CLOUDFLARE

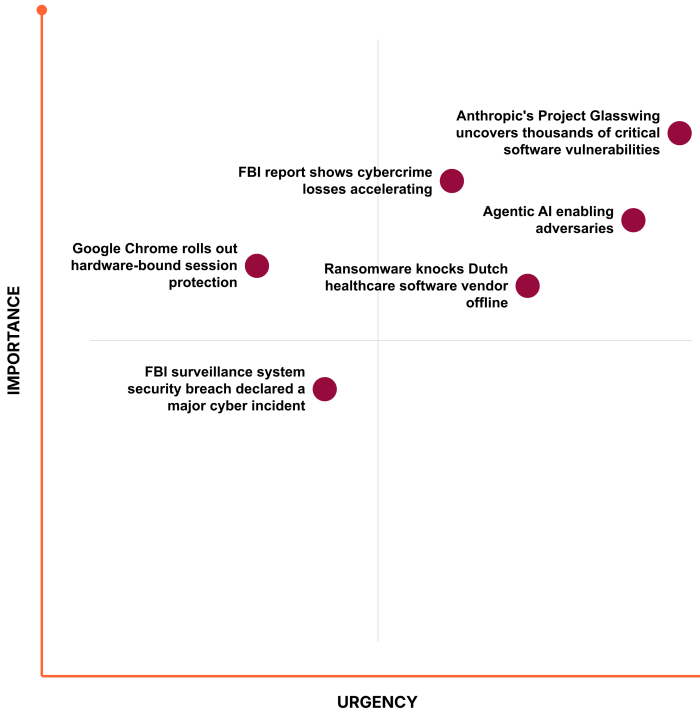
Cloudflare Cyber Briefing

April 17, 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.

The "AI Vulnerability Storm: Building a Mythos-Ready Security Program" has been released, built by 60+ contributors from Cloud Security Alliance, SANS, OWASP GenAI Security Project, and [un]prompted. Read here.

What you need to know:



AI cybersecurity

Anthropic's Project Glasswing uncovers thousands of critical software vulnerabilities

Anthropic has unveiled Project Glasswing, an initiative leveraging its unreleased Claude Mythos Preview AI model. This model has already autonomously identified thousands of high-severity vulnerabilities across major operating systems and web browsers.

CISO's takeaway: The emergence of AI models capable of autonomously discovering critical vulnerabilities necessitates a proactive and adaptive defense strategy. CISOs must invest in platforms that integrate advanced behavioral analytics to detect anomalous activities that could indicate AI-driven exploits. Implement robust application security services, including web application and API protection, to guard against newly discovered or exploited flaws, even zero-day exploits. Additionally, foster a culture of rapid patching and vulnerability management, leveraging tools that can automate vulnerability scanning and prioritize remediation efforts based on real-world exploitability.

Source: Anthropic

Agentic AI enabling adversaries

A new threat intelligence report highlights that agentic AI is enabling adversaries to automate multi-stage attacks with minimal human oversight. This technology allows for rapid adaptation during penetration testing, targeting endpoints continuously and shifting tactics as defenses respond.

CISO's takeaway: Traditional, reactive security operations cannot keep pace with the speed of autonomous AI agents. CISOs must pivot to automated bot management that uses behavioral analysis at the edge to identify and neutralize AI-orchestrated probes before they reach your application infrastructure.

Source: National Defense Magazine

Cyber incidents

FBI surveillance system security breach declared a major cyber incident

The FBI announced a major cyber intrusion into its surveillance systems, with Chinese-affiliated hackers suspected of targeting sensitive law enforcement information in March. It has now been escalated to a Major Cyber Incident. This incident highlights critical risks to national security and the vulnerability of even highly secured government networks.

CISO's takeaway: CISOs should enforce stringent security controls and continuous monitoring for all third-party vendors with access to sensitive systems or data. Implement a strong identity and access management framework with multi-factor authentication (MFA) for all users and systems, including vendors. Utilize a global network for distributed-denial-of-service (DDoS) protection and DNS security to safeguard against external threats and ensure the integrity of critical infrastructure, while employing web application firewall (WAF) services to protect against exploitation of vulnerabilities in Internet-facing applications.

Source: CPO Magazine

Ransomware knocks Dutch healthcare software vendor offline

ChipSoft, a major Dutch healthcare software vendor, was hit by a ransomware attack on April 7, 2026, causing a significant outage. This incident impacted patient record software used by approximately 80% of hospitals in the Netherlands, demonstrating systemic risk.

CISO's takeaway: CISOs in all sectors, particularly healthcare, must meticulously audit their vendor dependencies and implement rigorous vendor security programs. Deploy advanced threat intelligence and DNS filtering to block known ransomware command and control infrastructure. Utilize email security services to prevent phishing attempts, a common initial vector for ransomware. Furthermore, ensure robust data backup and recovery strategies are in place and regularly tested, coupled with a zero trust architecture to minimize the blast radius of any successful intrusion.

Source: The Record

Cyber insights

FBI report shows cybercrime losses accelerating

The FBI IC3 annual report revealed cybercrime losses grew 26% to $20.9 billion in 2025. Investment fraud, BEC, and tech support scams dominated. Victims over 60 suffered disproportionate losses. The report notes AI will continue driving cyber threat evolution.

CISO's takeaway: Cybercrime economics favor attackers at current defense investment levels. Security spending must increase to match the loss trajectory. Investment fraud and BEC schemes target process weaknesses more than technical vulnerabilities. Focus on business process controls for financial transactions, not just technical controls. Implement out-of-band verification for financial transactions and wire transfers. Support with technical controls to prevent phishing and automated fraud attempts.

Source: CyberScoop

Google Chrome rolls out hardware-bound session protection

Chrome 146 for Windows introduces Device Bound Session Credentials (DBSC), cryptographically linking session cookies to hardware TPM chips. The protection prevents infostealer malware from exfiltrating and using session tokens on other devices. Okta partnership demonstrated significant reduction in session theft during testing.

CISO's takeaway: Hardware-backed authentication represents the future of session security. Evaluate web applications for DBSC implementation. This mitigates the primary vector for account takeover following endpoint compromise. CISOs should ensure that even if the endpoint is compromised, the blast radius is contained through zero trust architecture, browser isolation, and data-centric security controls. The combination provides defense in depth against the infostealer epidemic.

Source: BleepingComputer

Cloudflare insights

Agents Week

Cloudflare's mission has always been to help build a better Internet. Sometimes that means building for the Internet as it exists. Sometimes it means building for the Internet as it's about to become. This week, we kicked off Agents Week, dedicated to what comes next. More can be found here.

---

500 Tbps of capacity: 16 years of scaling our global network

Cloudflare's global network has officially crossed 500 Tbps of external capacity, enough to route more than 20% of the web and absorb the largest DDoS attacks ever recorded. More can be found here.

Cloudflare targets 2029 for full post-quantum security

Recent advances in quantum hardware and software have accelerated the timeline on which quantum attack might happen. Cloudflare is responding by moving our target for full post-quantum security to 2029. More can be found here.

CXO events and resources

The 2026 Cloudflare Security Signals Report is now available. This year's report provides a map to hidden fault lines, the enterprise risks that only emerge as speed, scale, and disruption increase. Discover ways to identify and address these fault lines before they become major ruptures.

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

- SINETSilicon Valley, April 21, Mountain View, CA, US
- Immerse Montreal, April 22, Montreal, Canada
- Immerse Minneapolis, April 23, Minneapolis, MN, US
- Gartner Houston CISO Executive Summit, May 6, Houston, TX, US
- Immerse SoCal, May 6, Anaheim, CA, US
- Gartner, Charlotte CIO & CISO Executive Summit, May 7, Charlotte, NC, US

Find more resources from the CXO team here.