and oversee device usage throughout the organization. • **Device protection – Establishes** an IPsec/SSL VPN that terminates at a Palo Alto Networks Next-Generation Firewall, ensuring consistent policy enforcement, regardless of the user's location. • **Data control – Determines** the network resources mobile users can access, while unmanaged or noncompliant devices can be blocked from accessing sensitive agency resources.
Panorama™ network security management	Panorama administrators centrally manage the process of configuring devices, deploying security policies, performing forensic analysis and generating reports across an agency's entire network of next-generation firewalls.
Aperture™ SaaS security service	The use of SaaS applications is creating gaps in security visibility and new risks for threat propagation, data leakage and regulatory noncompliance. Aperture provides a unique approach to securing sanctioned SaaS applications with complete visibility across all user, folder and file activity within the SaaS application, and detailed analysis and analytics on usage to prevent data risk and compliance violations.
AutoFocus™ contextual threat intelligence service	AutoFocus enables you to distinguish the most important threats from everyday commodity attacks by matching events on your network to tags. Now, instead of simply seeing that a malicious event has occurred, you immediately know the context around an attack, such as the malware family, campaign or malicious actor targeting your organization. When identified, AutoFocus will alert your security team about high-priority events, enabling you to take swift action to mitigate their impact. AutoFocus provides unprecedented visibility into unknown threats, with the collective insight of thousands of global enterprises, service providers and governments feeding the service. AutoFocus correlates and gains intelligence from: • WildFire, the industry's largest threat intelligence service. • PAN-DB URL Filtering service. • Palo Alto Networks global passive DNS network. • Unit 42 threat intelligence and research team. • Unique artifact-level statistical analysis in AutoFocus. • Third-party feeds, including closed and open source intelligence.

Palo Alto Networks Next-Generation Security Platform provides a comprehensive, integrated security solution that covers an agency's networks, endpoints and cloud applications.

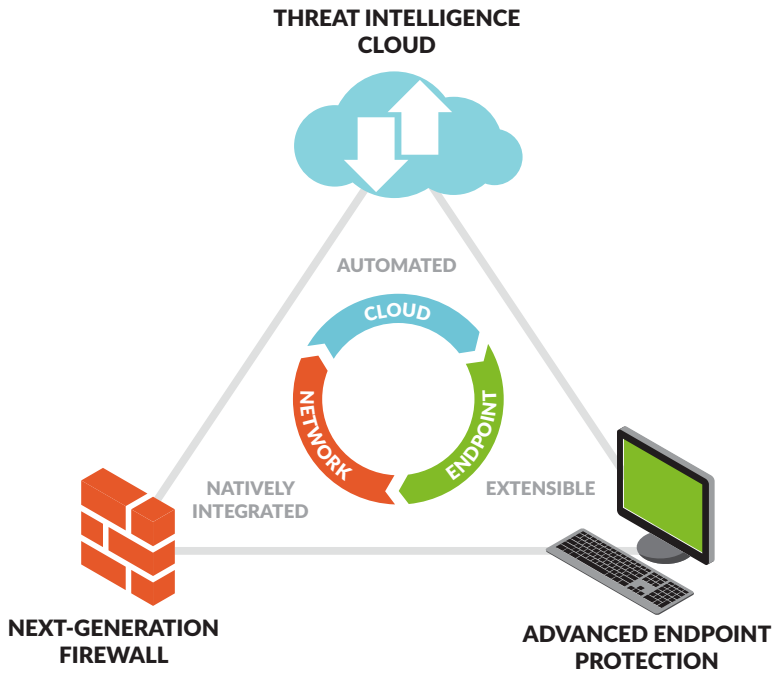


Figure 2: Palo Alto Networks Next-Generation Security Platform

Technology Alliances

Palo Alto Networks Next-Generation Security Platform provides real-time situational awareness of the network, including application usage, user tracking, cyberthreat detection/mitigation, and native integration and data sharing with systems from other vendors, such as ForeScout, Tanium®, IBM BigFix® and Splunk®. Conversely, cyber awareness gathered from those other systems can provide intelligence to the Next-Generation Security Platform for real-time mitigation and prevention. Furthermore, the platform assigns risk and severity levels to user activity and vulnerabilities/exploits.

The platform utilizes a RESTful XML API that integrates with GRC (governance, risk management and compliance) reporting platforms, such as EMC® RSA® Archer®, and business intelligence platforms, such as IBM Cognos. In this way, the Palo Alto Networks security platforms works with select technology partners to provide comprehensive CDM support.

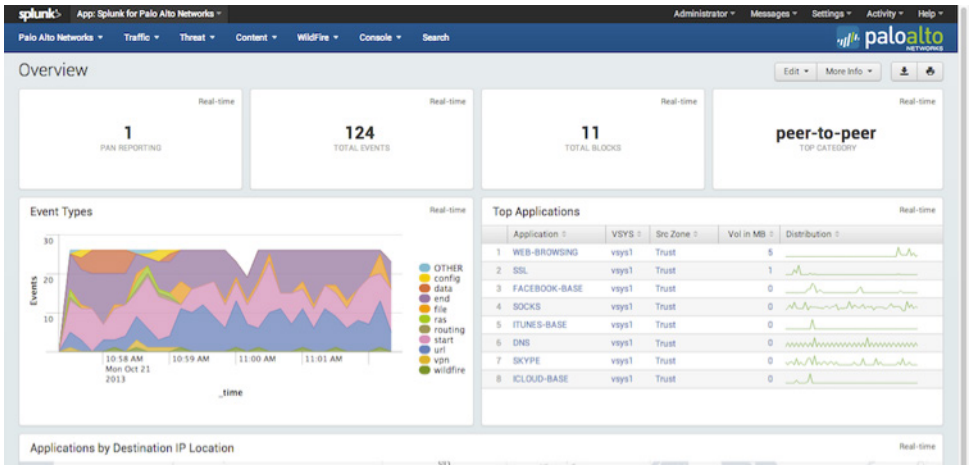
Splunk

Palo Alto Networks Next-Generation Security Platform fuels the Splunk data engine with invaluable security data network and endpoint traffic data, including details of the applications, users, content and threats responsible for and contained within each session. This serves to increase the visibility and improve the analysis results of Splunk.

The integration includes:

- Pre-defined dashboards for:
  - Traffic, apps
  - Security
  - Health
- Ability to search new malware IOCs:
  - Identifies compromised devices
- Automatic actions:
  - Register IP with tag
  - Update User-ID

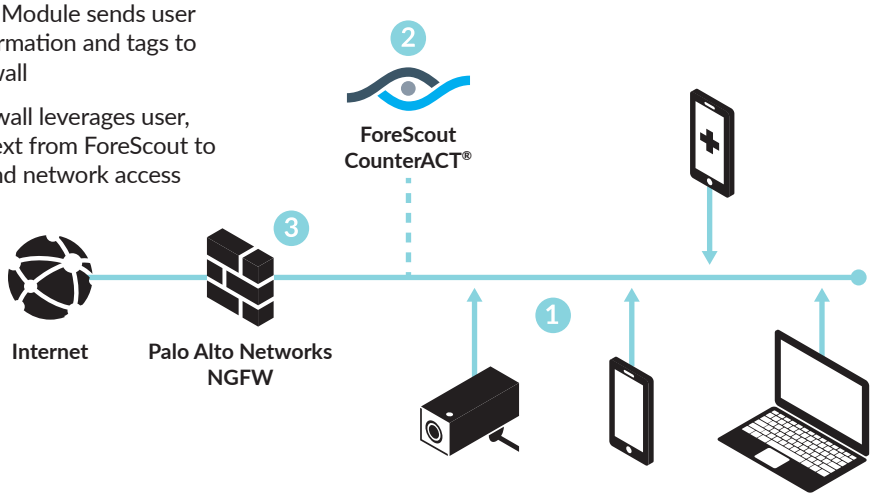
Palo Alto Networks and Splunk help CDM determine what and who is on the network, and automates control of what is happening on the network. Together, we provide true prevention to agencies benefiting from CDM.



ForeScout

The alliance combines the real-time endpoint visibility, profiling and remediation capabilities of ForeScout CounterACT® with multiple Palo Alto Networks platform capabilities to limit data breaches, detect advanced threats and take automated remediation actions. Joint capabilities are made possible through the following Extended Modules that enable threat intelligence sharing:

1. CounterACT discovers, classifies and assesses devices as they connect to the network
2. The ForeScout Extended Module sends user identity, host-profile information and tags to the next-generation firewall
3. The next-generation firewall leverages user, device and security context from ForeScout to enforce security policy and network access



Palo Alto Networks and ForeScout help control what and who is on the network by automating security policy to meet CDM goals. Together, we provide true prevention to agencies benefiting from CDM.

Delivery Partners

Approved system integrators that have partnered with Palo Alto Networks to design, deploy and manage CDM systems under the auspices of the GSA BPA include Booz Allen Hamilton, ManTech®, CGI Federal®, DXC and Northrop Grumman Corporation.

How Palo Alto Networks Next-Generation Security Platform Supports CDM Requirements

The CDM program currently consists of 15 tool functional areas rolled out in three phases, each focused on a set of requirements designed to incrementally improve network security. DHS recently announced phase four and is still working on defining its requirements.

Phase 1: Endpoint Integrity	Phase 2: Least Privilege and Infrastructure Integrity	Phase 3: Boundary Protection and Event Management
• HWAM – Hardware Asset Management • SWAM – Software Asset Management • CSM – Configuration Settings Management • VUL – Vulnerability Management	• TRUST – Access Control Management (Trust in People Granted Access) • BEHV – Security-Related Behavior Management • CRED – Credentials and Authentication Management • PRIV – Privileges	• Manage Events • Operate, Monitor and Improve • Design and Build in Security • BOUND – Boundary Protection

The new Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) task orders place these tool functional areas in five categories:

What Is on the Network?	Who Is on the Network?	How Is the Network Protected?	What Is Happening on the Network?	Emerging Tools and Technology
• HWAM – Hardware Asset Management • SWAM – Software Asset Management • CSM – Configuration Settings Management • VUL – Vulnerability Management	• TRUST – Access Control Management (Trust in People Granted Access) • BEHV – Security-Related Behavior Management • CRED – Credentials and Authentication Management • PRIV – Privileges	• Manage Network Access Controls	• Prepare for Contingencies and Incidents (CP) • Respond to Contingencies and Incidents (INC) • Manage Audit Information (AUD) • Manage Operation Security (OPS) • Design and Build in Requirements, Policy, and Planning (POL) • Design and Build in Quality (QAL)	• Includes CDM cybersecurity tools and technology not in any other subcategory

When deployed, CDM provides system and security administrators with continuous visibility into the activity of applications and users on their networks, enabling them to rapidly detect and eliminate cybersecurity threats.

Palo Alto Networks supports the following CDM requirements:

Palo Alto Networks Product/ Feature	Phase 1				Phase 2				Phase 3
	HWAM	SWAM	CSM	VUL	TRUST	BEHV	CRED	PRIV	BOUND
Network Visibility	X	X		X					X
Antivirus				X					X
IPS					X	X			X
URL & Data Filtering				X	X				X
App-ID	X	X							X
User-ID					X	X	X	X	X
Next-Generation Firewall			X	X		X	X		X
GlobalProtect		X					X		X
IPsec VPN									X
Panorama			X						
Traps				X					
WildFire				X					X
Aperture			X		X		X		X
AutoFocus				X					X

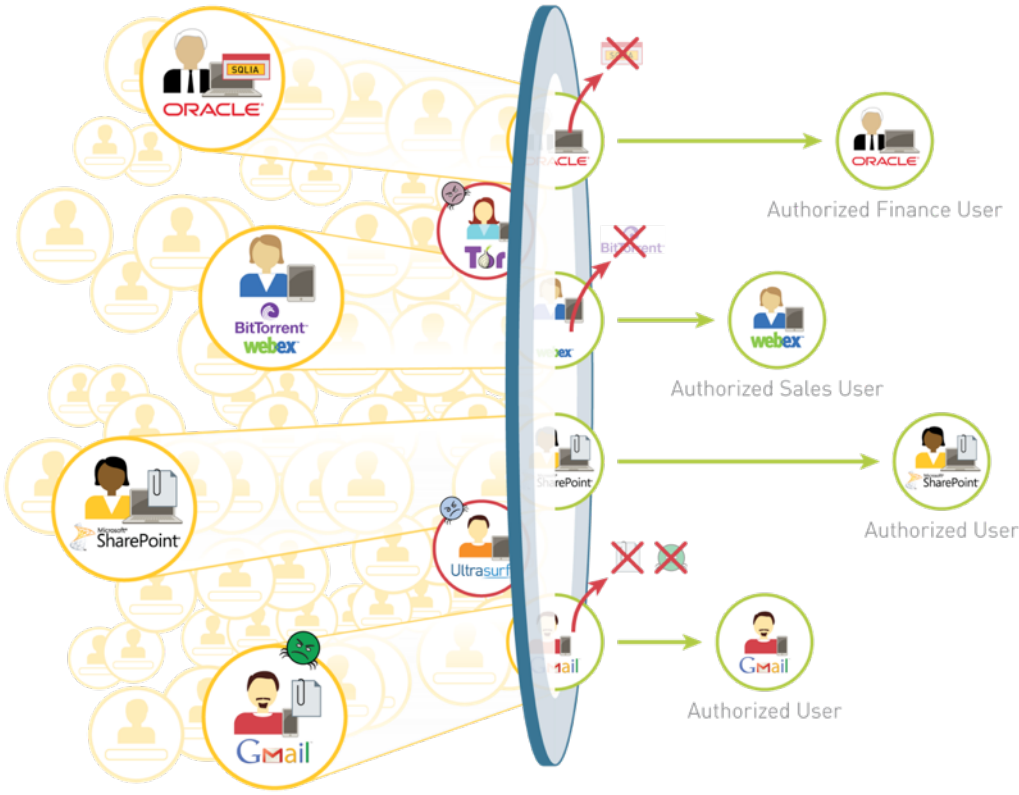
Full Support for Cloud and Mobile Assets

In addition to HWAM and SWAM assets identified during the first three phases of CDM, DEFEND expands the approach to include cloud and mobile assets.

Palo Alto Networks Next-Generation Security Platform protects private cloud or IaaS (infrastructure as a service) ecosystem environments just the same as on-premise assets.

For agencies that utilize shared services in the cloud or SaaS applications, the platform can limit access to only those services that have been sanctioned by the agency. Unsanctioned applications can be limited or restricted based on the App-ID and User-ID of the requesting party. By ensuring all mobile or remote workers are following security policies enforced by our next-generation firewalls, we can manage the use of GlobalProtect to enforce these policies by routing traffic the same as on-premise users.

For BYOD or contractor personnel who also have access to sanctioned cloud services, Aperture offers API-level connectivity and visibility into cloud applications. Aperture can identify vulnerabilities and provide automation activities to initiate actions or forensics. Adherence to policy based on appropriate access and sharing controls, and data loss prevention information to identify sensitive, at-risk data can also be autonomously remediated with notification to relevant parties.



Agencies are also expected to protect their mobile environments, and the Next-Generation Security Platform provides two capabilities that protect your mobile workforce: using Traps to prevent exploits and malware from infiltrating and infecting mobile endpoints closes an increasingly trafficked door into your agency, while GlobalProtect ensures all the protections available to on-premise users extend to your mobile workforce.

Phase 1: Endpoint Integrity

Palo Alto Networks begins by supporting the following functional requirements in Phase 1:

General Requirements[5]

- Receive and ingest relevant inventory data (HW/SW/etc.) in a standard interface and format to CDM Dashboard and other solution subsystems using a relational data structure.
- Record any number of hierarchical categories (attributes) by which the affected asset may be described, inclusive of HWAM/SWAM/CSM/VUL.
- Support encryption of data to prevent network sniffers from collecting inventory data and to prevent exfiltration from data stores.
- Send and receive asset inventory data from the central asset inventory system.
- Provide access controls for system functions.
- Provide tool component verification, such as digital fingerprints, for each software file used in the system, tied to specific software product versions and patch levels.

[5] Specific requirements shown below are taken from a U.S. government RFP

In addition to the general requirements, integration between the Palo Alto Networks Next-Generation Security Platform and the ForeScout CounterACT[6] and Tanium[7] endpoint products supports HWAM-specific requirements. Working together, these solutions discover and track all devices on the network.

HWAM – Hardware Asset Management Requirements

- Document and record authorized hardware inventory information, including but not limited to the identified key elements.
- Collect appropriate data to match actual to authorized inventory.
- Discover authorized (managed) and unauthorized (unmanaged) hardware within the network.
- Collect adequate data to enable personnel to easily locate the hardware devices on the network.
- Identify unauthorized hardware devices (physical and virtual) in the actual hardware inventory.

SWAM (Software Asset Management) is intended to ensure that only authorized software (including version number, patch levels, etc.), is on the network. The Next-Generation Security Platform identifies all hardware and software devices on the network and ensures only authorized applications are on the network.

SWAM – Software Asset Management Requirements

- Record software inventory information, including the identified key elements.
- Support population of the authorized inventory by manual or automated data entry methods.
- Discover authorized and unauthorized software within inventoried devices (authorized and unauthorized) on the network.
- Collect data to match actual to authorized inventory.
- Assess and validate software products and components on the network.
- Provide adequate data to locate the software easily on the network.
- Ensure that only authorized users can schedule detection of actual software inventory.
- Identify unauthorized software products, components and component fingerprints.
- Assess and validate the authorized software inventory, flag software products, components and component fingerprints (or equivalent) in authorized inventory that do not appear present in the actual inventory, including date last seen.
- Trigger email notifications and API notices based on user-defined business rules.
- Detect and report malware (including all non-whitelisted software and software not behaving as expected) and provide a means to remove and prevent malware from executing.
- Provide management and reporting of whitelist changes and software installation actions.
- Block unauthorized software from executing, based on an authorized software list specific to each hardware device.

[6] See "ForeScout CounterACT Integration with Palo Alto Networks Next-Generation Firewall" for more details.
[7] See "Tanium and Palo Alto Networks: Real-Time Cyberthreat Detection, Prevention and Remediation" for more details.

CSM (Configuration Settings Management) is used to track and manage configuration settings of assets, block software from executing potentially malicious input, and prevent device compromises caused by misconfigurations. The Next-Generation Security Platform captures device configuration information to identify devices that have been compromised and shares that data with other systems to prevent further contamination.

CSM – Configuration Settings Management Requirements

- Document authorized security configuration settings within benchmarks for specific software and hardware products.
- Store, process and distribute security configuration benchmarks.
- Permit authorized users to establish an authorized security configuration baseline for an (or a group of) IT asset(s).
- Track changes in the authorized security configuration baseline by date and authorized user.
- Add or tailor configuration checks with a low level of effort.
- Perform configuration assessments on a scheduled, event-driven or ad hoc basis.
- Ensure only authorized users can schedule assessments.
- Enumerate deviations from the authorized security configuration benchmark.
- Provide visibility of configuration deviations from the enterprise level to an individual user's area of responsibility.
- Apply business rules to determine responsibility for addressing deviation.
- Score (assign a numerical value to) deviations for purposes of computing risk.
- Assess the security configuration of networked IT assets.
- Store assessment results to enable reporting for a defined period of time.

VUL (Vulnerability Management) is designed to provide visibility into known vulnerabilities, delay or prevent malicious or compromised software from being installed on the network, and block vulnerable software from gaining access to other parts of the network.

These objectives are supported by the Next-Generation Security Platform through antivirus, network segmentation, endpoint analysis, patch-level verification and App-ID capabilities.

VUL – Vulnerability Management Requirements

- Provide timely coverage for CVEs, CWEs and clear directions for resolution.
- Discover actual vulnerabilities and weaknesses on the network.
- Collect appropriate data to map actual vulnerabilities and weaknesses to authorized hardware and software inventory.
- Conduct system scans to detect vulnerabilities and weaknesses on a scheduled, event-driven or ad hoc basis.
- Ensure that only authorized users can schedule scans to detect vulnerabilities and weaknesses.

Phase 2: Least Privilege and Infrastructure Integrity

The Palo Alto Networks security platform meets Phase 2 requirements by establishing network-to-device visibility of network users, applications and content platforms. These provide the ability to:

- Identify and categorize all applications seen on the network.
- Identify all users on the network, regardless of device, and tie those users to the applications they access and use.
- Scan the content within applications, identify file types and regular expressions within files, and tie that information to users and applications.

Palo Alto Networks Next-Generation Security Platform leverages Master User Records (MURs) and agency authentication systems such as RADIUS®, Active Directory®, eDirectory™ or terminal servers to enforce access restriction and filtering based on user ID, IP address and/or subnet. Identification can be used to establish access controls, privileges and behavior management, enabling agencies to restrict the types of content within specific applications; restrict applications to specific users and user groups; limit or filter out specific content types and regular expressions from all but limited users and user groups; and more. Using these technologies, administrators can establish Zero Trust zones in which only authorized users have access to key applications, ensuring compliance with TRUST (Access Control Management) requirements.

TRUST – Access Control Management Requirements

- Collect and report desired state information as defined within the defect check for TRUST.
- Collect and report actual state information as defined within the defect check for TRUST for all users.
- Evaluate and report state information as defined for TRUST.
- Document and record valid trust data elements and attributes as defined for TRUST.

Monitoring user or application behavior is covered by BEHV (Security-Related Behavior Management). The Palo Alto Networks platform ensures only authorized users who exhibit appropriate behavior can access facilities, systems and information. Adherence to policies tied to MURs and network segmentation prevents unwanted traffic from crossing boundaries and provides administrators with data that indicates whether a user is attempting to misuse network resources or use the network for unauthorized activity.

BEHV – Security-Related Behavior Management Requirements

- Collect and report actual state information as defined within the defect check for BEHV for all users.
- Evaluate and report state information as defined for BEHV to include utilization of PDP.
- Document and record valid BEHV data elements and attributes as defined for BEHV.

CRED (Credentials and Authentication Management) is an essential component of any security system to ensure only authorized individuals have access to sensitive systems. Palo Alto Networks Next-Generation Firewall leverages end-user credentials (rather than just device IP addresses) to control access to network resources. Interoperability with authentication systems enforces specific levels of access for individuals and groups.

CRED – Credentials and Authentication Management Requirements

- Collect and report desired state information as defined within the defect check for CRED.
- Collect and report actual state information as defined within the defect check for CRED for all users.
- Evaluate and report state information as defined for CRED.
- Document and record valid CRED data elements and attributes as defined for CRED.

To ensure compliance with PRIV (Privileges), the Next-Generation Security Platform ensures only authorized users with the appropriate credentials can access facilities, information and networks. Each Palo Alto Networks Next-Generation Firewall supports role-based management, which restricts user access to the management console.

PRIV – Privileges Requirements
• Collect and report desired state information as defined within the defect check for PRIV.
• Document the application of policy for authorization in the utilization of a PDP.
• Collect and report actual state information as defined within the defect check for PRIV for all users.
• Evaluate and report state information as defined for PRIV to include utilization of PDP.
• Document and record valid PRIV data elements and attributes as defined for PRIV.

Phase 3: Boundary Protection and Event Management

Phase 3 includes the following seven operational capabilities:

- Plan for events
- Respond to events
- Generic audit/monitoring
- Document requirements, policy, etc.
- Quality management
- Risk management
- BOUND – Boundary Protection, network, physical and virtual

BOUND – Boundary Requirements
• BOUND-F: Monitor and Manage Network Filters and Boundary Controls
• BOUND-E: Monitor and Manage Encryption

The BOUND requirements are defined in Tool Functional Area 5: Managed Network Access Controls. The function of NAC is to allow the agency to limit unauthorized network access to prevent attackers from exploiting network boundaries (i.e., firewalls and encryption/virtual private networks) and then pivoting to gain deeper network access and/or capture network data. Additionally, the function will limit unauthorized physical access.

Phase 3 support focuses primarily on boundary protection. Palo Alto Networks Next-Generation Security Platform – whether its components are physical or virtual deployments – natively monitors, identifies and responds to security events, and generates log files that provide an audit trail.

The table below lists the BOUND elements Palo Alto Networks Next-Generation Security Platform satisfies:

BOUND-F Elements	BOUND-E Elements
☐ Content Filter	☐ Cryptographic Algorithm
☐ Packet Filter	☐ Hash
☐ Layer 2 Filter	☐ Digital Certificate
☐ Encapsulation Filter	☐ Application Protocols
☐ Network Access Filter	☐ Transport Protocols

The platform inspects all traffic – inclusive of applications, threats and content – and ties it to the user, regardless of location or device type. Applications, content and users become integral components of your enterprise security policy. The result is the ability to align security with your key business initiatives. With our Next-Generation Security Platform, you reduce response times to incidents, discover unknown threats, and streamline secure network deployment. Moreover, our platform can:

- Safely enable applications, users and content by classifying all traffic, determining business use case, and assigning policies to allow and protect access to relevant applications.
- Prevent threats by eliminating unwanted applications to reduce your attack surface area, and apply targeted security policies to block known vulnerability exploits, viruses, spyware, botnets and unknown malware.
- Protect your data centers through the validation of applications, isolation of data, control over rogue applications and high-speed threat prevention.
- Safely enable public and private cloud computing environments; deploy, enforce and maintain security policies at the same pace as your virtual machines.

CDM Phase 3 Use Cases

Application-Aware Next-Generation Firewall

Palo Alto Networks defined the next-generation firewall security market. It applies policy based upon port, protocol and/or application. It integrates user identification into firewall policies so administrators can create granular policies. It decrypts SSL to inspect HTTPS connections. It can apply quality of service to individual policy flows. It performs IPS/IDS and URL categorization/web content filtering. It inspects traffic to prevent passage of predefined patterns, like credit card numbers, Social Security numbers or custom regular expression patterns.

Additionally, Aperture provides cloud-based, application-aware inspection for SaaS applications. Custom IPS, application and URL definitions can be created to map to government-specific environments. Among the capabilities of the next-generation firewall is the ability to be an NSA Commercial Solution for Classified/Suite B traffic filtering firewall. Palo Alto Networks Next-Generation Security Platform is certified for FIPS 140-2 – Level 2 for hardware and Level 1 for VM-based appliances. All systems can be managed individually via the GUI or via Palo Alto Networks Panorama network management system.

Stateful Firewall

Palo Alto Networks Next-Generation Firewall can operate at Layer 3 or Layer 4 as a port/protocol firewall – however, by default it operates at Layer 7 as an application-aware firewall. Different policies within the system can operate at different layers, allowing organizations to combine the most effective firewall policy checks possible. The policies can be tied to individual user identity through User-ID. User-ID enables precise user policies to account for distinctions in policy privileges granted to personnel in different roles. The platform maintains a built-in SSL decryption capability, allowing firewall policy checks against inbound or outbound HTTPS traffic.

Web Application Firewall

Palo Alto Networks Next-Generation Security Platform incorporates many web application firewall capabilities, including stateful inspection, application-layer firewall, intrusion prevention, intrusion detection and web content filtering. The systems decode HTTPS to allow deep packet inspection of HTTPS sessions. Application-layer firewalls provide detailed application-layer visibility. The systems can also use custom application definitions for granularity within individual applications, such as peer-to-peer file sharing applications.

Forward/Reverse Web Proxies

Palo Alto Networks Next-Generation Security Platform provides port/protocol and/or application-layer firewall functionality. Additionally, it offers web content filtering (URL classification) consistent with the SP 800-54r3 SC-7(8) boundary protection security control. Built-in IPS/IDS signatures scan client-to-server and server-to-client traffic (including responses). The application-layer firewall capabilities assess applications to validate that only valid application traffic traverses the network and other traffic does not masquerade on a specific port by riding over that port.

Intrusion Detection/Prevention Systems

Palo Alto Networks Next-Generation Security Platform is a full-fledged, stand-alone intrusion detection and prevention system. In conjunction with our WildFire public or private cloud, Palo Alto Networks intrusion detection and prevention systems maintain the latest signatures to protect an environment from attacks. WildFire performs analysis on unknown files and creates four types of signatures: antivirus, DNS, URL Filtering, and command-and-control. Additionally, AutoFocus provides the keen analysis capability of WildFire results to help determine if other parts of the network are susceptible to known attacks.

Database Firewalls

Palo Alto Networks Next-Generation Security Platform can create custom application definitions at Layer 7 to analyze specific application queries. This includes writing custom definitions for database languages. SQL, for example, is already a defined application within the included application decoders.

VPN Concentrator and Network-Layer Encryption

Palo Alto Networks Next-Generation Security Platform provides two forms of VPN termination: SSL- and IPsec-based systems. The SSL offering, GlobalProtect, provides a dynamic, load-balanced remote access tunnel to give remote personnel the same protections they would receive behind their company firewall. The IPsec termination capability provides remote access or site-to-site IPsec tunnel capability. Included in this capability is the NSA Commercial Solutions for Classified/Suite B capability for IPsec VPN gateways.

Incident Response Automation

Palo Alto Networks Next-Generation Security Platform works to automate workflow to handle security incidents within an organization. With the use of dynamic tags, we can leverage sources to automate the inclusion of hosts into security policy designed to reduce attack surface and exposure to incidents. We also work with third-party integration partners to automate the securing of compromised hosts as well as the sharing of additional threat and IOC information to aid in identifying and securing the infrastructure.

Palo Alto Networks Is CDM-Ready

Palo Alto Networks Next-Generation Security Platform provides an easy-to-use, cost-effective management environment that enables agencies to meet CDM requirements without compromising simplicity or mission requirements. Today, and moving into the future, Palo Alto Networks serves the cybersecurity needs of civilian agencies and other government entities both in the United States and throughout the world.

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

© 2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
leveraging-cdm-to-improve-cybersecurity-wp-063017