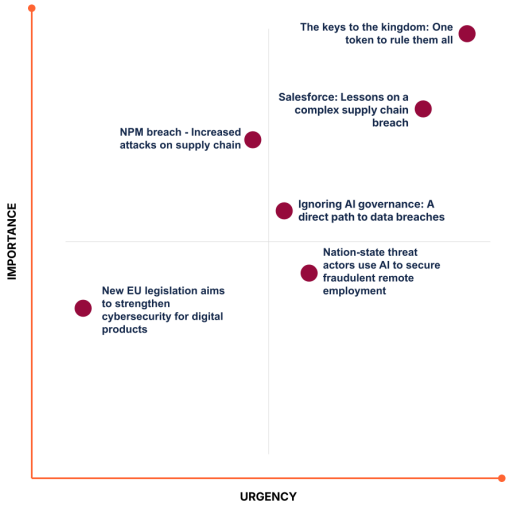
CLOUDFLARE

Cloudflare Cyber Briefing

September 19, 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:



Cyber insights

The keys to the kingdom: One token to rule them all

Microsoft has mitigated a critical Entra ID token validation vulnerability (CVE-2025-55241) that could have allowed cross-tenant impersonation via legacy Actor tokens and the Azure Active Directory (AD) Graph API. While Microsoft deployed mitigations, the issue's lack of logging means customers should investigate and harden immediately.

CISO's takeaway: Please take these steps now: Rotate app / service principal credentials, review and remove unused app permissions, reduce Global Admin counts and enable phishing-resistant MFA, and run the supplied detection queries. If you'd like assistance, our IR team (Cloudforce One R.E.A.C.T) can run an investigation and provide a remediation report.

Source: dirkjanm.io *Read more →*

Salesforce: Lessons on a complex supply chain breach

A major supply chain attack targeting a Salesforce CRM integration led to data breaches at multiple large organizations, including TransUnion, Farmers Insurance, Workday, and Google. The threat actor executed queries to retrieve information associated with Salesforce objects such as Cases, Accounts, Users, and Opportunities. For example, the threat actor ran the following sequence of queries to get a unique count from each of the associated Salesforce objects:

Query to Retrieve User Data

```
SELECT Id, Username, Email, FirstName, LastName, Name, Title, CompanyName,
Department, Division, Phone, MobilePhone, IsActive, LastLoginDate,
CreatedDate, LastModifiedDate, TimeZoneSidKey, LocaleSidKey,
LanguageLocaleKey, EmailEncodingKey
FROM User
WHERE IsActive = true
ORDER BY LastLoginDate DESC NULLS LAST
LIMIT 20
```

The attack vector was linked to the compromise of a third-party application, highlighting the critical risks associated with vendor and partner ecosystems. It underscores an era where the attack surface is expanding beyond vendors and partners that you can adequately assess or even be aware of.

CISO's takeaway: The incident highlights the diminishing returns we're getting from traditional point-in-time vendor risk assessments. The number of acquisitions, integrations, and inherited permissions will have shifted during the process of it being completed. Supply chain assurance will increasingly need to be built on continuous, real-time visibility to monitor behavior and data, rather than on static trust assessments on vendors.

Sources: IT Governance *Read more →* , CSO online *Read more →*, and Google Cloud Blog *Read more →*.

New EU legislation aims to strengthen cybersecurity for digital products

The EU's Cyber Resilience Act, which entered into force in late 2024, is now a major topic as organizations prepare for compliance. The act mandates that manufacturers and retailers of products with digital elements ensure robust cybersecurity throughout

their lifecycle, placing a new legal burden of care on vendors to create secure-by-design products.

CISO's takeaway: Manufacturers must comply with vulnerability reporting requirements by September 11, 2026. CRA obligations will be fully applicable by December 11, 2027.

Source: European Commission *Read more →*

AI cybersecurity

Nation-state threat actors use AI to secure fraudulent remote employment

Recent reporting shows North Korean state-sponsored operatives are using AI (deepfakes, resume / identity forgery, facilitators, etc.) to secure remote employment in tech roles at firms in the US and other Western countries. This new tactic allows them to bypass traditional hiring checks and gain a foothold inside target organizations, eliminating previous training and language barriers.

CISO's takeaway: CISOs need to strengthen hiring and onboarding by enforcing robust identity verification (including liveness checks, deepfake detection, and thorough background validation) while training HR and recruiters to spot fraud red flags. While currently small in scale, the ease of such attacks will continue to elevate insider risks if not adequately countered.

Source: Anthropic *Read more →*

Ignoring AI governance: A direct path to data breaches

An IBM survey shows most enterprises lack strong AI policies. Nearly all AI-related breaches hit organizations without access controls, while shadow AI drove one in five breaches. IBM put the rise of shadow AI in the top three most costly breach factors, outpacing security skills shortages. Governance, approvals, and audits are now essential safeguards.

CISO's takeaway: Establish clear AI governance frameworks, including data access policies, model validation, and usage guidelines. Conduct regular audits to identify and mitigate shadow AI instances within your organization.

Source: IBM survey *Read more →*

Cyber incidents

NPM breach — Increased attacks on supply chain

An npm software supply chain attack compromised a developer's account through social engineering and injected malicious code into widely used open-source packages. The attack was quickly detected and contained, limiting the impact despite the potential for widespread damage. The incident highlights the importance of rapid incident response and the role of the open-source community in mitigating threats.

CISO's takeaway: Review and enhance security protocols for software supply chains, particularly for open-source dependencies. Emphasize the need for two-factor authentication and educate developers on social engineering risks to prevent account compromise.

Source: CyberScoop *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:

The impact of the Salesloft Drift breach on Cloudflare

- Cloudflare's Salesloft Drift incident postmortem details a supply chain attack that impacted Cloudflare and hundreds of other companies. The breach, which occurred between August 9 and August 17, 2025, involved a threat actor named GRUB1, who exploited an OAuth credential from the Salesloft Drift chatbot's Salesforce integration. The attacker gained unauthorized access to Cloudflare's Salesforce tenant, which is used for customer support and case management. The breach was limited to text fields within Salesforce case objects.
- While Cloudflare does not require sensitive data in support cases, customers may have inadvertently included information such as **API tokens or logs**. This data should be considered compromised. No Cloudflare services or infrastructure were affected. Cloudflare's response included immediately containing the threat, securing their third-party ecosystem, and conducting a comprehensive analysis of the customer impact. We **rotated all 104 of our own API tokens** found in the compromised data and directly notified all affected customers.

Defending against AI infrastructure flaws (like NVIDIA Triton)

- Cloudflare's zero trust platform (Cloudflare One) can enforce granular access controls to your AI infrastructure, ensuring only authorized users and services can reach your NVIDIA Triton servers, even if a vulnerability is exploited at the application layer. This limits the blast radius.

- The Cloudflare Web Application Firewall (WAF) can be configured to detect and block malicious payloads targeting known vulnerabilities in web-facing AI inference APIs, providing a critical layer of defense until patches are applied.

Mitigating stealthy bots and evasive crawlers

- Cloudflare Bot Management offers industry-leading detection of sophisticated bots, including AI-powered stealth crawlers. It uses behavioral analysis, machine learning, and threat intelligence to identify and mitigate malicious automated activity, even when bots attempt to mimic legitimate user behavior or bypass robots.txt directives. This ensures your digital assets are protected from unwanted scraping, competitive intelligence gathering, and data exfiltration.
- Our WAF works in conjunction with Bot Management to block requests from known malicious bot networks and enforce granular rules based on traffic patterns and signatures associated with evasive crawlers.
- **Recent security enhancement:** We recently rolled out enhanced machine learning models for our Bot Management service, improving the detection rate of novel and rapidly evolving AI-driven bot techniques by **15%** in the past quarter, particularly targeting generative AI-powered scraping attempts.

AI agents are coming: Get security and governance ready

- AI agents are arriving fast and bring important risks — such as prompt manipulation, data leakage, and accountability gaps. A three-pillar framework of technical, operational, and compliance controls is needed. Success requires coordination across the enterprise, not just one team.
- Develop a cross-functional strategy for secure AI agent adoption. Implement technical controls like input validation and output sanitization, and establish clear operational procedures for agent deployment and monitoring.

Product launches

- Generative AI tools present a trade-off of productivity and data risk. Cloudflare One's new AI prompt protection feature provides the visibility and control needed to govern these tools, allowing organizations to confidently embrace AI.
- Cloudflare will provide confidence scores within our application library for GenAI applications, allowing customers to assess their risk for employees using shadow IT.
- Cloudflare CASB now scans ChatGPT, Claude, and Gemini for misconfigurations, sensitive data exposure, and compliance issues, helping organizations adopt AI with confidence.
- Cloudflare MCP Server Portals are now available in Open Beta. MCP Server Portals are a new capability that enable you to centralize, secure, and observe every MCP connection in your organization.

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.

Episode 1 — Security Signal: In Our Post-Quantum Era

Read the full 2025 Cloudflare Signals Report: Resilience at Scale

Find more resources from the CXO team here:
Dan Kent: Safeguarding critical infrastructure organizations — Using IT cybersecurity to prevent operational disruption
Trey Guinn: How to avoid outages in financial services — Three models for maximum uptime in financial services