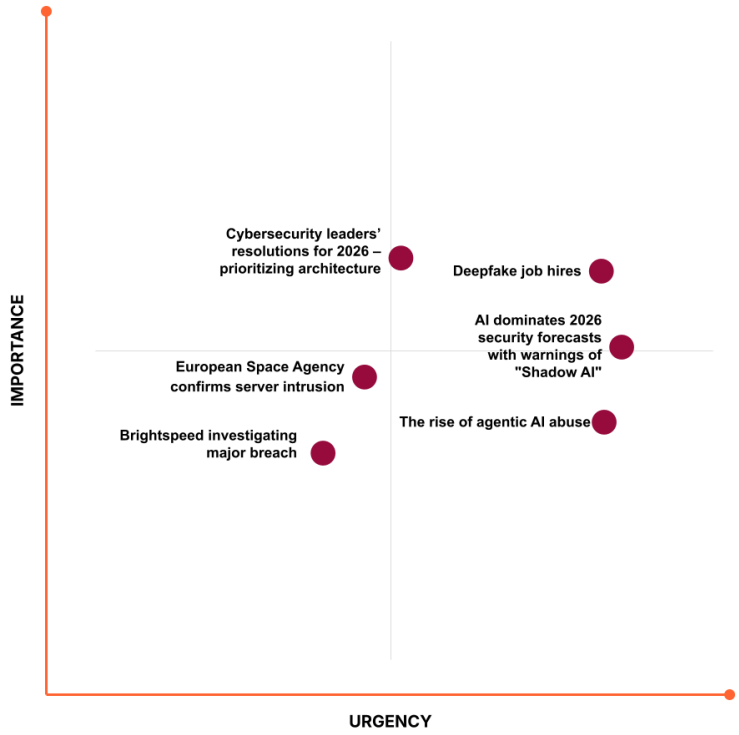
CLOUDFLARE

# Cloudflare Cyber Briefing

**January 9, 2026**

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 dominates 2026 security forecasts with warnings of "Shadow AI"

Security experts predict that 2026 will mark the first major AI-driven attack resulting in significant financial damage, driven largely by unmanaged "Shadow AI" tools. These unauthorized autonomous agents are increasingly leaking personally identifiable information and intellectual property as they operate outside traditional governance frameworks.

**CISO's takeaway:** To prevent unauthorized AI tools from becoming a silent conduit for data exfiltration, organizations must move beyond simple blocking. By deploying an AI-specific gateway, you can gain full observability into every prompt and response, while data loss prevention policies automatically redact sensitive code or customer data before it reaches external LLM providers.

Source: TechNewsWorld | Read more →

---

### Deepfake job hires

A new surge in "deepfake job hires" involves threat actors using real-time AI video and audio cloning to successfully pass remote interviews and secure positions at high-value targets. Once onboarded, these fraudulent employees use their legitimate access to plant backdoors or exfiltrate sensitive datasets from within the corporate perimeter.

**CISO's takeaway:** Traditional interview processes are no longer a reliable identity check in an age of real-time cloning. During the remote interviewing process, verify the digital footprint (e.g. through IP and geo tracking) or use specialized tools that require a "proof of life." Once hired, protecting the enterprise from these sophisticated insiders requires a shift to a zero trust architecture that continuously verifies every user and device posture, complemented by client certificates to ensure that only cryptographically verified hardware can access sensitive internal systems.

Source: The Hacker News | Read more →

## Cyber incidents

### European Space Agency confirms server intrusion

The ESA has admitted to a breach involving external collaborative servers, which reportedly resulted in the theft of 200 GB of data. The stolen material includes source code, API tokens, and CI/CD pipeline configurations, potentially exposing scientific supply chains.

**CISO's takeaway:** Data breaches often start at the developer and administrative interface level, even if the data on these servers is not necessarily critical. Utilizing a zero trust architecture can provide posture verification and additional controls, while sensitive API endpoints need protection from unauthorized automated access.

Source: TechRepublic | Read more →

---

### Brightspeed investigating major breach

The Crimson Collective hacking group has claimed responsibility for a significant data theft involving the personal information of more than one million Brightspeed customers. The telecommunications provider is currently investigating the scope of the unauthorized access to its internal systems.

**CISO's takeaway:** Mass exfiltration often stems from compromised internal credentials or lateral movement within the network. Protecting large-scale customer databases requires a move to a zero trust model that enforces strict, contextual access controls and eliminates the risk of single-point credential failures.

Source: SecurityWeek | Read more →

## Cyber insights

### The rise of agentic AI abuse

As companies deploy autonomous AI agents to automate business workflows, threat actors are shifting their focus toward "agentic manipulation" to hijack corporate logic. Strategic priorities for 2026 are pivoting toward resilience and recovery rather than just prevention.

**CISO's takeaway:** As automated links in the network multiply, manual permission management becomes impossible. Transitioning to a secure access service edge (SASE) model with built-in AI security provides the necessary global visibility and automated policy enforcement to manage both human and machine identities at scale.

Source: Dark Reading | Read more →

---

### Cybersecurity leaders' resolutions for 2026 — Prioritizing architecture

Leading CISOs are resolving to prioritize "intentional design" over reactive security, focusing on understanding end-to-end dependencies to prevent cascading failures. The goal is to build technology and security investments that are built to endure and evolve rather than just survive the next incident.

**CISO's takeaway:** Architectural resilience requires a fundamental move toward "failing small" and isolating blast radiuses. By leveraging global network-as-a-service connectivity, you can design a more resilient architecture that automatically reroutes traffic around failures and enforces consistent security policies regardless of where your applications or users are located.

Source: CSO Online | Read more →

# Cloudflare insights

### The 2025 Cloudflare Radar Year in Review

Cloudflare's 2025 Year in Review reveals a digital landscape defined by a 19% surge in global traffic, the explosive rise of AI-powered crawling, and a record-breaking year for DDoS attacks and post-quantum encryption adoption. More can be found here.

---

### Cloudflare's H1 2025 transparency report

Cloudflare's H1 2025 transparency report provides a comprehensive breakdown of the legal requests and abuse reports managed during the first half of the year, reinforcing the company's commitment to user trust. More can be found here.

---

### Code Orange: Fail Small — A plan for platform resilience

Cloudflare's "Code Orange" initiative outlines a strategic engineering shift toward a "Fail Small" architecture designed to prevent global outages by ensuring technical failures remain localized and manageable. More can be found here.

# CXO events and resources

Join Cloudflare at **Trust Forward 2026**, an exclusive executive side event at RSA on Wednesday, March 25, bringing together cybersecurity leaders, AI innovators, and technology executives for candid, peer-level dialogue. Trust Forward is designed as a forum for sharing real-world experiences and insights on the challenges reshaping trust, resilience, and risk across today's digital enterprises.

Attendees will engage in focused discussions on accelerating AI responsibly, securing autonomous and machine-to-machine systems, managing third- and fourth-party risk, and turning threat intelligence into meaningful business insight. The summit offers practical perspectives, forward-looking thinking, and the opportunity to connect with peers facing the same pressures at the intersection of security, innovation, and trust.

---

Find more resources from the CXO team here:
**James Todd, Field CTO:** Beyond signatures: Modernizing SecOps — Using AI behavioral detection to outpace advanced attackers

**Nan Hao Maguire, Field CTO:** The bot-dominated Internet: Identifying intent in the age of automation