Content Credit:
Cloudflare Threat Intelligence, 2025 Cloudflare Signals Report

CLOUDFLARE

Beyond the Firewall: The Human, AI and Network Revolution

Amanda Spencer
Director, Solutions Engineering, ANZ
Cloudflare

https://www.linkedin.com/in/amandaspencer-net/

Just like AI Prompt Basics..

Let's set context before we begin...

Themes for discussion

Resilience

Mindful Leadership

Human Factor

Data Driven Decision Making

Integrity, Ethics, Trust

Breaking down silos

Our People - Our most important asset

Visibility & Monitoring

Collaboration

Leadership is a Human Practise

Transparency

Culture

Community

Data Driven Insights

Why Tech? What shaped my career..

Onboarding Program - 1990’s Joburg Style

Study time..


CWNA
Certified Wireless Network Administrator


riverbed
ACCREDITED ASSOCIATE
RCPE
WAN Optimization


CompTIA
A+


BlueCoat


CLOUDFLARE


Sniffer
TECHNOLOGIES


CISCO
CCNA


Network
ASSOCIATES


CISCO
CCIE
LIFETIME
EMERITUS


WIRESHARK


CISCO
CERTIFIED
CCNP
ROUTING &
SWITCHING


CISSP


riverbed
CERTIFIED PROFESSIONAL
RCPE
Packet Visibility
and Analysis


CWAP
Certified Wireless Analysis Professional


Microsoft
CERTIFIED
Systems Engineer


education
Lifelong Learning
interests
PASSION


PACKETEER


f5

CLOUDFLARE

Data Driven Insights

Let's look at some stats..

Our Reality..

Cybercrime threat becomes harsh reality for super

Members of funds including Australian Retirement Trust, Rest, Hostplus, AustralianSuper and Insignia – were targeted by cybercriminals who likely acquired their account information (things like their name, email, password) on the dark web after it was stolen in a different hack.

Australian Human Rights Commission discovers data leak

The Akira ransomware gang has listed the Chinese-owned The Fullerton Hotels and Resorts as a victim on its darknet leak site and is claiming to have stolen more than 140 gigabytes of data.

"We are ready to upload more than 148 GB of essential corporate documents such as: NDA's and corporate licenses, agreements and contracts, driver licences, passports and other employee and customer documents, financial data (audits, payment details, reports), etc," Akira said in its leak post, dated 8 April.

13cabs, which also runs the Silver Service taxi service, is Australia's largest taxi company.

On 28 March, the company posted a public statement on its site, revealing that earlier in the month, it had detected that some of its user accounts for 13cabs and Silver Service were "potentially compromised" through "a sophisticated unauthorised type of suspicious activity".

Threat trends overview

773%

Increase in size of largest DDoS attack

From 26 million requests per second in 2022, to 201 million in 2023

33%

More APIs found via ML than what orgs self-reported

Organizations have larger API attack surface than they think

74%

Of orgs adopting Zero Trust **plan to or have replaced VPN** for all employees*

22 minutes

from POC to exploitation

Vulnerability weaponization is accelerating

Phishing is still the #1 initial attack vector

*Source: IT & security professionals implementing Zero Trust. Enterprise Strategy Group, a division of TechTarget, Inc. Research Survey, Cloudflare Zero Trust for the Workforce Survey, May 2024.

For threat intelligence to be useful, it must be...

Accurate

Actionable

Automated

One network, one control plane on a global scale

330+ cities
in 125+ countries, including mainland China

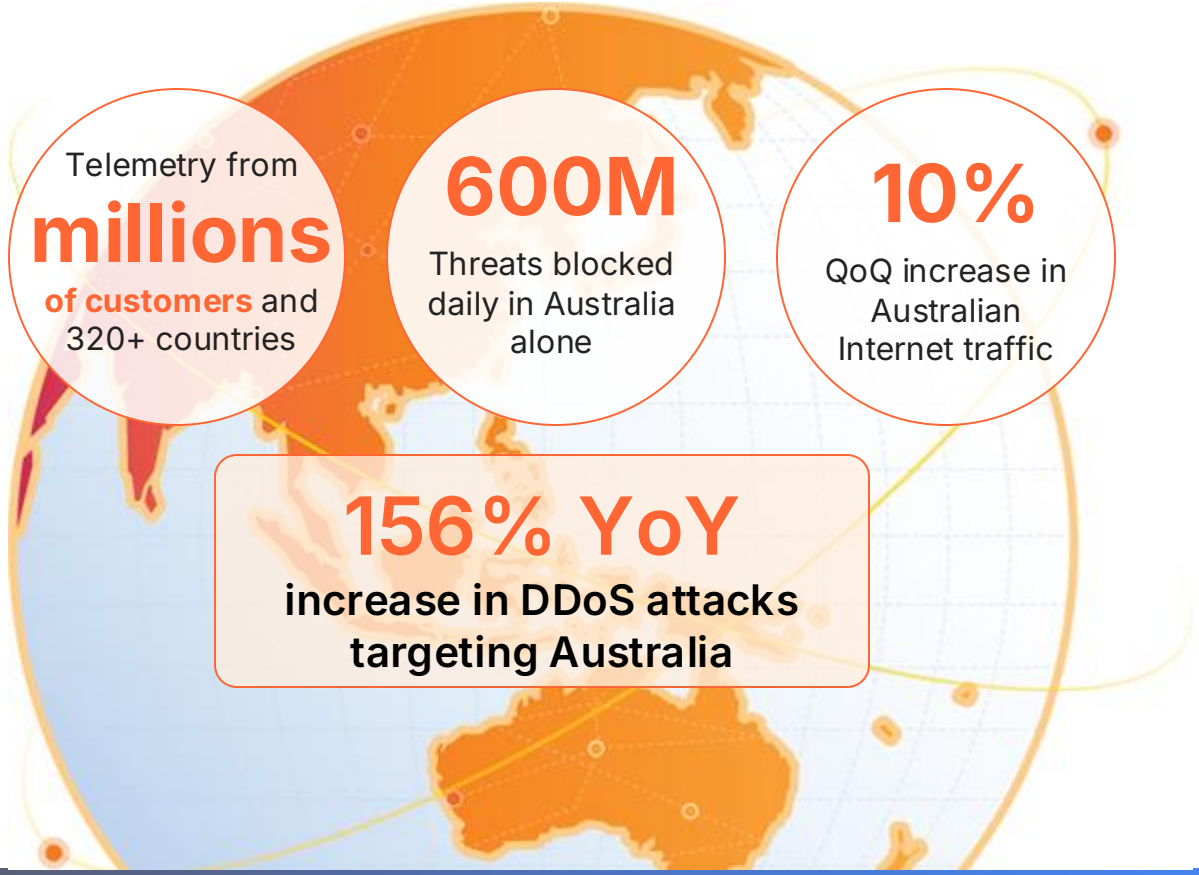
→ **w/190+ cities**
for AI inference powered by GPUs

~20%
of web properties sit behind Cloudflare

247 billion
cyber threats blocked every day

405 Tbps
of network capacity (and growing)

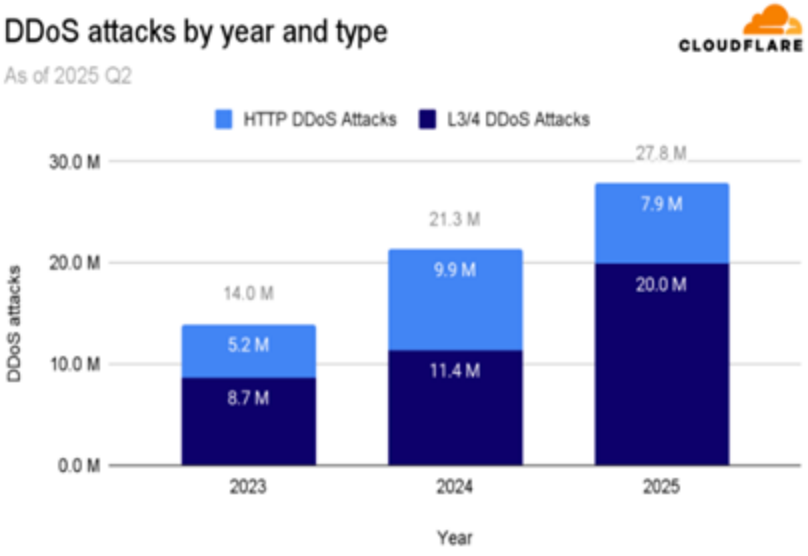
We see threats at massive scale

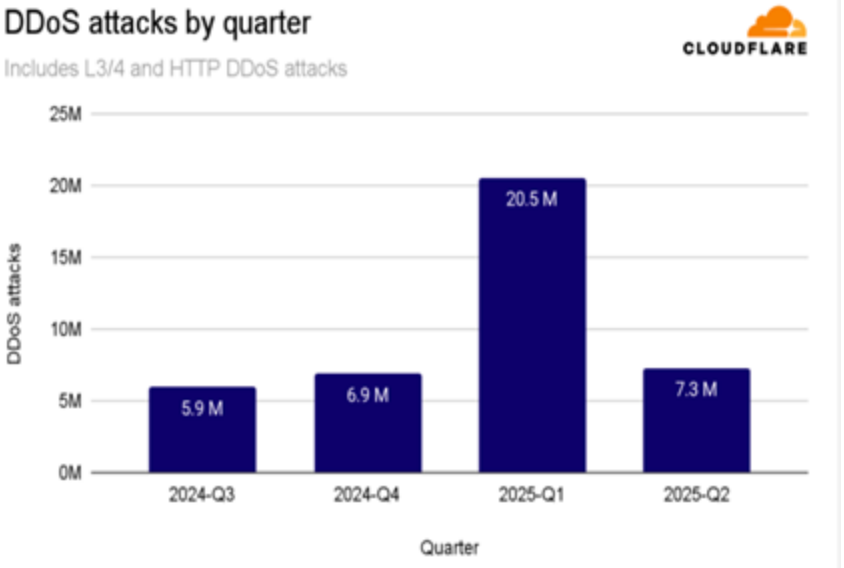


DDoS Attack Trends

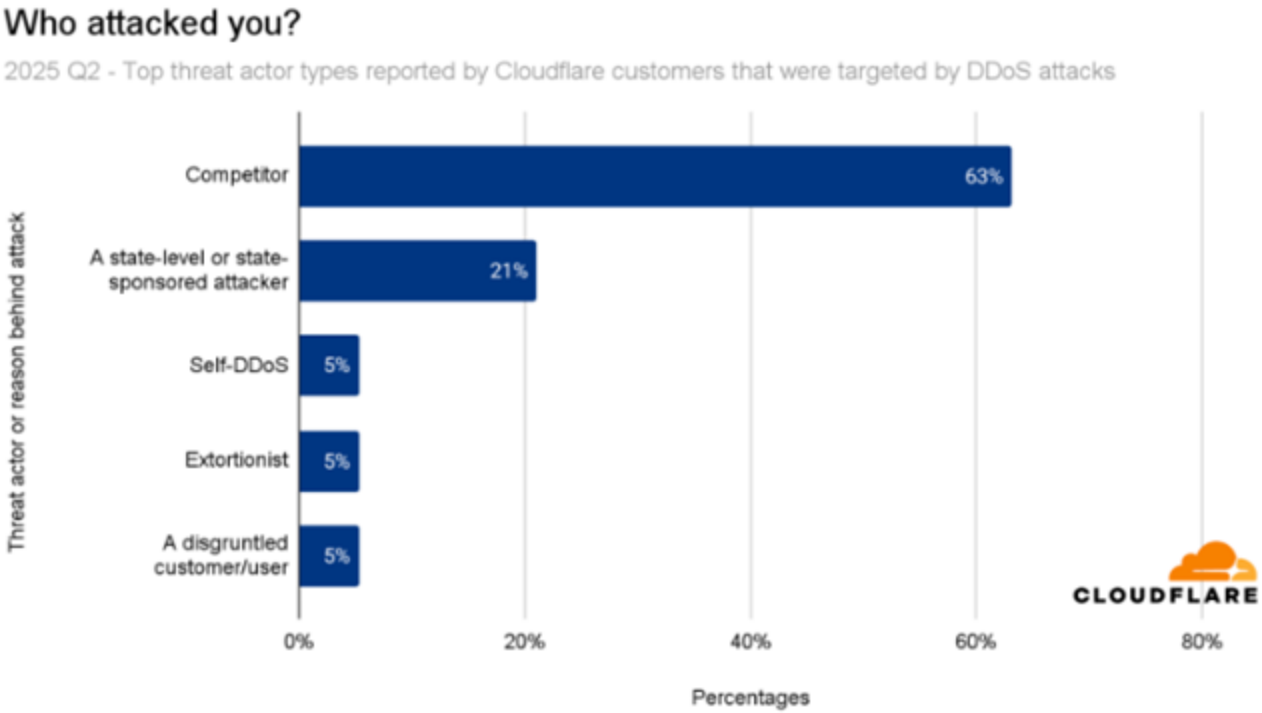
DDoS attacks increasing..

DDoS attacks by year and quarter

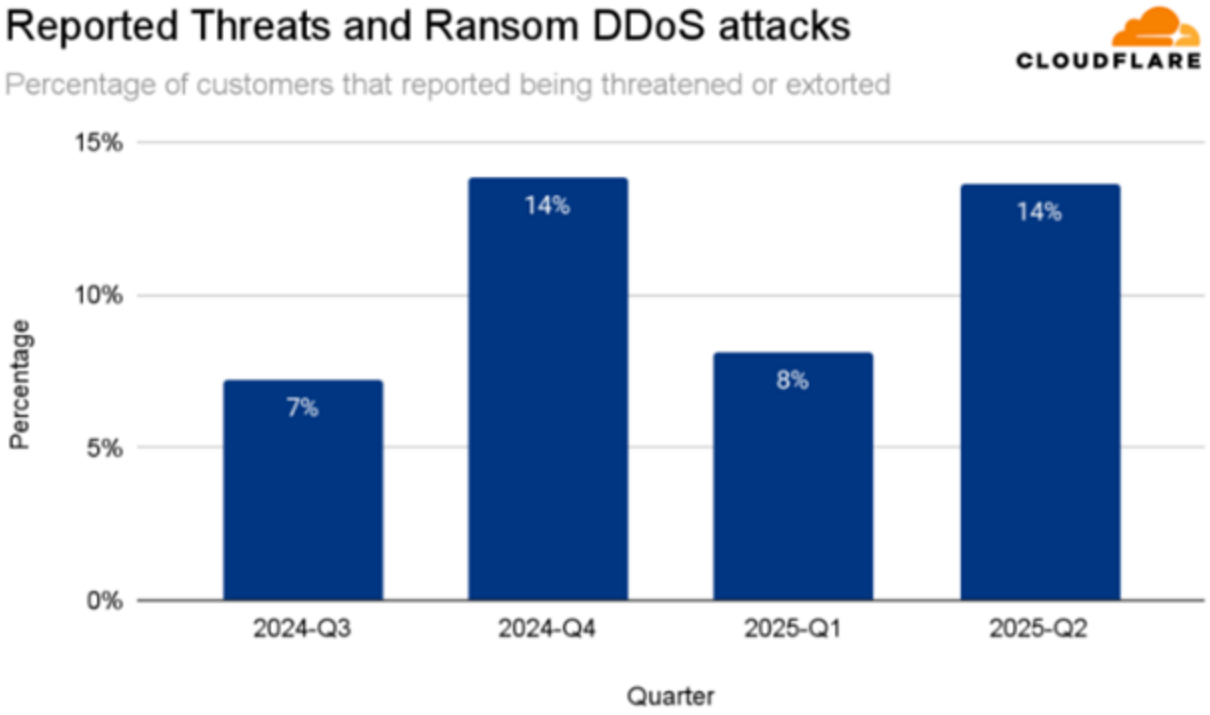




Who attacked you?

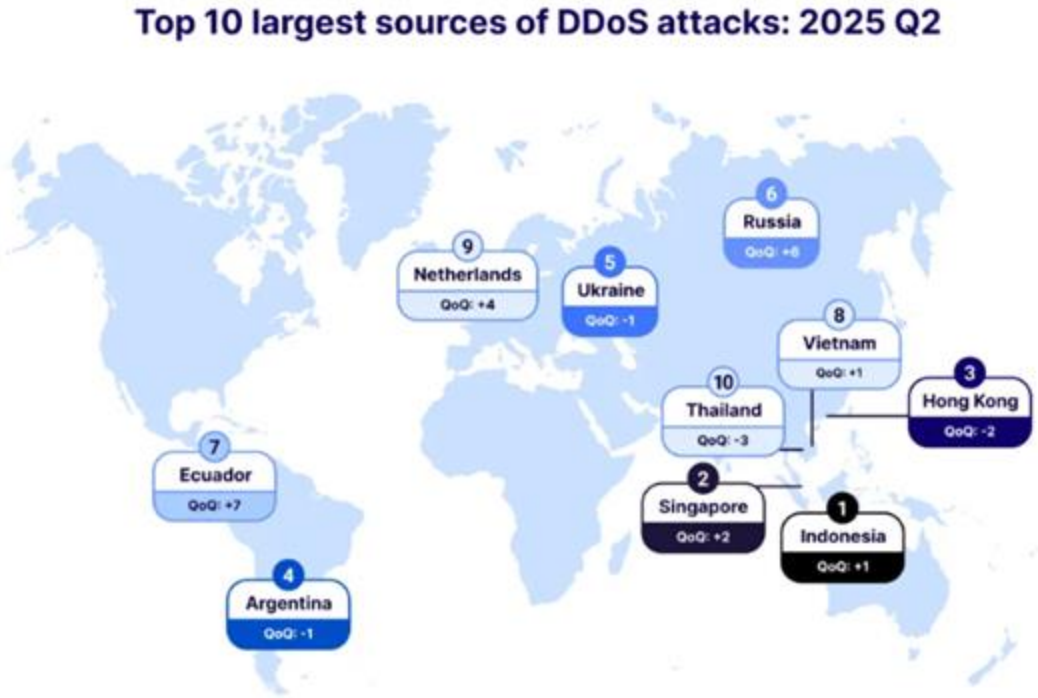


Ransom DDOS Attacks



Top Attacked Locations

Top Sources of DDOS Attacks



Widespread targeting across global industries

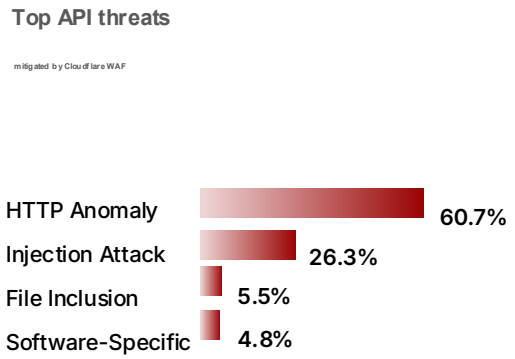
Unmanaged APIs leave organizations exposed

58%

Of Cloudflare HTTP traffic is API related

33%

Of API endpoints are unknown to security teams



Source: Cloudflare report *State of Application Security, 2024*

Phishing is still the #1 attack vector

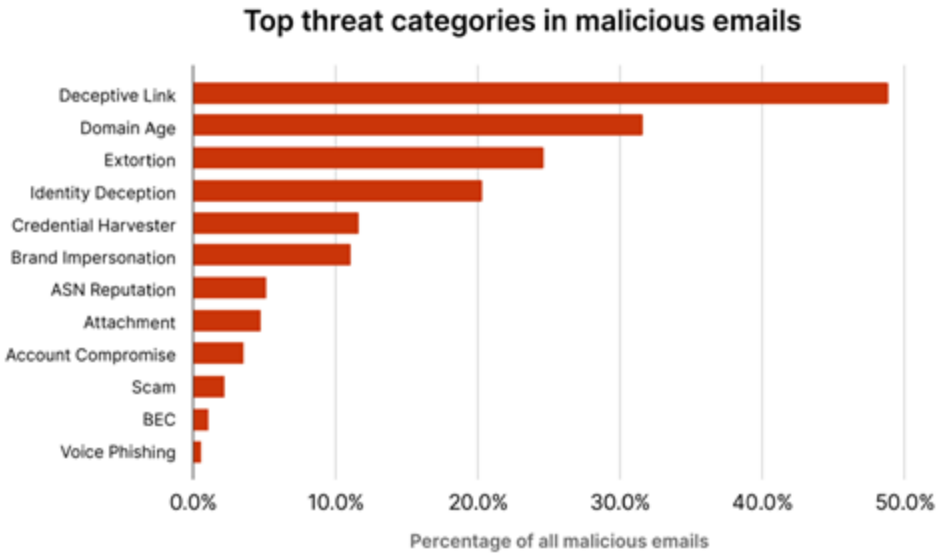
9 of 10
successful cyber attacks start with phishing

~80%
of firms exposed to multi-channel phishing*

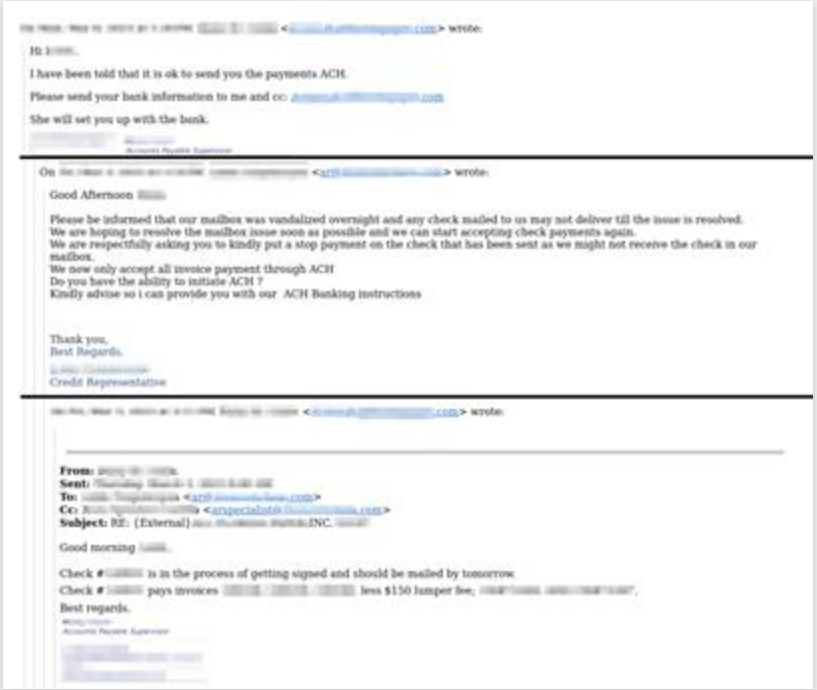
$50 Billion
losses in BEC since 2013, up 17% YoY†

* Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, February 2023
† Source: FBI, BEC the $50 Billion Scam

Deceptive links, & BEC



BEC attempt with entire faked conversation thread



wrote:

Hi

I have been told that it is ok to send you the payments ACH.

Please send your bank information to me and cc:

She will set you up with the bank.

Accounts Payable Supervisor

On wrote:

Good Afternoon

Please be informed that our mailbox was vandalized overnight and any check mailed to us may not deliver till the issue is resolved.
We are hoping to resolve the mailbox issue soon as possible and we can start accepting check payments again.
We are respectfully asking you to kindly put a stop payment on the check that has been sent as we might not receive the check in our mailbox.
We now only accept all invoice payment through ACH
Do you have the ability to initiate ACH ?
Kindly advise so i can provide you with our ACH Banking instructions

Thank you,
Best Regards,

Credit Representative

wrote:

From:
Sent:
To:
Cc:
Subject: RE: [External]

Good morning

Check # is in the process of getting signed and should be mailed by tomorrow

Check # pays invoices less $150 Jumper fee,

Best regards,

Accounts Payable Supervisor

CLOUDFLARE

What do we do next..

Connect, Protect, Build?

Mindset

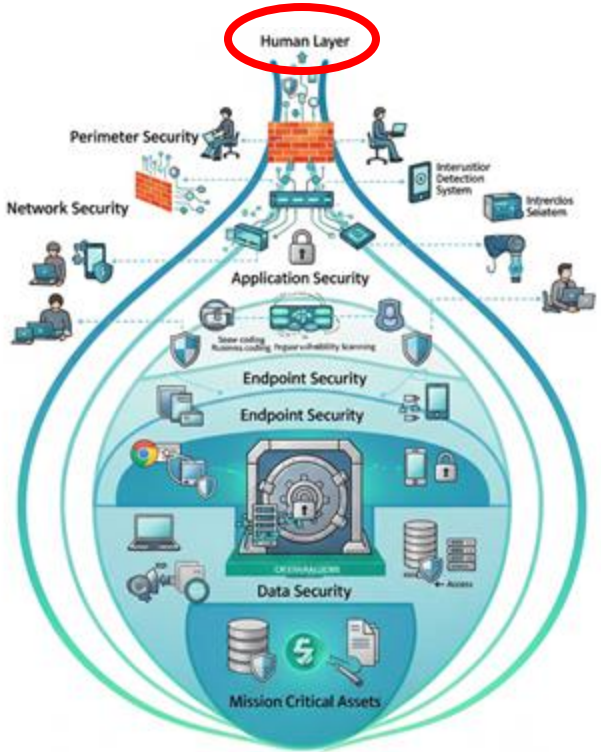
Core Components:

- Assume breach / Zero Trust
- Adversarial Thinking / Think like a hacker
- Risk based approach
- Continuous learning / growth mindset
- Human element as both strength and weakness
- Resilience and recovery
- Data driven decisions
- Holistic and integrated view - not just an IT problem
- Culture..

Connect

Why Mindset? Why Human/People Focus?

7 Layers of Cybersecurity



Human Centric Security

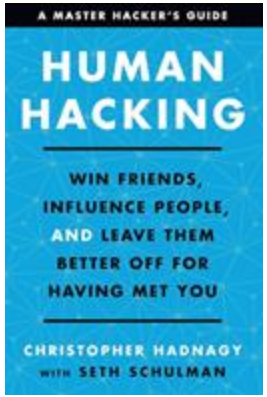
- Human centric security focuses on understanding and adapting to human behaviour, psychology and interaction
- The aim is to build a security culture that empowers employees, reduces human errors and mitigates cyber risks effectively
- **It recognises that humans play a critical role in an organisations security posture**
- **It develops strategies and practises that align with human needs, motivations and capabilities**
- https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
- Applying human factors and AI to move toward human centric cybersecurity culture and solutions

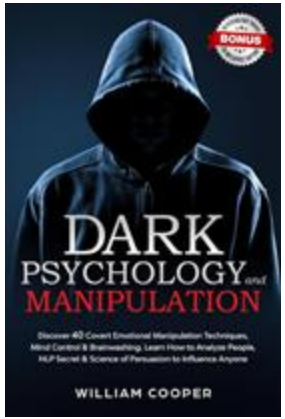
SYDNEY, Australia, February 22, 2024

Gartner Identifies the Top Cybersecurity Trends for 2024

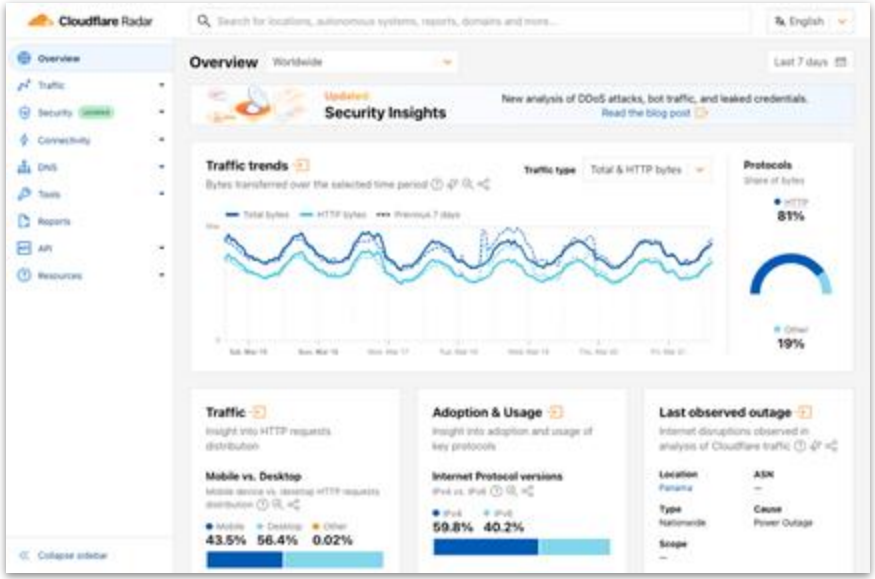
Gartner's Calling for a Human-Centric Approach to Cybersecurity – Here's How to Implement It

Community Driven Collaboration





What is Cloudflare Radar?

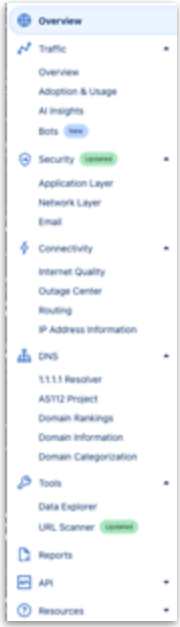


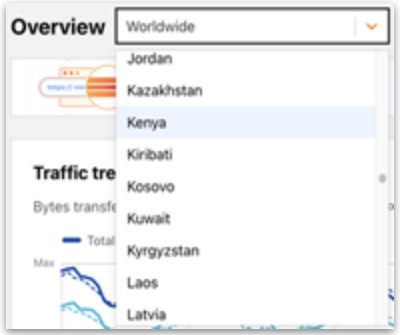
September 30, 2020 launch blog post:

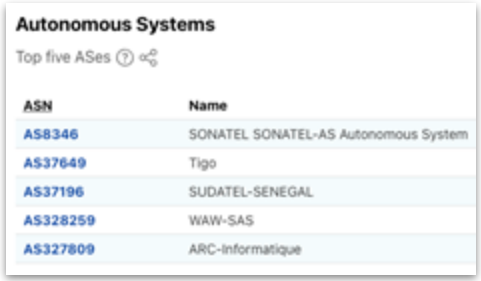
*Our goal is to help build a better Internet and we want to do this by **exposing insights, threats, and trends** based on the **aggregated data** that we have. We want to help anyone **understand what is happening on the Internet** from a **security, performance, and usage** perspective. Every Internet user should have easy access to answer the questions that they have.*

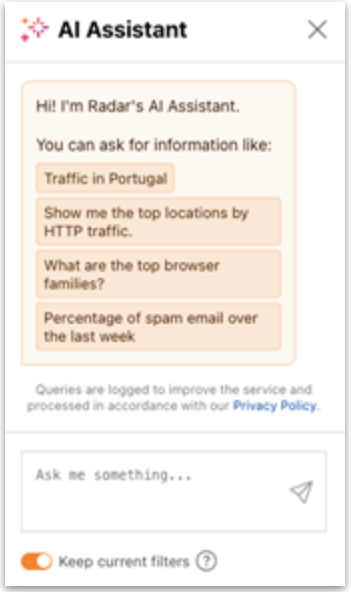
https://radar.cloudflare.com/

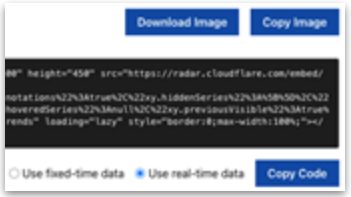
Features and functionality











Network Measurement: from censorship to shutdowns

How can Cloudflare Radar help detect and/or corroborate reports of Internet disruptions?

Macro/aggregate views of:

- Outages
- Internet Traffic
- Adoption & Usage
- Connection Quality
- Routing
- TCP Connection Tampering

Supporting capabilities:

- Graph sharing/embedding
- Notifications
- API

Visibility into filtering/blocking through adoption/usage

Protests in Iran, September 2022

- HTTP versions
- TLS versions

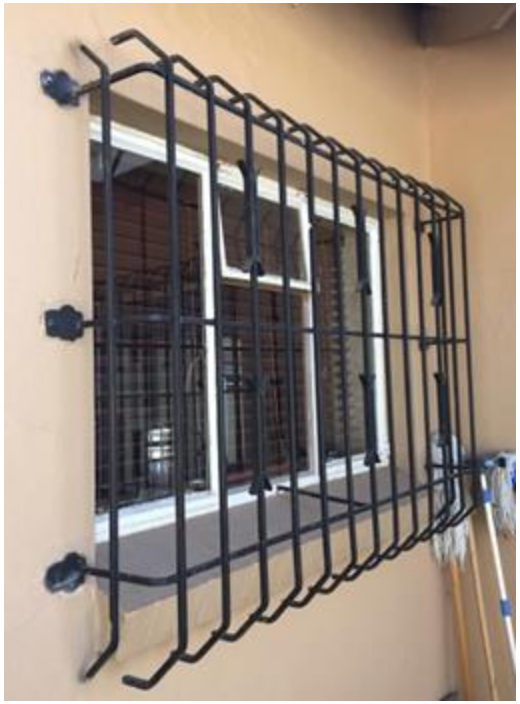
- IPv4 vs IPv6
- HTTP vs HTTPS

- Mobile vs Desktop Devices (Traffic page)

- Data available via API

Physical Security & Cyber Security Alignment

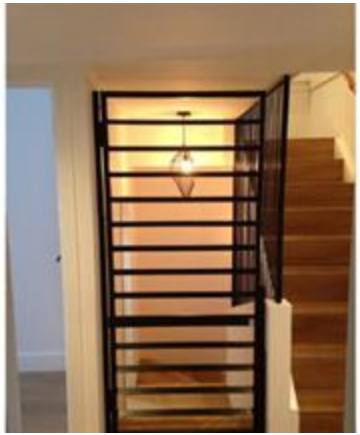
Physical Security & Cyber Security Alignment



Physical Security & Cyber Security Alignment

Physical Security & Cyber Security Alignment

Physical Security & Cyber Security Alignment


Physical Security & Cyber Security Alignment

Who is concerned about Organisational Culture?

Who is concerned about Insider Threat ?

Protect

Shifting to a People First Culture and Cyber Approach

- This approach recognises that employees are a critical part of defense, not just a liability
- The goal is to make security a shared responsibility and to build a sense of trust and collaboration
- This approach also helps to both reduce intentional threats and mitigate accidental ones

Actionable Strategies for Culture Change

Leadership and Communication

- Lead by Example: A security-first mindset must start at the top.
- Foster a "No-Blame" Culture: Encourage employees to report security incidents or mistakes without fear of retribution.

Training and Awareness

- Make it Relevant: Move beyond generic, annual training.
- Focus on the "Why": Explain the reasoning behind security policies.
- When employees understand why a policy exists and how it protects both them and the company, they are more likely to comply.

Collaboration and Accountability

- Break Down Silos: Encourage strong collaboration between security teams and other departments, especially HR, legal, and IT.
- The security team should be seen as an ally, not a punitive force.

Human Centric Security

- For any strategy to be successful, it requires people, process and technology
- **Know your business - know what the employees are doing and need to do - ensure you are communicating with the frontline employees - ensure you are monitoring and identify shadow process and solutions that are sometimes used as workarounds - communication - communication - communication!!**
- Sharing information and intelligence
- Defending through layers
- Security governance and posture management
- Protecting identities
- Protecting endpoints and devices
- Protecting networks
- Protecting applications
- Protecting data and assets
- Detection and Response

Embrace Simplicity and Resilience

- **Double down on employee security awareness training**
  - Consider incorporating an AI awareness module to keep pace with evolving threats
  - Goal should be to empower employees as part of the solution
  - Include you board of directors and c-suite, as they will be prime targets
- **Begin to implement zero trust principles**
  - Back this by robust multi layered security controls with an emphasis on safeguarding email inboxes from phishing attempts
  - Protect users at this common point of entry, the risk of employees inadvertently becoming a vector for attack can be significantly reduced
- **Retire legacy network devices and security appliances**
  - These not only consume time and resource to manage, but they may introduce vulnerabilities to your security stack
  - Streamline your tech stack and consolidate vendors where you can
- **Examine the entire organisation to reduce overall complexity**
  - Reduce the attack surface
  - Refocus on executing well on the fundamentals of cybersecurity
  - Consolidate and simplify where possible

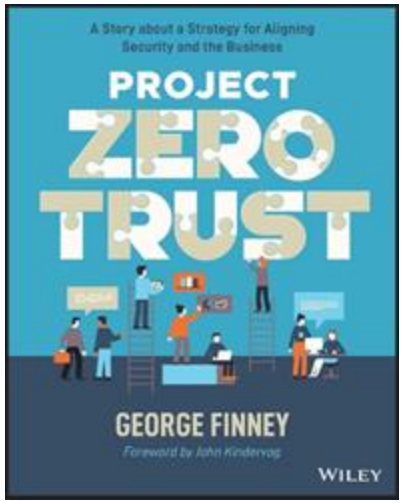
Build

We are living in unprecedented times..

1. AI driven threats require AI powered defenses
2. Zero Trust must be the standard
3. Post Quantum readiness is not a tomorrow problem

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

4. All of this requires C-suite engagement and endorsement
5. Resilience is not optional - its vital!



C Suite moves that build resilience at scale

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

Make resilience a shared strategic mandate

Automate and integrate to ensure scalability

Rethink cyber governance as a competitive advantage

Future proof now, not later

Test for failure - at scale

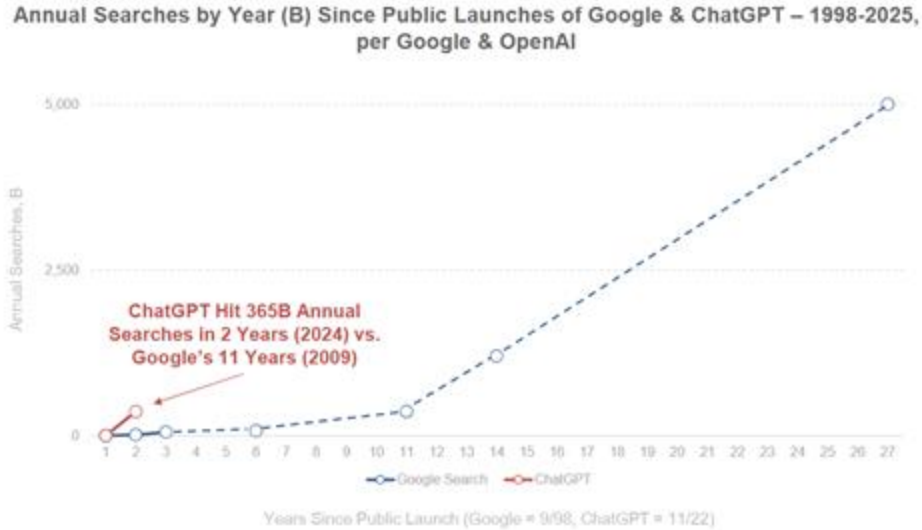
Integrate AI in offense and defense

AI - Demands & Opportunities

The Double Edged Sword..

AI Trends

Time to 365B Annual Searches = ChatGPT 5.5x Faster vs. Google



Trends – Artificial Intelligence (AI)
May 30, 2025

Mary Meeker / Jay Simons / Daegwon Chae / Alexander Krey

BOND

https://www.bondcap.com/report/tai/#view/1

Vint Cerf, one of the 'Founders of the Internet,' said in 1999, '…they say a year in the Internet business is like a dog year – equivalent to seven years in a regular person's life.' At the time, the pace of change catalyzed by the internet was unprecedented.

Widespread LLM adoption

Public LLMs

Accessed outside network boundaries, often for free

Product LLMs

Part of a product or service offered to customers

Internal LLMs

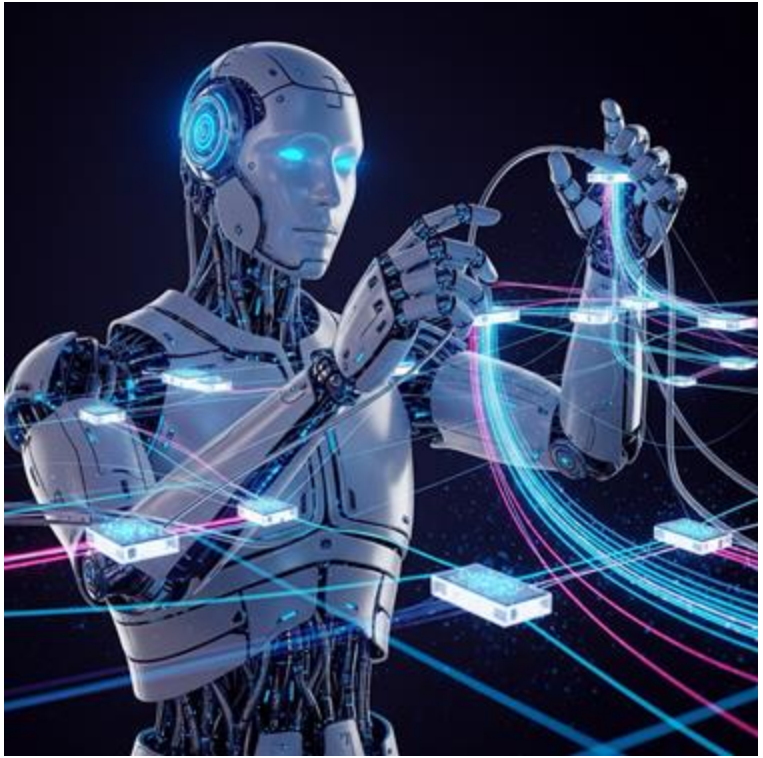
Custom models trained on internal data to assist employees and boost productivity

56% of employees are directly using AI to automate or augment their work

*Source: UKG, AI at Work: It's Here and It's Working, Whether You Know It or Not

Why Define your AI Use Cases First?

- Avoids significant financial waste and overruns
- Ensures business relevance for tangible objectives
- Mitigates risks and implements safeguards
- Shifts focus to a problem-first approach

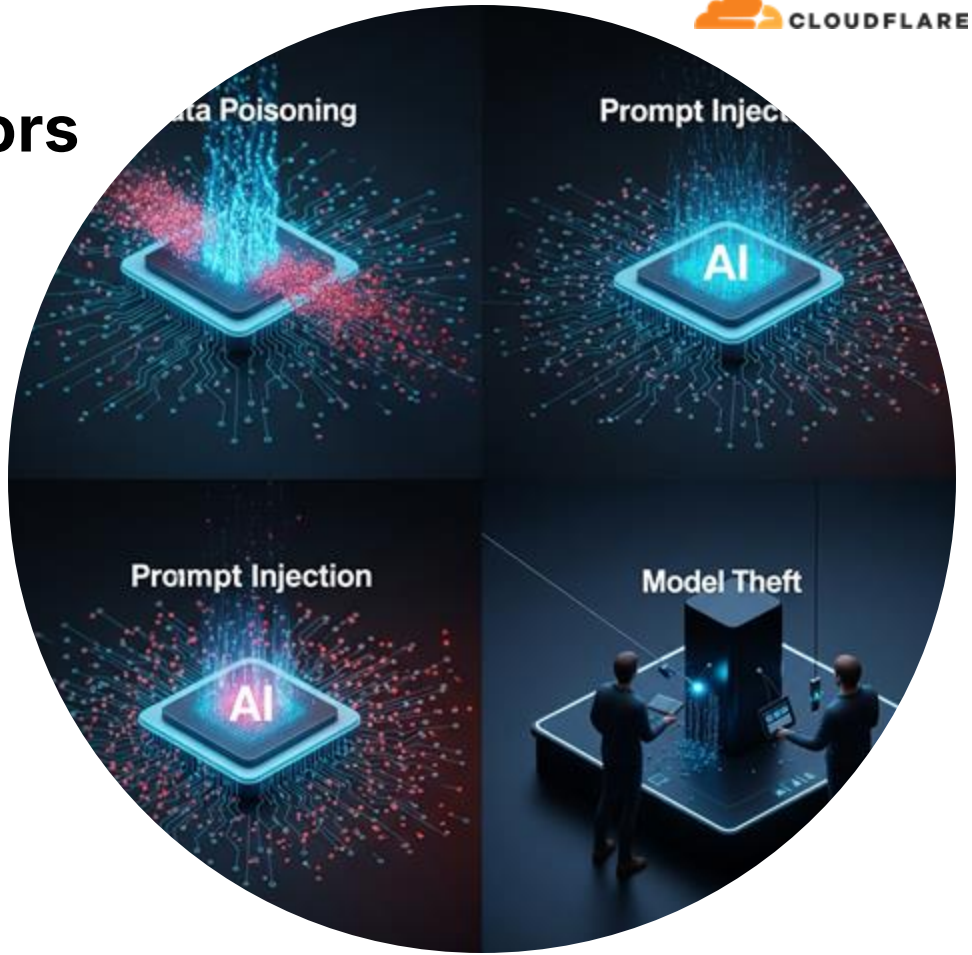


How to Define your AI Use Cases

- Identify business problems and opportunities.
- Assess data availability and quality.
- Evaluate feasibility and potential business impact.
- Create a phased roadmap for implementation.

New AI Model Attack Vectors

- AI models are becoming direct attack targets.
- Data poisoning subtly corrupts AI training data.
- Prompt injection manipulates AI behavior via inputs.
- Model theft allows exploiting or replicating AI.



The Rise of AI Powered Threats

- Phishing and Social Engineering
- Deep Fakes and Impersonation
- Automated Malware
- More important than ever to empower employees

AI - The Demands on the Network

- AI demands new network performance considerations.
- Focus on network quality and performance monitoring.
- Prioritising traffic may become critical again.
- Visibility into network traffic patterns and trends crucial.
- Unpredictability of AI workloads
- Network Congestion Control

AI - The Demands & Opportunities on the Carrier Network

- AI workloads are "bursty" and unpredictable
- Load balancing - AI creates uplink congestion and "elephant flows"
- Uplink Congestion - increasing volume from devices to the cloud/services
- Carriers can offer AI-as-a-Service
- Predictive maintenance enhances service quality
- AI Managed Network Solutions
- Dynamic QoS adjusts network for AI workloads.
- Intelligent traffic avoids congestion via rerouting.
- AI optimizes resource allocation based on demand.
- AI-powered management enhances network performance.

AI - The Demands & Opportunities on the Carrier Network

AI's Bandwidth Boom: How Artificial Intelligence Is Reshaping Internet Usage

How Meta Is Reinforcing its Global Network for AI Traffic

Visibility
Understand the Network

Impact of AI traffic in transport networks

Why global networks are the backbone of AI

AI needs a new networking core. Are we ready for it?

Understanding AI Network Congestion Control: A Comprehensive Guide

The ISP Revolution: How AI and Fiber Are Transforming Internet Access in 2025

AI’s Environmental Cost

- AI driving surge in electricity consumption
- Data centers projected to double energy use
- AI queries consume significant fresh water
- Hardware manufacturing depletes natural resources

AI for Good - Sustainability

- AI optimises energy use across industries
- AI enhances climate action and monitoring
- AI models are becoming more energy-efficient
- Tech companies invest in renewable energy
- Improved hardware reduces consumption

The Human Firewall - Everyday Personal Cyber Habits

- Hover over links and be skeptical of urgency.
- Go directly to the source for verification.
- Use long, unique passphrases or a password manager.
- Limit social media sharing and delete old accounts/audit and reduce online footprint.
- Enable Multi-Factor Authentication for added security.

What is this? (Don't judge a book by its cover)..

Cloudflare AI Week 2025

A week to focus on four core areas to help companies secure and deliver AI experiences safely and securely.

Read the blog!

State of Application Security

Get the report

cfl.re/3KRASrZ

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

Cloudflare Signals Report

5 critical security trends mandating a C-suite response

Get the report

https://cfl.re/signals-2025

Cloudflare Security Brief!

Get the report

cfl.re/security-brief-2024

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

Content Credit:
Cloudflare Threat Intelligence, 2025 Cloudflare Signals Report

Events -

Want to continue this conversation or book a speaker for your next event? I'd love to connect!

Amanda Spencer
Director, Solutions Engineering, ANZ
aspencer@cloudflare.com
https://www.linkedin.com/in/amandaspencer-net/