unisys

Identity-first security

Your enterprise guide to protecting the new perimeter

Contents

The new perimeter

For decades, enterprise security operated on a straightforward premise: build high walls, control the gates, and trust everyone inside. That model no longer reflects how work happens.

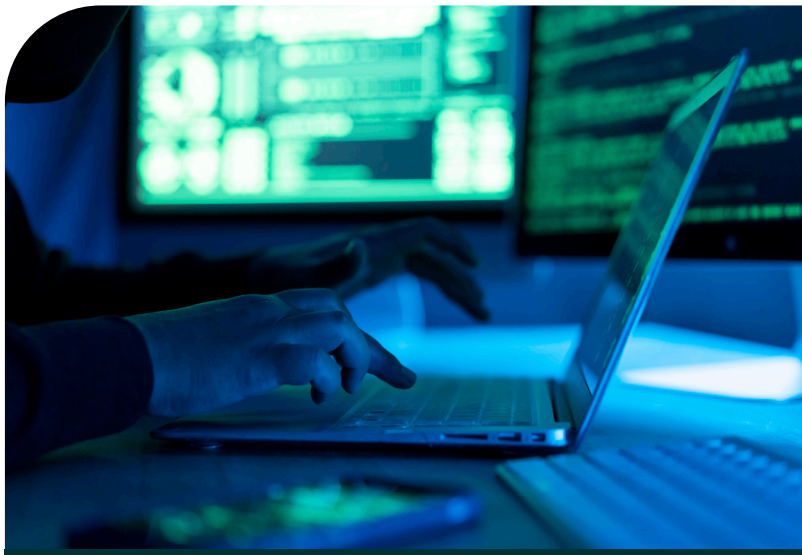
Remote work, cloud adoption, and hybrid IT environments have scattered those boundaries across thousands of locations and platforms. Identities — not networks — have become the new perimeter.

Every user account, service credential, application programming interface (API) key, and machine token is now a potential entry point. Attackers know it. The latest data shows that compromised identities account for the majority of successful enterprise breaches.

What changed and why it matters

- The corporate network no longer has four walls. It spans cloud platforms, home offices, third-party systems, and automated workflows.
- Traditional identity and access management metrics such as provisioning speed, password reset volumes, and orphan accounts were built for a different era. They don't capture the threats organizations face today.
- Machine identities, including bots, APIs, service accounts, and AI agents, now vastly outnumber human ones. Most security strategies weren't built with that in mind.

> Defending a perimeter that no longer exists is the most common gap in enterprise security today.



Attackers don't break in anymore. They log in.

Cybernews researchers recently discovered a publicly exposed database containing 24 billion records: usernames, passwords, and login URLs collected from infostealer malware, Telegram channels, and past breach compilations. Billions of accounts are at risk of takeover, particularly those not protected by multi-factor authentication.

The non-human identity blind spot

Ask most security teams how many identities they're managing, and the answer is almost always smaller than reality.

Machine identities, including bots, service accounts, APIs, workloads, and AI agents, now outnumber human identities by a significant margin and make up the majority of identity estates. Managing them effectively requires an approach different from one designed for people.

The agentic AI factor

Agentic AI is adding a new dimension to the non-human identity challenge. Unlike static machine identities, agentic AI systems access data, make autonomous decisions, and execute tasks without human intervention. As they become easier to create and deploy, the number of non-human identities to manage grows rapidly. Organizations that build NHI governance frameworks now, before agentic AI proliferates further, will be measurably better positioned to manage the risks it entails.

Four steps to closing the gap

- **See everything.** Start with a complete inventory. Visibility is the foundation of any effective non-human identity strategy.
- **Embrace new strategies.** Approaches explicitly designed for machine and agent identity management outperform retrofitted, people-focused frameworks.
- **Deploy the right tools.** Modern identity and access management, as well as privileged access management, platforms now support non-human identities from the ground up.
- **Measure what matters now.** Track the visibility index (discovered vs. actively managed non-human identities), secrets sprawl, orphan rate, and automated rotation frequency with the same rigor applied to human identity management.

> AI will accelerate cyber attacks. Organizations that make non-human identity management a core part of their identity programs now will be well ahead of those scrambling to catch up.

Source: **Unisys Top IT Insights for 2026**

When authentication isn't enough

For years, enterprise security focused on keeping attackers out: stronger passwords, single sign-on, multi-factor authentication, and biometric login. The locks got better and better. So attackers stopped picking them. Instead, they are stealing the keys.

A compromised credential opens the door. The attacker walks in, behaves like any other authorized user, and moves through the environment while standard access controls see nothing unusual. By the time unusual activity surfaces, significant damage may already have been done.

The question has shifted from "Did they get in?" to "What are they doing once they're inside?" Identity threat detection and response is how leading organizations are answering it.

Why continuous monitoring is essential

Identity governance, or verifying who gets access and under what conditions, remains important. Organizations that stop there, however, are operating without visibility into the most consequential part of the attack cycle: lateral movement after a legitimate login.

Bridging the gap between prevention and continuous detection is where security programs must advance.

The new identity threat detection and response KPIs

Leading organizations are tracking a new set of metrics to measure identity threat detection and response effectiveness:

- **Mean time to detect.** How quickly does your program flag a compromised identity? The target for high-risk accounts is 30 minutes or less.
- **Mean time to contain.** How fast can you revoke or step up an active session once a high-risk flag appears? Containment needs to happen in near real time.
- **Identity breakout time.** How long does it take an attacker to move laterally after compromising an initial identity? Keep this higher than your detection time.
- **False positive rate.** Behavioral analytics only work if security teams trust them. Mature AI-driven identity threat detection and response systems target a false positive rate below 5%, reducing alert fatigue and keeping response sharp.

> Stolen credentials let attackers masquerade as legitimate users. Standard access controls can't catch what they can't see.

The Unisys research report Top IT Insights for 2026 identifies AI as a significant force in cybersecurity on both sides.

The organizations that fare best will be those measured by how quickly they contain and recover, not just whether they were breached.

When seeing is no longer believing

Biometrics raised the bar on identity verification. A face, a voice, a fingerprint all felt like the final word on proving someone is who they claim to be. Generative AI has changed that reality.

Hyper-realistic voice cloning and real-time video deepfakes are now available to everyday attackers, and the verification methods organizations have relied on are simply not designed to handle synthetic media.

Know your exposure

Organizations can get ahead by tracking the right metrics:

- **Biometric false acceptance rate for AI spoofs**
  How often does your biometric system accept a synthetic clone as the real person? This is now a critical measure, distinct from traditional false acceptance rate testing.
- **False rejection rate**
  Legitimate users may face more friction as verification checks tighten. Track step-up authentication rates to find the right balance.
- **Help desk verification bypass rate**
  Social engineering attacks increasingly target help desk agents directly. Track how often those attempts succeed and tighten verification protocols accordingly.
- **Synthetic identity detection rate**
  Particularly relevant for financial services and education organizations, this measures how effectively your onboarding process flags synthetic or manipulated identities.

The fourth factor

Traditional authentication relies on three factors: something you know (passwords, PINs), something you have (tokens, smart cards), and something you are (fingerprint, facial recognition). Each can be observed, stolen, or replicated.

Behavioral biometrics adds a fourth: something you do: Keystroke dynamics, mouse movements, and gyroscope data. These create a continuous, dynamic authentication signal that adapts in real time and is significantly harder to fake.

For organizations with General Data Protection Regulation (GDPR), Payment Services Directive 2 (PSD2), and Know Your Customer/Anti-Money Laundering (KYC/AML) obligations, behavioral biometrics also satisfy a fourth authentication dimension that regulators increasingly expect.

> In 2024, scammers used AI-generated deepfakes to impersonate Arup's CFO on a video call and walked away with $25 million. No sophisticated operation required — just a convincing enough face.
>
> Source: **CNN, February 2024**

Time to retire the password

Passwords have been with us longer than computers. When Fernando Corbató introduced the digital password at MIT in 1961, it solved a real problem: giving multiple users private access to a shared mainframe. It wasn't long before a PhD researcher at the same institution figured out how to beat it.

The pattern has held ever since. As long as a human can know a credential, a human can leak it, share it, or be phished for it. The logical endpoint is removing passwords from authentication entirely.

What passwordless makes possible

Eliminating passwords delivers measurable business value alongside stronger security:

- Faster access and fewer interruptions for employees
- A smaller attack surface with fewer credentials to steal
- Stronger alignment to regulatory frameworks
- Reduced exposure to the financial and reputational cost of a breach

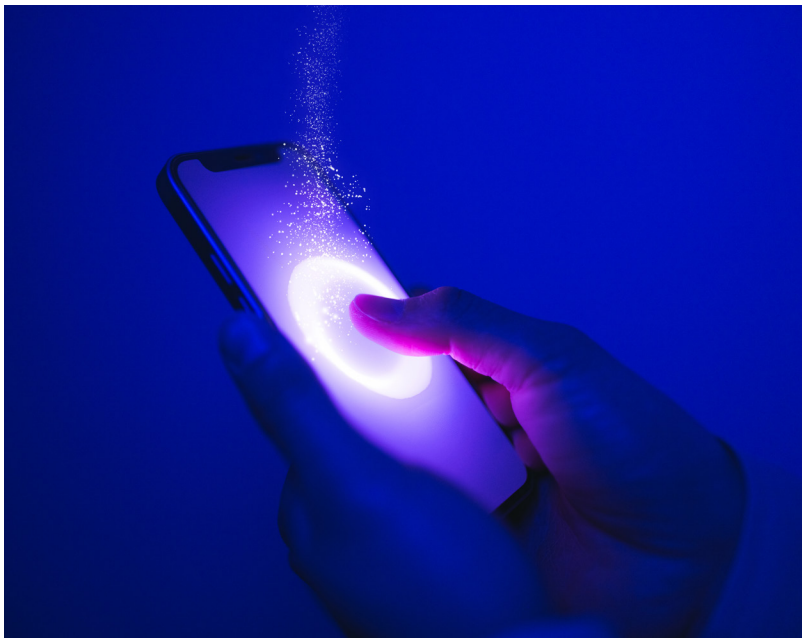
Passkeys are the leading technology making this possible. Using public-key cryptography, passkeys are stored on users' devices and tied to biometric authentication — with nothing stored on servers for an attacker to steal or crack.

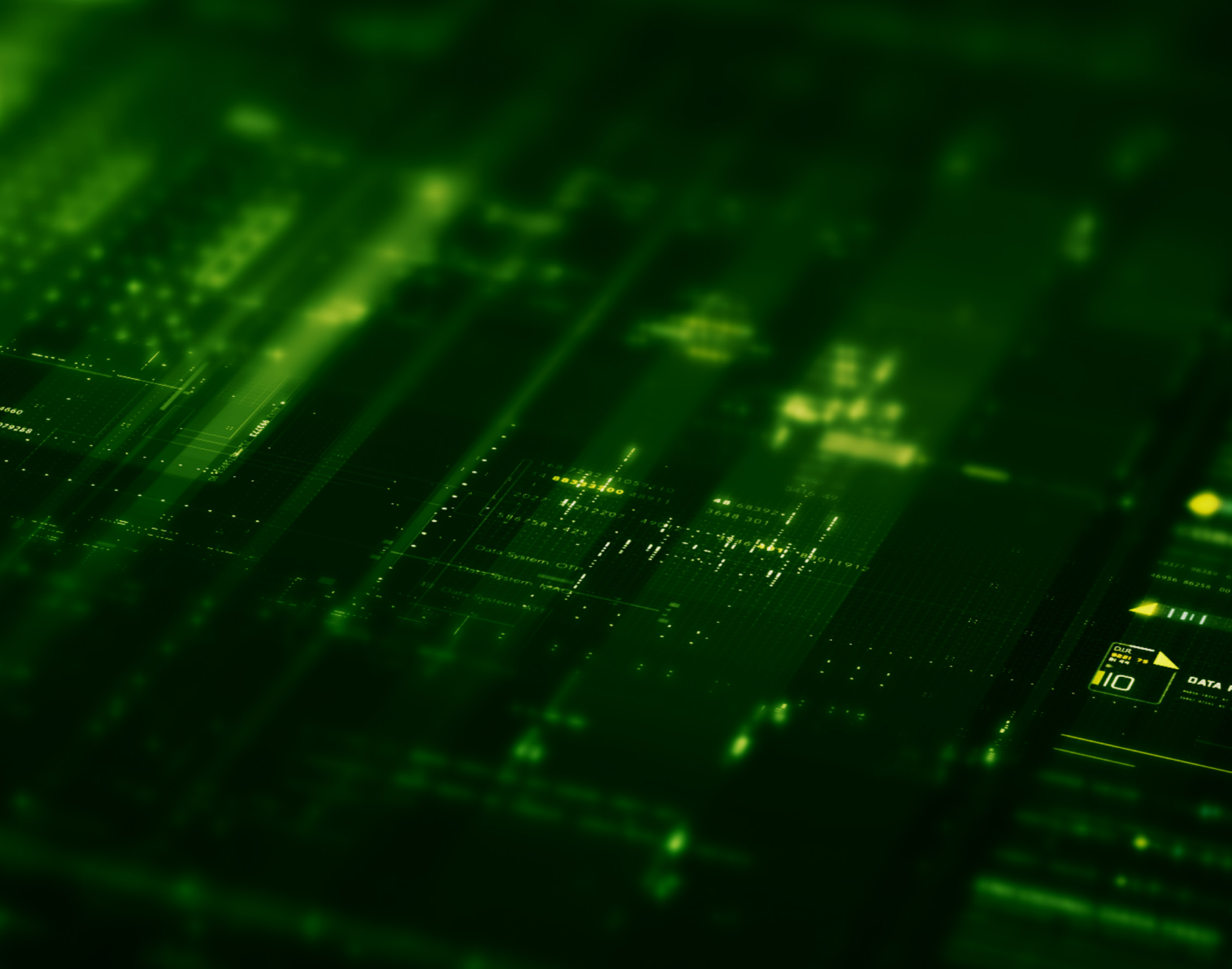
> 16 billion credentials exposed in a **major breach event**, making the case for eliminating passwords from authentication entirely

Building the business case

The business case becomes clear when you measure it with key benchmarks such as:

- Passwordless authentication for more than 50% of workforce logins
- Passkey enablement for 100% of high-risk business applications
- Reduction in help desk call volume tracked quarter over quarter
- Improved employee experience scores alongside security metrics





A strong passwordless business case connects reduced credential risk to broader outcomes: **lower cyber insurance costs, stronger regulatory standing, and a better experience for your workforce.**

What a strong identity-first security program entails

Systematically addressing identity threats requires a partner who understands the whole picture.

Unisys combines deep enterprise security expertise with industry-specific knowledge across public sector, financial services, healthcare, and manufacturing — backed by five global security operations centers and coverage for every major regulatory framework, including GDPR, PCI DSS, HIPAA, SOX, DORA, and Zero Trust.

Our business-centric approach to identity and access management encompasses people, processes, technology, operations, and governance as a connected whole.

- **Maturity assessment:** A clear picture of where your identity and access management controls stand today and a roadmap for what comes next
- **Passwordless and single sign-on:** Modern authentication that strengthens security and improves workforce productivity
- **Role- and attribute-based access:** The right people get access to the right resources and no more
- **Managed services operations:** Round-the-clock global support so your team can focus on strategic priorities
- **Integrated security testing:** Real-world attack scenarios built into every engagement

Take the next step

You already have an identity program. But was it built for the threats you're facing now? Three ways to find out:

- **Assess your current state.** Where does your identity program stand today across human and non-human identities, access governance, and authentication?
- **Identify your biggest gaps.** Use the KPIs in this guide as a benchmark.
- **Make the business case.** Connect identity investments to what your leadership team cares about: lower costs, stronger compliance, and reduced breach risk.

Ready to see what an identity-first security program looks like for your organization? Learn more and talk to a **Unisys cybersecurity** expert today.

unisys

unisys.com

06/26 6887-12547