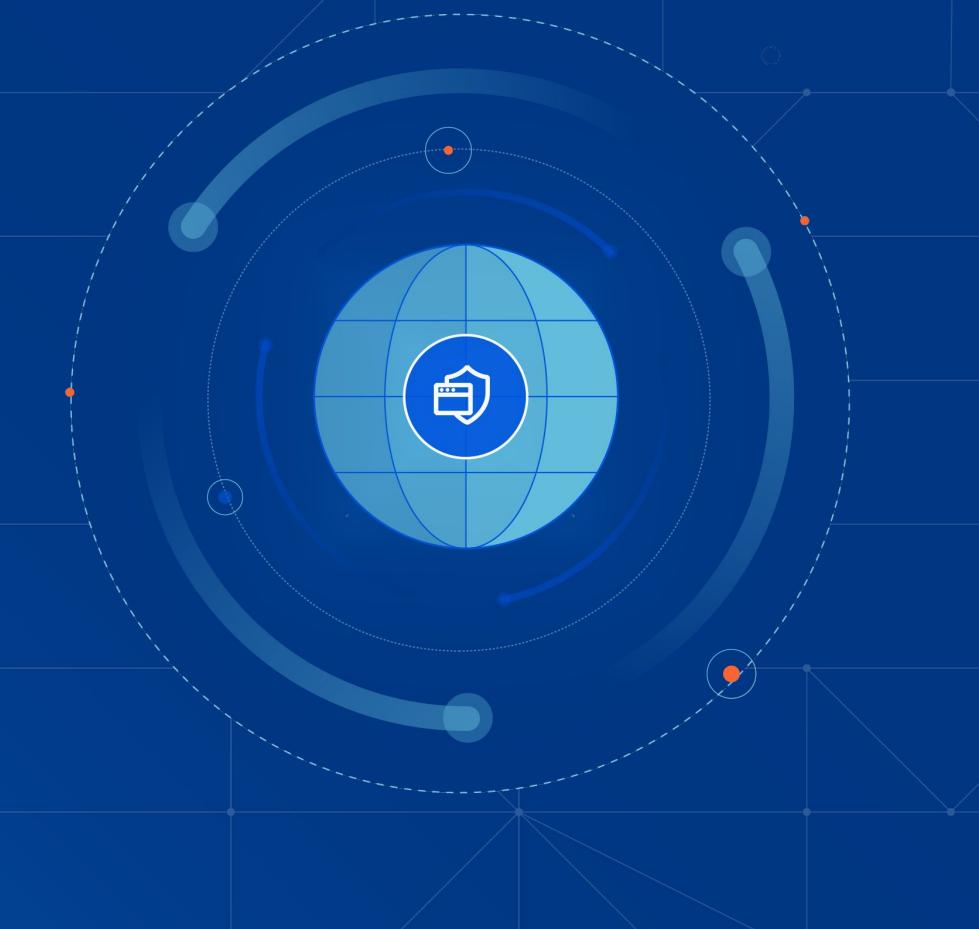




Bereid je samen met Cloudflare voor op de nieuwe Europese Cybersecurity Richtlijnen

Cloud Expo – 7 en 8 December 2022



WIE ZIJN WIJ?



Han Pieterse
Cyber Security Consultant



Michiel Appelman
Sr. Solutions Engineer – Cloudflare
michiel.cloudflare.com



Europese Cybersecurity Richtlijnen (NIS2)

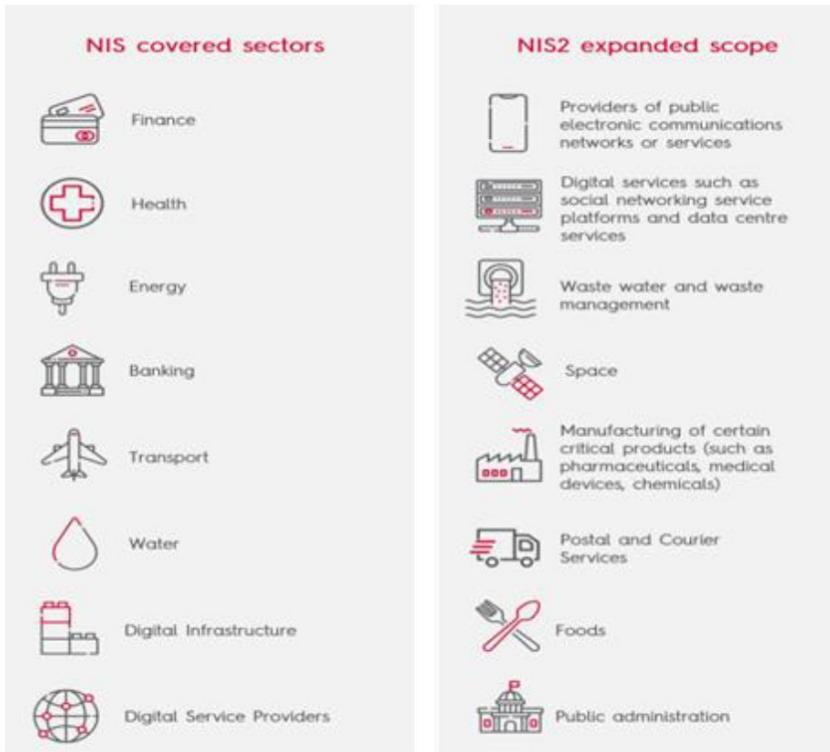
Wet beveiliging netwerk- en informatiesystemen (Wbni)

- 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 veiligheidsrisico's in toeleveringsketens en leveranciersrelaties te beheersen

Vernieuwing Wet beveiliging netwerk- en informatiesystemen (Wbni)



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

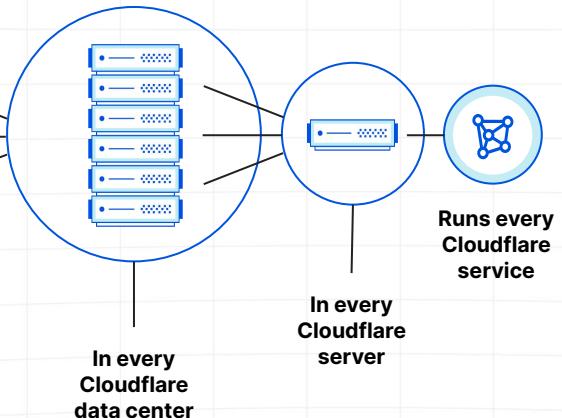
Hoe krijgen we de basis proactief op orde?

- 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

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

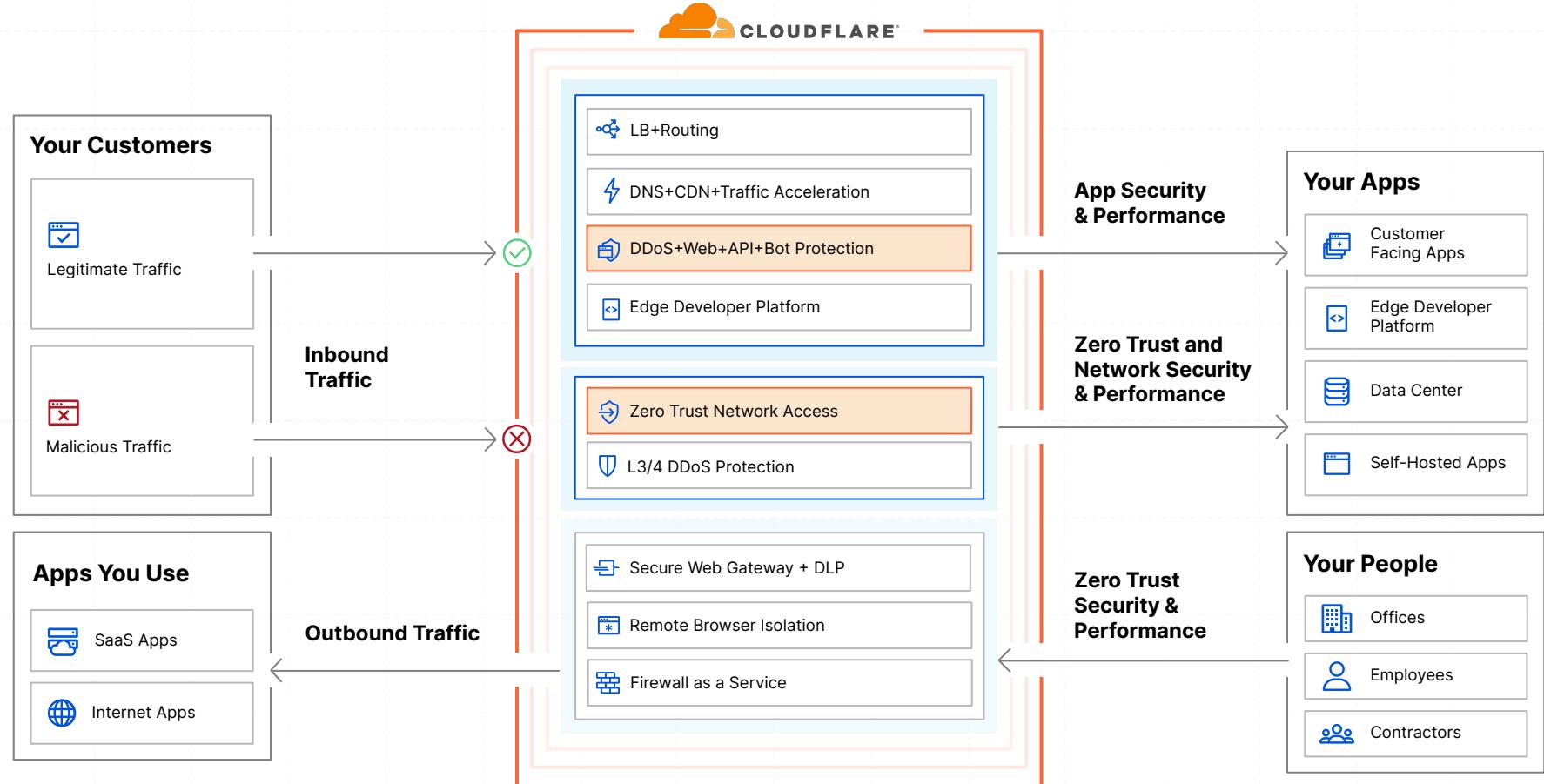


172 Tbps
of network capacity
with 11,000+ interconnects and
millions of internet properties

~50ms
from 95% of
Internet users

100%
uptime SLA

Single-pass Inspection for Ingress & Egress



Comprehensive coverage

against Internet-borne threats



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

Malware
Phishing
Cryptomining

Newly seen domains
New domains
Unreachable domains

DGA domains
DNS tunneling
C2 & botnet

Spyware
Spam
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 their customers exposed for an additional **NINE** hours.

Integrated Management & Analytics

Application DDoS
Block L7 DDoS attacks

WAF w/ advanced rate limiting
Stop attacks, abuse and exploits

Bot Management
Stop bot traffic

API Gateway
API security and management

Page Shield
Stop client-side attacks

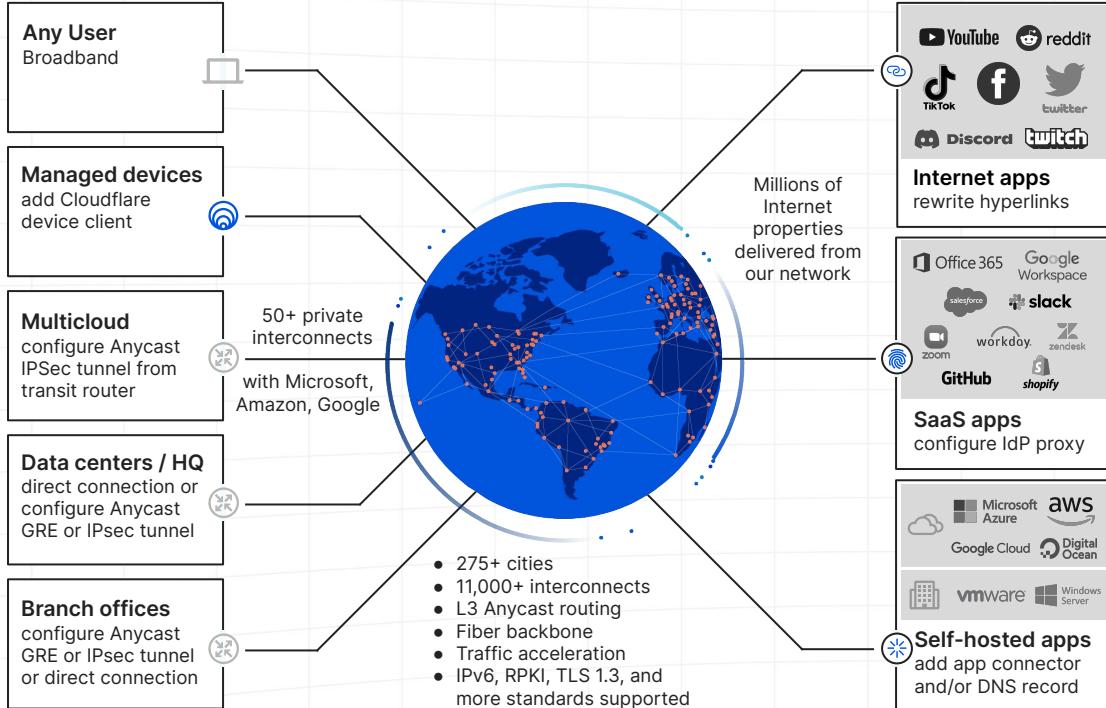
TLS/SSL
Data security

Cloudflare Security Center
Attack surface management



Cloudflare Zero Trust

Simple deployments, flexible architecture



Composable on-ramps

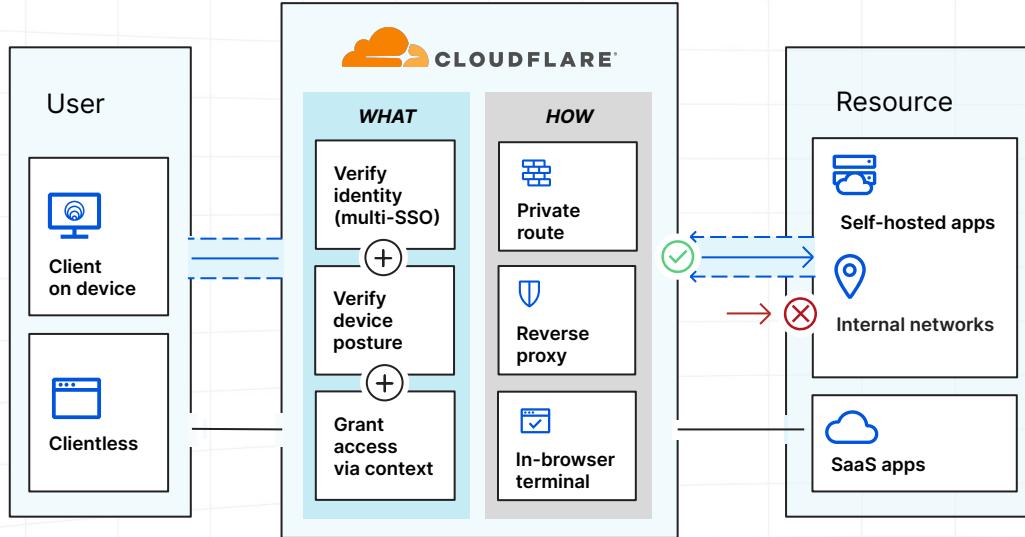
Clientless access
to rapidly adopt Zero Trust

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

One platform that simply works

Traditional Approach



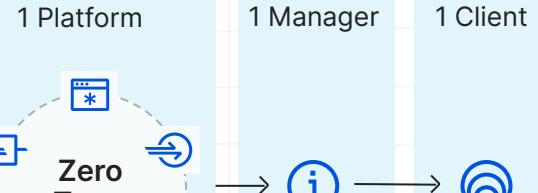
Problem #1:

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



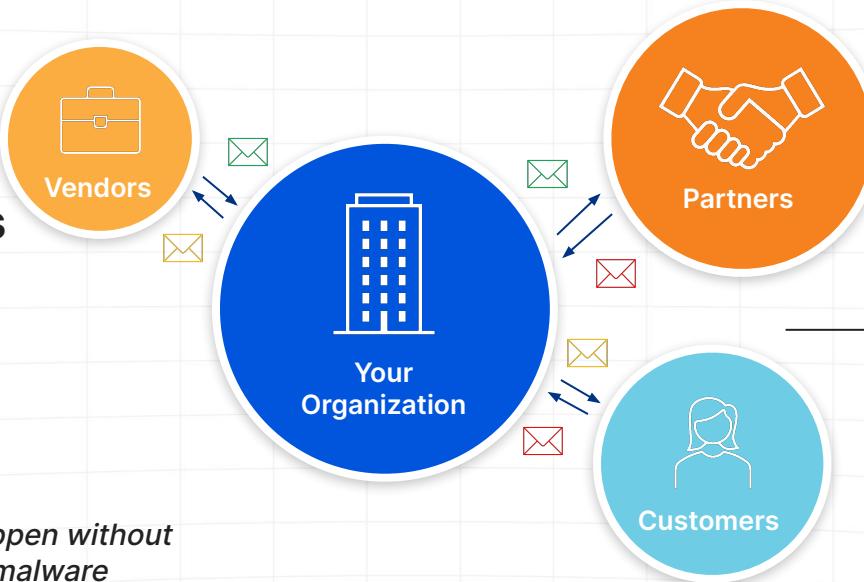
Email is the ...

#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)



Preemptive

Early Discovery
Campaign Hunting
Actor Infrastructure Monitoring



Continuous

Pre-Delivery
At-Delivery
Post-Delivery

Accountable

SLAs
Privacy
Biz Model

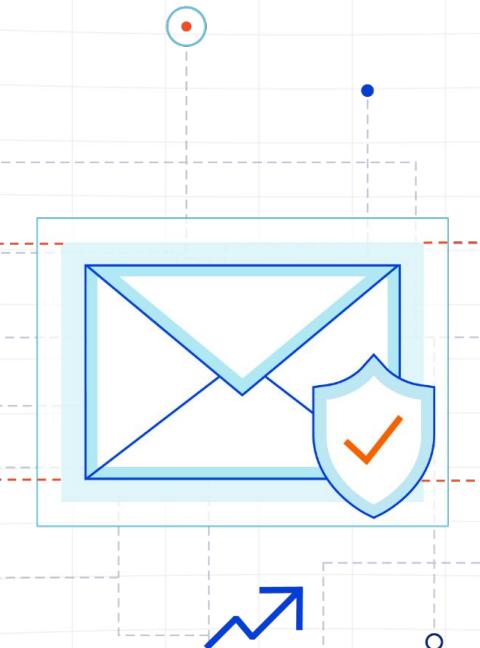


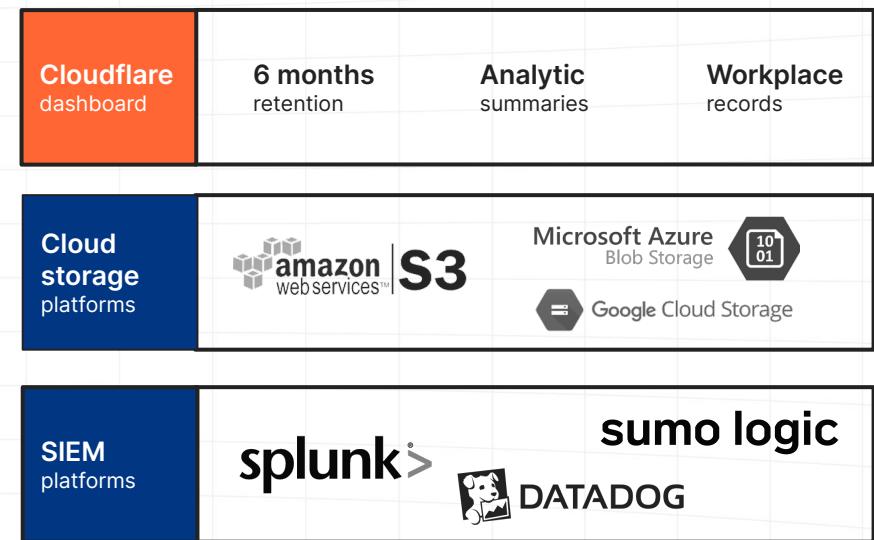
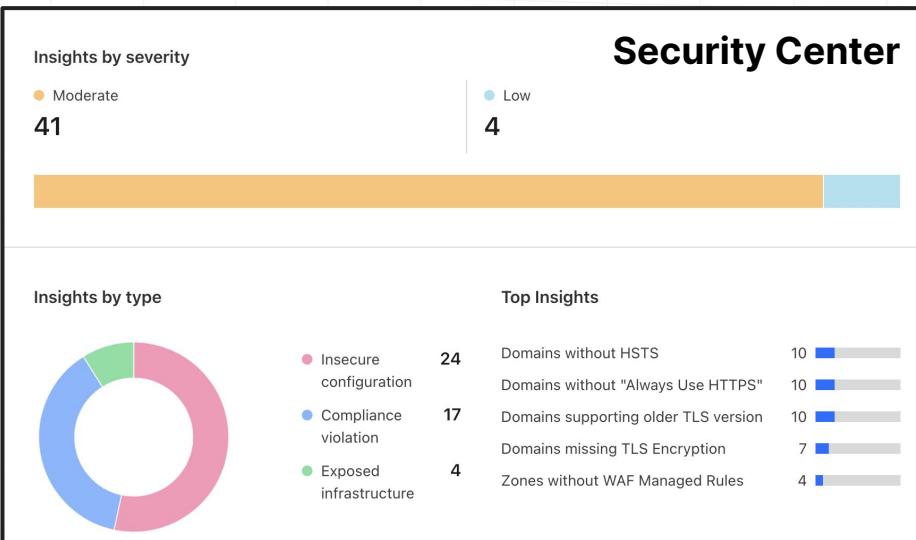
Comprehensive



Contextual

Natural Language Understanding
Sentiment Analysis
Intent, Tone & Relationships





REST API and Terraform – for SOAR and Audits



Summary

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

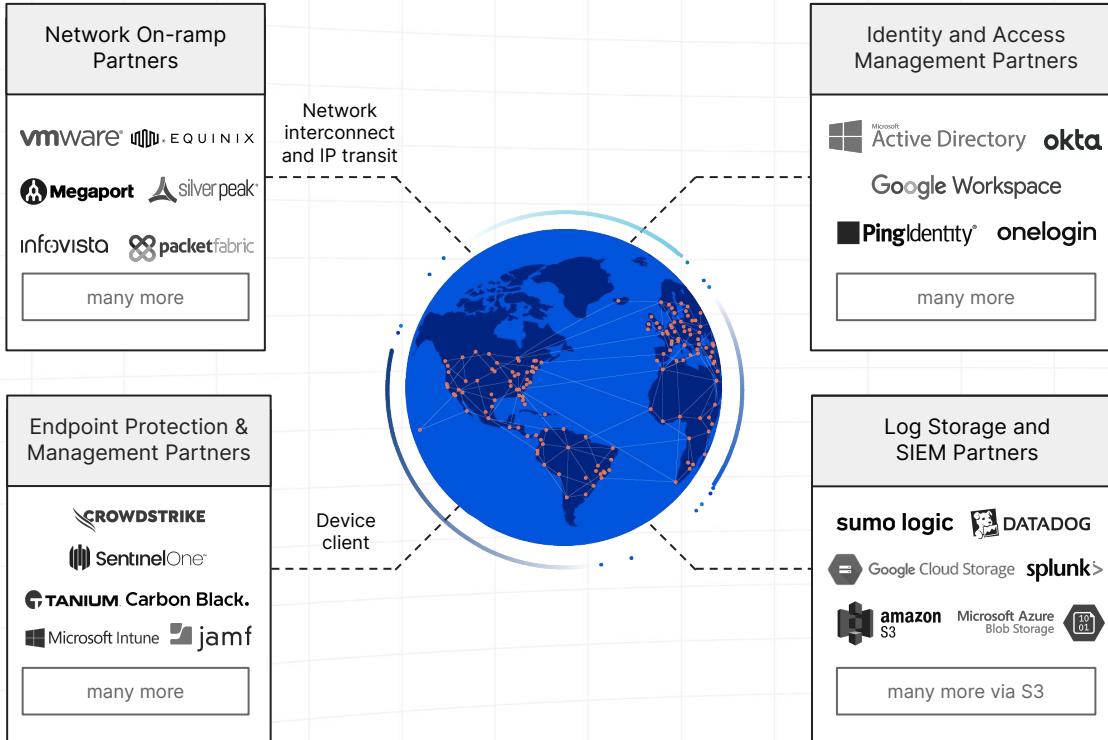
www.cloudflare.com

michiel.cloud/flare



Thank You

Connectivity and Visibility



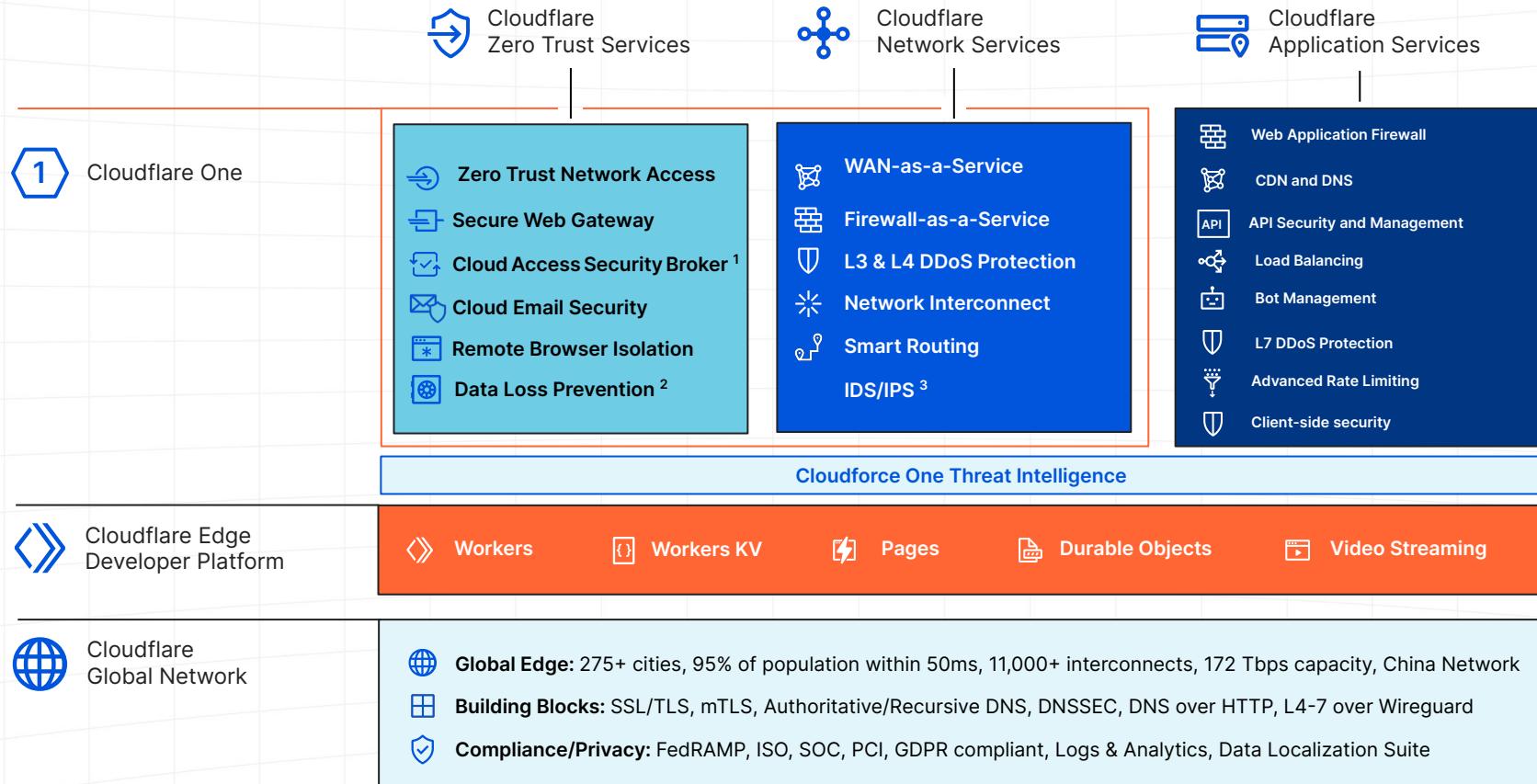
We fit into your world

Identity, endpoint,
and cloud agnostic

Concurrently use
multiple providers

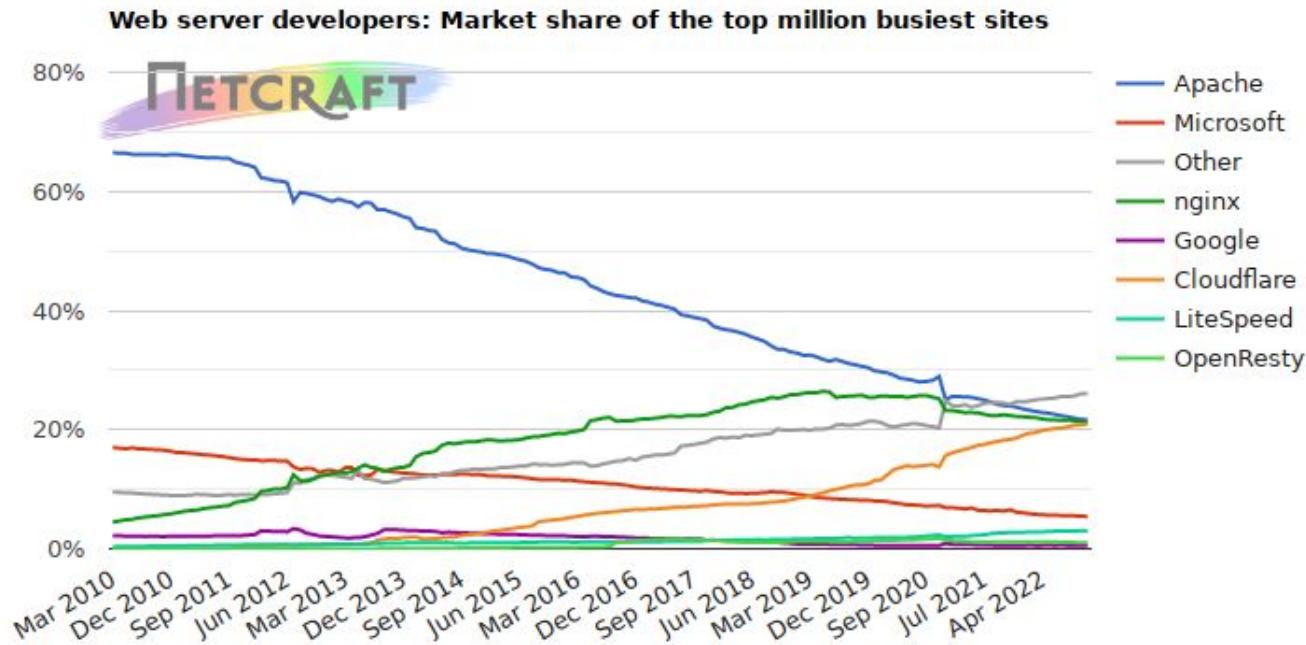
Programmable interface
with Terraform automation

Cloudflare at a Glance



Comprehensive coverage against Internet-borne threats

The Cloudflare Advantage



Source: Netcraft November 2022 Web Server Survey