AI is Hunting your Users—Your Business is on the Line

AI is redefining the threat landscape and your security needs to adapt

Rise in AI driven data breaches

One in six breaches now involve AI-driven attacks[1]. With Generative AI and Agentic AI, attackers can now easily create highly personalized, context-aware phishing attacks at scale and speed. IBM found Generative AI reduced the time needed to craft a convincing phishing email from 16 hours down to only five minutes and on average, 16% of data breaches involved attackers using AI, most often for AI-generated phishing (37%) and deepfake impersonation attacks (35%)[2].

These tools mimic the tone of executives and partners, blurring the line between authentic and malicious communication. In this new landscape, every user and non-human account with access to company IP or customer data is a high-value target.

> "AI-powered phishing has made my job significantly harder. Attacks are now highly personalized and convincing, making them difficult to detect. We've had to strengthen our defenses, train staff more intensively and stay constantly alert."
>
> **Marius Sinkevičius** |
> The Head of the IT Department (CTO) at Kaunas City Polyclinic

> "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** |
> Information Security Officer for Louis

$4.4 million
The global average cost of a data breach in 2025

1 in 6
Breaches reportedly involved attackers using AI, often used in phishing and deepfake attacks

97%
Of AI-related security breaches involved AI systems that lacked proper access controls

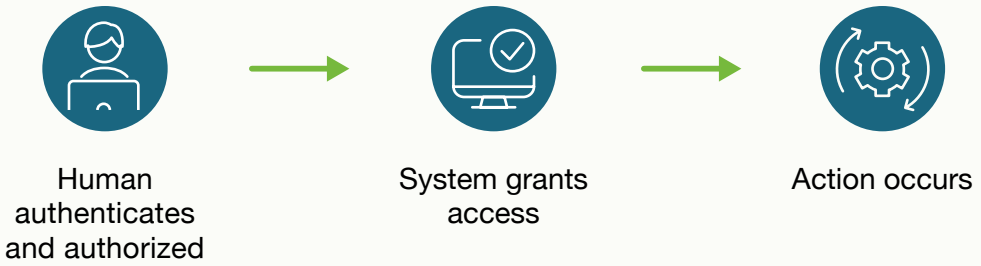
IBM Cost of a Data Breach Report 2025

Legacy security is a vulnerability in the age of AI

For human accounts, passwords are no longer sufficient—AI can crack 51% of common passwords in less than a minute and 71% in a day, and legacy mobile solutions such as SMS, OTP and push notification apps are easily bypassed[3]. If an authentication factor can be typed, shared, or intercepted, it can be stolen. As AI-generated attacks become indistinguishable from legitimate business, security strategies relying on human judgment are destined to fail.

In addition to human accounts that need to be secured, organizations also have AI agent accounts. AI agents are becoming what security leaders call 'digital workers'. They operate with legitimate credentials, interact with sensitive systems and increasingly have the authority to execute real actions. This raises a fundamental governance question: How do organizations prove that the right human intervened or authorized critical decisions made by AI?

Traditional identity systems that encompass human accounts assume a simple flow:



But when AI agents act autonomously, the identity layer must answer a more complex question: **Who authorized the action, and can we prove it?**

The solution is not to slow down AI or require humans to approve every action. Instead, organizations must identify specific categories of actions where human authorization is required. For example, access to highly sensitive documents or intellectual property or financial transfers above a defined threshold etc. In these cases, human authorization becomes a structural control – not a workflow preference. And it must be enforced **cryptographically**, not simply recorded in logs after the fact.

The ‘Human-in-the-Loop’ model: A powerful new architecture for trusted AI

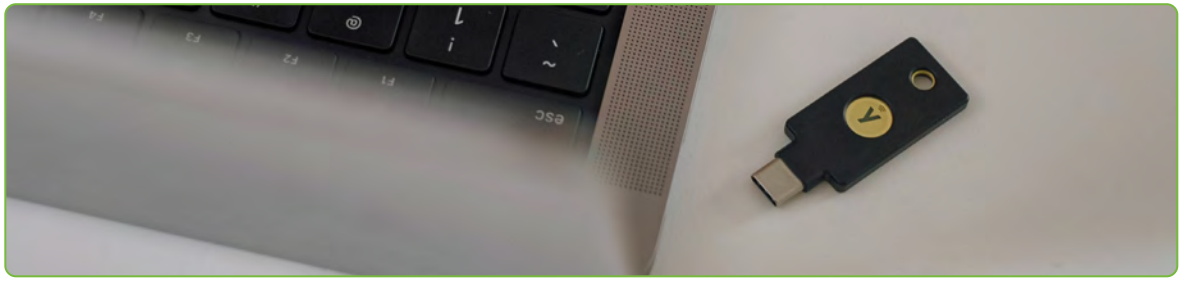
The YubiKey, Yubico’s hardware security key that offers the most secure passkey, delivers the hardware-backed root of trust, ensuring the right human is in the loop. The authorized user must physically tap the key, creating cryptographic proof of presence, ensuring that:

The approving individual is physically present

The authorization cannot be replayed or remotely manipulated

The approval is tied to a specific verified identity

In effect, the YubiKey becomes the **final human controlled point** protecting critical enterprise actions. This creates strong guarantees for regulatory compliance, risk management, financial accountability and business continuity. Most importantly, it provides **non-repudiation** – the clear proof that a specific, verified human authorized the action.



How the YubiKey stops AI-driven account takeovers

No shared secrets
YubiKeys use public key cryptography (PKC) to pair a public key with an unguessable private key which is never shared

Legitimate URL
Every credential is tied to a real URL, which is verified as legitimate or not

Intent to authenticate
Every credential is registered to a real human, blocking bots or other remote attackers through human authorization

> “The hard problem in Agentic AI security is accountability: can you prove a specific human approved a high-consequence action?” said Albert Biketi, Chief Product and Technology Officer at Yubico. “Hardware attestation without runtime enforcement is a signature with no enforcement point. Runtime enforcement without hardware attestation is a policy gate with no proof of human presence. Yubico’s integration with Delinea solves both sides.”
>
> yubico | Delinea
>
> Learn more

> “The collaboration between IBM, Auth0 and Yubico establishes a powerful model for governing Agentic AI systems. Together, these technologies create a workflow that combines AI speed with human accountability.”
>
> yubico | IBM
>
> Learn more

yubico

Immune to Deception:
While a human may be misled by a deepfake or AI-generated website, the YubiKey never falls for it with cryptographic verification and human authorization.

Agentic AI Ready:
As organizations deploy AI agents, hardware-backed identity becomes the primary control plane for trust. The YubiKey can be used as a layer of authentication security for AI agents using the Smart Card (PIV) standard that allows authentication to be cryptographically verified without an explicit need for human intervention.

Regulatory Resilience:
Drive compliance for FIPS, GDPR, PCI DSS 4.0, and NIS2 in an increasingly complex threat environment.

Powerful Protection:
Secure user access at scale across all devices, platforms, and systems.

99.9% Reduction in risk of credential theft when using YubiKeys

90% Fewer help desk tickets for password resets

265% ROI by stopping account takeovers and reducing help desk costs

$1.9 million Worth of business growth

Forrester The Total Economic Impact™ Of Yubico YubiKeys, January 2026

19 of the top 20 technology companies	**8 of the top 10** media companies	**9 of the top 10** financial services	**8 of the top 10** retail companies

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, we set the gold standard for secure, simple login, stopping account takeovers with phishing-resistant, hardware-backed authentication.

Our technology secures people in over 160 countries, delivering fast, passwordless access. Dual-headquartered in Stockholm and Santa Clara, we believe strong security should be within everyone's reach. Learn more at www.yubico.com.

> "We moved to phishing-resistant MFA with YubiKeys to prevent future incidents before they happen."

Marius Sinkevičius |
Head IT Department (CTO) | Kaunas City Polyclinic

> "We have a solution that is practical for us and, above all, sustainable. We know that we can use them for years to come. That's why it was so important for us to make the strategic decision to use YubiKeys. It was a huge step forward."

Sascha Neuhaus |
Information Security Officer, Louis

Contact us
yubi.co/contact

[1] IBM Cost of a Data Breach Report 2025
[2] IBM Cost of a Data Breach Report 2025
[3] https://www.securityhero.io/ai-password-cracking/

yubico