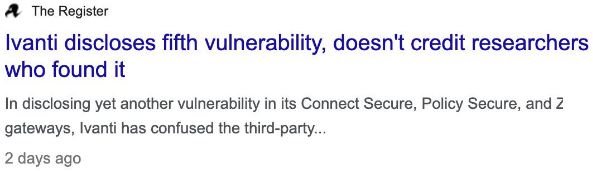
CLOUDFLARE

Santa Monica Networks

Your path to SASE & Zero Trust Architecture

Deniss Sagajevs
Andrey Moskvitin

VPN Vulnerabilities highlighted...

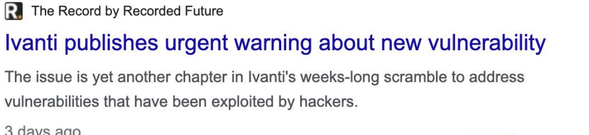


The Register

Ivanti discloses fifth vulnerability, doesn't credit researchers who found it

In disclosing yet another vulnerability in its Connect Secure, Policy Secure, and Z gateways, Ivanti has confused the third-party...

2 days ago

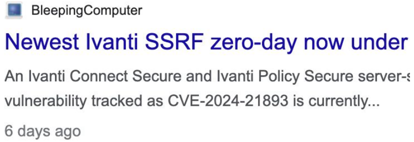


The Record by Recorded Future

Ivanti publishes urgent warning about new vulnerability

The issue is yet another chapter in Ivanti's weeks-long scramble to address vulnerabilities that have been exploited by hackers.

3 days ago

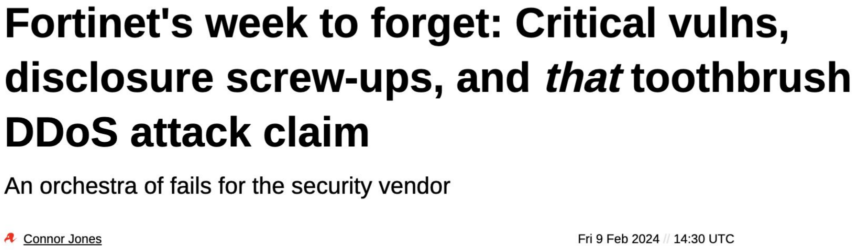


BleepingComputer

Newest Ivanti SSRF zero-day now under

An Ivanti Connect Secure and Ivanti Policy Secure server-s vulnerability tracked as CVE-2024-21893 is currently...

6 days ago

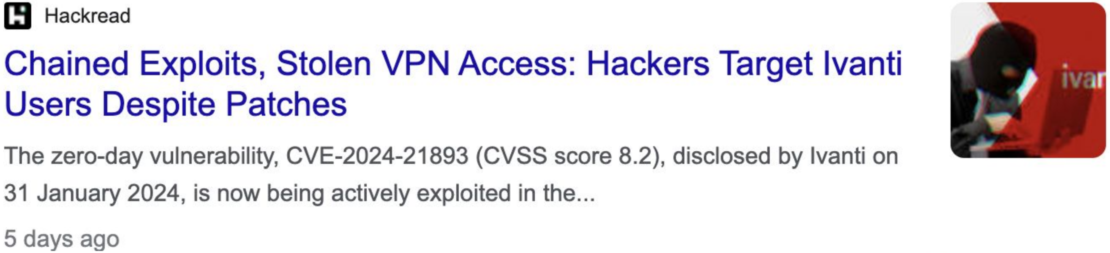


Fortinet's week to forget: Critical vulns, disclosure screw-ups, and *that* toothbrush DDoS attack claim

An orchestra of fails for the security vendor

Connor Jones

Fri 9 Feb 2024 // 14:30 UTC

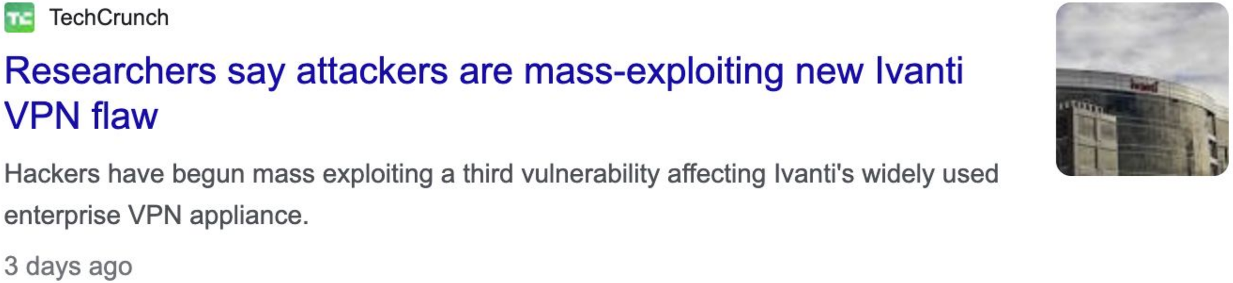


Hackread

Chained Exploits, Stolen VPN Access: Hackers Target Ivanti Users Despite Patches

The zero-day vulnerability, CVE-2024-21893 (CVSS score 8.2), disclosed by Ivanti on 31 January 2024, is now being actively exploited in the...

5 days ago



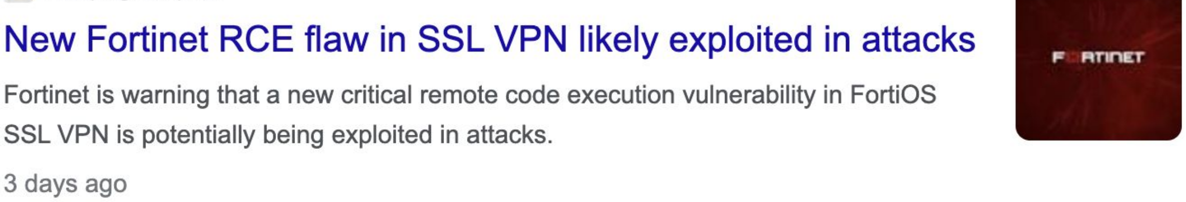
TechCrunch

Researchers say attackers are mass-exploiting new Ivanti VPN flaw

Hackers have begun mass exploiting a third vulnerability affecting Ivanti's widely used enterprise VPN appliance.

3 days ago

BleepingComputer

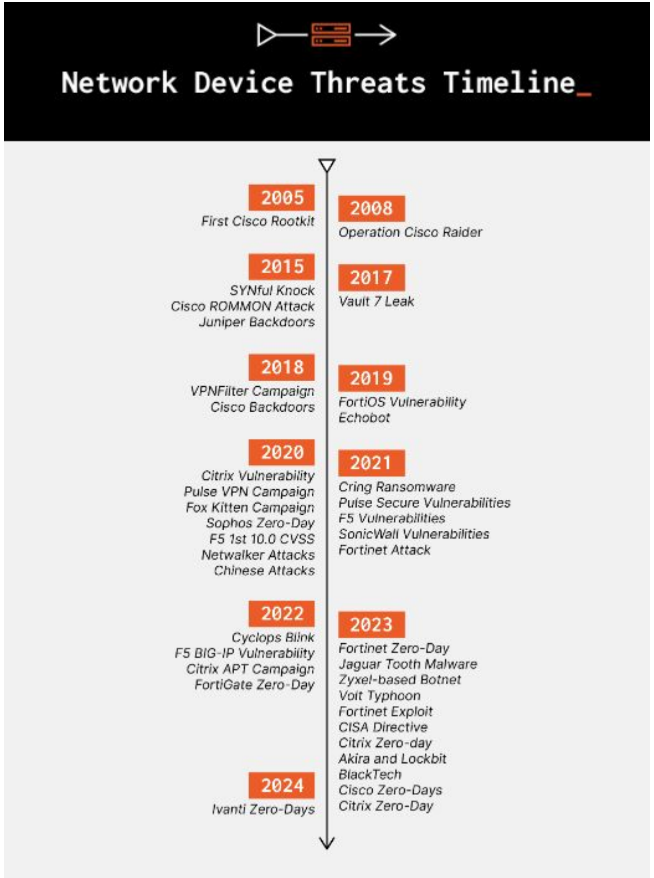


New Fortinet RCE flaw in SSL VPN likely exploited in attacks

Fortinet is warning that a new critical remote code execution vulnerability in FortiOS SSL VPN is potentially being exploited in attacks.

3 days ago

A LONG HISTORY OF VULNERABILITIES



Network Device Threats Timeline_

2005
First Cisco Rootkit

2008
Operation Cisco Raider

2015
SYNful Knock
Cisco ROMMON Attack
Juniper Backdoors

2017
Vault 7 Leak

2018
VPNFilter Campaign
Cisco Backdoors

2019
FortiOS Vulnerability
Echobot

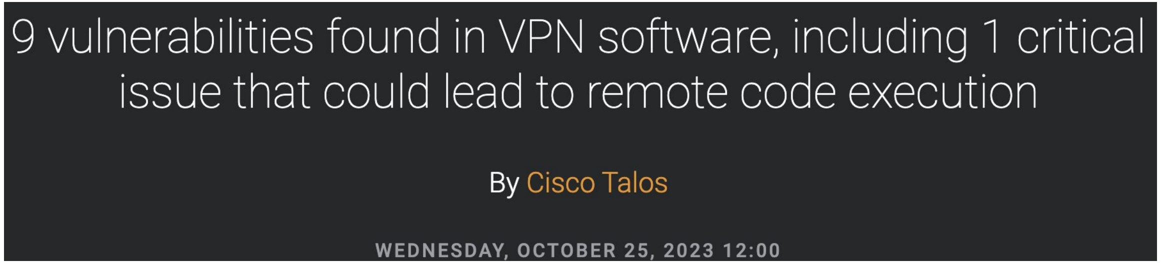
2020
Citrix Vulnerability
Pulse VPN Campaign
Fox Kitten Campaign
Sophos Zero-Day
F5 1st 10.0 CVSS
Netwalker Attacks
Chinese Attacks

2021
Cring Ransomware
Pulse Secure Vulnerabilities
F5 Vulnerabilities
SonicWall Vulnerabilities
Fortinet Attack

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
CISA Directive
Citrix Zero-day
Akira and Lockbit
BlackTech
Cisco Zero-Days
Citrix Zero-Day

2024
Ivanti Zero-Days

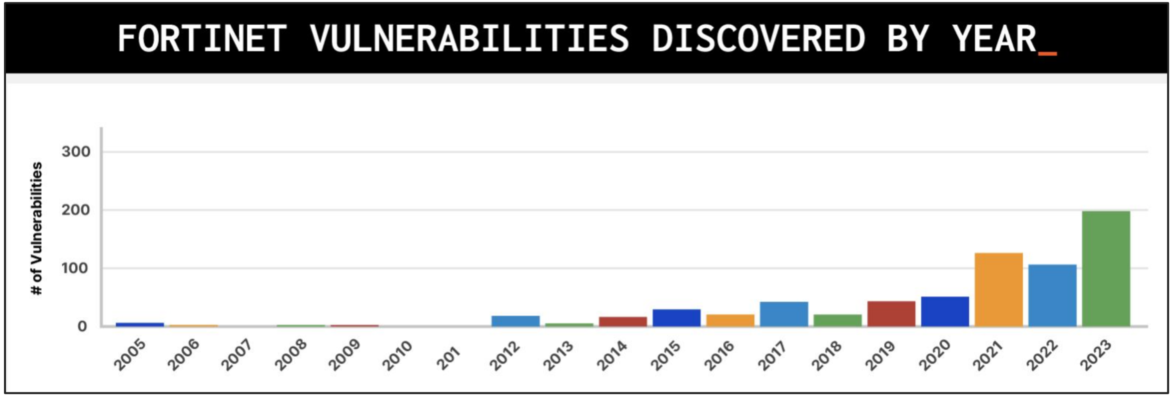


9 vulnerabilities found in VPN software, including 1 critical issue that could lead to remote code execution

By Cisco Talos

WEDNESDAY, OCTOBER 25, 2023 12:00

https://blog.talosintelligence.com/vulnerability-roundup-oct-25-2023/



FORTINET VULNERABILITIES DISCOVERED BY YEAR_

VPNs are inherently flawed

Putting users on the network creates risk

A VPN requires giving employees and third parties direct access to the corporate network. The moment a user tunnels into the network via VPN, they are viewed as “trusted” without knowing whether they have earned sufficient trust and are granted lateral access.

High costs and even higher complexity

The cost of a full VPN gateway appliance stack becomes more expensive as latency and capacity limitations require organizations to replicate the stacks at each of their data centers. In fact, the majority of companies (61%) have three or more VPN gateways, making it more difficult to manage and scale.

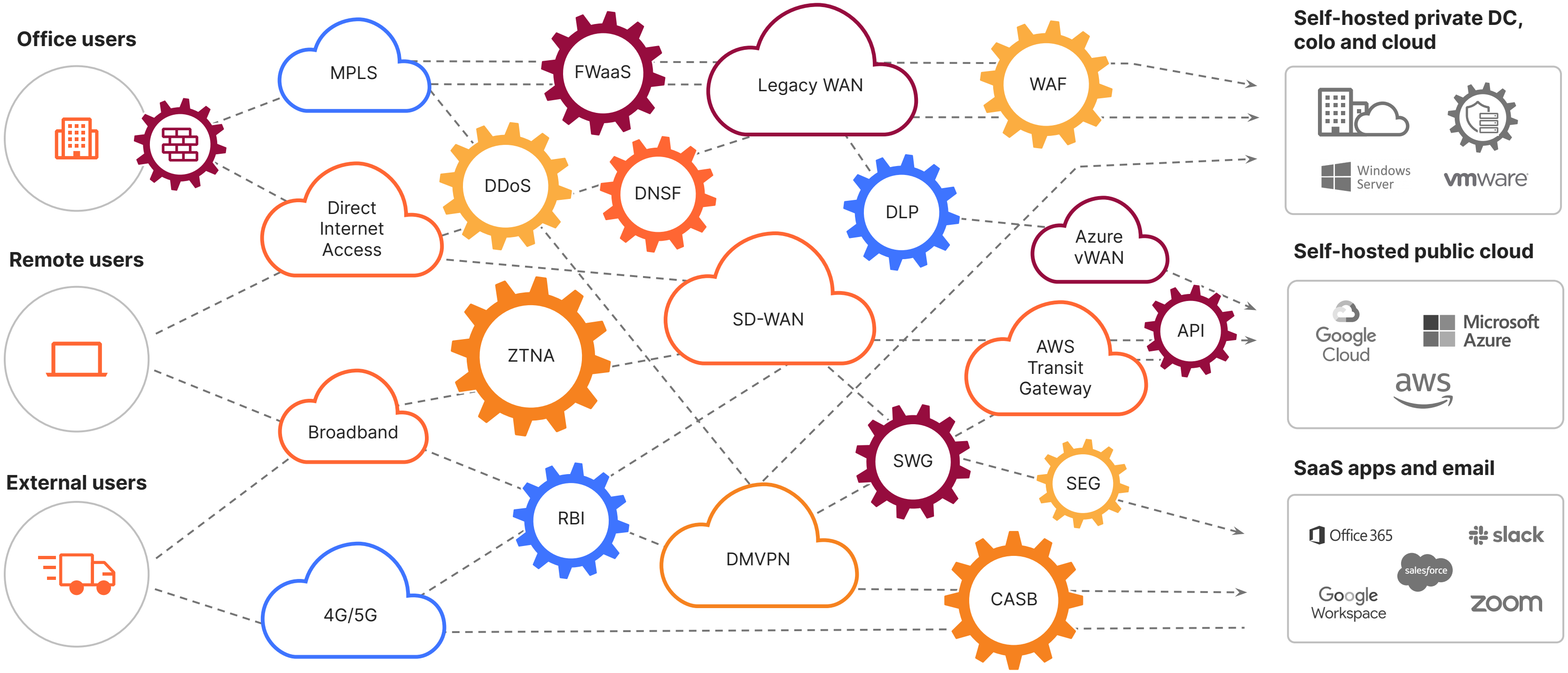
This is not the first Ivanti / Pulse Secure vulnerability

On April 20, 2021, it was reported that suspected Chinese-state backed hacker groups had breached multiple government agencies, defense companies and financial institutions in both the US and Europe after the hackers created and used a Zero-day exploit for Ivanti Pulse Connect Secure VPN devices

Zero Trust is a mindset shift

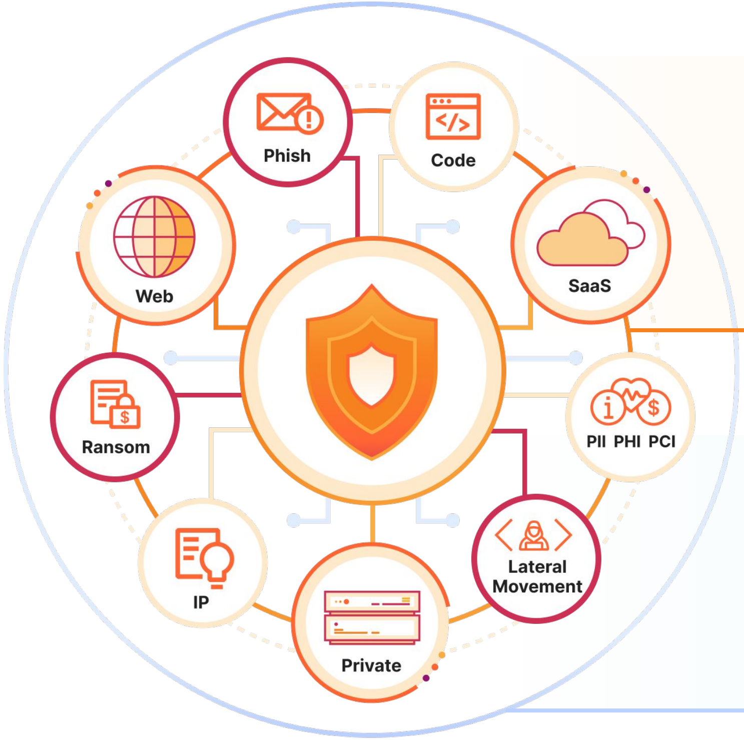
Perimeter determines trust		No perimeter, always verify
Secure perimeter, safe inside network (i.e. “castle & moat”)	Protection	Assume risk, reduce impact (encrypt, inspect, microsegment)
Log only login at the perimeter	Visibility	Log every login and request everywhere
Default allow, static access based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

Current network & security infrastructure
is not architected for your digital future



HOW IT WORKS

One composable, Internet-native platform



One unified platform

Secure access
by verifying and segmenting any user to any resource

Threat defense
by covering all channels with network-powered AI/ML & threat intel

Data protection
by increasing visibility and control of data in transit, at rest & in use

One programmable network

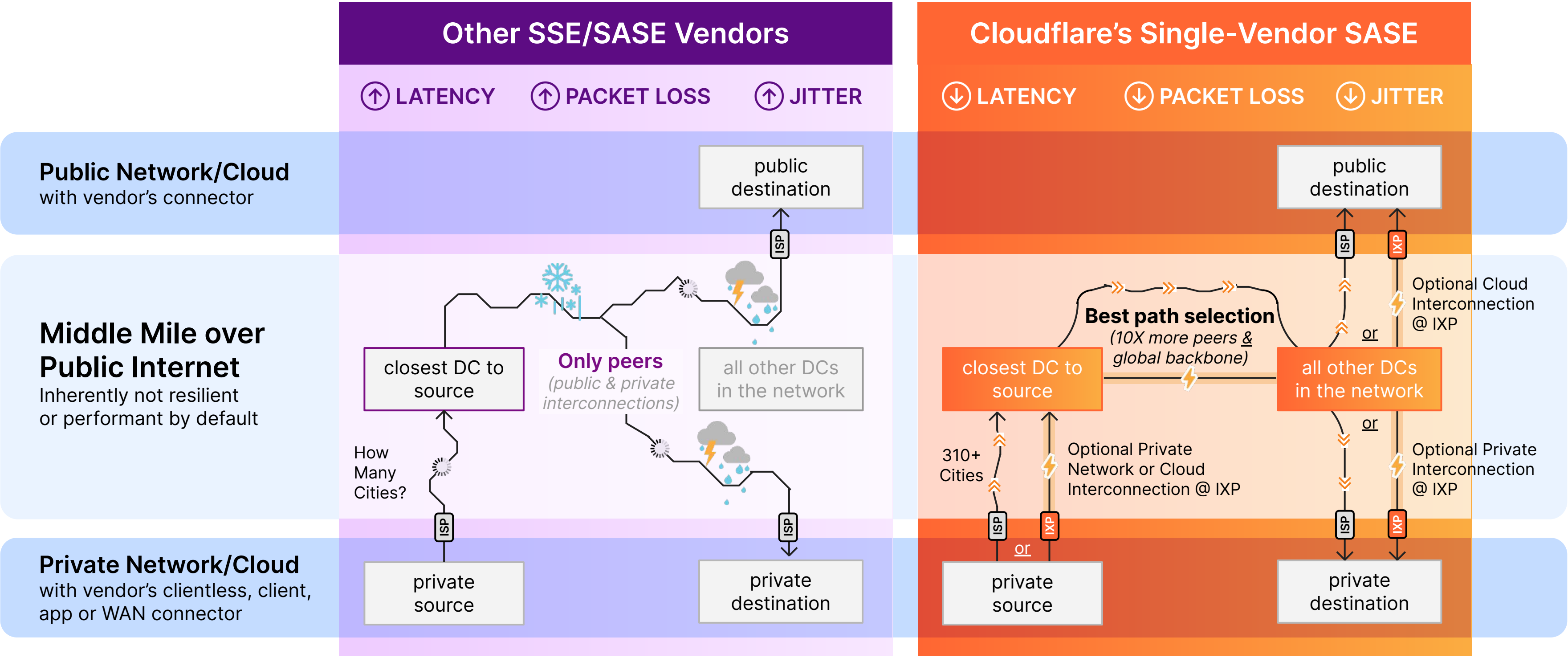
More effective
by simplifying connectivity and policy management

More productive
by ensuring fast, reliable, and consistent user experiences everywhere

More agile
by innovating rapidly to meet your evolving security requirements

Global backbone matters

for private + public traffic transport



Other SSE/SASE Vendors

↑ LATENCY ↑ PACKET LOSS ↑ JITTER

Cloudflare’s Single-Vendor SASE

↓ LATENCY ↓ PACKET LOSS ↓ JITTER

Public Network/Cloud
with vendor’s connector

Middle Mile over Public Internet
Inherently not resilient or performant by default

Private Network/Cloud
with vendor’s clientless, client, app or WAN connector

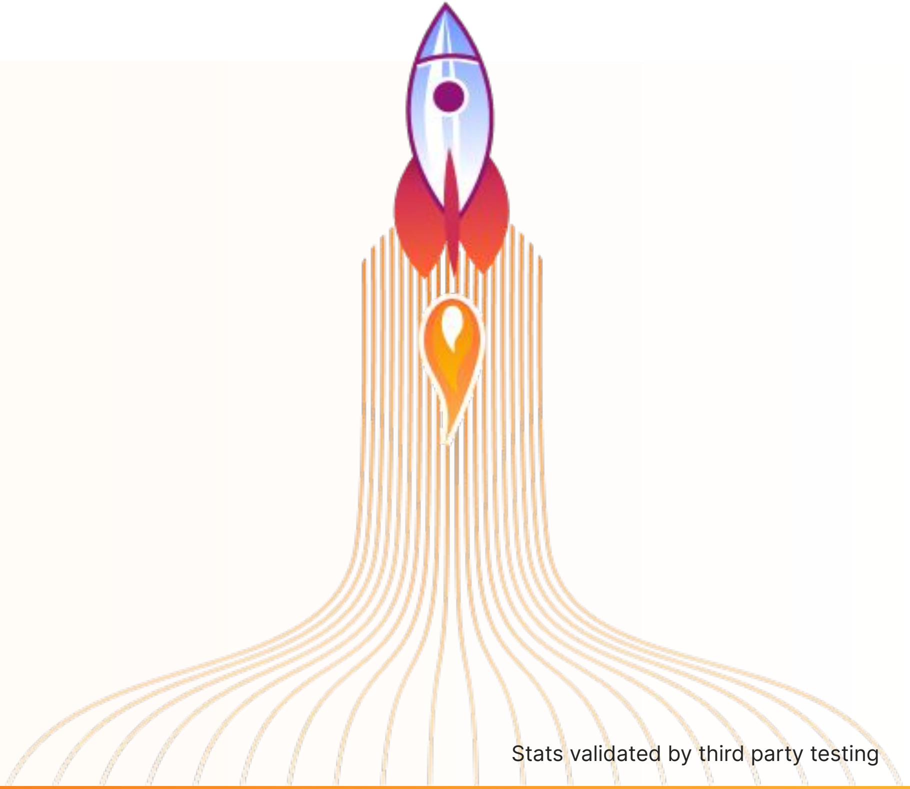
public destination
ISP
closest DC to source
Only peers
(public & private interconnections)
all other DCs in the network
How Many Cities?
ISP
ISP
private source
private destination
public destination
ISP
IXP
Optional Cloud Interconnection @ IXP
or
Best path selection
(10X more peers & global backbone)
closest DC to source
all other DCs in the network
or
310+ Cities
Optional Private Network or Cloud Interconnection @ IXP
Optional Private Interconnection @ IXP
ISP
IXP
or
ISP
IXP
private source
private destination

Cloudflare delivers better user experiences than Zscaler

58% faster for SWG

45% faster for RBI

38% faster for ZTNA



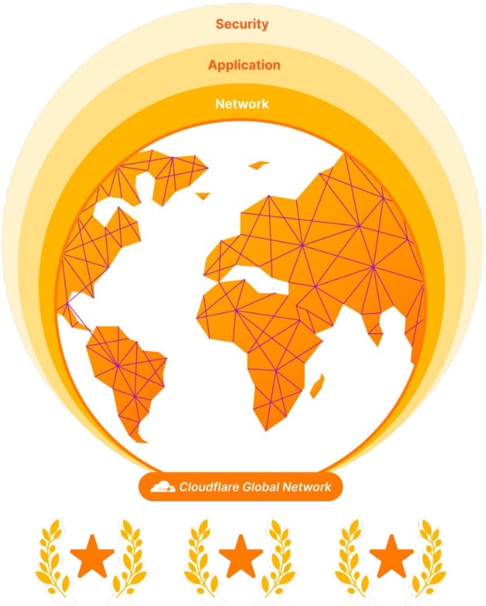
Stats validated by third party testing

ANALYST RECOGNITION

Cloudflare recognized over 60x by top 3 analyst firms

As a **global leader in network, application, and security solutions**, Cloudflare continues to innovate and deliver a cloud platform that transcends traditional boundaries – unifying diverse technologies to transform organizations and power the future of the Internet.

- NEW **LEADER - 2023 IDC MarketScape for ZTNA**
- NEW **LEADER - 2023 IDC MarketScape for NESaaS**
- NEW **LEADER - 2023 Forrester Wave for Email Security**
- **LEADER - 2022 Gartner MQ for WAAP**
- **LEADER - 2022 Forrester Wave for Web Application Firewalls**
- **LEADER - 2021 Forrester New Wave for Edge Development Platforms**



Gartner

Recognized in **30 reports**

FORRESTER

Recognized in **22 reports**

IDC

Recognized in **11 reports**

You’re in good company

whether you’re a digital native like us or traditional enterprise

Traditional enterprise outcomes

100K+
hybrid workers protected

Fortune 500 telecom secures Internet & app access with Zero Trust.

JAPAN AIRLINES

22K
Malicious emails

blocked over a 6-month period, mitigating phishing attacks.

50%
more cost effective

Fortune 500 oil & gas replaces Zscaler with Cloudflare for Zero Trust access.

100+
U.S. civilian agencies

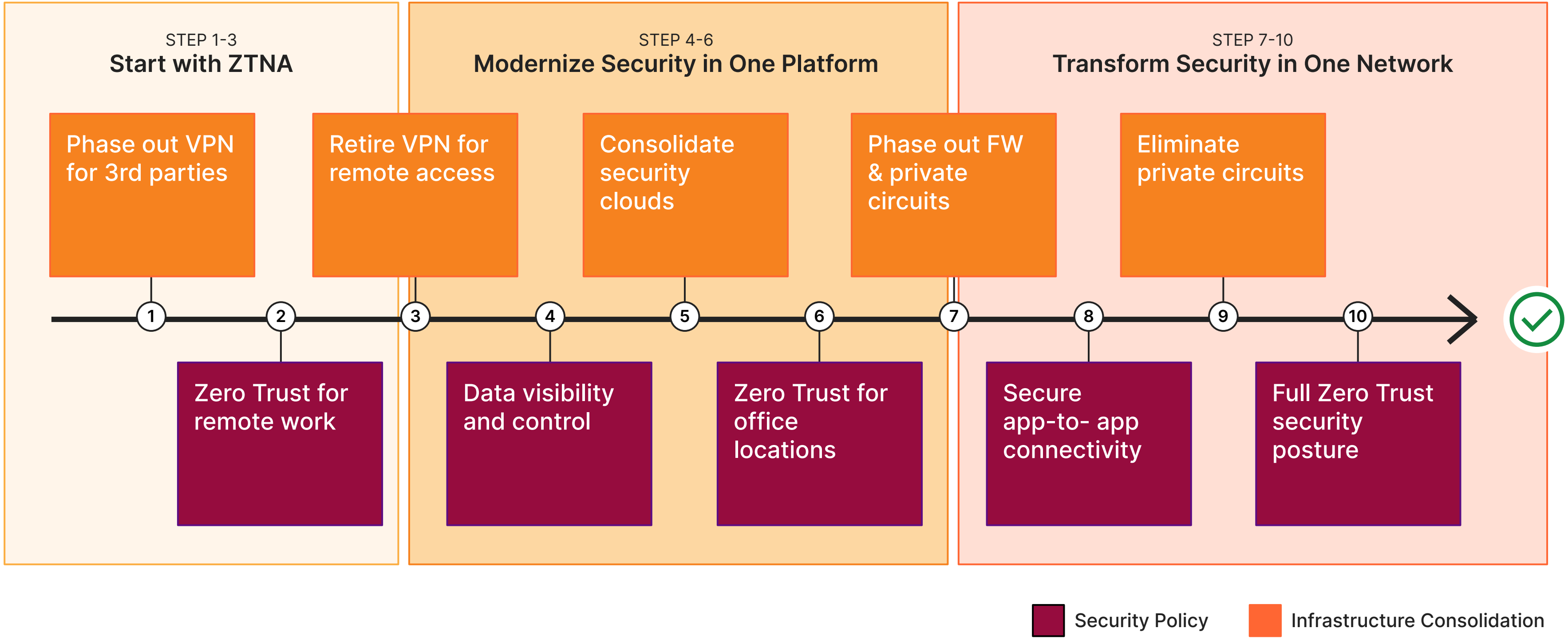
with office locations protected with Cloudflare’s DNS filtering.

Others on their SASE & SSE journey

APPLIED
WERNER ENTERPRISES
Delivery Hero
CONRAD
Sage
Investec
creditas
TEMPLE & WEBSTER
Swiss Re
TRUELAYER
L’ORÉAL
ezcater
INSEAD
BERKELEY LAB
Canva
jetBlue | travel products

PHASE

A common roadmap to Zero Trust
and single-vendor SASE consolidation



STEP 1-3
Start with ZTNA

STEP 4-6
Modernize Security in One Platform

STEP 7-10
Transform Security in One Network

1 Phase out VPN for 3rd parties

2 Zero Trust for remote work

3 Retire VPN for remote access

4 Data visibility and control

5 Consolidate security clouds

6 Zero Trust for office locations

7 Phase out FW & private circuits

8 Secure app-to- app connectivity

9 Eliminate private circuits

10 Full Zero Trust security posture

■ Security Policy
■ Infrastructure Consolidation

Roadmap to Zero Trust architecture

cfl.re/architecture-roadmap

Then, review our reference architecture whitepaper cfl.re/architecture-reference

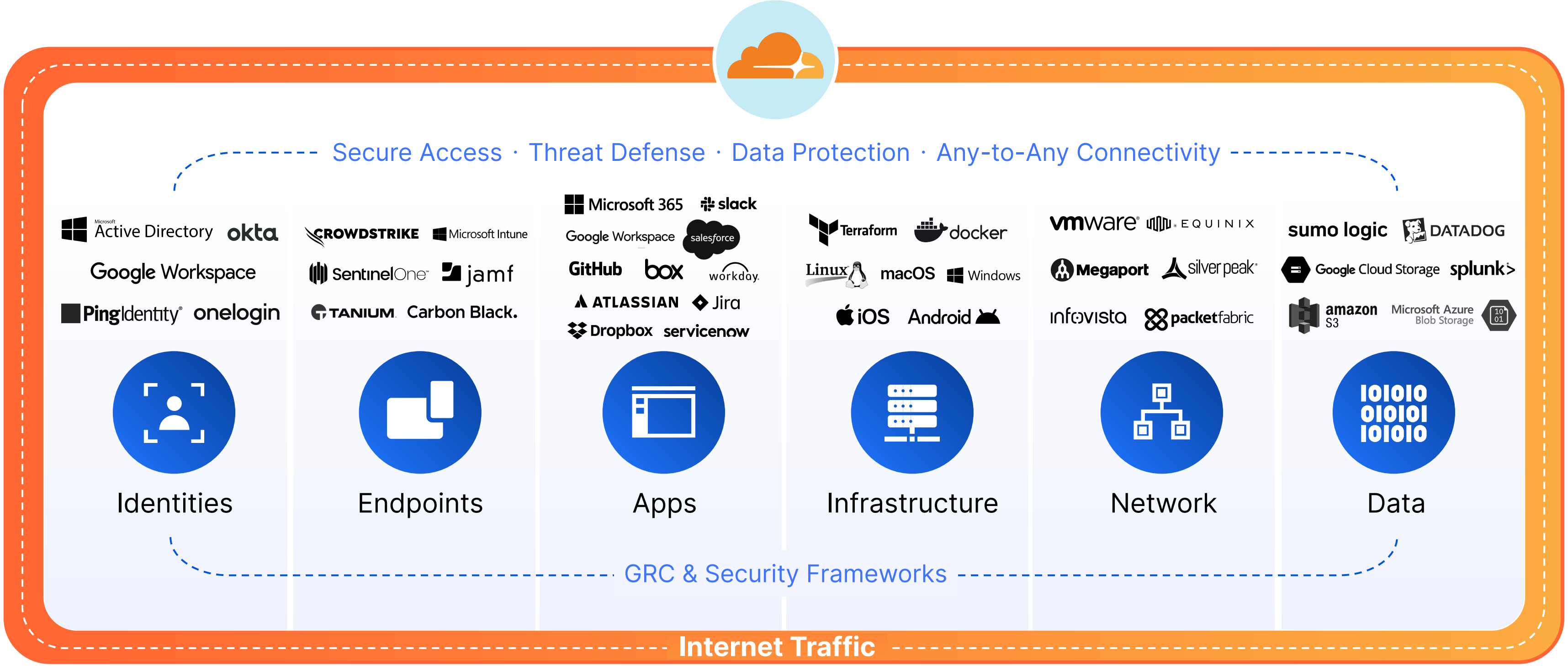
CLOUDFLARE

	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	▮▮▮

INTEGRATE

CLOUDFLARE

Adopt Zero Trust faster with one-time integrations



Secure Access · Threat Defense · Data Protection · Any-to-Any Connectivity

Microsoft Active Directory okta
Google Workspace
PingIdentity onelogin

Identities

CROWDSTRIKE Microsoft Intune
SentinelOne jamf
TANIUM Carbon Black.

Endpoints

Microsoft 365 slack
Google Workspace salesforce
GitHub box workday.
ATLASSIAN Jira
Dropbox servicenow

Apps

Terraform docker
Linux macOS Windows
iOS Android

Infrastructure

vmware EQUINIX
Megaport silver peak
infovista packetfabric

Network

sumo logic DATADOG
Google Cloud Storage splunk>
amazon S3 Microsoft Azure Blob Storage

Data

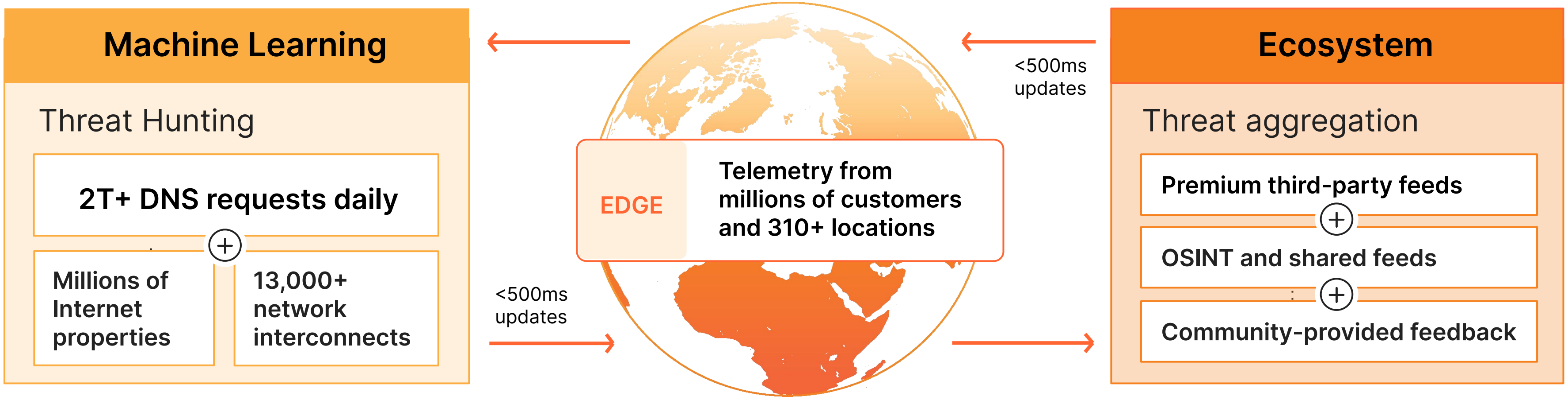
GRC & Security Frameworks

Internet Traffic

HOW IT WORKS

CLOUDFLARE

Cyber threat defense with Cloud*force* One



Machine Learning

Threat Hunting

2T+ DNS requests daily

+

Millions of Internet properties

13,000+ network interconnects

<500ms updates

EDGE

Telemetry from millions of customers and 310+ locations

<500ms updates

Ecosystem

Threat aggregation

Premium third-party feeds

+

OSINT and shared feeds

+

Community-provided feedback

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

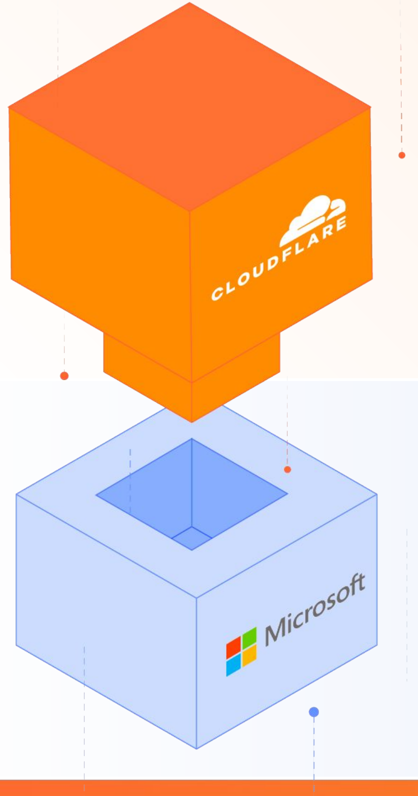
Malware	Newly seen domains	DGA domains	Spyware
Phishing	New domains	DNS tunneling	Spam
Cryptomining	Unreachable domains	C2 & botnet	Anonymizer

Cloudflare Services Mapped to MITRE ATT&CK Framework (using Gartner market terminology)

Cloudflare Services	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
ZTNA	Stop Internet Scans of Private Apps		Secure Remote Service Access Verify Trusted Relationships	Require EPP to Access Remote Services	Least- Privilege for Remote Service & Valid Accounts Stop Auth Process Mods	Stop Access Token Manipulation	Stop Auth Process Mods	Stop Unsecured Credentials, Brute Force, & MFA Interception	Limit Remote System Network Service Container/Resource Discovery	Enforce Principles of Least-Privilege Secure SSH & RDP Access	Encrypt Connections to Stop Adversary in the Middle		Least-Privilege to Stop Data Transfer to Cloud Account	
SWG	Stop Phishing for Info	Gather Infrastructure Intel	Stop Drive-By Malware, Phishing & Supply Chain				Stop Obfuscated Files or Info		Monitor File Access to Private Apps		Filter Network Traffic to Stop Adversary in the Middle	Stop Dynamic Resolution, Encrypted Channel, Protocol Tunneling	Stop Protocol Tunneling & Automated Exfiltration, & C2 Channels	Stop Resource Hijacking
CASB			Monitor Valid Accounts and Trusted Relationships		Identify Compromised Valid Accounts	Detect Valid Accounts Being Accessed		Monitor MFA Status & If App Access Token Stolen	Monitor for Indicators of Cloud Service Discovery				Manage Posture to Stop Data Transfer to Cloud Account	
RBI & DLP			Stop Drive-By Malware & Phishing	Stop Exploit of Client Execution & User Execution	Remove Browser Extensions					Stop Exploitation of Remote Services	Stop Keyboard Input Capture Stop Data Leaks from Local System		Stop Exfiltration over Web Service	
CES & Email Routing	Stop Phishing for Info	Stop Compromise Accounts	Stop Phishing							Stop Internal Spear-phishing	Audit Email Forwarding Rules to Stop Email Collection		Stop Exfiltration over Alternative Protocol (SMTP)	
L3 DDoS, WANaaS & FWaaS		Stop Compromised Infrastructure						Stop Network Sniffing	Stop Network Sniffing		Filter Network Traffic to Stop Adversary in the Middle	Stop Fallback Channel & Data Obfuscation via IPS & Network Flow Monitors	Stop Protocol Tunneling & C2 Channels	Stop Network-Layer DDoS
L7 WAAP Services	Stop Active Scanning Stop Scraping Victim Host Info	Reduce Risk of Look-alike Sites	Stop Exploiting Public Apps Stop Supply Chain Compromise	Stop Command & Script Interpreter	Stop Traffic Signaling		Stop Traffic Signaling	Stop Brute Force Credential Stuffing		Stop Exploitation of Remote Services				Stop Application -Layer DDoS
Threat Research Systems		Identify Compromised Infrastructure	Threat Intel and ML Models on Malware and Phishing							Threat Intel on Vulnerabilities		ML Models to Predict Dynamic Resolution	Threat Intel on C2 Channels and Protocol Tunneling	

HOW IT WORKS

Cyber threat defense together with Microsoft



Email Security

Preemptive Threat Defense
(URLs, Payloads, BECs, Spoofs)

Multichannel Protection
(Adaptive Link Isolation)

BEC Detection (Type 1/2/3/4)
(Vendor Compromise, Account Compromise)

Fast & Flexible Deployment
(Inline, API, Journaling, Multi-Mode)

Email Provider

Email Hygiene
(Anti-Virus, Anti-Spam)

Sender Authentication
(DMARC, DKIM, SPF)

Data Protection & Encryption
(Email & Message Encryption, DLP)

Data Management
(Data Controls, Archiving, Compliance)

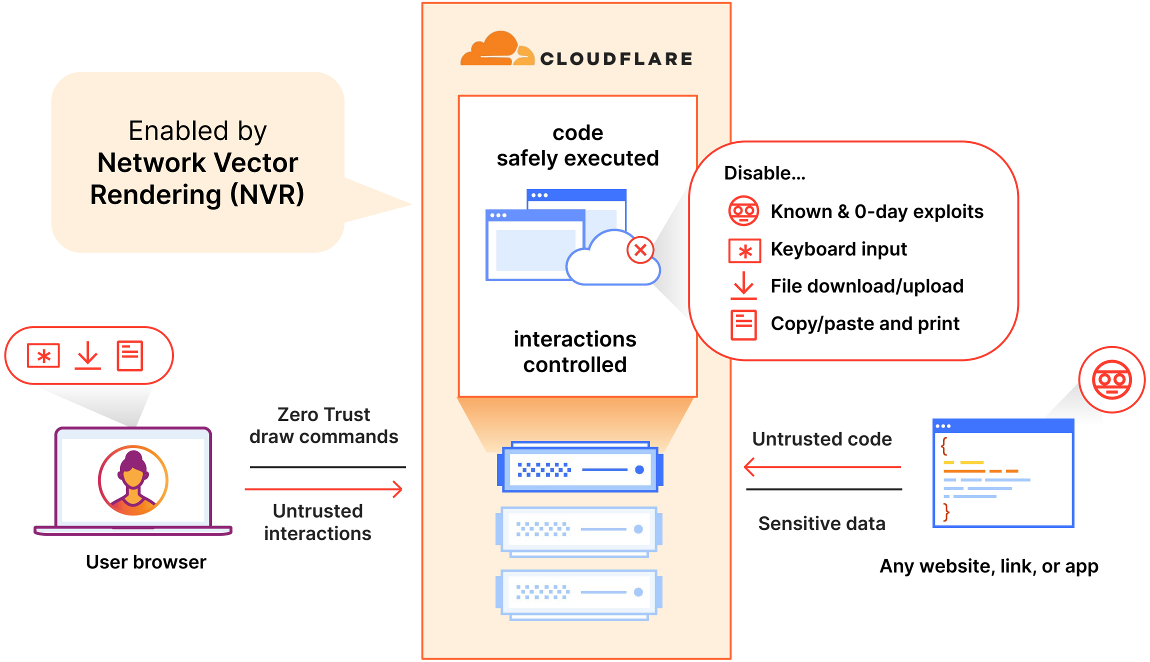
Cloud Email Security w/ Link Isolation

Block targeted phishing emails and campaigns

Isolate malicious links and multichannel attacks

Stop BEC and expose malware-less fraud

Remote Browser Isolation - for Internet and internal apps



Zero trust web browsing and email links

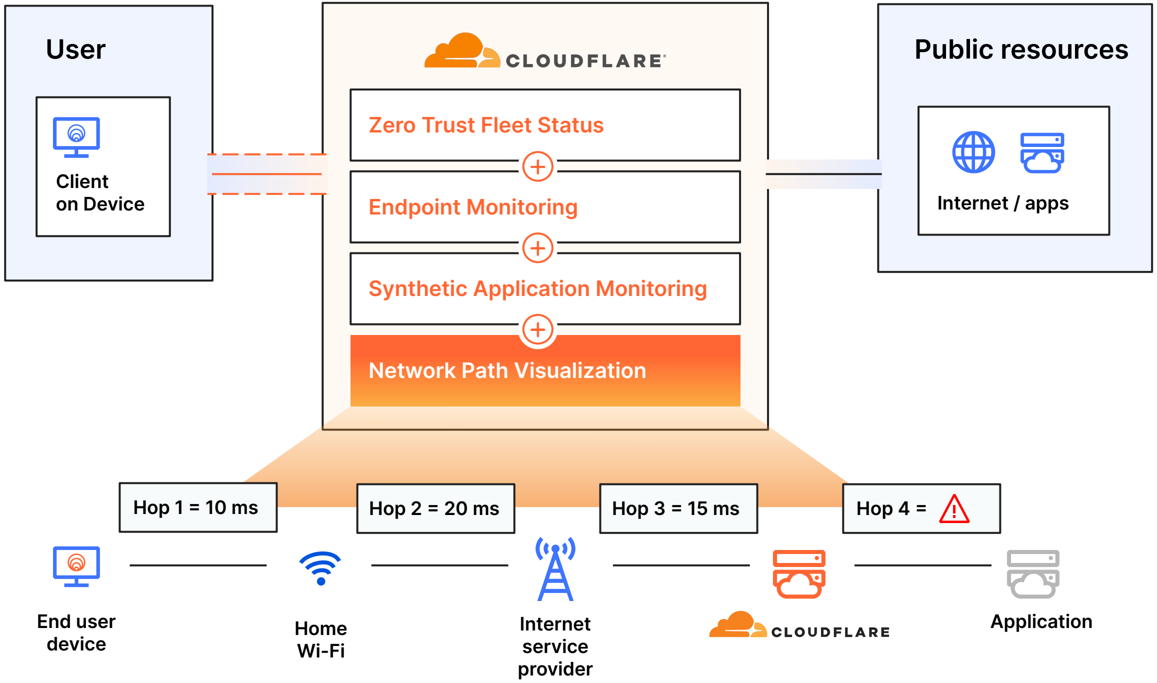
Protect data-in-use

Lightning-fast UX

Compatibility w/all browsers

HOW IT WORKS

Simple, secure access with performance monitoring



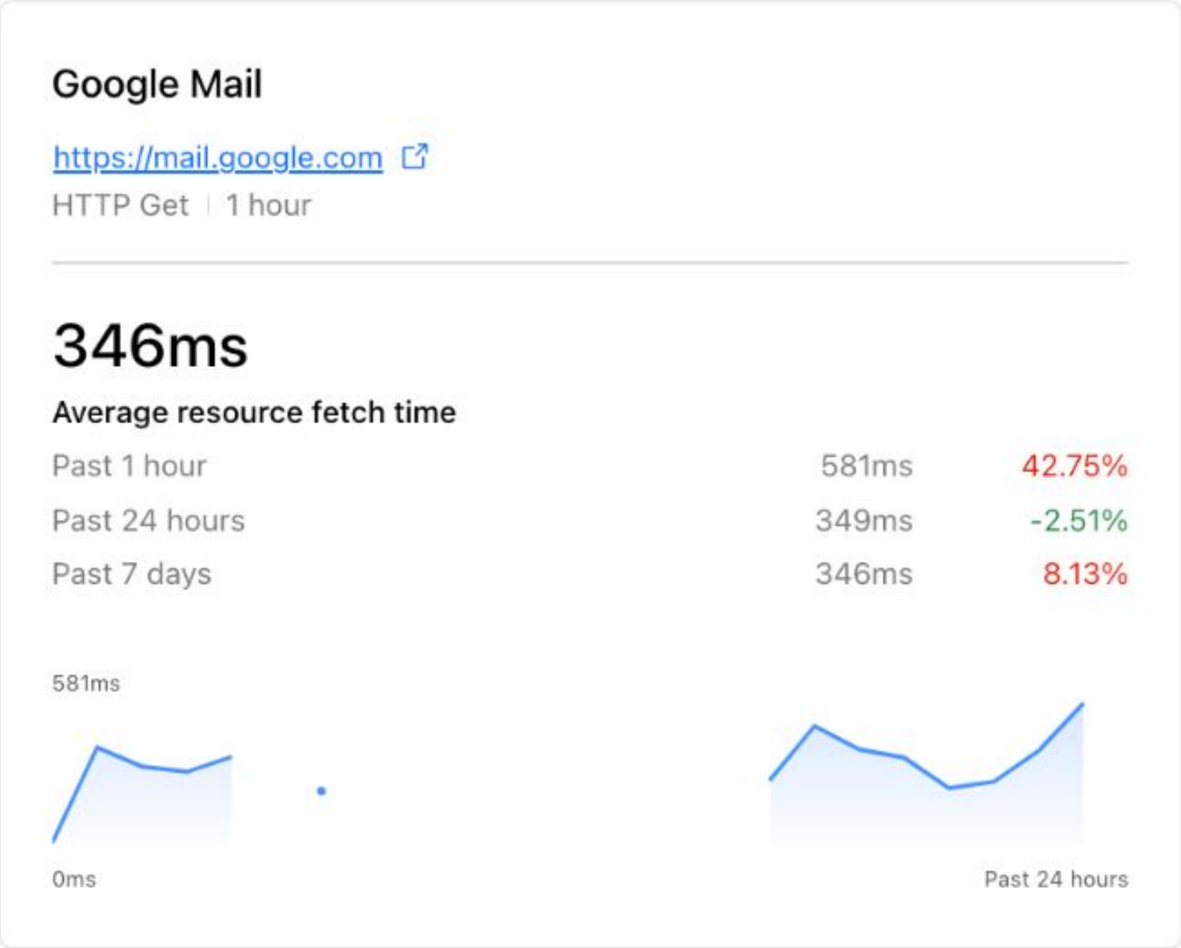
Digital Experience Monitoring

Troubleshoot connectivity issues faster

Get ahead of problems before they occur

Visualize end-user experiences

Understand performance and availability metrics



Google Mail

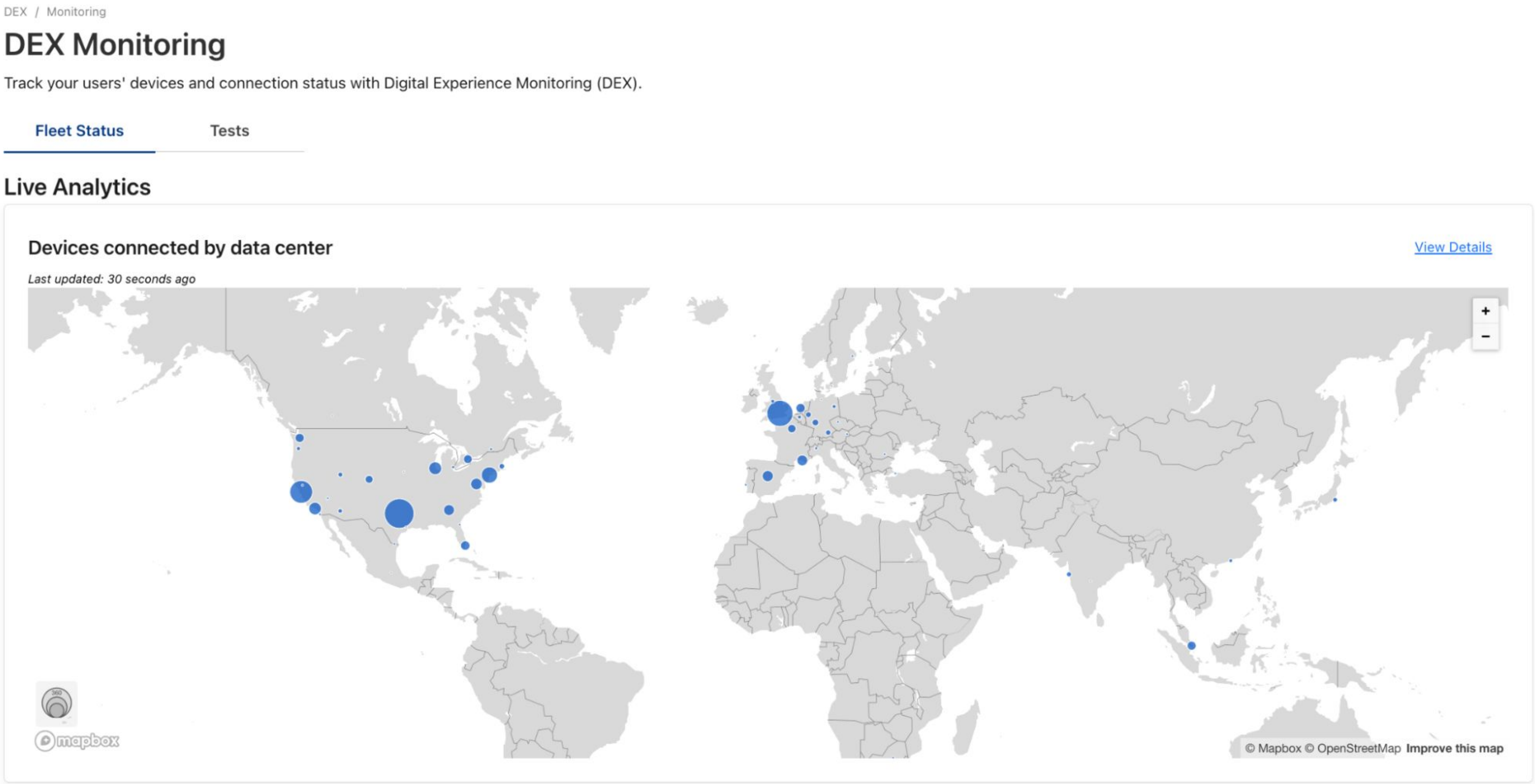
https://mail.google.com

HTTP Get | 1 hour

346ms

Average resource fetch time

Past 1 hour	581ms	42.75%
Past 24 hours	349ms	-2.51%
Past 7 days	346ms	8.13%



DEX / Monitoring

DEX Monitoring

Track your users' devices and connection status with Digital Experience Monitoring (DEX).

Fleet Status

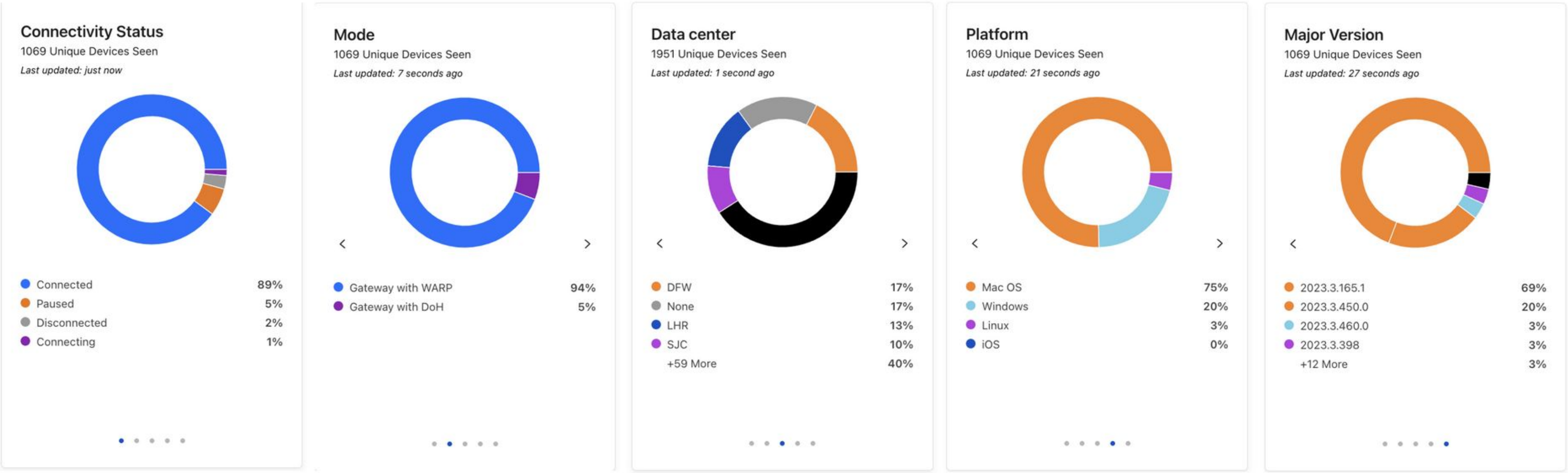
Tests

Live Analytics

Devices connected by data center

View Details

Last updated: 30 seconds ago



Connectivity Status

1069 Unique Devices Seen

Last updated: just now

● Connected	89%
● Paused	5%
● Disconnected	2%
● Connecting	1%

Mode

1069 Unique Devices Seen

Last updated: 7 seconds ago

● Gateway with WARP	94%
● Gateway with DoH	5%

Data center

1951 Unique Devices Seen

Last updated: 1 second ago

● DFW	17%
● None	17%
● LHR	13%
● SJC	10%
+59 More	40%

Platform

1069 Unique Devices Seen

Last updated: 21 seconds ago

● Mac OS	75%
● Windows	20%
● Linux	3%
● iOS	0%

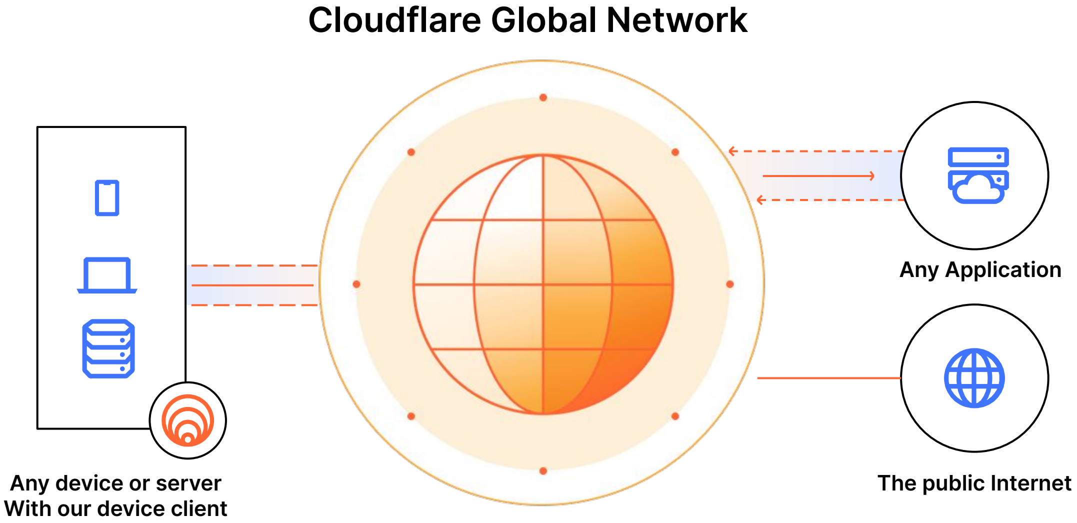
Major Version

1069 Unique Devices Seen

Last updated: 27 seconds ago

● 2023.3.165.1	69%
● 2023.3.450.0	20%
● 2023.3.460.0	3%
● 2023.3.398	3%
+12 More	3%

Device posture and VPN agent



Auto-connects

via Anycast to the nearest of 310+ cities

Mobile-friendly

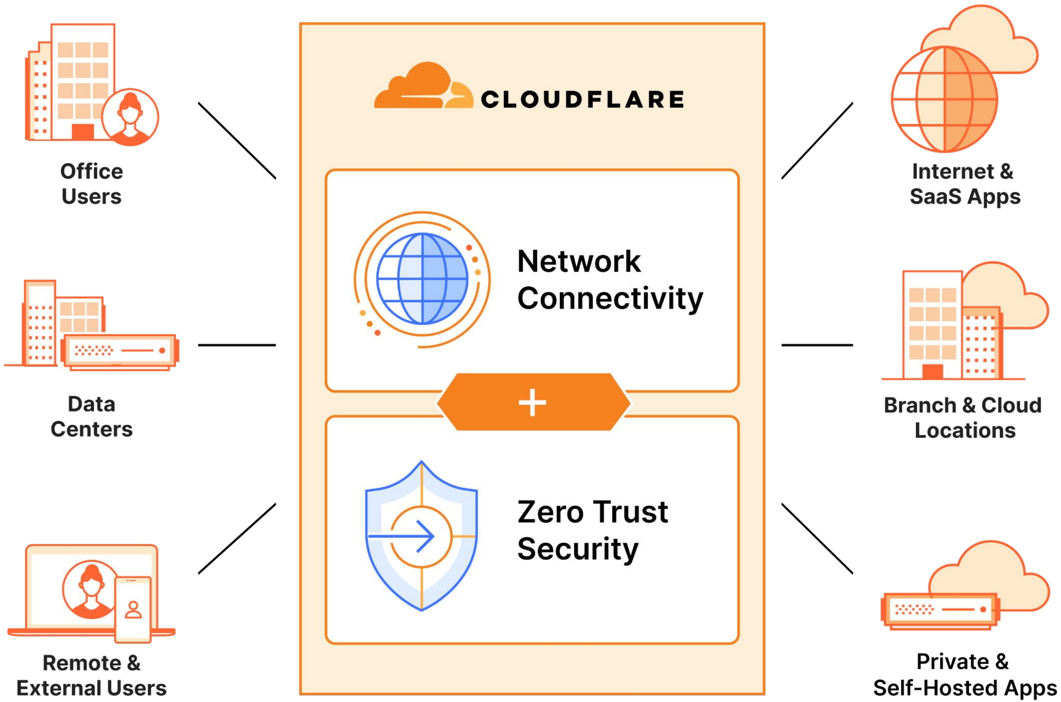
userspace Wireguard implementation to route and proxy L4-7 traffic

MDM or self-enrollment

for Win, Mac, Linux, iOS, ChromeOS and Android

HOW IT WORKS

WAN and Firewall as a service



Better operational agility; zero-touch configuration

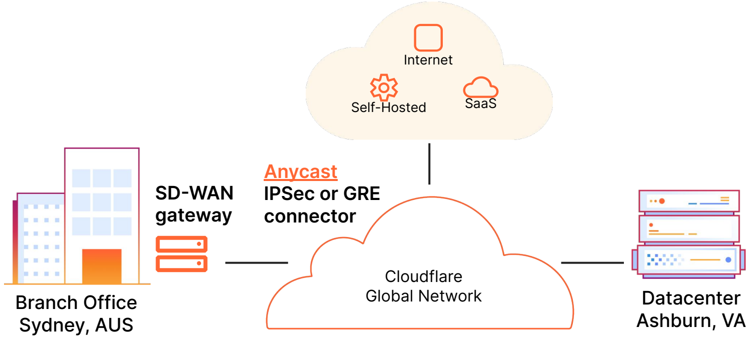
Built-in, not bolt-on, security; converged with SSE platform

Reduced network costs; augment or replace MPLS or SD-WAN deployments

Flexible on-ramps to support existing infrastructure

SD-WAN Partnerships

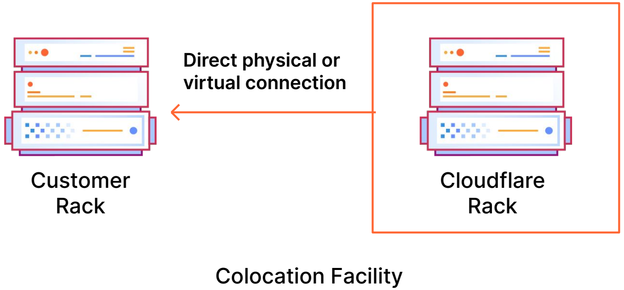
- **Improved Performance**: take advantage of the Cloudflare Global Network, reduce latency and improve reliability
- **Built-in Security**: Single-pass security functions at every location on the Cloudflare network
- **Open architecture**: connect using standards-based IPSec or GRE tunnels



vmware aruba ARISTA

Interconnect Anywhere *(1600+ locations)*

- **Increased Reliability**: eliminate best-effort Internet hops between customers’ networks and Cloudflare
- **Improved Performance**: reduced latency and dedicated bandwidth between Cloudflare and customer networks
- **Faster Provisioning**: software-defined virtual connections speed up provisioning times



consoleconnect by PCCW Global
EQUINIX
PACKETFABRIC
Megaport
CORESITE
epsilon

Magic WAN Connector

Lightweight software that makes it easy to route traffic to Cloudflare

- Cloudflare software
- Partner hardware
    - Dell box, fulfilled through TD SYNNEX

Purchase it pre-installed and configured on a Cloudflare certified **hardware appliance** for the lowest-friction path to SASE connectivity.

OR

Install the software on physical or virtual Linux appliances that you already manage.

Email Security

Preemptive

Early Discovery
Campaign Hunting
Actor Infrastructure
Monitoring

Comprehensive

Multi-Variety Attacks
Multi-Channel Attacks
Multi-Vector Attacks

Continuous

Pre-Delivery
At-Delivery
Post-Delivery

Accountable

SLAs
Privacy
Biz Model

Contextual

Natural Language
Understanding
Sentiment Analysis
Intent, Tone & Relationships

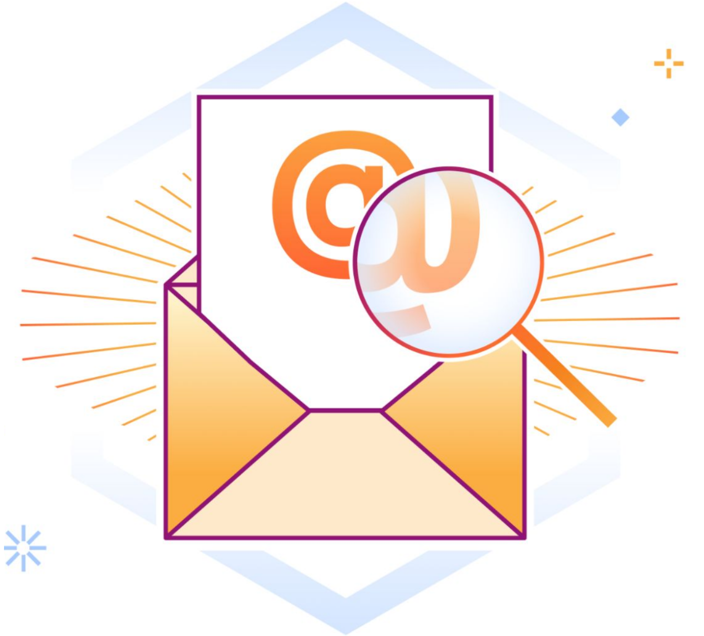
No-cost, no-obligation tool

CLOUDFLARE

Phishing retro scan and free assessment

What: Look back 14 days and see:

- what threats your current email security tool ***missed***
- & what Cloudflare ***would have caught*** with our threat hunting models.



How: In any Cloudflare account, including our free plan, open the tab labeled 'Area 1'

Cloudflare One for data protection

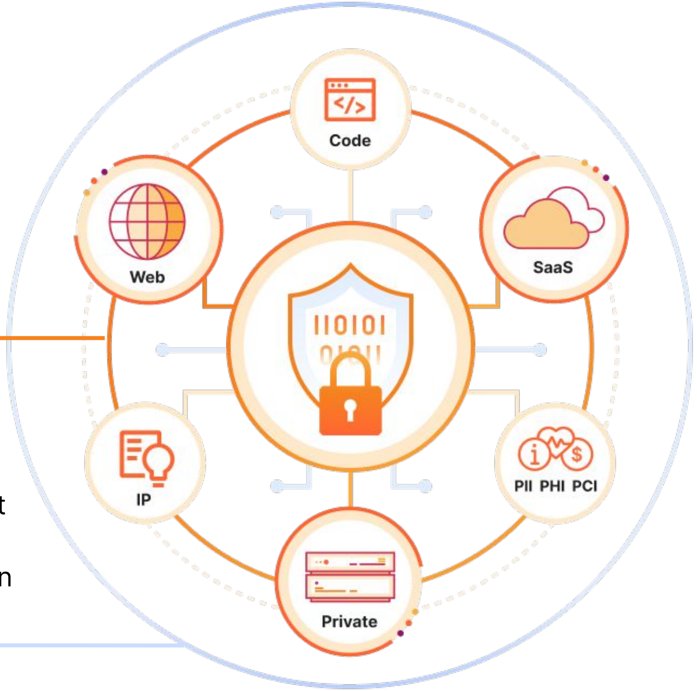
More effective, productive, and agile approach

One unified platform

Converged visibility and controls across DLP, CASB, ZTNA, SWG, RBI, and email security across web, SaaS, and private apps.

One programmable network

One control plane with services built on our own developer platform to enforce controls for data in transit, in use, and at rest.



Protect data everywhere

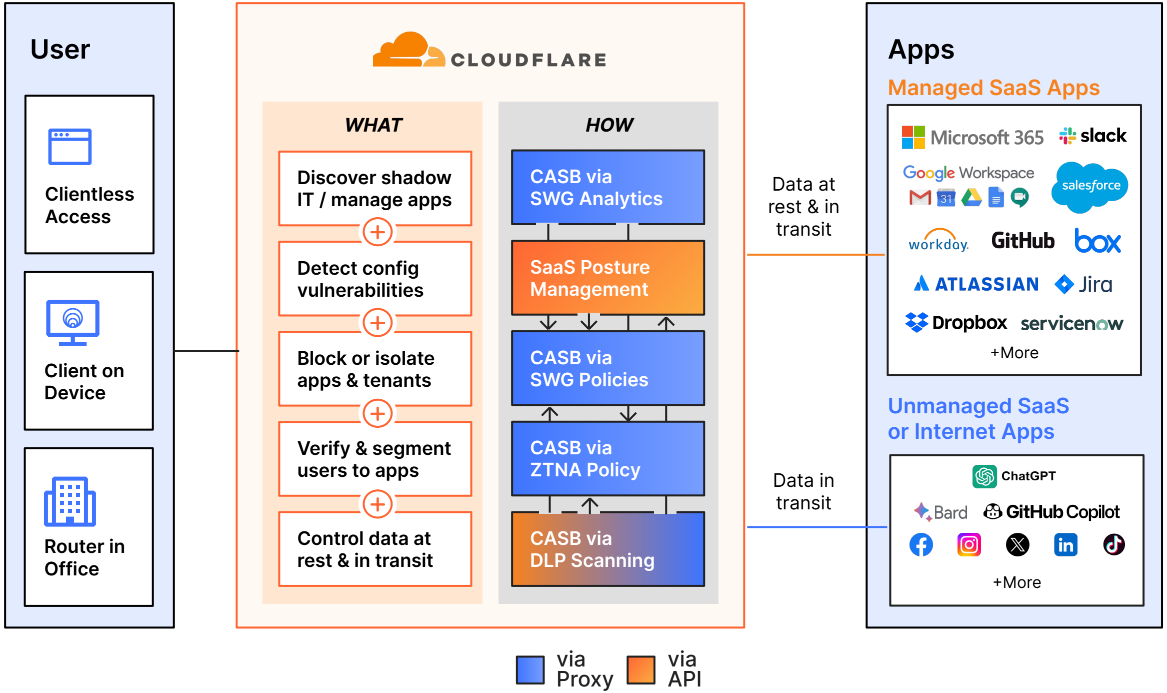
Comply with regulations

Data exposure visibility

Secure developer code

HOW IT WORKS

Data protection



Cloud Access Security Broker (multimode)

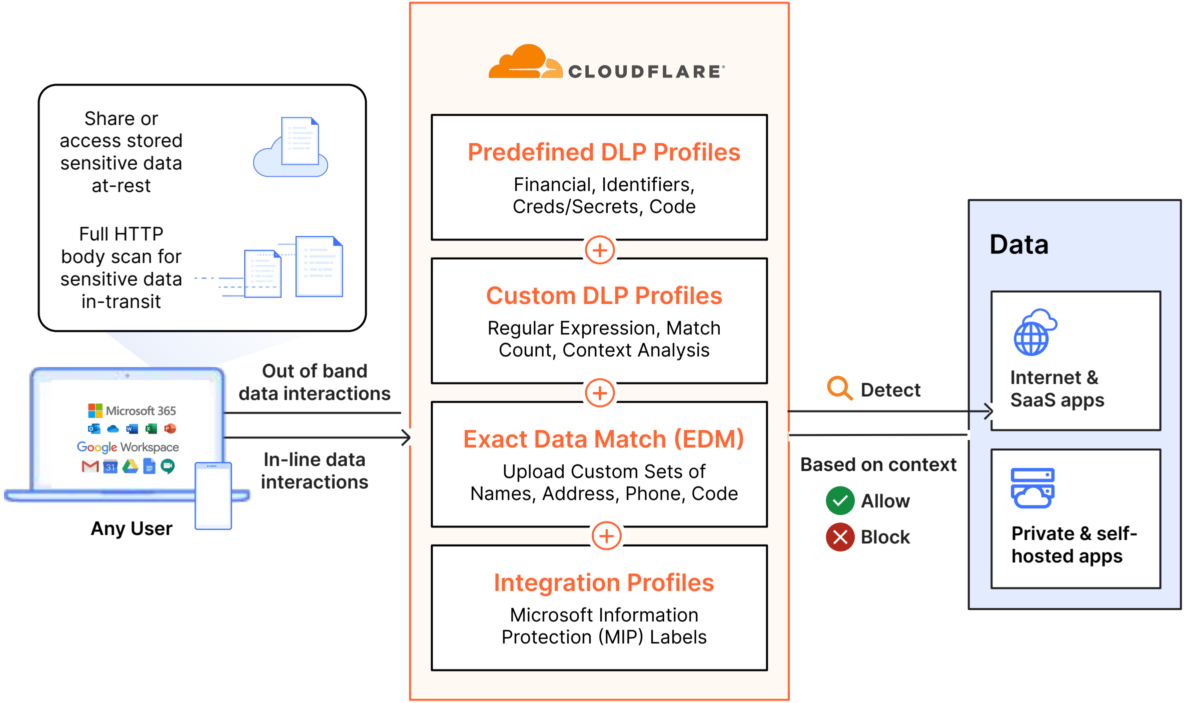
More visibility, less config

Prevent data exfiltration

Quickly identify new risks

HOW IT WORKS

Data protection


Share or access stored sensitive data at-rest
Full HTTP body scan for sensitive data in-transit
Microsoft 365
Google Workspace
Any User
Out of band data interactions
In-line data interactions
CLOUDFLARE
Predefined DLP Profiles
Financial, Identifiers, Creds/Secrets, Code
Custom DLP Profiles
Regular Expression, Match Count, Context Analysis
Exact Data Match (EDM)
Upload Custom Sets of Names, Address, Phone, Code
Integration Profiles
Microsoft Information Protection (MIP) Labels
Detect
Based on context
Allow
Block
Data
Internet & SaaS apps
Private & self-hosted apps

Integrated Data Loss Prevention

Simplify regulatory compliance

Reduce risk of data leakage and breaches

Increase in-line visibility across data, users, and apps

Do you have enough visibility across your SaaS stack?

Business suite

Would you know when internal files and folders are shared publicly to anyone with a link?

Google Workspace Microsoft 365 box

Chat apps

Would you see when individuals from outside your organization are added to a private channel?

slack

CRMs

Would you know if a departing Sales employee exported every sales record on their last day?

salesforce HubSpot

Version control

Would you get alerted if developer switched off Branch Protection to avoid PR review requirements?

GitHub GitLab

Identity providers

Would you find out if an employee disabled the minimum password strength requirement for your org?

okta

Video conferencing

Would you know if an employee disabled meeting passwords for all new meetings?

zoom

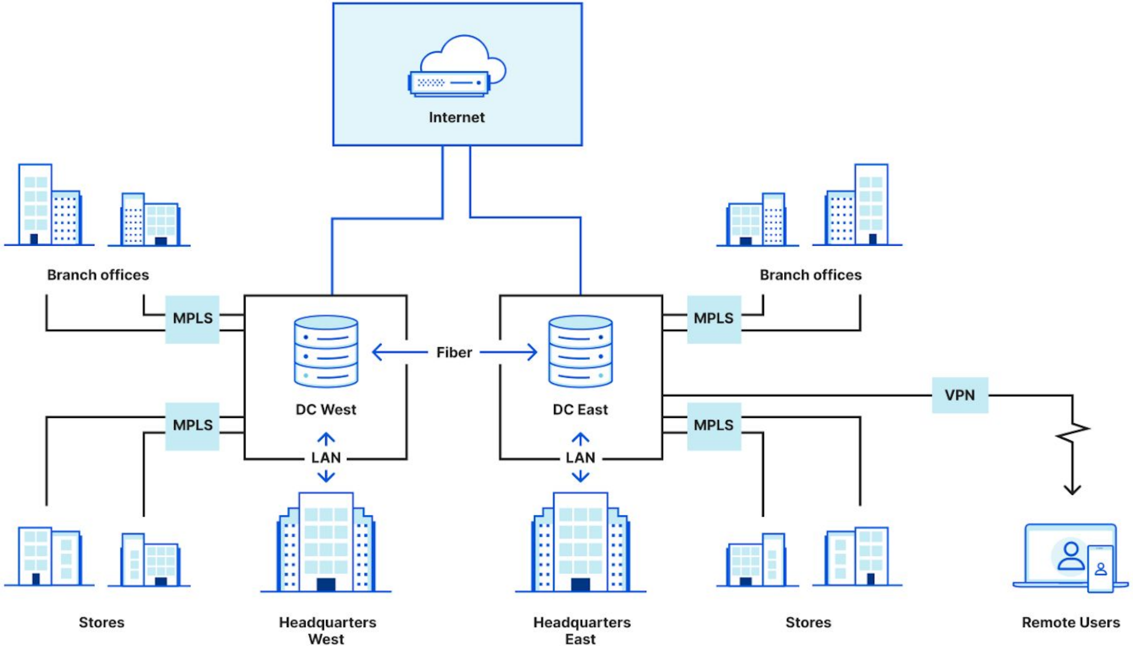
DEMO TIME!

CLOUDFLARE

AČIŪ LABAI
m@cloudflare.com

MISC / BACKUP

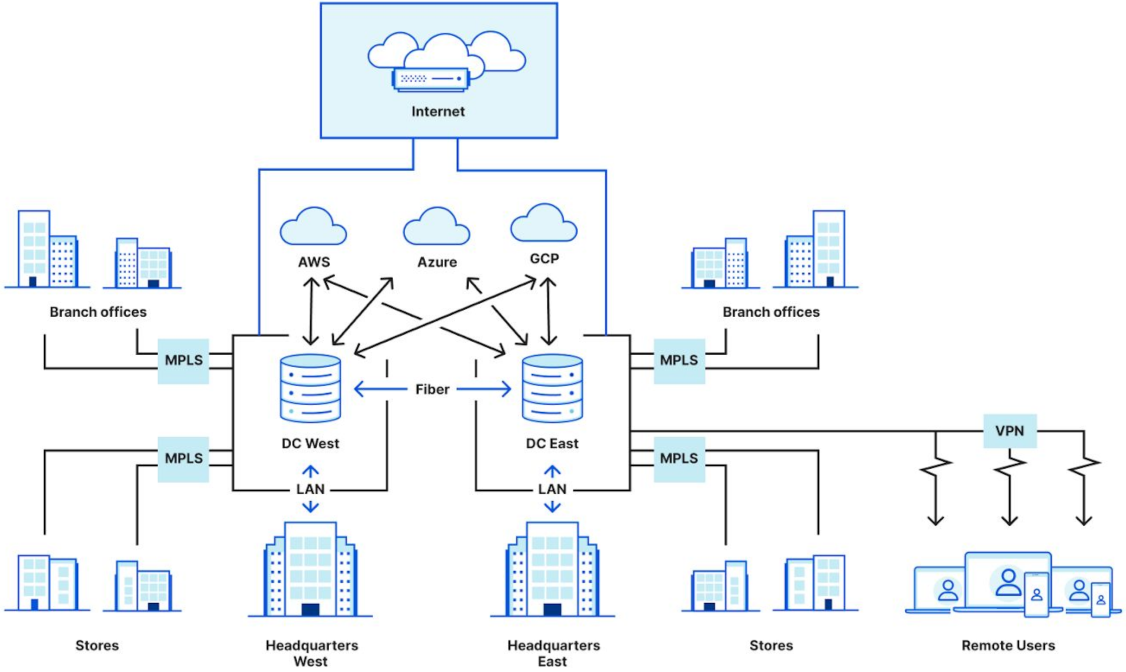
Traditional perimeter-based architecture



Attribute	Score	Description
Security	★★	All traffic flows through perimeter security hardware. Network access restricted with physical controls. Lateral movement is only possible once on network.
Performance	★★★	Majority of users and apps stay within the same building or regional network.
Reliability	★★	Dedicated DCs, private links, and security hardware present single points of failure. There are cost tradeoffs to purchase redundant links and hardware.
Agility	★	Significant network changes have a long lead time.
Visibility	★★★	All traffic is routed through central location, so it's possible to access NetFlow/packet captures and more for 100% of flows.
Policy	★	Controls are primarily exercised at the network layer (e.g., IP ACLs). Accomplishing "allow only HR to access employee payment data" looks like: IP in range X allowed to access IP in range Y (and requires accompanying spreadsheet to track IP allocation).
Cost	★★	Private connectivity and hardware are high cost capital expenditures, creating a high barrier to entry for small or new businesses. However, a limited number of links/boxes are required (trade off with redundancy/reliability). Operational costs are low to medium after initial installation.

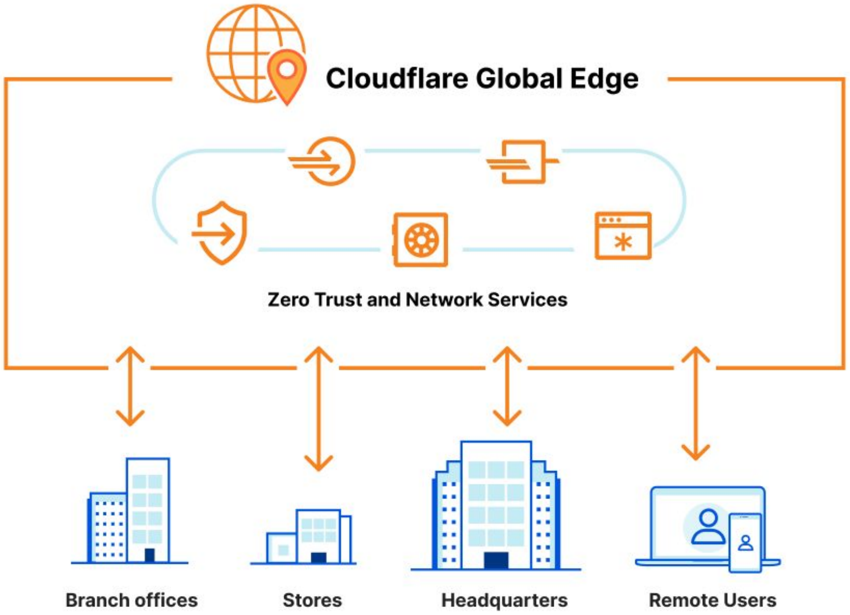
Scorecards

Hybrid overlay (SD-WAN w/bolt-on security)



Attribute	Score	Description
Security	★	Many traffic flows are routed outside of perimeter security hardware, Shadow IT is rampant, and controls that do exist are enforced inconsistently and across a hodgepodge of tools.
Performance	★	Traffic backhauled through central locations introduces latency as users move further away; VPNs and a bevy of security tools introduce processing overhead and additional network hops.
Reliability	★★	The redundancy/cost tradeoff from Generation 1 is still present; partial cloud adoption grants some additional resiliency but growing use of unreliable Internet introduces new challenges.
Agility	★★	Some changes are easier to make for aspects of business migrated to cloud; others have grown more painful as additional tools introduce complexity.
Visibility	★	Traffic flows and visibility are fragmented; IT stitches partial picture together across multiple tools.
Policy	★★	Mix of controls exercised at network layer and application layer. Accomplishing “allow only HR to access employee payment data” looks like: Users in group X allowed to access IP in range Y (and accompanying spreadsheet to track IP allocation)
Cost	★	Costs from Generation 1 architecture are retained (few companies have successfully deprecated MPLS/security hardware so far), but new costs of additional tools added, and operational overhead is growing.

SASE – built-in security by default



Attribute	Score	Description
Security	★★★	Granular security controls are exercised on every traffic flow; attacks are blocked close to their source; technologies like Browser Isolation keep malicious code entirely off of user devices.
Performance	★★★	Security controls are enforced at location closest to each user; intelligent routing decisions ensure optimal performance for all types of traffic.
Reliability	★★★	The platform leverages redundant infrastructure to ensure 100% availability; no one device is responsible for holding policy and no one link is responsible for carrying all critical traffic.
Agility	★★★	Making changes to network configuration or policy is as simple as pushing buttons in a dashboard; changes propagate globally within seconds.
Visibility	★★★	Data from across the edge is aggregated, processed and presented along with insights and controls to act on it.
Policy	★★★	Controls are exercised at the user and application layer. Accomplishing “allow only HR to access employee payment data” looks like: Users in HR on trusted devices allowed to access employee payment data
Cost	★★	Total cost of ownership is reduced by consolidating functions.

Agenda

1 Why change?

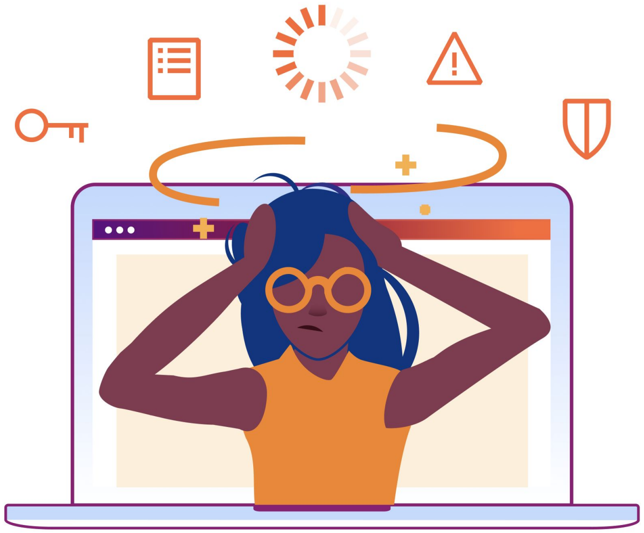
2 Where to start and how to get there fast?

3 How it works

4 Why get started now

MODERN CHALLENGES

Rising complexity, risks, and costs hold back business growth



Cybersecurity risks are escalating

- Attack surfaces expanding
- Data volume exploding

Info architectures are too complex

- Inflexible & disjointed point solutions
- Limited visibility and controls

Harder to stay efficient

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

C-LEVEL PRIORITIES

Accelerate digital transformation
with simple, secure access

CISOs enforce security everywhere

- Protect expanding attack surface
- Safeguard data and stay compliant

CIOs simplify IT architectures

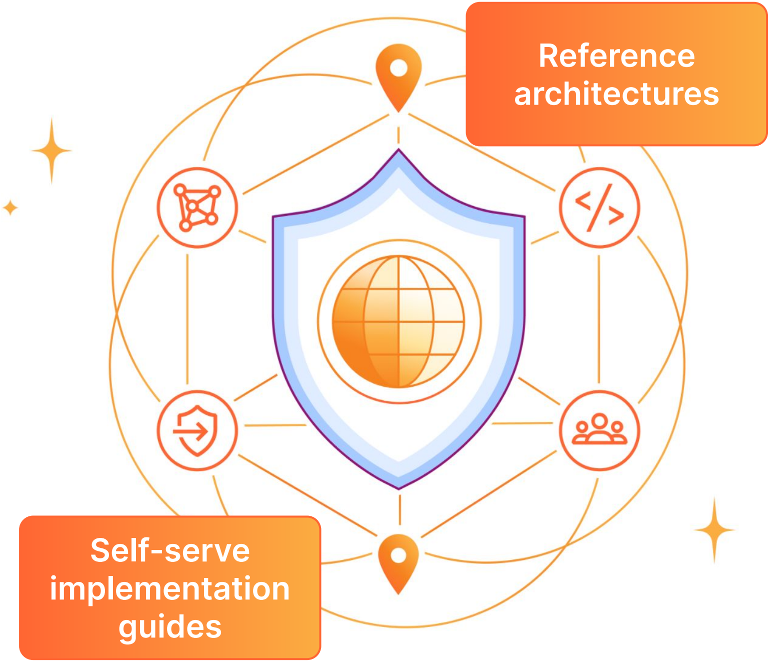
- Consolidate vendors and tools
- Modernize networks

CFOs & CTOs scale efficiently

- Lower total cost of ownership
- Innovate without sacrifices

REDUCED COMPLEXITY

Faster time to set up any-to-any connectivity
with flexible on-ramps for any team



IT & security teams

- Protect all user-to-app flows
- Secure bidirectional & site-to-site traffic

Traditional networking teams

- Simplify site-to-site connectivity
- Improve TCO with modern architecture

Modern DevOps teams

- Secure service-to-service workflows
- Simplify mesh/P2P connectivity

Quantify the business value of your SASE journey
and the cost of doing nothing

① Self-serve value calculator

② Detailed custom assessment

Value drivers

Risk reduction

Reduce likelihood of...

- Cyberattacks
- data breach

Operational efficiency

Reduce time spent...

- on IT administration
- responding to incidents

Business enablement

Accelerate growth by...

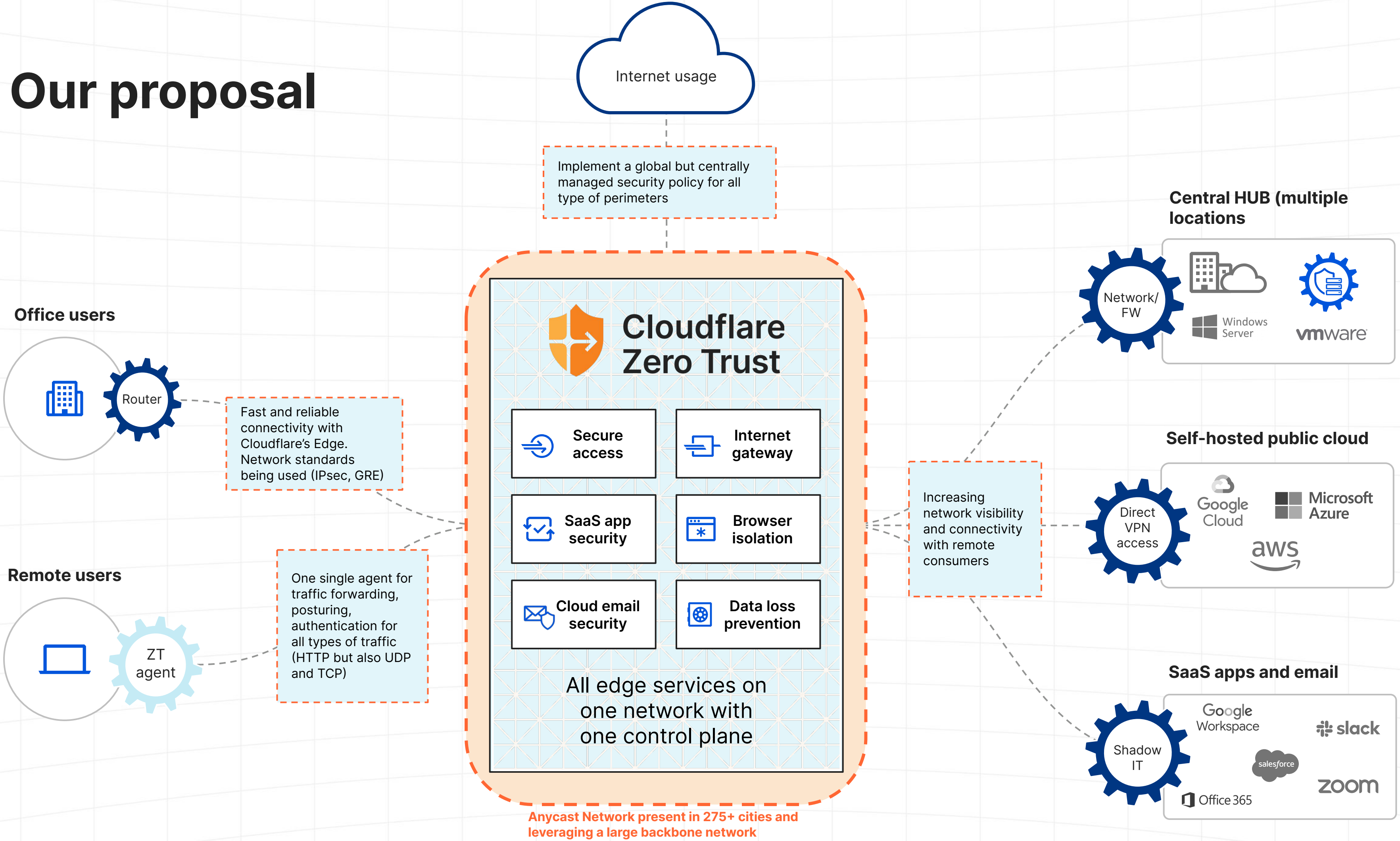
- attracting top talent
- unlocking IT agility

Direct cost savings

Reduce spend on...

- point solutions
- CapEx for hardware

Our proposal



Implement a global but centrally managed security policy for all type of perimeters

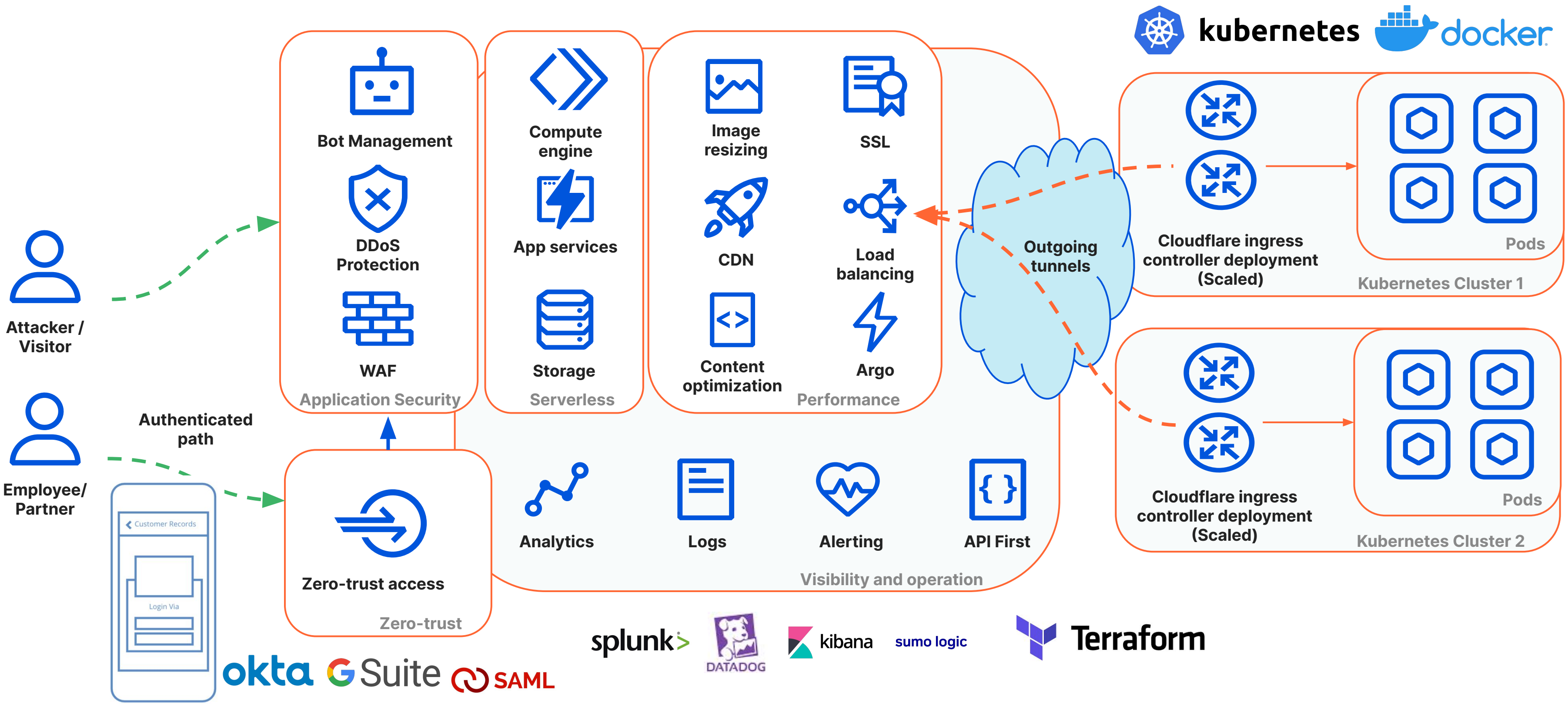
Fast and reliable connectivity with Cloudflare's Edge. Network standards being used (IPsec, GRE)

One single agent for traffic forwarding, posturing, authentication for all types of traffic (HTTP but also UDP and TCP)

Increasing network visibility and connectivity with remote consumers

All edge services on one network with one control plane

Anycast Network present in 275+ cities and leveraging a large backbone network



kubernetes docker

Attacker / Visitor

Employee/ Partner

Authenticated path

Application Security

Bot Management

DDoS Protection

WAF

Serverless

Compute engine

App services

Storage

Performance

Image resizing

SSL

CDN

Load balancing

Content optimization

Argo

Zero-trust

Zero-trust access

Visibility and operation

Analytics

Logs

Alerting

API First

Outgoing tunnels

Kubernetes Cluster 1

Cloudflare ingress controller deployment (Scaled)

Pods

Kubernetes Cluster 2

Cloudflare ingress controller deployment (Scaled)

Pods

okta G Suite SAML

splunk> DATADOG kibana sumo logic Terraform