We are helping build a better Internet.

Han Pieterse
Cyber Security Consultant

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

Europese Cybersecurity Richtlijnen (NIS2)

CLOUDFLARE

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

CLOUDFLARE

Vernieuwing Wet beveiliging netwerk- en informatiesystemen (Wbni)
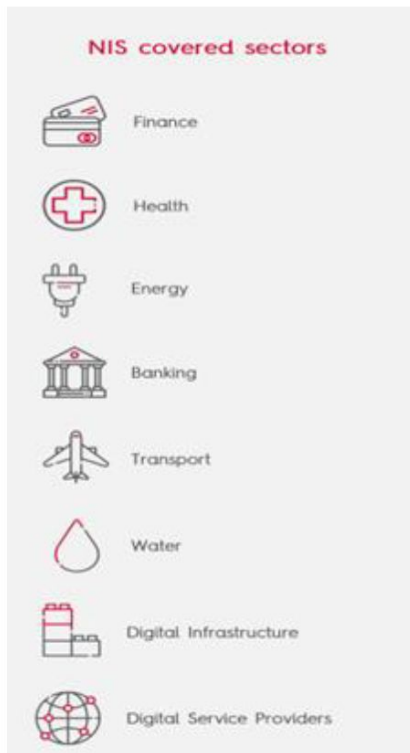
- Entiteiten worden ingedeeld in 'Essentieel' en 'Belangrijk'
- Expliciete governance vereisten
- Expliciete aansprakelijkheid voor bestuurders
- Rapportageverplichtingen
- Hogere administratieve boetes
- Basis op orde
- Leveranciers en partners medeverantwoordelijk in 'Essentiële' en 'Belangrijke' ketens
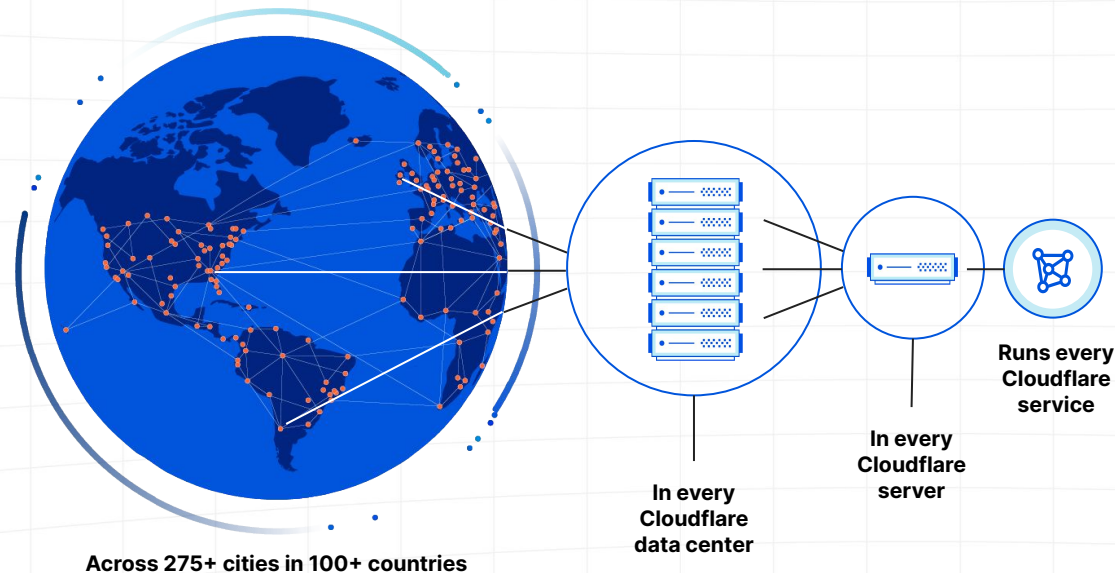
CLOUDFLARE

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 thrust architectuur

- Veilige communicatie binnen de keten

- Inzicht, rapportage en response

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

Across 275+ cities in 100+ countries

In every
Cloudflare
data center

In every
Cloudflare
server

Runs every
Cloudflare
service

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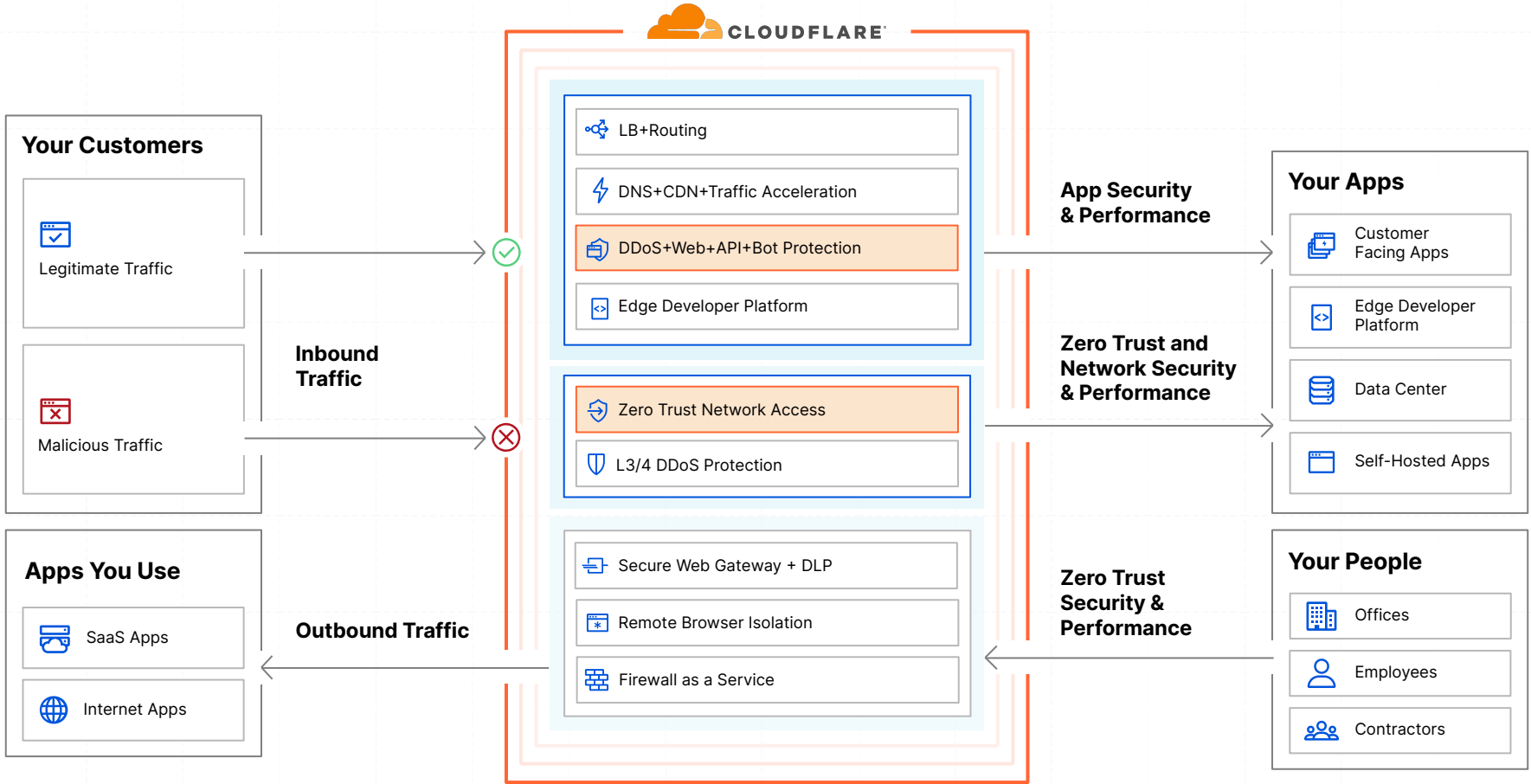of network capacity
with 11,000+ interconnects and
millions of internet properties

~50ms
from 95% of
Internet users

100%
uptime SLA

CLOUDFLARE • Cloudflare One

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

<500ms updates

EDGE **Telemetry from millions of customers and 275+ locations**

<500ms updates

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 • Cloudflare One

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.

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
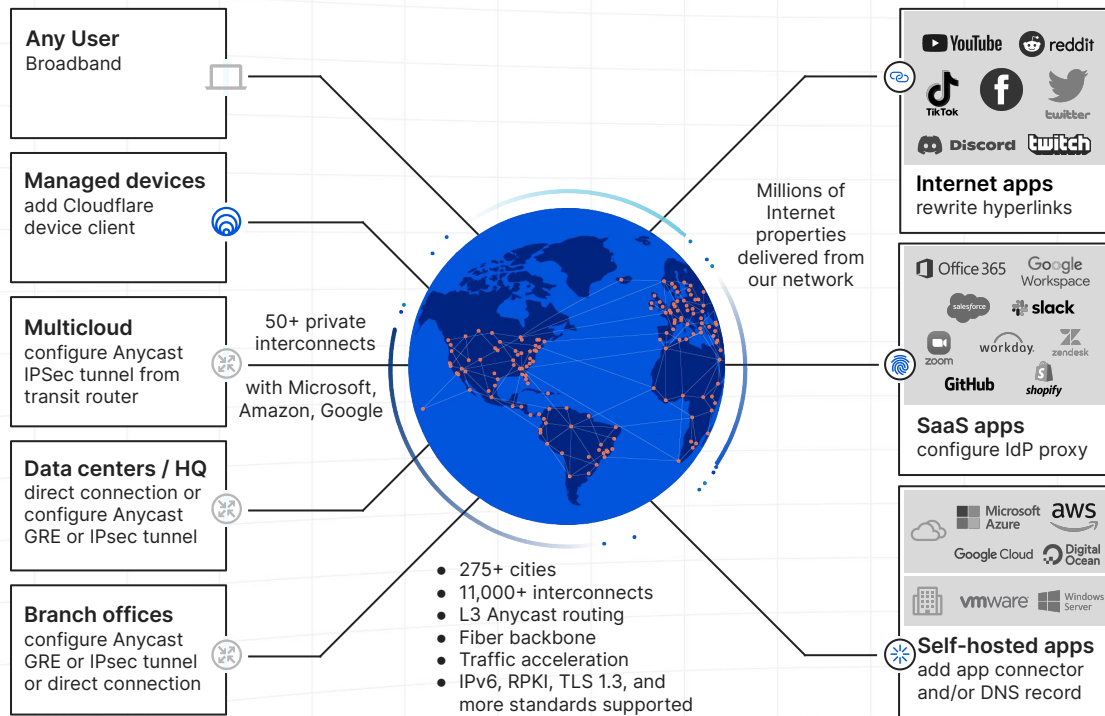Stop client-side attacks

TLS/SSL
Data security

Cloudflare Security Center
Attack surface management

Simple deployments,
flexible architecture

Any User
Broadband

Managed devices
add Cloudflare
device client

Multicloud
configure Anycast
IPSec tunnel from
transit router

Data centers / HQ
direct connection or
configure Anycast
GRE or IPsec tunnel

Branch offices
configure Anycast
GRE or IPsec tunnel
or direct connection

50+ private
interconnects

with Microsoft,
Amazon, Google

Millions of
Internet
properties
delivered from
our network

- 275+ cities
- 11,000+ interconnects
- L3 Anycast routing
- Fiber backbone
- Traffic acceleration
- IPv6, RPKI, TLS 1.3, and
  more standards supported

Internet apps
rewrite hyperlinks

SaaS apps
configure IdP proxy

Self-hosted apps
add app connector
and/or DNS record
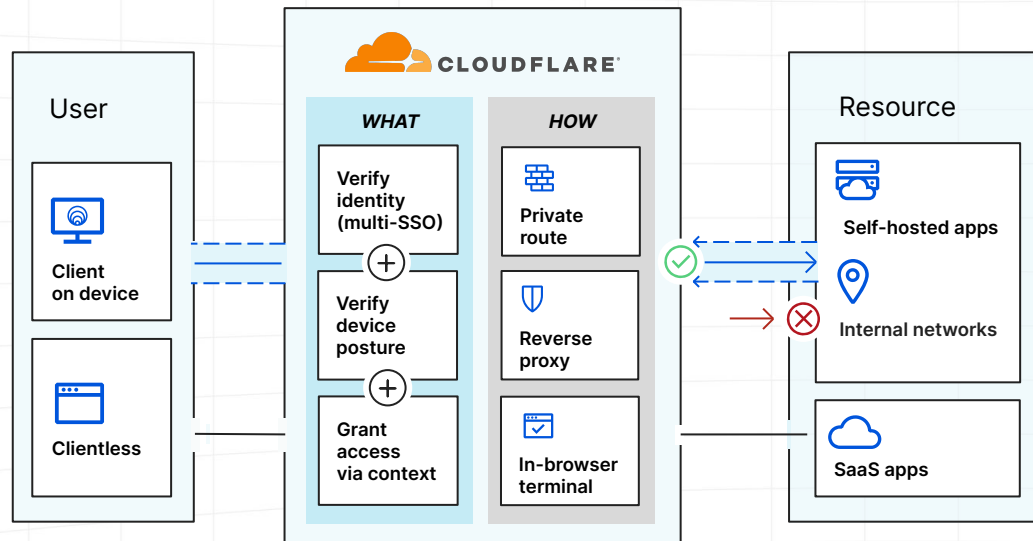
Composable
on-ramps

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

CLOUDFLARE • Cloudflare One

Connecting private applications and networks

Use Cases:

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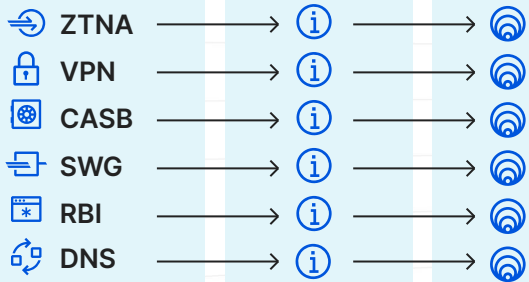
2. **Enable Private Network Access**

Application Supported:

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

CLOUDFLARE

One platform that simply works

Traditional Approach	Cloudflare

Traditional Approach

6 Products
- ZTNA
- VPN
- CASB
- SWG
- RBI
- DNS
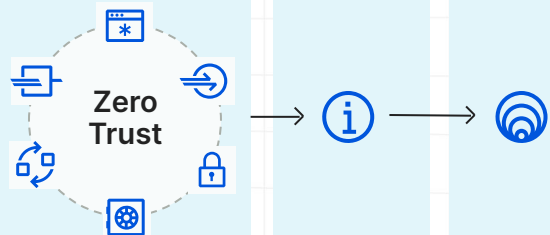
6 Managers

6 Clients

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

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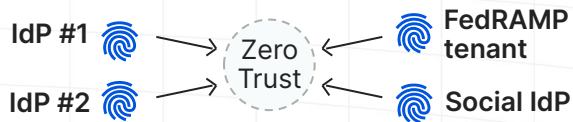One seamless platform uses one policy manager, and one client deployment

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

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

IdP #1   IdP #2

Cloudflare

1 Platform

Zero Trust

1 Manager

1 Client

IdP #1

IdP #2

Zero Trust

FedRAMP tenant

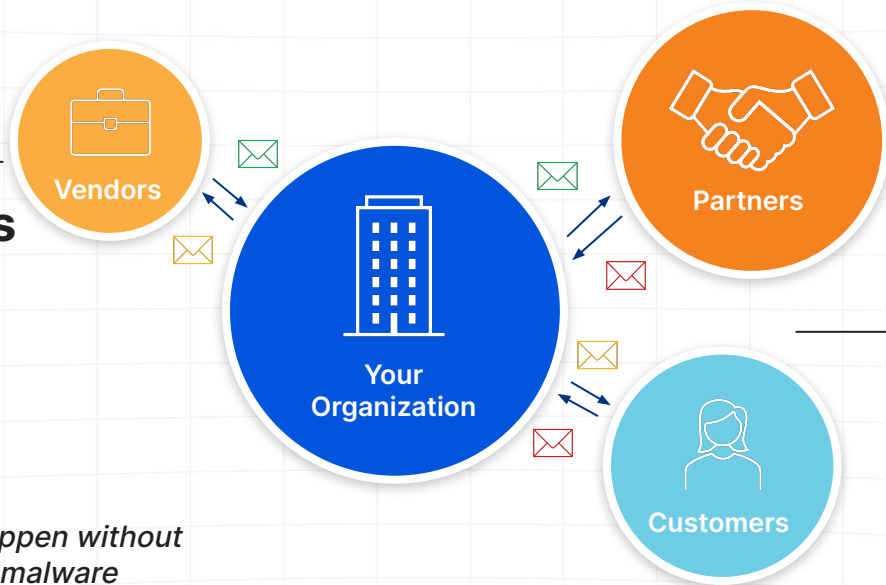Social IdP

CLOUDFLARE

Email is the ...

#1 way organizations communicate

70%

of organizations use cloud email solutions today. (Gartner)
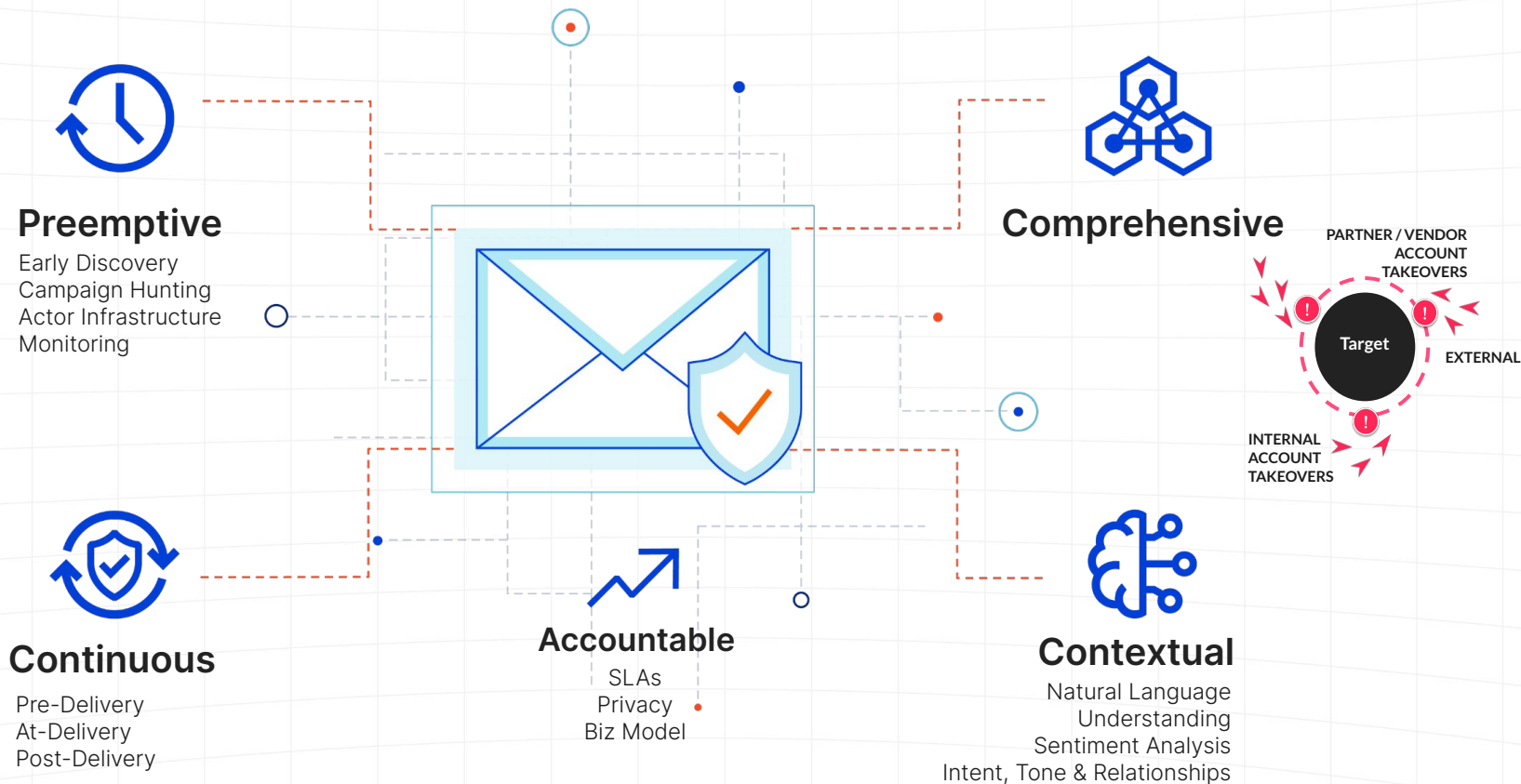
- *Email attacks can happen without network intrusion or malware*

- *Extends beyond direct employee access decisions*

#1 threat attack vector

91%

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

CLOUDFLARE EMAIL SECURITY

Preemptive
Early Discovery
Campaign Hunting
Actor Infrastructure
Monitoring

Comprehensive

PARTNER / VENDOR
ACCOUNT
TAKEOVERS

Target

EXTERNAL

INTERNAL
ACCOUNT
TAKEOVERS

Continuous
Pre-Delivery
At-Delivery
Post-Delivery

Accountable
SLAs
Privacy
Biz Model

Contextual
Natural Language
Understanding
Sentiment Analysis
Intent, Tone & Relationships

CLOUDFLARE®

Security Center

Insights by severity

● Moderate
41

● Low
4

Insights by type

Top Insights

● Insecure configuration   24

● Compliance violation   17

● Exposed infrastructure   4

Top Insights	
Domains without HSTS	10
Domains without "Always Use HTTPS"	10
Domains supporting older TLS version	10
Domains missing TLS Encryption	7
Zones without WAF Managed Rules	4

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>
DATADOG
sumo logic

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 op legacy applicaties
  - ✅ 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

Cloudflare

Thank You