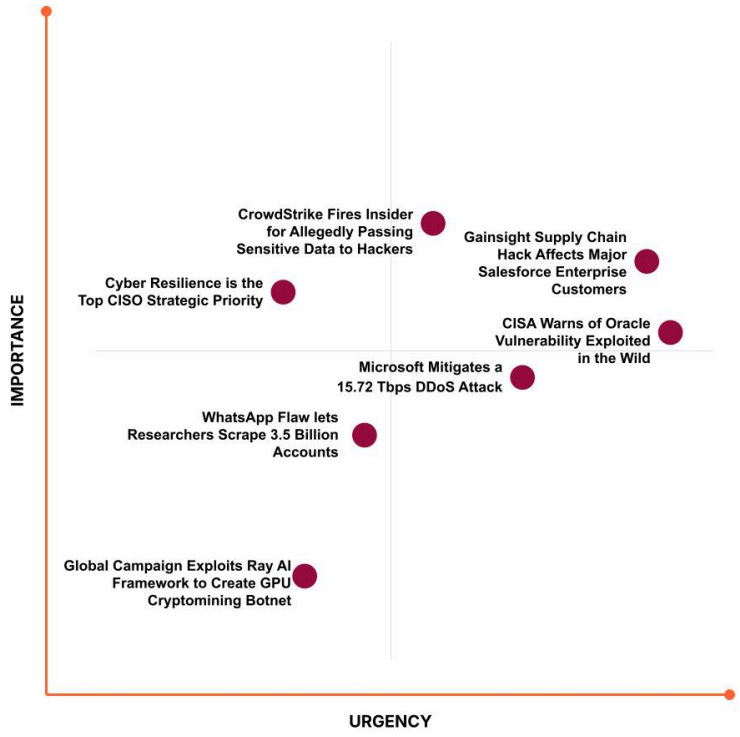
CLOUDFLARE

Cloudflare Cyber Briefing

November 28, 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

Global campaign exploits Ray AI framework to create GPU cryptomining botnet

A new campaign, dubbed ShadowRay 2.0, is exploiting a known, unauthenticated API flaw in the open-source Ray AI framework to hijack NVIDIA GPU clusters worldwide. Attackers automate the spread of their cryptocurrency mining payload by leveraging Ray's legitimate orchestration features.

CISO's takeaway: Secure all open-source AI infrastructure with virtual patching and strict access control to prevent resource hijacking and data leakage from your AI pipelines. Use WAF and API security to inspect and block unauthenticated traffic to Ray's Job Submission API and other exposed endpoints.

Source: Oligo | Read more →

Cyber incidents

Gainsight supply chain hack affects major Salesforce enterprise customers

A supply chain attack targeting CRM provider Gainsight's Salesforce connector potentially exposed customer data across multiple Fortune 500 enterprises. The incident underscores how compromise of a single third-party SaaS vendor can create a systemic breach across interconnected corporate environments.

CISO's takeaway: Mandate zero trust network access (ZTNA) and strong segmentation for all third-party SaaS connections and APIs to limit the blast radius of a breach. Use a robust cloud access security broker (CASB) to monitor and control data movement between your environment and critical SaaS platforms like Salesforce.

Source: Salesforce | Read more →

CrowdStrike fires insider for allegedly passing sensitive data to hackers

CrowdStrike confirmed it fired a suspicious employee who was allegedly passing confidential company and customer information to an outside hacking group. The incident highlights the persistent insider threat risk, particularly involving privileged access to sensitive customer data.

CISO's takeaway: Treat all privileged internal accounts as high-risk by enforcing granular, context-aware access controls and continuous behavioral monitoring. Use DLP and ZTNA solutions to detect and block abnormal data movement or access

patterns by authenticated employees.

Source: TechCrunch | Read more →

WhatsApp flaw lets researchers scrape 3.5 billion accounts

Researchers compiled a list of 3.5 billion WhatsApp mobile phone numbers and associated personal information by abusing a contact-discovery API that lacked rate limiting. The team reported the issue to WhatsApp, and the company has since added rate-limiting protections to prevent similar abuse.

CISO's takeaway: Use a web application firewall and API security to rate limit and secure exposed applications and APIs. Use bot management to identify sophisticated scrapers and malicious API calls, challenging or blocking them using advanced behavioral and machine learning analysis, regardless of volume.

Source: Universität Wien | Read more →

Microsoft mitigates a 15.72 Tbps DDoS attack

Azure automatically detected and mitigated a record-breaking multi-vector DDoS attack measuring 15.72 Tbps and nearly 3.64 billion packets per second (pps) on October 24, 2025. The attack, launched by the Aisuru botnet from over 500,000 source IPs, targeted a single endpoint in Australia, demonstrating the massive scale of modern threats.

CISO's takeaway: Verify your DDoS mitigation solution can handle Tbps-level, multi-vector attacks by using a global, distributed network that operates at the edge, close to the source. Conduct regular DDoS simulations to assess your operational readiness and ensure uninterrupted service availability for all Internet-facing workloads.

Source: Microsoft | Read more →

Cyber insights

Cyber resilience is the top CISO strategic priority

Gartner's latest CISO survey reveals that "Cyber Resilience" is now the top strategic priority, moving past the aim of preventing every breach, to instead focus on sustaining business operations under persistent attack. This requires full coordination across IT, legal, and business continuity planning.

CISO's takeaway: Integrate cyber-specific resilience planning (DR / BCP) with network and application continuity services to ensure a minimum viable company. Utilize resilient application architectures and attack mitigations to fail over or absorb attacks while ensuring a swift response to potential incidents.

Source: Gartner | Read more →

CISA warns of Oracle vulnerability exploited in the wild

The US Cybersecurity and Infrastructure Security Agency (CISA) on November 21, 2025 added a critical security flaw impacting Oracle Identity Manager to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation. The vulnerability in question is CVE-2025-61757 (CVSS score: 9.8), a case of missing authentication for a critical function that can result in pre-authenticated remote code execution.

CISO's takeaway: Apply the Oracle Critical Patch Update as soon as possible. Apply a zero trust approach to all applications and apply continuous monitoring for suspicious behavior.

Source: CISA | 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 outage on November 18, 2025

On November 18 at 11:20 UTC, Cloudflare's network began experiencing significant failures to deliver core network traffic. This showed up to Internet users trying to access sites as an error page indicating a failure within Cloudflare's network. More can be found here.

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

- 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...

Replicate is joining Cloudflare. This acquisition will accelerate the company's vision to make Cloudflare Workers the leading end-to-end platform for building and running scalable, fast, and reliable AI applications. Soon, developers building on Cloudflare will be able to access any AI model globally with just one line of code. Read more.

Find more resources from the CXO team below:
Daniel Creed, Field CISO: Serving up coffee networking - enabling secure remote access, with a side of network simplification. Learn more.