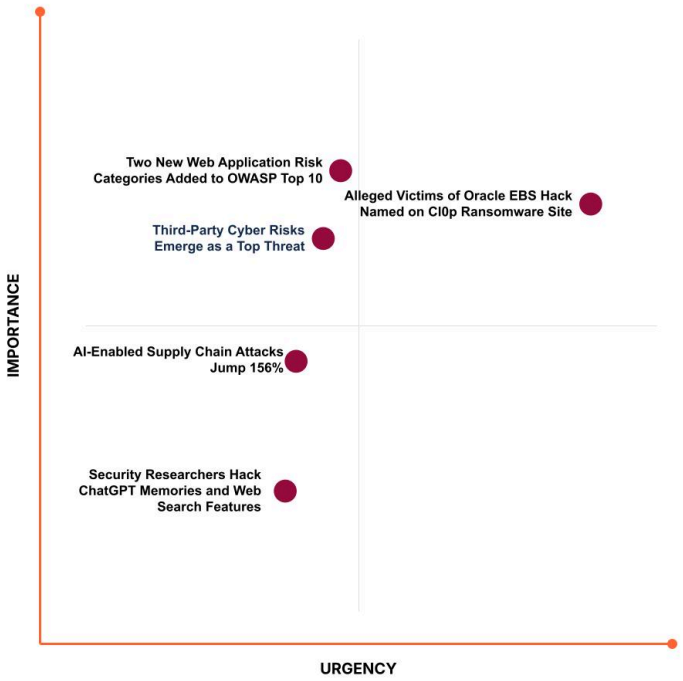
CLOUDFLARE

Cloudflare Cyber Briefing

November 14, 2025

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

What you need to know:



AI cybersecurity

AI-enabled supply chain attacks jump 156%

Malicious package uploads to open-source repositories surged by 156% in the last year, driven by AI-generated malware that is polymorphic, context-aware, and evasive. Traditional defenses like static analysis are failing against these advanced threats, with breach identification times potentially lengthening beyond the current 276-day average.

CISO's takeaway: Ensure that tools detect shapeshifting, deep-learning-powered malware in code dependencies. Implement a zero trust framework for all human and non-human identities accessing your supply chain assets.

Source: The Hacker News | Read more →

Security researchers hack ChatGPT memories and web search features

Researchers successfully demonstrated vulnerabilities in OpenAI's ChatGPT, specifically by manipulating its "Memories" and "Web Search" features. This highlights critical security gaps in large language models (LLMs) that could be exploited to leak sensitive data or manipulate model output.

CISO's takeaway: Define strict data loss prevention (DLP) policies to prevent sensitive enterprise data from reaching public LLMs used by employees. Secure your internal AI applications with granular access controls, guardrails, and API protection to prevent model manipulation.

Source: Tenable | Read more →

Cyber incidents

Alleged victims of Oracle EBS hack named on Cl0p ransomware site

We recently reported on the Oracle E-Business Suite (EBS) vulnerability. The Cl0p ransomware gang now has listed nearly 30 high-profile organizations, including industrial giants and major enterprises, as victims of a recent attack targeting Oracle EBS vulnerabilities. The incident underscores the continued risk of third-party software exploitation and the use of zero-day / unpatched flaws for massive data extortion.

CISO's takeaway: Verify all external-facing application APIs and endpoints for the latest patches and continuously monitor them for exploitation attempts. Apply a layered defense strategy including web application firewall (WAF) and distributed

denial-of-service (DDoS) protection in front of critical enterprise applications like Oracle EBS.

Source: SecurityWeek | Read more →

Cyber insights

Two new web application risk categories added to OWASP Top 10

The first new vision of the OWASP Top 10 since 2021 has been released, introducing two new categories. Supply chain risks take an increasing prominence replacing "vulnerable and outdated components" with a new category added for the "mishandling of exceptional conditions". Broken access control remains the top issue with security misconfiguration coming in a close second.

CISO's takeaway: Mandate security design reviews as a required gate in your SDLC to eliminate design-level flaws before coding begins. Utilize a unified security platform to continuously scan for integrity failures and policy violations across your application and API landscape. Ensure the WAF has updated rules to stop potential attacks.

Source: OWASP | Read more →

Third-party cyber risks emerge as a top threat

Recent major incidents, including an attack on a critical aviation technology provider, highlight that third-party cyber risk is now the most significant threat to operational resilience for enterprises. The impact is shifting from data breach fines to widespread, immediate, and systemic business disruption across multiple downstream organizations.

CISO's takeaway: Integrate third-party risk management (TPRM) into your business continuity planning to focus on recovery and resilience from a vendor outage. Enforce continuous, risk-based posture management for all high-risk, Internet-facing third-party applications using a comprehensive security platform.

Source: S&P Global | 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:

Your AI is only as good as its foundation
The shift to hyper-personalized AI apps built on "nanoservices" demands a new IT foundation beyond traditional hyperscalers. Cloudflare advocates for an edge platform that offers the necessary many-to-many scalability, statefulness, and cost-efficiency for secure AI agent deployment. More can be found here.

Cloudflare launches DIY BYOIP
Cloudflare has launched a self-serve Bring-Your-Own-IP (BYOIP) API, enabling customers to onboard and manage their own IP prefixes instantly without manual review. This DIY approach leverages the RPKI and secure ownership checks (IRR / rDNS) to streamline the process, replacing the complex, time-consuming requirement for physical Letters of Authorization (LOAs). More can be found here.

Come chat with Cloudflare's Field CXO team at the following events:

- Gartner DACH CISO Executive Summit, November 25–26, Frankfurt, DE
- AWS re:Invent 2025, December 1–5, Las Vegas, NV, US
- Gartner Seattle CIO & CISO Executive Summit, December 9, Seattle, WA, US
- Gartner Chicago CISO Executive Summit, December 10, Chicago, IL, US

Join the team at **The Trust Forward Summit by Cloudflare**, an exclusive side event at AWS re:Invent 2025 on Wednesday, December 3, connecting cybersecurity leaders, AI innovators, and technology executives to tackle the most pressing challenges in digital trust and AI-driven innovation.

Attendees will explore how to accelerate AI safely, secure AI systems, and harness AI for cybersecurity advantage, leaving with practical strategies, forward-thinking insights, and peer connections. We hope to see you there!

In case you missed it...

Resilience at scale used to be optional. Not anymore. A new generation of smarter, stronger, and faster global digital threats is creating heightened exposure across the pillars of the enterprise — finance, operations, compliance, security, and reputation — demanding a coordinated, C-suite-wide response. Read the full 2025 Cloudflare Security Signals report at **cloudflare.com/signals**.

Find more resources from the CXO team here:
Gregory Van den Top, Field CSO: Defend against rising app-layer DDoS attacks

DDoS attacks are rapidly changing in size and deployed tactics. Application-layer attacks are becoming more common, are cheaper and easier to launch, and apply different techniques. Some of these techniques blur the line between DDoS and more general app-layer tactics: They are used for data exfiltration as well as service denial. More can be found here.