



Using Palo Alto Networks® Security platform to meet CDM Phase 2 Requirements

CHALLENGE:

Compliance programs which lack real-time metrics, such as 3-year attestation cycles, to “cyber security readiness” don’t give timely visibility to an agency’s proficiency to thwart or respond to today’s zero-day attacks and other malicious threats. The longer it takes to identify or respond to these sophisticated attacks and cyber threats today, the more damage or critical data leakage an agency can face.

SOLUTION:

The Continuous Diagnostics and Mitigation (CDM) program entails three phases of government cyber-readiness. The 1st phase focuses on identifying what is on the network in terms of hardware, software and those configurations as well as any vulnerabilities within those systems. The 2nd phase identifies who is on the network—the networks’ users and the appropriate privileges for each user. The 3rd and final phase provides for events monitoring, i.e. that ongoing view of events happening on the network that have the potential to impact the network and its data.

BENEFIT:

To protect government resources, the CDM program can enable government agencies to a) have the necessary visibility to know that its systems are free from vulnerabilities, its users are authenticated and approved for only the appropriate access, and that its data has the utmost protection from both internal and external threats and b) when this is not the case, to have the actionable intelligence to determine any necessary steps that must immediately be taken to ensure that protection.

The U.S. Government Continuous Diagnostics and Mitigation (CDM) program provides a three-phased approach to securing the government’s networks and systems. Phase 2 focuses on capabilities to provide Least Privilege and Infrastructure Integrity tool options.

Palo Alto Networks unique platform approach provides solutions to meet Phase 2’s five Least Privilege and Infrastructure Integrity capabilities in a singular platform, reducing the costs and complexity of implementing these important capabilities. Starting with the important foundation of visibility to who and what applications and content are on the network, agencies can more easily establish access controls called for in Phase 2, set policies and application permissions to manage behaviors and privileges on the network. In addition, MA’s establish ongoing visibility for access control, behavior, credentials and authentication management, privileges, and boundary protection.

Several key features of the Palo Alto Networks enterprise security platform form the foundation for the controls and protections required to meet Phase 2 requirements. Palo Alto Networks **identification technologies** establish end-to-end network-to-device visibility to the networks’ users, applications and content:

- 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. User-ID™ integrates with the widest range of directory services on the market;
- Scan the content within the application, identify file types and regular expressions (regex) within files and tie that to users and applications.

All identifications can be associated together to establish access controls, privileges, and behavior management for CDM Phase 2. As such, agencies can restrict the types of content within specific applications, restrict applications to specific users and user groups, limit or filter out specific content types and regex from all but limited users and user groups, and more. With these identification technologies, administrators can establish “zero trust zones” to which only authorized users have access to key applications. See Figure 1. As such, agencies can use the Palo Alto Networks platform in either the physical appliance or the virtual machine version to readily establish network, physical, and virtual boundary protection for Phase 2 and to provide ongoing security monitoring for traffic behavior between zones.

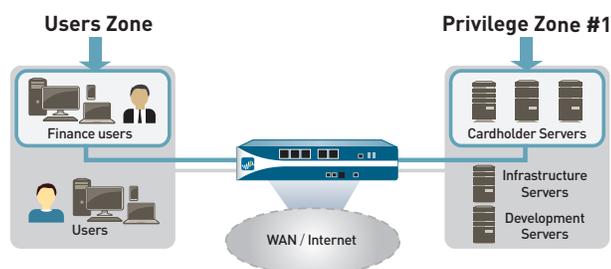


Figure 1: Zero-Trust zones

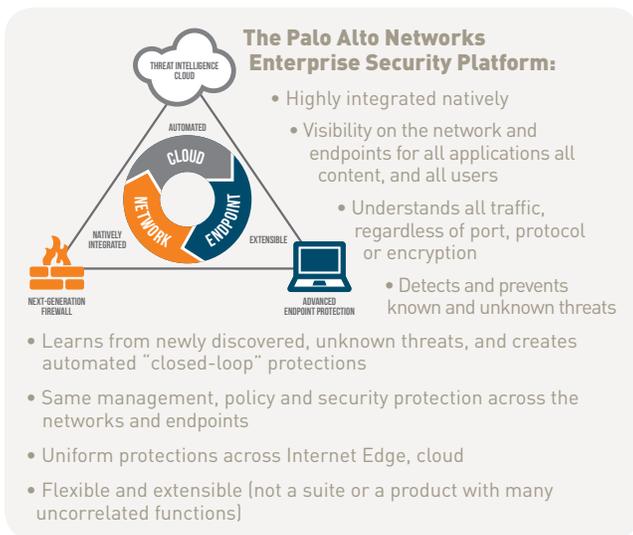


Figure 2: Palo Alto Networks Enterprise Security Platform

The following section describes how the Palo Alto Networks enterprise security platform, shown in figure 2, addresses each of the five CDM Phase 2 capabilities.

Manage Network Access Controls/Boundary Protection (Network, Physical, Virtual) (Functional Area 5)

To ensure threats into and lateral movement through the network are prevented, visibility and segmentation are critical. Palo Alto Networks enterprise security platform can ensure that all devices, users and applications are segmented into authorized enclaves, access to privileged network segments is controlled, and that blacklisting or whitelisting of applications and devices is supported. Palo Alto Networks provides access restriction and access filtering based on user identification and/or ip address and/or subnets with authentication systems such as RADIUS, Active Directory, eDirectory or Terminal Servers. Palo Alto Networks safely enables applications and manages user access and content at the platform.

TRUST: Manage Trust in People Granted Access/Access Control Management (Functional Area 6)

Palo Alto Networks visibility extends not only to communications coming into the network, but communications and lateral movement within the network, as well as exfiltration of information leaving the network. Starting with this visibility as a baseline, users can work safely and access their applications, and insider threats can be readily identified. Agencies can ensure only authorized users with the required trust levels are accessing information and networks. Palo Alto Networks platform can leverage Master User Roles (MURs) and agency authentication systems such as RADIUS, Active Directory, eDirectory or Terminal Servers to provide access restriction and access filtering based on users' ID's, ip addresses and/or subnets.

BEHV: Manage Security-related Behavior/Behavior Management (Functional Area 7)

Palo Alto Networks platform visibility ensures only authorized users who exhibit appropriate behavior can access facilities, systems, and information. Adherence to policies tied to the Master User Roles (MURs) and network segmentation on the Palo Alto Networks platform prevents unwanted traffic from crossing boundaries and provides the administrators with data to indicate if a network user is attempting to misuse unauthorized network resources or use the network for unauthorized activity.

CRED: Manage Credentials and Authentication/Credentials and Authentication Management (Functional Area 8)

Palo Alto Networks user identification features can block user access to network resources. Interoperability with authentication systems like RADIUS, Active Directory, eDirectory or RSA can provide specific levels of access. Palo Alto Networks platform will help manage the authentication process.

PRIV: Manage Account Access/Privileges (Functional Area 9)

Palo Alto Networks can ensure only authorized users with the authorized credentials access facilities, information, and networks. Each Palo Alto Networks system supports role-based management which can restrict user access to the management console. Other authentication systems, for ex, RADIUS, can also be leveraged for this restriction.

SUMMARY

Government networks are dynamic, just like the threats against them. CDM will provide government agencies with a means to continuously monitor the ongoing influx of new applications and users required to meet today's and tomorrow's mission demands while reducing mission risks from an unending onslaught of threats. Palo Alto Networks enterprise security platform provides a cost-effective means to meet CDM Phase 2's Least Privilege and Infrastructure Integrity capabilities without compromising simplicity or mission requirements.

PALO ALTO NETWORKS FOR GOVERNMENT

Today, Palo Alto Networks serves the cyber security needs of the U.S. warfighter and civilian agencies, as well as those of allied countries throughout the world.

SEE FOR YOURSELF
 Call 866.320.4788 to participate in a free Ultimate Test Drive where you get hands-on experience in a free half-day workshop. See for yourself as you create the security policies that provide the application, user and content visibility and network segmentation needed for CDM Phase 2.



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

Copyright ©2014, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. PAN_SB_CDM_072514