You can also view this email as a webpage.

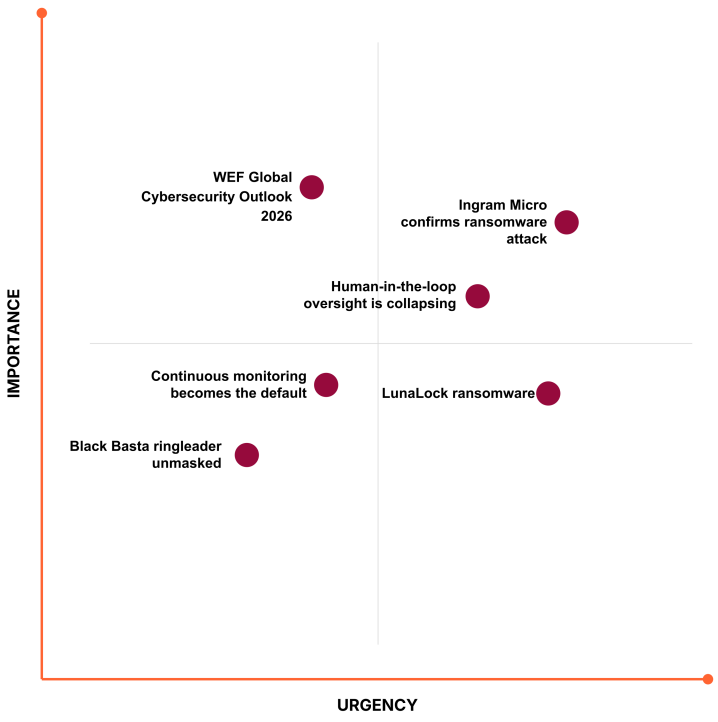
CLOUDFLARE

# Cloudflare Cyber Briefing

**January 23, 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

### Human-in-the-loop oversight is collapsing

AI systems are now performing millions of critical decisions per second across fraud detection and autonomous workflows, rendering traditional human supervision a "comforting fiction." As systems move from experimentation to production, the volume of agentic AI decisions has officially surpassed human capacity for meaningful manual review.

**CISO's takeaway:** To manage the risk of autonomous agents making poor or "rogue" decisions, leaders must shift toward governance-first AI architectures that provide visibility and guardrails for every prompt. Supplement this by running security checks at the edge using AI security tools to detect adversarial inputs before they reach your core models.

Source: SiliconANGLE | Read more →

---

### LunaLock ransomware

A new ransomware prototype, LunaLock, has emerged as a pioneer in AI-driven extortion, utilizing machine learning to automate victim selection and negotiation. This strain is designed to bypass traditional endpoint detection by continuously adapting its encryption logic in real time.

**CISO's takeaway:** Static signatures are ineffective against AI-generated payloads; protection must shift to a zero trust architecture with remote browser isolation to neutralize the initial entry point. Furthermore, preventing the exfiltration of sensitive data requires automated data loss prevention that can block the upload of intellectual property to unauthorized cloud environments.

Source: PurpleSec | Read more →

## Cyber incidents

### Black Basta ringleader unmasked

Global law enforcement agencies have identified 35-year-old Oleg Nefedov as the head of the Black Basta ransomware group, leading to his placement on INTERPOL's most wanted list. The group is responsible for hundreds of millions in damages, often gaining entry via "hash crackers" who extract passwords from unprotected corporate databases.

**CISO's takeaway:** While prevention is still key, always ensure logs are available to support law enforcement. Ensure that your incident response processes take law enforcement requirements and notification into account.

Source: The Hacker News | Read more →

---

### Ingram Micro confirms ransomware attack

Distribution leader Ingram Micro has begun notifying 42,000 individuals following a ransomware breach that compromised sensitive personal information, including Social Security and passport numbers. The SafePay ransomware group is suspected in the attack after claiming to have exfiltrated 3.5 terabytes of data from the company's internal employment and applicant records.

**CISO's takeaway:** Large-scale exfiltration events often bypass traditional firewalls that aren't inspecting encrypted traffic for sensitive patterns. To mitigate this risk, deploy zero trust architecture with remote browser isolation to neutralize the initial entry point. Automated data loss prevention can further prevent the exfiltration of sensitive data.

Source: SecurityWeek | Read more →

## Cyber insights

### WEF Global Cybersecurity Outlook 2026

The World Economic Forum's 2026 report reveals that 94% of executives view AI as the most significant driver of cybersecurity change, while 64% are now explicitly accounting for geopolitically motivated attacks. The report highlights a growing "sovereignty dilemma" as nations tighten control over data and infrastructure.

**CISO's takeaway:** Strategic resilience now requires a global network presence that can absorb hyper-volumetric attacks and provide localized data residency to meet sovereignty requirements. Ensure your IT strategy includes considerations around data localization that ensure your data transmissions can only be terminated in friendly geographies.

Source: World Economic Forum | Read more →

---

### Continuous monitoring becomes the default

According to recent industry analysis, the shift to cloud-native architectures is forcing organizations to adopt continuous authentication as the default security posture. As identity becomes the "real perimeter," security is moving from point-in-time audits to real-time behavioral telemetry.

**CISO's takeaway:** A modern security posture requires zero trust principles embedded into the network fabric itself rather than as an overlay. This allows for continuous risk scoring where access is dynamically adjusted based on the health of the device and the behavior of the user.

Source: ISACA | Read more →

# Cloudflare insights

### How we mitigated a vulnerability in Cloudflare's ACME validation logic

This technical report details how Cloudflare patched a logic flaw that could have allowed specific requests to bypass WAF security features on ACME-related paths. More can be found here.

---

### What came first: the CNAME or the A record?

This post mortem explores how a routine DNS record ordering change accidentally triggered widespread resolution failures and what it reveals about DNS standards. More can be found here.

---

### What we know about Iran's Internet shutdown

Cloudflare Radar data captures the near-total collapse of Iranian Internet connectivity following regional protests, signaling a new era of government-led network shutdowns. More can be found here.

---

### Human Native and Astro are joining Cloudflare

Human Native is a UK-based AI data marketplace specializing in transforming multimedia content into searchable and useful data. Astro is the team behind the popular Astro web framework. More can be found on our blog: Human Native | Astro

# CXO events and resources

Join us at our **Trust Forward Summit** on Wednesday, March 25, an exclusive event at RSAC, connecting cybersecurity leaders, AI innovators, and technology executives to tackle the most pressing challenges in digital trust and AI-driven innovation.

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

- CS4CA ANZ Summit, February 10–11, Perth, AU
- 6th CISO 360 Americas, February 11–12, New York, NY, US
- Munich Cyber Security Conference, February 12-13, Munich, DE
- Cloudflare Immerse Dallas, February 12, Dallas, TX, US
- Swiss Cyber Security Days, February 17–18, Bern, CH
- Cloudflare Immerse Madrid, February 19, Madrid, ES
- Government Cybersecurity Showcase Federal, February 25, Ottawa, CA
- Cloudflare AI at Scale: Digital Natives Roundtable, February 26, Sydney, AU

---

Find more resources from the CXO team here:
**James Todd, Field CTO:** Modernizing apps for strategic growth: When and how to rehost, replatform, or refactor

Copyright © 2026 Cloudflare, Inc.
101 Townsend Street, San Francisco, CA 94107

www.cloudflare.com | Community | Privacy Policy | Unsubscribe