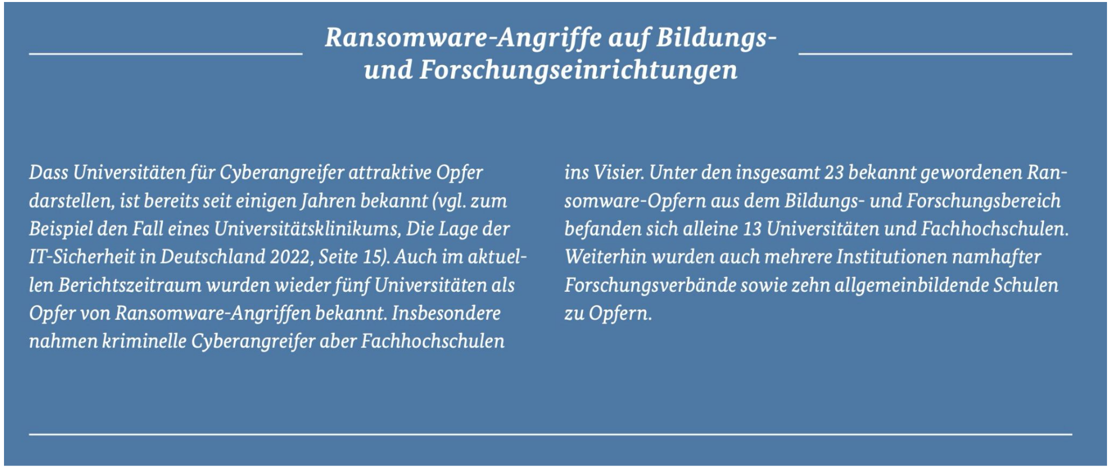
CLOUDFLARE

IT-Sicherheit im Wandel: Cloud-Dienste als Schutzschild für Bildung und Forschung

2024

Aktuelle Lage

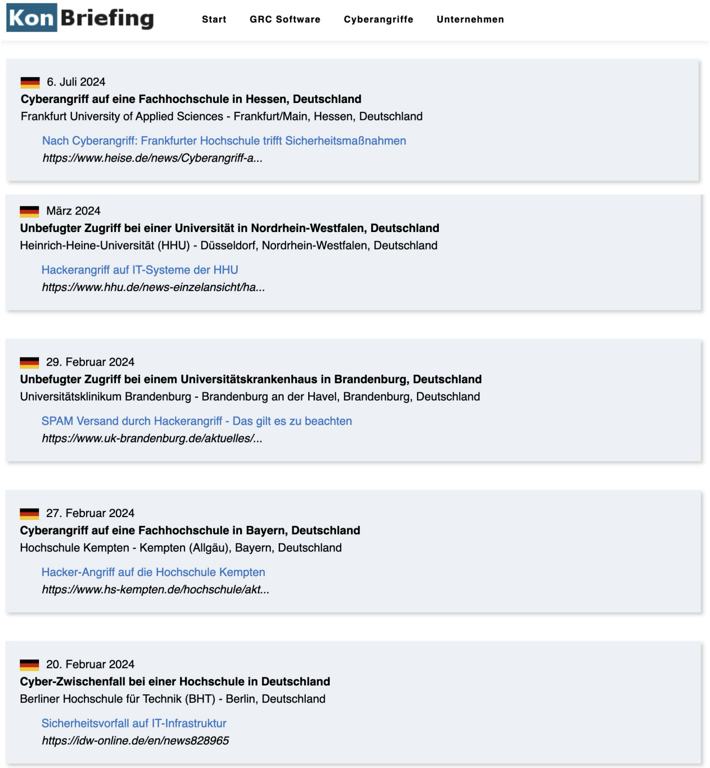
Hochschulen im Visier von Cyberkriminellen



Ransomware-Angriffe auf Bildungs- und Forschungseinrichtungen

Dass Universitäten für Cyberangreifer attraktive Opfer darstellen, ist bereits seit einigen Jahren bekannt (vgl. zum Beispiel den Fall eines Universitätsklinikums, Die Lage der IT-Sicherheit in Deutschland 2022, Seite 15). Auch im aktuellen Berichtszeitraum wurden wieder fünf Universitäten als Opfer von Ransomware-Angriffen bekannt. Insbesondere nahmen kriminelle Cyberangreifer aber Fachhochschulen ins Visier. Unter den insgesamt 23 bekannt gewordenen Ransomware-Opfern aus dem Bildungs- und Forschungsbereich befanden sich alleine 13 Universitäten und Fachhochschulen. Weiterhin wurden auch mehrere Institutionen namhafter Forschungsverbände sowie zehn allgemeinbildende Schulen zu Opfern.

[Bericht zur Lage der IT-Sicherheit in Deutschland]



6. Juli 2024
Cyberangriff auf eine Fachhochschule in Hessen, Deutschland
Frankfurt University of Applied Sciences - Frankfurt/Main, Hessen, Deutschland
Nach Cyberangriff: Frankfurter Hochschule trifft Sicherheitsmaßnahmen
https://www.heise.de/news/Cyberangriff-a...

März 2024
Unbefugter Zugriff bei einer Universität in Nordrhein-Westfalen, Deutschland
Heinrich-Heine-Universität (HHU) - Düsseldorf, Nordrhein-Westfalen, Deutschland
Hackerangriff auf IT-Systeme der HHU
https://www.hhu.de/news-einzelansicht/ha...

29. Februar 2024
Unbefugter Zugriff bei einem Universitätskrankenhaus in Brandenburg, Deutschland
Universitätsklinikum Brandenburg - Brandenburg an der Havel, Brandenburg, Deutschland
SPAM Versand durch Hackerangriff - Das gilt es zu beachten
https://www.uk-brandenburg.de/aktuelles/...

27. Februar 2024
Cyberangriff auf eine Fachhochschule in Bayern, Deutschland
Hochschule Kempten - Kempten (Allgäu), Bayern, Deutschland
Hacker-Angriff auf die Hochschule Kempten
https://www.hs-kempten.de/hochschule/akt...

20. Februar 2024
Cyber-Zwischenfall bei einer Hochschule in Deutschland
Berliner Hochschule für Technik (BHT) - Berlin, Deutschland
Sicherheitsvorfall auf IT-Infrastruktur
https://idw-online.de/en/news828965

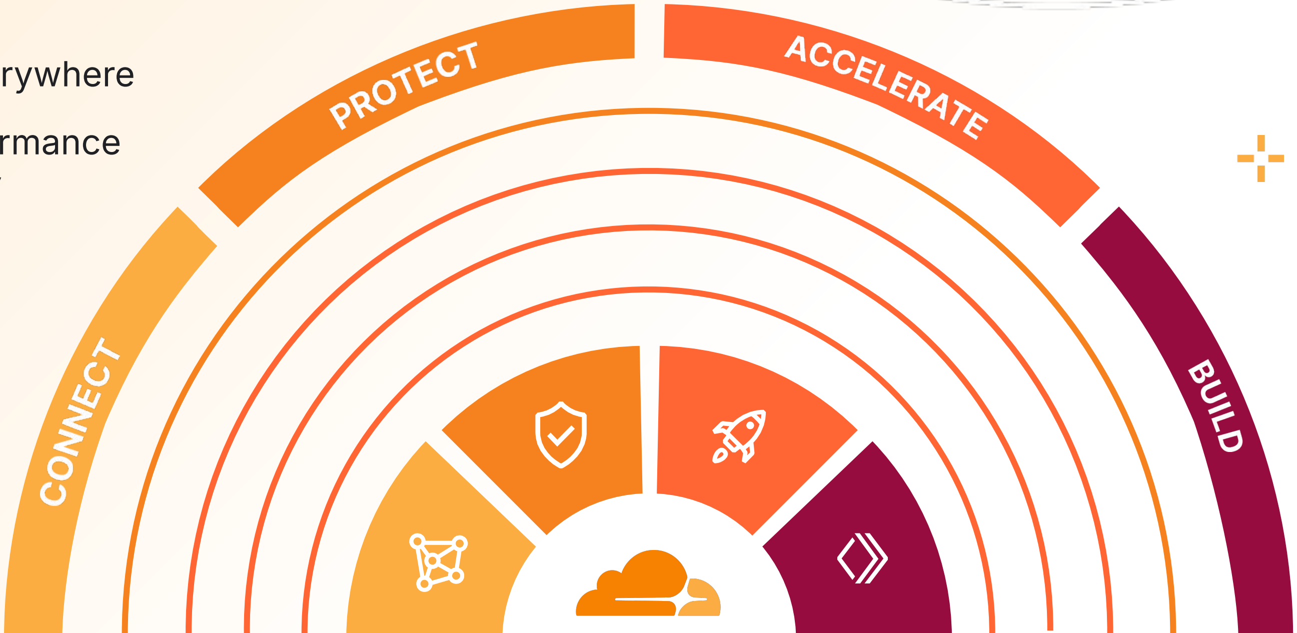
https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html

OUR MISSION

We are helping build a better Internet

With Cloudflare, customers can:

- **Connect** users, networks, applications, and clouds globally
- **Protect** data, applications, infrastructure, and users everywhere
- **Accelerate** application performance and user experiences on any device, anywhere
- **Build** full-stack applications on a modern cloud platform with no vendor lock-in



A single network that delivers local capabilities with global scale

320+ cities

in 120+ countries, including mainland China

~50 ms

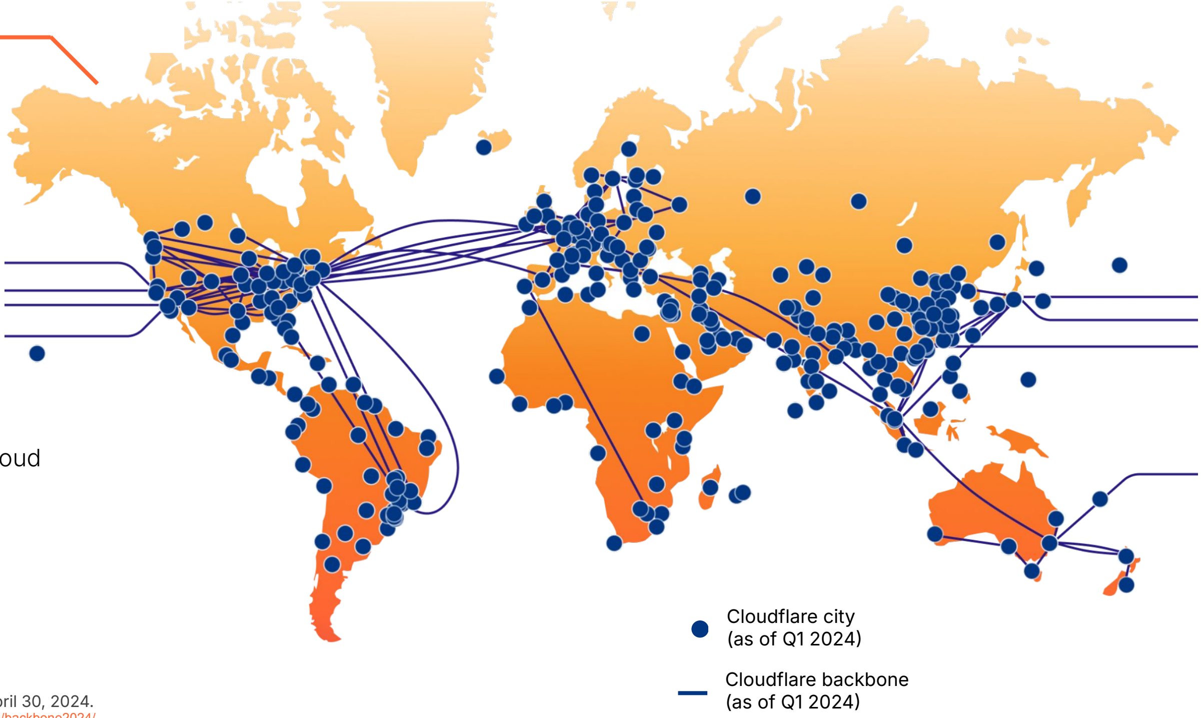
from ~95% of the world's Internet-connected population

~13,000 networks

directly connect to Cloudflare, including ISPs, cloud providers, and large enterprises

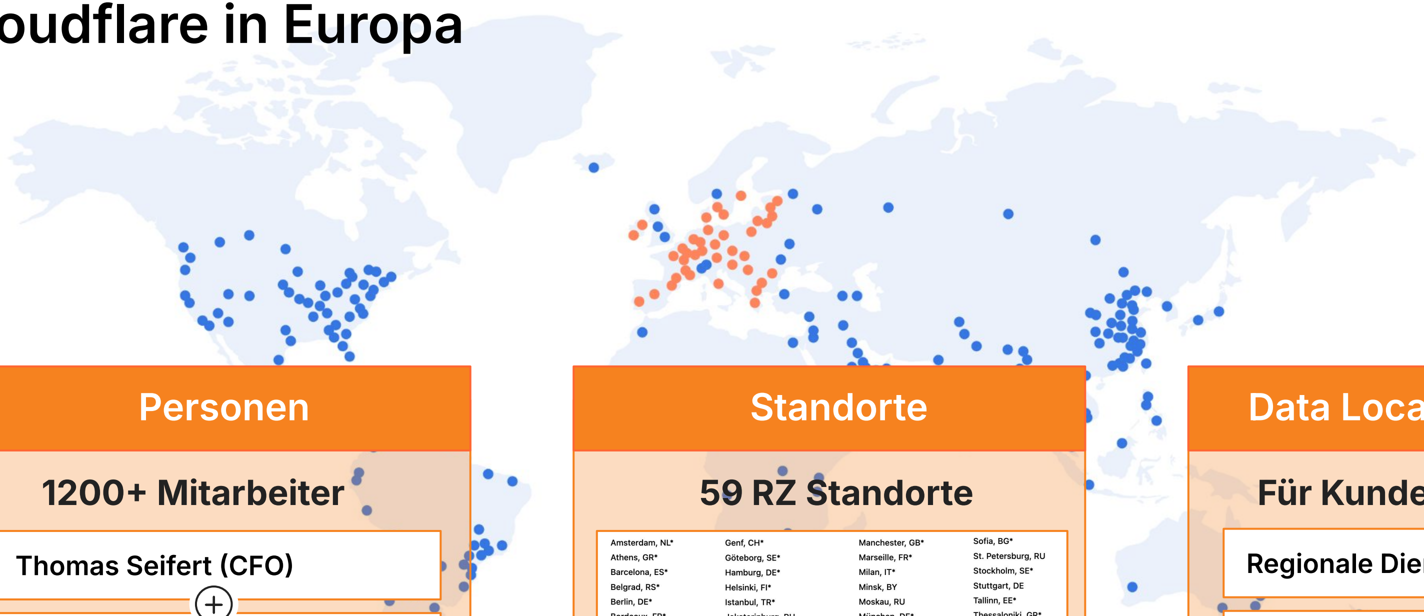
280 Tbps

of network capacity and growing


● Cloudflare city (as of Q1 2024)
— Cloudflare backbone (as of Q1 2024)

Note: Figures as of March 31, 2024, except for network capacity, which is as of April 30, 2024.
https://blog.cloudflare.com/backbone2024/

Cloudflare in Europa



Personen

1200+ Mitarbeiter

Thomas Seifert (CFO)

+

John Graham-Cumming (CTO)

+

Dr. Katrin Suder (Vorstand)

Standorte

59 RZ Standorte

Amsterdam, NL*
Athens, GR*
Barcelona, ES*
Belgrad, RS*
Berlin, DE*
Bordeaux, FR*
Bratislava, SK*
Brüssel, BE*
Budapest, HU*
Bukarest, RO*
Cork, IE*
Dublin, IE*
Düsseldorf, DE*
Edinburgh, GB*
Frankfurt, DE*

Genf, CH*
Göteborg, SE*
Hamburg, DE*
Helsinki, FI*
Istanbul, TR*
Jekaterinburg, RU
Khabarovsk, RU
Kiew, UA
Kopenhagen, DK*
Krasnoyarsk, RU
Lissabon, PT*
London, GB*
Luxembourg City, LU*
Lyon, FR*
Madrid, ES*

Manchester, GB*
Marseille, FR*
Milan, IT*
Minsk, BY
Moskau, RU
München, DE*
Nikosia, CY
Oslo, NO*
Palermo, IT*
Paris, FR*
Prag, CZ*
Reykjavík, IS*
Riga, LV*
Rom, IT*
Skopje, MK

Sofia, BG*
St. Petersburg, RU
Stockholm, SE*
Stuttgart, DE
Tallinn, EE*
Thessaloniki, GR*
Tirana, AL
Tver, RU
Vilnius, LT*
Warschau, PL*
Wien, AT*
Zagreb, HR*
Zürich, CH*
İzmir, TR

*Standorte für KI-Inferenz

Data Localization Suite

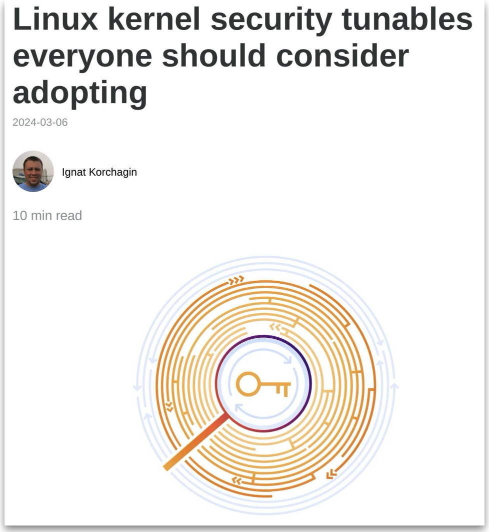
Für Kunden entwickelt

Regionale Dienste

Geo Key Manager (keyless SSL)

Meta Data Boundary

Further Information



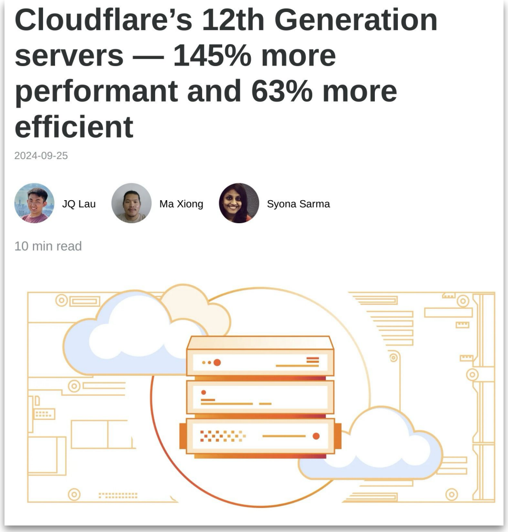
Linux kernel security tunables everyone should consider adopting

2024-03-06

Ignat Korchagin

10 min read

https://blog.cloudflare.com/linux-kernel-hardening/



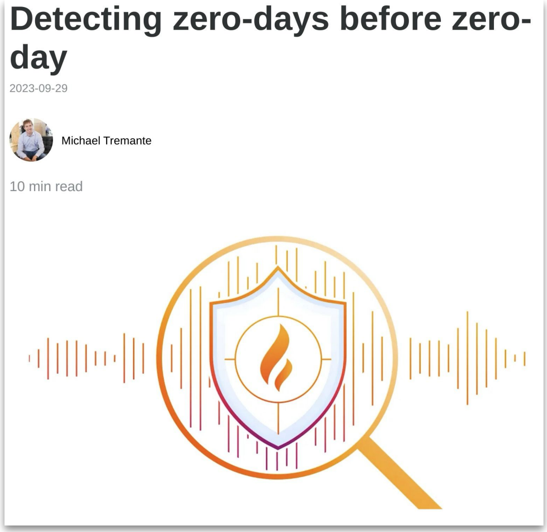
Cloudflare's 12th Generation servers — 145% more performant and 63% more efficient

2024-09-25

JQ Lau Ma Xiong Syona Sarma

10 min read

https://blog.cloudflare.com/gen-12-servers/



Detecting zero-days before zero-day

2023-09-29

Michael Tremante

10 min read

https://blog.cloudflare.com/detecting-zero-days-before-zero-day/

ARCHITECTURE AT MASSIVE SCALE

To provide a private, secure, reliable, performant, agile enterprise-grade Internet experience, Cloudflare is everywhere

209B

Daily threats blocked

3T

DNS Requests daily

55M

HTTP requests per second

This is only possible because ~20% of the Web runs on Cloudflare

Welche Erkenntnisse liefert ein globales Netz?

Project Galileo

EST. 2014

Humanitarian organizations, artistic groups, and the voices of political dissent are often vulnerable to cyber attacks. In collaboration with 50+ civil society partners, Cloudflare protects public interest groups from attacks intended to silence them online.

Learn more and apply at
cloudflare.com/galileo

2,400
Internet properties

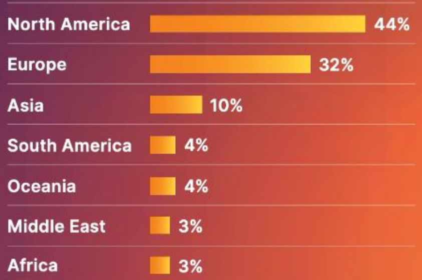
111
countries

67.7 million
average number of daily attacks Cloudflare mitigates for participants

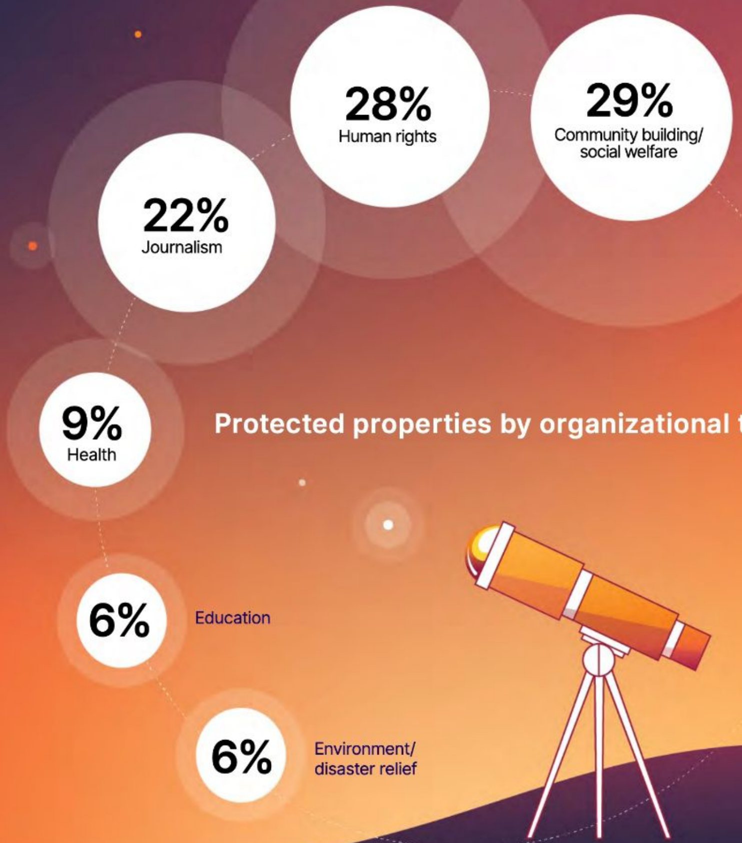
2 billion
average number of monthly attacks Cloudflare mitigates for participants

50+
partners to help identify at-risk sites

Protected properties by region



Protected properties by organizational type



Athenian Project

EST. 2014

We created the Athenian Project to ensure that state and local governments have the highest level of protection and reliability for free, so that their constituents have access to election information and voter registration.

Learn more and apply at **cloudflare.com/athenian**

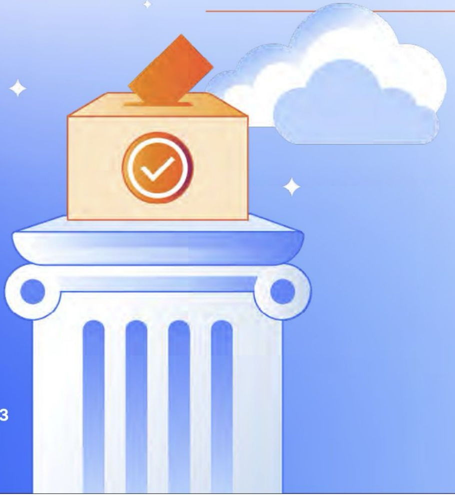
Election security at a glance

390
Internet properties protected

6
countries

33 US states
receive free Cloudflare services through the Athenian Project

213.78 million
threats to government election websites mitigated between November 1, 2022, and August 31, 2023, an average of 703,223 threats per day



Securing infrastructure with Project Safekeeping

In 2022, we launched Project Safekeeping to support critical yet vulnerable infrastructure such as neighborhood hospitals, water treatment facilities, and local energy providers. These types of entities can be obvious targets for attack since they support the basic functioning of communities.

Through Project Safekeeping, we offer free Zero Trust tools to help organizations:

- Connect users to applications
- Protect sensitive data
- Filter traffic
- Improve email security
- Secure cloud applications
- Increase web browsing safety

To be considered for the program, infrastructure entities must meet these requirements:

- ✓ Located in Japan, Australia, Germany, Portugal, or the United Kingdom
- ✓ Considered critical infrastructure by governments in their respective localities
- ✓ Up to 50 people and/or less than USD $10 million in annual revenue/ balance sheet total

Cloudflare assistance to Ukraine

Since the Russian invasion, Cloudflare has protected Ukrainian government institutions, civil society organizations, and citizens from cyber attack at no cost. We have provided updates on the status of the Internet inside Ukraine, making sure valuable information gets out to the world.

Free services for Ukrainian government and infrastructure

On February 24, 2022, when Russia invaded Ukraine, Cloudflare moved quickly to offer free services and support to a wide variety of Ukrainian government and infrastructure providers. In addition to **protecting the .ua top-level domain**, we currently protect approximately 130 Ukrainian domains in this program, run by more than 50 different Ukrainian government agencies and companies.

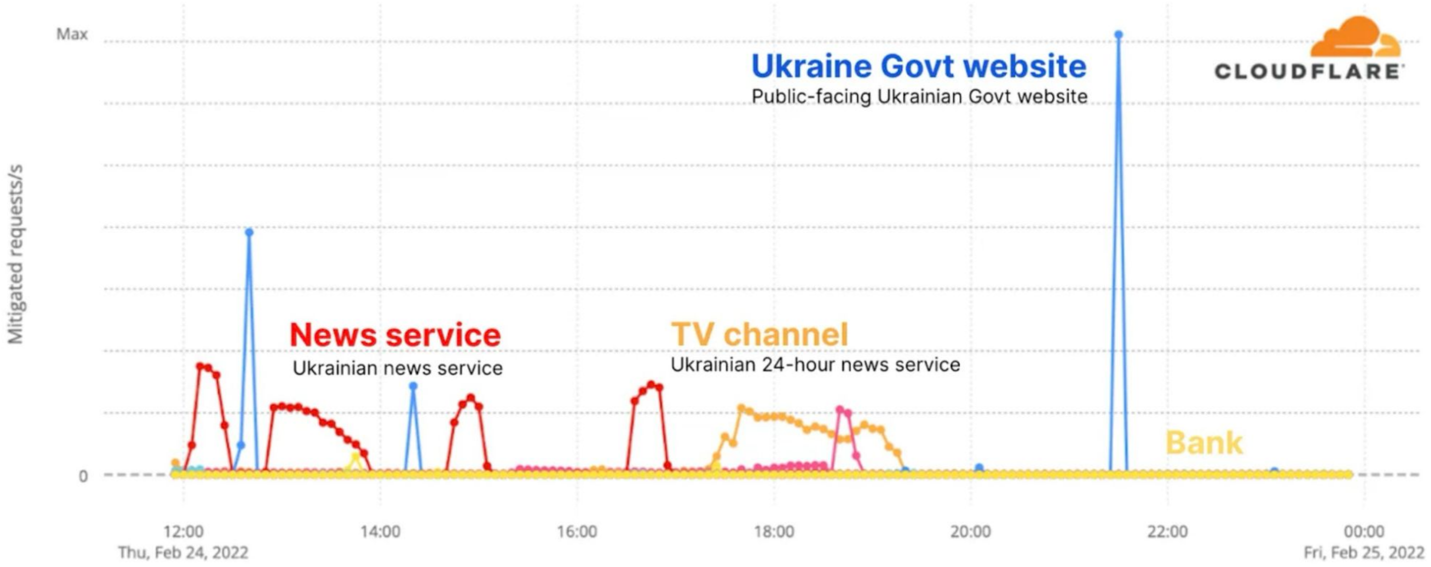
Free services for Ukrainian nonprofits

We've also provided free assistance to nonprofit groups that are helping refugees, documenting war crimes, sharing information, and providing local services — these groups are simultaneously contending with cyber attacks. Overall, we protect 79 organizations in Ukraine, which includes 54 onboarded since the beginning of the invasion.

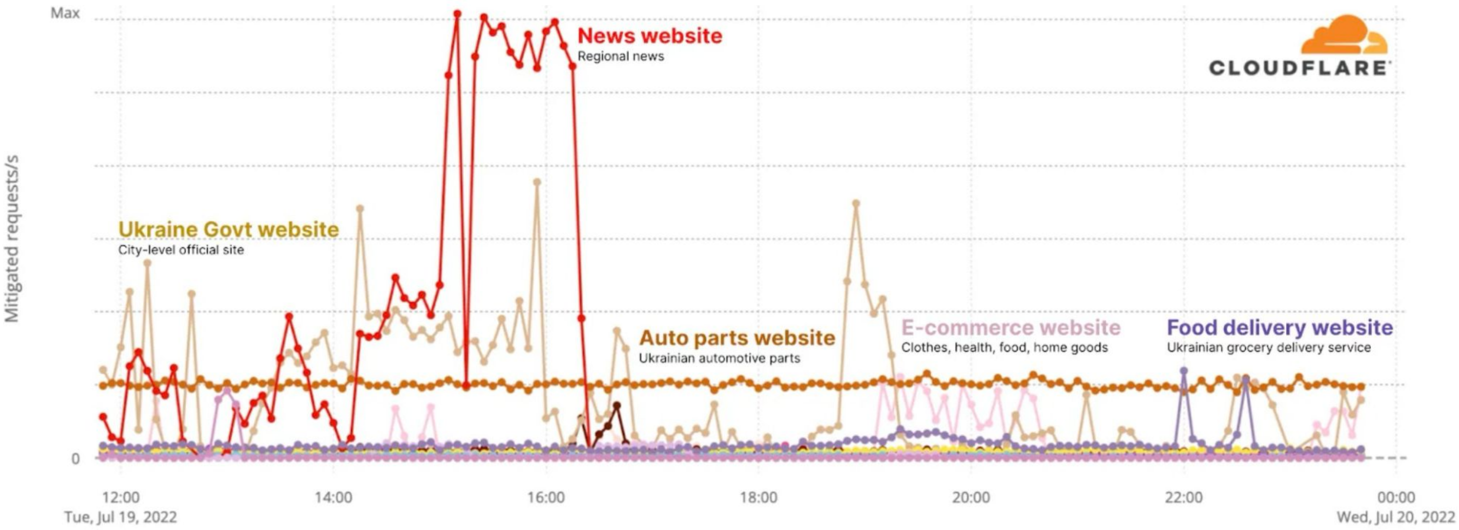
" I want to mention Cloudflare because they reached out to us proactively and offered help. We took their help and we relied on them immensely and I really want to express gratitude to the leadership and the team there."

— Dimitry Kohmanyuk, .ua TLD strategist in Heise Online interview, 3/24/22

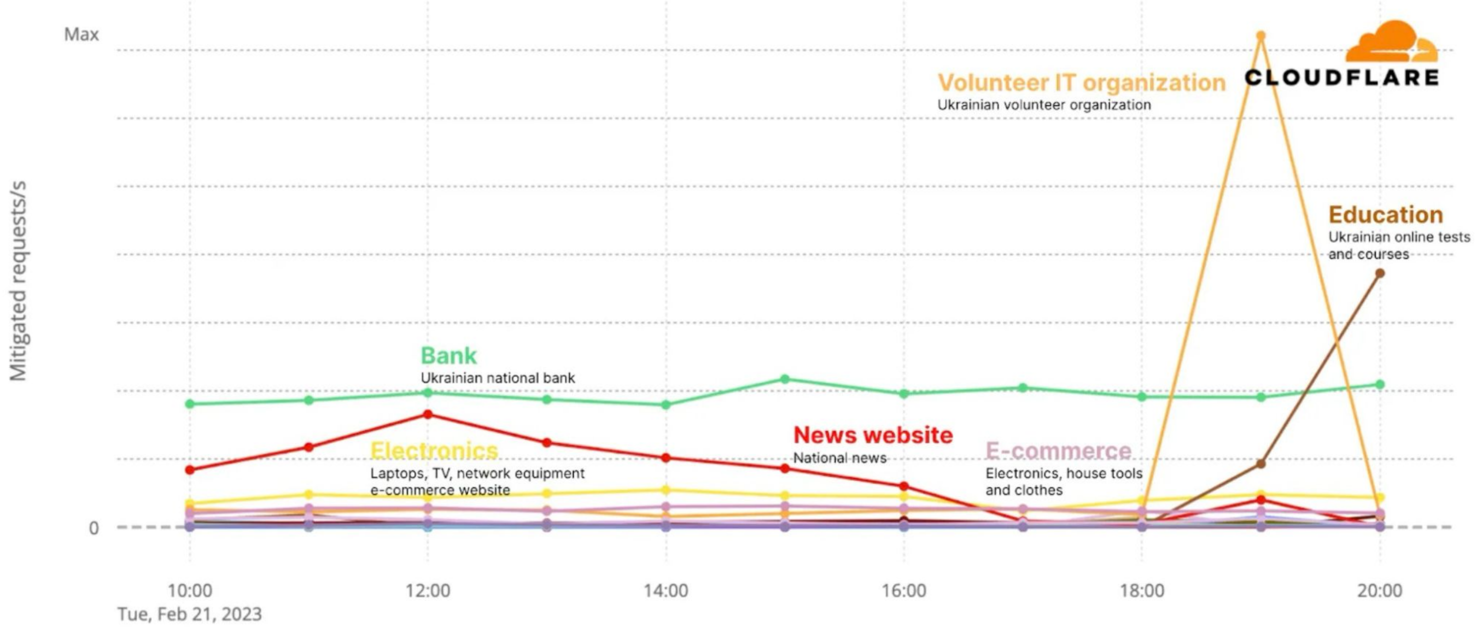
Traffic in Ukraine



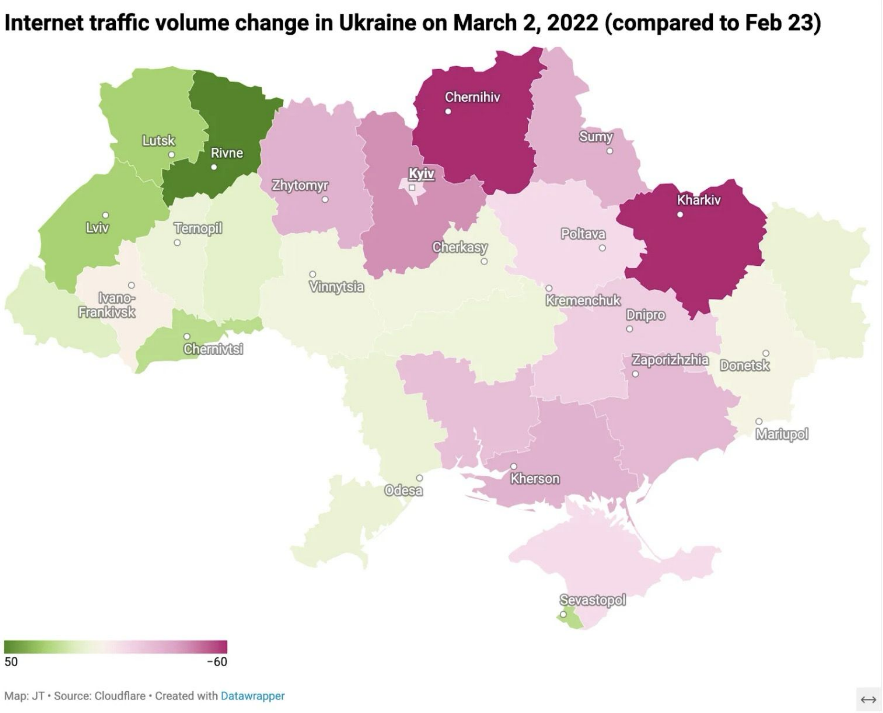
Traffic in Ukraine



Traffic in Ukraine



Traffic in Ukraine

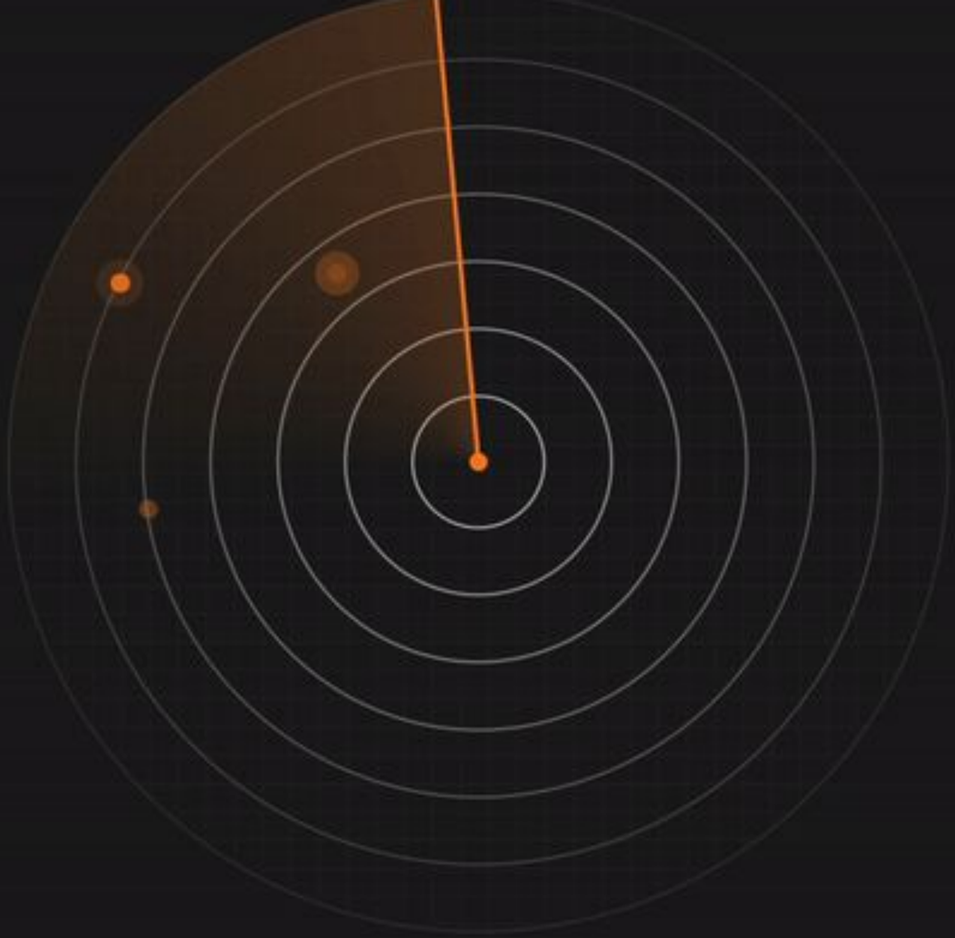


Internet traffic volume change in Ukraine on March 2, 2022 (compared to Feb 23)

Map: JT • Source: Cloudflare • Created with Datawrapper

Source: https://datawrapper.dwcdn.net/dsUSJ/2/

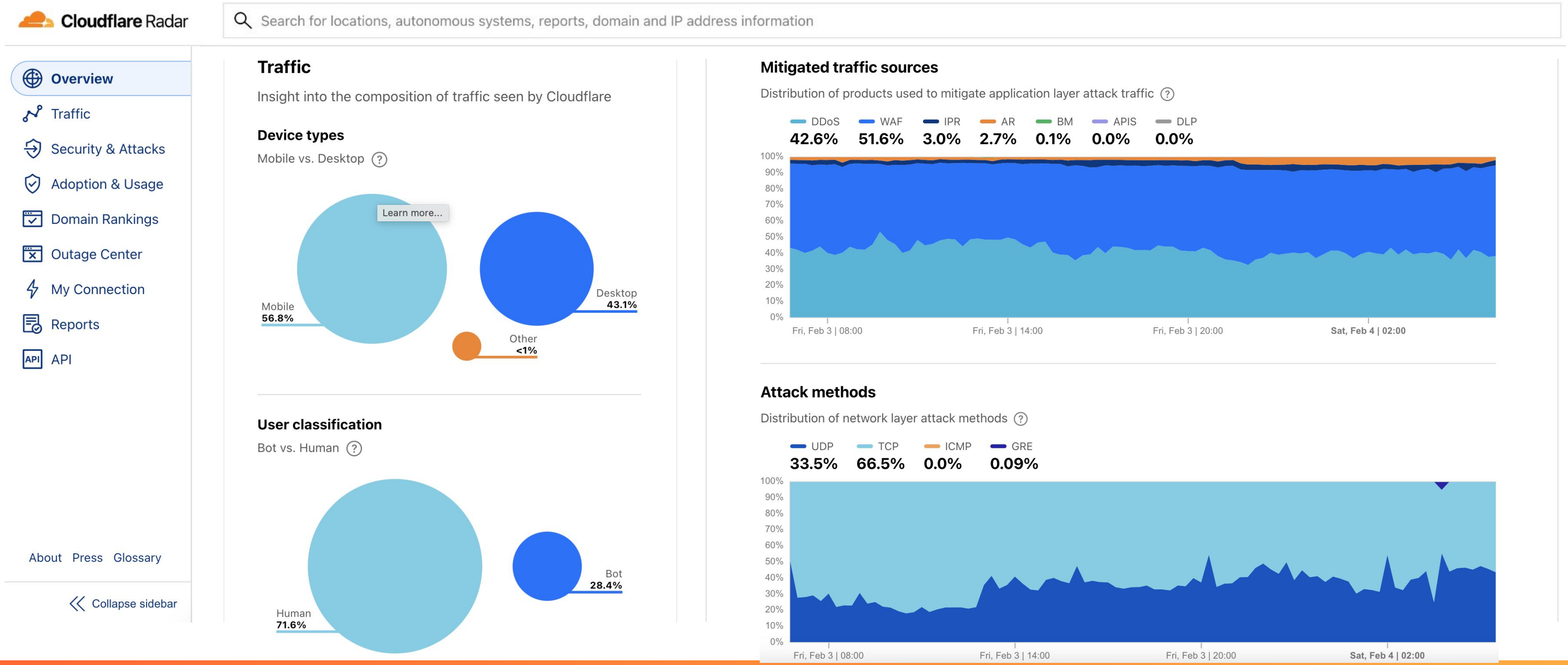
Cloudflare Radar



Cloudflare Radar

CLOUDFLARE RADAR

radar.cloudflare.com



Traffic

Insight into the composition of traffic seen by Cloudflare

Device types

Mobile vs. Desktop ?

User classification

Bot vs. Human ?

Mitigated traffic sources

Distribution of products used to mitigate application layer attack traffic ?

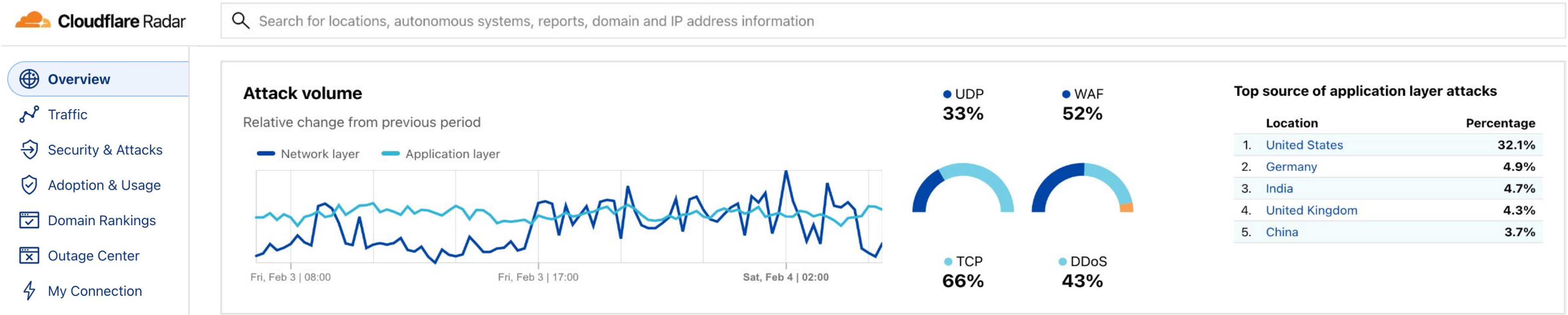
DDoS	WAF	IPR	AR	BM	APIS	DLP
42.6%	51.6%	3.0%	2.7%	0.1%	0.0%	0.0%

Attack methods

Distribution of network layer attack methods ?

UDP	TCP	ICMP	GRE
33.5%	66.5%	0.0%	0.09%

radar.cloudflare.com



Cloudflare Radar

Search for locations, autonomous systems, reports, domain and IP address information

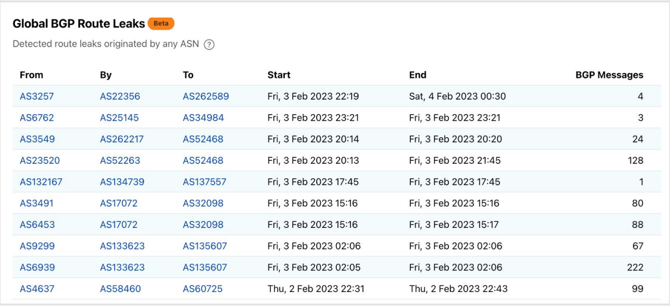
- Overview
- Traffic
- Security & Attacks
- Adoption & Usage
- Domain Rankings
- Outage Center
- My Connection

Attack volume

Relative change from previous period

Top source of application layer attacks

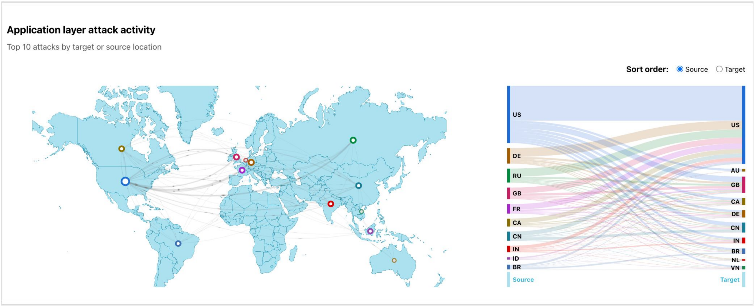
	Location	Percentage
1.	United States	32.1%
2.	Germany	4.9%
3.	India	4.7%
4.	United Kingdom	4.3%
5.	China	3.7%



Global BGP Route Leaks Beta

Detected route leaks originated by any ASN

From	By	To	Start	End	BGP Messages
AS3257	AS22356	AS262589	Fri, 3 Feb 2023 22:19	Sat, 4 Feb 2023 00:30	4
AS6762	AS25145	AS34984	Fri, 3 Feb 2023 23:21	Fri, 3 Feb 2023 23:21	3
AS3549	AS262217	AS52468	Fri, 3 Feb 2023 20:14	Fri, 3 Feb 2023 20:20	24
AS23520	AS52263	AS52468	Fri, 3 Feb 2023 20:13	Fri, 3 Feb 2023 21:45	128
AS132167	AS134739	AS137557	Fri, 3 Feb 2023 17:45	Fri, 3 Feb 2023 17:45	1
AS3491	AS17072	AS32098	Fri, 3 Feb 2023 15:16	Fri, 3 Feb 2023 15:16	80
AS6453	AS17072	AS32098	Fri, 3 Feb 2023 15:16	Fri, 3 Feb 2023 15:17	88
AS9299	AS133623	AS135607	Fri, 3 Feb 2023 02:06	Fri, 3 Feb 2023 02:06	67
AS6939	AS133623	AS135607	Fri, 3 Feb 2023 02:05	Fri, 3 Feb 2023 02:06	222
AS4637	AS58460	AS60725	Thu, 2 Feb 2023 22:31	Thu, 2 Feb 2023 22:43	99

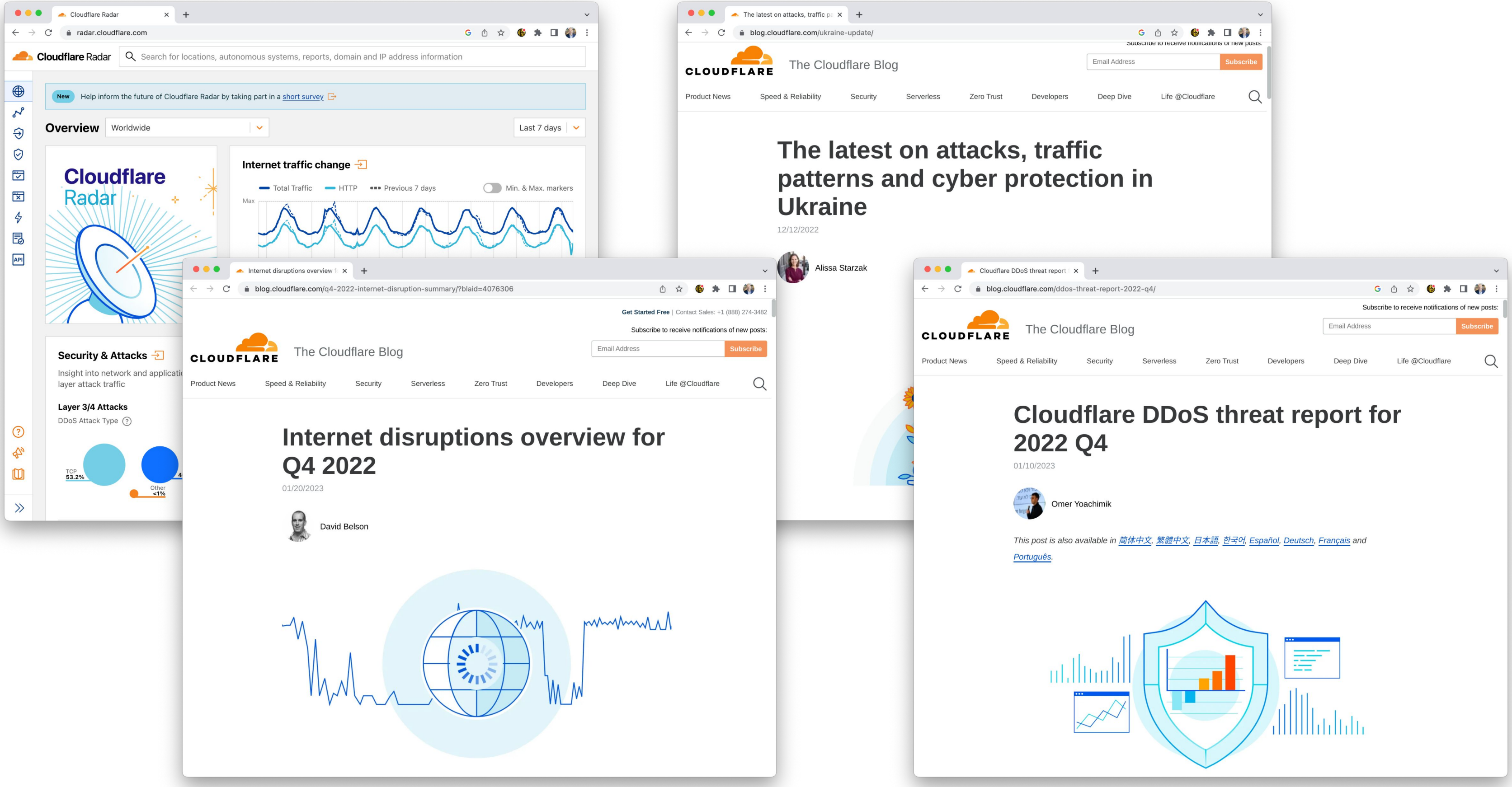


Application layer attack activity

Top 10 attacks by target or source location

Sort order: ● Source ○ Target

CLOUDFLARE RADAR



Cloudflare Radar

radar.cloudflare.com

Cloudflare Radar

Search for locations, autonomous systems, reports, domain and IP address information

New Help inform the future of Cloudflare Radar by taking part in a short survey

Overview Worldwide Last 7 days

Cloudflare Radar

Internet traffic change

Total Traffic HTTP Previous 7 days Min. & Max. markers

Max

Security & Attacks

Insight into network and applicati layer attack traffic

Layer 3/4 Attacks

DDoS Attack Type

TCP 53.2%

Other <1%

The latest on attacks, traffic pa

blog.cloudflare.com/ukraine-update/

Subscribe to receive notifications of new posts:

CLOUDFLARE The Cloudflare Blog

Email Address Subscribe

Product News | Speed & Reliability | Security | Serverless | Zero Trust | Developers | Deep Dive | Life @Cloudflare

The latest on attacks, traffic patterns and cyber protection in Ukraine

12/12/2022

Alissa Starzak

Internet disruptions overview f

blog.cloudflare.com/q4-2022-internet-disruption-summary/?blaid=4076306

Get Started Free | Contact Sales: +1 (888) 274-3482

Subscribe to receive notifications of new posts:

CLOUDFLARE The Cloudflare Blog

Email Address Subscribe

Product News | Speed & Reliability | Security | Serverless | Zero Trust | Developers | Deep Dive | Life @Cloudflare

Internet disruptions overview for Q4 2022

01/20/2023

David Belson

Cloudflare DDoS threat report f

blog.cloudflare.com/ddos-threat-report-2022-q4/

Subscribe to receive notifications of new posts:

CLOUDFLARE The Cloudflare Blog

Email Address Subscribe

Product News | Speed & Reliability | Security | Serverless | Zero Trust | Developers | Deep Dive | Life @Cloudflare

Cloudflare DDoS threat report for 2022 Q4

01/10/2023

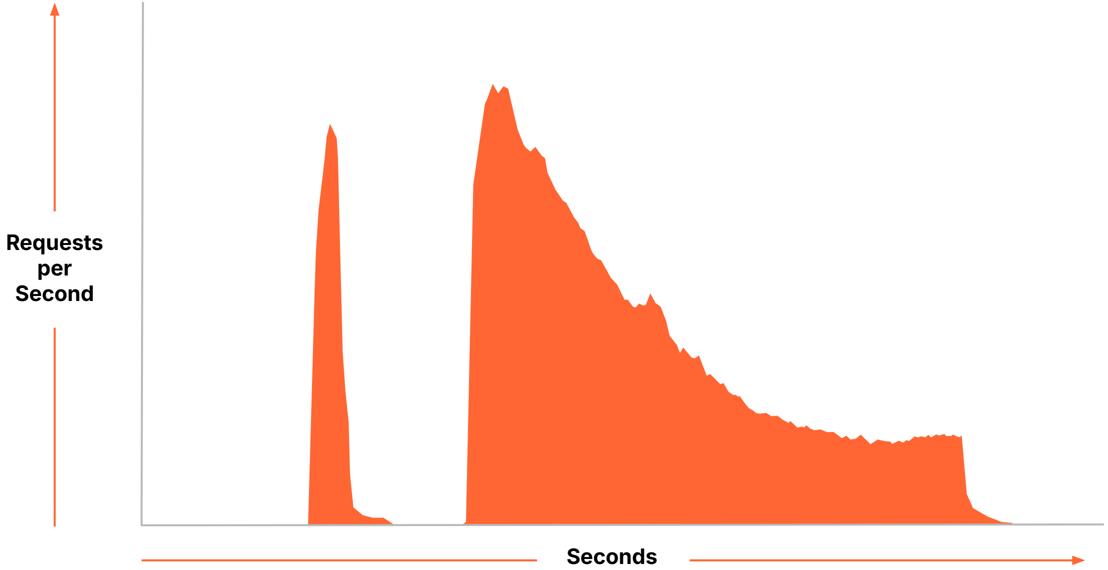
Omer Yoachimik

This post is also available in 简体中文, 繁體中文, 日本語, 한국어, Español, Deutsch, Français and Português.

Angriffsarten

DDoS

Cloudflare stops record-breaking DDoS attack

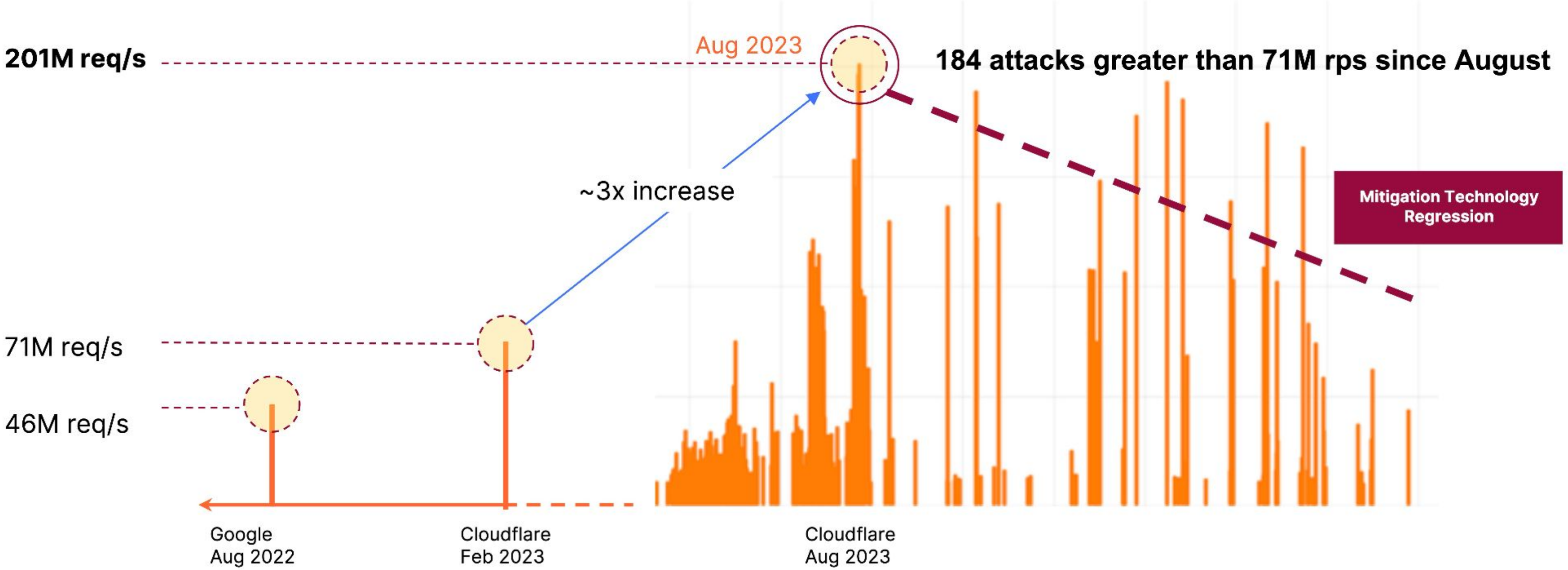


ATTACK DETAILS:

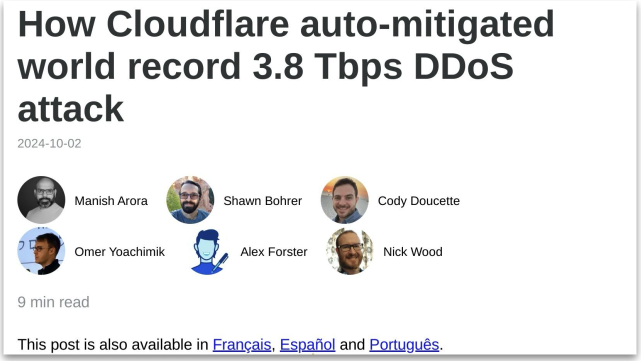
- **Attack vector:** HTTP/2
- **Bots:** 30K
- **Botnet type:** VPS-based
- **Rate:** 71M rps
- **Duration:** <5 minutes

For more details, read our blog post: https://blog.cloudflare.com/cloudflare-mitigates-record-breaking-71-million-request-per-second-ddos-attack/

Cloudflare was attacked and we mitigated against the largest HTTP DDoS attack on our record



For more details, read our blog post: https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/



How Cloudflare auto-mitigated world record 3.8 Tbps DDoS attack

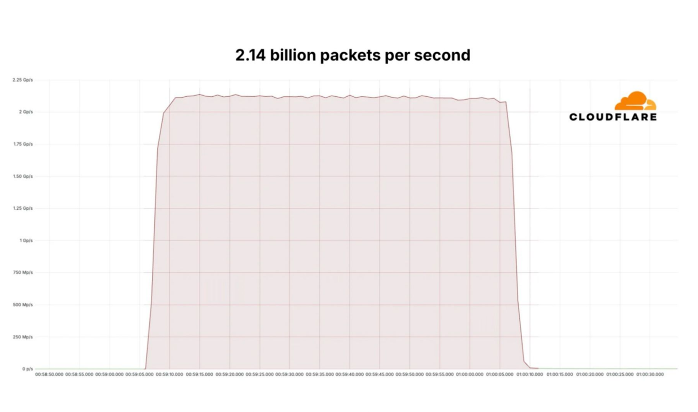
2024-10-02

Manish Arora · Shawn Bohrer · Cody Doucette · Omer Yoachimik · Alex Forster · Nick Wood

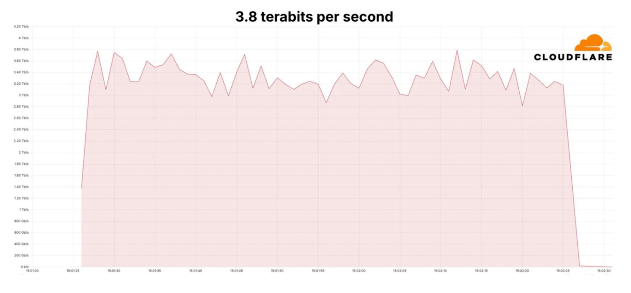
9 min read

This post is also available in Français, Español and Português.

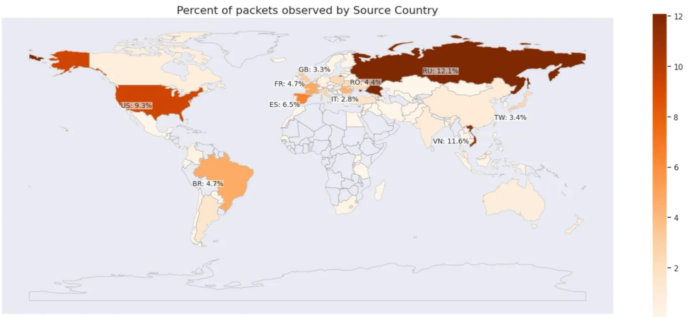
https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/



A mitigated 2.14 billion packet per second DDoS attack that lasted 60 seconds



A mitigated 3.8 Terabits per second DDoS attack that lasted 65 seconds



APIs

Key Findings

2024 API Security & Management Report by Cloudflare

APIs dominate the web

Successful API requests accounted for 57% of Internet traffic (dynamic HTTP traffic) processed by Cloudflare

Shadow APIs

Machine learning models discovered nearly one-third (30.7%) more API endpoints than what organizations self-reported

#1 attack mitigated: DDoS

One-third (33%) of API mitigations comprised blocking Distributed Denial of Service (DDoS) attacks

+ many more

The unfortunate side-effect of the API explosion...

So many APIs living in the shadows

Uneven, sometimes broken, attempts at building security into APIs

No consolidated analytics and management

Shadow APIs and associated risks

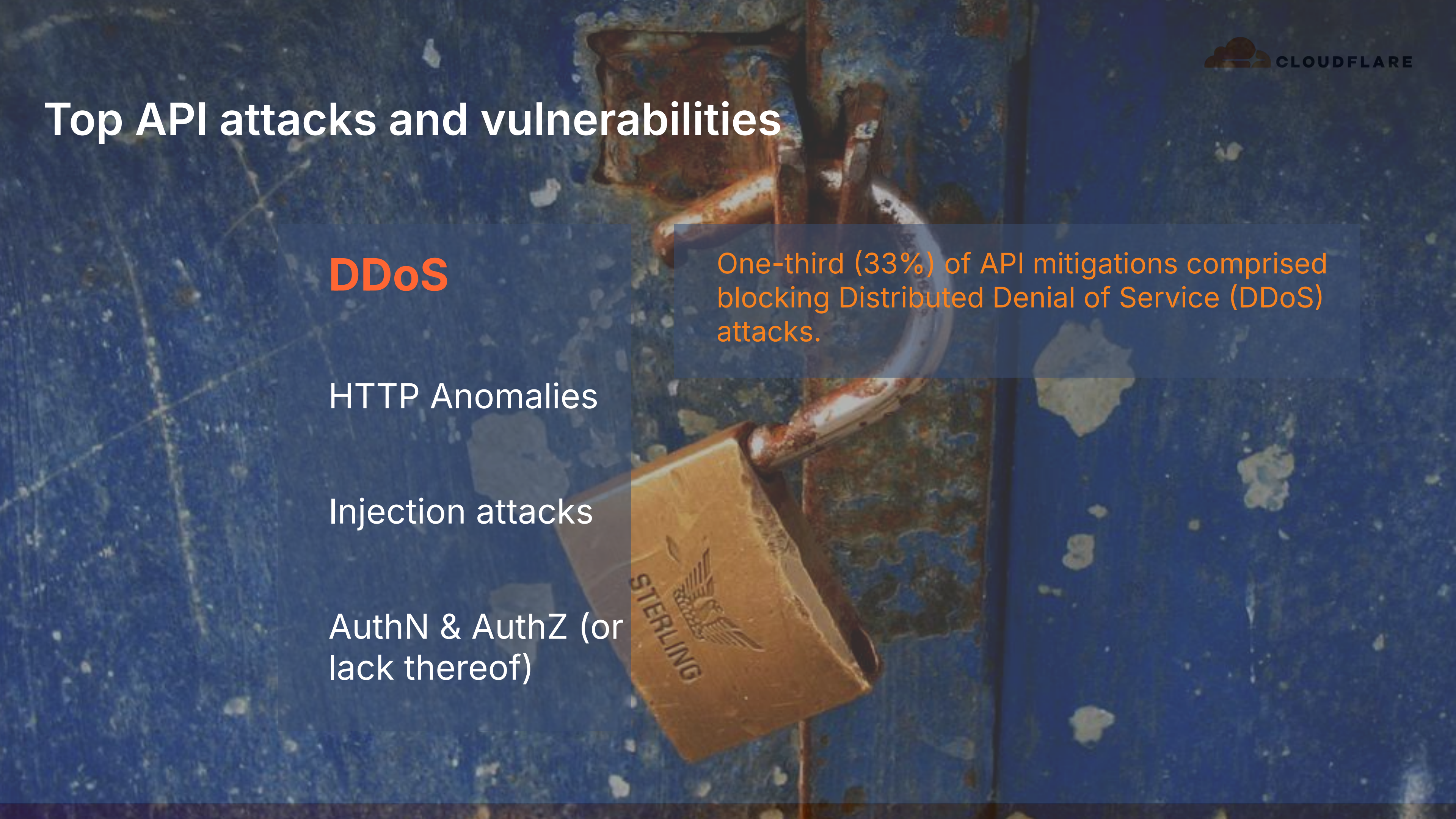
30.7%

more API endpoints found by Cloudflare than what organizations self-reported

How do you identify all your APIs?

Old school	New school
• "Email and ask" • Manual log analysis • Focus on "crown jewels" only	**AI/ML based automated discovery augments IT & Security knowledge**

Top API attacks and vulnerabilities



DDoS

HTTP Anomalies

Injection attacks

AuthN & AuthZ (or lack thereof)

One-third (33%) of API mitigations comprised blocking Distributed Denial of Service (DDoS) attacks.

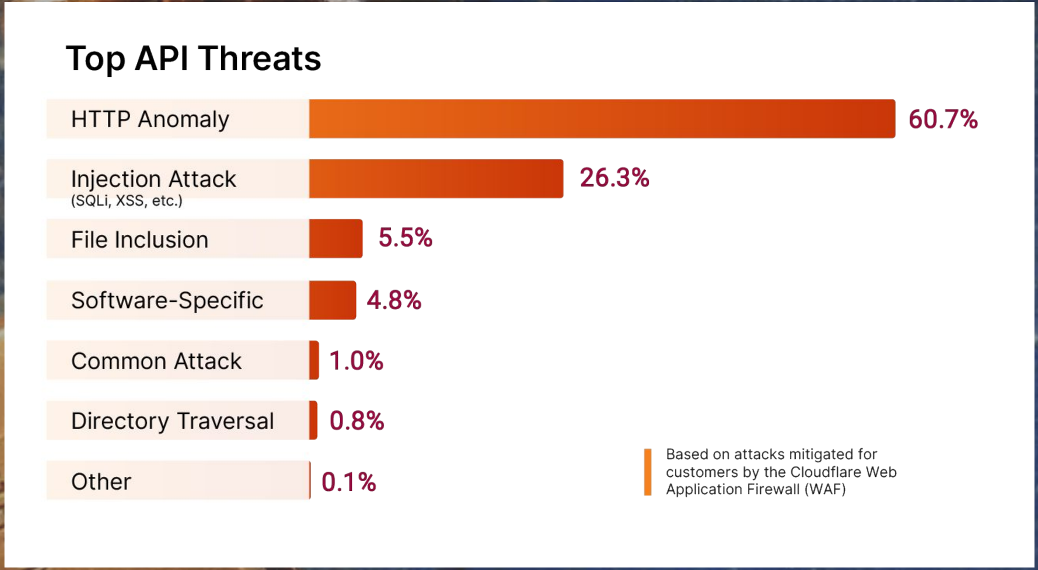
Top API attacks and vulnerabilities

DDoS

HTTP Anomalies

Injection attacks

AuthN & AuthZ (or lack thereof)



Based on attacks mitigated for customers by the Cloudflare Web Application Firewall (WAF)

CLOUDFLARE

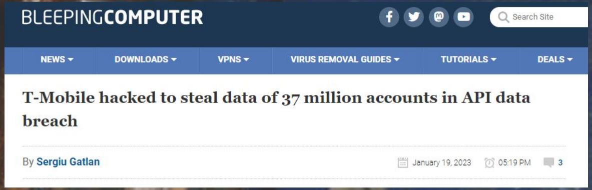
Top API attacks and vulnerabilities

DDoS

HTTP Anomalies

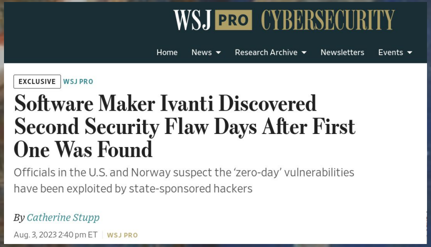
Injection attacks

AuthN & AuthZ (or lack thereof)



T-Mobile hacked to steal data of 37 million accounts in API data breach

By Sergiu Gatlan January 19, 2023 05:19 PM 3



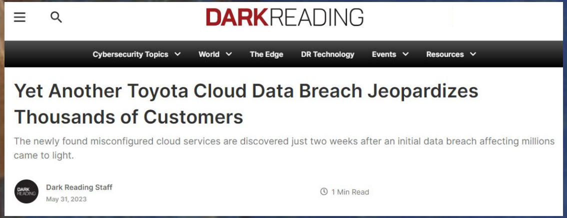
EXCLUSIVE WSJ PRO

Software Maker Ivanti Discovered Second Security Flaw Days After First One Was Found

Officials in the U.S. and Norway suspect the 'zero-day' vulnerabilities have been exploited by state-sponsored hackers

By *Catherine Stupp*

Aug. 3, 2023 2:40 pm ET | WSJ PRO



Yet Another Toyota Cloud Data Breach Jeopardizes Thousands of Customers

The newly found misconfigured cloud services are discovered just two weeks after an initial data breach affecting millions came to light.

Dark Reading Staff
May 31, 2023

1 Min Read

Key API Gateway Use Cases

Discover new APIs in use

API Discovery detects new APIs in use so companies also have a clear picture of all of their API endpoints. Sequence Analytics highlights which endpoints to focus on first.

Block malicious API requests and abuse

Move to a positive API security model with schema validation, mTLS, and JWT validation to block non-conforming clients and requests. GraphQL Query Protection and Volumetric API abuse detections see and stop abusive API traffic.

Block credential stuffing & data exfiltration

Sensitive Data Detection alerts on sensitive data exposure in API responses like PII, financial Information, credit card numbers
or secrets like API keys. Exposed credential checks detect brute force attacks with stolen credentials.

Manage and monitor APIs

Central API management registers APIs on Cloudflare and then monitors API performance monitoring. Schema Learning protects newly discovered APIs. API routing and more authentication coming soon.

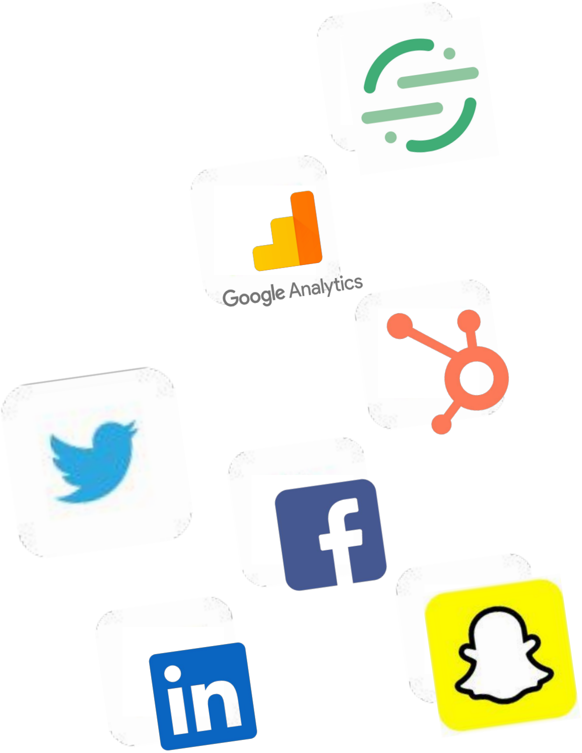
3rd Party Scripts

What are third-party scripts?

Third-party scripts are externally created JavaScript code that adds functionalities to a website.

Third-party script categories include analytics, marketing, advertising, CRM, chatbots and other widgets.

94% of websites use at least one third party.



Third-party scripts facilitate growth

New revenue streams

Unlocks new functionalities

Faster time-to-market

and many more…

Security challenges of third-party dependencies

Data from the Cloudflare Global Network shows that:

13% of enterprise applications load new scripts every **24h**

18% of enterprise applications load new scripts every **48h**

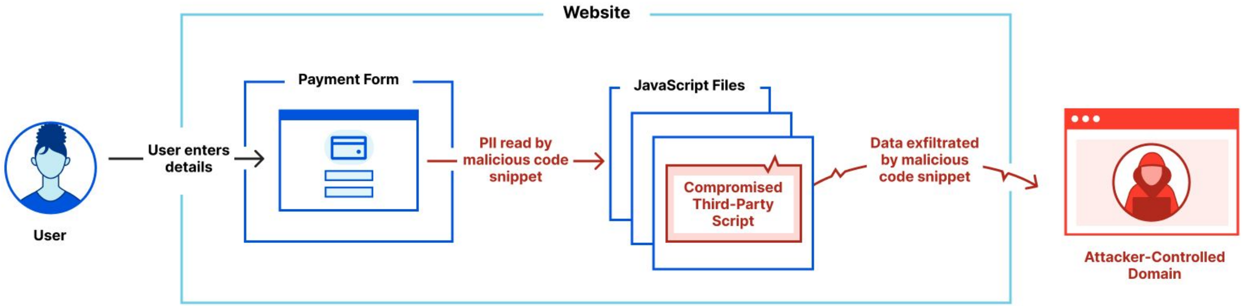
32% of enterprise applications load new scripts every **week**

50% of enterprise applications load new scripts every **2 w**

New scripts are not always added due to internal development efforts.

Uncontrolled third-party scripts lead to client-side attacks

Client-side attack is a type of software supply chain attack carried out in a web app visitor’s browser.


Website
User
User enters details
Payment Form
PII read by malicious code snippet
JavaScript Files
Compromised Third-Party Script
Data exfiltrated by malicious code snippet
Attacker-Controlled Domain

Client-side attacks in news

BRITISH AIRWAYS

macy's

ticketmaster

MISSION HEALTH

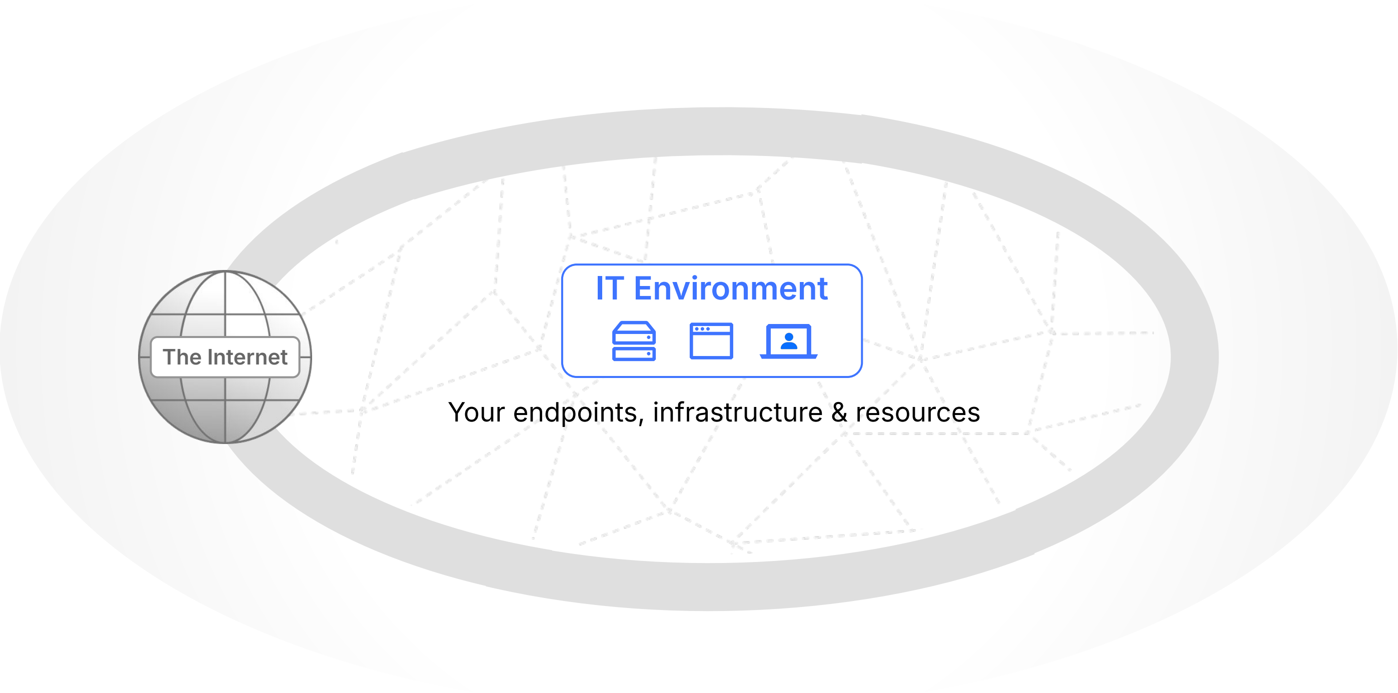
WARNER MUSIC GROUP

twilio

Datendiebstahl

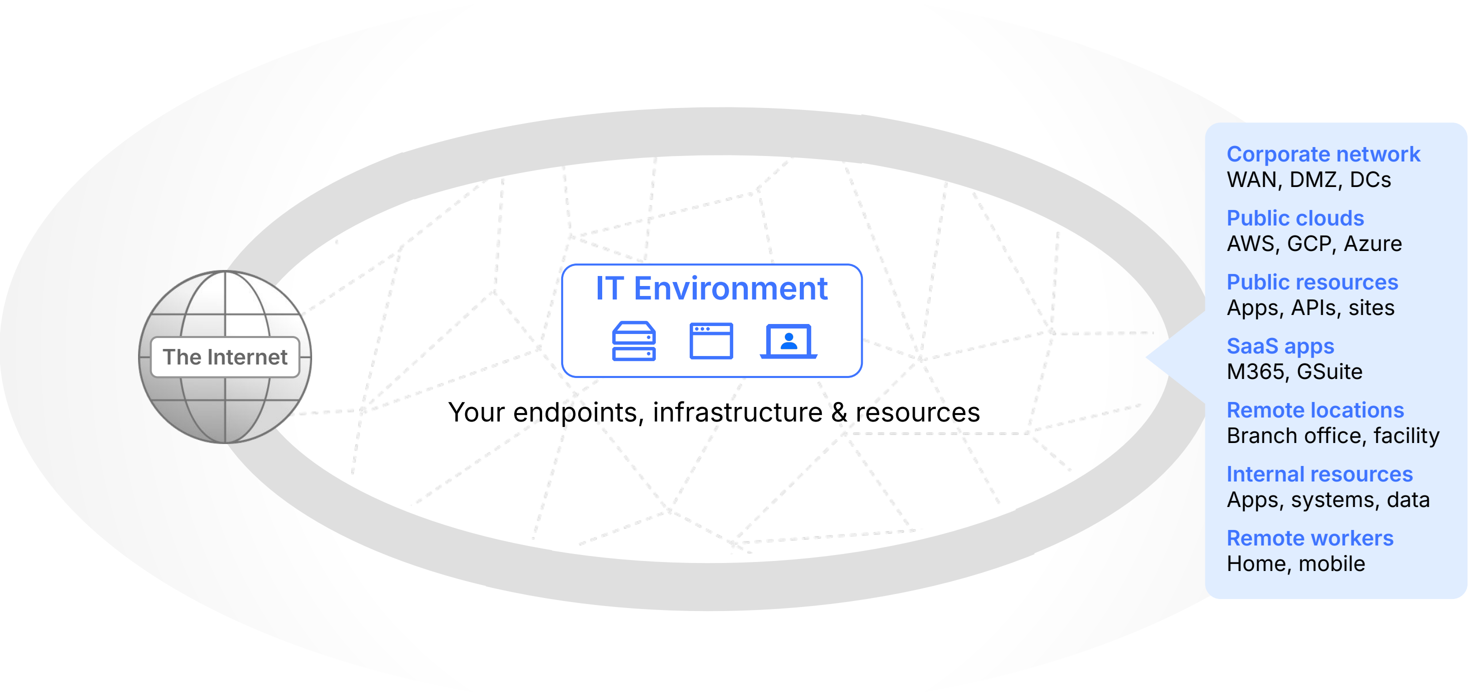
THE PROBLEM

Chaos creates opportunity for cyber attacks



THE PROBLEM

Chaos creates opportunity for cyber attacks



Corporate network
WAN, DMZ, DCs

Public clouds
AWS, GCP, Azure

Public resources
Apps, APIs, sites

SaaS apps
M365, GSuite

Remote locations
Branch office, facility

Internal resources
Apps, systems, data

Remote workers
Home, mobile

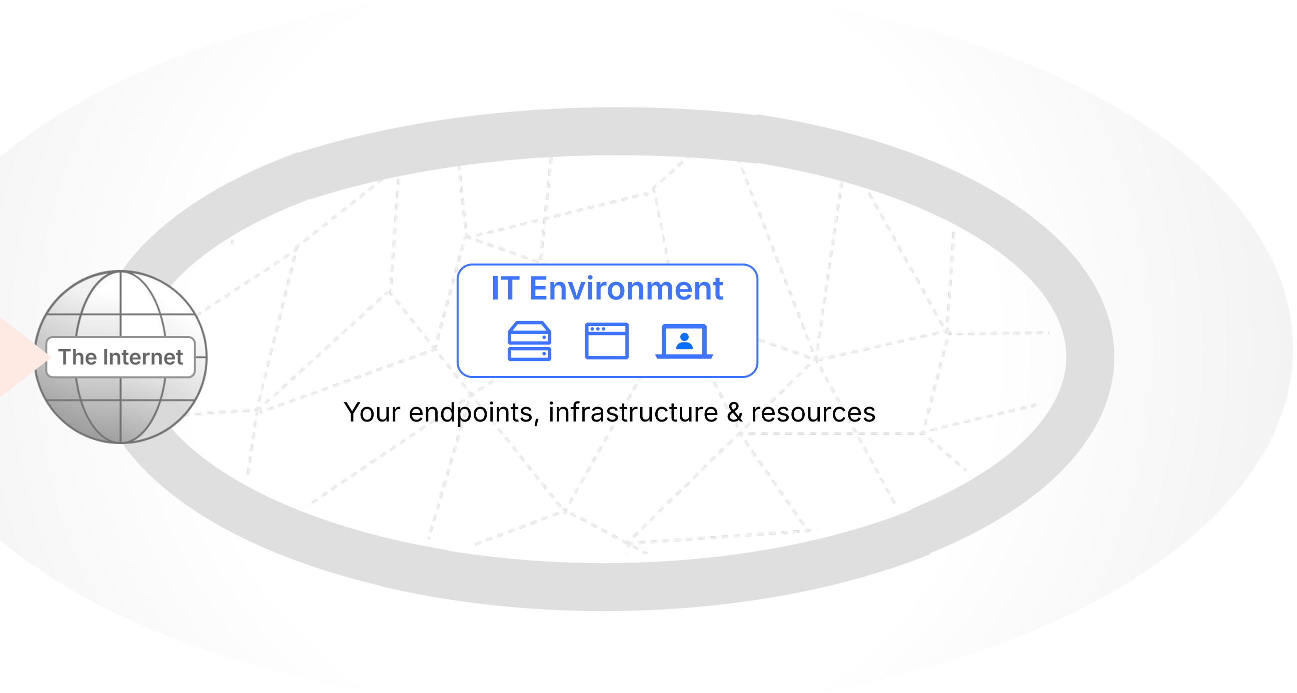
THE PROBLEM

Chaos creates opportunity for cyber attacks

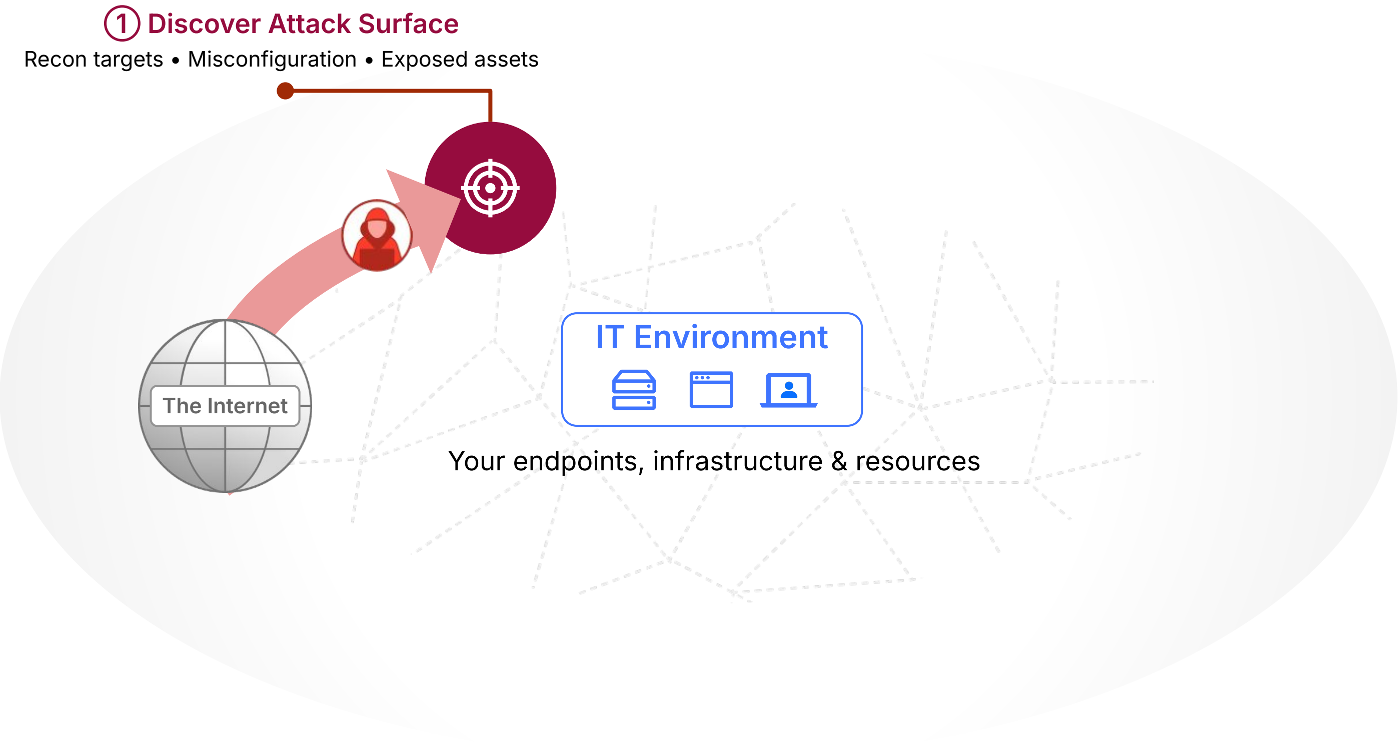
Inbound risks
API abuse
Email phish & BEC
Ransomware
DDoS & bots
0-day exploits

Browsing risks
Encrypted traffic
Drive-by malware
Phish/risky site

Outbound risks
Data loss
Data exposure
Noncompliance

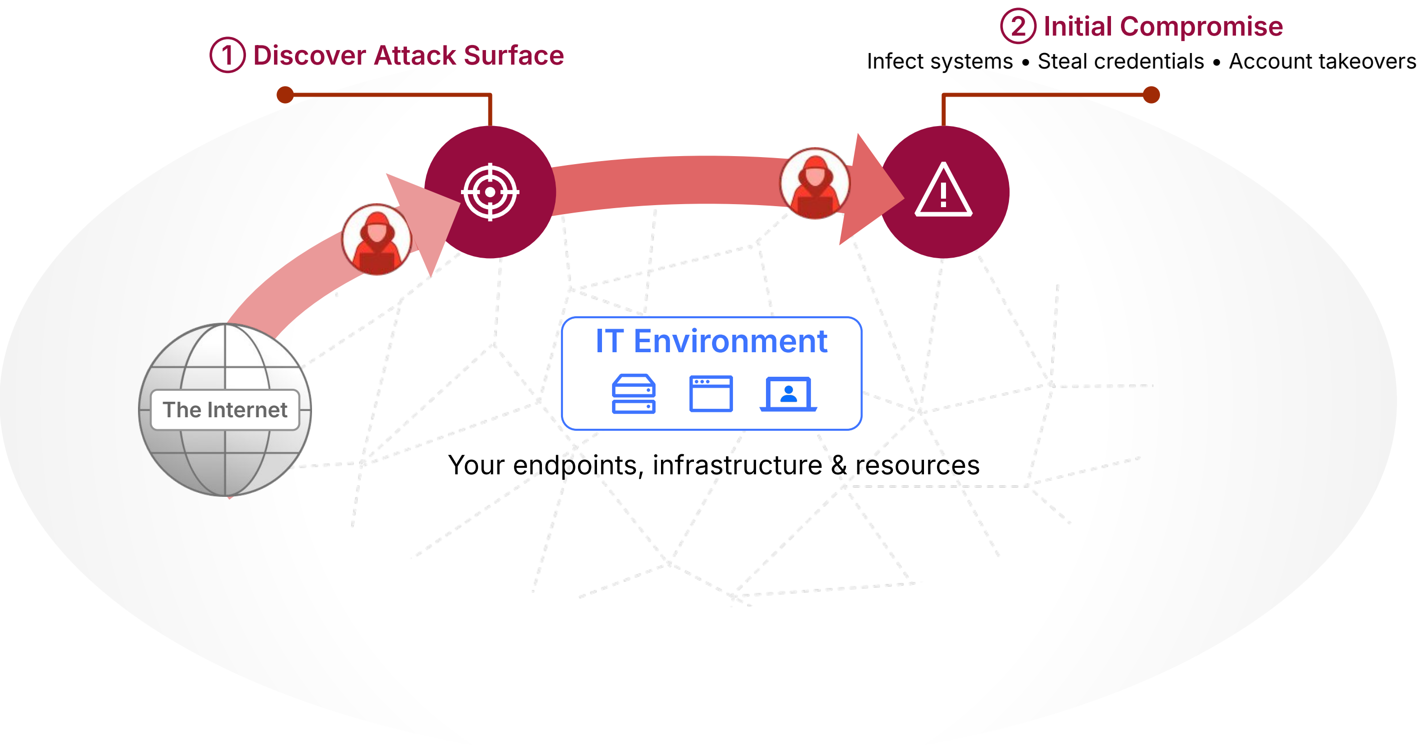


Chaos creates opportunity for cyber attacks


① Discover Attack Surface
Recon targets • Misconfiguration • Exposed assets
The Internet
IT Environment
Your endpoints, infrastructure & resources

THE PROBLEM

Chaos creates opportunity for cyber attacks



1 Discover Attack Surface

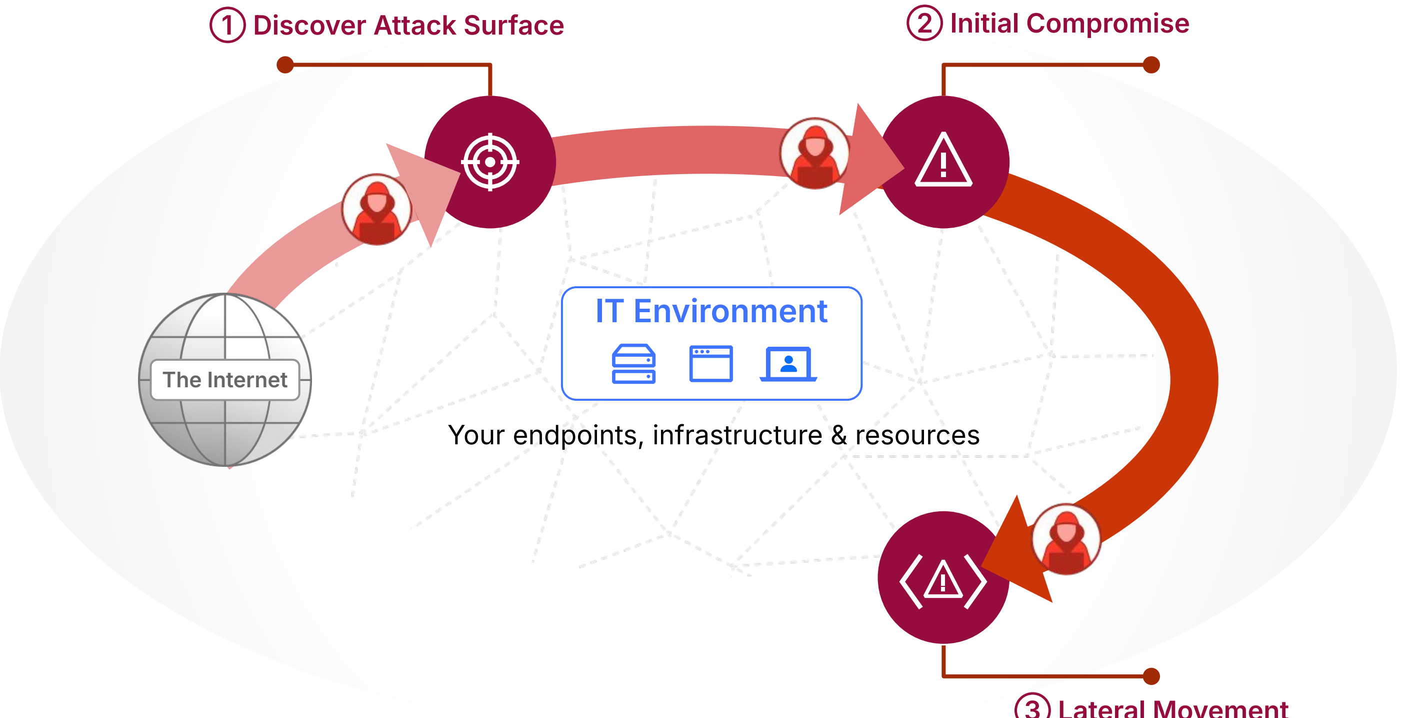
2 Initial Compromise

Infect systems • Steal credentials • Account takeovers

Your endpoints, infrastructure & resources

THE PROBLEM

Chaos creates opportunity for cyber attacks

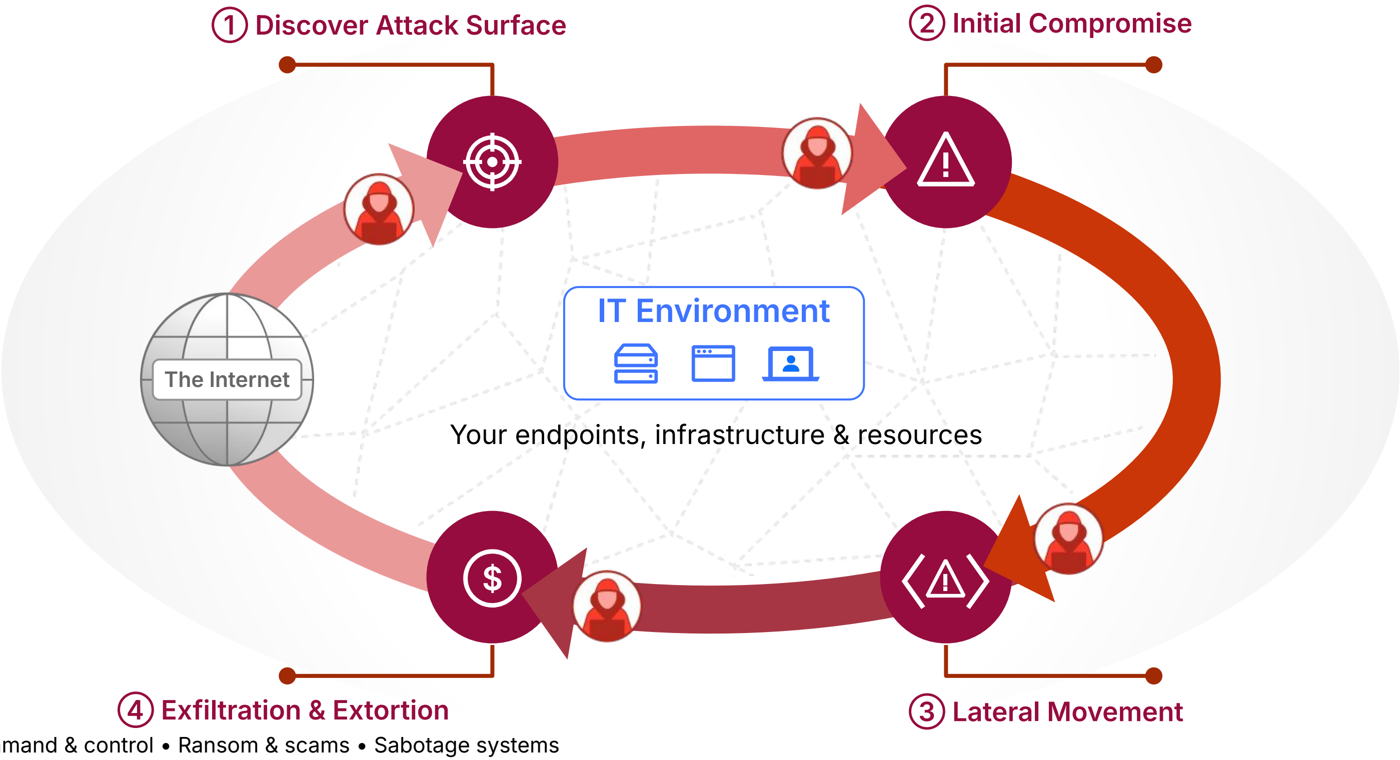


1 Discover Attack Surface
2 Initial Compromise
The Internet
IT Environment
Your endpoints, infrastructure & resources

3 Lateral Movement

Unsegmented flat network • Unrestricted system access • Privilege escalation

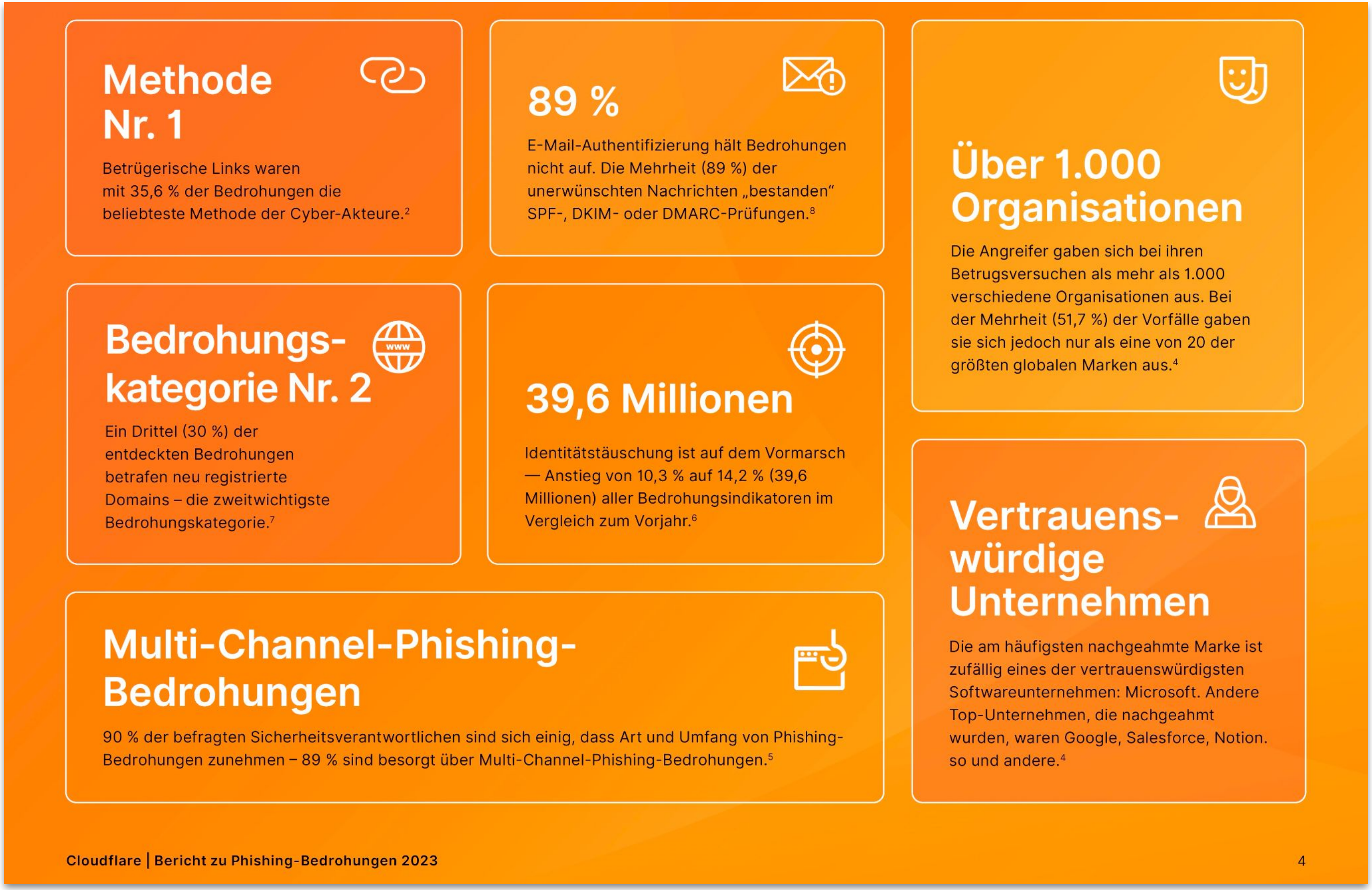
Chaos creates opportunity for cyber attacks



① Discover Attack Surface
② Initial Compromise
IT Environment
The Internet
Your endpoints, infrastructure & resources
③ Lateral Movement
④ Exfiltration & Extortion

Command & control • Ransom & scams • Sabotage systems

Cloudflare Bericht zu Phishing Bedrohungen - 1



Methode Nr. 1

Betrügerische Links waren mit 35,6 % der Bedrohungen die beliebteste Methode der Cyber-Akteure.[2]

89 %

E-Mail-Authentifizierung hält Bedrohungen nicht auf. Die Mehrheit (89 %) der unerwünschten Nachrichten „bestanden" SPF-, DKIM- oder DMARC-Prüfungen.[8]

Über 1.000 Organisationen

Die Angreifer gaben sich bei ihren Betrugsversuchen als mehr als 1.000 verschiedene Organisationen aus. Bei der Mehrheit (51,7 %) der Vorfälle gaben sie sich jedoch nur als eine von 20 der größten globalen Marken aus.[4]

Bedrohungskategorie Nr. 2

Ein Drittel (30 %) der entdeckten Bedrohungen betrafen neu registrierte Domains – die zweitwichtigste Bedrohungskategorie.[7]

39,6 Millionen

Identitätstäuschung ist auf dem Vormarsch — Anstieg von 10,3 % auf 14,2 % (39,6 Millionen) aller Bedrohungsindikatoren im Vergleich zum Vorjahr.[6]

Vertrauenswürdige Unternehmen

Die am häufigsten nachgeahmte Marke ist zufällig eines der vertrauenswürdigsten Softwareunternehmen: Microsoft. Andere Top-Unternehmen, die nachgeahmt wurden, waren Google, Salesforce, Notion. so und andere.[4]

Multi-Channel-Phishing-Bedrohungen

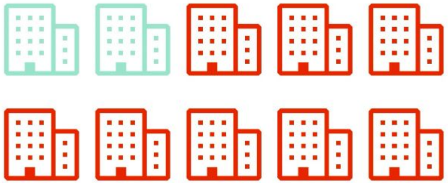
90 % der befragten Sicherheitsverantwortlichen sind sich einig, dass Art und Umfang von Phishing-Bedrohungen zunehmen – 89 % sind besorgt über Multi-Channel-Phishing-Bedrohungen.[5]

Cloudflare Bericht zu Phishing Bedrohungen - Multi-Channel-Phishing

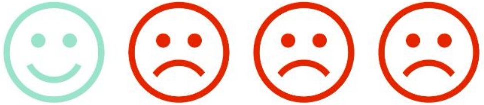
Wir verzeichnen immer mehr Angriffe, die Nutzer über mehrere Kommunikationskanäle ins Visier nehmen – in der Regel zunächst mit einem Link. **Wir bezeichnen diese Angriffsart als Multi-Channel-Phishing**. Und laut der von uns in Auftrag gegebenen Umfrage, die von Forrester Consulting durchgeführt wurde, **sind 89 % der Sicherheitsverantwortlichen besorgt über diese über mehrere Kanäle laufenden Phishing-Bedrohungen**[5]:

Ca. 8 von 10

berichteten von der Exposition ihres Unternehmens über mehrere Kanäle hinweg, wie IM/Cloud Collaboration-/Produktivitätstools, Mobile/SMS und sozialen Kanälen.



Nur 25 % der

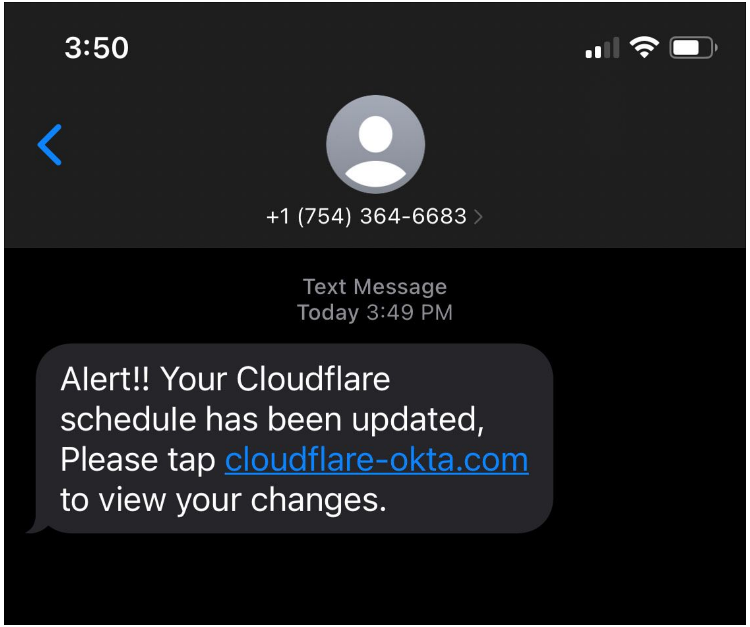


Befragten waren der Meinung, dass ihre Unternehmen vollständig auf Phishing-Bedrohungen über verschiedene Kanäle vorbereitet sind.

Definitionen von Angriffen

- **Multi-Channel-Angriff**
  Ein Phishing-Angriff, der versucht, einen Benutzer auszunutzen, indem er ihn über mehrere Anwendungen hinweg anspricht
- **Multi-Vektor-Angriff**
  Versuch, sich durch gleichzeitige Angriffe auf mehrere Zugangspunkte unbefugten Zugang zu verschaffen
- **Multi-Modus-Angriff**
  Die verschiedenen Phasen eines Angriffs, mit denen ein Angreifer auf sein finales Ziel zusteuert

Phishing Bedrohungen - Angriff auf Cloudflare

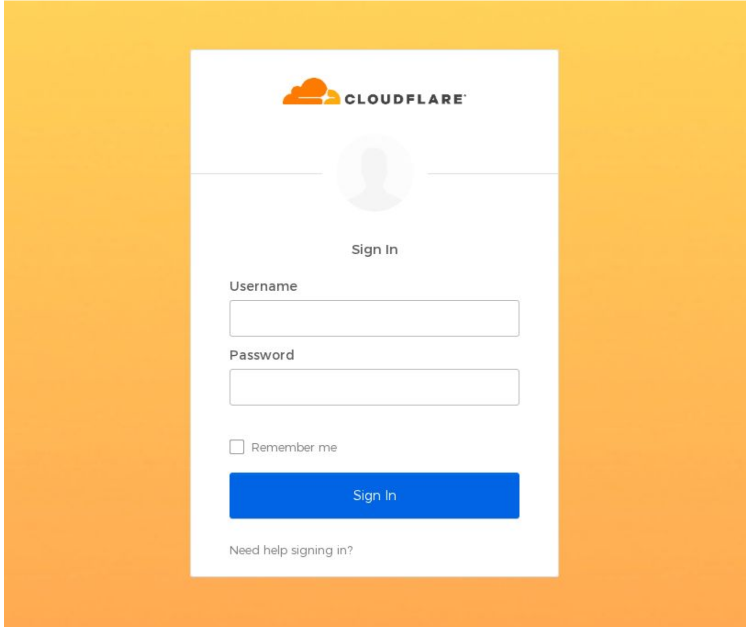


3:50

+1 (754) 364-6683

Text Message
Today 3:49 PM

Alert!! Your Cloudflare schedule has been updated, Please tap cloudflare-okta.com to view your changes.



Sign In

Username

Password

□ Remember me

Sign In

Need help signing in?

https://blog.cloudflare.com/2022-07-sms-phishing-attacks/

Wie können Sie sich schützen?

Four traffic flows for network modernization

Inbound Traffic

Protect network and apps from DDoS

On-prem products:
On-prem firewall, DMZ infrastructure, ISP filtering, VPN

Cloud-based products:
WAF, CDN, WAAP

Public Cloud Networking

Connect, secure and build apps in public cloud and hybrid cloud

Traditionally DIY or cloud-based products:
Cloud-specific functionality, multi-cloud networking startups

Outbound Traffic

Protect users & offices from threats
Protect data movement

On-prem products:
On-prem firewall, on-prem Proxy

Cloud-based products:
SASE/SSE, SWG, CASB, ZTNA

WAN Networking

Connect and secure offices, users, devices, DCs and infrastructure

On-prem/In-house:
Physical networking, virtualized networking, SD-WAN, private interconnects, MPLS carriers

Cloud-based products: SASE/SD-WAN

Zero Trust is a mindset shift

Never trust, always verify

Assume risk & reduce impact

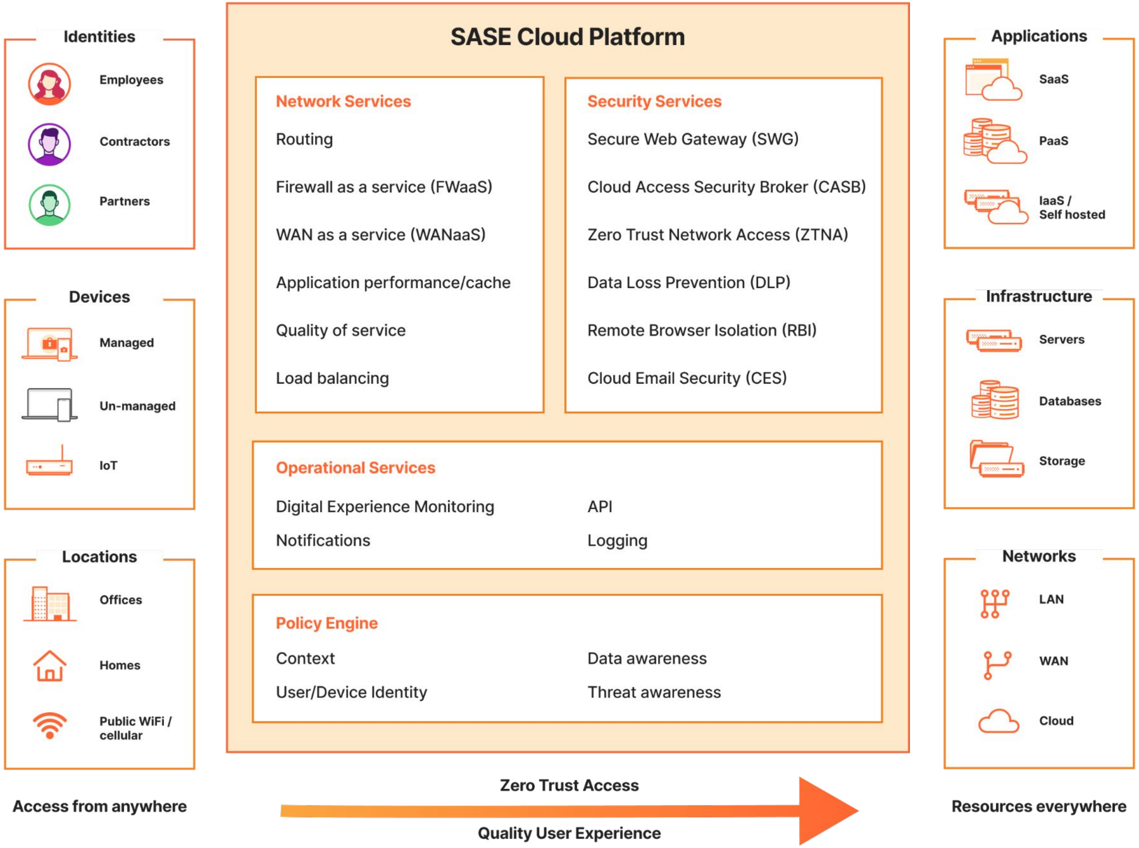
Default deny + least privilege access

Context based (identity, posture etc)

Prevent lateral movement

CLOUDFLARE'S SASE ARCHITECTURE

CLOUDFLARE



Identities

Employees

Contractors

Partners

Devices

Managed

Un-managed

IoT

Locations

Offices

Homes

Public WiFi / cellular

Access from anywhere

SASE Cloud Platform

Network Services

- Routing
- Firewall as a service (FWaaS)
- WAN as a service (WANaaS)
- Application performance/cache
- Quality of service
- Load balancing

Security Services

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)
- Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI)
- Cloud Email Security (CES)

Operational Services

Digital Experience Monitoring	API
Notifications	Logging

Policy Engine

Context	Data awareness
User/Device Identity	Threat awareness

Zero Trust Access

Quality User Experience

Applications

SaaS

PaaS

IaaS / Self hosted

Infrastructure

Servers

Databases

Storage

Networks

LAN

WAN

Cloud

Resources everywhere

One

programmable network and control plane to build new capabilities on and enforce security controls

100%

uptime SLA for paid plans that only an Anycast-enabled architecture can deliver

All

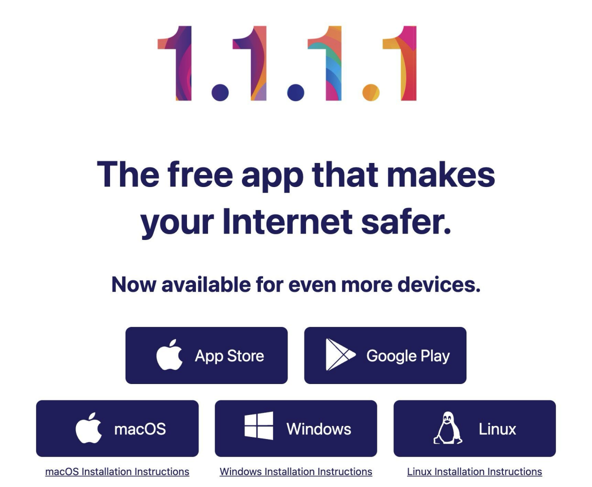
services designed to run in every Cloudflare network location, so all traffic is inspected closest to its source for consistent speed and scale everywhere.

CLOUDFLARE

Roadmap to Zero Trust architecture

	Component	Goal	Level of Effort
Phase 1	Internet traffic	Deploy global DNS filtering	▮
	Applications	Monitor inbound emails and filter out phishing attempts	▮
	DLP & logs	Identify misconfig and publicly shared data in SaaS tools	▮
Phase 2	Users	Establish corporate identity	▮▮
	Users	Enforce basic MFA for all applications	▮
	Applications	Enforce HTTPS and DNSsec	▮
	Internet traffic	Block or isolate threats behind SSL	▮▮
	Applications	ZT policy enforcement for publicly addressable apps	▮
	Applications	Protect applications from layer 7 attacks	▮
	Networks	Close all inbound ports open to the Internet for app delivery	▮
Phase 3	Applications	Inventory all corporate applications	▮▮
	Applications	ZT policy enforcement for SaaS applications	▮▮
	Networks	Segment user network access	▮▮▮
	Applications	ZTNA for critical privately addressable applications	▮
	Devices	Implement MDM/UEM to control corporate devices	▮▮
	DLP & logs	Define what data is sensitive and where it exists	▮▮
	Users	Send out hardware based authentication tokens	▮▮
	DLP & logs	Stay up to date on known threat actors	▮
Phase 4	Users	Enforce hardware token based MFA	▮▮
	Applications	ZT policy enforcement and network access for all applications	▮▮▮
	DLP & logs	Establish a SOC for log review, policy updates and mitigation	▮▮
	Devices	Implement endpoint protection	▮▮
	Devices	Inventory all corporate devices, APIs and services	▮
	Networks	Use broadband Internet for branch to branch connectivity	▮▮▮
	DLP & logs	Log and review employee activity on sensitive apps	▮▮
	DLP & logs	Stop sensitive data from leaving your applications	▮▮▮
	Steady state	DevOps approach for policy enforcement of new resources	▮▮
	Steady state	Implement auto-scaling for on-ramp resources	▮▮▮

Ein Anfang

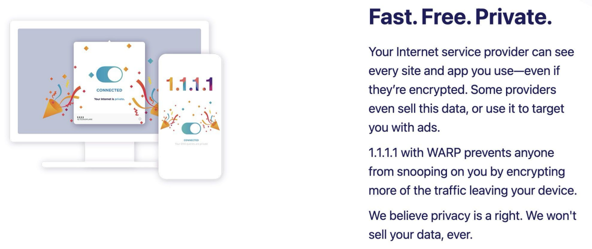


1.1.1.1

The free app that makes your Internet safer.

Now available for even more devices.

macOS Installation Instructions Windows Installation Instructions Linux Installation Instructions

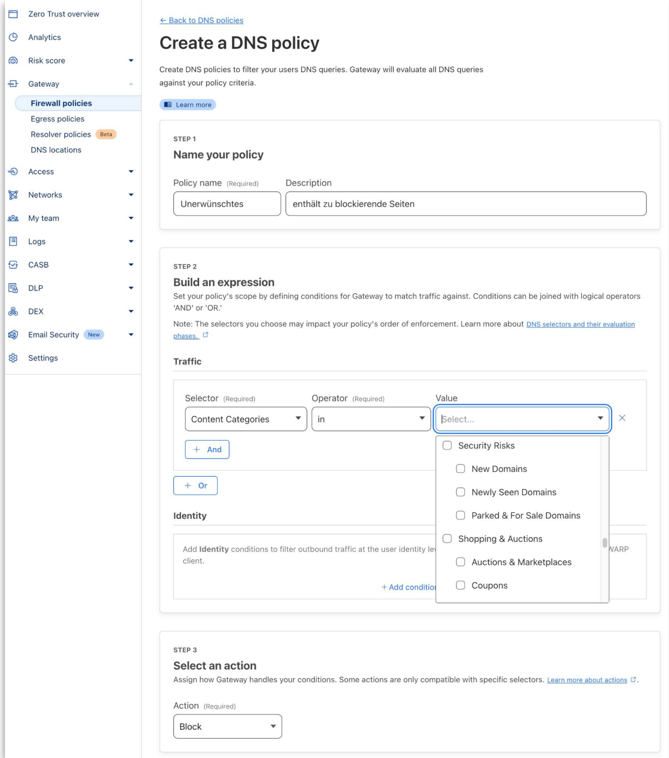


Fast. Free. Private.

Your Internet service provider can see every site and app you use—even if they're encrypted. Some providers even sell this data, or use it to target you with ads.

1.1.1.1 with WARP prevents anyone from snooping on you by encrypting more of the traffic leaving your device.

We believe privacy is a right. We won't sell your data, ever.



← Back to DNS policies

Create a DNS policy

Create DNS policies to filter your users DNS queries. Gateway will evaluate all DNS queries against your policy criteria.

STEP 1

Name your policy

Policy name (Required): Unerwünschtes

Description: enthält zu blockierende Seiten

STEP 2

Build an expression

Set your policy's scope by defining conditions for Gateway to match traffic against. Conditions can be joined with logical operators 'AND' or 'OR.'

Note: The selectors you choose may impact your policy's order of enforcement. Learn more about DNS selectors and their evaluation phases.

Traffic

Selector (Required): Content Categories

Operator (Required): in

Value: Select...

- ☐ Security Risks
  - ☐ New Domains
  - ☐ Newly Seen Domains
  - ☐ Parked & For Sale Domains
- ☐ Shopping & Auctions
  - ☐ Auctions & Marketplaces
  - ☐ Coupons

Identity

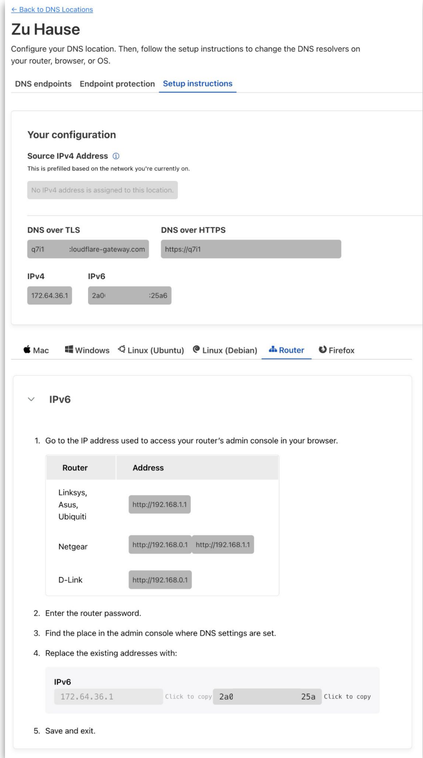
Add **Identity** conditions to filter outbound traffic at the user identity le ARP client.

STEP 3

Select an action

Assign how Gateway handles your conditions. Some actions are only compatible with specific selectors. Learn more about actions.

Action (Required): Block



← Back to DNS Locations

Zu Hause

Configure your DNS location. Then, follow the setup instructions to change the DNS resolvers on your router, browser, or OS.

Your configuration

Source IPv4 Address

This is prefilled based on the network you're currently on.

No IPv4 address is assigned to this location.

DNS over TLS: q7i1 :loudflare-gateway.com

DNS over HTTPS: https://q7i1

IPv4: 172.64.36.1

IPv6: 2a0 :25a6

IPv6

1. Go to the IP address used to access your router's admin console in your browser.

Router	Address
Linksys, Asus, Ubiquiti	http://192.168.1.1
Netgear	http://192.168.0.1 http://192.168.1.1
D-Link	http://192.168.0.1

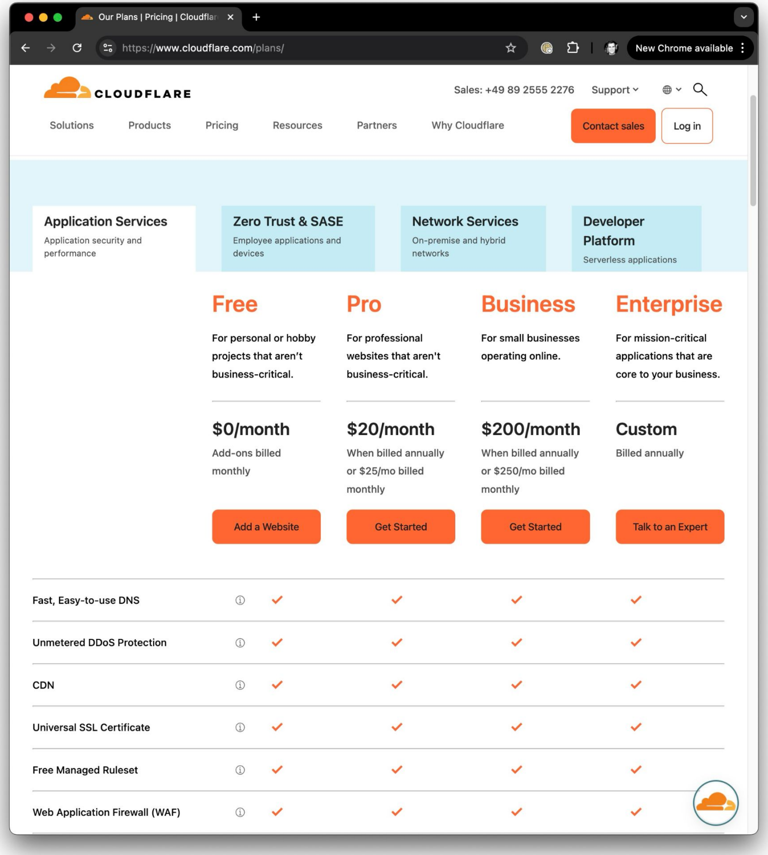
2. Enter the router password.
3. Find the place in the admin console where DNS settings are set.
4. Replace the existing addresses with:

   IPv6

   172.64.36.1 Click to copy 2a0 25a Click to copy

5. Save and exit.

Ein Anfang



Our Plans | Pricing | Cloudflar
https://www.cloudflare.com/plans/
New Chrome available

CLOUDFLARE

Sales: +49 89 2555 2276 Support

Solutions Products Pricing Resources Partners Why Cloudflare

Contact sales Log in

Application Services
Application security and performance

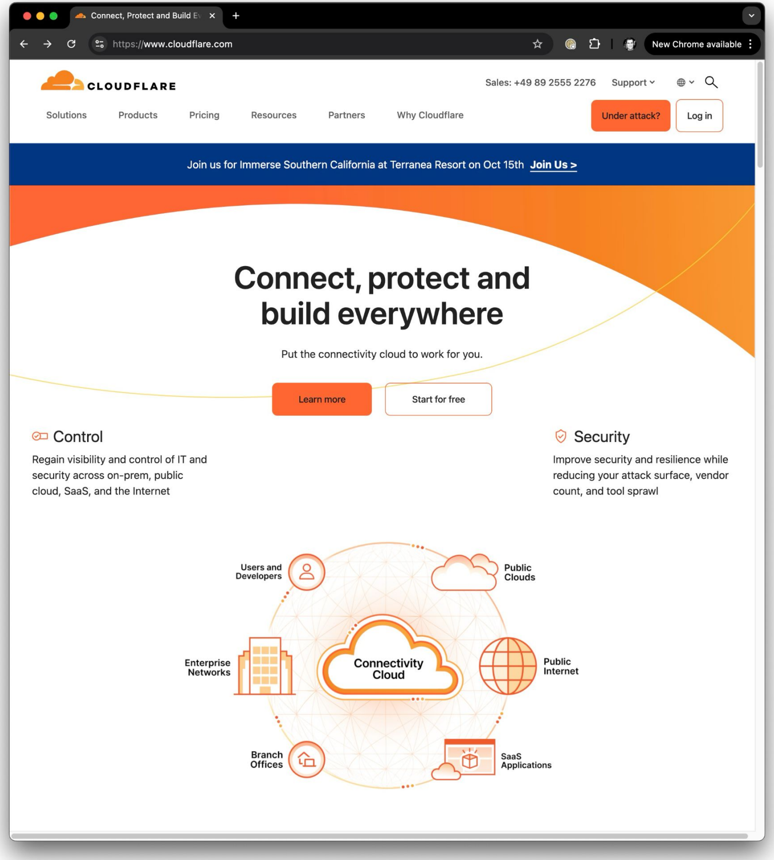
Zero Trust & SASE
Employee applications and devices

Network Services
On-premise and hybrid networks

Developer Platform
Serverless applications

Free	Pro	Business	Enterprise
For personal or hobby projects that aren't business-critical.	For professional websites that aren't business-critical.	For small businesses operating online.	For mission-critical applications that are core to your business.
$0/month	$20/month	$200/month	Custom
Add-ons billed monthly	When billed annually or $25/mo billed monthly	When billed annually or $250/mo billed monthly	Billed annually
Add a Website	Get Started	Get Started	Talk to an Expert

	Free	Pro	Business	Enterprise
Fast, Easy-to-use DNS	✓	✓	✓	✓
Unmetered DDoS Protection	✓	✓	✓	✓
CDN	✓	✓	✓	✓
Universal SSL Certificate	✓	✓	✓	✓
Free Managed Ruleset	✓	✓	✓	✓
Web Application Firewall (WAF)	✓	✓	✓	✓



CLOUDFLARE

Sales: +49 89 2555 2276 Support

Solutions Products Pricing Resources Partners Why Cloudflare

Under attack? Log in

Join us for Immerse Southern California at Terranea Resort on Oct 15th **Join Us >**

Connect, protect and build everywhere

Put the connectivity cloud to work for you.

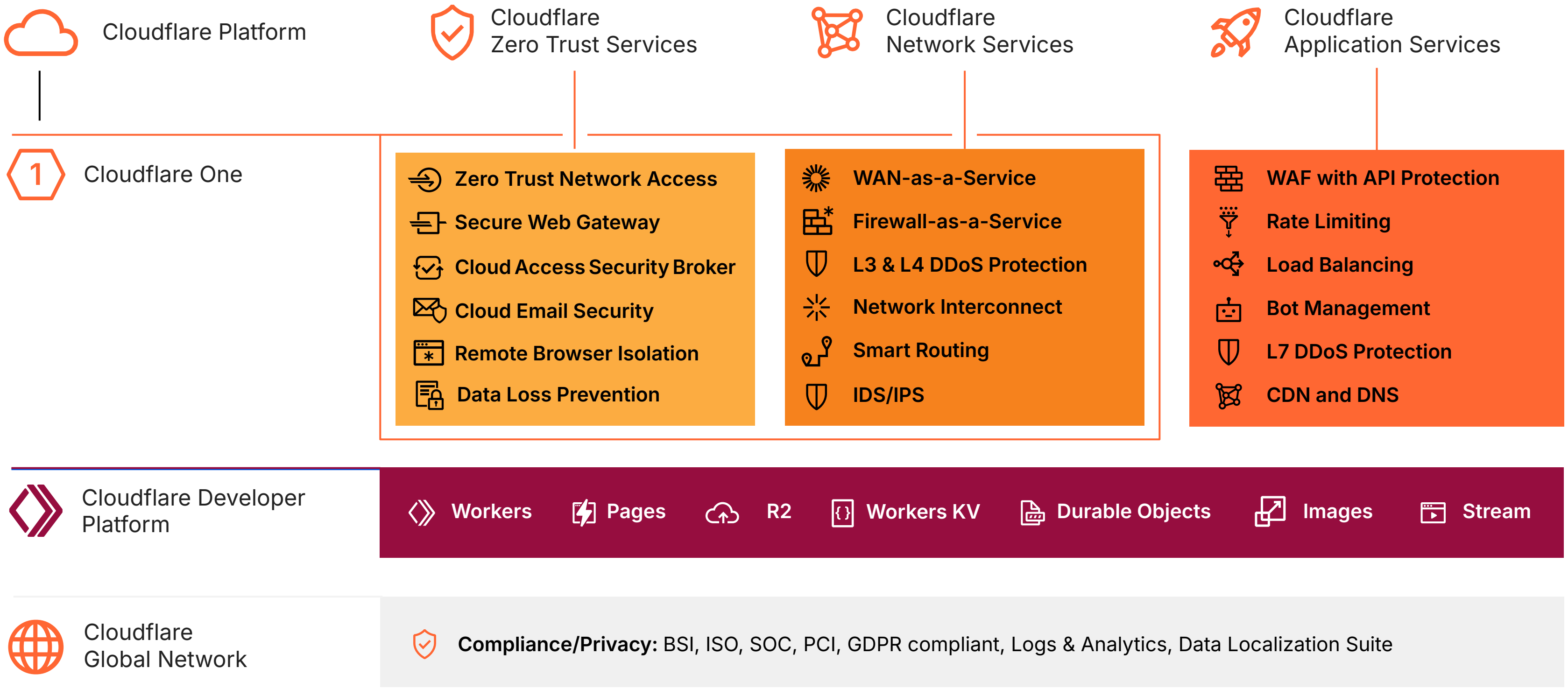
Learn more Start for free

Control
Regain visibility and control of IT and security across on-prem, public cloud, SaaS, and the Internet

Security
Improve security and resilience while reducing your attack surface, vendor count, and tool sprawl

WHAT WE OFFER

Integrated Global Cloud Platform



Cloudflare Platform

Cloudflare Zero Trust Services

Cloudflare Network Services

Cloudflare Application Services

Cloudflare One

- Zero Trust Network Access
- Secure Web Gateway
- Cloud Access Security Broker
- Cloud Email Security
- Remote Browser Isolation
- Data Loss Prevention

- WAN-as-a-Service
- Firewall-as-a-Service
- L3 & L4 DDoS Protection
- Network Interconnect
- Smart Routing
- IDS/IPS

- WAF with API Protection
- Rate Limiting
- Load Balancing
- Bot Management
- L7 DDoS Protection
- CDN and DNS

Cloudflare Developer Platform

Workers · Pages · R2 · Workers KV · Durable Objects · Images · Stream

Cloudflare Global Network

Compliance/Privacy: BSI, ISO, SOC, PCI, GDPR compliant, Logs & Analytics, Data Localization Suite

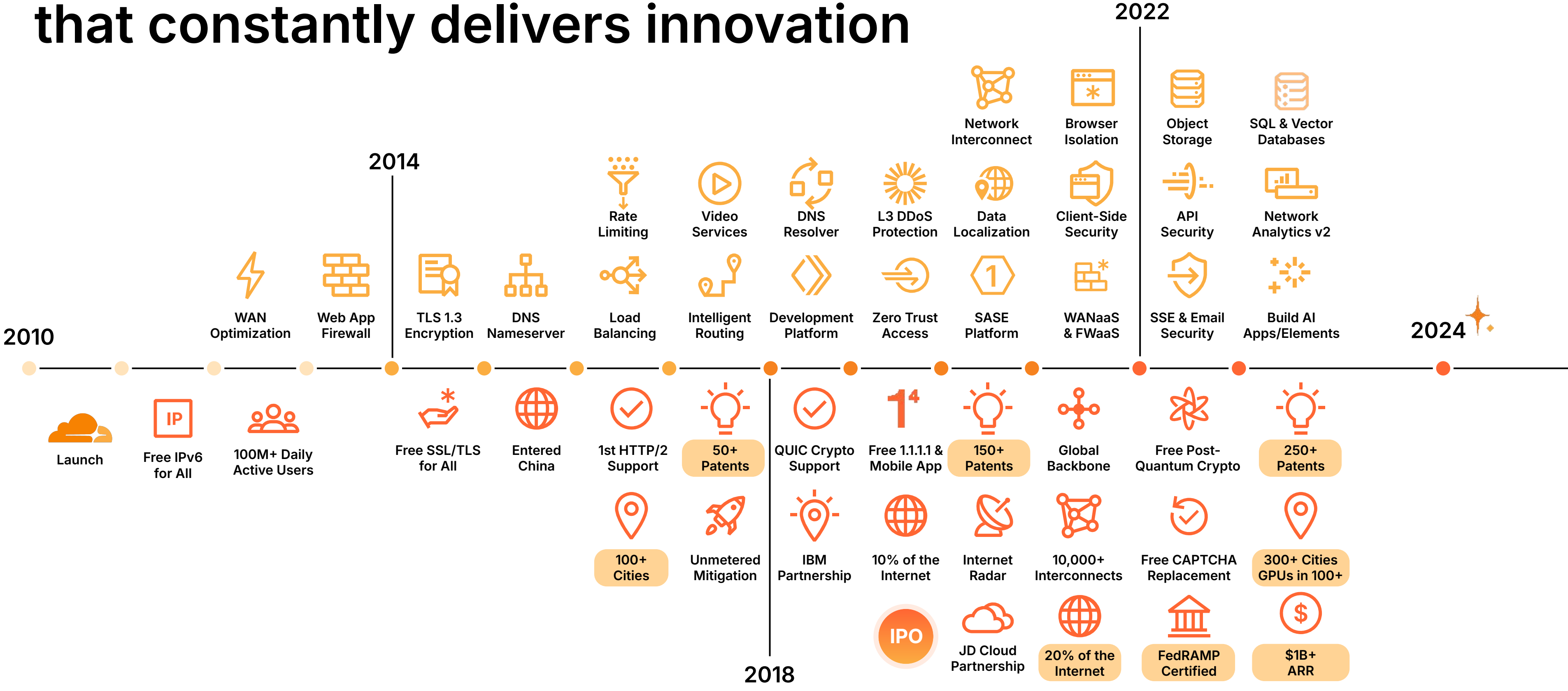
CLOUDFLARE

Let us build a better Internet together

Einblick zu Innovation

BUILDING FOR TOMORROW, TODAY

Move faster with a platform that constantly delivers innovation



2010

Launch

Free IPv6 for All

WAN Optimization

100M+ Daily Active Users

Web App Firewall

2014

TLS 1.3 Encryption

Free SSL/TLS for All

DNS Nameserver

Entered China

Rate Limiting

Load Balancing

1st HTTP/2 Support

100+ Cities

Video Services

Intelligent Routing

50+ Patents

Unmetered Mitigation

2018

DNS Resolver

Development Platform

QUIC Crypto Support

IBM Partnership

L3 DDoS Protection

Zero Trust Access

Free 1.1.1.1 & Mobile App

10% of the Internet

IPO

Network Interconnect

Data Localization

SASE Platform

150+ Patents

Internet Radar

JD Cloud Partnership

Browser Isolation

Client-Side Security

WANaaS & FWaaS

Global Backbone

10,000+ Interconnects

20% of the Internet

2022

Object Storage

API Security

SSE & Email Security

Free Post-Quantum Crypto

Free CAPTCHA Replacement

FedRAMP Certified

SQL & Vector Databases

Network Analytics v2

Build AI Apps/Elements

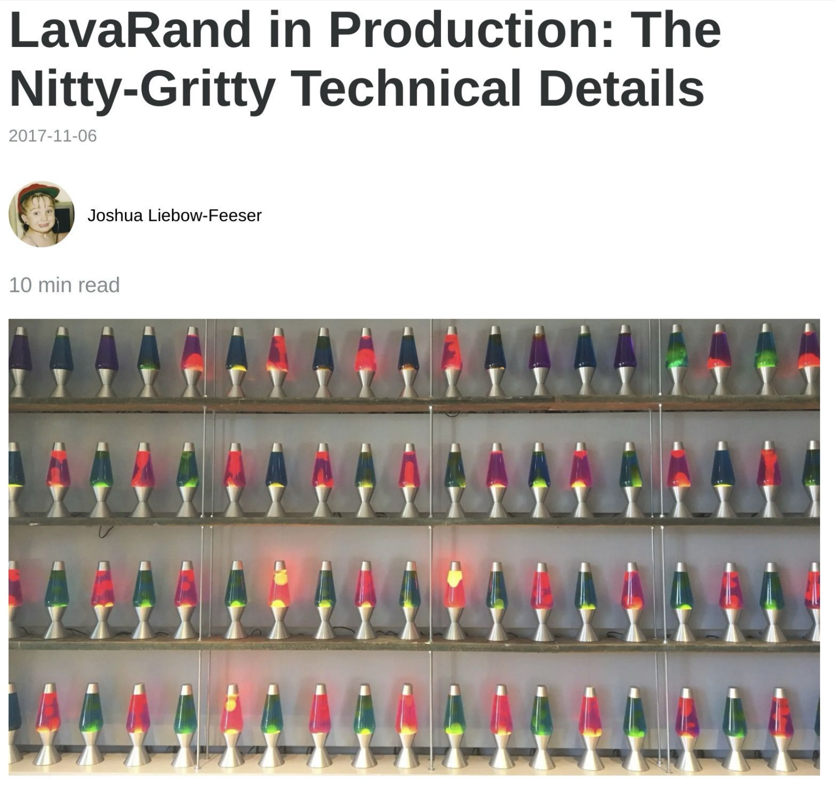
250+ Patents

300+ Cities GPUs in 100+

$1B+ ARR

2024

Randomness at Cloudflare

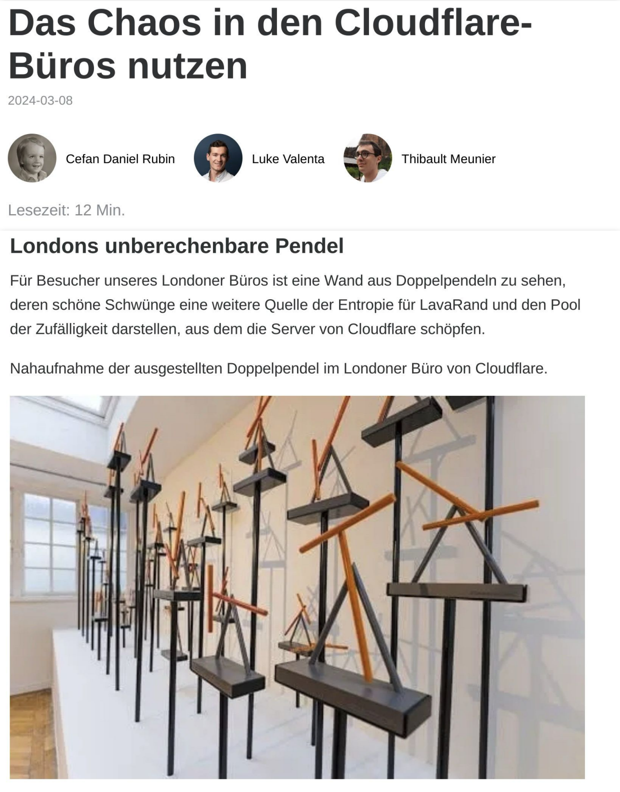


LavaRand in Production: The Nitty-Gritty Technical Details

2017-11-06

Joshua Liebow-Feeser

10 min read



Das Chaos in den Cloudflare-Büros nutzen

2024-03-08

Cefan Daniel Rubin Luke Valenta Thibault Meunier

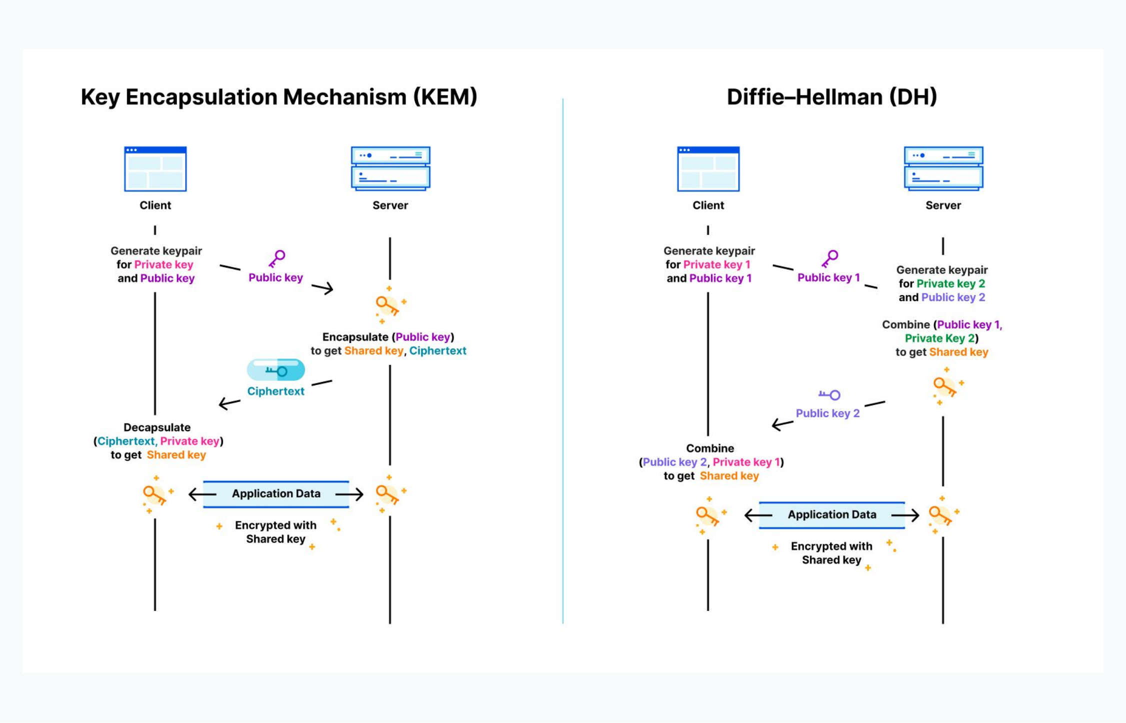
Lesezeit: 12 Min.

Londons unberechenbare Pendel

Für Besucher unseres Londoner Büros ist eine Wand aus Doppelpendeln zu sehen, deren schöne Schwünge eine weitere Quelle der Entropie für LavaRand und den Pool der Zufälligkeit darstellen, aus dem die Server von Cloudflare schöpfen.

Nahaufnahme der ausgestellten Doppelpendel im Londoner Büro von Cloudflare.

Cloudflare Research



Key Encapsulation Mechanism (KEM)

Client

Server

Generate keypair for Private key and Public key

Public key

Encapsulate (Public key) to get Shared key, Ciphertext

Ciphertext

Decapsulate (Ciphertext, Private key) to get Shared key

Application Data

Encrypted with Shared key

Diffie–Hellman (DH)

Client

Server

Generate keypair for Private key 1 and Public key 1

Public key 1

Generate keypair for Private key 2 and Public key 2

Combine (Public key 1, Private Key 2) to get Shared key

Public key 2

Combine (Public key 2, Private key 1) to get Shared key

Application Data

Encrypted with Shared key

No, AI did not break post-quantum cryptography

Kyber is a post-quantum (PQ) key encapsulation method (KEM). After a six-year worldwide competition, the National Institute of Standards and Technology (NIST) selected Kyber as the post-quantum key agreement they will standardize. The goal of a key agreement is for two parties that haven't talked to each other before to agree securely on a shared key they can use for symmetric encryption (such as Chacha20Poly1305).

As a KEM, it works slightly different with different terminology than a traditional Diffie–Hellman key agreement (such as X25519).

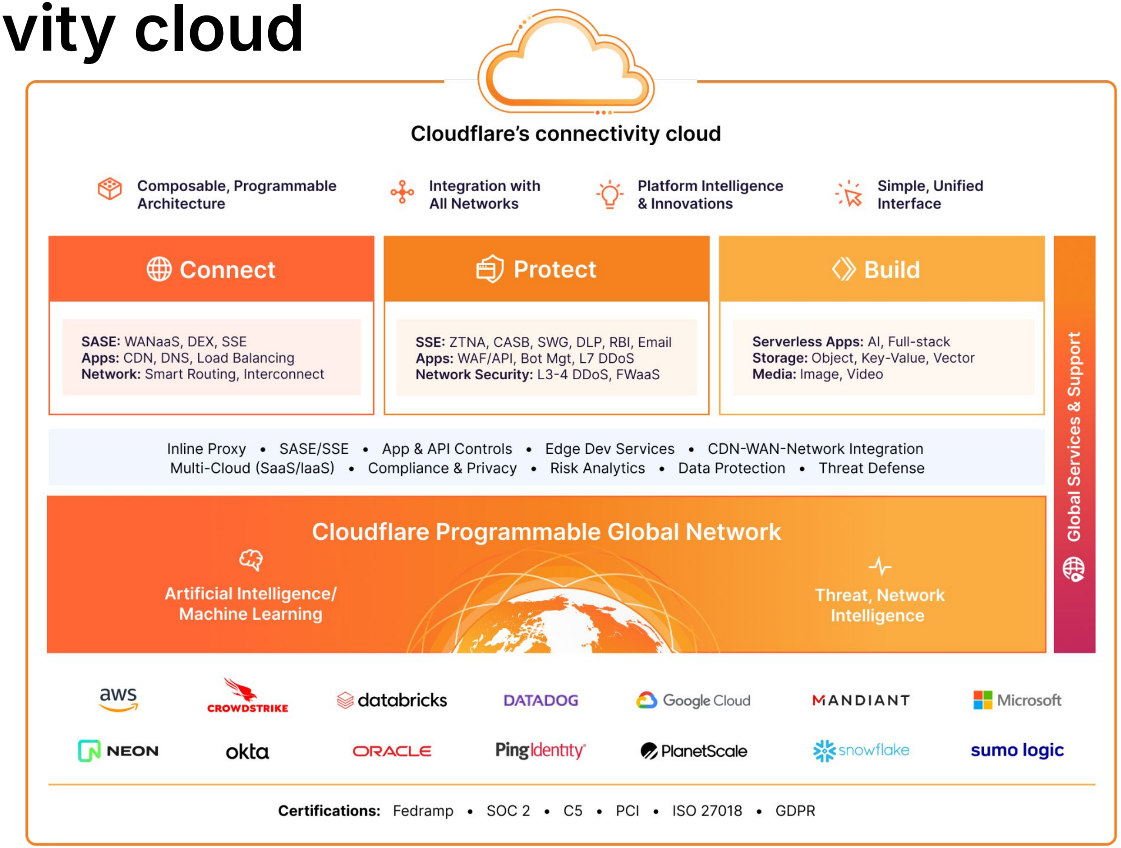
CLOUDFLARE

Let us build a better Internet together

Cloudflare's connectivity cloud

With Cloudflare organizations can:

- **Connect** users, networks, apps and clouds globally
- **Protect** data, apps, infrastructure, and users everywhere
- **Build** innovative digital services and experiences anywhere



Cloudflare's connectivity cloud

Composable, Programmable Architecture · Integration with All Networks · Platform Intelligence & Innovations · Simple, Unified Interface

Connect

SASE: WANaaS, DEX, SSE
Apps: CDN, DNS, Load Balancing
Network: Smart Routing, Interconnect

Protect

SSE: ZTNA, CASB, SWG, DLP, RBI, Email
Apps: WAF/API, Bot Mgt, L7 DDoS
Network Security: L3-4 DDoS, FWaaS

Build

Serverless Apps: AI, Full-stack
Storage: Object, Key-Value, Vector
Media: Image, Video

Inline Proxy • SASE/SSE • App & API Controls • Edge Dev Services • CDN-WAN-Network Integration
Multi-Cloud (SaaS/IaaS) • Compliance & Privacy • Risk Analytics • Data Protection • Threat Defense

Cloudflare Programmable Global Network

Artificial Intelligence/ Machine Learning

Threat, Network Intelligence

Global Services & Support

aws · CROWDSTRIKE · databricks · DATADOG · Google Cloud · MANDIANT · Microsoft
NEON · okta · ORACLE · PingIdentity · PlanetScale · snowflake · sumo logic

Certifications: Fedramp • SOC 2 • C5 • PCI • ISO 27018 • GDPR