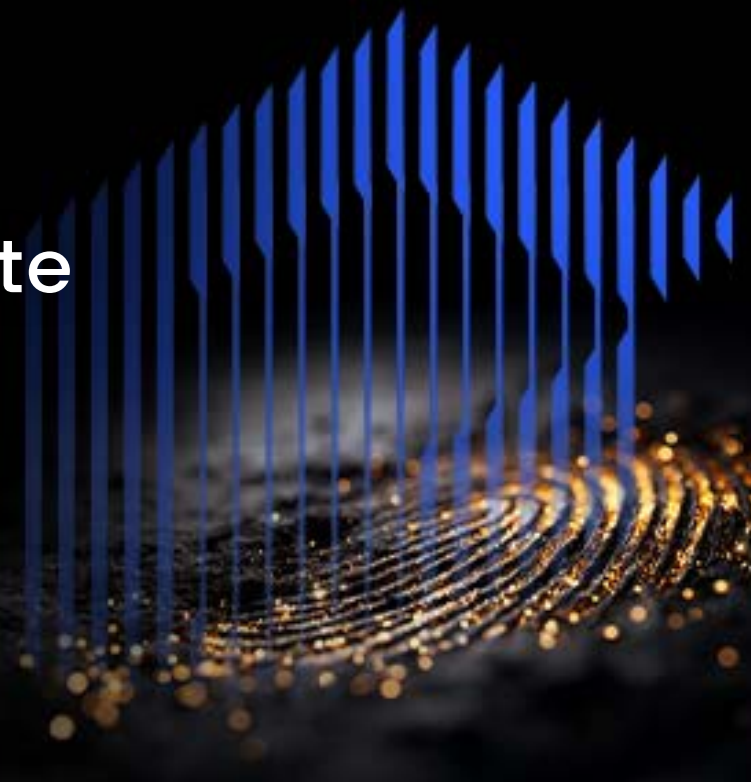
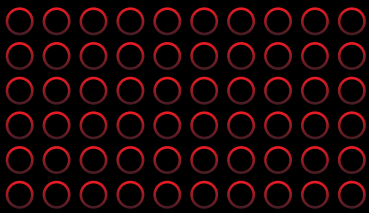


Secure the Complete User Journey

Your workforce is more dynamic and complex than ever. As employees log in to an exponential number of applications or browse the web using corporate and personal endpoints, every step along their journey becomes a potential entry point for attackers. Relying solely on login checkpoints is no longer enough to keep up with today's evolving threats.

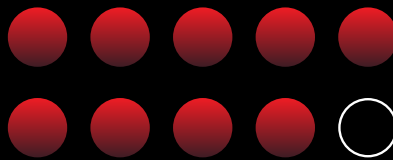


It's Time to Rethink Identity and Access Management



600M

identity attacks happen per day, 99% of which are password-based.¹



9/10

organizations suffer identity-based phishing and vishing attacks.²



<6sec.

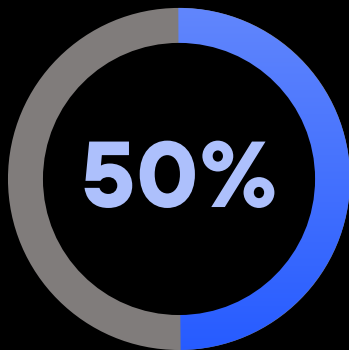
is the average time it takes users to fall for phishing emails.³

YOUR SOLUTION?

A modern, multilayered approach that extends the right amount of privilege controls to each identity at every point along the user journey, from device login to session termination.

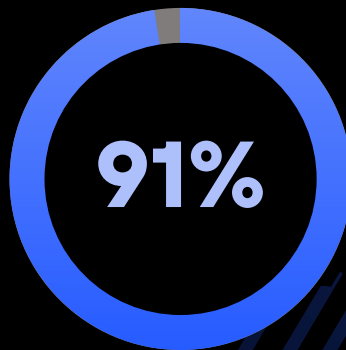
Why Identity and Access Management Needs an Upgrade

Sprawling Endpoints



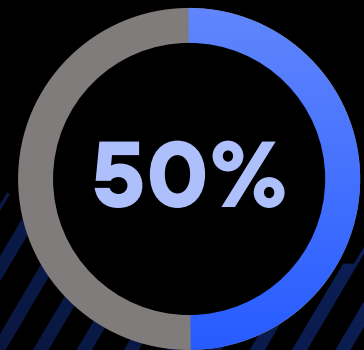
of unmanaged devices access sensitive corporate resources, resulting in ransomware.⁴

Dynamic Workforce



of security professionals are concerned about risks from third parties who use inadequately protected personal devices to access internal company resources.⁵

MFA Bypass Attacks



of incident responses involved MFA bypass attacks.⁶

Secure Your Workforce with a Modern, Identity-Centric Approach

SSO and MFA secure the login. Alone, they can't prevent modern identity-related attacks stemming from preauthentication threats, like compromised credentials, or postauthentication threats, like cookie hijacking. To secure the complete user journey, you need a continuous, adaptive, end-to-end identity and access management strategy centered on five core principles.



1. IDENTITY SECURITY STARTS AT THE ENDPOINT

Extend zero trust and identity security practices to managed and unmanaged workstations. This approach prevents giving any privileges to an attacker, minimizes the attack surface, meets compliance, and reduces IT security and operational costs.



2. END-TO-END PASSWORDLESS EXPERIENCE

Enable a fast and simple passwordless experience, from the endpoint to the browser, to every federated application and resource. Together, with phishing-resistant authenticators, passkeys, and enterprise-grade password managers, you can prevent credential-based attacks and facilitate a frictionless user experience.



3. CONTINUOUS GOVERNANCE

Prevent unauthorized access by limiting users to only the resources and applications they need based on their roles.



4. RISK-AWARE PRIVILEGE CONTROLS

Secure users at every touchpoint with user-friendly privilege controls that don't hinder productivity.



5. SECURE BEYOND THE LOGIN

Guard sensitive resources and apps from postauthentication compromise with layered controls that protect user sessions beyond the login.

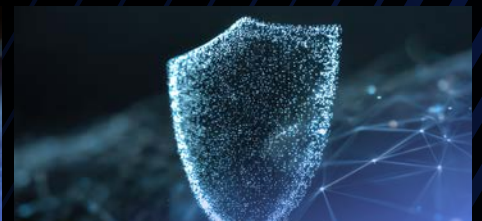
Protect Your Identity and Access Management, End to End

Today's evolving threat landscape requires a security-first mindset and controls that are:

Unified to ensure essential controls work together for a comprehensive user experience.

Easy to use to help provide complete identity protection.

Continuous for real-time prevention, threat detection, and response.



Learn more about identity and access management in the e-book *Beyond the Login: Modern Identity Security for the Workforce.*

Sources

1. *Microsoft Digital Defense Report 2024*, Microsoft, October 2024.
2. *Identity Security Threat Landscape Report 2024*, CyberArk, May 12, 2024.
3. *2024 Data Breach Investigation Report*, Verizon Business, May 5, 2024.

4. "How to Secure Unmanaged Devices with Palo Alto Networks," CXOTalk podcast, March 4, 2024.
5. CyberArk, *Identity Security Threat Landscape*.
6. *Incident Response Threat Summary for Jan-March 2024*, Cisco Talos, April 2024.



© 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.

3000 Tannery Way, Santa Clara, CA 95054 | Support: +1.866.898.9087
www.paloaltonetworks.com