

Local Admin Rights: Securing Your Biggest Cyber Vulnerability

Eliminating Local Admin Rights to Reduce the Endpoint
Attack Surface and Prevent Zero-Day Attacks

Why Users Shouldn't Have Local Admin Rights

Local administrator rights grant users unrestricted control over their systems. With these privileges, users can install software, modify system settings, disable security controls and access sensitive data. While administrative access might seem necessary for productivity, it remains one of the most widely exploited attack vectors in the modern cyberthreat landscape.

Threat actors exploit local admin rights to disable reactive endpoint security tools, like endpoint detection and response (EDR), install malware, move laterally across networks, and establish persistent backdoors, putting the entire organization at risk. From ransomware campaigns and credential theft to zero-day attacks, adversaries actively target organizations that fail to reduce the endpoint attack surface and prevent zero-day attacks by extending zero trust and identity security to the endpoint with intelligent privilege controls.

Building on previous additions, CISA and international partners continue to expand the Known Exploited Vulnerabilities (KEV) Catalog and Secure by Design blueprints, highlighting the sprawl of defects that enables privilege escalation. *Unit 42 Global Incident Response Report 2026* underscores the fact that the window for containing such threats has shrunk to minutes, marking identity-based privilege escalation as the most critical path for modern, automated threat actors.¹

Yet, many organizations continue to grant users, including IT admins, help desk teams, backup operators, and database admins, excessive privileges under the assumption that they are necessary to perform everyday tasks. While these users require some level of privilege to perform their jobs, they don't need full local admin rights. No user should be a local admin.

This whitepaper highlights:

- The importance of removing local admin rights to reduce the endpoint attack surface and prevent zero-day attacks.
- A strategic approach to eliminating local admin rights while balancing enterprise security and user productivity.
- How Idira™ Endpoint Privilege Manager, by Palo Alto Networks, can help extend identity security and zero trust to endpoints.

While users require some level of privilege to perform their jobs, they don't need full local admin rights. No user should be a local admin.

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

Powerful, Yet, Local Admin Rights

While local admin rights can support a multitude of IT operations, they also introduce significant security risks when misused or exploited. If a threat actor gains access to local admin rights, they can take full control of a system, move laterally across networks, and launch devastating cyberattacks.

Once inside, an attacker impersonating a local admin can perform a multitude of malicious activities.

Malicious Activity	Description
Accessing and manipulating system memory Analyze, modify, or dump memory contents to extract sensitive information, including passwords and encryption keys.	Amplify impact through system manipulation Modify configurations to disable shadow copies, encrypt MBRs, and destroy data or hardware, maximizing the overall operational disruption.
Disabling security controls Bypass or disable user access control (UAC), endpoint security tools like endpoint detection and response (EDR), endpoint protection platform (EPP), and next-gen antivirus (NGAV).	Installing and executing any software Deploy admin tools and malware, create a stealthy attacker's toolbox, install cryptominers, and maintain persistent access without triggering antivirus alerts.
Modifying hardware and firmware Downgrade drivers and flash firmware on connected devices (e.g., disable security LEDs on cameras or load modified firmware onto a PLC). Also, manipulate access supervisory control and data acquisition (SCADA) control panels to disrupt operations.	Hijacking network configurations Alter DNS settings, set up malicious trust zones, or reroute traffic, enabling covert exfiltration of sensitive data.
Enable lateral movement and persistence Compromise admin credentials to pivot through the network, gain long-term persistence, and reach restricted resources across the entire enterprise environment.	Exfiltrating sensitive information Copy, encrypt, or transfer confidential files by using stealthy methods, including hardware trackers, hidden tunnels, and airgap jumping techniques.

If a user has full local admin rights, they have too much control over your organization's security. Worse, if an attacker obtains these privileges, no barriers are built in to prevent them from escalating attacks, stealing data, or disrupting operations. Without another layer of security, threat actors can operate undetected until it's too late.

While some attack techniques remain possible without admin rights, implementing identity-first protection and intelligent privilege controls increases the difficulty for attackers. Removing local admin rights and enforcing least privilege at the endpoints create significant friction, forcing adversaries to seek easier targets elsewhere. The fewer privileges they have, the fewer ways they can attack.

Unprivilege the Attacker by Removing Local Admin Privileges

Though removing local admin rights is a well-established security practice among IT and security professionals, implementing it is often easier said than done.

A common concern among IT teams is that, while restricting users to standard rights significantly enhances security, it can also create friction for users. Without admin privileges, employees can struggle to complete routine tasks, leading to productivity issues, increased helpdesk tickets, and resistance to security policies. In many cases, IT teams revert to granting local admin rights to avoid business disruptions and user backlash.

Endpoint Security and User Experience

Organizations can address these challenges with a defense-in-depth endpoint security strategy, fortified with intelligent privilege controls. The right approach both removes local admin rights and ensures that users can perform their tasks seamlessly while maintaining security.

With policy-based privilege elevation, endpoint privilege management solutions enable users to run approved applications or complete necessary tasks without security prompts or IT assistance. When elevated access is required, users can request privileges to access an application temporarily or permanently, or request a full time-boxed audit privileged session. Additionally, by integrating with IT ticketing systems, endpoint privilege management can streamline workflows and enable fast, secure privilege elevations, improving both security and efficiency.

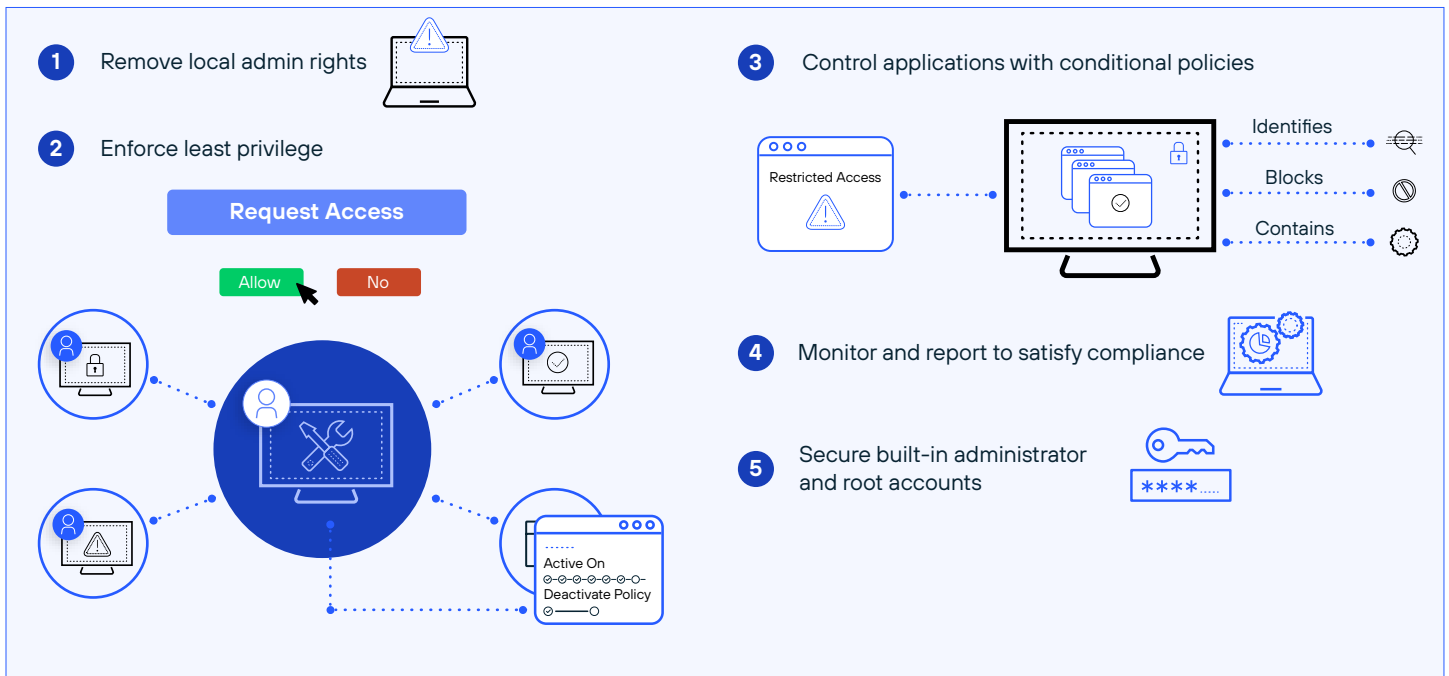
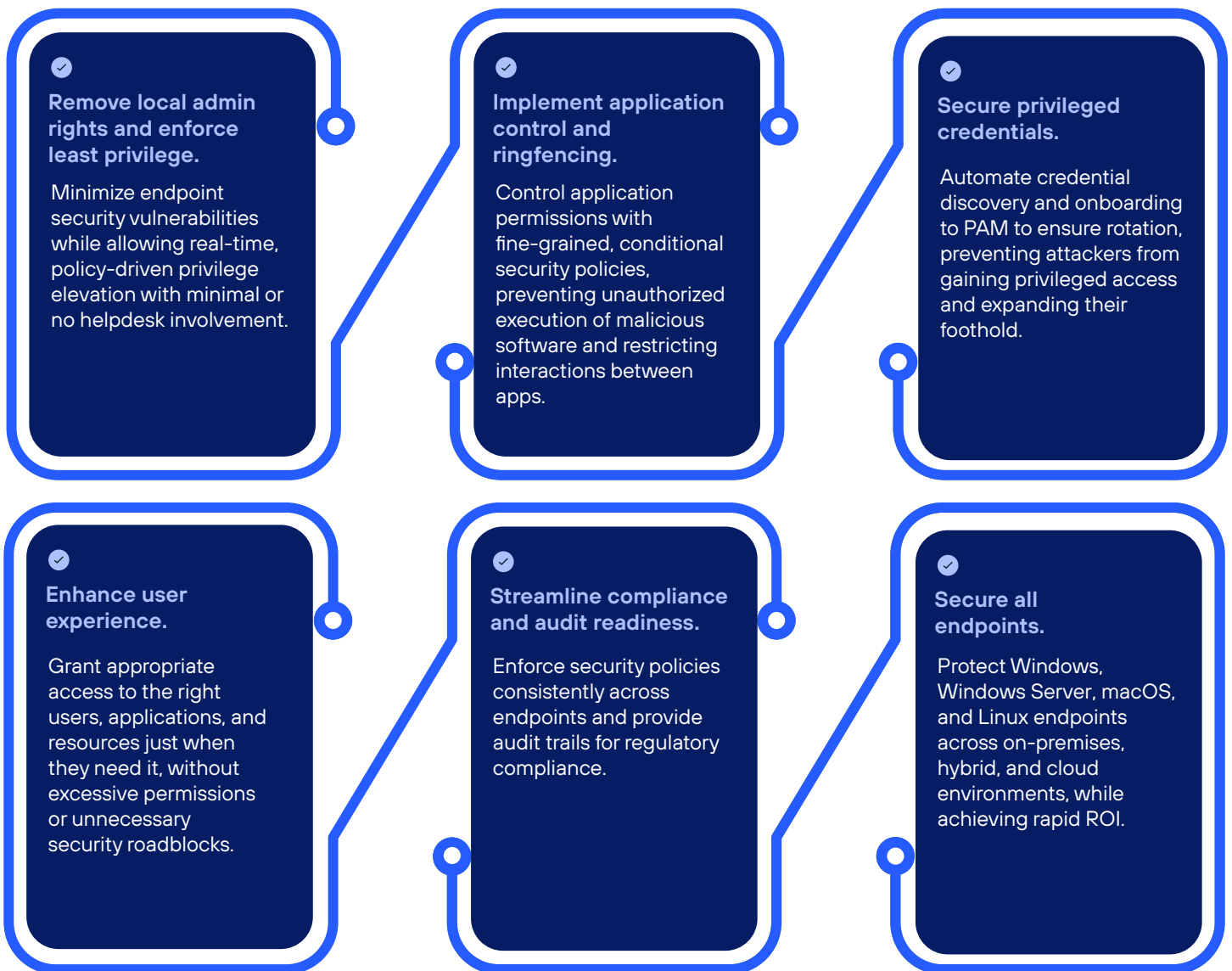


Figure 1. Effective endpoint privilege management is more than removing local admin rights

Key Benefits of a Robust Endpoint Identity Security Solution

A comprehensive endpoint privilege management solution is a cornerstone of modern endpoint security, but not all solutions are created equal. A robust solution enables organizations to:



By adopting a comprehensive identity security strategy on the endpoint, organizations can eliminate local admin rights without sacrificing productivity, ensuring strong security while keeping end users efficient and empowered.

Removing Local Admins with Idira Endpoint Privilege Manager

Defense-in-depth endpoint privilege management removes local admin rights and ensures a seamless user experience, strong security controls, and operational efficiency. Idira Endpoint Privilege Manager is purpose-built to deliver this balance, reducing the endpoint attack surface while safeguarding against emerging threats.

Beyond removing local admin rights, Idira Endpoint Privilege Manager enforces least-privileged access, provides comprehensive application control, protects against credential theft, and enables granular application isolation. With intelligent privilege controls and identity-first protection, it prevents and detects lateral movement, ensuring that endpoint infrastructure remains resilient against advanced threats.

Idira Endpoint Privilege Manager enables organizations to eliminate local admin rights quickly and effectively while maintaining business continuity.

1. Identify and Audit Administrative Users

Run a report on administrative users. Before you make any changes, know which users and groups have administrative access to which applications and systems. Some users might require temporary privilege elevation for specific tasks.

In Idira Endpoint Privilege Manager:

1. Navigate to the **Reports** page.
2. Click **Local Administrative Groups Report**.
3. Select **Users in Local Administrators Group**.
4. Click **Full Report in Excel** to create a backup of the current local administrative users.

2. Enable Program Elevation for a Smooth User Experience

Users and groups often need temporary administrative privileges for certain applications. By configuring policy-based privilege elevation, organizations can prevent security disruptions while ensuring users can perform necessary tasks without IT intervention.

In Idira Endpoint Privilege Manager:

1. Navigate to the **Default Policies** page.
2. On the **Additional** tab, under **Privilege Management**, enable **Elevate Unhandled Applications**.
3. Click **On**, and then select **Edit Policy Settings** to fine-tune the privilege elevation rules.

3. Remove Local Administrator Rights

Removing local admin rights is the most critical step in defending against ransomware risks, preventing lateral movement, and controlling application access to stop insider threats. This proactive approach significantly reduces the endpoint attack surface.

In Idira Endpoint Privilege Manager:

1. Navigate to **Default Policies** page on the console.
2. Find the **Local Privileged Accounts Management** group of policies, select **Remove Local Administrators** policy and click **On** to activate it.

The policy activation removes users and groups from the local administrators group, except for built-in admin users and other specified users or groups defined by the administrator.

Note: **Remove Local Administrators** is a default policy, available out of the box, for Idira Endpoint Privilege Manager. You can either accept the default settings and activate the policy right away or change the settings to define specific targets for the policy.

4. Protect Administrative User Groups from Unauthorized Modifications

This step is important to prevent privilege escalation attempts. It ensures robust protection of administrative user groups from unauthorized modifications—whether by elevated applications started by nonadministrative users or any user or program that attempts to modify admin rights.

In Idira Endpoint Privilege Manager:

1. Within the **Remove Local Administrators** policy settings, configure the protection options.
2. Restrict modifications either from the elevated applications run by nonadmin users or from any user or program.

Zero Trust Security on the Endpoint

By following these steps, you take a proactive and effective approach to securing your endpoints. In just a few clicks, you help to:

- ✓ Significantly reduce the attack surface and minimize cyber risks across your organization.
- ✓ Eliminate the dangers of privilege misuse and exploitation by removing local admin rights.
- ✓ Ensure seamless productivity by enabling policy-based privilege elevation, allowing users to securely access necessary applications without security roadblocks.
- ✓ Reduce IT burden by minimizing helpdesk requests for privilege-related issues, enabling IT teams to focus on strategic initiatives.

With Idira Endpoint Privilege Manager, you can strengthen endpoint security, enhance user experience, and ensure a frictionless security posture—all with just a few clicks.

Conclusion

With Idira Endpoint Privilege Manager, organizations no longer have to choose between security and user experience. Beyond eliminating unnecessary privileges, our solution provides a comprehensive, identity-centric approach to securing endpoints.

Idira Endpoint Privilege Manager helps organizations:

- ✓ Extend identity security and zero trust to endpoints.
- ✓ Reduce the endpoint attack surface and prevent emerging threats.
- ✓ Lower IT security and operational costs with endpoint privilege controls.
- ✓ Demonstrate continuous compliance and meet audit requirements on endpoints.

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.

Next Steps

See for yourself how Idira Endpoint Privilege Manager helps secure endpoints and servers.

[REQUEST A DEMO](#)



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_local-admin-rights-securing-your-biggest_042226