CLOUDFLARE

2025

Cloudflare Signals Report

Resilience at Scale

FOREWORD BY MICHELLE ZATLYN

We are living in unprecedented times. Technology is advancing at a dizzying pace.

From the explosive rise of generative AI — full of both promise and fear — to increasingly ever-present cyber threats, and from a new paradox of a hyper-connected world to the implications for local societies and a global economy, the only constant seems to be change. The rules of the game are in constant flux, and if our playbook is not continuously refined, it will quickly be obsolete.

That's why I'm proud to introduce the inaugural edition of the ***Cloudflare Signals Report***: an annual report outlining cybersecurity trends and findings critical to building a game plan that's right for you.

Cloudflare protects 20% of the world's websites and blocks an average of more than 227 billion cyber threats each day. That gives us a very interesting vantage point. We see more than just data — we see patterns, behaviors, and inflection points that signal where the world is heading.

What we know to be true: AI-driven threats require AI-powered defenses. Zero Trust must be the standard. Post-quantum readiness is not a tomorrow problem — it needs to happen today. And, all of this requires C-suite engagement and endorsement. **Resilience is not optional: it's vital.**

The ***Cloudflare Signals Report*** is intentionally designed to provide insights into the forces shaping the security landscape to help businesses of all sizes, governments, and individuals across the globe make informed decisions optimized for resilience.

We are on a mission to help build a better Internet, and that starts with helping you succeed.

Michelle Zatlyn
Co-founder and President,
Cloudflare

EXECUTIVE SUMMARY

In 2025, resilience at scale is no longer optional — it's a defining test of leadership.

As digital threats grow more complex and geopolitical volatility intensifies, every corner of the enterprise — finance, operations, compliance, and reputation — faces heightened exposure. AI-powered attacks, shifting regulatory frameworks, and sprawling digital ecosystems demand a coordinated, C-suite response.

The *2025 Cloudflare Signals Report* highlights five critical fault lines where resilience must be built in, not bolted on. Together, they reveal a new mandate for executive teams: to embed resilience into the core of how the business operates, innovates, and grows — at scale.

Savvy business leaders see a clear shift: resilience is no longer the responsibility of a single function — it's a shared, strategic priority for the entire C-suite. Leading enterprises are moving beyond reactive defenses toward proactive, intelligence-driven, and scalable technology environments, integrated across the business. Those that approach resilience as a shared C-suite responsibility and driver of growth, not just a safeguard, will be best positioned to lead in an increasingly volatile world.

This report highlights Cloudflare's commitment to building a secure, performant, and resilient digital ecosystem — at scale, enabling businesses of all sizes to withstand disruptions and operate with confidence at global scale.

Five critical fault lines

where resilience must be built in, not bolted on.

1

AI-powered threats and insider risks

demand close **CTO collaboration**, as adversaries now use AI to automate and scale attacks faster than traditional defenses can respond. AI-driven threats require AI-powered defenses, capable of adapting in real time. Automating these capabilities not only increases coverage but enables organizations to scale their defenses without slowing the pace of business.

2

Zero Trust, identity protection, and cloud complexity

require **CIO leadership**, as companies move beyond perimeter-based models to identity-first frameworks. Zero Trust has become the de facto standard for scalable, cloud-native risk management — ensuring usability, visibility, and control across distributed systems.

3

Resilience is no longer optional

for **CFOs and CROs**. As third-party risk grows and regulatory frameworks expand, finance and risk leaders must ensure investments go beyond mitigation, driving operational continuity, compliance automation, and scalable governance. Resilience at this level must be proactive, embedded, and cost-efficient — not a patchwork of point solutions.

4

Data privacy and post-quantum readiness

require early **CPO involvement**. With quantum computing poised to break traditional encryption, future-proofing data requires immediate action. Leaders must accelerate the adoption of post-quantum cryptography to protect long-lived data and meet evolving regulatory expectations.

5

Geopolitical risk and targeted cyber operations

demand direct **CEO and board engagement**. As state-sponsored campaigns increasingly target leadership, supply chains, and global operations, resilience must scale to the top of the house — supported by real-time intelligence, executive readiness, and cross-border coordination.

> "AI-powered attacks, shifting regulatory frameworks, and sprawling digital ecosystems demand a **coordinated, C-suite response.**"

Content

1

Mirror match: Defending the enterprise in the age of adversarial AI

Mirror match: Defending the enterprise in the age of adversarial AI

AI-driven cyber threats are evolving at an unprecedented pace, making traditional security approaches ineffective. Attackers now use AI to automate attacks, evade detection, and exploit vulnerabilities faster than organizations can respond. The shift from passive defense to proactive, AI-driven security is no longer optional — it is essential.

AI-powered attacks are already causing real business impact. Seventy-four percent of IT security professionals report that AI-driven threats are significantly affecting their organizations.[1] Deepfake scams, such as fraudulent video calls, have resulted in millions in losses, with one case in Australia leading to a $25 million theft.[2] AI-generated phishing attacks are becoming more convincing, while AI-enhanced malware adapts to evade traditional defenses.

Beyond direct attacks, AI is fueling misinformation campaigns, data poisoning, and model manipulation, potentially compromising AI-driven systems.

Enhanced attacker productivity straining security teams

Many AI-enabled tools may not unlock breakthrough attack techniques, but these tools can help adversaries improve productivity, efficiency, and the volume of attacks. These tools speed up tasks such as crafting phishing emails and using “dark chatbots” for help coding malware.

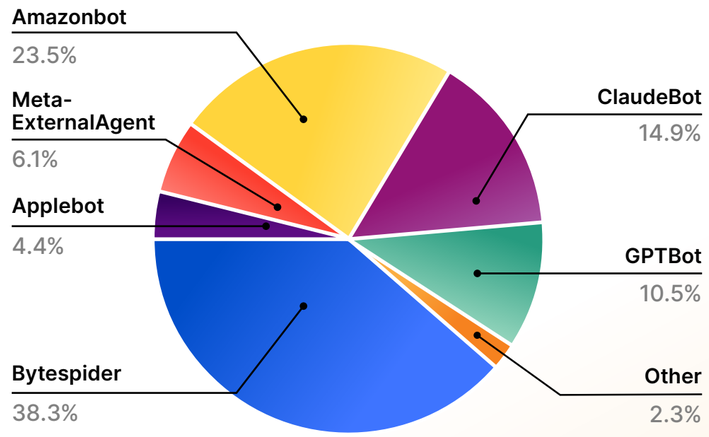
This means that organizations will start facing higher volumes of attacks that will be more sophisticated, often using modern attack methods. Manual security processes, such as triaging phishing emails and manually tuning detections to stop the latest threats, will certainly be strained as attack volumes increase.

AI scraping threatening digital content creators

AI models need data to train on, and many AI companies gather this information through automated web scraping. In fact, AI crawlers already represent 2% of all the bot traffic Cloudflare processes on our network.[3]

AI-derived content can divert traffic and interactions away from websites, severely hurting organizations that rely on online content and advertising for revenue. And the pushback is mounting. In February 2025, education company Chegg sued Google for hurting their traffic with AI, and the UK creative industry launched the “Make It Fair” campaign against content being used without permission.[4]

Top AI crawlers by share of application-layer traffic



Nearly all **(98%)** AI crawler traffic observed by Cloudflare in 2024 **originated from just six companies.**[5]

For organizations that rely heavily on publishing digital content or digital advertising, **AI scrapers are an existential threat.**

Synthetic identity fraud disrupting critical industries

AI is fueling the rise of synthetic identity fraud (SIF), where criminals create hyper-realistic identities by blending real and fake data to bypass traditional verification systems. AI-generated personal details, deepfakes, and automated credential stuffing make these identities harder to detect, posing major risks to heavily targeted industries such as financial services, healthcare, and government agencies.

Unlike traditional fraud, SIF often goes unnoticed as it lacks immediate victims, allowing fraudsters to build credit histories and execute large-scale scams.

AI supercharging insider threats

Remote work and cloud adoption have expanded the attack surface for insider threats, making them harder to detect. More than half of organizations report having experienced an insider threat in the last year, with 8% encountering more than 20 incidents.[6]

AI is now amplifying this challenge, giving insiders powerful tools to evade detection. AI-enabled phishing, deepfake scams, and automated social engineering attacks can generate convincing, context-aware messages in seconds, making deception easier and attacks more frequent.[7]

Not all insider threats are intentional attacks. Verizon's 2024 DBIR found that 68% of data breaches were caused by human factors, such as individuals being deceived by social engineering scams or making errors.[8] AI-assisted spear phishing exploits these mistakes, mimicking real colleagues or executives with near-perfect accuracy to trick employees into sharing credentials, approving transactions, or exposing sensitive data.

Organizations must deploy behavioral analytics, real-time monitoring, and anomaly detection to spot such risks before they escalate. AI-powered security automation is now essential to match the speed and scale of AI-driven threats.

AI-driven bots reshaping the cybersecurity landscape

AI-driven bots are increasing both attack sophistication and risk exposure. In 2024, 28% of all application traffic observed by Cloudflare came from bots, a number that has remained steady at around 30% over the preceding four years. While bots can serve legitimate purposes — such as customer service automation and search engine indexing — the vast majority (93%) are unverified and potentially malicious.[9]

The critical shift is AI-powered bots enabling large-scale, automated attacks with unprecedented efficiency. Attackers now use bots to conduct credential stuffing, launch distributed denial-of-service (DDoS) attacks, scrape sensitive data, and execute fraud at machine speed. AI models supercharge these capabilities by generating realistic phishing attempts, bypassing traditional CAPTCHAs, and evading detection with adaptive behavior.

AI-powered security automation is now **essential** to match the speed and scale of AI-driven threats.

28%

of all application traffic observed by Cloudflare **came from bots**

QUESTIONS FOR THE C-SUITE

Building an AI-driven defensive capability

To stay ahead of AI-powered threats, organizations need to adopt a proactive approach that prevents and mitigates these threats in real time.
Here are a few questions C-suite leaders can ask to assess their organization's readiness.

Q1

Are we using AI to drive comprehensive security observability?

Are we unifying logs, analytics, alerts, and forensics in a single interface to identify risks and their root cause?

Q2

Are we leveraging AI-driven security to detect and neutralize threats in real time?

Do we have AI-powered detection to analyze vast datasets, identify anomalies, and automate responses to emerging threats?

Q3

How protected are we against AI-powered phishing, deepfakes, and malware?

Are we deploying AI-driven detection, phishing-resistant authentication, and adaptive security controls to counter evolving attacks?

Q4

Are we securing our proprietary data from AI scrapers and automated threats?

Do we have bot management, API authentication, and digital watermarking in place to prevent data theft and exploitation?

Q5

Are we leveraging AI-driven behavioral analytics to detect insider threats in real time?

Are we continuously analyzing user behavior, including access patterns, privilege escalations, and data exfiltration attempts?

EXECUTIVE PERSPECTIVES

The new guardrails of AI data security

Dane Knecht
Chief Technology Officer, Cloudflare

Securing AI-era data: Trust, access, and visibility

The most pressing pain point for organizations today is data access — specifically, how to manage and secure it in an enterprise increasingly populated by AI tools. As generative AI becomes embedded in workflows, the challenge is no longer just reacting to threats, but preventing risky or unauthorized access to sensitive data.

This raises urgent questions at the board and C-suite levels. How do we safely grant tools access to enterprise data? How do we ensure an innocuous-looking AI add-on isn't a gateway for data exfiltration? Business and reputational consequences are real — and mounting.

What we're missing: Shadow AI and blind governance gaps

A major blind spot is the uncontrolled spread of AI tools across the enterprise. Employees are adopting AI well ahead of formal policy — often unaware of the risks. These "shadow AI" deployments sidestep traditional reviews, creating unseen attack surfaces and new compliance risks.

Few organizations have mapped where AI is in use. Without that visibility, it's nearly impossible to manage data exposure or respond effectively to incidents.

What comes next: Proactive control and enhanced regulatory scrutiny

Over the next 12–18 months, enterprise security will shift from reactive threat detection to proactive governance of AI access and use. Regulatory scrutiny will intensify — demanding transparency, operational oversight, and strong data protection practices.

Organizations that move fast — by forming cross-functional governance teams, defining AI use policies, and implementing access controls for both tools and users — will reduce risk and position themselves as leaders.

The future of resilience isn't just about spotting threats — it's about controlling how and where AI touches your data.

"Employees are **adopting AI well ahead of formal policy** — often unaware of the risks."

2

Beyond the perimeter: Zero Trust, identity, and the new security frontier

Beyond the perimeter: Zero Trust, identity, and the new security frontier

The shift to multi-cloud environments, SaaS platforms, and API-driven architectures has created a fragmented security landscape, where misconfigurations, identity risks, and shadow IT expose businesses to growing cyber threats. In this environment, Zero Trust security has replaced outdated perimeter-based models to become the foundation for securing cloud applications, workloads, and data with identity-centric, continuous verification approaches.

To keep pace, organizations must enforce Zero Trust principles across cloud and SaaS platforms.

Zero Trust replaces traditional VPNs

Threat actors now actively target VPN providers with zero-day exploits and brute-force attacks for access to the network.[10] As network perimeters collapse, organizations are shifting to identity-centric security, enforcing continuous verification, least-privilege access, and contextual authentication across cloud workloads and SaaS applications.

Zero Trust Network Access (ZTNA) is now essential, replacing legacy VPNs that leave enterprises vulnerable to credential-based attacks, lateral movement, and insider threats. Without Zero Trust, businesses risk exposure to unauthorized access, compromised credentials, and supply chain vulnerabilities.

APIs: The emerging attack vector

With 60% of Internet traffic now API-based, unsecured APIs have become a prime target for attackers.[11] Many organizations fail to track and secure APIs, leaving them vulnerable to data exfiltration, credential abuse, and injection attacks. Cloudflare's machine learning-based analysis found that organizations underreport API endpoints by a factor of four, creating a significant security blind spot.[12]

To mitigate risks, businesses must adopt automated API discovery, authentication enforcement, and AI-driven anomaly detection to prevent breaches and data leaks.

Cloudflare's machine learning-based analysis found that **organizations underreport API endpoints by a factor of four**

Shadow IT and unmanaged cloud services escalate risk

The rapid adoption of unsanctioned cloud services makes it increasingly difficult for IT teams to monitor and secure cloud environments effectively. Employees frequently use unapproved collaboration tools, exposing sensitive data and bypassing corporate security policies.

Cloud access security brokers (CASBs), AI-powered discovery tools, and automated policy enforcement are now critical to gaining real-time visibility, ensuring compliance, and preventing unauthorized data exposure.

Identity-centric security: The end of passwords

As cyber threats become more sophisticated, identity remains a primary attack vector. Twenty-five percent of Cisco's incident response engagements related to users accepting fraudulent multi-factor authentication (MFA) push notifications in Q1 2024.[13] Compromised credentials have also led to significant breaches, such as the targeting of at least 160 Snowflake customers including Santander Group, Ticketmaster, and Advance Auto Parts.[14]

Cybercriminals increasingly bypass MFA, hijack active sessions, and steal credentials, exposing enterprises to widespread breaches and account takeovers.

Challenges:

- **Credential reuse puts enterprises at risk** – Forty-six percent of all human login attempts involve compromised credentials, a number that rises to 60% for enterprise organizations.[15] Attackers automate credential stuffing, gaining access to enterprise systems with minimal effort.
- **Automated credential attacks are scaling rapidly** – Ninety-four percent of login attempts using leaked credentials come from bots, testing thousands of stolen passwords per second.[16] Without real-time bot mitigation and adaptive authentication, organizations remain highly vulnerable to large-scale breaches.
- **Passwords are insufficient** – Static passwords and even basic MFA methods are increasingly ineffective against modern threats, which include MFA bypass, session hijacking, and phishing-resistant credential theft. To combat these risks, organizations must adopt passwordless authentication, enforce Zero Trust access controls, and deploy FIDO2-compliant security keys to eliminate reliance on static credentials.

46%
of all human login attempts involve **compromised credentials**

94%
of login attempts using leaked credentials come from bots, testing **thousands of stolen passwords per second**

QUESTIONS FOR THE C-SUITE

Securing the cloud and rethinking authentication

As cloud adoption accelerates, organizations must rethink security and authentication to protect against evolving threats. A Zero Trust approach, AI-driven visibility, and strong identity protection are essential to securing cloud services, SaaS applications, and APIs. **Determine how proactive your organization is at addressing these challenges with questions such as:**

Q1

Are we enforcing Zero Trust security across clouds, SaaS apps, and APIs?

Do we have continuous verification, least-privilege access, and risk-based authentication across all environments?

Q2

Do we have full visibility into shadow IT and unmanaged cloud services?

Are we using AI-driven discovery tools to detect unauthorized applications and enforce security policies?

Q3

Are our APIs secured against unauthorized access and data breaches?

Are we implementing automated API discovery, authentication controls, and AI-driven anomaly detection?

Q4

Have we eliminated password-based vulnerabilities in our authentication strategy?

Are we adopting passwordless authentication, phishing-resistant MFA, and adaptive identity protection?

Q5

Are we prepared to detect and respond to automated credential attacks?

Can we deploy AI-driven bot mitigation, behavioral analytics, and automated credential revocation to prevent unauthorized access?

EXECUTIVE PERSPECTIVES

Zero Trust for a resilient future

Corey Mahan
Vice President,
Product Management,
Cloudflare

Right now, the biggest challenge organizations face is balancing security with usability. Hybrid work is here to stay, cloud adoption is accelerating, and users expect frictionless access — regardless of where they are or what device they're using. But traditional architectures can't keep up. We're seeing too many businesses rely on a patchwork of point solutions that don't scale well, leading to outages, latency, and frustrated users.

Executives are asking a critical question: How do we deliver secure access without slowing the business down? That pressure is what's bringing Zero Trust to the forefront — not just as a security model, but as a business enabler.

Common pitfalls

Many organizations start with the right intent, but then get stuck. A common pitfall is thinking that buying a 'Zero Trust solution' equates to implementing a strategy. It doesn't. Zero Trust is a mindset and an architectural shift.

Another issue is assuming that unified means integrated — many so-called platforms are just stitched-together products that don't share data or policies or even backends. That creates blind spots, especially across modern environments like cloud APIs, DevOps pipelines, and AI applications.

And then there's shadow IT and shadow AI — tools employees are using that IT teams don't know about, which create serious governance gaps.

What's next (12–18 months)

In the next year or so, we'll see Zero Trust evolve from isolated controls to a foundational layer that spans the entire enterprise. The focus will shift from secure, remote access management alone to unifying identity, data, and traffic policies across every environment. Leaders are already moving toward platforms that are resilient by design, are global by default, automate responses, and offer real-time visibility. That's where the real value is: not just reducing risk, but enabling agility.

The organizations that get ahead will be the ones that embed Zero Trust into their digital foundation — making it part of how they build, scale, and innovate securely.

"A **common pitfall** is thinking that buying a 'Zero Trust solution' equates to implementing a strategy."

3

Stronger, not just safer: Scaling protection across infrastructure, ecosystems, and oversight

Stronger, not just safer: Scaling protection across infrastructure, ecosystems, and oversight

Building resilience across networks, supply chains, and compliance frameworks is essential for maintaining operational integrity and competitive advantage.

However, cyber threats such as DDoS attacks today are faster, larger, and more complex — pushing beyond the reach of traditional defenses. At the same time, digital supply chains are exposing hidden vulnerabilities, while the regulatory environment grows more demanding and fragmented.

To stay competitive, organizations must reframe cybersecurity from an IT issue to a business resilience strategy — one that scales across infrastructure, ecosystems, and oversight.

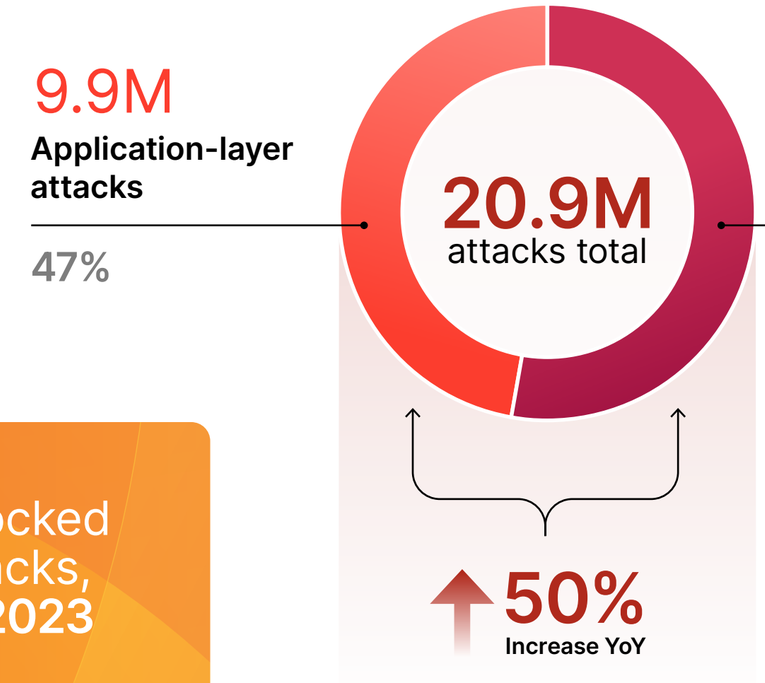
DDoS attacks surging in scale and sophistication

DDoS attacks have evolved into precision tools used by cybercriminals, hacktivists, and nation-states to disrupt operations and create regulatory and reputational fallout. DDoS attacks are crippling businesses across industries. In 2024, Cloudflare blocked 20.9 million DDoS attacks, a 50% increase from 2023.[17]

The scale and sophistication of DDoS attacks are escalating, with attackers leveraging botnets, IoT devices, and AI-driven automation to launch persistent, high-impact assaults on critical digital services.

In 2024, Cloudflare blocked 20.9 million DDoS attacks, a 50% increase from 2023

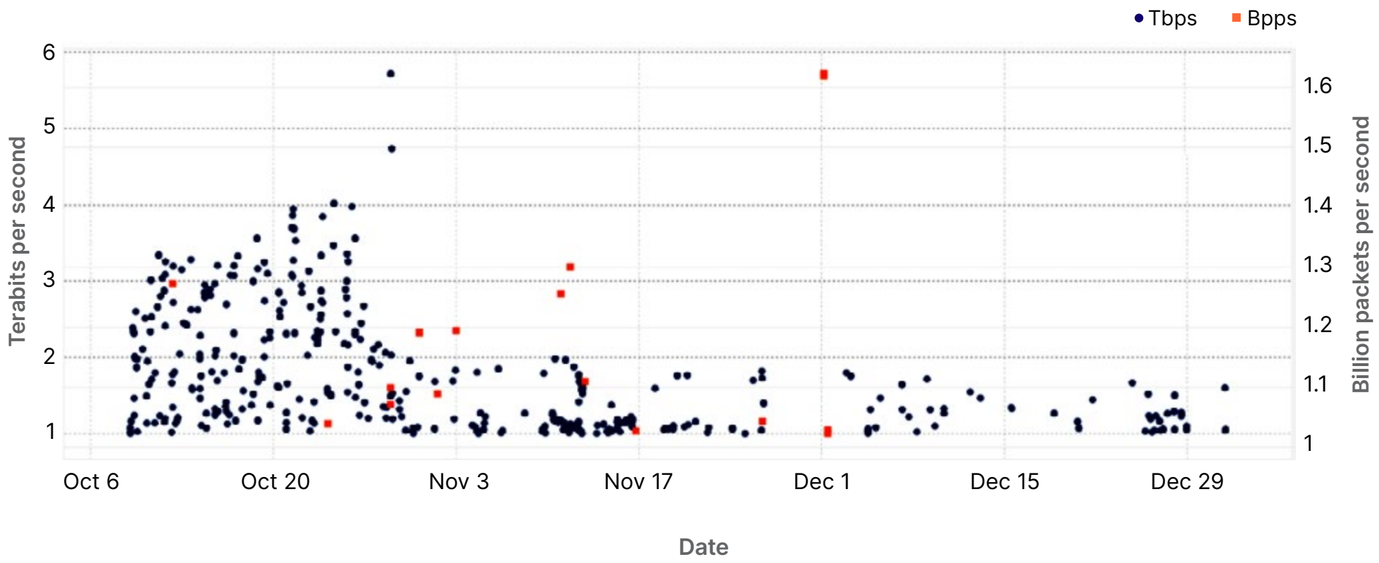
DDoS attacks 2024



The rise of hyper-volumetric DDoS attacks

Q4 2024

In Q4 2024, hyper-volumetric network-layer attacks surged to unprecedented levels. The number of attacks exceeding 1 Tbps spiked by 1,885% quarter over quarter (QoQ), while attacks surpassing 100 million packets per second (pps) rose by 175% QoQ. Notably, 16% of attacks exceeding 100 million pps also surpassed 1 billion pps, highlighting the growing intensity and scale of modern DDoS threats.[18]



Cloudflare data shows the average enterprise organization uses **at least 20 third-party scripts**

Escalating supply chain attacks

According to the World Economic Forum, 54% of large enterprises identify third-party risk management as their top cyber resilience challenge.[19] Attacks on software supply chains, cloud platforms, and third-party integrations are rising sharply; in 2024, 15% of breaches involved a third party.[20]

Compounding the issue is the growing concentration of risk in a handful of dominant cloud providers. A single vulnerability or outage in one of these providers can ripple across industries — as evidenced by the major IT outages in 2024, which caused billions in losses and exposed the fragility of hyperconnected digital ecosystems. These incidents were a stark reminder that in today's interdependent environment, a single point of failure can bring entire operations to a standstill.

A particularly vulnerable area is client-side attacks, where enterprises regularly rely on third-party scripts to speed up web app development. These scripts are embedded code — often JavaScript — that originates from an external server.

While these scripts boost efficiency, they also create significant security vulnerabilities: Every connection to external functions increases the risk of browser-based supply chain attacks.

Cloudflare data shows the average enterprise organization uses at least 20 third-party scripts, while some unknowingly have hundreds of thousands, each representing a potential entry point for attackers.

One major ecommerce organization had more than 340,000 third-party scripts attached to their site.[21]

Regulations such as the EU's Cyber Resilience Act and the Payment Card Industry Data Security Standard (PCI DSS 4.0) help address supply chain security, but enforcement remains a challenge.

Cybersecurity regulations proliferating

Cybersecurity regulations are expanding at a rapid pace, placing greater demands on businesses to enhance security, transparency, and incident reporting. The US Securities and Exchange Commission (SEC) now requires public companies to disclose material cybersecurity incidents and detail their risk management strategies. The EU General Data Protection Regulation (GDPR) remains one of the strictest data privacy laws, imposing penalties of up to 4% of global revenue for non-compliance. The Australian Prudential Regulation Authority (APRA) CPS 234 mandates that financial institutions maintain robust information security measures, while the EU's Digital Operational Resilience Act (DORA) sets unified cybersecurity standards for the financial sector.

In other words, compliance is no longer an afterthought. Organizations that successfully navigate this landscape will embed compliance into their operations, leveraging automation to streamline reporting and ensure continuous alignment with evolving regulations.

Mounting compliance automation

Compliance automation is emerging as a critical trend as organizations face mounting regulatory complexity and operational risk. With over 52 cyber incident reporting requirements currently active or proposed in the US alone, and global frameworks like GDPR, DORA, and PCI DSS 4.0 expanding in scope, manual compliance processes are no longer sustainable.[22] A Deloitte survey found that 62% of global organizations plan to increase investment in compliance automation, citing regulatory fragmentation and the need for real-time response.[23]

To meet jurisdictional data requirements without sacrificing performance, companies are adopting strategic data localization, routing traffic through regional nodes, and deploying automated auditing tools to verify compliance. At the same time, the line between compliance and security is blurring — enterprises are implementing integrated frameworks that align threat detection, policy enforcement, and audit readiness.

This convergence enables businesses to reduce risk, respond faster to regulatory changes, and scale governance across borders. Organizations that automate and operationalize compliance will gain a strategic edge — accelerating entry into regulated markets, enhancing customer trust, and minimizing financial and reputational exposure.

The growing regulatory landscape

The global regulatory framework for cybersecurity and data protection continues to evolve rapidly, with organizations now navigating a complex web of compliance requirements across jurisdictions.

For example:

SEC cybersecurity rules

The US SEC has implemented comprehensive cybersecurity disclosure requirements for public companies. These rules mandate timely reporting of material security incidents and detailed disclosures about risk management strategies, governance, and expertise.

NIS2

The EU's NIS2 Directive sets stricter security requirements across 18 critical sectors. It mandates resilience, risk management, incident response, and reporting measures, with enhanced oversight and penalties for non-compliance.

APRA CPS 234

The Australian Prudential Regulation Authority's CPS 234 information security standard requires financial institutions to maintain robust information security capabilities commensurate with the size and extent of threats to their information assets.

DORA

DORA represents Europe's represents Europe's comprehensive approach to digital operational resilience in the financial sector. It establishes uniform requirements for the security of network and information systems supporting financial entities' operations.

QUESTIONS FOR THE C-SUITE

Continuity and compliance reimagined

In a threat landscape shaped by large-scale DDoS attacks, opaque supply chains, and complex global regulations, true resilience goes beyond defense. It means designing systems that continue to operate under pressure — and treating compliance as both a safeguard and a strategic enabler. **These five questions help CXOs assess their organization's readiness to withstand and adapt to disruption.**

Q1

Can our infrastructure absorb large-scale DDoS attacks and maintain uptime under pressure?

Mitigation capacity should exceed both peak legitimate traffic and the largest recorded attacks. Resilient organizations implement geographically redundant infrastructure and compliance-aware failover plans, and regularly test recovery procedures to ensure both uptime and regulatory alignment.

Q2

Do we have real-time visibility into our most critical third-party dependencies?

Supply chain vulnerabilities are a leading cause of security incidents. Forward-looking organizations continuously monitor external vendors and services, enforce contractual security requirements, and integrate third-party risk insights into broader governance processes.

Q3

Have we automated compliance workflows to keep pace with global regulations?

With so many regulatory frameworks evolving rapidly, a manual approach to compliance cannot scale. High-performing enterprises use automated auditing, real-time monitoring, and jurisdiction-aware data routing to maintain continuous alignment and reduce overhead.

Q4

Are our security and compliance functions fully integrated?

Siloed teams create inefficiencies and gaps. Unified platforms that align threat detection with regulatory reporting streamline audit processes, improve visibility, and reduce risk across the board.

Q5

Have we tested our full resilience posture — from incident detection to recovery and reporting?

Proactive organizations develop playbooks that link technical controls to regulatory requirements, simulate disruptions regularly, and adapt compliance architectures to scale across jurisdictions.

EXECUTIVE PERSPECTIVES

The new rules of readiness

Emily Hancock
Chief Privacy Officer, Cloudflare

Securing the future: Regulation, risk, and readiness

Cybersecurity regulation is entering a new era defined by stricter requirements, heightened scrutiny, and broader accountability. From the SEC's mandatory incident disclosures to the GDPR's steep privacy penalties and new standards like DORA and APRA CPS 234, global regulators are raising expectations around data protection, operational continuity, and transparency. For executive teams, compliance is no longer just a legal obligation — it's a strategic priority.

At the same time, new technologies and evolving threat models are challenging traditional approaches to security. As innovation accelerates, regulators and stakeholders are paying closer attention to long-term risk management, especially around sensitive data. Organizations must demonstrate they can safeguard not just today's assets, but also the data and systems that will underpin tomorrow's digital trust.

What we're missing: Misconceptions and overlooked gaps

Many organizations still treat security and compliance as isolated functions, managed by technical teams without cross-functional coordination. This creates blind spots — particularly in understanding where sensitive data resides, how encryption is applied, and where vulnerabilities lie across third-party systems.

Without a clear inventory and governance framework, organizations risk falling behind both regulators and attackers.

Another gap is in data minimization. Too often, enterprises retain personal data they no longer need, increasing exposure without business benefit. Embedding privacy-by-design principles — limiting data collection, automating deletion, and building in controls at the architectural level — can reduce risk and improve regulatory alignment.

What comes next: A shift toward embedded compliance

In the next 12–18 months, we expect regulators and standards bodies to put more emphasis on proactive, verifiable security practices. This includes stronger controls around data governance, encryption, and third-party risk. Enterprises that act early — by adopting integrated platforms, automating compliance workflows, and embedding security into core operations — will reduce complexity, avoid costly remediation, and position themselves as trusted leaders.

The shift is clear: Compliance, continuity, and security must be designed in from the start. Organizations that internalize this mindset won't just keep up with regulation — they'll lead in a world that demands accountability, transparency, and trust.

"Without a clear inventory and governance framework, **organizations risk falling behind both regulators and attackers.**"

4

Breaking the code: Future-proofing privacy in the quantum era

Breaking the code: Future-proofing privacy in the quantum era

Quantum computing promises transformative advances in science and industry — but it also poses a foundational threat to digital security. Once large-scale quantum systems mature, they'll be capable of breaking public-key cryptosystems widely used to secure the Internet. That includes TLS encryption, VPNs, code signing, and blockchain systems.

The danger isn't hypothetical. Threat actors are already harvesting encrypted data today, betting that future quantum computers will be able to decrypt it — a strategy known as "harvest now, decrypt later." As adoption of post-quantum cryptography accelerates, visibility into cryptographic systems, automated policy enforcement, and a clear migration path will define organizational readiness.

Quantum threats are already in motion

The National Institute of Standards and Technology (NIST) has warned that organizations should act now to avoid being caught off guard.[24] Nation-state actors and sophisticated adversaries are actively collecting encrypted traffic, intellectual property, and state secrets to decrypt later. Communications that require decade-long confidentiality (or longer) — such as healthcare records, military intelligence, and legal contracts — are already vulnerable if not protected with quantum-resilient key agreement.

PQC adoption has surged — but gaps remain

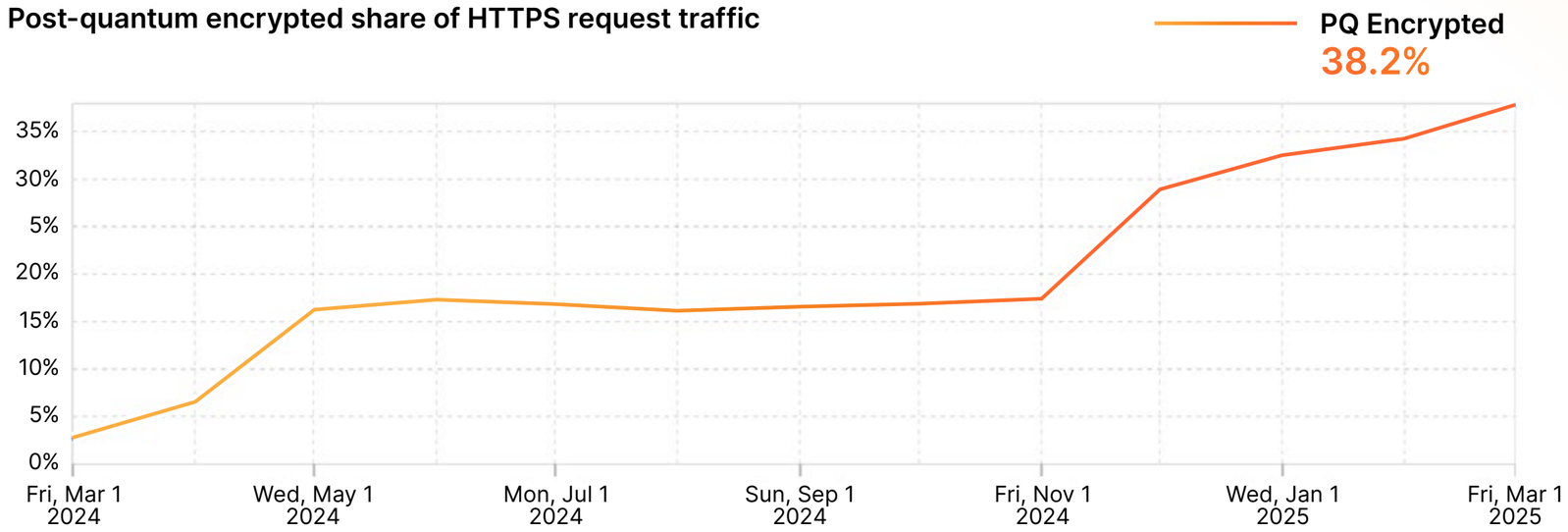
Post-quantum cryptography (PQC) has moved from theoretical research to production implementation. Major tech firms, including Cloudflare, are leading the charge toward PQC adoption.

In early 2024, Cloudflare reported that only 3% of HTTPS traffic was encrypted using post-quantum algorithms. By March 2025, that number reached 38%, following Cloudflare's rollout of hybrid post-quantum TLS by default, and browser support from Chrome, Edge, and Firefox.[25]

Still, adoption is uneven. Most enterprise environments are early in discovery or pilot phases, and cryptographic sprawl complicates transition. Enterprises that fail to prioritize quantum-resistant encryption risk falling behind regulatory requirements and exposing their data to long-term vulnerabilities.

Post-quantum encryption adoption worldwide

Post-quantum encrypted share of HTTPS request traffic



Quantum migration gameplan

1

Start by documenting all places cryptography is in use.

Create a list of migration projects, prioritized by risk and level of effort.

2

Make post-quantum readiness part of your vendor evaluation process now.

Not all vendors are equal when it comes to adopting the latest standards. Validate vendor crypto-agility, especially your Zero Trust vendors that tunnel corporate network traffic.

3

Prioritize key agreement migrations first.

Due to the threat of harvest now, decrypt later, there is a clear benefit to ensuring your key agreement is quantum-resistant now. Vendors have largely converged on transitioning TLS 1.3 to support X25519MLKEM768: a hybrid of the conventional elliptic curve X25519 together with the post-quantum ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203).

4

Signature migrations should be documented, but not prioritized at this point.

Organizations are still working to reach consensus on the right approach for migrating to post-quantum signatures. Fortunately, post-quantum signatures primarily protect against active on-path attacks, making this migration a lower priority.

Crypto visibility and XDR-driven automation will accelerate the transition

Post-quantum migration is not just about deploying new algorithms — it's about understanding where cryptography lives across sprawling environments. That includes embedded systems, cloud workloads, legacy applications, APIs, and IoT devices. Security teams using extended detection and response (XDR) platforms with deep network and endpoint telemetry are better positioned to discover outdated crypto, detect insecure fallback behavior, and automate remediation workflows.

Vendor crypto-agility will become a risk differentiator

Regulatory bodies (e.g., NIST, BSI, ANSSI) are beginning to recommend or mandate crypto-agile architectures. Enterprises will increasingly assess post-quantum readiness in RFPs and supply chain audits. However, not all vendors are moving at the same pace. Those who fail to support hybrid or quantum-safe encryption may face disqualification — especially in government, financial services, and defense sectors.

QUESTIONS FOR THE C-SUITE

Preparing for quantum risks

As attackers adopt harvest now, decrypt later tactics and regulators move toward post-quantum mandates, organizations must begin preparing today. Executives who lead this transition will not only future-proof their infrastructure but also gain a strategic edge in trust, compliance, and resilience. **Consider your readiness for the near-term era of quantum risks by asking these questions:**

Q1

Do we have full visibility into where cryptography is used across our environment — from clouds and applications, to embedded systems and third-party tools?

Cryptographic systems are often deeply embedded and poorly documented. Without full visibility, organizations risk leaving critical systems unprotected or unknowingly exposed to quantum-era threats.

Q2

Have we prioritized migration to post-quantum key agreement protocols, particularly for systems securing sensitive or long-lifespan data?

Harvest now, decrypt later attacks target data that must remain confidential for years. Migrating key exchange mechanisms — such as TLS handshakes — is a high-impact, time-sensitive step in securing future confidentiality.

Q3

Are our detection and asset monitoring tools capable of identifying outdated or quantum-vulnerable cryptography across the enterprise?

XDR, SIEM, and asset discovery platforms should help detect cryptographic drift, legacy libraries, and fallback protocols. This is essential for preventing misconfigurations and guiding migration priorities.

Q4

Are we evaluating the crypto-agility of our vendors and partners as part of our procurement and risk review process?

Vendors that lack a roadmap for post-quantum readiness may become weak links. Incorporating PQC alignment into due diligence helps reduce downstream exposure and ensures long-term resilience.

Q5

Do we have a phased, risk-based migration strategy that includes governance, automation, and executive visibility?

Post-quantum migration is a complex, multi-year journey. A clear roadmap with accountability, automation for deployment, and real-time metrics for progress is essential for maintaining momentum and board-level confidence.

EXECUTIVE PERSPECTIVES

Cutting through cryptographic confusion

Wesley Evans
Senior Product Manager, Cloudflare

Organizations are facing a surge in cryptographic complexity. Where we once had a few well-defined standards, we now have a fragmented ecosystem of algorithms and deployment models. This rapid evolution, coupled with growing regulatory and operational pressure to adopt quantum-safe encryption, has created confusion at the enterprise level.

Leaders are told to embrace crypto-agility and prepare for quantum resilience, but most lack a clear inventory of where and how cryptography is used. Without visibility, planning becomes guesswork. Budgeting stalls. Ownership is unclear. And that makes it easy for executives to deprioritize action, even when the risks are well understood.

Common pitfalls

A major blind spot is the assumption that organizations haven't already been compromised. Harvest now, decrypt later attacks are real and active — particularly for data with long-term value, such as health records, intellectual property, and national security information. If your data falls into these categories, it may already be in the hands of a threat actor waiting for the capability to decrypt it.

Another misconception is that quantum risk will be preceded by a clear milestone, like a public breakthrough in Shor's algorithm. But attackers don't need instant results.

If it takes weeks or months to break a key and the payoff is significant, they'll make that investment. This delay in perception contributes to a dangerous sense of complacency.

Future direction

Two shifts are coming fast. First, advances in quantum error correction will make the threat of quantum decryption feel real — not theoretical. This will trigger increased pressure from regulators, boards, and the public. Second, organizations will begin rolling out crypto-agile systems. That means finally taking stock of where cryptography lives, how it's used, and who owns it.

It won't be easy. Most teams are walking into this like a long-overdue visit to the cryptographic dentist — expect discomfort, cost, and surprises. But waiting only makes it worse. The priority now isn't to replace everything overnight, but to build visibility, assign responsibility, and start the upgrade path. Those that act early will be best positioned to manage the post-quantum shift — before it becomes a crisis.

"Advances in quantum error correction will make the **threat of quantum decryption** feel real — not theoretical."

5

Tipping the scales: Governance, geopolitics, and ethics

Tipping the scales: Governance, geopolitics, and ethics

As global power dynamics shift, the intersection of cybersecurity, geopolitics, and ethics is redefining leadership responsibilities. Today, cyber attacks are tools of geopolitical influence, regulatory bodies are holding executives personally accountable, and AI is introducing ethical dilemmas that challenge traditional oversight.

With incidents like the SEC's 2023 mandate for rapid cyber incident disclosure and widespread reports of state-sponsored cyber operations, leaders must embed robust governance, transparent AI ethics, and agile risk management into their strategy.

Security governance moves from guidance to accountability

Regulatory oversight is tightening. In 2023, the SEC mandated that public companies disclose cyber incidents within four days, marking a shift toward enforced accountability. Nearly 72% of companies now prioritize cybersecurity expertise on their boards, with 71% featuring it in at least one director biography — up from just 34% in 2018.[26] Boards increasingly recognize that neglecting cybersecurity can lead to severe operational, legal, and reputational consequences.

Geopolitics and cyber warfare directly impact the enterprise

Nation-state actors and hacktivist groups are increasingly leveraging cyber operations as strategic weapons. In recent years, state-backed campaigns have targeted financial, energy, and tech sectors to disrupt global supply chains and influence market dynamics. For instance, politically motivated threat actor LameDuck conducted more than 35,000 confirmed DDoS attacks in the span of a year, leading to operational disruption for organizations including Microsoft, OpenAI, and Scandinavian Airlines.[27] Even ostensibly neutral organizations can be drawn into geopolitical conflicts.

Executives must be treated like attack surfaces

C-suite leaders face direct cyber threats. High-profile deepfake scams and executive impersonation schemes have increased exponentially, with several CEOs reportedly targeted by fraudulent audio and video messages designed to mislead stakeholders.[28] Such incidents underscore how vulnerable leadership is to cyber risk, and targeted reputational and financial attacks.

Regulatory fragmentation and supply chain uncertainty are intensifying

Global enterprises now navigate a maze of diverging cybersecurity, AI, and data sovereignty laws. Trade restrictions and export controls have forced companies to reassess vendor relationships and reconfigure supply chains. For example, changing tariffs and the EU's NIS2 Directive have disrupted established supply chain protocols, increasing both compliance costs and the risk of operational delays.

AI ethics and shadow AI demand governance at scale

The explosion of generative AI in the workplace is outpacing organizational control. McKinsey reports that 65% of companies now use GenAI in at least one business function, up from one-third in 2023.[29] Cloudflare's AI Gateway processed over five billion requests between October 2024 and February 2025, a 60% increase in just five months.[30] Adoption is lightning fast: In January 2025, DeepSeek AI reached #3 on Cloudflare Radar's AI services list within nine days of launching its R1 model.[31]

This grassroots adoption is fueling the rise of shadow AI — unauthorized tools used by employees without oversight. These tools pose serious risks: data leakage, regulatory non-compliance, and exposure of sensitive information to public models.

To respond, organizations must go beyond basic policy statements. Effective governance requires clear approval frameworks, prompt logging, URL filtering, and usage monitoring. Without active enforcement, AI ethics and security will remain theoretical.

Nation-state actors and hacktivist groups are increasingly leveraging cyber operations as **strategic weapons**.

QUESTIONS FOR THE C-SUITE

Navigating ethical and geopolitical risk

As cyber threats become geopolitical, AI ethics grow more complex, and regulatory expectations tighten, executive teams must go beyond technical controls. **These questions can help leaders assess whether their governance, intelligence, and response strategies are fit for a world where leadership itself is part of the threat surface.**

Q1

Do we have clear board-level accountability for security and digital resilience, with defined roles and cyber-literate leadership?

Given that regulators now hold executives personally liable — as seen with the SEC's rapid disclosure requirements — ensuring that the board is equipped with dedicated cyber expertise is critical for mitigating legal and reputational risks.

Q2

Are we monitoring geopolitical shifts and their impact on our threat landscape, including state-sponsored cyber attacks and activist campaigns?

With recent state-backed operations disrupting supply chains and targeting market-critical sectors, having real-time intelligence on geopolitical risk is essential to safeguard both global operations and leadership.

Q3

Do we have a proactive response plan for executive-targeted attacks such as deepfake scams and impersonation campaigns?

As leadership faces growing risks from AI-driven misinformation and impersonation, response strategies must include targeted incident response protocols and continuous reputation management measures.

Q4

Are our policies and security controls robust enough to detect and manage unauthorized AI usage across our workforce?

With more organizations leveraging GenAI and increasing reports of shadow AI, granular monitoring and enforcement of strict guidelines are necessary to prevent data leaks and ensure regulatory compliance.

Q5

Are we aligning our cybersecurity and AI strategies with evolving regional regulations on data sovereignty and ethical AI, and are we using this alignment as a strategic advantage?

Diverging regulatory frameworks — such as the EU's NIS2 Directive and regional data sovereignty laws — demand that security policies be both agile and forward-thinking. This alignment both reduces legal risk and enhances market trust and competitive positioning.

EXECUTIVE PERSPECTIVES

Governance and accountability in a polycrisis world

Ramy Houssaini
Chief Cyber Solutions Officer, Cloudflare

Organizations must navigate a polycrisis landscape where geopolitical, economic, and technological risks intersect. The SEC's cyber incident disclosure mandate exemplifies the shift from cybersecurity guidance to executive accountability. Organizations must develop real-time breach detection and response capabilities. Non-compliance risks severe penalties, while reputational damage can erode stakeholder trust. Boards must embed cybersecurity expertise and proactive risk management to remain resilient.

Blind spots: Geopolitical, AI, and supply chain risks

A key blind spot is underestimating geopolitical cyber threats. Many enterprises assume neutrality, yet state-sponsored attacks increasingly disrupt financial, tech, and energy sectors, leaving supply chains vulnerable.

Another overlooked risk is shadow AI — unauthorized AI tools used without oversight. Without robust monitoring, sensitive data may be exposed, leading to regulatory penalties and competitive disadvantages.

Additionally, fourth- and fifth-party vendors introduce hidden vulnerabilities. While companies focus on direct suppliers, extended vendor ecosystems often lack visibility, making them susceptible to cyber threats and operational disruptions.

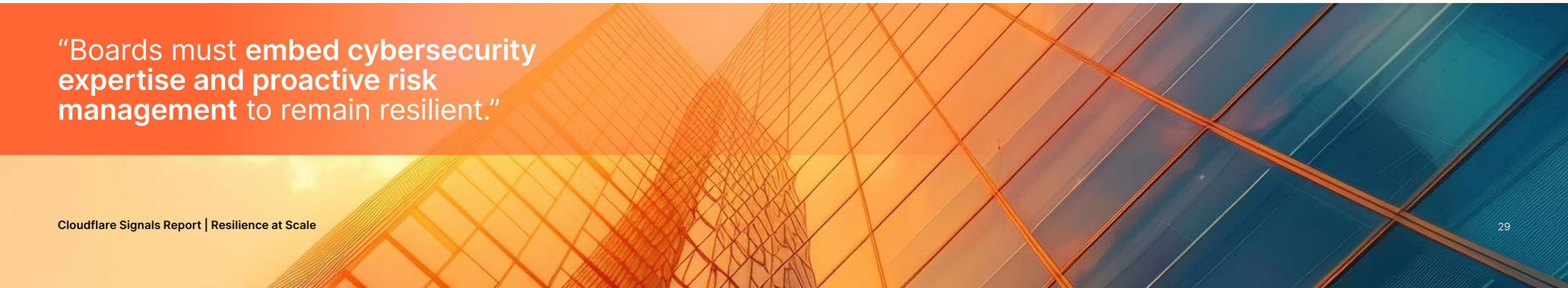
Future developments and strategic preparation

Over the next 12–18 months, organizations should anticipate:

- **Regulatory expansion:** The EU's NIS2 Directive and similar frameworks will intensify compliance requirements. Leaders must establish regulatory task forces to stay ahead.
- **AI governance acceleration:** With shadow AI surging, regulators will impose stricter controls. Companies must enforce monitoring and governance frameworks to mitigate risks.
- **Executive targeting:** Deepfake scams and impersonation attacks will grow more sophisticated, increasing fraud and misinformation risks. Organizations should deploy AI-driven detection systems and enhance executive security training.
- **Supply chain resilience:** Cyber threats and geopolitical instability will continue impacting supply chains. Enterprises must strengthen risk assessments, enforce security obligations, and improve vendor monitoring.

To succeed in this polycrisis era, leaders must integrate cybersecurity into governance, assess geopolitical risks, enforce AI oversight, and build resilient supply chains. Agility and superior risk management will be essential for navigating evolving regulations and ensuring long-term stability.

"Boards must **embed cybersecurity expertise and proactive risk management** to remain resilient."



CONCLUSION

C-suite moves that build resilience at scale

The nature of cybersecurity has shifted — it now touches every corner of the enterprise. In 2025, AI-powered attacks, geopolitical risk, regulatory complexity, and supply chain interdependencies demand a coordinated, cross-functional response. Securing the future means more than reacting to threats; it means embedding resilience into how organizations operate, innovate, and grow. These calls to action are designed for CXOs to build resilience as a strategic capability — together.

1 Make resilience a shared strategic mandate

Build cross-functional ownership for cybersecurity by ensuring that the C-suite jointly aligns on security posture, resource allocation, and contingency planning. Resilience isn't one team's job — it is an enterprise capability that must scale across functions and geographies.

2 Automate and integrate to ensure scalability

Manual compliance and fragmented defenses cannot keep pace with AI-enabled threats and expanding regulatory requirements. Invest in automation for threat detection, compliance workflows, and incident response. Integrate compliance, risk, and security tooling to eliminate silos and improve visibility.

3 Rethink cyber governance as a competitive advantage

With executive accountability rising, ensure your board and C-suite include cyber-literate leadership and formalized roles for digital risk oversight. Embed cyber risk into enterprise risk frameworks and treat regulatory alignment as a competitive differentiator.

4 Future-proof now, not later

Start your post-quantum (PQC) cryptography migration and AI governance readiness today. Leaders who wait will find themselves vulnerable to "harvest now, decrypt later" threats or ungoverned AI sprawl. Visibility, vendor crypto-agility, and phased migration strategies are key.

5 Test for failure — at scale

Resilience is not about avoiding failure; it's about operating through it. Simulate real-world crises — from hyper-volumetric DDoS to insider misuse or executive-targeted attacks — and stress test your ability to detect, contain, and recover. Factor compliance, comms, and supply chain into your scenarios.

6 Integrate AI in offense and defense

AI should no longer be treated as just a tool; instead, it is a strategic capability within the C-suite, driving agility, resilience, and innovation across the enterprise. By harnessing AI-powered insights, organizations can rapidly adapt to market shifts, anticipate risks, and optimize decision making in real time.

AI enhances resilience by automating threat detection, streamlining crisis response, and fortifying cybersecurity postures against evolving risks. Moreover, it fuels innovation by uncovering new revenue streams, accelerating R&D, and personalizing customer experiences at scale. As AI becomes deeply integrated into core business functions, it transforms organizations into more adaptive, future-ready enterprises, enabling leaders to navigate complexity with confidence.

Securing the future means more than reacting to threats; it means **embedding resilience into how organizations operate, innovate, and grow.**

Resilience@Cloudflare: The foundations to enable a more scalable future

RESILIENCE@CLOUDFLARE

A single, programmable network unlike any other

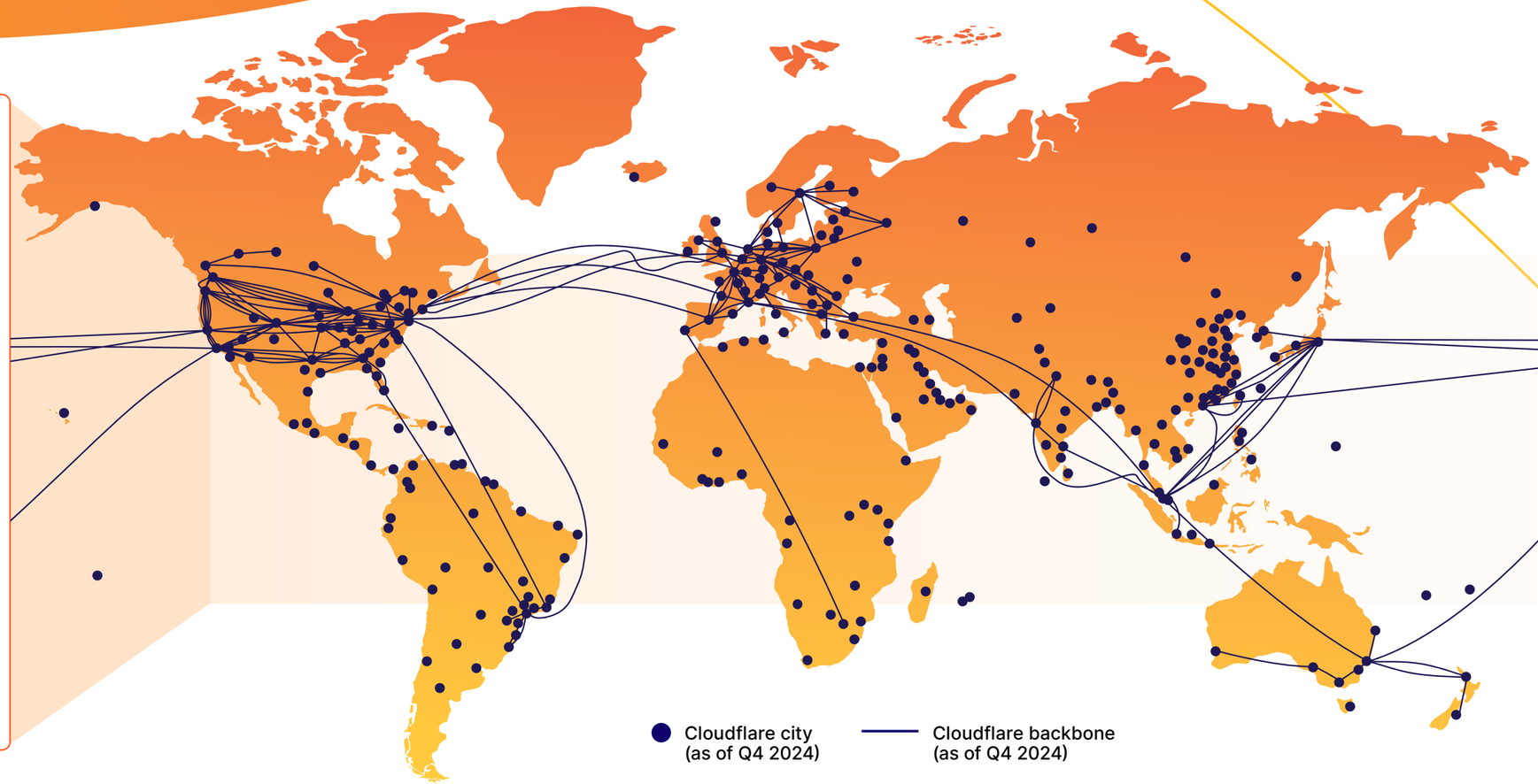
335+ cities
in 125+ countries, including mainland China

↳ **w/190+ cities**
for AI inference powered by GPUs

~50 ms
from ~95% of the world's Internet-connected population

~13,000 networks
directly connect to Cloudflare, including ISPs, cloud providers, and large enterprises

348 Tbps
of network capacity and growing



RESILIENCE@CLOUDFLARE

Cloudflare Workers

The best platform for developers to build and scale AI inference and agents

Cost and scalability

Scale up and down to zero

Run AI models on GPUs without having to pay for pre-provisioned resources for months in advance, at peak. Simply pay for what you use.

No compute = no bills for usage

Compute-based pricing means you're not charged when your function is idle and waiting on I/O. (Applications can spend up to **10 times** more time waiting on I/O than actually using the CPU.)

Performance

Deploy from region: Earth

Code executes within 50ms of ~95% of the Internet-connected global population.

Orchestration and execution in one place

Workers are able to interface with APIs, LLMs, and external or internal services — wherever it is the most efficient for them to run.

Developer experience

All the products you need

Access inference, state management, UI deployment, or workflows in one platform.

Idea to production in seconds

Easy development experience, including local development and rapid deployment.

Save time

No tuning necessary. Automatic placement for optimal performance.

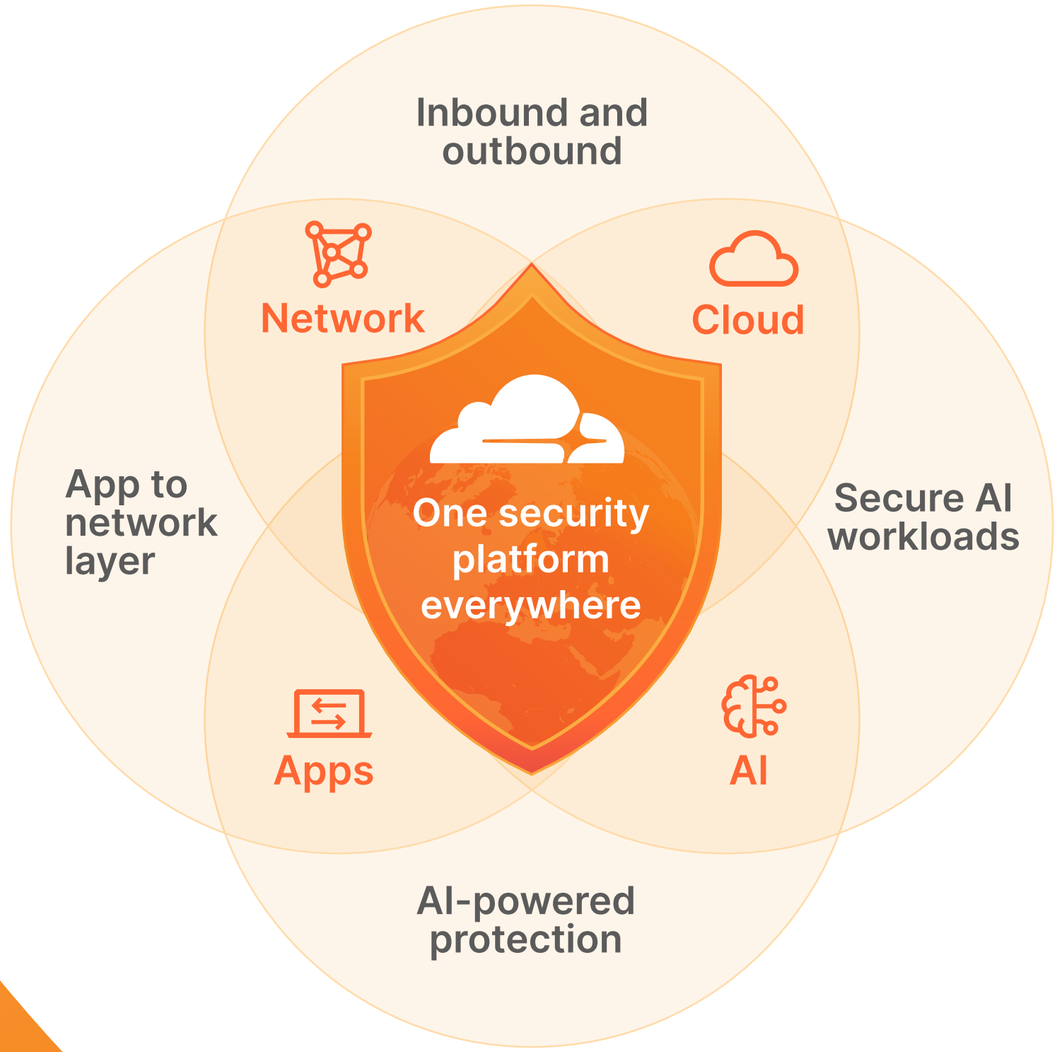
You write the code. We handle the rest.

RESILIENCE@CLOUDFLARE

One security platform. Network to cloud. Apps to AI.

Enabling organizations to:

- Regain operational control
- Improve security posture
- Accelerate vendor consolidation
- Enhance user experience and productivity
- Achieve data governance and compliance



RESILIENCE@CLOUDFLARE

Cloudflare is built for what's next

One composable platform

Unified security

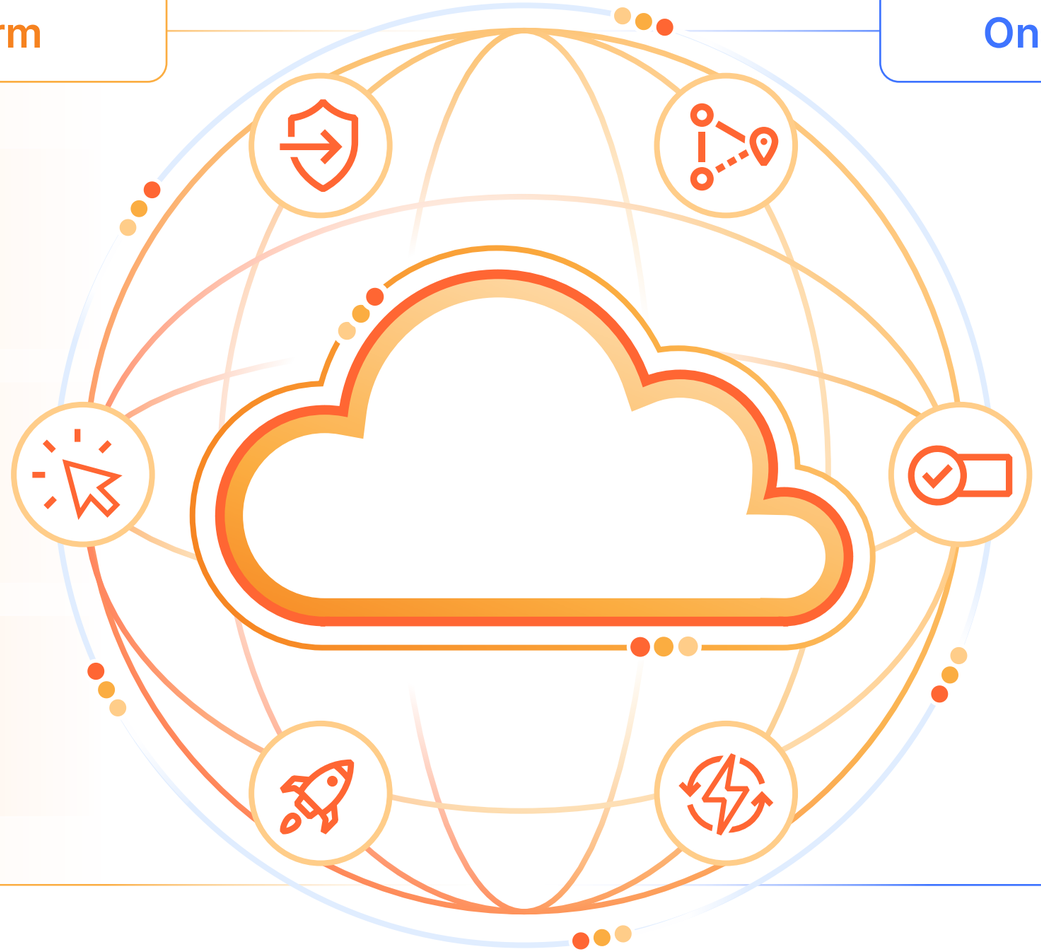
for external-facing systems and internal resources

Any-to-any connectivity

for users, apps, branches, data centers, and clouds

Flexibility

to customize the platform with full-stack developer tools



One programmable network

More effective

by simplifying connectivity and policy management

More productive

by ensuring fast, reliable, and consistent user experiences everywhere

More agile

by innovating rapidly to meet evolving security requirements

RESILIENCE@CLOUDFLARE

Run inference tasks on Workers AI, the first globally distributed serverless AI inference platform

335+ cities

in 125+ countries, including mainland China

Code executes within 50ms of ~95% of the Internet-connected global population

190+ cities

with GPUs

Growing constellation of cities for AI inference powered by GPUs

Deploy from region:

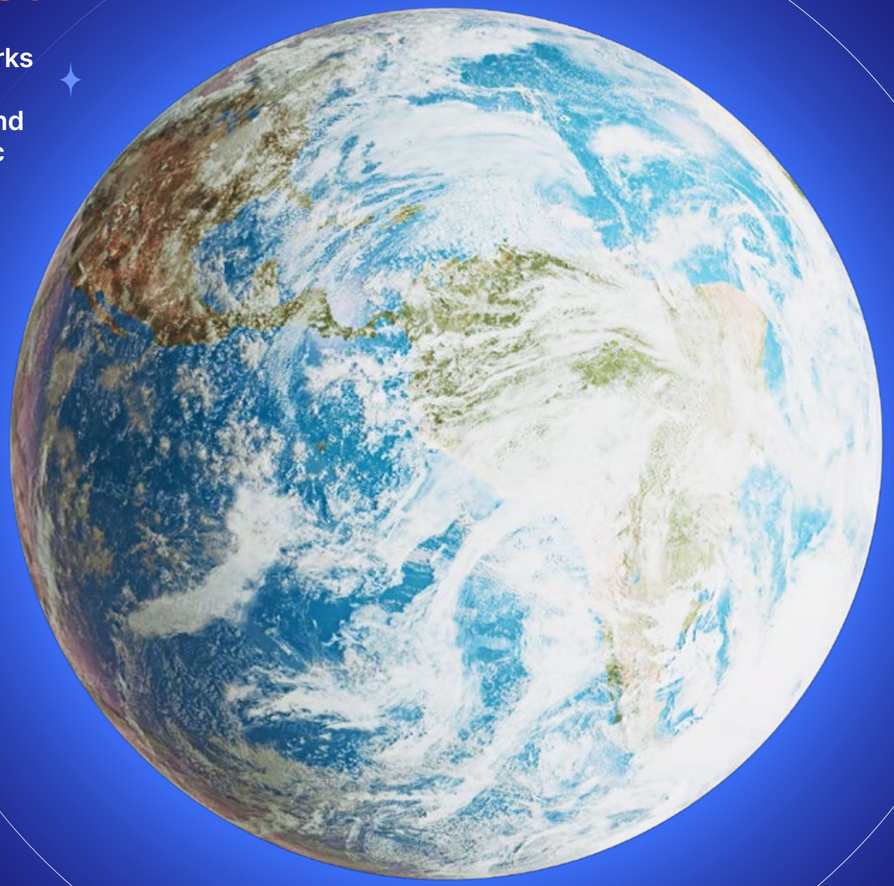
Earth

RESILIENCE@CLOUDFLARE

Fighting for the open Internet

The Internet is a miracle. The connection of diverse networks with common standards enables us to exchange data around the world in a way that is resilient, interoperable, and accessible to anyone. Today, we depend on it for economic growth and innovation, access to information and free expression, and rule of law and democratic principles.

Cloudflare is proud to be part of the global community standing up for the Internet.



- Advocating for network neutrality
- Monitoring places where the Internet is not open
- Protecting human rights and democratic institutions
- Deploying standards that improve the privacy and security of data flows
- Participating in Internet standards development
- Supporting multistakeholder Internet governance

CLOUDFLARE

2025

Cloudflare Signals Report

Learn more

Resilience at Scale

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-6966.2025APR24

Endnotes

The findings in this report are primarily based on aggregated traffic patterns observed across Cloudflare's global network between Jan. 2, 2024 and Dec. 31, 2024.

1. https://www.darktrace.com/blog/survey-findings-ai-cyber-threats-are-a-reality-the-people-are-acting-now/
2. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
3. Cloudflare network traffic data, 2024
4. https://www.cnbc.com/2025/02/24/chegg-sues-google-for-hurting-traffic-as-it-considers-alternatives.html; https://www.theguardian.com/gnm-press-office/2025/feb/25/make-it-fair
5. Cloudflare network traffic data, 2024
6. https://nationalcioreview.com/wp-content/uploads/2024/07/2023_Insider_Threat_Report-16d8d8f7.pdf
7. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
8. https://www.verizon.com/business/resources/T1e3/reports/2024-dbir-data-breach-investigations-report.pdf
9. Cloudflare network traffic data, 2024
10. https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/; https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day
11. Cloudflare network traffic data, 2024
12. Cloudflare network traffic data, 2024
13. https://blog.talosintelligence.com/how-are-attackers-trying-to-bypass-mfa/
14. https://therecord.media/advance-auto-parts-data-breach-2million
15. Cloudflare analysis of compromised credentials from Oct. 12, 2024 to Dec. 31, 2024
16. Cloudflare analysis of compromised credentials from Oct. 12, 2024 to Dec. 31, 2024
17. Cloudflare network traffic data, 2024
18. Cloudflare network traffic data, Q4 2024
19. https://reports.weforum.org/docs/WEF_Global_Cyber security_Outlook_2025.pdf
20. https://www.verizon.com/business/resources/Tdd6/reports/2024-dbir-data-breach-investigations-report.pdf
21. Cloudflare network traffic data, 2024
22. https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf
23. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-survey-findings-on-esg-disclosure-and-preparedness.pdf
24. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
25. Cloudflare network traffic data, 2024
26. https://www.ey.com/en_us/board-matters/cyber-disclosure-trends
27. https://www.cloudflare.com/threat-intelligence/research/report/inside-lameduck-analyzing-anonymous-sudans-threat-operations/
28. https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam
29. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024
30. Cloudflare network traffic data, Oct. 2024 to Feb. 2025
31. Cloudflare network traffic data, Jan. 2025