
Modern Identity and Access Management for Your Workforce

Minimizing Risk with End-to-End Protection
Across the Entire User Journey



Contents

- The Uncontrolled Privilege Gap**3
 - Fragmented Tools Are Failing 3
 - Pillars of a Unified Approach 3
- Challenges in Securing Workforce Access**4
 - Growing Endpoint Risks 4
 - Evolution of Workforce Identities 4
 - Perils of Privilege Creep..... 4
 - Cost of Identity Silos 4
- Workforce Identities as the New Security Battleground**5
- The Need for an Identity-First Approach**5
- 6 Key Requirements to Secure Workforce Identities**6
 - 1. Continuous Endpoint Identity Security 6
 - 2. Credential Protection and Acceleration of Passwordless Experiences 6
 - 3. Access Governance 6
 - 4. Controls That Secure Browsing and Web Sessions..... 7
 - 5. Automation and Orchestration 7
 - 6. Strong Audit and Reporting 7

- The New Foundation of Workforce Identity Security**8
 - Secure, Seamless Access 8
 - Intelligent Privilege Controls 9
 - Centralized Management 9
- Business Value of Modern Identity and Access Management**10
- The Future Is a Unified Platform**10
- About Palo Alto Networks**11



The Uncontrolled Privilege Gap

Traditional defenses have crumbled, leaving identity as the last standing perimeter of enterprise security, one that's under constant attack. Historically, enterprise-grade privilege controls applied narrowly to traditional IT admins and developers, for example, while the rest of the workforce operated without them.

In the modern enterprise, the line between identity types has vanished. The assumption that privilege is a label reserved only for IT administrators is also obsolete. Today, rapid adoption of the cloud, SaaS, and automation means that every user, whether an employee or contractor, holds immense privilege based on the data they can reach and the actions they can take. This reality has created a dangerous uncontrolled privilege gap.

Fragmented Tools Are Failing

For the past two decades, organizations have attempted to manage this gap by fragmenting identity security into disconnected disciplines:

- Identity and access management (IAM) secured the front door.
- Privileged access management (PAM) locked down IT admins.
- Identity governance and administration (IGA) managed compliance.

Attackers don't respect category boundaries. While they don't break in, they log in, moving freely in the gaps between these siloed tools by using stolen credentials, multifactor authentication (MFA) bypasses, and hijacked sessions.

Traditional, standalone access controls, like basic MFA and single sign-on (SSO), continue to remain foundational, but they aren't enough. Securing the modern workforce requires a unified approach.

Pillars of a Unified Approach

To close the uncontrolled privilege gap, organizations must shift to a unified identity security operating model that consolidates authentication, privileged access, and governance. This model is built on three critical pillars:

- **Discover:** Continuously uncover every human identity, entitlement, and access path across the environment to build a live inventory of privilege.
- **Control:** Enforce layered, adaptive controls from the endpoint to the target session, ensuring users operate with zero standing privileges (ZSP).
- **Govern:** Automate lifecycle management so access is continuously aligned with business needs, behavior, and risk.

In This Guide

This guide focuses on how the Control pillar of this model helps protect your workforce. It explores how to secure user identities at the endpoint, fortify their access through intelligent privilege controls, and protect the resources and web sessions they connect to.

Read on to discover how you can secure the complete user journey and ensure that all users can work everywhere and access everything safely.

Challenges in Securing Workforce Access

In the last year, 9 in 10 organizations suffered two or more identity-related breaches.¹ While securing workforce identities has never been more important, it's easier said than done. Several factors play a role in why enterprises are finding it difficult to adequately secure workforce access.

Growing Endpoint Risks

The absence of a proactive, identity-centric approach to endpoint security leaves systems vulnerable to sophisticated threats. Existing security measures seem like an obstacle course for end users to overcome, hindering their workflows. While inefficiencies in compliance and audit processes exacerbate risk, they are marked by a lack of real-time visibility and control over endpoint security measures. It's no wonder corporate-owned and corporate-managed workstations are a leading attack vector. With remote working and bring-your-own-device (BYOD) programs now a part of the mainstream office, this already significant attack surface has increased exponentially.

Evolution of Workforce Identities

Workforce used to mean only employees, but not anymore. The average enterprise has become a complex web of internal and third-party users, working on a mix of remote and in-office devices using cloud workflows and SaaS solutions. Contractors, partners, and other external users need access to an organization's internal resources. These third parties all have identities that need management and user journeys that must be secured.

Perils of Privilege Creep

Any identity can become privileged under certain circumstances. Workforce identities navigate various levels of risk every day, making endpoint security, identity, and access management moving targets. A workforce user might start off with access to their Windows or macOS workstation, native applications, and some level of access to certain line-of-business (LOB) applications as part of their regular duties. However, as their responsibilities increase or they need access to more tools, their permissions expand, creating a pathway to an organization's most valuable assets—an attacker's dream.

Cost of Identity Silos

For too long, organizations have deployed IAM, PAM, and IGA as separate disciplines. If these capabilities operate in silos, a user can pass every IAM control at the front door and still hold excessive standing privileges that IGA hasn't reviewed and PAM has never seen. Attackers understand this, and they exploit the gaps between these disconnected systems.

1. *2025 Identity Security Threat Landscape Report*, CyberArk, May 2025.
2. *CyberArk, Identity Security Threat Landscape*.
3. *2024 Data Breach Investigations Report Executive Summary*, Verizon, May 2024.
4. *IBM X-Force Threat Intelligence Index 2026*, IBM, February 2026.
5. *2024 Trends in Securing Digital Identities*, Identity Defined Security Alliance, accessed March 27, 2026.

94%

of organizations experienced an identity-related breach in 2024.²

71%

year-on-year increase in cyberattacks using stolen or compromised credentials.³

~4x

increase in the number of major supply chain or third-party breaches over 5 years.⁴

84%

of identity stakeholders say security incidents have had a direct impact on the business.⁵

Workforce Identities as the New Security Battleground

Whether users access high-risk SaaS platforms or general workforce SaaS applications—or conduct personal tasks on a corporate machine—their primary entry point is the web browser. The vehicle for accessing all these resources takes place on users' endpoints. What's concerning is that almost 60% of breaches are attributed to a combination of compromised credentials and exploitable vulnerabilities, from poorly protected web applications to associated threats like session abuse or cookie hijacking.⁶

Workforce identities have become the new security battleground for the enterprise, and foundational endpoint and user access controls alone, such as MFA and SSO, are no longer enough. Although a necessity, these solutions act more like static checkpoints in the road.

As standalone controls, they are outdated and unable to adapt to the diverse needs of today's workforce or the sophisticated tactics of modern attackers.

Instead, the new baseline for a successful defense is holistic, end-to-end protection. It secures the complete user journey and accounts for every attacker pathway, from the first mile of access at the endpoint to the last mile of data consumption.

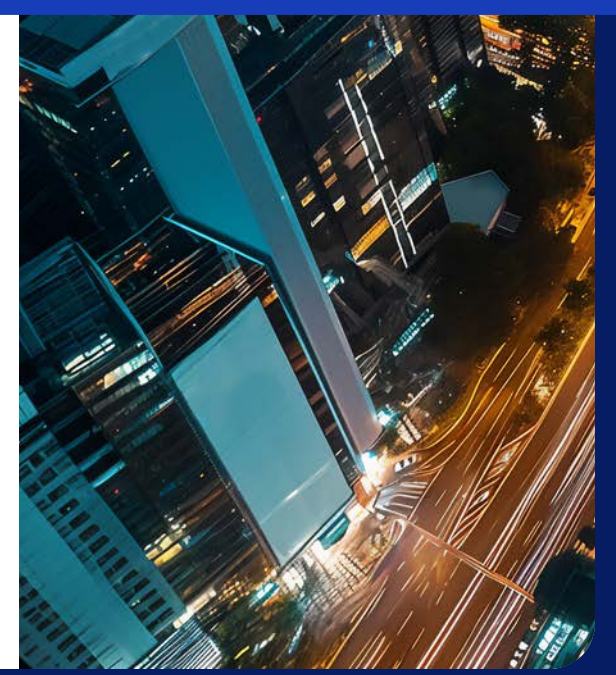
While securing the initial login is crucial, it's just the starting point. Organizations need a strong, layered approach that safeguards the digital journey of every user, at every step.

The Need for an Identity-First Approach

In response to how the threat landscape is evolving, organizations must find a way to secure their workforce users' credentials, browsers, sessions, and the machines they work on, while dynamically governing access permissions. To start, their security teams must adopt an identity-first approach to protecting enterprise systems from privilege misconfigurations, identity-based attacks, and insider threats. By protecting workforce users and their digital journeys, from

the initial endpoint login through the last session interaction, they can prevent access pathways from becoming attack vectors. This approach enables organizations to link actions to specific users, giving security teams better visibility into user sessions. In turn, it helps with tracking and reviewing activity, identifying suspicious behavior, and holding users accountable.

While securing the initial login is crucial, it's just the starting point. Organizations need a strong, layered approach that safeguards the digital journey of every user, at every step.



6 Key Requirements to Secure Workforce Identities

Organizations must also consider user experience in this context. They must ensure that robust security measures do not impede user productivity or contribute to security fatigue.

The challenge lies in delivering seamless access while maintaining stringent security controls across the workforce, which can be distilled into six key requirements.

1. Continuous Endpoint Identity Security

Enterprises must extend identity security to endpoints, instigating and fine-tuning privilege control policies based on user roles. Workforce users should be continuously authenticated and challenged for additional authentication where needed, based on an active risk assessment.

2. Credential Protection and Acceleration of Passwordless Experiences

Stolen credentials continue to be the foremost cause of breaches, making passwordless authentication vital to reduce the attack surface and minimize friction. Many work applications still require a username and password at login, so companies must prioritize securing these credentials.

3. Access Governance

Workforce users should have only the permissions they need to perform their current role or task. Once completed, those privileges must be removed. This governance can be enhanced with the capability to evaluate real-time risk based on contextual factors.

Hallmarks of an Identity-First Approach

Consistent

Leans on centralized policies to consistently manage access across decentralized systems. Ensures access controls are uniformly applied to reduce the risk of privilege mismanagement.

Context-Aware

Uses identity data and context—including location, time, device, and security status—to make dynamic, real-time decisions.

Continuous

Adapts controls throughout the user session and adjusts access rights in real time such as if a user moves to a new location.

4. Controls That Secure Browsing and Web Sessions

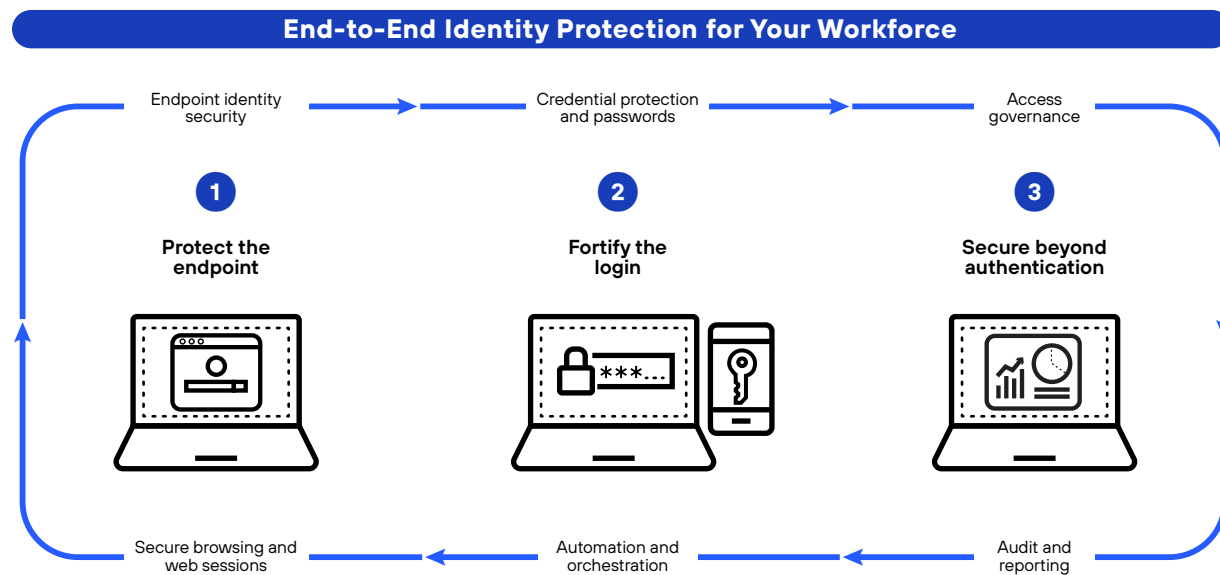
Enterprises must extend intelligent privilege controls to high-risk users, applications, and sessions, making sure every sensitive resource is protected with risk-appropriate controls beyond the point of login.

5. Automation and Orchestration

To eliminate the risk of human error, improve efficiency, and reduce costs, teams might want to automate their processes. By creating no-code workflows, organizations can orchestrate onboarding and offboarding, for example, or respond to security alerts quicker.

6. Strong Audit and Reporting

Security teams must be able to continuously audit and enforce least privilege across the entire system—including devices, applications, browsers, and sessions—to ensure compliance.



The New Foundation of Workforce Identity Security

Once an identity-first foundation has been established, organizations must consider a defense-in-depth approach. This strategy spans the three main pillars of modern identity and access management. Let's look at each pillar and the actions to take to secure the modern workforce.

Secure, Seamless Access

The first step is to streamline access to services, apps, and resources from anywhere and on any device. This foundation of workforce identity security provides a baseline of protection for all identities and endpoints.

Set in Motion

Security teams enable end-to-end passwordless access by layering SSO with phishing-resistant MFA, setting the foundations for advanced authentication policies based on behavioral risk. From there, they layer up to browser security, web session security, and automated web session summaries that can enable them to monitor and audit end-user actions at scale.

Identity Security Advantage

In addition to boosting productivity, this seamless access strengthens the overall security posture. It minimizes the risk of password and login fatigue, which encourage workforce users to use insecure workarounds and weak recycled passwords.



Intelligent Privilege Controls

Workforce users engage with various endpoints, data, and applications as part of their daily tasks. They might handle sensitive information through high-risk endpoint native and SaaS applications, embodying a level of risk that fluctuates with their access privileges. The blurring of the lines between identity roles compounds this issue.

For example, employees are commonly given administrator rights to their machine and then tasked with installing their own applications and managing security software, all while having access to sensitive systems and data through their browser. A single click can lead to endpoint compromise, credential and web session data theft, and, ultimately, data exfiltration.

Set in Motion

To protect the enterprise, your team must apply the principle of least privilege and dynamically adjust that privilege based on risk behavior through context-aware, real-time security controls. One of the most critical controls is an active defense of credentials and trust tokens scattered across the operating system, browser, and third-party applications.

Identity Security Advantage

Intelligent privilege controls provide granular, layered protection without increasing the burden on already-stretched security and IT teams. In turn, they curb the inevitable risks of user identity theft and privilege creep by providing deeper insights into identity-based threats and protections against both preauthentication and postauthentication attacks.

7. CyberArk, *Modern Identity Security for the Workforce*.

Centralized Management

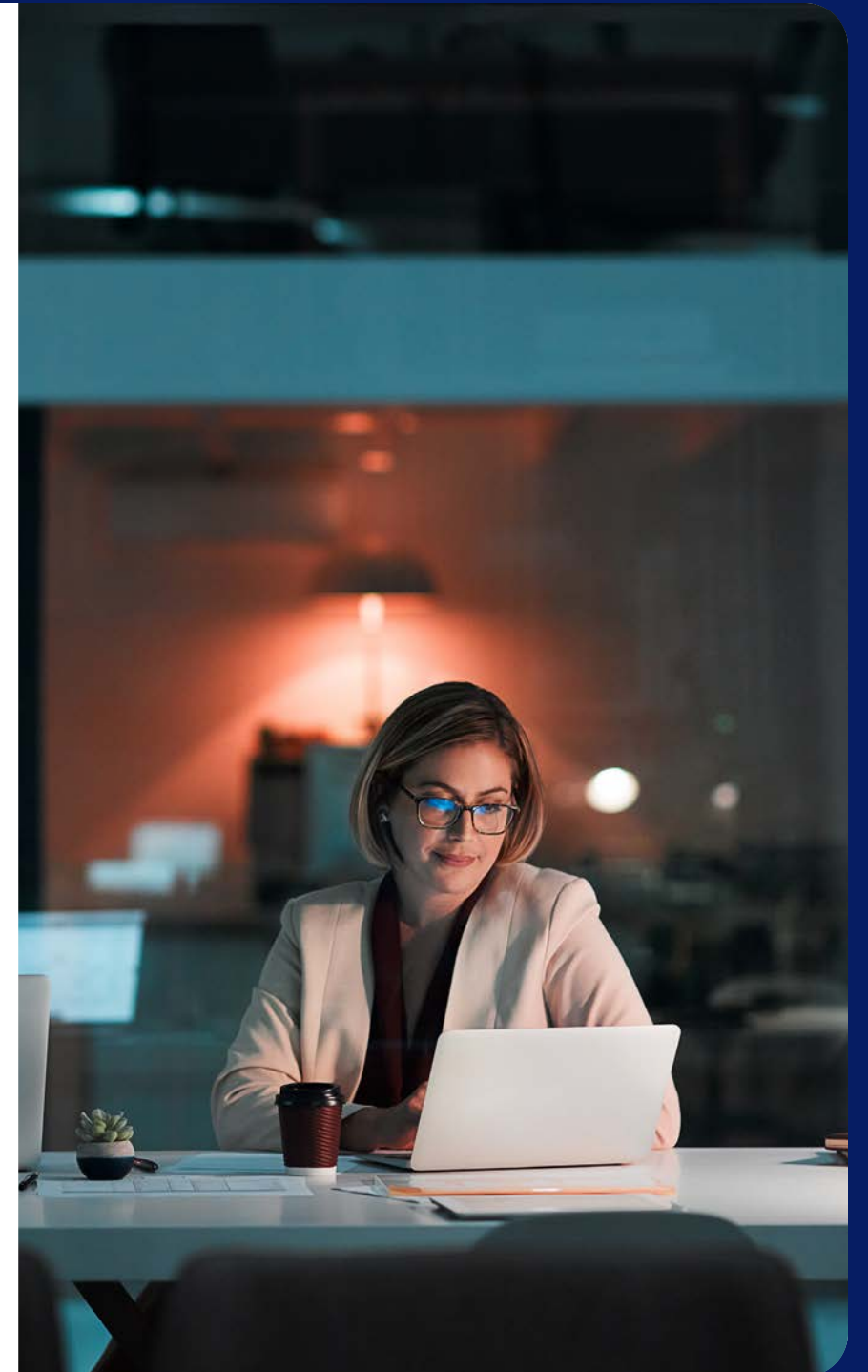
Achieving secure, seamless access depends on a mindset shift when it comes to security management. At present, nearly all (94%) security decision-makers rely on more than 10 vendors for identity-related cybersecurity initiatives.⁷ However, given the limitations of siloed controls and the inherent visibility gaps this creates, modern workforce identity security depends on the introduction of a holistic, unified approach to managing and securing user journeys.

Set in Motion

Look for opportunities to consolidate controls and efforts to strengthen your overall security posture by fully integrating siloed solutions. Also, consider how a centralized management platform will enable you to automate smart flows throughout the entire identity lifecycle by using a single administration dashboard.

Identity Security Advantage

Centralized management unlocks end-to-end visibility across the enterprise. In today's highly volatile IT environment where any user can gain privileged access, bringing centralized management to identity security enables underlying solutions to share controls and collectively benefit from threat intelligence. Because greater visibility means greater control, this approach also delivers enhanced risk mitigation for the organization while enabling security teams to be more efficient.



Business Value of Modern Identity and Access Management

Adopting a modern IAM framework for your workforce ensures that a compromise doesn't reward bad actors. By gaining visibility into all user journeys and implementing a blend of proactive and reactive controls, organizations can better monitor, manage, and audit access across workforce identities and enterprise resources. The result is a significantly reduced attack surface, which, in turn, minimizes the overall impact of security incidents, including brand and reputational damage that can have a long-term impact on the business.

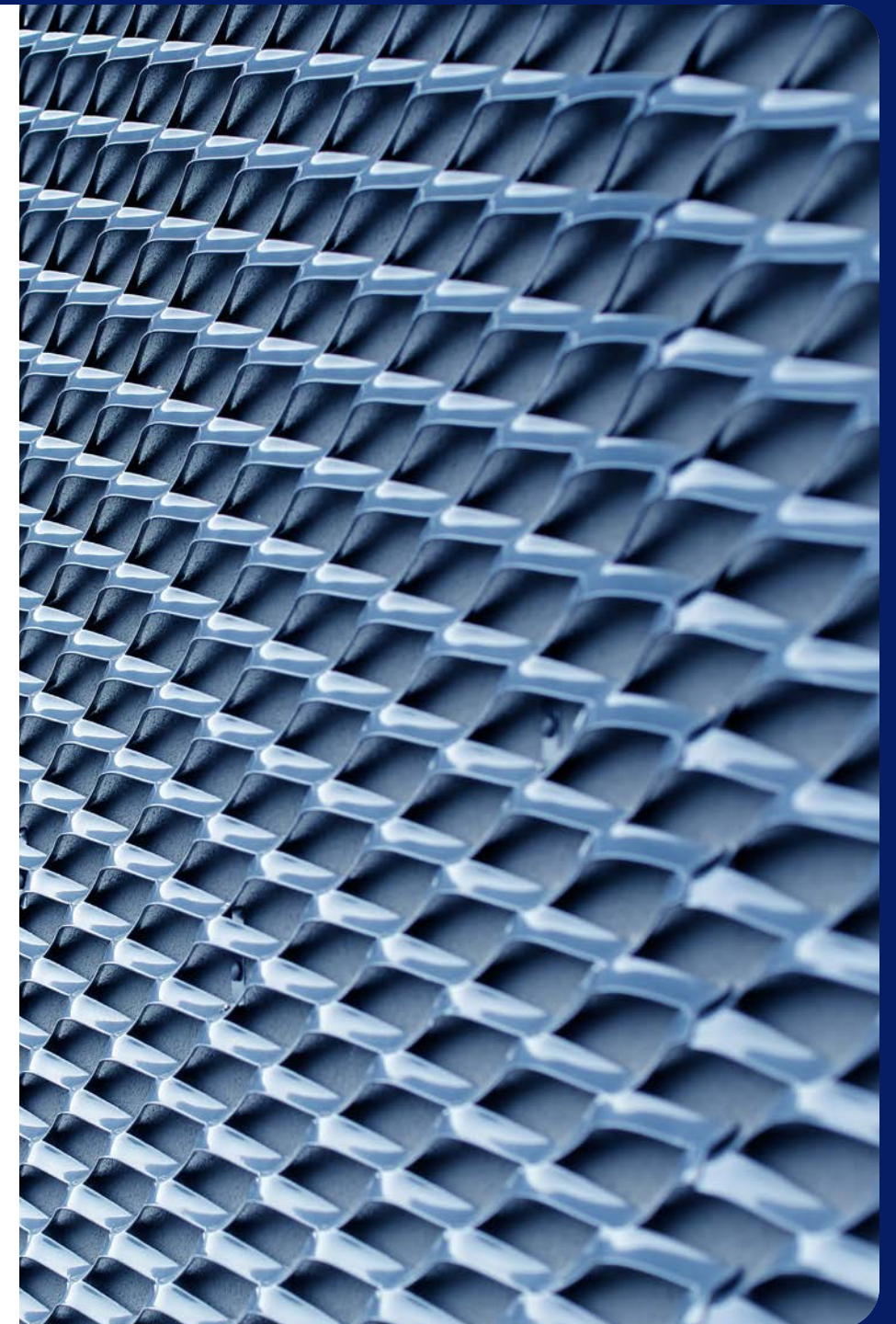
The continued proliferation of workforce identities and the evolution of sophisticated threats mean that security must extend far beyond the initial login. Managing these challenges depends on taking a holistic approach that protects user journeys across all potential attack pathways, from endpoint security and credential protection to secure browsing and user sessions.

The Future Is a Unified Platform

The future of workforce identity security lies in platformization. When you converge IAM, PAM, and IGA capabilities into a single, AI-native platform with one unified data model and one policy engine, the security math changes. Discovery informs access control, access control informs governance, and governance continuously informs your overall risk posture.

By anchoring your strategy in a unified Discover, Control, and Govern model, you can confidently apply enterprise-grade privilege controls to your IT admins and every human identity.

To learn more about IAM, download *Identity and Access Management for Your Workforce*.



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.



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_modern-identity-and-access-management-for-your-workforce_040126