Idira Endpoint Privilege Manager

Zero Trust for the Endpoint by Replacing Standing Privileges with Policy-Based Elevation

The Privilege Gap Dilemma

The modern security perimeter has fundamentally shifted to the point where identity meets the operating system. Identity weaknesses play an end-to-end role in 90% of security incidents, which clearly shows that attackers choose logging in over hacking in.[1] Also, the endpoint attack surface plays a role in 61% of incidents, for which the primary fuel is unmanaged local administrative rights on workstations and servers.[2]

Overpermissioned end users, applications, and now AI agents create a privilege gap that adversaries exploit to disable security tools, harvest credentials, and move laterally. The time from initial compromise to data exfiltration has shrunk to just 72 minutes,[3] making manual security reviews and reactive measures no longer sufficient. Now, the rise of agentic AI introduces a new class of ungoverned privileged identities.

In this atmosphere, organizations face a critical dilemma. They can enforce the principle of least privilege, but doing so traditionally triggers a surge in helpdesk tickets and user friction. Yet, failing to enforce it leaves them vulnerable to rapid, automated exploitation.

Intelligent Privilege Controls for the Endpoint Security

To counter such identity-based threats on the endpoint, organizations must incorporate intelligent privilege controls into their endpoint security stack to bridge the gap between identity and the operating system. The foundational step is systematically removing permanent administrative rights from all users across Linux, macOS, and Windows, effectively neutralizing the primary vector for lateral movement.

Instead of granting standing permissions, this approach pivots to an automated, policy-driven model that elevates only specific, authorized processes rather than the users themselves. This just-in-time (JIT) elevation enables end users' productivity while maintaining the principle of least privilege. To combat the speed of modern attacks, the solution must provide continuous application control and ringfencing, which prevents authorized software from being hijacked to access sensitive files or network resources.

This defense extends to the new frontier of agentic AI, ensuring the agents along with their toolchains and identities operate under the same governance constraints as human users and native software. By unifying these controls within a central identity framework and bridging fragmented environments, organizations achieve comprehensive identity security across their endpoints and servers. This methodology eliminates the traditional friction between security and operations, reducing the attack surface while keeping the users productive.

Security Grounded in Proven Results

Effective endpoint privilege management requires a methodology that works in the real world, not just in theory. Our approach focuses on removing the technical friction of least privilege, providing the control necessary to stop high-speed attacks without impacting user productivity. We also have the credibility to prove it.

- **Critical Capabilities scores:** Received the highest score for the Privileged Elevation and Delegation Management (PEDM) Use Case in the 2025 Gartner® Critical Capabilities for Privileged Access Management report.[4]
- **Industry recognition:** Recognized as a Leader in Gartner® Magic Quadrant™ for Privileged Access Management,[5] and The Forrester® Wave™: Privileged Identity Management.[6]
- **Operational efficiency:** Organizations typically see a 40% drop in helpdesk tickets related to system permissions and software requests.[7]
- **Measurable risk reduction:** Documented results include a 74% reduction in overprivileged accounts and 57% fewer successful account takeover attacks.[8]
- **Blueprint shaped by experience:** Organizations reach a least-privileged state faster by using Idira Blueprint—a roadmap built from thousands of real-world deployments at the world's largest companies.

1–3. *Unit 42 Global Incident Response Report 2026*, Palo Alto Networks, February 17, 2026.

4. *2025 Gartner® Critical Capabilities for Privileged Access Management*, Paul Mezzera, Abhyuday Data, Shubham Gera, and Michael Kelley, Gartner, October 27, 2025.

5. *Magic Quadrant™ for Privileged Access Management*, Abhyuday Data, Paul Mezzera, Shubham Gera, Tarun Rohilla, and Michael Kelley, Gartner, October 13, 2025.

6. *2025 Forrester Wave™: Privileged Identity Management Solutions*, Forrester Research, August 7, 2025.

7–8. *The Business Value of CyberArk Endpoint Privilege Manager*, an IDC report commissioned by CyberArk, a Palo Alto Networks company, September 2025.

How Idira Endpoint Privilege Manager Stops Sophisticated Attacks

Idira™ Endpoint Privilege Manager, by Palo Alto Networks, neutralizes the risk of cybersecurity failure by removing local administrative rights from all users across Linux, macOS, and Windows. By replacing standing permissions with automated, policy-based elevation for specific applications, Idira Endpoint Privilege Manager prevents attackers from using compromised accounts to move laterally or disable defenses. Comprehensive application control and ringfencing, which restrict software activity to only what is necessary for the task, reinforce this approach.

Beyond workstations, Idira Endpoint Privilege Manager simplifies operations by bridging Linux systems with the central directory, eliminating the security risks associated with scattered local accounts. This architectural foundation acts as an automated enforcement engine for extended detection and response (XDR), security orchestration, automation, and response (SOAR), and NetSec solutions. It provides the surgical control required to block unauthorized privilege escalation at the source, ensuring security teams can contain threats before they reach the point of data exfiltration.

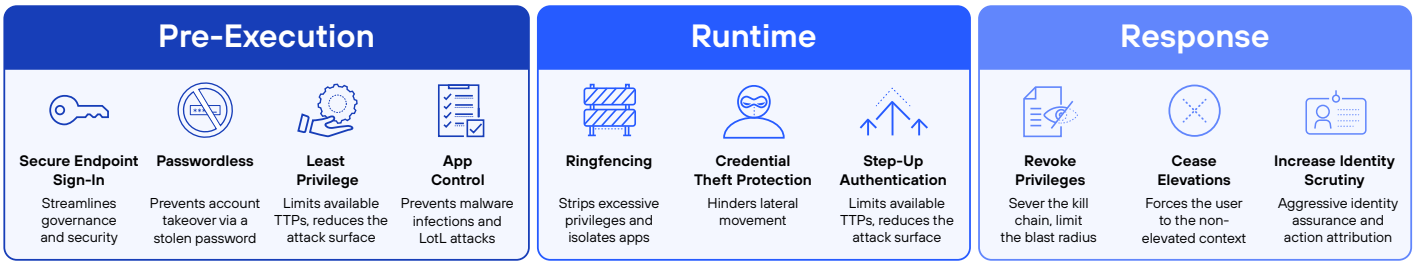

Figure 1. How Idira Endpoint Privilege Manager blocks identity-based attack pathways

Extends Identity Security and Zero Trust to Workstations and Servers

Modern security requires a foundational layer that hardens the operating system where identity meets the asset. Idira Endpoint Privilege Manager extends zero trust and identity security principles to the workstation. Organizations can close the privilege gap—the space between a user's standing permissions and the minimal access required for their role. They neutralize the most common path for initial access—gaining persistence, moving laterally, and delivering impact.

- **Removal of local admin rights:** Establishes a zero standing privilege (ZSP) architecture by revoking permanent administrative power across Linux, macOS, and Windows, neutralizing the primary fuel for lateral movement. This foundational shift contributes to a 50% reduction in the risk of a major security breach.[9]
- **Policy-based elevation for applications:** Maintains productivity by elevating specific, authorized processes rather than user accounts, allowing employees to perform necessary tasks without administrative status.
- **Enforce role-based least privilege:** Secures the last mile of identity by applying granular, context-aware permissions that ensure users and processes possess only the minimum access required for their function. Organizations achieve a 74% reduction in overprivileged accounts through this enforcement.[10]
- **Secure endpoint sign-in against IdP:** Strengthens the initial access point by integrating endpoint login with your primary identity provider, enabling modern phishing-resistant multifactor authentication (MFA) to block credential harvesting.

9–10. IDC, *Business Value Assessment of CyberArk.*

- **End-to-end passwordless experience:** Eliminates the risk of password keylogging by providing users with a seamless, passwordless sign-in and elevation flow across Linux, macOS, and Windows.
- **Step-up authentication for high-risk actions:** Requires a fresh MFA challenge before allowing sensitive operations or policy-based elevations, ensuring that an active session can't be hijacked for unauthorized administrative tasks.

Reduces the Endpoint Attack Surface and Prevents Zero-Day Attacks

True resilience is defined by what happens after a successful login. Idira Endpoint Privilege Manager proactively reduces the attack surface by moving from a reactive detection model to a deny-by-default preventative stance. It ensures that, if an attacker bypasses the initial defenses, they are contained within a restricted environment where they can't escalate privileges or manipulate system resources.

- **Comprehensive application control:** Establishes a hardened environment where only vetted and approved software can execute, effectively blocking unknown malware and unauthorized scripts by using granular application definitions with comprehensive logic and parent and child process control.
- **Ringfencing for applications:** Contains potential exploits by restricting authorized applications from accessing sensitive system files, network locations, or memory of other processes, preventing Living-off-the-Land techniques.
- **Intelligent privilege control for agentic AI:** Governs the emerging class of autonomous identities by applying the same rigorous least privilege frameworks to AI agents and Model Context Protocols (MCPs) on the operating system.

Reduces IT Security and Operational Costs with Endpoint Privilege Controls

A legacy approach to least privilege often collapses under the weight of helpdesk tickets and manual security reviews. Idira Endpoint Privilege Manager uses automation and AI-driven insights to operationalize security at scale, allowing IT and security teams to enforce strict controls without creating friction for the workforce or increasing administrative overhead.

- **Discovery and securing of local privileged accounts:** Automates the identification of dark unmanaged accounts and shadow identities, providing the visibility needed to decommission legacy risks without manual intervention.
- **Granular identity- and privilege-based SOC response:** Enhances XDR and SOAR playbooks with instant attack surface reduction by using privilege restrictions and reauthentication prompts, instead of disruptive full-machine isolation.
- **AI policy recommendations:** Leverages AI to analyze endpoint events and generate prescriptive policy insights, reducing the manual effort required to fine-tune least privilege settings.
- **QuickStart policies:** Accelerate time to value with predefined, expert-vetted templates designed to immediately address high-risk vectors like ransomware and credential theft.

Demonstrates Compliance and Meets Audit Requirements on the Endpoint

Regulatory frameworks and cyber insurance providers increasingly mandate the removal of local administrative rights and the centralization of identity. Idira Endpoint Privilege Manager provides the unified audit trails and standardized controls necessary to satisfy these requirements across heterogeneous environments, including specialized Linux infrastructures.

- **Enforce compliance via least privilege:** Directly satisfies the core Access Control and Least Privilege requirements of NIST SP 800-53, PCI DSS, CIS Controls, HIPAA, and others. Organizations report a 26% gain in compliance team productivity and significantly faster audit preparation.[11]
- **Meet cyber insurance underwriting standards:** Addresses the mandatory security controls required by carriers, including the removal of standing administrative privileges. Implementation can lead to significant operational cost savings, averaging $810,000 annually, while reducing the total cost of security-related downtime by 60%.[12]
- **Active Directory (AD) bridging:** Modernizes Linux IAM by bridging the identity gap. It enables technical users to log in with centralized corporate credentials and ensures all activity is attributed to a single, audited identity.

Modern Architecture to Accelerate Your Security Strategy

Idira Endpoint Privilege Manager is designed to eliminate the traditional trade-off between security posture and operational velocity. Designed for rapid enterprise-scale implementation, Idira Endpoint Privilege Manager replaces manual, error-prone privilege management with an automated, policy-driven engine.

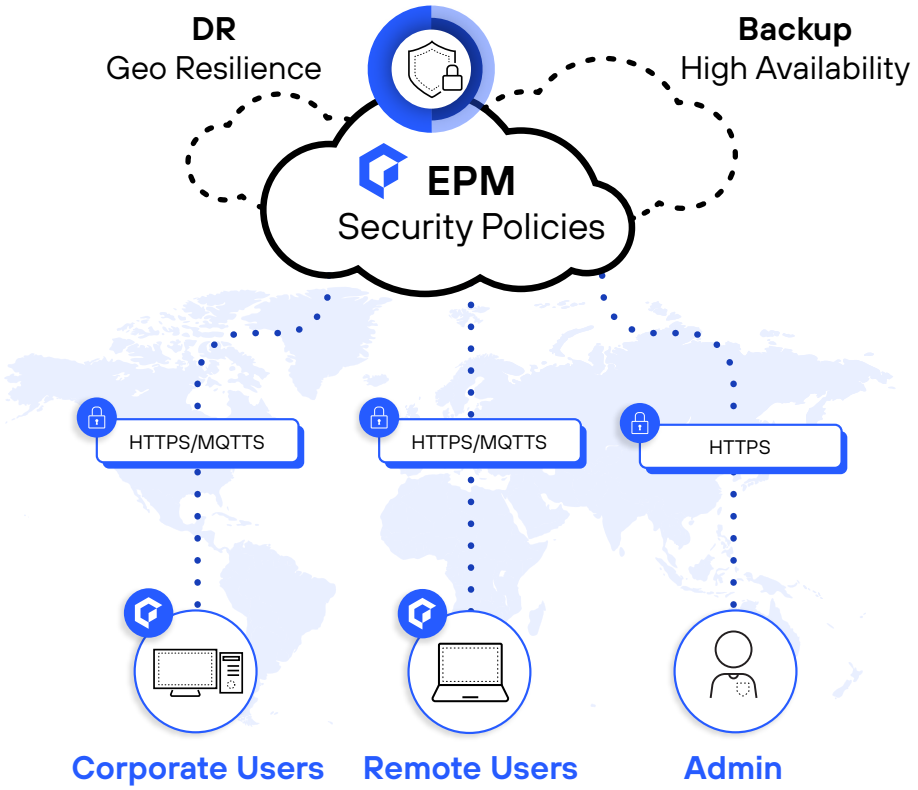

Figure 2. Idira Endpoint Privilege Manager architecture

11–12. IDC, *Business Value Assessment of CyberArk.*

By providing a prevention-first framework that works across Linux, macOS, and Windows, the platform helps achieve ZSP on the endpoint without the typical surge in helpdesk volume. The result is a hardened operating system that serves as a transparent zero trust enforcement point, ensuring that security is a business enabler rather than a productivity hurdle.

- **Accelerate time to value with built-in policies and framework:** The QuickStart framework and one-click default policies streamline the implementation, quickly and safely removing local admin rights and rapidly reducing privilege risk on the endpoint. The policies enable a prescriptive shift toward visibility into privilege events or straight to active enforcement.
- **Continuous automation and remediation:** Seamless integration with Idira Privilege Cloud enables automatic discovery and onboarding of privileged accounts, coupled with built-in account security thanks to automatic credential rotation.
- **Intelligent management via AI:** AI transforms endpoint privilege events into actionable policy intelligence. The AI policy recommendation engine suggests secure actions for unhandled applications based on community insights.
- **Expertise at scale with Idira Blueprint:** Idira Identity Security Blueprint provides an identity security maturity roadmap distilled from thousands of global deployments. This repeatable methodology scales across Linux, macOS, and Windows endpoints and server infrastructures to quickly get results and avoid common pitfalls.

Beyond the Endpoint: Idira Identity Security Platform

While Idira Endpoint Privilege Manager provides the foundational resilience required at the asset level, true defense-in-depth requires securing the entire identity journey. As part of the Idira platform, Idira Endpoint Privilege Manager contributes to a unified, next-generation identity security operating model that converges identity and access management (IAM), privileged access management (PAM), and identity governance and administration (IGA). This architectural shift eliminates the dangerous seams between disconnected tools that attackers exploit to move from a standard user account to a production cloud environment.

Idira establishes a single privilege model and policy engine that governs every human identity from the first authentication to the last privileged action. By combining phishing-resistant passwordless access with ZSP across the estate, organizations close the uncontrolled privilege gap. This unified approach ensures that every identity, whether an employee, contractor, or developer, is continuously discovered, controlled, and governed through a single, audited control plane.

Explore all the ways Idira can secure the identities across your organization. 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.

paloalto NETWORKS

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

idira_ds_endpoint-privilege-manager_043026