



Extending Zero Trust and Identity Security to Workstations and Servers

Enterprise endpoint devices, including workstations and servers, are where identities interact with critical resources. However, as IT infrastructure has evolved, foundational security practices focused on identity, least privilege, credential defense, browser security and password management have largely ignored the endpoint attack vector, leaving users vulnerable to endpoint attack and compromise.

This paper looks at strategies for layering security-first access management, intelligent privilege controls, and flexible identity governance and administration controls for servers and workstations that can help secure all human identities on the endpoints, and avoid advance persistent threats (APTs) and other increasingly sophisticated attacks caused by the lack of identity-first protection for these critical resources.

The evolving endpoint threat landscape

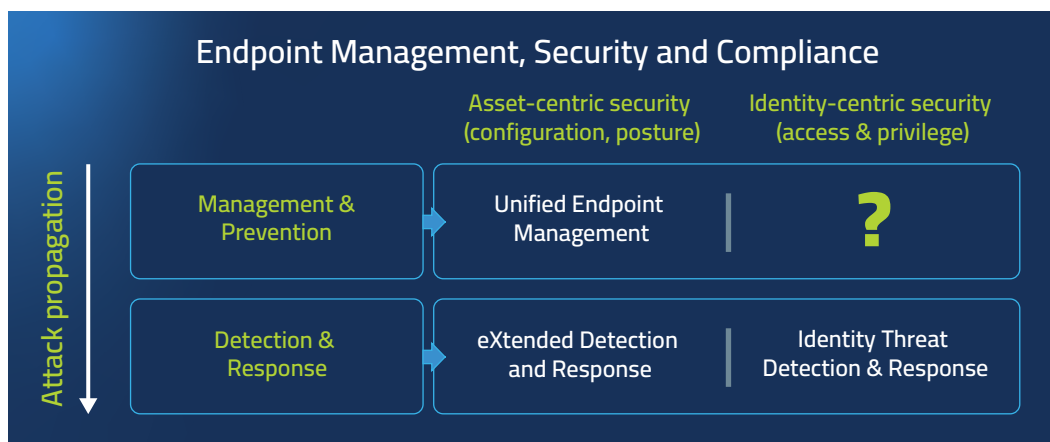
A recent survey of security leaders found that 9 out of 10 organizations faced a successful identity-related breach in the last year¹. However, despite the near ubiquity of these threats, human identities are expected to grow by 56%, and an alarming 96% of them hold excessive access beyond what their roles require². Organizations are also expanding exposure by adopting AI agents; these are projected to increase by 85%, with 40% already having access to organizational data³. Ransomware remains a dominant threat, with encryption occurring in 78% of extortion cases⁴. Disturbingly, when victims pay, attackers provide proof of data deletion only 58% of the time.⁵

In fact, foundational, identity-based endpoint security is very often ignored, and administrative rights are given freely with little regard to possible negative impacts down the line. As a result, the new network perimeter is the entirety of the internet. Bad actors can access critical endpoints from virtually anywhere at any time.

Looking for the “silver bullet”

Many organizations purchase security offerings to prevent breaches without first having a foundation of security in place to build upon. As a result, best practices typically applied to user security such as identity and privilege management are largely ignored when planning endpoint security. The results are often disastrous.

Security professionals are now recognizing that endpoint detection and response and extended detection and response tools are great at finding threats but fall far short of the mark in reducing the attack surface.



The “silver bullet” that IT is looking for doesn’t exist—endpoint security demands a back-to-basics plan for foundational security that includes layered defenses, and that takes an identity-first approach to security with intelligent privilege controls.

¹ [2026 Identity Security Landscape](#), Palo Alto Networks, May 11, 2026.

² Palo Alto Networks, [2026 Identity Security Landscape](#).

³ Palo Alto Networks, [2026 Identity Security Landscape](#).

⁴ [Unit 4.2 Global Incident Response Report 2026](#), Palo Alto Networks, February 17, 2026.

⁵ Palo Alto Networks, [Global Incident Response Report 2026](#).



The stakes are high for endpoints

The lack of a strong endpoint security plan can lead to credential compromises, enabling future attacks that can undermine other security defenses.

Undetected APTs rely on the following:

- Credential theft.
- Lateral movement.
- Ability to arbitrarily execute malicious code on endpoints.
- Innocent or malicious actions by insiders to be able to deploy and detonate their payloads on servers and workstations.
- Impact amplification through extended attacker's reach and tampering with security measures

To be truly safe from these attacks, enterprises must take a proactive approach rather than the reactive stance typical of security and IT professionals in years past.

The case for zero-trust endpoint privilege management

Zero-trust principles have been gaining broad acceptance for user identities and are being widely applied, especially for cloud infrastructure. However, endpoints—servers and workstations—are where the rubber meets the road for security. Endpoints are the intersection between critical resources and identity.

By extending zero trust to endpoints, enterprises can gain many benefits:

- Discover and remove local administrative rights to help enforce a role-based least-privilege approach.
- Detect those identity-based threats that are targeting endpoints.
- Reduce the endpoint attack surface and prevent zero-day attacks while slashing IT security and operational costs
- Accelerate the organization's strategic cybersecurity initiatives.

What security professionals want for endpoints

Those professionals responsible for endpoint security who manage to stay ahead of the curve and maintain a successful endpoint security program have a laundry list of must-have security capabilities to elevate endpoint security, including the following:

- A security-first access management program that includes a passwordless experience for both login and elevation on the endpoint.
- Strong continuous end user authentication and secure device sign-in.
- Reauthentication on initiation of high-risk actions.
- Intelligent privilege controls that elevate privilege based on policy and only for a short duration.
- Comprehensive application control to ensure rogue applications are not executing on endpoints and servers.
- Integration with SOC tools to act as an identity- and privilege-based enforcement engine to allow for faster and more secure response
- Detection of and protection from living-off-the-land attacks that target native, legitimate binaries.

To achieve this, zero trust and identity security approaches must converge to provide a comprehensive endpoint defense because human identity is essentially the new perimeter.

The Palo Alto Networks Idira difference

Applying the right level of privilege controls across all users and their endpoints enables organizations to meet today's—and tomorrow's—security challenges. The Palo Alto Networks approach leans on the strength of the Idira Identity Security Platform. This unique approach recognizes that every identity can become privileged under certain circumstances. While tools such as MFA are usually difficult to deploy on endpoints, Idira Endpoint Privilege Manager offers the broadest range of security controls for continuous user authentication and authorizations to reduce risk on endpoints while delivering a high-quality end-user experience.

Applying the right level of privilege controls across all users and their endpoints enables organizations to meet today's—and tomorrow's—security challenges.

Idira Endpoint Privilege Manager is an integral part of Idira Identity Security Platform which secures all identities with the correct level of privilege controls and appropriate types of access to enable the enterprise to stay a step ahead of attackers. This unified platform enables organizations using Idira to discover identities across their infrastructure, apply security-first access management capabilities and the right level of privilege controls for each of their secured identity groups.

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.