

How Cloudflare Zero Trust can help you align to NIS2 cyber security risk management obligations?



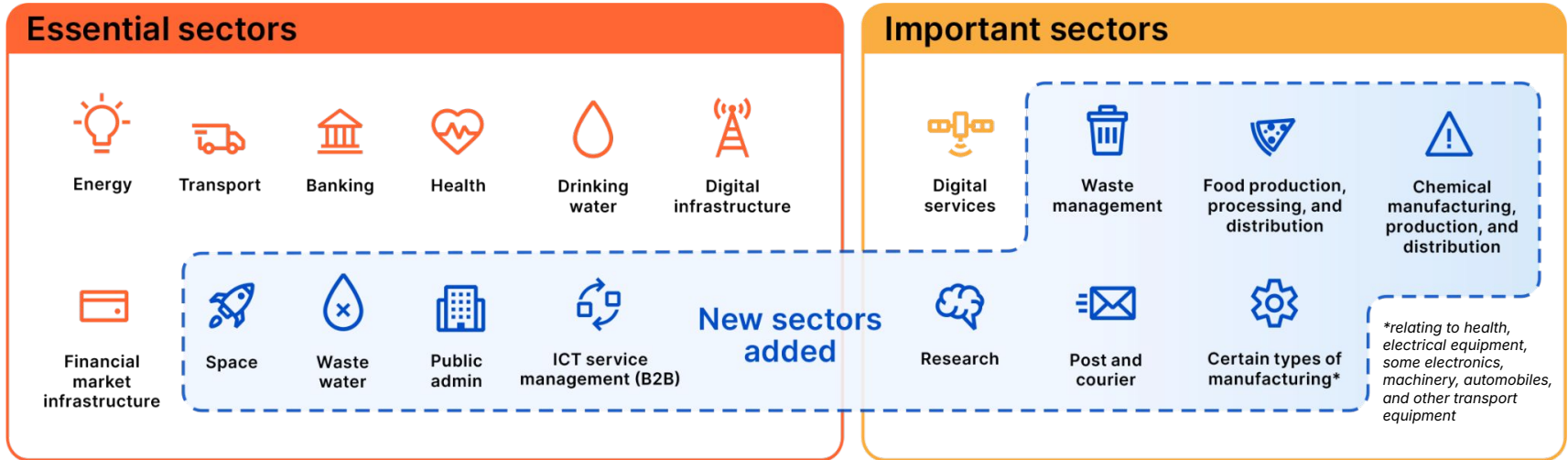
Jose Dores
Solutions Architect - Zero Trust
Cloudflare

NIS2 brings important changes regarding scope, requirements and enforcement

- The NIS2 Directive (2022) sets EU-wide minimum standards for cybersecurity
- EU Member States must transpose the new rules into national laws by October 17, 2024
- **Main changes:**
 - Broadened scope
 - New and stricter requirements for organizations in scope
 - Stronger enforcement



Significantly more organizations impacted by NIS2






Scope (simplified): Entities in **these sectors** with more than 50 employees and +€10M turnover*




*exceptions for some firms with a high security risk profile

More harmonized but more challenging obligations, with stronger enforcement

Obligations

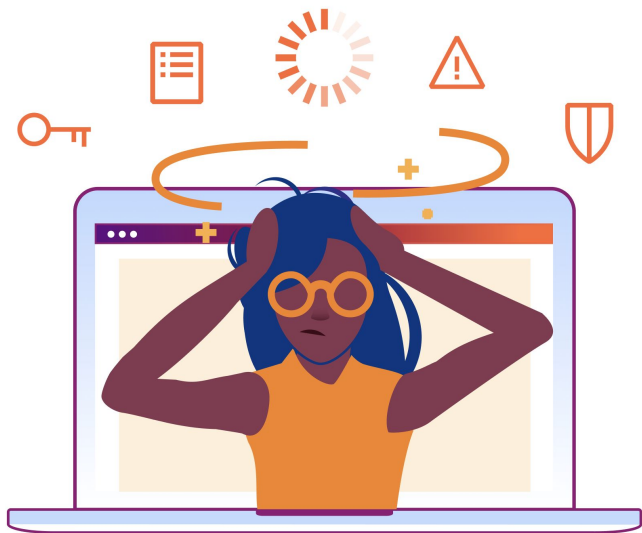
-  Accelerated incident reporting
-  Expanded, more granular risk management measures
-  Mandatory training for management

Enforcement

-  More enforcement powers
-  Higher administrative fines
-  Possible suspension of services/responsible management

Rising complexity, risks, and costs

hold back business growth



Cybersecurity risks are escalating

- Attack surfaces expanding
- Data volume exploding



Harder to stay efficient

- Stricter, more expansive regulations
- Legacy vendors and tool sprawl

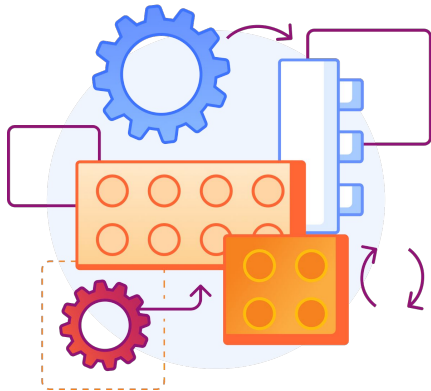
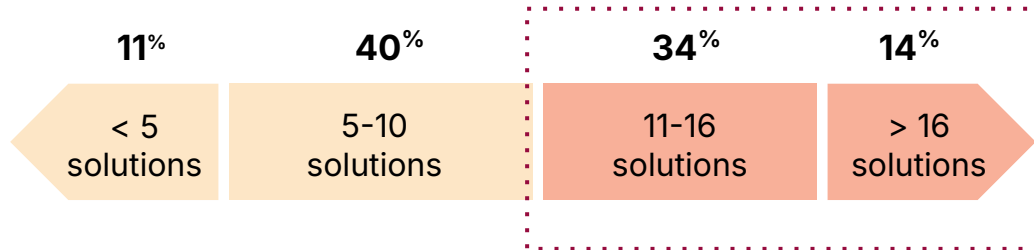


Traditional architectures are too complex

- Inflexible & disjointed point solutions
- Limited visibility and controls

More products... do not mean better protection

Number of cybersecurity solutions implemented among respondents



Organizations with **more than 10 solutions** are experiencing more overall incidents, longer incident response times, and **incurring greater financial losses...**

...and **two-thirds of respondents** expect the number of solutions they use to **increase** over the next 12 months.

Major increase in attacks against VPNs & other security appliances

2022

- Cyclops Blink
- F5 Big-IP Vulnerability
- Citrix APT Campaign
- Fortigate Zero-Day

2023

- Fortinet Zero-Day
- Jaguar Tooth Malware
- Zyxel-based Botnet
- Volt Typhoon
- Fortinet Exploit
- Citrix July Zero-Day
- Akira and Lockbit
- Cisco Zero-Days
- Citrix October Zero-Day

2024 (so far)

- Ivanti VPN Zero-Days
- Palo Alto VPN/Firewall Zero-Day
- Cisco VPN/Firewall Zero-Day
- Brute force campaign against major VPN and SSH providers

Attackers actively targeting “trusted” connections

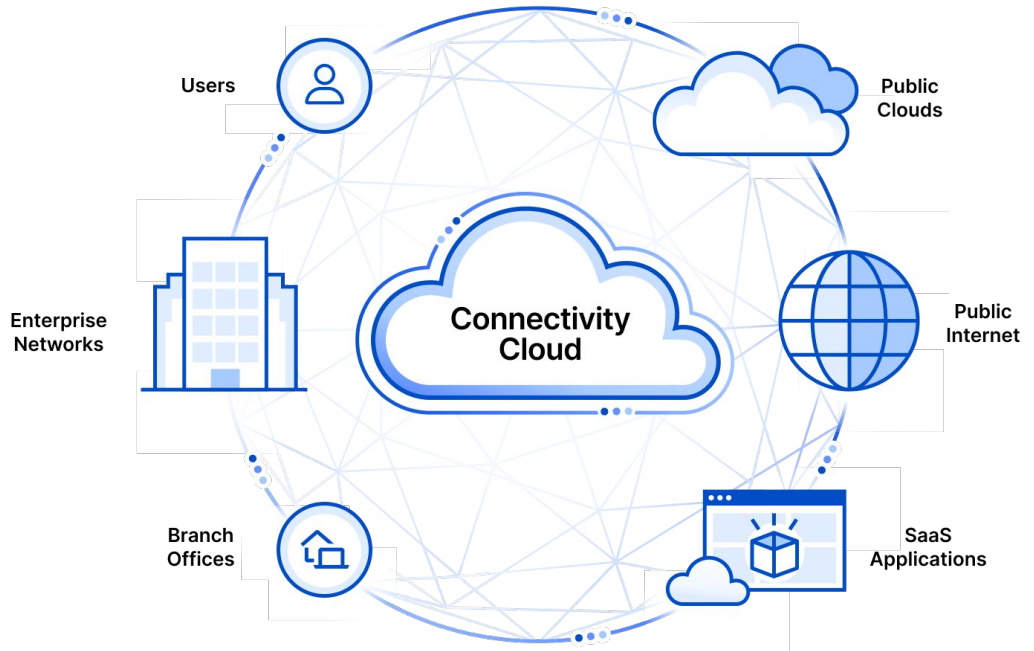


Introducing Cloudflare's Connectivity Cloud

With Cloudflare organizations can:

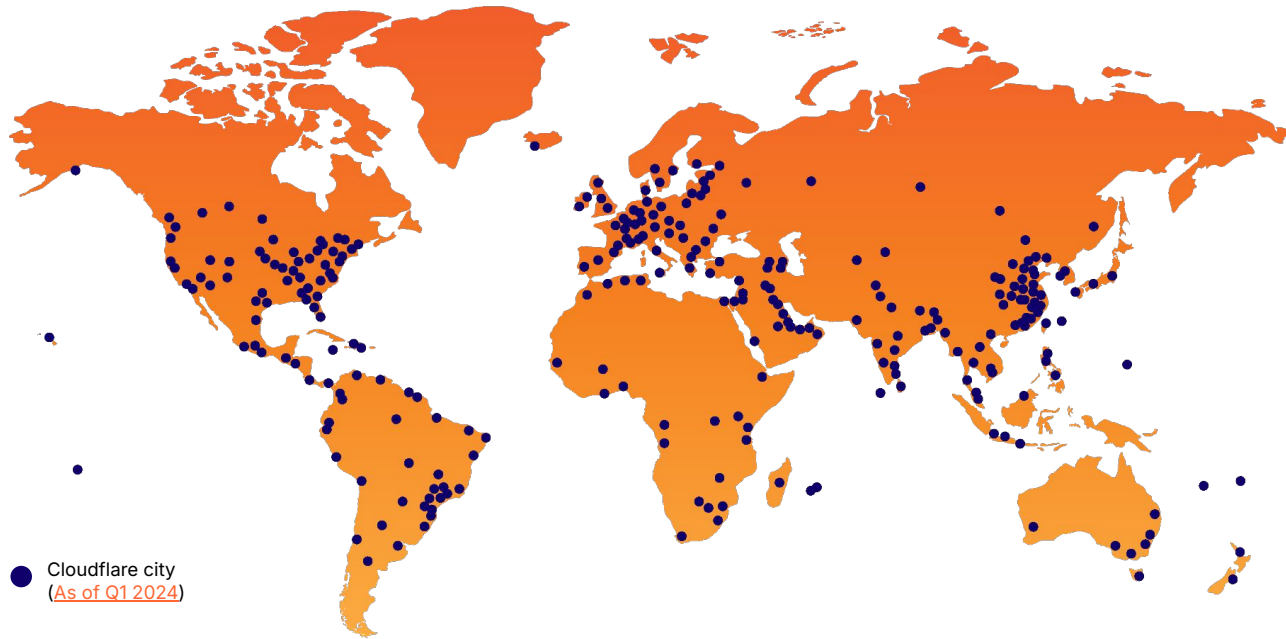
- **Connect** users, networks, apps and clouds globally
- **Protect** data, apps, infrastructure and users everywhere
- **Build** innovative digital services and experiences anywhere

with security, speed, programmability and resilience



Introducing Cloudflare's Connectivity Cloud

a single network that delivers local services at global scale



330

cities in 120+ countries,
including mainland China

150+

AI inference locations powered by GPUs

12,500+

networks directly connect to Cloudflare,
including every major ISP, cloud
provider, and enterprise

296 Tbps

global network edge capacity,
consisting of transit connections,
peering and private network
interconnects

~50 ms

NIS2 adheres to a **Zero Trust** approach

Measure 4: Supply chain security

Focuses on managing risks relating to external vendors and suppliers

Measure 5: Security in network and information systems

Enhance security throughout the full lifecycle of network and information systems

Measure 7: Training and basic cyber hygiene

Adopt Zero Trust principles, secure device configuration, network segmentation, identity and access management

Measure 9: Human resources security, access control, and asset management

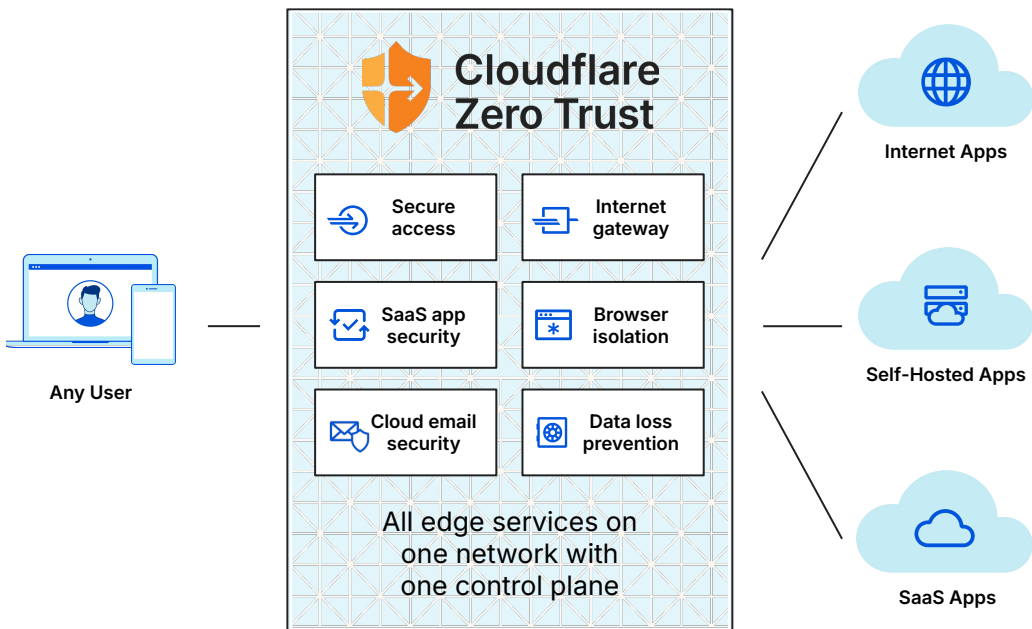
Protecting sensitive employee data, only authorized user have access to IT systems. Cyber security asset management

Measure 10: Use of multi-factor authentication and secure communications

Secure authentication beyond just username-password



How Cloudflare Zero Trust can help?



Use cases

Secure access

simplify and secure connecting any user to any resource

Threat defense

keep your data safe from threats over any port and protocol

SaaS security

visibility and control of applications including email

Security modernization

Improved productivity, simpler operations, reduced attack surface

How Cloudflare Zero Trust can help?

Measure 4: Supply chain security

Focuses on managing risks relating to external vendors and suppliers



Measure 5: Security in network and information systems

Enhance security throughout the full lifecycle of network and information systems



Measure 7: Training and basic cyber hygiene

Adopt Zero Trust principles, secure device configuration, network segmentation, identity and access management



Measure 9: Human resources security, access control, and asset management

Protecting sensitive employee data, only authorized user have access to IT systems. Cyber security asset management



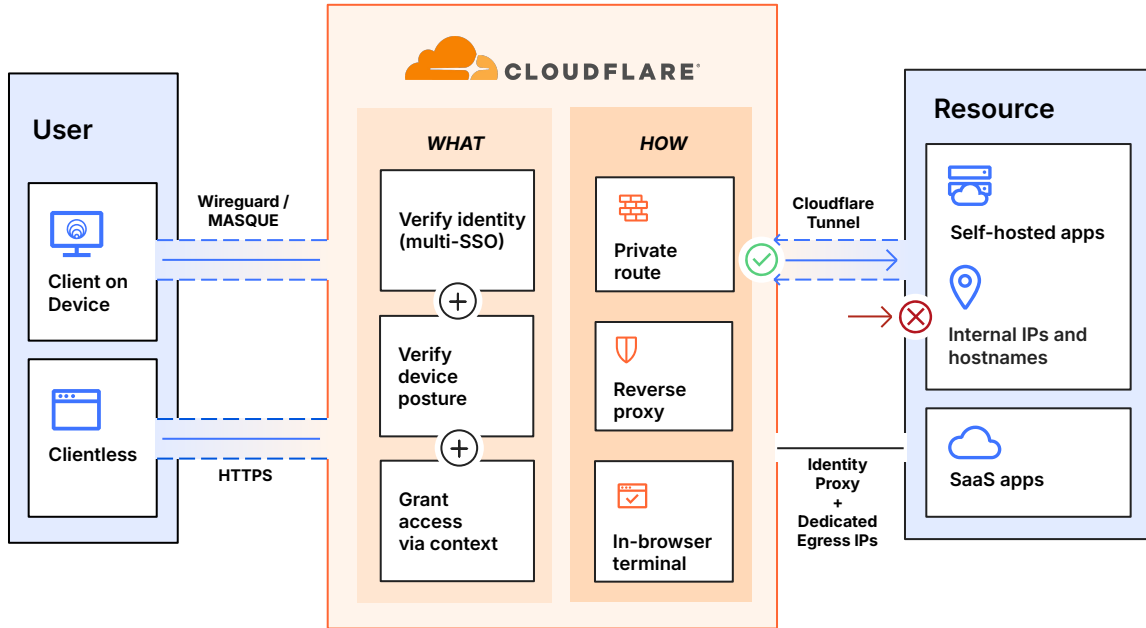
Measure 10: Use of multi-factor authentication and secure communications

Secure authentication beyond just username-password



Cloudflare Access

Zero Trust Network Access



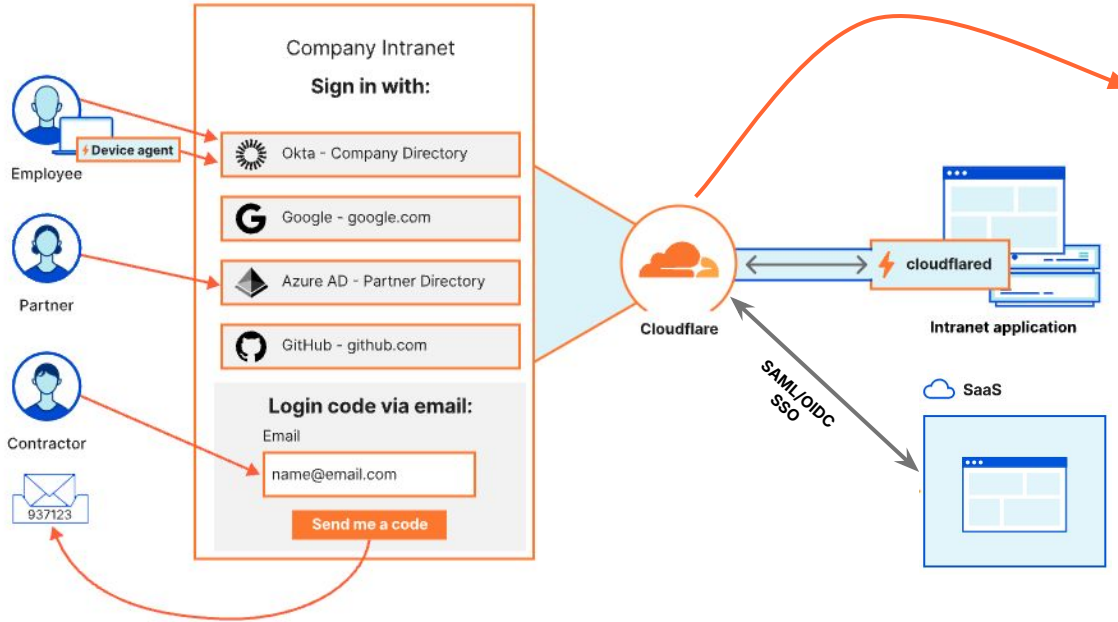
Simplify remote access;
augment or replace VPNs

Improve user experience for
all, including contractors

Reduce IT / help desk tickets
& eliminate lateral movement

Cloudflare Access

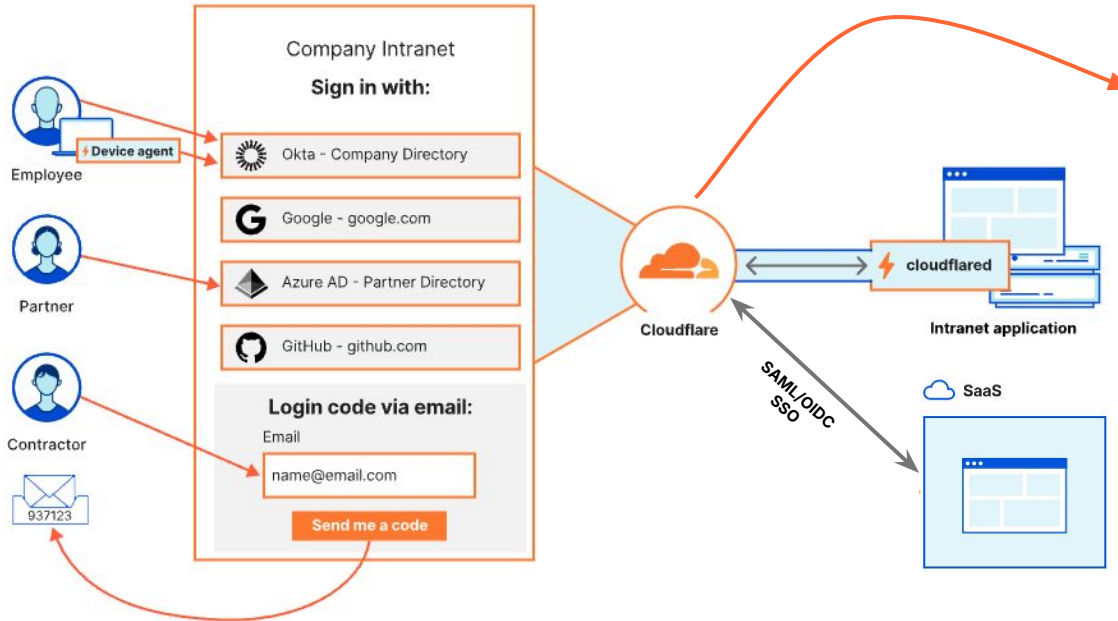
Secure access to applications consistently



Include	
Selector	Value
Okta Groups	finance
Azure Groups - Dev Account	Sales and Marketing
Require	
Selector	Value
Gateway	Gateway
Country	Netherlands
Authentication Method	mfa - multiple-factor authentication
Application Check	AppCheckWindows - Required SW
CrowdStrike Service to Service	CrowdStrike Overall ZTA score

Cloudflare Access

Logging of every access request



Export Logs (logpush)

3rd party storage and/or SIEM tools

Access denied

4 policies evaluated for Salesforce

User details

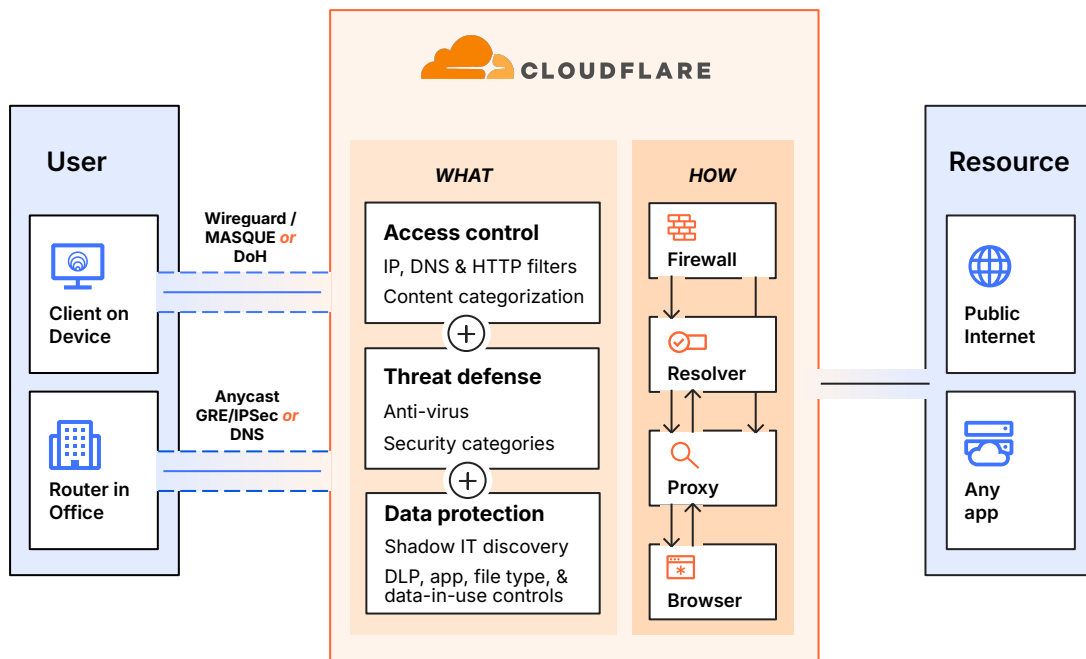
Name	Finance guru	Gateway	True
Email	finance@jdores.xyz	User ID	5181aff1f-
Last login	13 Oct 2023 · 11:25 AM	Authentication Method	None
Location	NL	Service token ID	None
IP Address	2a09:bac1:5500::22b:15	Service token status	None
Common name	None		
idP	Okta		
WARP	True		

Policies

- > marketing only ALLOW [Edit](#)
 - > finance only + MFA + require GW + posture MAC ALLOW [Edit](#)
 - > finance only + MFA + require GW + posture WINDOWS ALLOW [Edit](#)
- Configuration for the selected policy:
- Include 'Okta Groups':
 - Require 'Gateway':
 - Require 'Country':
 - Require 'Authentication Method':
 - Require 'Application Check':

Cloudflare Gateway

Internet threat and data protection



Simplify policy compliance

Stop phishing

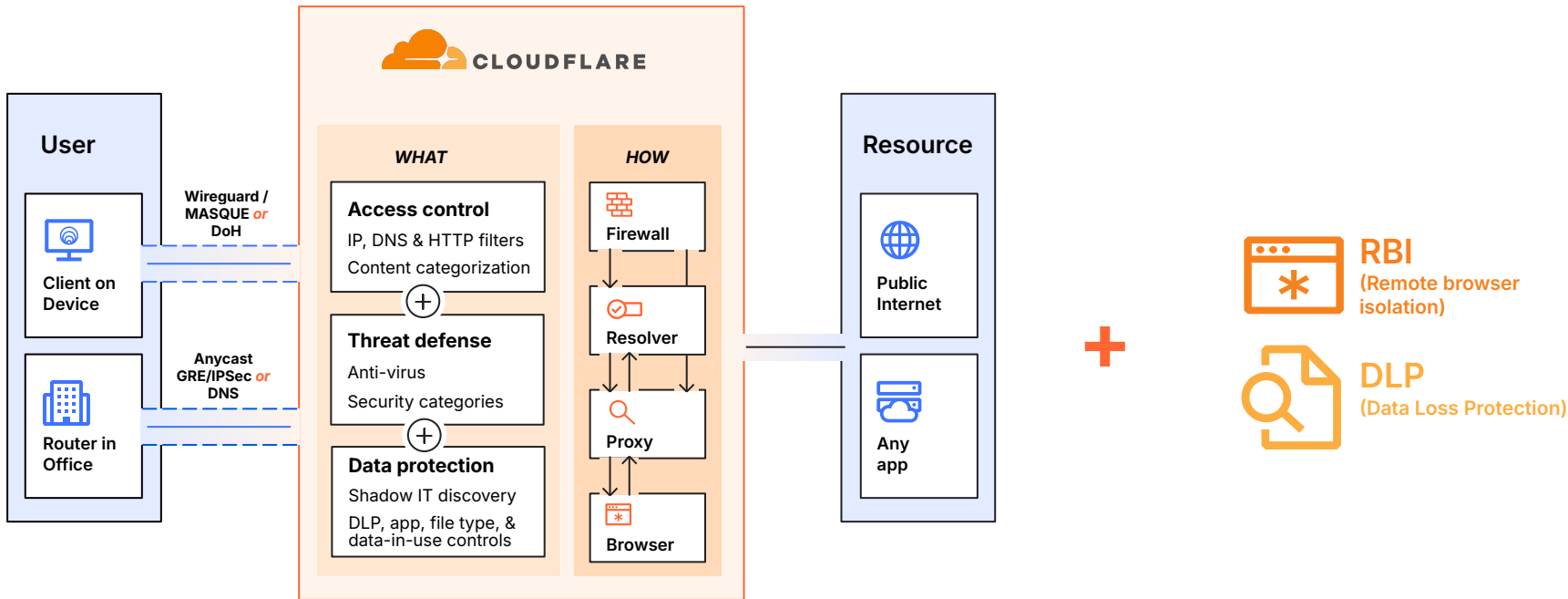
Stop ransomware

Stop shadow IT

Stop unknown threats

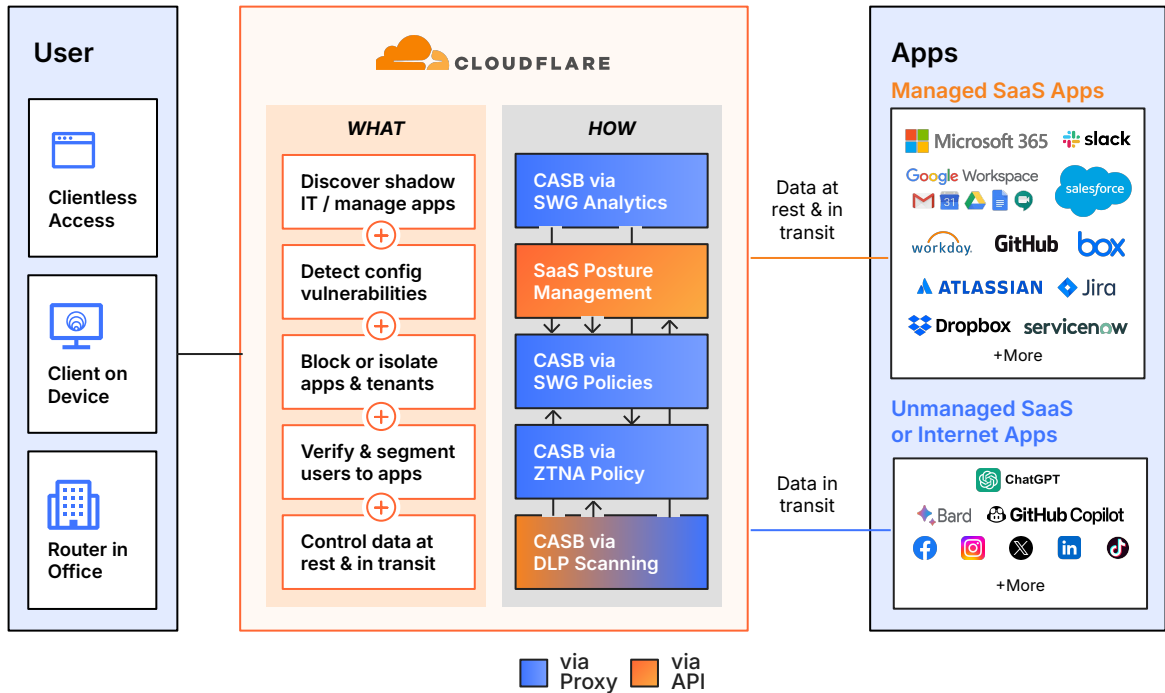
Cloudflare Gateway

Internet threat and data protection



SaaS data protection

Inline & API Cloud Access Security Broker



Inline

- Control access to unmanaged apps
- Set policies to block risky behaviors
- Stop data from leaving your tenants

API

- Integrate with your most used apps
- Detect security issues like:
 - Misconfigurations
 - Data exposure
 - Out-of-band access

Cloudflare **Application Services** are also relevant to NIS2

Measure 3: Business continuity

Keep applications running without interruption
DDoS protection, CDN, Spectrum, Magic Transit, ...

How Cloudflare auto-mitigated world record 3.8 Tbps DDoS attack



Measure 4: Supply chain security

Identifying potential vulnerabilities in or threats from third-party applications
WAF, Page Shield, Zaraz

Automatically replacing polyfill.io links with Cloudflare's mirror for a safer Internet



Measure 8: Cryptography and encryption

Configure state-of-the-art encryption and implement automated certificate management
Universal SSL, Advanced Certificate Manager, Geo Key Manager, ...

Cloudflare now uses post-quantum cryptography to talk to your origin server



A wide range of organizations rely on Cloudflare in the Baltic region



RIIGI INFOSÜSTEEMI AMET

Imt



VILNIUS

airBaltic



EESTI RAUDTEE



Litgrid

Delfi

Bolt



KERTINIS VALSTYBĖS
TELEKOMUNIKACIJŲ
CENTRAS

Vinted



NORD
SECURITY



Surfshark®



WHITEPAPER

A Roadmap to Zero Trust Architecture

Learn the steps, tools, & teams needed to transform your network and modernize your security



WHITE PAPER

Aligning to NIS2 cyber security risk management obligations in the EU

