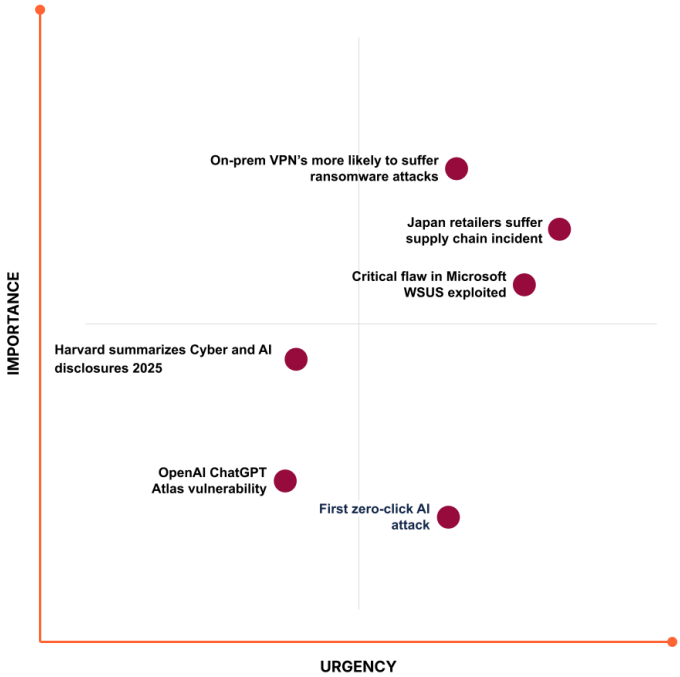
CLOUDFLARE

Cloudflare Cyber Briefing

October 31, 2025

Welcome to the Cloudflare Cyber Briefing from our Field CXO Team, helping leaders stay ahead in a fast-moving landscape of threats, technology shifts, and criminal tactics.

What you need to know:



AI cybersecurity

First zero-click AI attack

A new zero-click attack has been identified that targets popular AI agents to exfiltrate sensitive data. Shadow Escape is a novel prompt injection attack that uses malicious instructions hidden in public PDFs to trick MCP-enabled AI assistants into exfiltrating sensitive corporate and customer data.

CISO's takeaway: Securing MCP and agent identities is critical. Secure development of AI needs to be considered. Furthermore, a zero trust network access approach should be adopted for AI agents.

Source: Cyber Security News | Read more →

OpenAI ChatGPT Atlas vulnerability

Cybersecurity researchers have discovered a new vulnerability in OpenAI's ChatGPT Atlas web browser that could allow malicious actors to inject nefarious instructions into the artificial intelligence (AI)-powered assistant's memory and run arbitrary code.

CISO's takeaway: Organizations should consider if AI browsers are enterprise ready. When they use them in their environments, they need to ensure appropriate controls and guardrails are put in place to defend against malicious instructions.

Source: LayerX | Read more →

Cyber incidents

Japan retailers suffer supply chain incident

A ransomware attack crippled the operations of Japanese office supplies seller Askul, forcing major retailers like Muji and The Loft to suspend their e-commerce sales. This incident highlights the acute supply chain vulnerability within Japan's shared e-commerce and logistics infrastructure.

CISO's takeaway: Organizations should review their third-party risks. Controls such as business continuity plans and contractual provisions should be in place. Furthermore, organizations should avoid spread of such events by deploying stringent access, API security, monitoring, and incident response controls across their supply chain.

Source: The Hacker New | Read more →

Critical flaw in Microsoft WSUS exploited

A critical remote code execution vulnerability in Windows Server Update Services (WSUS), which was public since October 14, is being exploited in the wild. The flaw is specifically due to unsafe deserialization of AuthorizationCookie objects that are received by the GetCookie() endpoint. This endpoint decrypts encrypted cookies

using AES-128-CBC, and then deserializes them using BinaryFormatter without proper type validation.

CISO's takeaway: Organizations should apply the patch for CVE-2025-59287 as soon as possible. Furthermore, WSUS network access should be isolated.

Source: Huntress | Read more →

Cyber insights

On-prem VPNs more likely to suffer ransomware attacks

A report found that organizations using on-premise VPNs were nearly seven times more likely to suffer a ransomware attack. This elevated risk is due to the complexity of maintaining on-prem Next-Generation Firewalls (NGFWs) and VPNs, often leading to missed patches and outdated configurations.

CISO's takeaway: Deploying devices on-prem can be complex and time-consuming. Organizations should evaluate transitioning from on-premise VPNs to cloud-based Secure Access Service Edge (SASE) solutions to reduce their external attack surface and enforce strong MFA.

Source: CRN | Read more →

Harvard summarizes cyber and AI disclosures 2025

This Harvard Law School Forum post highlights that corporate board oversight of AI risk has nearly tripled in 2025, with almost half of companies now citing it as a major enterprise risk. Concurrently, companies are enhancing cybersecurity governance by increasingly aligning with external frameworks (like NIST CSF 2.0) and mandating director expertise and crisis preparedness exercises.

CISO's takeaway: Formalizing and documenting framework alignment generates trust, and more organizations are taking this route. Furthermore, organizations need to own AI security and risk to maintain this trust.

Source: Harvard Law School Forum on Corporate Governance | Read more →

Cloudflare insights

Cloudflare continuously enhances our security capabilities to address the very threats discussed above. Here's how our products and recent improvements provide tangible solutions:

Cloudflare AI Security Suite

Cloudflare has released its AI Security Suite, a set of tools that secure AI interactions by controlling data and managing risk across the AI lifecycle. The AI Security Suite protects AI from external threats, the use of AI by the workforce, protects data in AI prompts, and enables secure innovation of AI. Read more here.

State of the post-quantum Internet in 2025

Cloudflare has achieved a major milestone with over 50% of human-initiated traffic using post-quantum encryption (X25519MLKEM768), mitigating the "harvest-now / decrypt-later" quantum threat. This update details the urgent migration for key agreement and the more challenging path for post-quantum certificates / signatures, which is essential before the inevitable arrival of powerful quantum computers ("Q-day") between 2030-2035. A write-up on the timeline and issues encountered can be found here.

Missed us at Cloudflare's Global Connect?

Come chat to Cloudflare's Field CXO Team at the following events:

- Forrester Security & Risk Summit 2025: November 5–7, Austin, TX, US
- Evanta Dallas CISO Executive Summit: November 6, Dallas, TX, US
- Gartner IT Symposium/Xpo™ 2025 conference: November 10–3, Barcelona, Spain
- Gartner DACH CISO Executive Summit: November 25–26, Frankfurt, Germany
- AWS re:Invent: 2025: December 3, Las Vegas, NV, US
- Gartner Chicago CISO Executive Summit: December 10, Chicago, IL, US

In case you missed it...

Uncover the signal from the noise and focus on today's most important cybersecurity trends via our Security Signal series.

Each episode of the Security Signal podcast translates cybersecurity complexities into actionable intelligence for executives at the helm.

Security Signal: The Perimeter Problem

You can also read the full 2025 Cloudflare Security Signals report at cloudflare.com/signals.