

---

# Buyer's Guide to Managing Endpoint Privileges

Extend Zero Trust to Endpoints  
for Ransomware Defense



# Contents

<b>Introduction</b> .....	3	6. End-to-End Continuous Identity Security .....	10
<b>Why Manage Privileges on the Endpoints</b> .....	4	7. Administrative Reports and Dashboards.....	10
<b>Choosing the Right Endpoint Privilege Management Solution</b> .....	5	8. AD Bridging: Modernize Linux Identity and Access Management .....	11
Highlights of a Complete EPM Solution .....	5	9. Extend Your XDR and NetSec with Identity-Based Endpoint Enforcement .....	11
<b>Evaluation Criteria</b> .....	6	<b>Endpoint Privilege Management Tool Checklist</b> .....	12
1. Removing Local Admin Rights.....	6	<b>Secure Access and Privilege at the Endpoint</b> .....	13
2. Password Rotation, Automatic Discovery, and Onboarding of Privileged Accounts.....	6	<b>Benefits of Modern Endpoint Privilege Management Solutions</b> .....	14
3. Least Privilege Enforcement .....	7	<b>Take the Next Step Toward Managing Endpoint Privilege</b> .....	15
4. Managing Endpoint Privileges Is Foundational .....	8	<b>About Palo Alto Networks</b> .....	16
5. Conditional Application Control and Ringfencing .....	9		

# Introduction

The financial stakes are high for organizations—specifically for 9 out of 10 organizations that report having experienced an identity-centric breach.<sup>1</sup> Today, attacks reach exfiltration in just 72 minutes.<sup>2</sup> The cost of resolving these attacks and restoring operations alone can stretch costs into billions of dollars, with median initial ransom demands alone surging to \$1.5 million in 2025.<sup>3</sup>

Attackers get in by compromising identities at the endpoints and then logging in. Endpoints—including the desktops, laptops, servers, and workstations that connect to an organization's network—provide attackers a potential open door to corporate assets and applications.

Once attackers and cybercriminals gain access privileges to an endpoint, they exploit it to:

- Alter configurations.
- Completely disable threat detection, antivirus programs, or disaster recovery tools.
- Launch ransomware and other malware and increase impact.
- Steal confidential data.

This guide reviews key endpoint privilege management (EPM) capabilities, provides tips for evaluating products, and takes the guesswork out of selecting the right tool for your organization.

---

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

2. *Unit 42 Global Incident Response Report 2026*, Palo Alto Networks, February 17, 2026.

3. Palo Alto Networks, *Global Incident Response Report*.

**9 out of 10**  
organizations report  
having experienced  
an identity-centric  
breach.

---

**72 minutes**  
the amount of time  
it takes for attacks to  
reach exfiltration.

# Why Manage Privileges on the Endpoints

Privileged endpoint accounts, like Microsoft Windows, macOS, and Linux administrator accounts, are a common target for threat actors. If they gain access to an organization's systems through just one endpoint, they then have a launchpad to move laterally across the network and steal data or plant ransomware. Once adversaries gain access to privileged accounts, they can take over workstations, servers, and other critical parts of the infrastructure. These identities could be service accounts, hard-coded secrets, or any off-the-shelf homegrown solution requiring powerful credentials to perform its function.

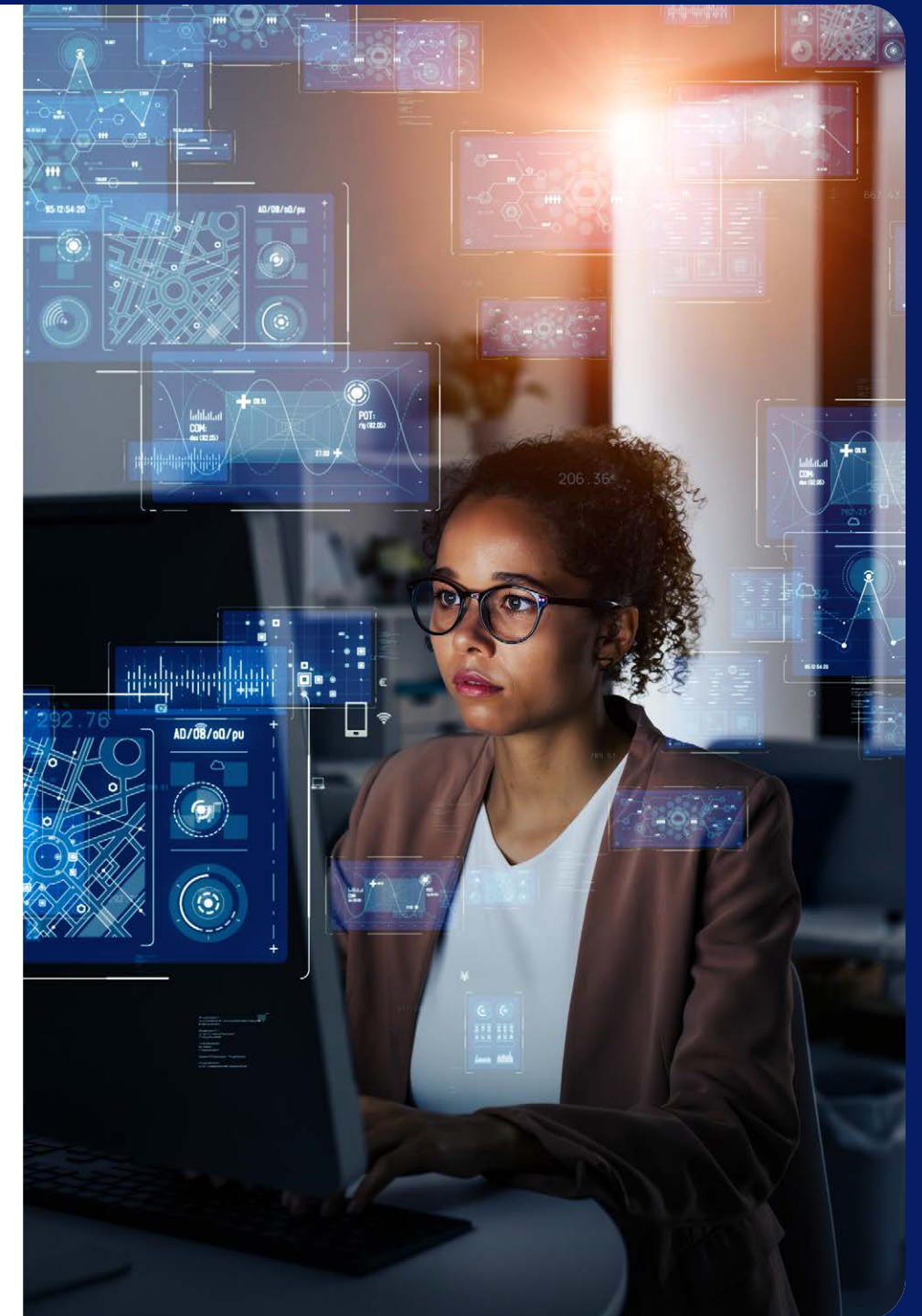
To protect all human identities—users, developers, or IT administrators—organizations must extend identity security and zero trust to their endpoints. Solutions that manage privileges for endpoints put the control over privileged accounts back into the hands of the IT team. Coincidentally, 88% of organizations report facing stricter requirements from cyber insurance providers to implement privilege controls.<sup>4</sup>

Endpoint privilege management (EPM) tools are crucial cybersecurity defense for one simple reason. Most cyberattacks begin at the endpoint, which is where identities interact with critical resources. At the endpoint, identity security and zero trust principles must converge to provide a comprehensive defense.

4. CyberArk, 2025 Identity Security Landscape.

In today's environment, characterized by new identities, environments, and AI-driven threats, security rests on building a seamless identity security fabric with complete coverage of your assets. EPM solutions provide the cornerstone of this strategy by delivering preventative identity-centric measures, as opposed to reactive asset-based measures. They reduce the attack surface by granting right-time, right-level access that ensures staff can safely access the IT systems, services, and data they need to be effective. These solutions also help mitigate cyber risk by providing foundational endpoint security controls, locking down endpoint privileges, and improving application governance.

EPM tools help organizations implement the principle of least privilege, identity security, and zero trust, empowering users and admins to perform their duties without compromising security or opening gaps for cybercriminals. These tools are integral for implementing a comprehensive zero trust strategy because they secure user access from the first mile of user access to the last mile of information consumption at the endpoints.



# Choosing the Right Endpoint Privilege Management Solution

Because ransomware attacks typically start on workstations and servers, cyber insurance underwriters are tightening their scrutiny of endpoint privilege controls. In particular, they are focusing on an organization's ability to remove local admin rights from all users, including senior system administrators, developers, and people using legacy applications that require admin rights.

## Highlights of a Complete EPM Solution

- **Helps remove local admin rights** without impacting the user experience or creating operational bottlenecks.
- **Enforces the principle of least privilege** to reduce endpoint vulnerabilities and shrink attack surfaces.
- **Supports smart (conditional) application control and ringfencing** to defend against unknown malware variants.
- **Provides visibility and guardrails** for AI agents, MCP servers, AI skills, and other agentic AI implementations that attackers target.
- **Integrates with an IdP** to provide desktop sign-in, continuous strong authentication with a variety of multifactor authentication (MFA) options, including passwordless, support step-up, and over-the-shoulder authentication for high-risk actions.
- **Includes comprehensive administrative reports and dashboards** to improve oversight, increase visibility, and streamline compliance audits and forensics investigations so that endpoint privilege policies are easy to enforce and prove.
- **Provides Active Directory (AD) Bridging** for Linux machines to enable logging in with centralized cloud directory accounts.
- **Acts as an identity- and privilege-based enforcement engine** for XDR and network security components.
- **Includes AI-powered policy recommendations** to simplify initial rollout, configuration, and usage of the solution. Default policies, frameworks (like QuickStart), and AI policy recommendations that deliver insights tailored to your organization's environment can help shape your least-privileged configuration, provide an optimal user experience, and maximum risk reduction.

# Evaluation Criteria

## 1. Removing Local Admin Rights

Removing local admin rights as a security measure is nothing new. Restricting users to standard user accounts has a profound and positive impact on security. However, without the right tools and planning, removing local admin rights can impair the user experience.

Too many IT departments hastily remove local admin rights only to face an immediate backlash from disgruntled users. Some IT teams, however, believe that removing local admin rights hurts an organization more than it helps. Other not-so-radical teams probably had different experiences based on their setup. For example, maybe they remote into user machines to install a font or printer, update a program, or change the time zone. Or they tried to force their way with users but eventually had to budge and return the local admin rights to them.

A well-rounded EPM tool can solve these challenges by discovering privileged accounts and removing local admin rights. Based on policies, the tool should transparently elevate certain programs or tasks so a user never sees a prompt or needs to ask IT for assistance. If a user has a special case, they can request elevation, which can be approved without remoting to the machine. On the backend, this type of EPM solution should integrate with an IT ticketing system for smooth workflows and fast elevations.

## 2. Password Rotation, Automatic Discovery, and Onboarding of Privileged Accounts

Addressing the local admin account password challenge requires a powerful and reliable solution. Organizations can mitigate this persistent risk by applying endpoint security controls for loosely connected devices.

When considering a solution, critical capabilities should include both automated local privileged account discovery and enforcement of password rotation based on policies. These capabilities deliver security reinforcement even when endpoints have limited internet connectivity.

Organizations can streamline operational efficiency by heightening security on loosely connected devices and transforming how they manage and safeguard endpoints, achieving both security and convenience.

Every endpoint should have a unique, never-before-used password. Even without a skeleton key for endpoints, admins can simply authenticate to any endpoint.

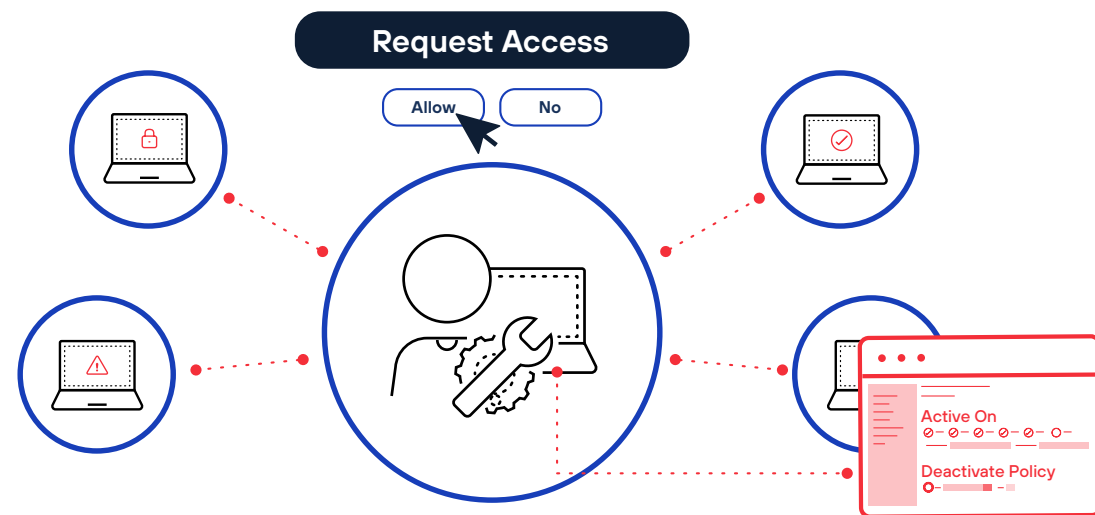


### 3. Least Privilege Enforcement

Endpoint privilege managers grant end users the minimum set of privileges they need to perform a task, called the principle of least privilege. By removing local admin rights from standard user accounts and elevating user privileges only when required, EPMs reduce endpoint security vulnerabilities and prevent ransomware and other threats.

Most EPMs also support just-in-time (JIT) privilege elevation, escalating privileges for a prescribed length of time to allow end users to install applications or reconfigure endpoint settings. Best-in-class solutions support automated workflows that enable on-demand privilege elevation without impairing the user experience or burdening support teams.

Leading solutions also provide APIs to integrate permission request and approval processes into help desk workflows or other IT operations systems. Ideally, AI-driven policy suggestions that are customized to the needs of your environment can help you refine your least privilege settings and achieve the best user experience with the most risk reduction.



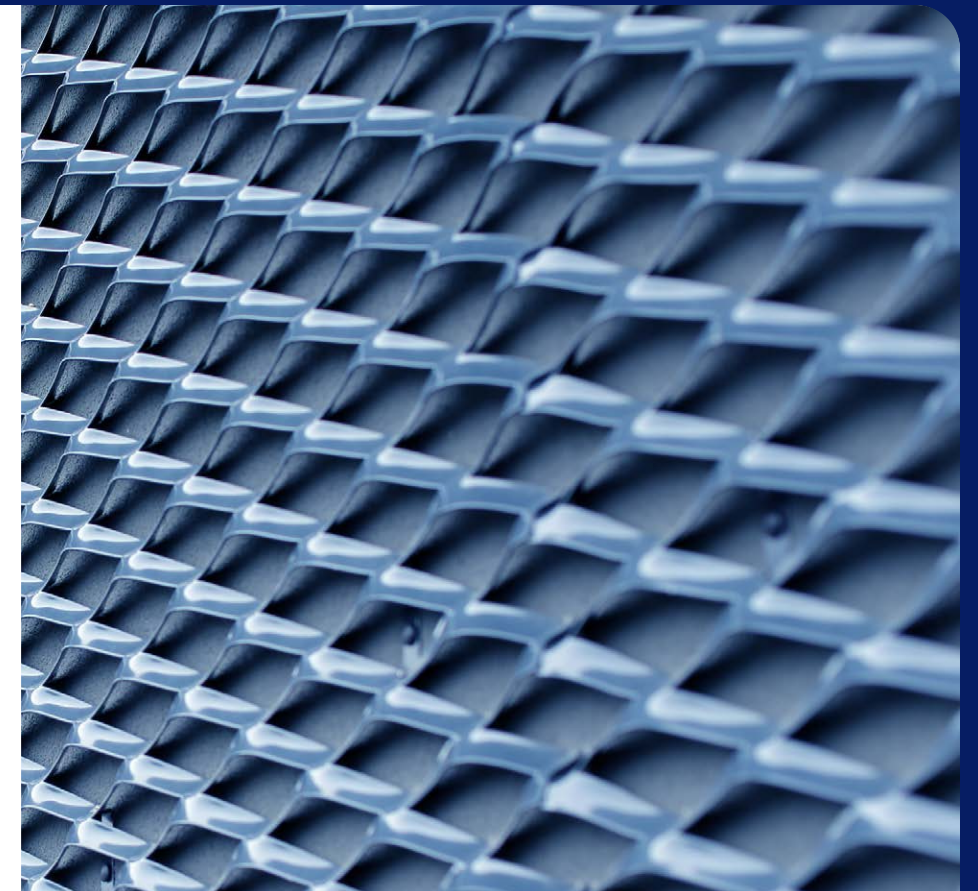
## 4. Managing Endpoint Privileges Is Foundational

Endpoint security should begin with privilege management. Most adversaries exploit privileged accounts to orchestrate attacks. A solution that manages your endpoints is central to the endpoint security stack and underpins other endpoint threat detection and mitigation tools.

Endpoint detection and response (EDR) solutions and other endpoint security products identify and block malware and other threats, but they aren't designed to prevent privilege abuse. Attackers are always switching up their approach and finding ways to turn off or bypass EDR/XDR by abusing administrative credentials. This practice has prompted more underwriting scru-

tiny around endpoint privilege controls, particularly the need for companies to strip local admin rights from everyone, including high-level system administrators, developers, and users of older software that demands admin privileges.

EPM tools are specifically designed to lock down privileged accounts and tightly control the applications privileged accounts can run and the resources they can access. These solutions serve as the first and most important line of endpoint defense, stopping attackers at their point of entry and working in concert with other endpoint security products to block, contain, and remediate threats.



### Identity Security on the Endpoint



## 5. Conditional Application Control and Ringfencing

Most endpoint privilege management tools let you denylist applications to prevent known malware from running or allowlist applications to allow only trusted applications to run.

Deny listing helps detect and block previously identified malware samples, but it's not effective at defending against modern and continuously evolving threats like ransomware. Every day, cybercriminals introduce thousands of new ransomware variants into the wild, and each threat can be packaged and repackaged to avoid list-based detections.

Allowlisting and denylisting can also be quite challenging to implement and maintain because business software continually evolves. Leading endpoint privilege management solutions let you keep pace with change by controlling execution permissions based on various parameters such as file attributes, digital signature, location, source, update server, or reference image. For example, admins can set them to only allow an application that's delivered by designated trusted updater programs.

Best-in-class EPM products enable admins to implement conditional policies so they block attacks that involve trusted applications. For example, they can create a rule allowing users to launch PowerShell with certain parameters, but then create another rule that prevents other apps from launching PowerShell as a child process, eliminating chained exploit techniques.

Leading endpoint privilege management technologies support application graylisting to help you defend against unknown malware variants without impeding the operation of unknown applications that pose no known security risks. Graylist policies apply to applications that aren't explicitly allowlisted or denylisted. Leading solutions include prebuilt policies that provide out-of-the-gate protection against ransomware and other advanced threats.

### Restriction X

Restrict access to selected sensitive resources by unhandled applications downloaded from the internet.

Important: Access must be restricted to at least one of the following resources:

- Internet ⓘ
- Intranet ⓘ
- Network shares ⓘ
- Memory of other processes (Windows only) ⓘ

Notify end users when an unauthorized access attempt occurs.

Dialog



Restricted Access



Preview

## 6. End-to-End Continuous Identity Security

Authentication and authorization are akin to swiping your company badge as you enter your workplace. While you have access to enter, you might not be free to open every door. You might need to reauthenticate before entering another department, such as HR, accounting, the data center, or the warehouse.

If you step away from your desk without locking your laptop, another colleague can sneak in and gain access to restricted software on your unattended laptop by using your still-open session. The moment they try to execute a command that requires elevated privileges, the endpoint privilege management tool intervenes. An authentication prompt appears, requiring additional verification before proceeding. Because your organization has strong MFA prompts in place, your colleague is unable to continue.

In a layered security approach, endpoint privilege sign-in validations work hand in hand with an identity provider. They provide continuous risk assessment and dynamic security based on the context of user actions, helping ensure that your credentials aren't misused.

## 7. Administrative Reports and Dashboards

Most endpoint privilege management solutions provide monitoring and reporting capabilities to track the behavior of users and applications, help administrators improve visibility, and support compliance audits and forensics investigations. Most solutions offer administrators canned reports indicating which endpoints and applications are protected and the specific policies and business rules enforced. Some also offer historical reports to help administrators track the status of endpoint privilege management deployments and coverage, and demonstrate progress to executives and compliance auditors.

Many solutions also include privileged management, application activity, and threat intelligence reports to help information security teams keep tabs on suspicious behavior and simplify compliance. EPM solutions should generate detailed event messages whenever a policy is invoked and include dashboards and tools for observing and exploring policy-use events and statistics—called a policy audit.



## 8. AD Bridging: Modernize Linux Identity and Access Management

Many organizations struggle with identity sprawl on Linux systems, where scattered local accounts create security gaps and administrative burdens. A modern EPM solution addresses these challenges by integrating Linux machines with a centralized directory or cloud identity provider (IdP). This solution eliminates the need for siloed local accounts, enabling users to log in with their existing corporate credentials across the entire fleet.

By centralizing authentication, organizations can enforce consistent security policies across on-premises and multicloud environments. This approach supports modern, phishing-resistant MFA and passwordless options, significantly hardening the security posture compared to legacy local management. Centralization also simplifies audit and compliance by tying all system actions to a single, verifiable identity, providing the flexibility to modernize IAM strategies without being locked into specific legacy directory vendors.

## 9. Extend Your XDR and NetSec with Identity-Based Endpoint Enforcement

Modern endpoint privilege management must act as a primary enforcement engine that translates identity policy into operational reality. By integrating your solution with the broader SOC, network security, and IAM stacks, you gain identity-in-action telemetry. This level of telemetry provides security analysts with the specific identity context behind every elevation or blocked action, streamlining investigations and ensuring maximum architectural synergy.

By adopting this type of integration, security teams can disrupt attack chains with minimal productivity impact. It solves the classic SOC dilemma of choosing between full machine isolation and leaving an endpoint uncontained. Instead of disconnecting a user, XDR playbooks can trigger policies to dynamically increase restrictions and reverify identities. This surgical containment prevents lateral movement and ransomware execution while allowing the employee to continue working securely, effectively bridging the gap between identity state and endpoint enforcement.

Ransomware attacks typically begin by targeting endpoints, like Windows PCs and Macs, by using phishing schemes, malware downloaders, stolen credentials, or known vulnerabilities to penetrate systems. Once an attacker gains access to an endpoint, they can traverse the network, using elevated privileges to spread malware and encrypt files on high-value targets like Windows servers and Linux servers.

Endpoint privilege management solutions provide foundational endpoint security controls that are fundamental for preventing ransomware. When deployed as part of a comprehensive endpoint security strategy, the right EPM product can restrict endpoint privileges on both desktops and servers. It can also defend against identity compromise and contain vertical and lateral movement, stopping ransomware in its tracks before it spreads across your organization.

**\$1.5 million**  
the amount  
the median  
initial ransom  
demand  
jumped to in  
2025.<sup>5</sup>

5. Palo Alto Networks, *Global Incident Response Report*.

# Endpoint Privilege Management Tool Checklist

When evaluating an endpoint privilege management product, look for a solution that has the following capabilities:

- ☑ **Removes local admin rights** on Linux servers, macOS, Windows workstations, and Windows servers to defend against ransomware and vulnerability exploitation.
- ☑ **Supports JIT privilege elevation** for a prescribed length of time so users can update software, make configuration changes, or perform other actions requiring administrative privileges.
- ☑ **Automates privilege elevation requests** to improve the user experience and reduce helpdesk burdens.
- ☑ **Provides agentic AI security** with intelligent privilege controls, ringfencing, and application inventory to provide visibility and enforce security policies across AI agents, MCP servers, and AI skills.
- ☑ **Integrates with IdPs** to provide desktop sign-in and continuous strong authentication with a variety of MFA options, including passwordless, and to support step-up and over-the-shoulder authentication for high-risk actions.
- ☑ **Tightly controls application permissions and actions** based on context to limit areas of attack and prevent software abuse.
- ☑ **Comes with predefined policies** to simplify deployment and accelerate time to value.
- ☑ **Includes administrative reports and dashboards** to improve visibility and streamline compliance and forensics.
- ☑ **Provides AD bridging** for centralized identity management for Linux endpoints, eliminating local accounts and enabling modern MFA and passwordless authentication through integration with a corporate directory or IdP.
- ☑ **Acts as an identity- and privilege-based enforcement engine** for XDR and network security solutions.
- ☑ **Assists with deployment, initial configuration, and administration** in refining your least privilege settings. It should include default policies, rapid risk reduction, least privilege frameworks, and AI-driven policy suggestions customized to your organization's specific environment.



# Secure Access and Privilege at the Endpoint

Endpoint privilege management supports multiple teams across the organization, with benefits that map to security, operations, end-user productivity, and compliance.



## Identity and Access Management

- Extend identity security and zero trust to your workstations and servers.
- Discover and remove local admin rights and enforce role-based least privilege.
- Detect identity-based threats targeting your endpoints.
- Gain better visibility into credential-based attack paths, credential misuse, and risky exposures.



## Endpoint and Server or Infrastructure Security

- Defend against ransomware, prevent credential theft, and protect browser memory.
- Control applications and processes to stop insider threats.
- Detect and prevent lateral movement and contain attacks.



## End-User Computing

- Deliver increased operational efficiency and improved user experience.
- Enable dynamic environments, such as developers' machines.
- Reduce security event noise.
- Reduce incidents requiring IT intervention and response.
- Reduce the potential for server downtime and service disruption.
- Improve visibility.



## Compliance and Certification

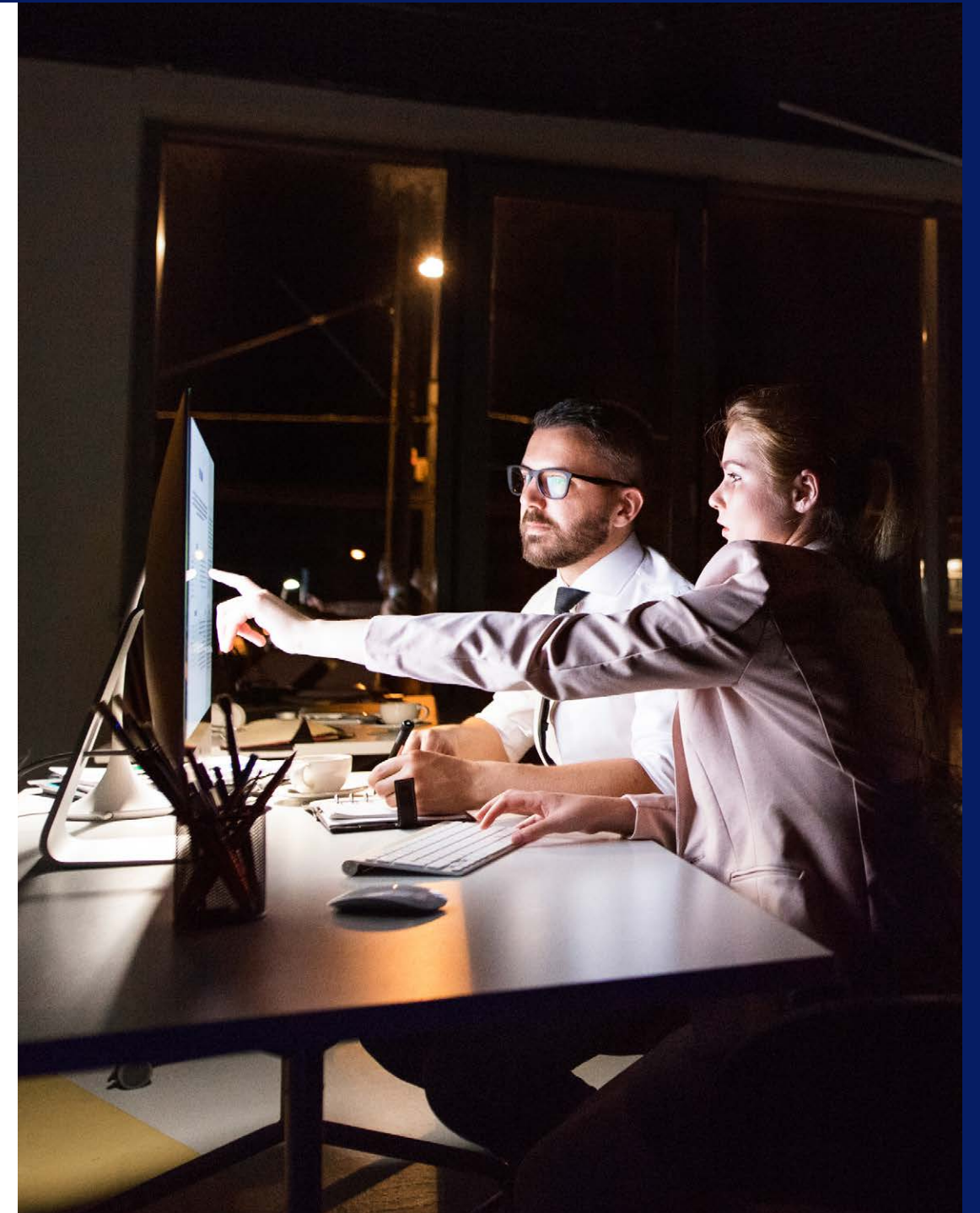
- Improve visibility and implementation of foundational endpoint security controls required by regulations and auditors.
- Enable the ability to demonstrate compliance at any time.
- Reduce cyber insurance costs.

# Benefits of Modern Endpoint Privilege Management Solutions

Endpoint privilege management products centered on a proactive zero trust stance are the cornerstone of the modern endpoint security stack and are fundamental for protecting against ransomware and advanced threats. These solutions offer several advantages:

- **Remove local admin rights** while protecting the user experience and keeping work moving.
- **Defend against attack threats** that target and originate on endpoints.
- **Drive operational efficiencies** by hardening endpoints while ensuring workforce productivity.
- **Enable the digital business** by allowing more user independence and maintaining security.
- **Satisfy audit and compliance requirements** by making it easy to enforce and demonstrate policies.

Endpoint privilege management tools can help you strengthen security, reduce risk, and improve user experience by giving the right people and applications the right access to the right resources at the right time.



# Take the Next Step Toward Managing Endpoint Privilege

A single vulnerability—unmanaged administrative rights on the endpoint—often drives cybersecurity failure. Idira™ Endpoint Privilege Manager, by Palo Alto Networks, neutralizes this risk by removing permanent administrator status from all users across Linux, macOS, and Windows.

By replacing standing privileges with a modern, automated, policy-based elevation model, Idira Endpoint Privilege Manager stops attackers at the source from using compromised accounts to move laterally or disable defenses. Idira further simplifies operations by integrating Linux systems into your central directory, removing the security risk of scattered local accounts.

See how Idira Endpoint Privilege Manager can solve your organization's endpoint privilege challenges. [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<sup>®</sup> 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](https://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](https://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\_cb\_buyers-guide-to-managing-endpoint-privileges\_042126