OUR MISSION

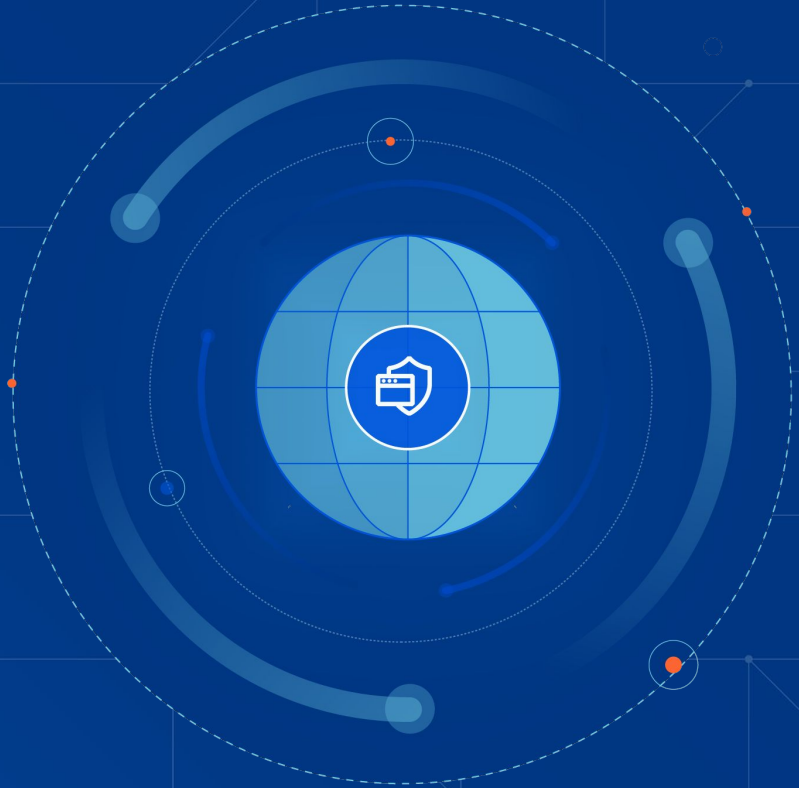
We are helping build a better Internet.

CLOUDFLARE

CLOUDFLARE

Bereid je samen met Cloudflare voor op de nieuwe Europese Cybersecurity Richtlijnen

Cloud Expo – 7 en 8 December 2022



WIE ZIJN WIJ?

Han Pieterse
Cyber Security Consultant

Michiel Appelman
Sr. Solutions Engineer – Cloudflare
michiel.cloud/flare

CLOUDFLARE

Europese Cybersecurity Richtlijnen (NIS2)

Wet beveiliging netwerk- en informatiesystemen (Wbni)

- Risico’s beperken door bescherming en detectie (minimaal de basis op orde)
- Security risico’s in kaart brengen
- De gevolgen van cyberincidenten beperken

Vernieuwing

- Digitale weerbaarheid vergroten en de gevolgen van cyberincidenten verkleinen (o.a. meldplicht cyber incidenten)
- Pro-actief passende technische en organisatorische maatregelen voor informatiebeveiliging nemen
- De veiligheid van toeleveringsketens verbeteren door cyber veilig-heidsrisico's in toeleveringsketens en leveranciersrelaties te beheersen

Vernieuwing Wet beveiliging netwerk- en informatiesystemen (Wbni)

- Entiteiten worden ingedeeld in ‘Essentieel’ en ‘Belangrijk’
- Expliciete governance vereisten
- Expliciete aansprakelijkheid voor bestuurders
- Rapportageverplichtingen
- Hogere administratieve boetes
- Basis op orde
- Leveranciers en partners medeverantwoordelijk in ‘Essentiële’ en ‘Belangrijke’ ketens

CLOUDFLARE

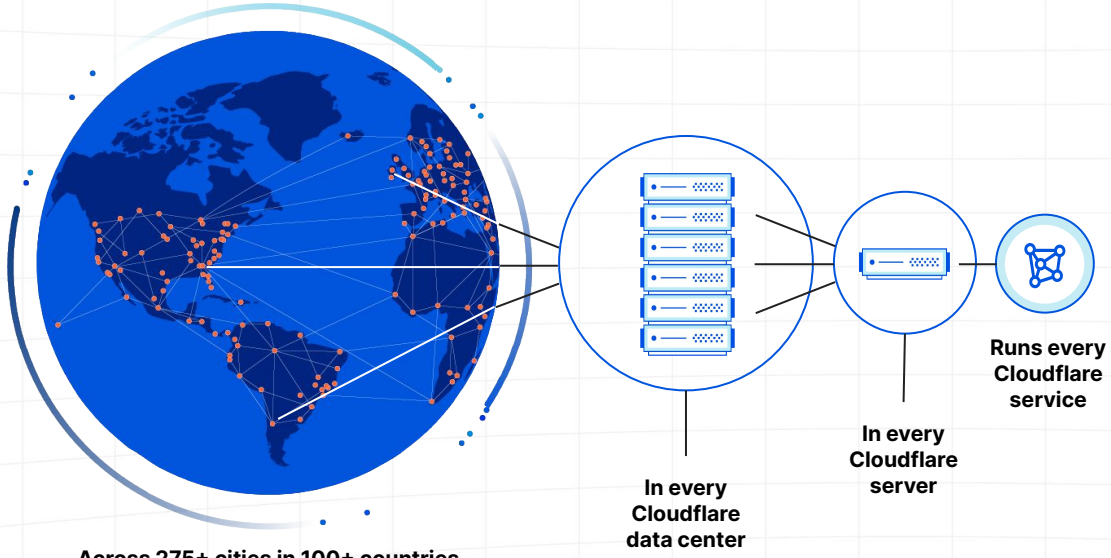
Hoe krijgen we de basis proactief op orde?

- Patchen van software en bewaak applicaties op vulnerabilities
- Applicatie toegang op basis van identiteit
- Multi-factor authenticatie en/of Zero Trust architectuur
- Veilige communicatie binnen de keten
- Inzicht, rapportage en response

Cloudflare Application Security

CLOUDFLARE

Make the Internet secure, fast, and reliable
for your business

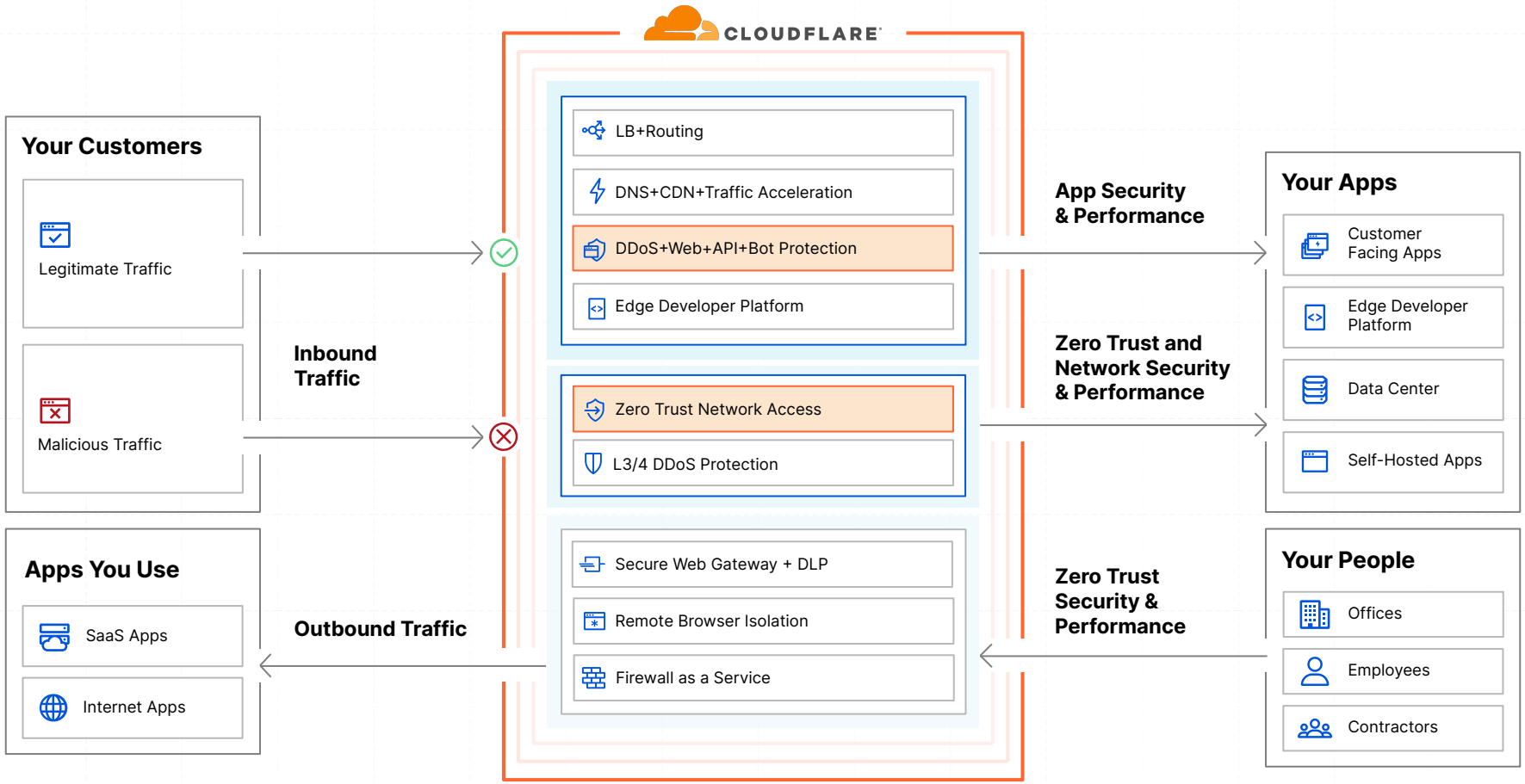


172 Tbps
of network capacity
with 11,000+ interconnects and
millions of internet properties

~50ms
from 95% of
Internet users

100%
uptime SLA

Single-pass Inspection for Ingress & Egress

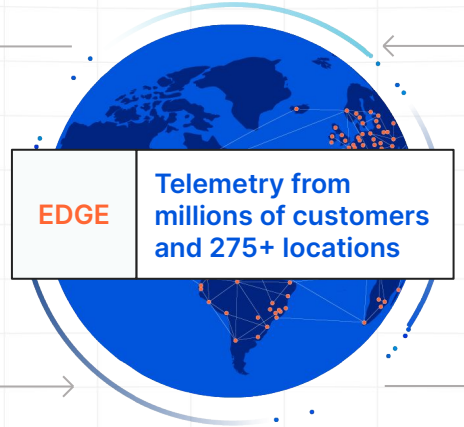


Comprehensive coverage
against Internet-borne threats

CORE Intelligence based on our machine learning

Threat hunting using our network data

- 1T+ DNS requests resolved per day with no sampling
- Millions of Internet properties
- 11,000+ network interconnects



CORE Intelligence based on our ecosystem

Threat aggregation across our partners

- Premium third-party feeds
- OSINT and shared feeds
- Community-provided feedback

Security risk categories to block, isolate or logpush to SIEM per policy rule

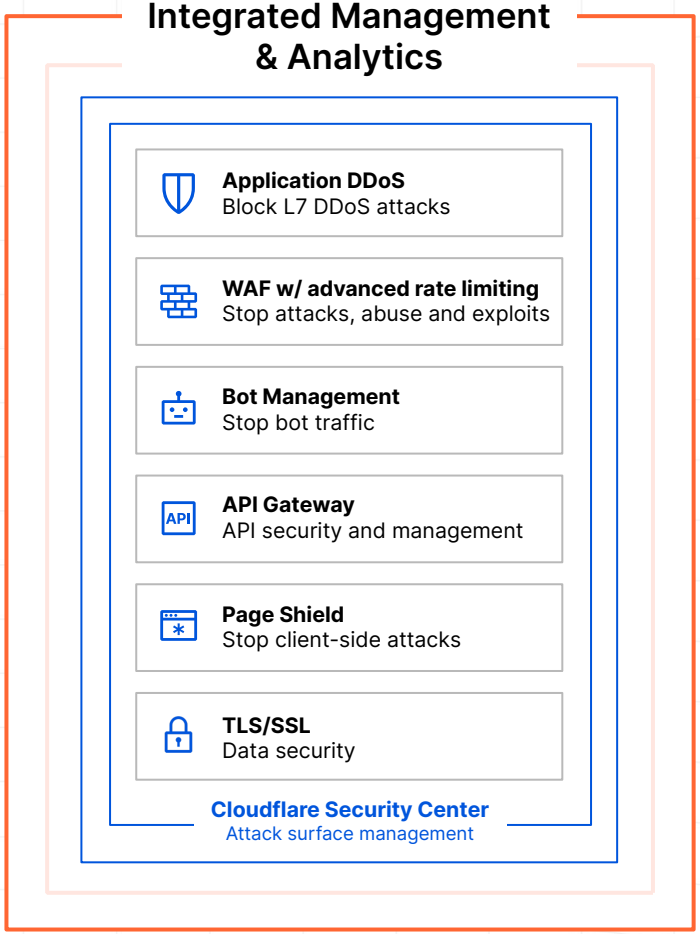
Malware	Newly seen domains	DGA domains	Spyware
Phishing	New domains	DNS tunneling	Spam
Cryptomining	Unreachable domains	C2 & botnet	Anonymizer

Cloudflare Application Security

WAF: Protecting faster before patching

Protecting a full business day faster than leading competitor

Log4J put the world on alert as a "critical" vulnerability. Cloudflare deployed 4 new rules, fully tested, within hours of public disclosure. Our leading WAF competitors left they customers exposed for an additional **NINE** hours.

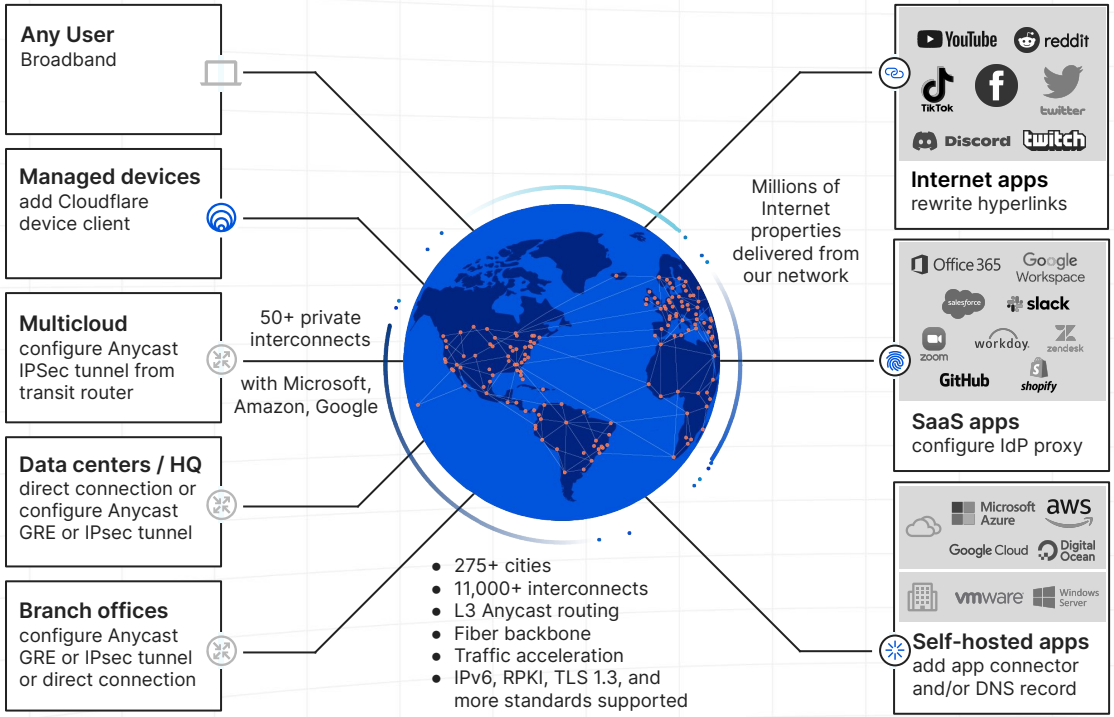


CLOUDFLARE

Cloudflare Zero Trust

CLOUDFLARE

Simple deployments, flexible architecture



Composable on-ramps

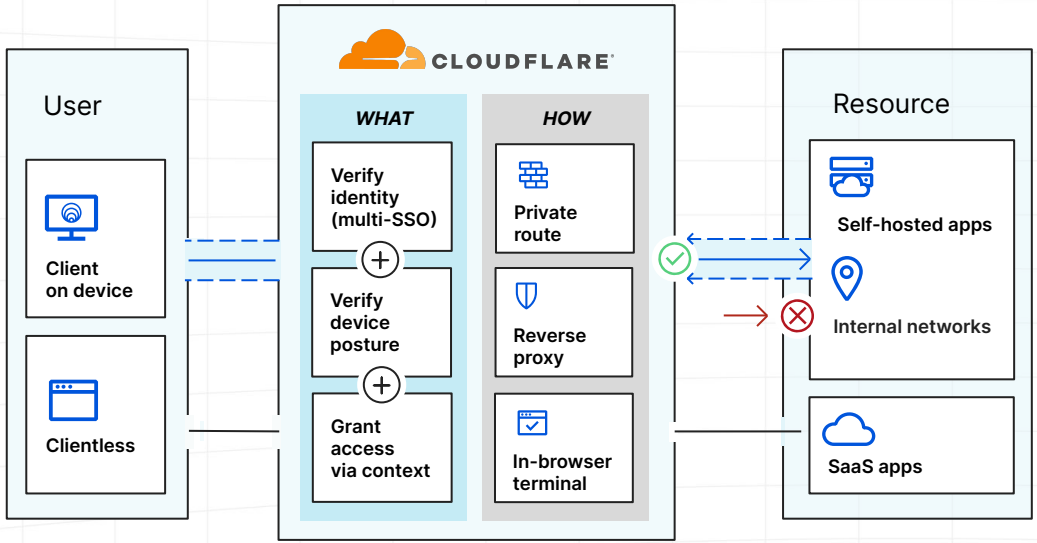
Clientless access
to rapidly adopt Zero Trust

Device clients
to fully replace your VPN

IP tunnels
over GRE/IPSec to phase out legacy MPLS networks

Direct connections
bring SASE to your doorstep at 1600+ colos and up to 1000 offices

Connecting private applications and networks



Use Cases:

1. **Enable Self-Hosted App Access via Public Hostnames**
2. **Enable Private Network Access**

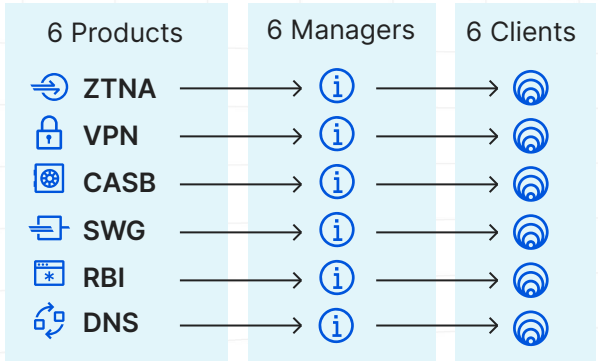
Application Supported:

- **HTTP/S**
- **RDP, SSH, and VNC**
- **SMB**
- **Kubectl**
- **unix socket**
- **arbitrary TCP and UDP**

CLOUDFLARE

One platform that simply works

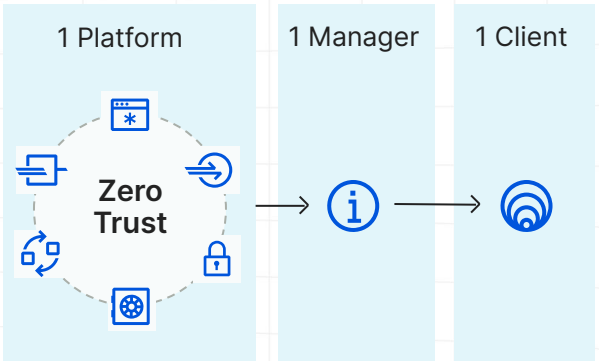
Traditional Approach



Problem #1:
Multiple point products require multiple policy managers, and multiple client deployments

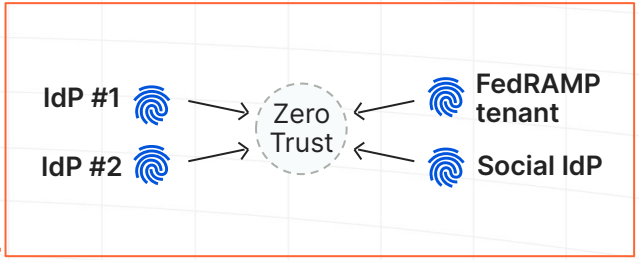
Solution:
One seamless platform uses one policy manager, and one client deployment

Cloudflare



Problem #2:
Integrate only one identity provider (IdP) repeatedly and inconsistently

Solution:
Integrate many IdPs and tenants of the same IdP just once



CLOUDFLARE

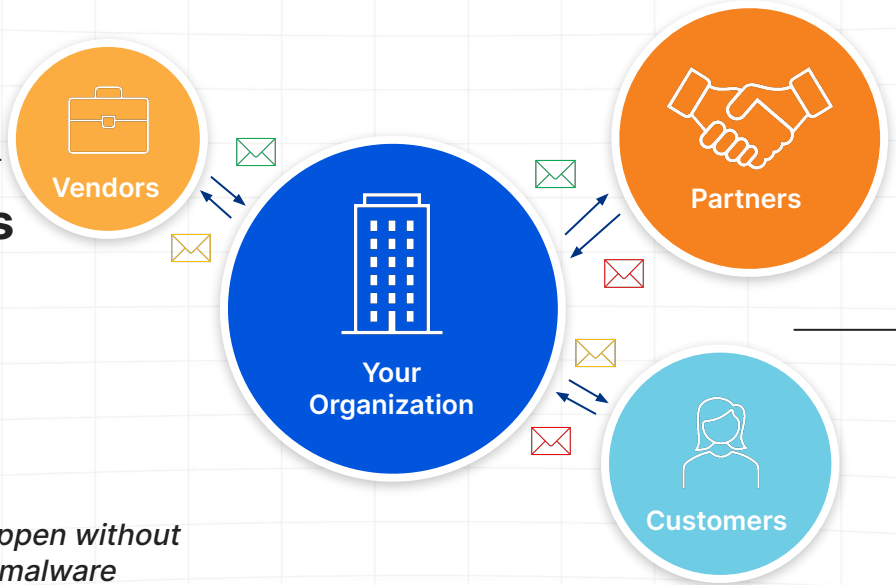
Email is the ...

#1 way organizations communicate

70%

of organizations use cloud email solutions today. (Gartner)

- *Email attacks can happen without network intrusion or malware*
- *Extends beyond direct employee access decisions*



#1 threat attack vector

91%

of all cyber attacks begin with a phishing email. (Deloitte)

CLOUDFLARE

Preemptive

Early Discovery
Campaign Hunting
Actor Infrastructure
Monitoring

Comprehensive

Continuous

Pre-Delivery
At-Delivery
Post-Delivery

Accountable

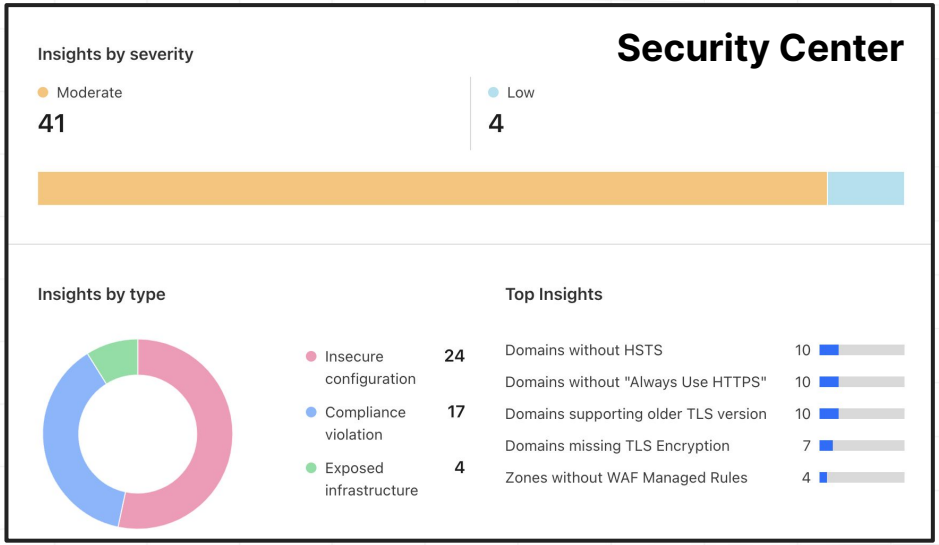
SLAs
Privacy
Biz Model

Contextual

Natural Language
Understanding
Sentiment Analysis
Intent, Tone & Relationships

REPORTING AND AUDITING

CLOUDFLARE



Cloudflare dashboard	**6 months** retention	**Analytic** summaries	**Workplace** records
Cloud storage platforms	amazon web services S3	Microsoft Azure Blob Storage	Google Cloud Storage
SIEM platforms	splunk>	sumo logic	DATADOG

REST API and Terraform – for SOAR and Audits

Summary

CLOUDFLARE

Hoe krijgen we de basis proactief op orde?

- Patchen van software en bewaak applicaties op vulnerabilities
  - ✅ Cloudflare WAF Managed Ruleset
- Applicatie toegang op basis van identiteit
  - ✅ Cloudflare Zero Trust
- Multi-factor authenticatie en/of Zero Trust architectuur
  - ✅ Cloudflare Zero Trust
- Veilige communicatie binnen de keten
  - ✅ Cloudflare Email Security
- Inzicht, rapportage en response
  - ✅ Security Center and Logpush

Meer informatie?

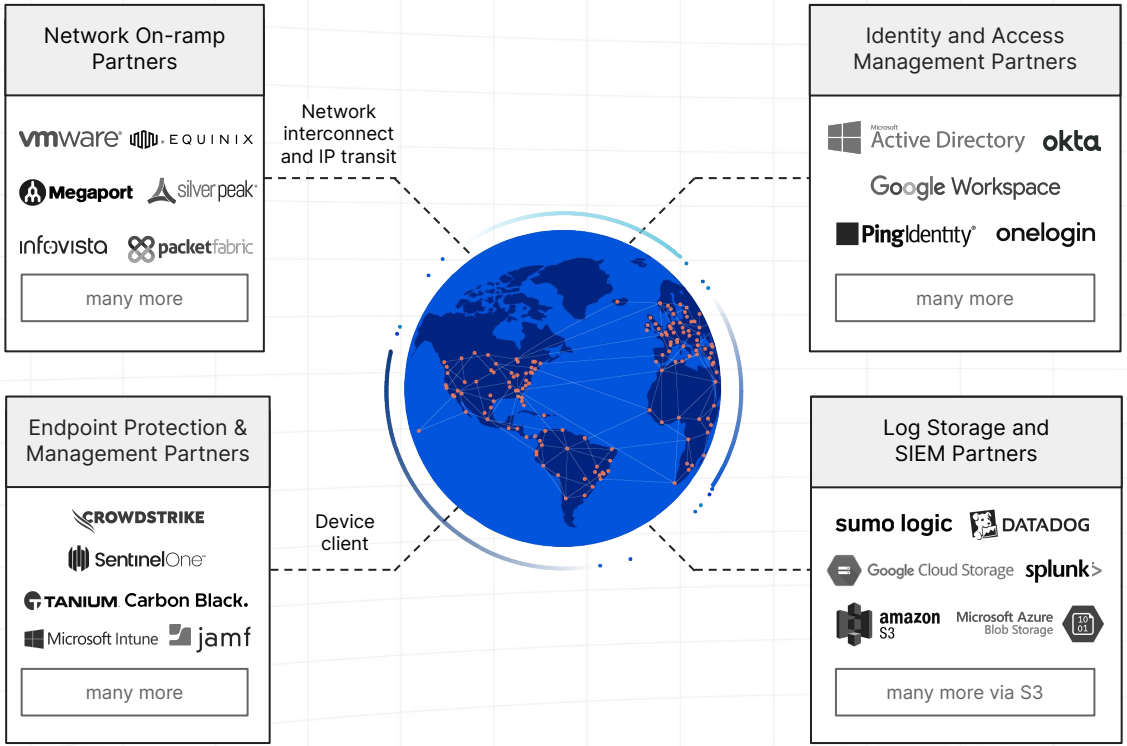
- **Booth C029** → Application / Zero Trust Security
- NIS2 whitepaper van Han Pieterse
- Webinar met Mark Tissink - 'Grip op informatiebeveiliging'
- Start een gratis Phishing Risk Assessment

zerotrustroadmap.org www.cloudflare.com

michiel.cloud/flare

Thank You

Connectivity and Visibility



We fit into your world

Identity, endpoint, and cloud agnostic

Concurrently use multiple providers

Programmable interface with Terraform automation

Cloudflare at a Glance

CLOUDFLARE

Cloudflare One

Cloudflare Zero Trust Services

- Zero Trust Network Access
- Secure Web Gateway
- Cloud Access Security Broker [1]
- Cloud Email Security
- Remote Browser Isolation
- Data Loss Prevention [2]

Cloudflare Network Services

- WAN-as-a-Service
- Firewall-as-a-Service
- L3 & L4 DDoS Protection
- Network Interconnect
- Smart Routing
- IDS/IPS [3]

Cloudflare Application Services

- Web Application Firewall
- CDN and DNS
- API Security and Management
- Load Balancing
- Bot Management
- L7 DDoS Protection
- Advanced Rate Limiting
- Client-side security

Cloudforce One Threat Intelligence

Cloudflare Edge Developer Platform

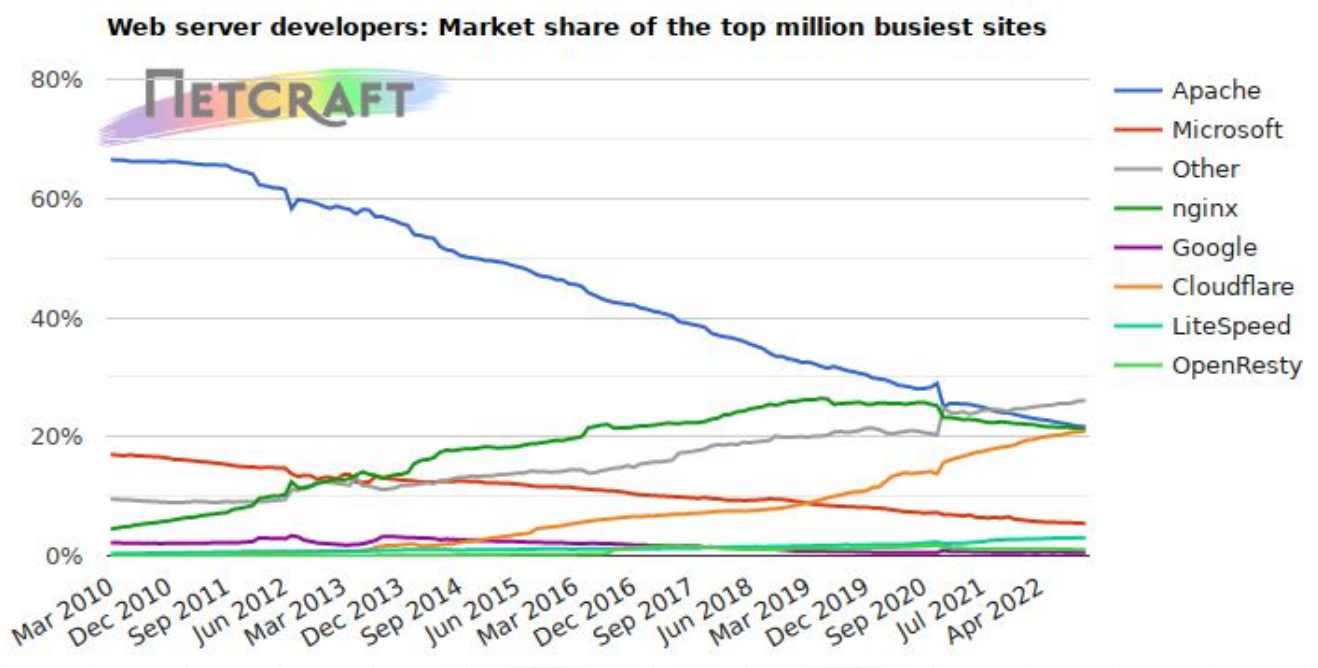
Workers | Workers KV | Pages | Durable Objects | Video Streaming

Cloudflare Global Network

- **Global Edge:** 275+ cities, 95% of population within 50ms, 11,000+ interconnects, 172 Tbps capacity, China Network
- **Building Blocks:** SSL/TLS, mTLS, Authoritative/Recursive DNS, DNSSEC, DNS over HTTP, L4-7 over Wireguard
- **Compliance/Privacy:** FedRAMP, ISO, SOC, PCI, GDPR compliant, Logs & Analytics, Data Localization Suite

Comprehensive coverage against Internet-borne threats

The Cloudflare Advantage



Source: Netcraft November 2022 Web Server Survey

CLOUDFLARE

Bereid je samen met Cloudflare voor op de Europese Cyber- Security Richtlijn

Traditionele Web Security oplossingen hebben een impact op de performance door de additionele apparatuur die al dan niet elders draait. Met de groei in belang van e-commerce, SEO en real-time APIs is dat niet langer houdbaar. Hetzelfde geldt ook de andere kant op voor het beveiligen van werknemers die het Internet door klikken. Cloudflare maakt in beide richtingen het verkeer veiliger zonder impact op performance, schaalbaarheid en compliancy en hoe gaat het bedrijfsleven om met de NIS2 Cybersecurity richtlijnen van de Europese Overheid.

Agenda

1. Intro (1m)
2. Wat is NIS2? (Han - 8m)
    a. Lijst van eisen?
3. Wat kan Cloudflare doen?
    a. Cloudflare Intro + Application Security + Zero Trust (15m)
4. Samenvatting (5m)
    a. Lijst van eisen + groene vinkjes ✅
    b. Closing remarks (Han)
5. Call to Action - kom naar booth/stuur mail om
    a. White paper van Han
    b. Phishing Risk Assessment te starten
    c. Meer te leren over Application / Zero Trust security
    d. Zerotrustroadmap.org / cloudflare.com

Zero Trust is a mindset shift

Perimeter determines trust		No perimeter, always verify
Secure perimeter, safe inside network (i.e. “castle & moat”)	Protection	Assume risk, reduce impact (encrypt, inspect, microsegment)
Log only login at the perimeter	Visibility	Log every login and request everywhere
Default allow, static access based on network location	Control	Default deny, least privilege based on identity & context

CLOUDFLARE

CLOUDFLARE

Simple, effective threat defense