# Secure Every Identity with the Right Privilege Controls

paloalto NETWORKS | IDIRA™

# Contents


**The Evolving Identity Challenge** ..... 3

**Attackers Don't Break In, They Log In.** ..... 4

**Strategic Evolution of Next-Generation Platformization** ..... 4

**A Complete Model with Nothing to Steal or Exploit** ..... 4

- The Privilege Principle ..... 5
- Clarifying JIT and ZSP Standards ..... 5

**The Zero Standing Privilege Model in Practice** ..... 5

**Blast-Radius Risk Scenarios of the AI-Ready Workforce** ..... 6

**Secure Access from Endpoint to Session** ..... 7

**Improving Compliance Programs** ..... 8

- Security Regulations Applicable to Any Industry ..... 8
- Healthcare Industry Security Regulations ..... 8
- Financial Sector Regulations ..... 8
- Critical Infrastructure Security Regulations ..... 8

**Idira Blueprint** ..... 9

**The Identity Security Operating Model** ..... 9

- Discover Privilege Everywhere ..... 9
- Guiding Principles ..... 9
- Control Access with Layered Defense ..... 10
- Govern the Full Identity Lifecycle ..... 10

**Securing Every Identity Starts with Idira** ..... 10

- AI-Powered Intelligence ..... 10

**About Palo Alto Networks** ..... 11

# The Evolving Identity Challenge

Identity has become the most reliable target for attack success. Because it's now the last standing perimeter, getting identity security right is more critical than ever. A key reason is that identity weaknesses have played a material role in 89% of investigations handled.[1] In modern environments, privilege is no longer a label reserved for a handful of administrators. It's a condition that applies to every employee, contractor, and developer, wherever your business runs.

For two decades, identity and access management (IAM) has been fragmented into disconnected disciplines that were never designed to share context or enforce a single policy. This fragmentation has created an **uncontrolled privilege gap** that attackers exploit to move laterally and escalate access. Palo Alto Networks Idira™ ends this era by establishing a unified, next-generation identity security operating model. Idira converges identity and access management (IAM), privileged access management (PAM), and identity governance and administration (IGA) into a single platform.

As this e-book explains, Idira enables security leaders to transform the identity security programs in their strategic framework by implementing three critical core pillars for every human identity:

- **Discover** how to close the uncontrolled privilege gap by proactively identifying every human identity, account, and entitlement across the enterprise to build a live inventory, exposing hidden risks before attackers can find them.
- **Control** access for every user by implementing the zero standing privileges (ZSP) model, which replaces static credentials with layered, adaptive defenses that enforce least privilege from the endpoint to any target.
- **Govern** the full human identity journey with a secure-at-birth mindset by embedding automated policy enforcement into the identity lifecycle to eliminate privilege creep and satisfy compliance requirements in real time.

Learn how Idira closes the privilege gap through next-generation platformization to secure every access endpoint.

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


**89%**

of investigations handled had identity weakness play a material role.

# Attackers Don't Break In, They Log In

Identity security has been traditionally fragmented into different responsibilities, teams, and business units across authentication, privileged access, and governance. Each security level was built to solve a different problem for a specific team at a particular point in time. Together, they created an illusion of coverage while leaving dangerous seams that attackers exploit daily.

This siloed approach has created a fragmented environment that AI-activated attackers now exploit with speed and precision. Because attackers don't respect these category boundaries, they compromise a standard employee account, abuse the privileges it holds, and move laterally through seams that no single tool has full visibility into. This structural failure has resulted in an uncontrolled privilege gap, where meaningful access across cloud, SaaS, and on-premises systems is protected by minimal or nonexistent controls.

The risk is compounded by a widening governance gap. In most organizations, IT and engineering teams provision access to keep the business moving, while security teams are left to remediate risk after the fact. This disconnect means security teams spend their capacity chasing inherited risk rather than preventing it. Identity has become the control plane of enterprise security, yet many organizations manage it with three separate security programs that simply don't talk to each other.

# Strategic Evolution of Next-Generation Platformization

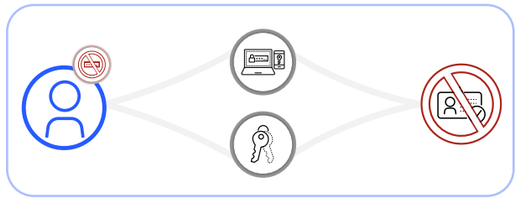
A successful identity security program requires a unified platform view to eliminate the visibility and policy gaps that fragmentation creates. For organizations that currently use self-hosted PAM versions, migrating to this SaaS-native model offers true backend unification.

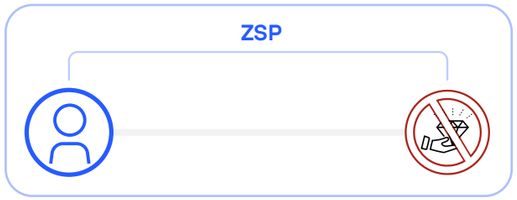
By moving to the cloud, organizations eliminate the heavy administrative burden of managing a disconnected infrastructure. Security teams can then shift from managing individual tools to making high-impact decisions backed by Precision AI® intelligence. Idira is built with Precision AI from the ground up. Its AI operates on a unified data foundation that maintains a correlated inventory. This agentic capability simplifies complex workflows by providing reasoning and recommendations grounded in the complete platform picture rather than the limited view of a single product.

Idira Identity Security Platform is built with the precision that identity security demands, at the scale and integration that Palo Alto Networks delivers. This platform provides one complete operating model that's purpose-built to secure every human, machine, and agentic identity across the enterprise.

# A Complete Model with Nothing to Steal or Exploit

The strongest security posture addresses both sides of the attack chain. When an identity authenticates without a password, using phishing-resistant multifactor authentication (MFA) or passkeys, no credential is available to steal at the front door. However, when that same identity operates under ZSP, once an attacker is inside, no persistent privilege is available for them to abuse. This complete model ensures they can't steal a password at authentication, abuse privileges, and hijack a session without detection.





## The Privilege Principle

Privilege must exist only when work exists. ZSP starts from a different premise. Standing access should be the exception, not the operating model. While some accounts, such as break-glass scenarios or root accounts, will always require some standing presence, the goal is to drive standing access to the absolute minimum. By using ZSP, organizations significantly reduce their attack surface and shrink the blast radius of a potential compromise.

## Clarifying JIT and ZSP Standards

The industry often uses JIT and ZSP interchangeably, but the technical distinction is critical for a high-maturity security posture:

- **Just-in-time (JIT)** refers to a mechanism. In most current implementations, JIT still assumes something is standing underneath. Privilege already exists, but it's waiting to be activated for a specific time window.
- **Zero standing privileges** refers to a model. It removes the standing part entirely. Privilege is created dynamically based on context and risk. When the work ends, the privilege is destroyed automatically.

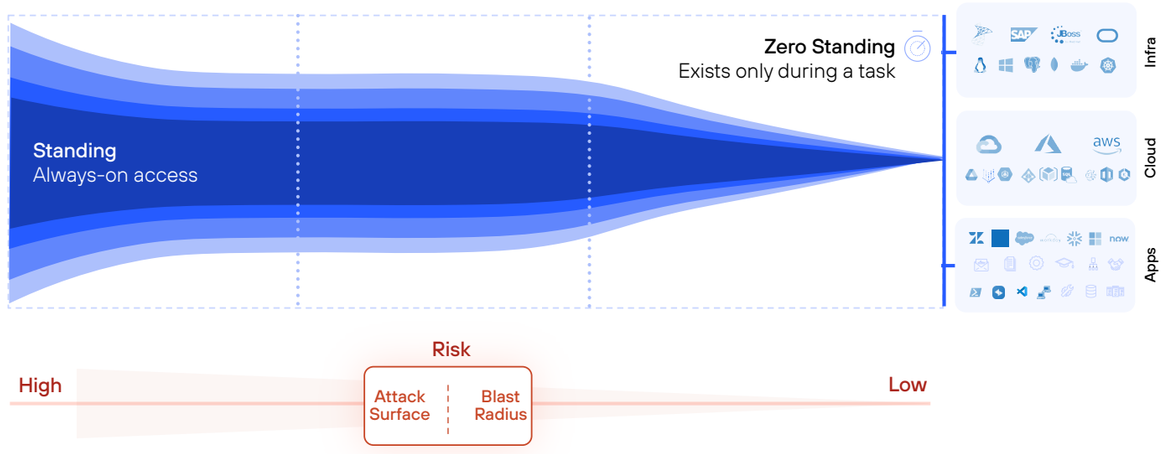



**Figure 1.** Privilege exists only when work exists

# The Zero Standing Privilege Model in Practice

Idira delivers this model through a straightforward flow that maintains speed for users while enforcing strict control for security teams:

- **Authentication:** The identity authenticates through the identity provider (IdP).
- **Evaluation:** An access request triggers an evaluation of context and risk against centralized policy, determining who is asking, what they need, and for how long.
- **Creation:** Ephemeral privilege is created, scoped specifically to the task, and time-bound.
- **Audit:** The task is performed under continuous session monitoring and audit.
- **Termination:** Privilege is automatically terminated when the session ends, leaving no standing access behind to be reused by an adversary.

# Blast-Radius Risk Scenarios of the AI-Ready Workforce

The traditional boundary between standard and privileged users has collapsed. Privilege is now distributed across every identity type, creating various blast-radius scenarios that security leaders must address.

**Table 1. Organizational Risk Scenarios and Impact**

| Identity | Access | Risk | Impact |
|---|---|---|---|
| **IT administrators, service engineers, and helpdesk** | Active Directory, network infrastructure, and endpoint management tools. | Account compromise allows an attacker to move laterally across the entire environment, providing a launchpad for full environment takeover. | **Catastrophic:** Total loss of administrative control over the core infrastructure. |
| **Developers and SREs** | GitHub; AWS, Azure, and Google Cloud consoles; Kubernetes clusters; and production terminals. | Stolen CI/CD pipeline credentials allow an attacker to inject malicious code directly into a production build. | **Catastrophic:** Full environment takeover and a wide-scale supply chain compromise. |
| **Third-party vendors and contractors** | Cloud storage, internal project management tools, and specific infrastructure via VPN. | External vendor access becomes an unmonitored attack vector due to a lack of session controls or lifecycle governance. | **High:** Third-party access vectors account for nearly 35% of all breaches.[2] |
| **Workforce users: C-suite, finance, HR, and marketing** | SaaS apps (e.g., Salesforce or Workday), banking portals, customer and sensitive data, M&A, and company and board information. | Social engineering is used to compromise a service desk account to perform unauthorized password resets for high-value targets. | **Critical:** Identity-based social engineering currently drives 33% of initial access in breaches.[3] |
| **Machine and AI identities** | API keys, secrets, and automated service-to-service communication pipelines. | Stolen secrets or misaligned AI agents acting outside approved limits automate the exfiltration of sensitive data at scale. | **Critical:** Machines outnumber humans 109 to 1 and often hold hidden, all-powerful access.[4] |

2. *2025 SecurityScorecard Global Third-Party Breach Report*, SecurityScorecard, March 2025.
3. Palo Alto Networks, *Global Incident Response Report 2026.*
4. *2026 Identity Security Landscape*, Palo Alto Networks, May 11, 2026.

# Secure Access from Endpoint to Session

Resilience begins with visibility. Automating the discovery of identities, accounts, and entitlements across hybrid environments creates a live inventory of your privileged accounts, roles, and entitlements. By surfacing privilege sprawl in real time, leaders can close the uncontrolled privilege gap before adversaries exploit it.

Privilege must be enforced dynamically based on context and risk. Your organization can achieve this comprehensive control by choosing a unified platform solution that secures the entire journey from endpoint to session. Idira Endpoint Privilege Manager systematically removes local admin rights while delivering secure, passwordless sign-in. Simultaneously, Idira Secure Cloud Access enforces ephemeral ZSP for multicloud environments. For third parties, session brokering provides isolated, credential-free access that ensures the activity is never a blind spot.

Identity governance must be a continuous process grounded in the actual state of privilege rather than in stale records. Automated lifecycle management ensures that joiner, mover, and leaver events trigger immediate access adjustments. By adopting a secure-at-birth mindset, security teams shift from chasing risk to enforcing policy at the exact moment an identity is created. This automation ensures that baseline entitlements are governed from day one.

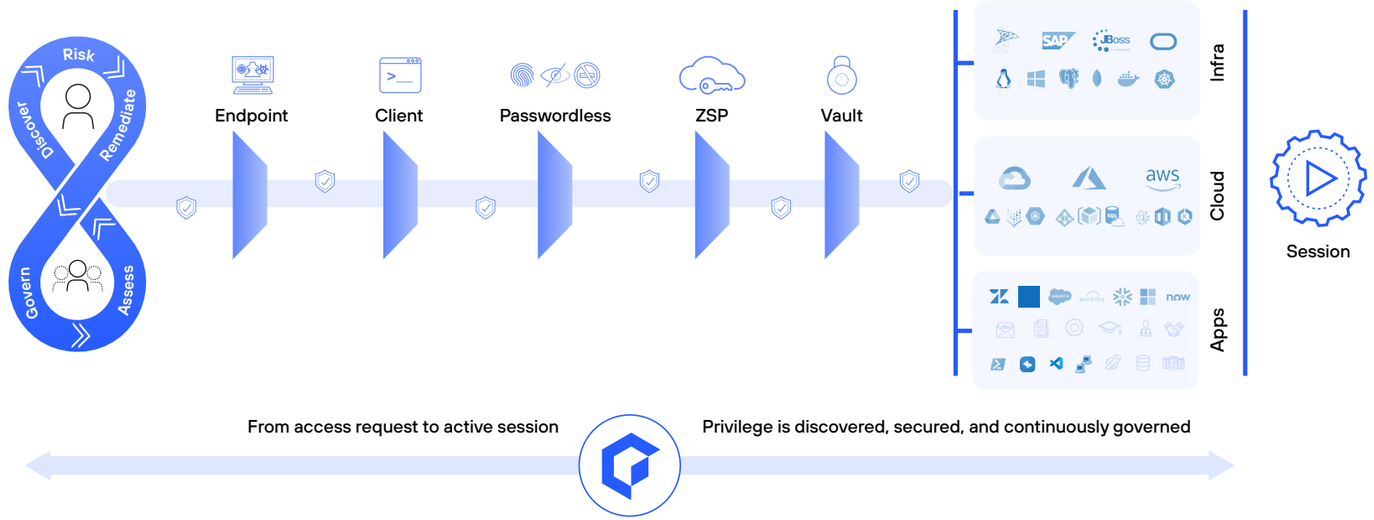



**Figure 2.** The Idira model for human identity security

Identity threat detection and response (ITDR) serves as the integrated kill switch that ties this entire model together. Unlike bolted-on tools, ITDR is embedded directly into privileged workflows to analyze logs, telemetry, and behavior in real time. At the endpoint, ITDR monitors for credential harvesting and unauthorized MFA bypass. Within the session, it identifies risky commands or vault sweeping and acts instantly by elevating authentication requirements or terminating access.

By analyzing authentication patterns, ITDR detects impossible travel or session hijacking, while also flagging entitlement creep in the governance layer. This unified platform closes the loop that standalone products cannot, stopping identity-driven attacks in progress before they escalate or move laterally.

# Improving Compliance Programs

An effective identity security program helps organizations proactively satisfy continuously changing global regulatory requirements. By moving away from stale, point-in-time access reviews, the platformization of IAM, PAM, and IGA enables continuous access certification. It ensures compliance is no longer a reactive reporting exercise, but real-time alignment between corporate policy and actual access. The result is a defensible, auditor-ready evidence trail that covers both application entitlements and vaulted privileged access.

## Security Regulations Applicable to Any Industry

- AICPA SOC II and SOC III
- NIST SP 800-207 Zero Trust Architecture
- ISO/IEC 27001
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX) Financial Fraud Controls
- Cybersecurity Maturity Model Certification (CMMC)
- EU General Data Protection Regulation (GDPR)

## Healthcare Industry Security Regulations

- Health Insurance Portability and Accountability Act (HIPPA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act


## Financial Sector Regulations

- SWIFT Customer Security Controls Framework
- Digital Operational Resiliency Act (DORA)
- Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines
- Gramm-Leach-Bliley Act (GLBA)

## Critical Infrastructure Security Regulations

- EU Network and Information Systems (NIS2) Directive
- German Critical Infrastructure Regulation
- Australian Critical Infrastructure Security Act

# Idira Blueprint

Every organization understands the need for identity security, but few know where to start or how to scale. Idira Blueprint is a prescriptive framework built from two decades of real-world experience, guiding organizations through a prioritized roadmap.

Built on the three guiding principles of preventing credential theft, stopping lateral movement, and limiting privilege escalation, Idira Blueprint has evolved to encompass the full human identity security program. It provides the execution framework for the Discover, Control, and Govern operating model, ensuring organizations continuously mature their security posture as threats evolve and environments change.

# The Identity Security Operating Model

Idira is a single identity security platform that's purpose-built on the principles of ZSP and continuous identity assurance. By converging authentication, privilege, and governance into a unified operating model, organizations can move beyond managing disconnected tasks and start achieving platform outcomes. This model covers the full spectrum of human identity security across any infrastructure, including on-premises, cloud-native, and SaaS environments.

The strategy is executed through three critical pillars that function as a single continuous motion.

## Discover Privilege Everywhere

Visibility is the first step toward control. Idira uses continuous, automated discovery to identify every human identity, account, entitlement, and shadow privilege across the entire enterprise. This process builds a live identity inventory that includes machine identities and AI agents that human users own or operate. By exposing privilege sprawl and permission creep in real time, organizations can proactively close the uncontrolled privilege gap before attackers can find it.

## Guiding Principles

The Idira Blueprint guiding principles help organizations secure their environment and contain threats:

- **Prevent credential theft:** Whether administrative account passwords or SSH keys are used to secure application traffic, secure your environment as the first step toward safeguarding credentials.
- **Stop lateral and vertical movement:** Prevent bad actors from jumping from lower-value targets, like workstations, to your most critical assets like servers through proper enforcement of credential boundaries and credential randomization.
- **Limit privilege escalation and abuse:** Enforce the principle of least privilege to contain attackers, shrink implicit trust zones, and minimize the blast radius.

## Control Access with Layered Defense

Access must be secured from the endpoint to any target through layered, adaptive controls. By default, every human identity operates with the least privilege and is continuously validated against context and risk. Using a combination of MFA, vaulting, session isolation, and ZSP, the platform ensures that controls adapt dynamically based on real-time risk signals. This unified enforcement experience provides administrators with a single, centralized control plane for all user types.

## Govern the Full Identity Lifecycle

Governance is a continuous process rather than a point-in-time review. Idira uses lifecycle automation to ensure that joiners, movers, and leavers are granted appropriate access and governed in real time. Automated, compliance-ready access reviews and certifications reduce manual toil while satisfying rigorous audit and regulatory requirements. Robust policy engines continuously detect and remediate risk, keeping access aligned with actual business needs.

# Securing Every Identity Starts with Idira

Idira unifies privileged access across all identities and infrastructures on a single platform with one privilege model, one policy engine, and one governance layer for every human and machine identity. Built on proven PAM capabilities, with modern, dynamic access management, like JIT and ZSP, this platform enables your organization to secure every infrastructure and identity to any target.

And, by consolidating the capabilities of multiple vendors into a single platform, your organization can finally eliminate the fragmentation that attackers have exploited for decades.

**Learn more about how Idira Blueprint helps organizations modernize an effective PAM program**.

REQUEST A DEMO →

### AI-Powered Intelligence

Idira is powered by Precision AI with intelligence operating across a unified data foundation that spans IAM, PAM, and IGA. This architecture leverages AI to predict identity risk and automate remediation before a liability materializes. Agentic assistance simplifies complex security workflows for both admins and users, providing reasoning and recommendations that allow security teams to make faster, more informed decisions.

# 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

© 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_secure-every-identity_042026