

Intelligent Privilege Controls on the Endpoint

Secure Every Human Identity to Close the Privilege Gap

The traditional boundary between privileged and standard identities has collapsed. In modern enterprise environments, every human identity, from the marketing specialist to the software engineer, carries risk that's proportional to the targets they reach and the actions they perform. As organizations transition toward a unified identity security operating model, the endpoint has emerged as the most critical junction of this defense.

Idira™ Endpoint Privilege Manager, by Palo Alto Networks, represents a fundamental shift from tactical threat detection to structural prevention. By treating the workstation as the last mile of identity security, Idira Endpoint Privilege Manager hardens the operating system and enforces zero trust at the source.

Discover how intelligent privilege controls on the endpoint close the uncontrolled privilege gap and provide the high-fidelity telemetry required for a resilient identity security posture.

Identity Crisis at the Edge

Identity weaknesses play a role in 89% of all security investigations.¹ Attackers no longer focus on breaking into infrastructure directly. They log in using compromised credentials and exploit unmanaged local administrative rights to move laterally.

The mandate for security leaders is clear. The window for response is shrinking. Attacker speed has accelerated to the point where data exfiltration can occur in just 72 minutes.² Relying on detection-based tools alone is insufficient when the adversary operates at machine speed. Organizations must implement automated, system-level controls that block unauthorized actions the moment they are attempted.

The OS as the Zero Trust Enforcement Engine

The endpoint is where identity meets the asset. When a workstation operates with standing administrative privileges, it provides a permanent foothold for credential harvesting and lateral movement. Idira Endpoint Privilege Manager replaces this legacy risk with a model of zero standing privilege (ZSP).

From Detection to OS-Level Prevention

While endpoint detection and response (EDR) solutions focus on identifying malicious behavior after it begins, the endpoint privilege management capabilities of the Idira platform provide a foundational prevention layer. By removing local administrator rights across Windows, macOS, and Linux, Idira Endpoint Privilege Manager neutralizes the fuel for modern attacks.

When a specific task requires elevation, the decision is made automatically based on predefined security policies. It ensures that users remain standard users at all times, with elevated permissions granted only for authorized applications and only for the duration of the task.

Identity-in-Action Telemetry

Beyond simple blocking, Idira Endpoint Privilege Manager provides high-fidelity Identity-in-Action Telemetry. This data enables security teams to differentiate between a legitimate employee performing a sensitive task and an attacker attempting to escalate privileges. The shared visibility within the Idira platform enables the entire security stack to respond to threats with greater accuracy and speed.

Extending Privilege Controls to Every Human Identity

Historically, enterprise-grade privilege controls were reserved for a small group of IT administrators. Today, we must recognize the democratization of privilege. A finance manager with access to payment systems or a developer with access to production pipelines is a privileged identity.

Application Ringfencing

Even authorized applications can be hijacked. Idira Endpoint Privilege Manager uses application ringfencing to restrict a trusted application's ability to reach out and touch sensitive files or network locations that it does not need. It prevents living-off-the-land techniques where attackers use legitimate tools to perform malicious actions.

Proof Point: The 72-Minute Mandate

In 2025, our Unit 42® team found that the time from initial compromise to exfiltration dropped to 72 minutes, making automated, policy-based prevention at the OS level a nonnegotiable requirement for structural resilience.

1-2. *Unit 42 Global Incident Response Report 2026*, Palo Alto Networks, February 17, 2026.

Bridging the Identity Gap for Linux

Linux security has traditionally been managed in a silo, often relying on unmanaged local accounts. Idira Endpoint Privilege Manager bridges this identity gap by connecting Linux machines directly to the central enterprise directory. It enables technical users to follow the same identity security standards as the rest of the workforce, eliminating the risk of scattered, unmanaged local identities.

Securing the Agentic Workforce

As automated AI agents and Model Context Protocols (MCPs) begin to perform tasks on enterprise systems, they represent a new class of privileged identity. The Idira platform treats these autonomous agents with the same rigor as human employees. Idira Endpoint Privilege Manager applies the same privilege frameworks to these agents, preventing automated privilege abuse and ensuring that agentic AI operates within governed policy bounds.

Operational Excellence with Security as a Productivity Driver

A primary objection to removing administrative rights has always been the impact on end-user productivity. Idira Endpoint Privilege Manager capabilities eliminate this friction.

Reduced IT Friction

By automatically allowing known-good applications to run with the privileges they need, Idira Endpoint Privilege Manager keeps the workforce productive without IT intervention. Organizations that implement it typically see a 40% reduction in helpdesk tickets related to software permissions.

Transparent Enforcement

Security measures are most effective when they are transparent. Idira Endpoint Privilege Manager provides a seamless user experience where policy-based elevation occurs in the background. The end user remains focused on their work, while the organization maintains a posture of continuous identity assurance.

The Path Forward

Identity is the last standing perimeter. Securing every human identity requires a unified platform that sees the full picture from the first authentication to the last privileged action. By anchoring the Idira platform at the endpoint, organizations can enforce zero trust, eliminate the credential attack surface, and build a foundation of structural resilience.

The workstation is the last mile. When you secure it, you secure the enterprise.

To explore all the ways Idira can secure the identities across your organization, visit www.paloaltonetworks.com/idora.

Strategic Interlock: Platform Synergy

Idira Endpoint Privilege Manager is not a standalone tool. As part of the Idira Identity Security platform, it aligns with the Discover, Control, Govern framework. Discovery identifies the privilege gap, Control enforces least privilege, and Governance provides the immutable audit trails required for compliance.



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.

idora_wp_intelligent-privilege-controls_041426