

---

# Nine Best Practices for Workstation Protection

A Strategic Framework for Identity-Centric Endpoint Defense



# The Architecture of Resilience

The security perimeter has fundamentally shifted. It no longer resides at the network edge but at the point where identity meets the operating system. While traditional security measures focus on the point of entry, what happens after a successful login defines true resilience.

Modern defense requires a foundational layer that hardens the operating system itself. By extending zero trust principles to the workstation, organizations can close the privilege gap. This gap is the space between the permissions a user possesses and the minimal access they require for productivity.

A unified approach to identity and access management (IAM) is critical to this mission. By centralizing accounts and enabling a seamless, passwordless experience, organizations can effectively disable an attacker's ability to compromise credentials, establish persistence, or move laterally. When combined with transparent, policy-based elevations, this model ensures that security does not become a hurdle for the end user. This e-book outlines nine essential practices to secure the workstation—the last mile of identity.

---

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

While traditional security measures focus on the point of entry, what happens after a successful login defines true resilience.

## The 72-Minute Mandate

Unit 42® reports that the time from initial compromise to data exfiltration has shrunk to 72 minutes. At this velocity, security must be built into the architecture and not rely on manual detection.<sup>1</sup>

# Practice 1: Discover and Secure Privileged Accounts

Visibility is the prerequisite for any zero trust implementation. Most enterprises operate with a dark layer of unmanaged local accounts. These might be legacy administrator accounts, service accounts with forgotten credentials, or ad hoc support identities created during troubleshooting.

## Best Practice

Establish a continuous, automated discovery process to inventory every account with administrative permissions across Linux, macOS, and Windows. This inventory includes built-in identities and accounts that are manually added to local groups.

## Benefit

By identifying and securing these shadow admin accounts, you eliminate the ungoverned footholds that attackers use to bypass central security policies. This discovery phase provides the data necessary to map attack paths and inform a transition to a standard user model without disrupting business continuity.

2. Palo Alto Networks, *Unit 42 Global Incident Response*.

# Practice 2: Remove Local Admin Rights

Local administrative rights are the primary fuel for cyberattacks. They provide the necessary permissions for an attacker to disable endpoint detection and response (EDR) sensors, harvest credentials from memory, and install sophisticated malware. Regardless, nearly 99% of identities in enterprise environments hold more power than they need.<sup>2</sup>

## Best Practice

Commit to the full removal of administrative privileges from every user account. Every employee, from the executive suite to the engineering department, should operate as a standard user by default.

## Benefit

Stripping away administrative rights fundamentally breaks the attacker's attack lifecycle. It prevents the unauthorized modification of system files and registry keys, significantly reducing the success rate of initial exploits. It's the single most effective step an organization can take to harden the workstation operating system.



## Practice 3: Enforce Least Privilege with Policy-Based Elevation

The removal of administrative rights often creates friction between security and IT operations. Users still need to perform legitimate tasks like installing vetted software, updating drivers, or modifying local settings.

### Best Practice

Implement automated, policy-based elevation for applications. Instead of elevating the user's account, the system elevates the specific process being executed.

### Benefit

This practice enables a transparent user experience where legitimate tasks occur without a help desk ticket. By granting privilege to the application rather than the human identity, you maintain a state of zero standing privilege (ZSP). This approach typically results in a 40% reduction in help desk tickets related to permissions.<sup>3</sup>

<sup>3</sup>. Dickson, Frank, and Megan Szurley, *The Business Value of CyberArk Endpoint Privilege Manager*, IDC paper commissioned by CyberArk, September 2025.

## Practice 4: Implement Application Control and Ringfencing

Authorized applications can still be turned against the organization. Attackers frequently use Living-off-the-Land (LotL) techniques, hijacking trusted software like web browsers or PDF readers to execute malicious scripts or communicate with external command-and-control (C2) servers.

### Best Practice

Deploy intelligent application control to prevent unknown or unauthorized software from running. Complement this with application ringfencing, which restricts even authorized software from interacting with sensitive files or network locations that it doesn't strictly need.

### Benefit

Ringfencing creates a containment zone around every application. Even if an attacker exploits a vulnerability in a trusted browser, they are trapped within the fence of that application's legitimate scope, preventing lateral movement or data exfiltration from the local file system.



## Practice 5: Privilege Controls for Agentic AI

As organizations integrate agentic AI (AI agents, Model Context Protocols [MCPs], and autonomous skills) into their workflows, a new class of identity has emerged. These nonhuman agents often require significant permissions to automate tasks, creating a massive new attack surface if left ungoverned.

### Best Practice

Extend endpoint privilege controls to AI agents and the MCPs they use. Apply the same principles of least privilege and ring-fencing to the skills and API calls these agents execute on the workstation.

### Benefit

Providing intelligent visibility into AI-driven activity ensures that an autonomous agent can't be coerced into performing unauthorized administrative actions. This identity-in-action monitoring for AI ensures that the democratization of productivity does not lead to the democratization of risk.

## Practice 6: Modern AD Bridging for Linux Systems

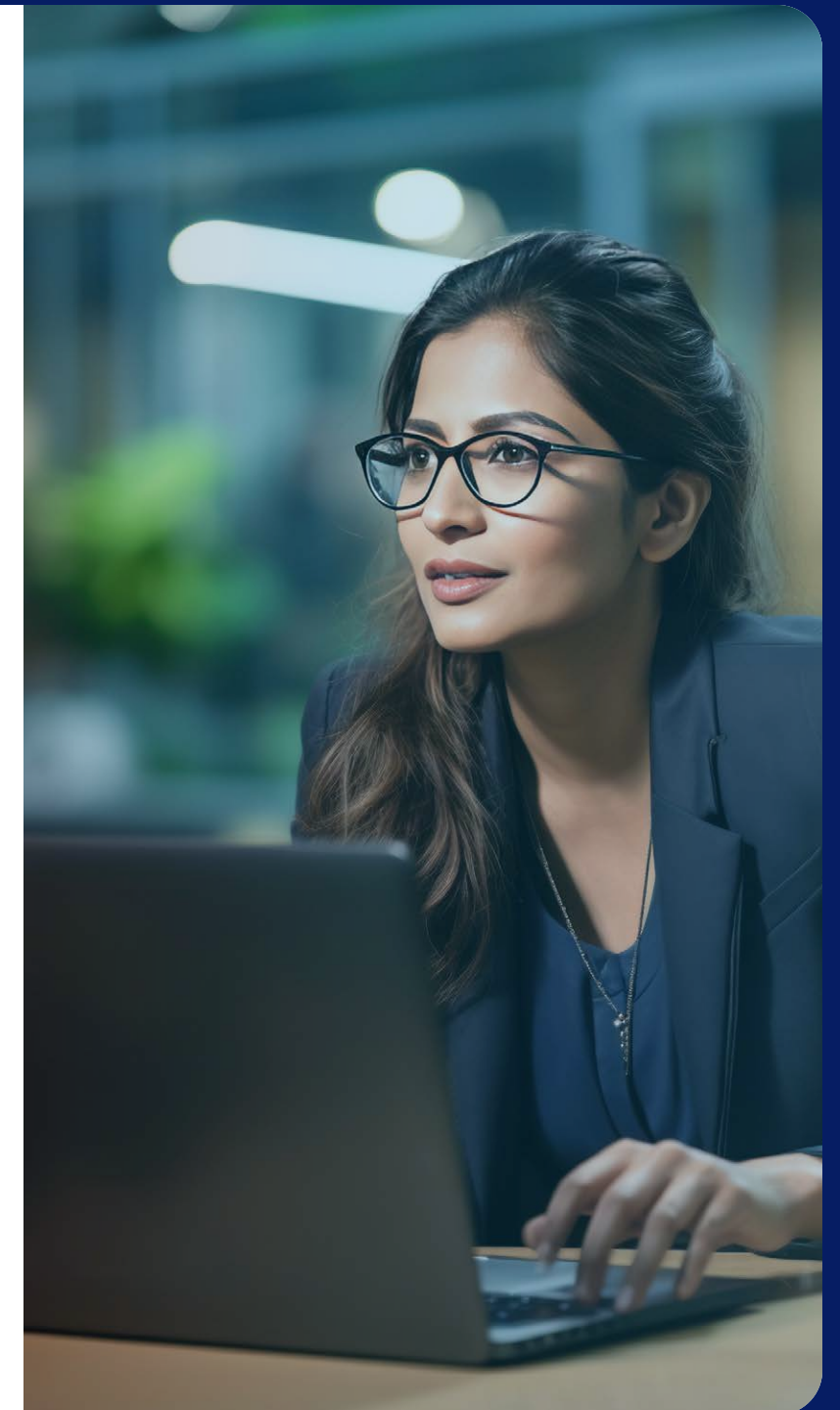
Linux workstations and technical workstations often exist as identity islands, relying on local SSH keys or unmanaged accounts. This fragmentation complicates auditing and leaves the most technical and often most privileged users outside the central security umbrella.

### Best Practice

Use modern Active Directory (AD) bridging to integrate Linux systems with cloud-based directories. This practice enables users to log in with their corporate credentials, ensuring that central policies and multifactor authentication (MFA) requirements are applied consistently while users' activity is properly reflected and attributed in the audit logs.

### Benefit

AD bridging eliminates the Linux exception. It ensures that your technical workforce follows the same security standards as the rest of the company while providing a streamlined, single sign-on experience for complex multi-OS environments.



# Practice 7: EPM as an Identity-Based Enforcement Engine

A modern endpoint privilege management (EPM) solution should not operate in a vacuum. It must act as the primary enforcement engine that translates identity policy into operating system reality.

## Best Practice

Integrate your EPM solution with your broader SOC, NetSec, and IAM stacks. Use the solution to provide identity-in-action telemetry, which gives security analysts the specific identity context behind every elevation or blocked action. Better yet, opt for a unified platform to streamline deployment and ensure maximum synergies from platformization.

## Benefit

By serving as an enforcement engine, EPM enables the security team to instantly disrupt the attack lifecycle with minimal impact on productivity. It solves a classic SOC dilemma—the choice between isolating a machine, which stops the employee from working, and leaving the endpoint uncontained during an investigation. Instead of full isolation, EPM policies can be triggered via XDR playbooks to dynamically increase restrictions on software and elevations while revalidating the user's identity. This surgical containment prevents lateral movement and impact without disconnecting the user from the network.



# Practices 8 and 9: Continuous Assurance and Passwordless Sign-In

The final layer of workstation protection is the assurance of the identity itself. Static logins are insufficient in an era of session hijacking and sophisticated phishing.

## Practice 8: Adaptive MFA

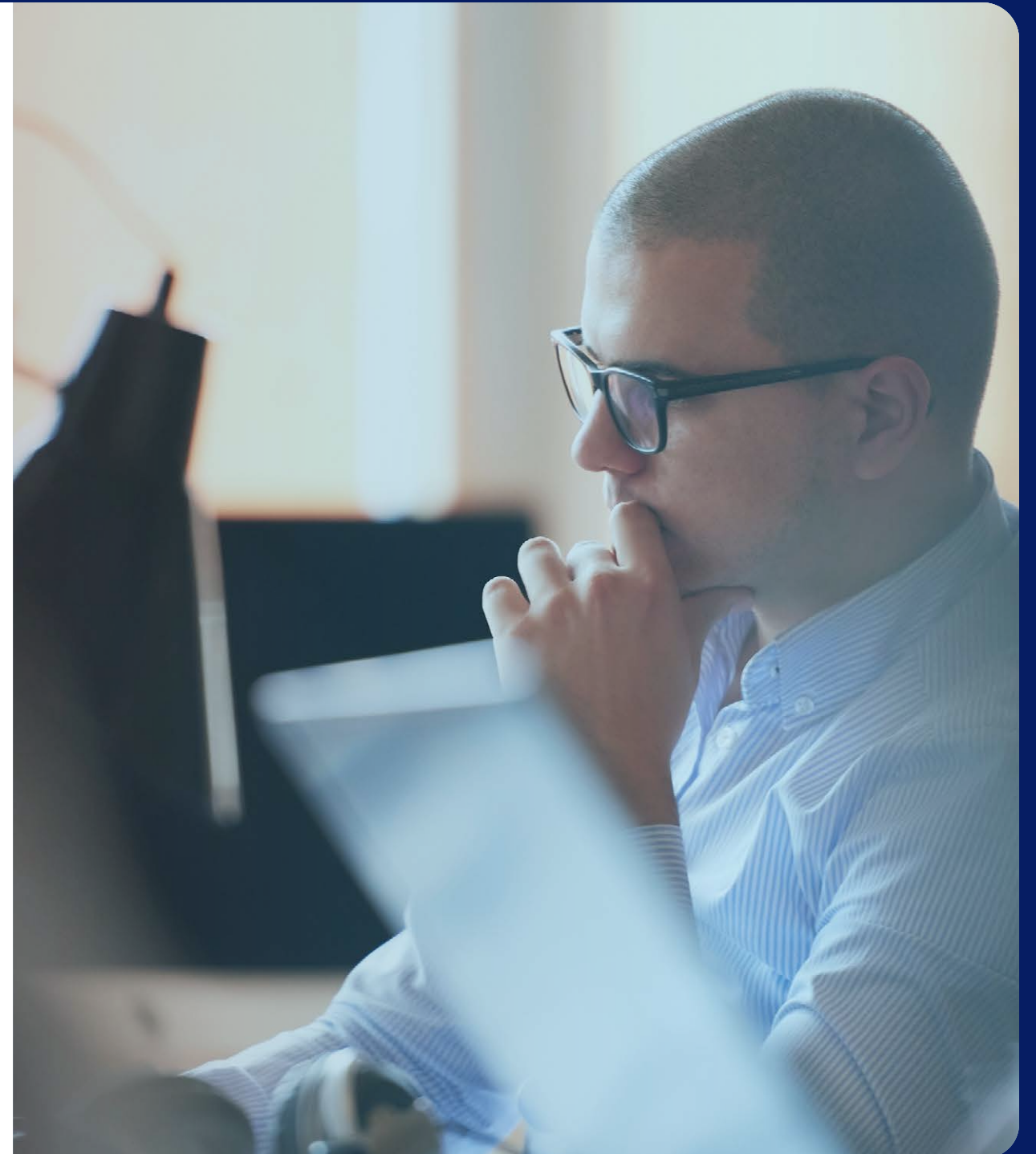
Enforce step-up adaptive MFA for high-risk actions. If a user attempts a sensitive system modification, the system should prompt for a fresh biometric or hardware-key verification.

## Practice 9: Passwordless Experience

Provide a secure endpoint sign-in using modern, strong MFA options. An end-to-end passwordless experience removes the most common attack vector—the password itself.

## Benefit

By combining continuous identity assurance with a passwordless workflow, you eliminate credential compromise as a viable attack method. Users enjoy a frictionless experience, while the organization gains the certainty that the person behind the keyboard is who they claim to be.



# The Path to Modern Endpoint Security

Workstation protection is no longer a matter of simply locking down a device. It's about the intelligent governance of identity and privilege at the operating system level. By adopting these nine practices, organizations can close the privilege gap and ensure that every user, application, and AI agent operates with the minimal permissions required for success.

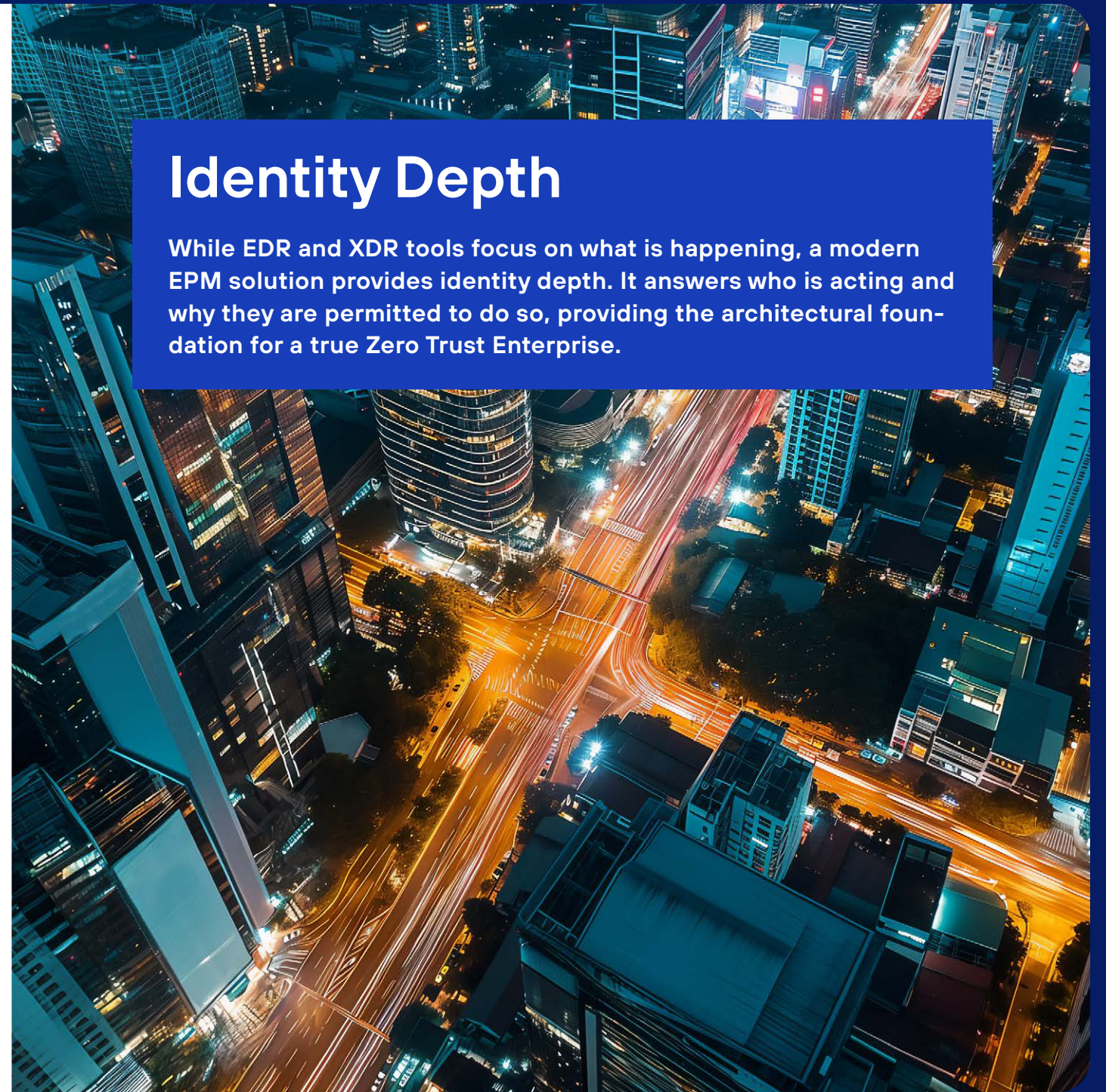
1. Discover unmanaged accounts to eliminate blind spots.
2. Remove local admin rights to stop attackers in their tracks.
3. Elevate processes, not users, to maintain productivity.
4. Ring-fence applications to contain potential exploits.
5. Govern AI agents to secure the future of work.
6. Bridge Linux systems to unify identity across the enterprise.
7. Enforce the policy through a modern EPM engine.
8. Verify identity continuously with adaptive MFA.
9. Secure sign-in with a passwordless experience.

## Take the Next Step: Schedule a Live Demo

The shift to an identity-centric defense model requires a platform approach. See how a unified EPM solution can operationalize these nine best practices in your environment today. [Request a demo.](#)

## Identity Depth

While EDR and XDR tools focus on what is happening, a modern EPM solution provides identity depth. It answers who is acting and why they are permitted to do so, providing the architectural foundation for a true Zero Trust Enterprise.



# 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](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\_eb\_nine-best-practices-for-workstation-protection\_043026