

How Endpoint Privilege Management Fulfills Federal Mandates

Extend Zero Trust and Identity Security
to Endpoints and Servers

Table of Contents

The Call for Endpoint Privilege Security.....	3
Federal Directives Require Action to Protect Privileged Accounts	3
Why Foundational Protection Is Vital.....	4
Idira Endpoint Privilege Manager Reduces Ransomware-Related Risks	5
Idira Endpoint Privilege Manager Enables an Effective Cybersecurity Program	6
Satisfy Federal Endpoint Privilege Management Requirements with Idira	7
About Palo Alto Networks.....	7

The Call for Endpoint Privilege Security

Cyber adversaries continue to pose an increasing global threat to information systems, particularly those used by the US federal government. The extensive government systems, many of them storing and processing high volumes of confidential information, and the vast number of third-party partners and contractors, all increase the attack surface to federal endpoints. The increasing threat levels place more demands on security personnel, yet agencies face workforce shortages and budget pressure challenges. Protecting network and computing infrastructure is critical to preserve the confidentiality, integrity, and availability of communication and services across an agency enterprise.

Among security leaders, 49% say they lack complete visibility into entitlements and permissions across their cloud environments.¹ Even when an attacker does not directly use a privileged account as the initial point of entry, they quickly find ways to enumerate and attack accounts with elevated rights.

Privilege escalation is a key exposure tactic. The MITRE ATT&CK[®] taxonomy of tactics, techniques, and procedures (TTPs) includes a whole suite of privilege escalation techniques in the arsenal used for attacking and compromising systems. Adversaries use privilege escalation—taking advantage of system weaknesses, misconfigurations, and vulnerabilities—to gain higher-level permissions so they can enter and explore a network or system.

Agencies have been directed to place increased focus on endpoint detection and response (EDR). While these approaches are vital, by definition, they provide a limited and reactive capability that applies only after an adversary has already experienced some level of success. A more proactive strategy is to use endpoint privilege security as a preventive approach, to address privilege misuse, enforce role-specific least privilege policies, and reduce or remove the ability for the adversary to gain access.

Federal Directives Require Action to Protect Privileged Accounts

Recent administrative directives recognize the importance of enforcing principles of least privilege and protecting key accounts from unauthorized access. For example, [Executive Order \(EO\) 14028](#), Improving the Nation's Cybersecurity, reminds us that the United States faces persistent and increasingly sophisticated malicious cyber campaigns. While they threaten the public and private sectors, they ultimately threaten the American people's security and privacy.

Application of the required EO security measures, including mandates to follow privilege access management principles for network-based administration and configuration management of critical software platforms, are greatly improved through the use of automated endpoint privilege management (EPM). EPM is an effective force multiplier, enabling agency success in fulfilling these increasing requirements in the face of workforce and budget challenges. Agencies that apply EPM solutions improve productivity, reduce help desk inquiries, and avoid costly losses and disruptions, often resulting in a measurable return on investment.

Endpoint privilege management solutions, such as Idira™ Endpoint Privilege Manager, by Palo Alto Networks, are front and center in a digital identity ecosystem. These efforts build on EO 14028 initiatives, notably through application of a zero trust architecture and major improvements in cyber supply chain risk management. EO 14028 emphasizes the significance of ensuring the security and integrity of critical software. Supply chain cybersecurity controls, including those for the developers and providers of critical software, require endpoint privilege security-like protections. For example, configuration management practices must maintain EO-critical software platforms and all software deployed to them. They must identify the hardened configuration of each platform and all the software deployed to it.²

1. *2025 Identity Security Landscape*, CyberArk, May 2025.

2. "Executive Order 14028, Improving the Nation's Cybersecurity," NIST, updated April 25, 2025.

Why Foundational Protection Is Vital

EO 14028 requires agencies to improve the ability to detect malicious cyber activity on federal networks by enabling EDR solutions. This represents an important step but may not be sufficient to prevent cyber intrusions. Endpoint privilege security serves as the cornerstone of an endpoint privilege management strategy, which can then be bolstered by effective EDR. Idira Endpoint Privilege Manager works with Palo Alto Networks Cortex® solutions to provide a comprehensive approach to preventing, detecting, and responding to advanced threats.

Agencies have invested significant resources into EDR solutions and often feel this investment delivers adequate endpoint security. Yet, many conventional endpoint threat detection and response tools must rely upon the integrity of the agents and protections on the endpoints—agents that can be manipulated or disabled before the EDR tool can do its work. The cybersecurity landscape is littered with examples of sophisticated attacks that sidestepped EDR solutions. This includes the widely publicized SolarWinds SUNBURST incident, a massive supply chain attack that went undetected for nine months, impacting over 18,000 organizations across the globe including nearly every Fortune 500 company.³

Idira Endpoint Privilege Manager is specifically designed to fill the gaps left by traditional threat detection and mitigation solutions and defend businesses against privileged attackers. Unlike EDR and XDR products, the Idira Endpoint Privilege Manager strengthens security and mitigates risk by removing standing admin privileges and enforcing the principle of least privilege. More importantly, Idira Endpoint Privilege Manager is designed to remove local admin rights, implement policy-based, just-in-time elevation and application control, as well as discover and secure privileged accounts on the endpoint.

Because many of today's cyberattacks occur through privilege abuse or escalation at the endpoint, combining effective EDR/XDR with EPM fulfills federal requirements and reduce the attack area significantly.

Zero trust architecture (ZTA), described in [NIST Special Publication \(SP\) 800-207](#) and associated guidance, is an important engineering model for federal stakeholders, and it's a practical approach for any organization. Despite the name, zero trust doesn't mean "don't trust anyone." Rather, it draws on the old saying "trust, but verify." The concept means zero assumed trust. For example, just because packets are arriving from an internal server, don't presume that the traffic is safe. Even though a request indicates it's from a known device, service, or user, don't presume that they are whom they claim to be. CISA has announced major ZTA initiatives including a new office that will guide and drive ZTA improvements. Idira solutions will help agencies make progress on these mandatory requirements, of course while also working to defeat adversaries.

**The SolarWinds
SUNBURST
incident, a massive
supply chain
attack that went
undetected for nine
months, impacted
over 18,000
organizations across
the globe including
nearly every Fortune
500 company.**

³. "How SolarWinds Responded to the 2020 SUNBURST Cyberattack," Harvard Business Review podcast, January 16, 2024.

Idira Endpoint Privilege Manager helps fulfill the requirements of [CISA's five ZTA pillars](#) as described in NIST SP 800-207 and CISA's Zero Trust Architecture:

1. **Identity:** Specific to privileged identities or users, access needs to be continuously monitored and validated in terms of user trustworthiness to govern access and privileges. Incorporating identity access with a least-privileged approach is foundational to zero trust. Privileged identities should only be provided access to the systems when specifically required. Access should be as limited as possible, and access should be immediately revoked when it is no longer required. Idira Endpoint Privilege Manager supports this identity and access management aspect of ZTA effectively for human and nonhuman identities (e.g., service accounts).
2. **Devices:** Through robust privilege on endpoints and servers, Idira Endpoint Privilege Manager improves prevention, detection, and response. The CISA Zero Trust Maturity Model (ZTMM) recommends integrated threat protections for your agency endpoints. Because most breaches involve the compromise of privileged accounts and credentials, Idira Endpoint Privilege Manager is a vital part of that protection, which extends to the vital tools that detect and respond to sophisticated threats.
3. **Networks:** Idira Endpoint Privilege Manager supports the network pillar by limiting untrusted access to internet and intranet systems. ZTMM calls for tailored local controls, dynamic updates, and secure external connections based on application and user workflows. The solution helps to prevent malware communication back to command-and-control servers and protects from network-born encryption, such as when files on network shares are encrypted from a compromised machine. In partnership with zero trust network security architecture such as network segmentation, traffic management, and traffic encryption, Idira Endpoint Privilege Manager supports a holistic security model.
4. **Applications:** Idira Endpoint Privilege Manager supports granular execution and elevation. It also includes resource access controls and integrated threat protections for enhanced situational awareness and to mitigate application-specific threats. The approach includes enforcement of least-privileged controls and granular application access controls. Idira Endpoint Privilege Manager can manage application elevation, allow or deny access to internet and intranet services, and control and restrict access to memory space of other process. Application control extends to how and when a program can be executed. For example, Idira Endpoint Privilege Manager can enable an application to run based on the day of the week or time of the day. It can also restrict what other applications can launch and do, depending on the elevation state. These capabilities help to automate application configurations to continuously optimize for security and performance—another ZTMM recommendation.

Notably, while these EPM capabilities already greatly support the applications pillar, integration through extensive partnerships and APIs with the world's most trusted protection, detection, and response solutions extend agencies' application and workload security to new heights.

5. **Data:** ZTMM states that, "Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure and backups (including on-premises and virtual environments) as well as the associated metadata."⁴ By applying the elements above, Idira Endpoint Privilege Manager enables agency practitioners to identify where critically important and sensitive data live, enforce least privilege and access to that data, and integrate that solution with effective EDR and monitoring solutions.

Idira Endpoint Privilege Manager Enables Significant Advancement in Zero Trust Maturity

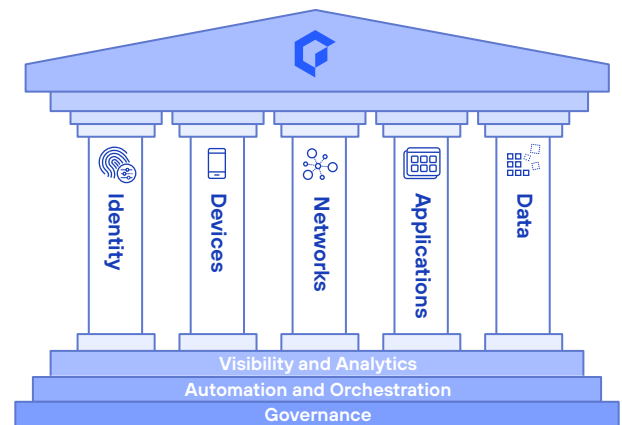


Figure 1. Zero trust maturity model pillars

4. *Zero Trust Maturity Model*, Cybersecurity and Infrastructure Security Agency, April 2023.

Idira Endpoint Privilege Manager Reduces Ransomware-Related Risks

Among the biggest risks to data today is the threat of a ransomware attack. The likelihood and impact of ransomware can be greatly reduced by using a well-rounded endpoint privilege manager, which can remove local admin rights and then, based on policies, elevate certain programs or tasks in a transparent manner. Agencies don't have to remove all privileges from their users—and potentially hinder their ability to perform their work duties. Instead, Idira Endpoint Privilege Manager enables automated policy-based and ad hoc workflows that enable on-demand privilege elevation without impairing the end-user experience or burdening support teams.

A glance at the MITRE ATT&CK TTPs described in an earlier section reminds us that sophisticated attacks, including ransomware attempts, rely on a workflow that includes reconnaissance, initial access, execution, and privilege escalation. Effective endpoint privilege management provides multiple methods to thwart these tactics, including through conditional policies to block attacks involving trusted applications. For example, Idira Endpoint Privilege Manager could support a rule that would allow users to launch PowerShell with certain parameters while preventing other apps from launching PowerShell as a child process, thus eliminating chained exploit techniques.

Completely blocking endpoint applications can reduce a user's effectiveness or bury the IT service desk in constant changes. This situation leads endpoint privilege managers to support application greylisting and ringfencing to help defend against unknown malware variants without impeding the users' operation of unknown applications that pose no known security risks. Greylist policies apply to applications that aren't explicitly allowlisted nor denylisted. Through automated policies that provide out-of-the-gate reduction of endpoint attack surface while supporting and reporting access management, EPM is an important element of an agency's comprehensive cybersecurity suite.

Idira Endpoint Privilege Manager Enables an Effective Cybersecurity Program

While each of these initiatives is important, the key mission for agency security leadership and operations is to establish effective cybersecurity solutions at the enterprise, mission/business, and system levels. Idira Endpoint Privilege Manager provides the right solution for many of the security requirements for protecting agency systems.

Idira Endpoint Privilege Manager satisfies key requirements in many of the families of security and privacy controls found in the catalog known as [NIST Special Publication 800-53](#). Primarily, Idira Endpoint Privilege Manager supports the Access Control family. For example, Account Management (AC-2) calls for diligent and secure management of various types of accounts, and for restricted, controlled policies for granting elevated privileges. Control enhancement AC-2 (6) specifically calls out the need for dynamic privilege management as "dynamic access control approaches [that] rely on runtime access control decisions facilitated by dynamic privilege management." Idira Endpoint Privilege Manager also supports Access Enforcement (AC-3) and Least Privilege (AC-6), which emphasize applying the principle of least privilege. They refer to authorizing essential access only for users (or processes acting on their behalf) to accomplish assigned tasks.

88% of security leaders say they face stricter requirements from cyber insurance providers to implement privilege controls.⁵

5. CyberArk, *Identity Security Landscape*.

Many of these same needs are reflected in the requirements for Protecting Controlled Unclassified Information in [Nonfederal Systems and Organizations, NIST SP 800-171 Revision 3](#). These requirements are an important part of an agency's cybersecurity supply chain risk management (C-SCRM) approach and are often included in agency security reviews (including the emerging Cybersecurity Maturity Model Certification [CMMC] program).

Through implementation of Idira Endpoint Privilege Manager, especially as integrated through APIs to other protection, detection, and response tools, agencies are able to effectively plan, achieve, and monitor many of the elements for agency cybersecurity needs. Idira Endpoint Privilege Manager helps agencies work with contractors and partners to ensure robust cybersecurity in nonfederal systems.

Satisfy Federal Endpoint Privilege Management Requirements with Idira

Agencies have a duty to safeguard citizens' information and services using every tool available. Key stakeholders not only expect secure performance but improvement, as demonstrated by increasing programs to drive agency accountability. By implementing Idira Endpoint Privilege Manager, federal agencies can fulfill all these needs. They can thwart the adversaries, reduce burdens on internal systems (like help desks and administrators), and propel the entity to an advanced zero trust and supply chain maturity.

Learn how Idira Endpoint Privilege Manager can help your organization reduce attack surfaces, mitigate risk, and help fulfill federal requirements. [Request a demo.](#)

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.



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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

idira_wp_how-endpoint-privilege-management-fulfills-federal-mandates_041526