



STRATEGIC SOURCING

The Executive Guide to Identity Platforms

What to Consider in the New Era of Identity Risk



Contents

Introduction 3

Defining Next-Generation Identity Security Platform 6

Why Intelligent Privilege Controls Are Foundational to Identity Security..... 8

Shared Services that Make a Platform a Platform 10

Shared Services for a Modern Identity Security Platform11

The Role of AI in an Identity Security Platform 12

Evaluating an Identity Security Platform..... 13

Get to Know Idira Identity Security Platform 13

About Palo Alto Networks..... 14



Introduction

If you're reading this, you've probably been to at least one meeting where someone asks: "Have we locked down every privileged identity?"

It's a hard question to answer.

Privileged access now hides in plain sight—in users, in service accounts, in SaaS apps, and in browsers. The more security tools you add, the less likely they are to work together, and the harder it gets to gauge what's exposed.

Today, identity isn't just the center of cybersecurity investment. It's one of the most complex risk areas to govern, thanks in part to the sheer volume and velocity of identity growth. If you're responsible for choosing a defense, you're facing three converging challenges:

1. A rising wave of machine and AI identities that have privileged access to your sensitive resources.
2. Increasingly sophisticated AI-driven phishing and impersonation attacks.
3. A fractured solution landscape that makes it hard to see the full picture for identities.

What Is Identity Security

Identity security is the cybersecurity discipline concerned with reducing all aspects of identity-related risk. This discipline requires governing, identifying, and protecting all identities used within an organization, including those used to access applications, endpoints, infrastructure, and data stores. It also covers processes for detecting and responding to identity-related threats.¹

1. *The Identity Security Imperative*, CyberArk, January 2025.

Modern attackers exploit identity seams between tools for identity and access management (IAM), privileged access management (PAM), cloud and SaaS session controls—where no single tool sees the full picture. If your security team focuses only on user accounts, they're missing the hidden privileges living in packages, bots, pipelines, and developer workflows.

In this sophisticated threat landscape, technology choices matter.

The right identity security platform can strengthen your security posture and identity becomes the control plane for the enterprise. The wrong one leaves gaps for attackers to walk right through. Organizations need a fully integrated identity security platform that applies intelligent privilege controls, enforces zero standing privileges (ZSP), and gives teams a complete picture of identity risk across users, machines, bots, and applications.

Follow this guide to help you cut through the noise so you can choose a platform that's purpose-built for the identity threats of today and tomorrow.

Case in Point

The Shai-Hulud npm attack was disclosed in the fall of 2025. Rather than hack code, the attackers exploited trusted developer and machine identities to spread like a worm across supply chains, using stolen credentials and automation tokens to infiltrate CI/CD pipelines, cloud resources, and downstream dependencies.

This attack wasn't a flaw in one application. It was a collapse of identity trust, impacting human and machine identities, developer accounts, build tools, and production infrastructure. When identity-based attacks can leap from dev credentials to production systems with a single npm install, the risk surface explodes. Identity security should be designed to cover every identity—human, machine, developer—across code, cloud, and runtime environments.

The Difference Between a Platform and a Pile of Products

You likely already have parts of an identity strategy in place—a PAM tool to protect admin credentials, a single sign-on (SSO) or a multifactor authentication (MFA) solution for workforce access, and maybe a cloud identity store or secrets vault.

Chances are, however, you've also noticed the cracks. These tools weren't designed to work together or to manage the exploding number of human, machine, and agentic identities you're dealing with today. They overlap in places, and more importantly, they leave gaps, leaving you wondering:

- Shouldn't session monitoring apply to a cloud engineer, too?
- Shouldn't bots get the same protections as users?

The challenge lies in using siloed tools:

- They can't share controls.
- They can't share intelligence.
- They can't give you a complete picture of identity risk.

Most organizations feel this pain in the seams between tools, which is where attackers often strike. A modern identity security platform seals these gaps. Beyond integrating tools, it correlates data, applies shared controls, and delivers a unified view of identity risk. This connective tissue separates having a collection of tools from having a fully connected platform.

Fragmentation Drives Identity Risk

97%

of organizations experience identity silos.

97%

report that identity tool fragmentation delays incident response.

12 hours

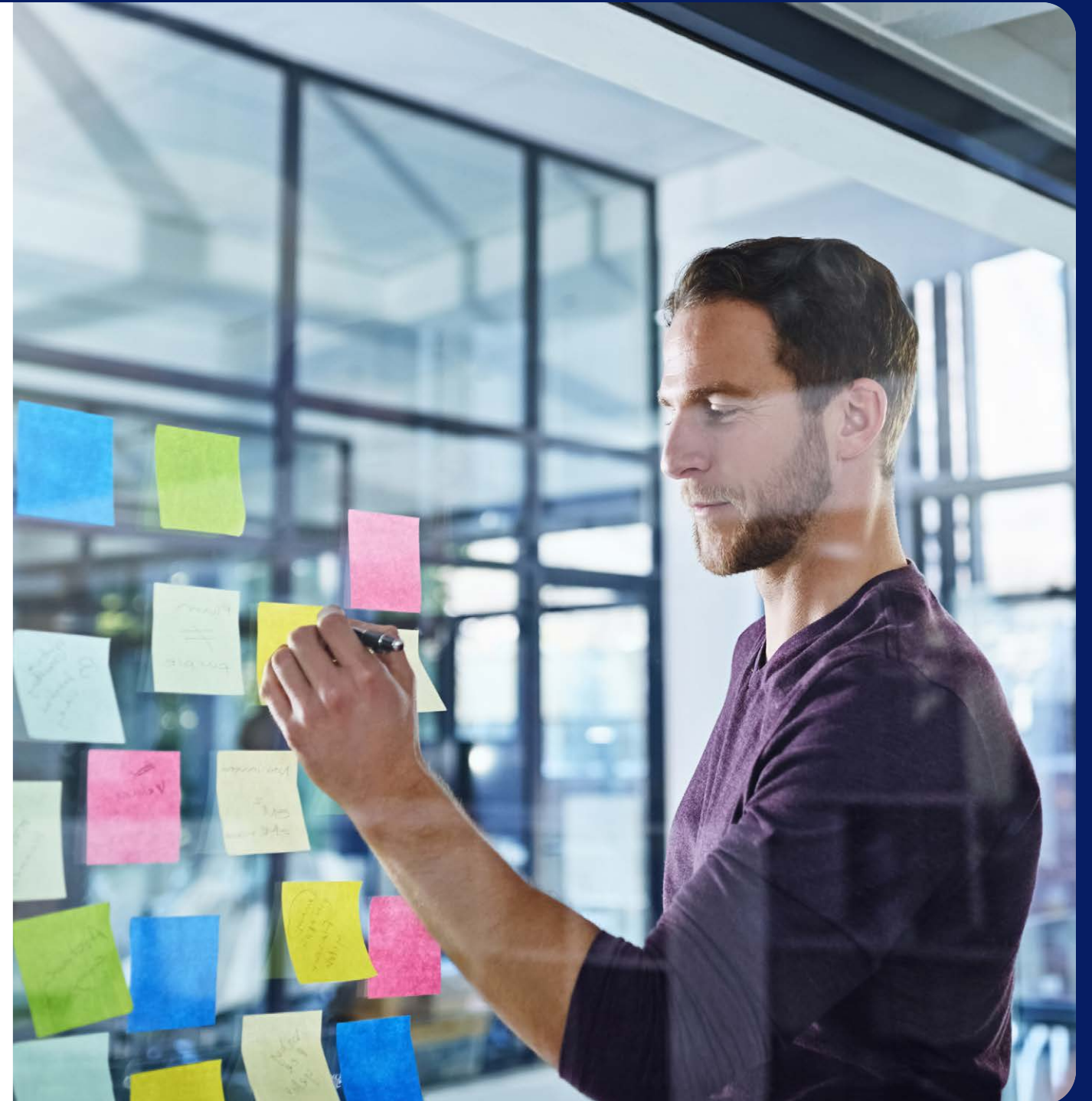
is the average time of response delay per incident.²

2. 2026 Identity Security Landscape, Palo Alto Networks, April 2026.

Defining Next-Generation Identity Security Platform

With a unified, connected solution in mind, a next-generation identity security platform should include the following capabilities:

- **Secure human, machine, and AI identities** across physical, virtual, and cloud environments.
- **Layer and coordinate controls** like MFA, SSO, PAM, and identity lifecycle management across users and machines.
- **Provide threat detection, session monitoring, and access reviews.**
- **Harness AI to analyze data** for proactive threat detection.
- **Manage and secure diverse environments**—from endpoints to cloud platforms and SaaS applications—across every industry.
- **Extend intelligent privilege controls** to all identities across all environments.



Core Features of a Modern Identity Security Platform

To enable your security teams to take advantage of those capabilities, an identity security platform should include the following core features.

Endpoint Privilege Security

Most ransomware starts here. A modern identity security platform should help you take control of unmanaged privileges on endpoints by removing local admin rights, enforcing role-specific least privilege, and improving audit readiness.

Privileged Access Management

PAM should be applied inside the tools they already use. To drive real adoption, low-friction privilege controls should fit naturally into native IT workflows, so users stay both secure and efficient.

Agentic Identity Security

Extending privilege controls to agentic identities is a prerequisite for a modern identity security platform. AI agents require broad privileges to sensitive resources, and you need a way to discovery, control and govern them.

Secrets Management

Hard-coded and unmanaged secrets can be ticking time bombs. The platform should secure and manage the credentials used by applications, workloads, and other machine identities across both enterprise and external IT environments.

Cloud Security

A modern identity security platform should extend PAM to the cloud and handle complexity and multicloud sprawl at scale. It should continuously analyze permissions, grant just-in-time (JIT) access, and monitor actions across accounts and regions—aligned to major cloud frameworks and audit requirements.

Identity Management, Governance, and Administration

The platform should clean up entitlement sprawl, remove orphaned accounts, and automate reviews by handling provisioning and deprovisioning, policy-based access, approvals, certifications, and risk-based reviews. This way, access stays aligned with roles, compliance, and least privilege.

Access Controls Across Browsers, SaaS, and Modern Environments

If work happens in the browser, attacks do too. A platform should include secure browser or browser-based session protection that can enforce policy, isolate risky actions, and record high-risk SaaS sessions without agents. It should also support zero trust access models with just-in-time privileged access across operating systems, endpoints, and cloud infrastructure.

Integration with Existing Tools

The right platform should connect identity signals to the rest of your SOC stack so you don't have to fly blind during a breach. Integration between the platform and other security and IT tools improves visibility into identity-related vulnerabilities, speeds up attack detection, and expedites containment.

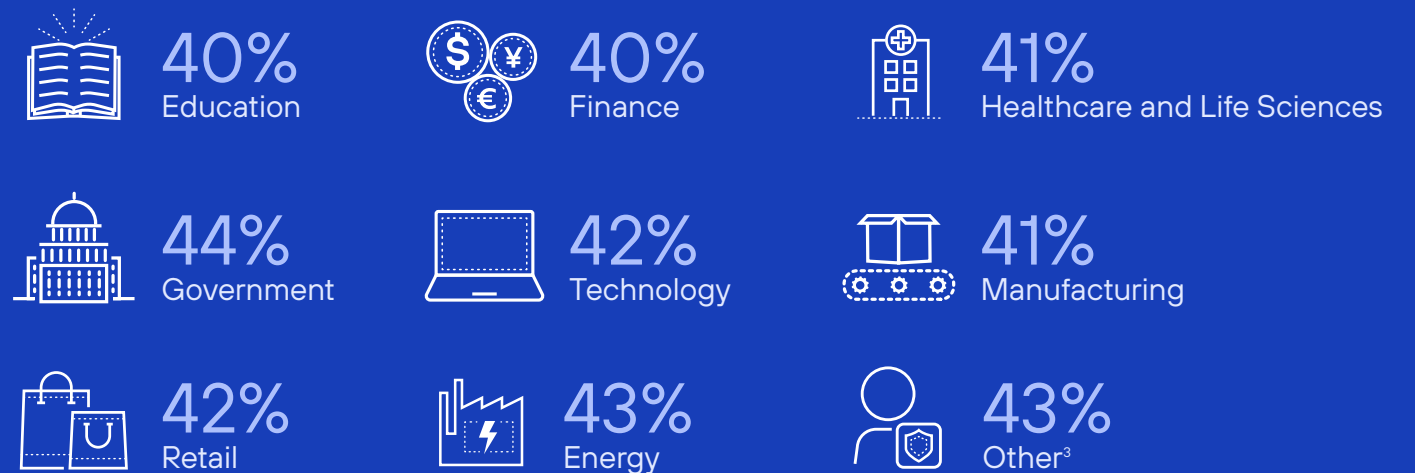
Why Intelligent Privilege Controls Are Foundational to Identity Security

Privilege controls are identity security measures that adjust in real time to govern how identities access and interact with enterprise resources. They are intelligent because they make dynamic modifications based on factors like risk and the requester's level of authorization.

As identities, access paths, and workloads multiply, privilege is no longer a static concept. Today, any human or machine identity can become privileged the moment it touches sensitive data, a risky API, or a production system.

The industry breakdown, shown at right, indicates that larger percentages of the workforce are given access to sensitive corporate data, and why it's essential to ensure that access is secure with privilege controls.

Average Percentage of Workforce Given Access to Sensitive Corporate Data



3. Palo Alto Networks, 2026 Identity Security Landscape.

A modern platform should be able to dynamically apply least-privileged controls based on risk, context, and behavior. Here are the essential controls you should expect.

Privilege Control	What It Does	Why It Matters
Zero standing privileges	Grants access only when needed, and then removes it automatically.	Prevents privilege creep, misconfigurations, and long-lived admin rights that attackers exploit.
Vaulting and credential management	Protects passwords, keys, tokens, and secrets.	Machines and AI identities now outnumber humans, and each carries credentials attackers can steal or abuse.
Session protection, isolation, and monitoring	Provides oversight and control of high-risk actions.	Visibility into privileged behavior is crucial for detecting misuse, meeting compliance requirements, and expediting incident response.
Endpoint identity security	Removes local admin rights and enforces role-based least privilege.	Many attacks begin with endpoint privilege escalation. Controlling workstation and server privileges cuts off one of the most common escalation paths.
Identity threat detection and response (ITDR)	Spots privilege misuse, lateral movement, and identity anomalies as they happen.	Early detection of identity threats can help reduce dwell time and prevent escalation before critical systems are exposed.

While these capabilities set the standard for protecting privilege, don't be swayed by the identity platform with the longest feature list. What matters most is whether those features work together—across identity types, environments, and control points.

In the past, organizations relied on fragmented tools: IAM for workforce access, PAM for IT admins, cloud security posture management (CSPM) for cloud permissions, and identity governance and administration (IGA) for access governance. But today, identity risk doesn't stay in one lane. Attackers move laterally between SaaS, endpoints, cloud infrastructure, and machine identities—often slipping through the seams.

MFA now reaches deep into endpoint protection. PAM needs to extend into the browser. Cloud permissions must be governed as tightly as workforce credentials. Your platform must remove the silos between domains and apply controls cohesively—wherever identity risk emerges.

Shared Services that Make a Platform a Platform

Ultimately, the value of a platform depends on how well it helps your team work. A modern platform should be designed to eliminate friction, not create it.

The platform should not require your team to:

- Switch between different security solutions and user interfaces.
- Cross-reference varying sources of threat intelligence data.
- Assemble reports manually during an audit.

Platform vendors enjoy talking about features. But shared services are the real test of whether those features work together.

Pressure Testing a Vendor's Coverage

Based on your most top-of-mind need—maybe one you presented to your board—you might go into vendor meetings asking if they have a solution for one specific purpose, such as for protecting IT admins' credentials.

Then, Ask for More

You know attackers will take advantage of any vulnerable credential, such as a network admin's credential leading to critical infrastructure or an HR admin's password to an app containing employee data. The solution you are evaluating must apply the same tight security controls across all credentials and identities.

Get Answers to These Questions

- Can your platform protect every form of credential for human, machine, and AI identities?
- What types of privilege controls do you have in place for securing identities of all users?
- How do each of these controls generate measurable cyber risk reduction?
- How does your platform handle AI identities, machine identities, and ephemeral cloud identities?

Shared Services for a Modern Identity Security Platform

The following features help ensure your team has a user experience that supports the most important job—protecting your organization.

United User Interface

A single pane of glass gives administrators one place to manage every identity, access type, privilege level, and session.

A shared UI helps reduce cognitive load, speed decision-making, and ensure identity decisions are made with the full picture in view.

Centralized Identity Administration

A unified function manages roles, policies, app access, and access workflows across all users and environments.

Teams can unintentionally create inconsistent rules across tools, resulting in overprivileged access and audit findings that are expensive to correct. A central function enforces consistency—and dramatically reduces manual work.

Identity Security Intelligence

A single threat engine processes all shared analytics across identity, privilege, cloud, and behavioral signals.

Most breaches exploit what one tool misses. When signals are correlated in one place, you detect risk before escalation, not after. Correlation turns noise into early warnings.

Automated Connector Management

Connector deployment, configuration, and maintenance are handled automatically across cloud and on-premises environments.

Teams should not waste time downloading agents, installing connectors, or manually configuring integrations across different systems. Automation helps eliminate brittle integrations and enforce security controls consistently, giving teams back time and helping reduce operational fatigue.

Real-Time Intelligence That Drives Action

Signals alone aren't enough. Platforms must surface risk scores, suggest next steps, and prioritize dangerous behavior automatically.

Security teams don't have time to dig through logs or session recordings. AI-driven insight and prioritization accelerate investigations and help ensure the most dangerous identity behaviors don't get buried in a long queue of alerts.

The Role of AI in an Identity Security Platform

AI can feel like a buzzword that vendors use to sell you on features that aren't fully realized. But the reality is that AI empowers attackers to analyze public data at scale, mimic tone and formatting, and adapt its messaging in real time.

Your identity platform needs AI to adapt just as quickly. AI should do more than add convenience. It should multiply the impact of your defense. AI should quickly surface risky behavior, anomalies, privilege misuse, and suspicious session activity—without forcing analysts to sift through logs.

How a Modern Identity Platform Uses AI

Streamlines Onboarding and Lifecycle Decisions

AI identifies newly discovered identities, surfaces pending access needs, and makes policy recommendations based on similar users.

Accelerates Threat Detection and Investigation

AI surfaces high-risk behaviors and generates concise session summaries so analysts don't have to sift through logs or recordings. This method shortens investigation time and improves response.

Detects Machine Identity Anomalies

AI flags unusual access to secrets or token misuse—especially in automated workflows where deviations are subtle but dangerous.

Evaluating an Identity Security Platform

Evaluating identity security in 2026 is more complex than comparing feature lists. You're defending against AI-powered phishing, machine-identity sprawl, and attackers who exploit the blind spots created by fragmented tools. Leading industry guidance favors cloud-first platforms that deploy quickly, update continuously, scale across any environment, and simplify policy management for modern applications.

Security is a team sport. When vetting vendors, look beyond the product pages and ask about the people behind the solution.

As you move from evaluation to action, the most important question is whether your identity security strategy is helping your team stay ahead—or forcing them to react. That's where the true differences emerge. The Idira™ Identity Security Platform, by Palo Alto Networks, is built around our customers. It helps teams lead with confidence instead of chasing alerts, incidents, and attackers.

Get to Know Idira Identity Security Platform

Idira is the industry leading, next-generation platform that secures all identities for the AI enterprise. Explore all the ways Idira helps the world's leading organizations build resilient identity security programs designed for today's threats.

[Request a demo.](#)

Ask the Vendor

- Can you detect and respond to identity-based attacks in real time?
- Do you have an integrated team of threat researchers studying the latest attack methods?
- Do you have a red team that can evaluate and spot our vulnerabilities before attackers do?
- Do you have leadership that has been on the front lines of security and cyber warfare?
- Do these teams come together, collaborate, and continuously improve your offerings?

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.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

© 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_the-executive-guide-to-identity-platforms_o42326