Identity: The Practical Perimeter

Executive Insights from the 2026 Global Incident Response Report

It's easy for attackers to obtain a set of legitimate credentials to your organization.

Through phishing, the black market, or prior breaches, threat actors gain access by compromising legitimate accounts more than any other method. Managing and continuously validating identity is foundational to modern defense; yet a fragmented identity estate, disjointed systems, accounts, permissions and policies, make unified governance impossible.

Weak identity controls give threats a way in. Overpermissioned accounts give them room to roam.

A lack of visibility gives them cover to advance their destructive goals.

- Identity weaknesses played a material role in almost 90% of Unit 42 investigations.
- 99% of cloud identities (users, roles, and services) possess excessive permissions.
- 65% of initial access is driven by identity-based techniques.

Identity is the new perimeter. Bringing order and security to the identity estate not only improves defense, but also operational confidence and agility.

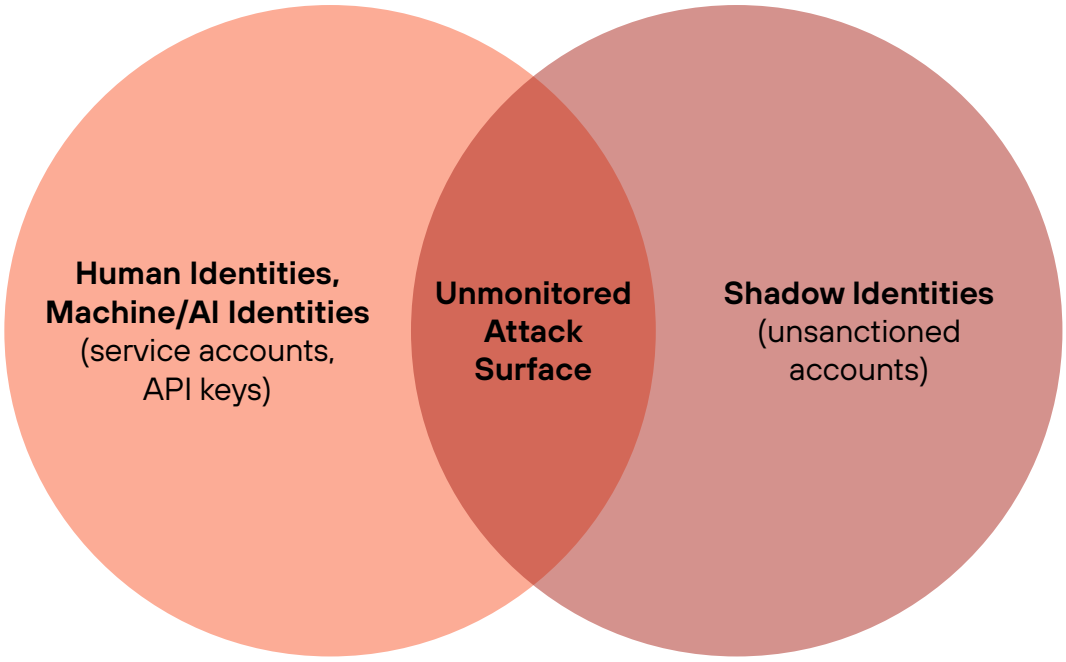

Figure 1: The Fragmented Identity Estate

Identity-Driven Access & Impact

In 65% of investigations, initial access is driven by identity-based techniques. Attackers are moving beyond credential theft, now working to circumvent multi-factor authentication controls and hijack user sessions. These social engineering tactics allow them to bypass authentication by exploiting trusted identity workflows. Previously compromised credentials and brute force activity let attackers skip the phishing process, gaining access without interaction in order to avoid suspicion. Because organizations assume trust in legitimate accounts, attackers can escalate the privileges of the compromised identity without raising red flags.

A compromised account can create just as much risk as an unpatched vulnerability. By exploiting overpermissioned and orphaned accounts, attackers can escalate quickly without flagging an alert. When credentials are reused across production and non-production, attackers can pivot between systems to find the most advantageous escalation path. Once inside, attackers can steal session tokens to persist without repeated logins and fewer conspicuous alerts. This is how a single compromised identity can quickly expand into broad access and disruptive results.

Disrupting Identity-Driven Tradecraft

Identity hygiene and hardening should be a routine discipline for every security and IT team. However, none of us is a stranger to the astounding daily workload involved in maintaining and securing the digital ecosystem. The perennial questions arise of where to start and how to keep going.

These four improvements can eliminate an immense amount of identity risk.

Deploy phishing-resistant MFA

Standard MFA controls aren't enough against modern attacks. Focus on securing high-value roles (admins, executives, developers) by implementing passkeys or hardware keys.

Manage machine identities

Most organizations fail to apply the same rigor to non-human identities as they do human ones. Model them like users in terms of least privilege, credential rotation, ownership, and lifecycles.

Harden the session

Think of sessions themselves as a high-value asset. Keep validating risk signals throughout the session, limit scope and lifetime, and apply contextual scrutiny around device, location, and browser.

Adopt Just-In-Time (JIT) access

Roles don't need access to their highest privileges every day. Treat your most sensitive permissions like a tool that users can temporarily check out. Issue access for specific jobs and automatically revoke them when the job is done.

Pursuing Zero Trust

A compromised identity turns an external attacker into a malicious insider. They don't have to hack their way in or gather access permissions from scratch, because they simply inherit all the powers and trust of a legitimate user. Due to overpermissioned roles and signal noise, suspicious behavior goes unflagged. Indicators of compromise lie buried and uncorrelated in siloed logs.

Identity comes down to validating who is doing what, and whether they should be doing it. An account is just a mask that anyone can wear—you can never fully trust who's behind it. Ergo, validation is necessary at every digital step, transaction, and interaction. This is the foundation of Zero Trust. Beyond continuous validation, organizations must establish a baseline of normal, approved behavior against which to gauge and recognize abnormal, suspicious behavior.

The Expanding Identity Attack Surface

The identity landscape will only become more complex with the continued adoption of cloud, SaaS, and AI. So will the risks.

Exploding machine and AI identities

As digital transformation continues and evolves to include more innovations, including AI models and agents, they will give rise to new risks and vulnerabilities. Non-human identities will increase exponentially and must be managed at scale.

Shadow identities and IT

These accounts or credentials exist outside your formal identity and access management program. These accounts have access to your systems, but they are practically invisible to security teams.

Identity siloes

Most organizations maintain numerous identity systems and directories that each hold their own view of users and permissions, making it difficult to implement and enforce security baselines consistently. All attackers need to do is find and exploit the weakest silo.

Identity Risks Are Business Risks

Every identity in your environment, human or non-human, has a passport to perform actions that impact the business, from moving money and changing data to shipping code and disrupting operations. Managing identities isn't just a hygiene project for IT and security teams. It's a core function of protecting revenue and reputation. Bringing the identity estate into a unified, coherent state of governance is a northstar not just for security, but for business agility and resilience.

Palo Alto Networks helps collapse identity siloes into a single security control plane, enabling teams to discover shadow and over-privileged identities, enforce least privilege, and manage access from one place across hybrid and multi-cloud environments.

Palo Alto Networks can help you progress toward Zero Trust, shrink your attack surface, and defend against the most sophisticated threats. Schedule a call with us to tell us more about your goals and organization.

CONTACT US TODAY

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