

Securing Digital Identities

Defending Privileged Access Against AI Cyber Threats

Securing Privileged Access is Table Stakes

In today's hyper-evolving threat landscape, digital identity has emerged as the baseline enterprise perimeter. With Generative AI and autonomous Agentic AI accelerating the speed, scale, and sophistication of corporate account takeovers, securing privileged access is no longer just a compliance checkbox—it is an urgent operational necessity. Privileged credentials remain the prime target for adversarial networks looking to execute high-impact ransomware deployments and data exfiltration loops.

According to the landmark [Verizon Data Breach Investigations Report \(DBIR\)](#), identity and credential abuse stands as the leading cause of modern enterprise breaches. Stolen credentials alone account for 22% of all global initial access vectors, while credential stuffing campaigns drive a staggering 25% of daily authentication volume

Expand your definition of 'privileged users'

Privileged users are no longer just IT admins. Privileged accounts—including administrators, service identities, and cloud operators— remain prime targets; as do users across C-suite, HR, finance, marketing, and sales that have access to critical data.

AI agents are a new class of privileged identity — also called Non-Human Identities (NHIs). Like service accounts, they hold credentials and interact with sensitive systems, but they are able to make autonomous decisions at machine speed and can spawn sub-agents, multiplying both capability and risk. The governance gap here isn't just who has access, but proving that a human authorized a specific decision in an auditable, tamper-evident way.



The number one threat is phishing. New technology, such as AI, is helping threat actors create automated attacks that are much more difficult to differentiate from normal emails—and faster than ever before”

Sascha Neuhaus | Chief Information Security Officer | Louis
[Read more here](#)



Privilege is defined more by function at CERN – it's not dependent on the people, but about what they need access to. If you are an administrator of a computer service, you are subject to MFA. If you are an operator of an industrial installation, you're subject to MFA. Next, we're looking to extend MFA to other communities such as procurement, management, and secretariats. In each step, we extend control to cover more corners.”

Dr. Stefan Lüders | CISO | CERN
[Read more here](#)



The YubiKey is a purpose-built, hardware security key that contains the most secure passkey. With the YubiKey, organizations can fast track to passwordless by securing digital identities against AI-driven cyber attacks. It is the most secure and user-friendly option for protecting all users across business units; providing authentication that moves with users no matter how they work across devices, platforms and systems.

Attacks are getting more sophisticated with Generative AI and Agentic AI, and while a human may be misled into inputting their credentials on a fake phishing website, the YubiKey is never fooled.

Why choose Yubico to secure privileged access

- Reduce risk of credential theft by 99.9% and stops account takeovers while delivering 265% ROI
[Source](#)
- Help desk support savings of up to \$476,000 related to password resets and prior traditional MFA solutions
[Source](#)
- Provide secure user access at scale on any device with the best user experience
- Drive regulatory compliance to FIPS, GDPR, SOX, SOC2, PCI DSS 4.0, GLBA, PSD2, NIS2, E8MM and more
- Support the 'Trust nothing, verify everything' Zero Trust approach with strong user identity and device authentication
- Help lower cyber insurance premiums by 30%
[Source](#)
- Bridge to modern passwordless with multi-protocol support for Smart Card/ PIV, FIDO2/WebAuthn, FIDO U2F, OTP and OpenPGP on a single key
- Deploy the most secure passkey strategy: hardware-backed that is purpose built for security, FIPS 140-3 validated and Authenticator Assurance Level 3 (AAL3) compliant
- Yubico offers YubiKey as a Service for fast and frictionless deployment of enterprise-grade security
- Yubico and trusted partners provide services to support global distribution of pre-enrolled YubiKeys to anyone, anywhere
- Introduce or expand use of the YubiKey in your organization to secure digital identities with the most secure passkey

“Security keys are one of the best ways to protect accounts from phishing, and Yubico has played a leading role in making that protection practical and accessible. We’ve made YubiKeys a standard part of how we protect OpenAI employees, and with Advanced Account Security, we’re making it easier for ChatGPT users to choose that same kind of phishing-resistant protection when it’s right for them.”

Dane Stuckey | Chief Information Security Officer | OpenAI
[Read more here](#)

“Once the YubiKey started to be adopted, it became a very strong case for the right way to do things to protect the organization. The average tenure of a CSO right now is a year and a half. I am two-and-a-half years plus—and I’m still sleeping.”

Morey J. Haber | Chief Security Officer | BeyondTrust
[Read more here](#)

