CLOUDFLARE

Zero Trust:

The modern way of achieving the least privilege principles

Fernando Serto
Chief Evangelist, APJC
Cloudflare

September 2022, Singapore

Uber details how it got hacked, claims limited damage

CLOUDFLARE

While there's no evidence the rideshare company's codebase was altered, the attacker did gain access to Slack, vulnerability reports and financial data.

Published Sept. 19, 2022

Matt Kapko
Reporter

Troy Hunt ✓
@troyhunt

The @Uber breach reads like a 101 of the modern fundamentals: infected device, stolen credentials, annoying 2FA prompts, privilege escalation, etc

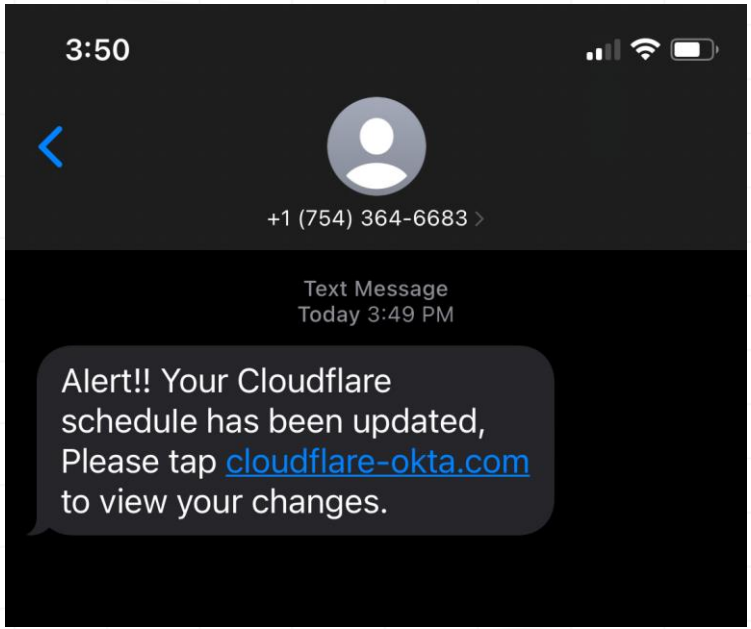
The mechanics of a sophisticated phishing scam and how we stopped it

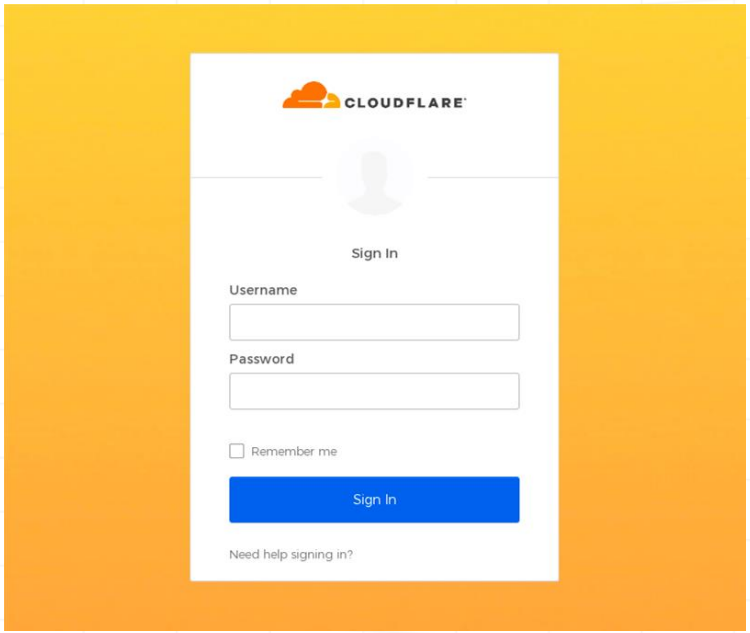
10/08/2022

Matthew Prince Daniel Stinson-Diess Sourov Zaman

This post is also available in 简体中文, 日本語 and Español.

What Cloudflare employees saw





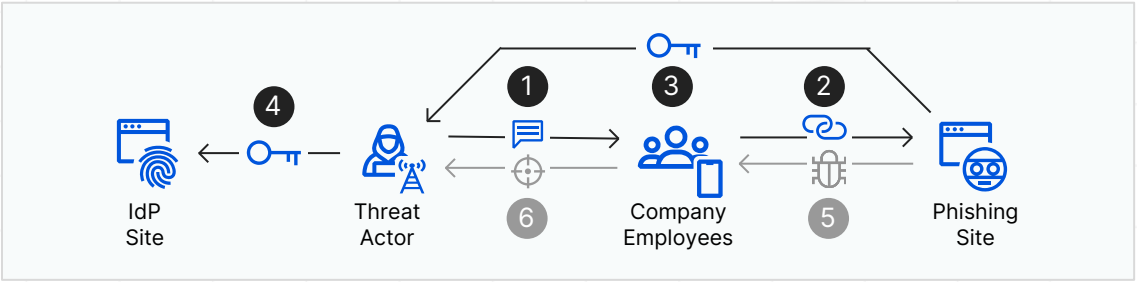
Threat actor attempted cred harvesting playbook
but was unsuccessful gaining full access

CLOUDFLARE

[1-2] Targeted text messages

[3-4] Sophisticated real-time phishing

[5-6] Remote access payload



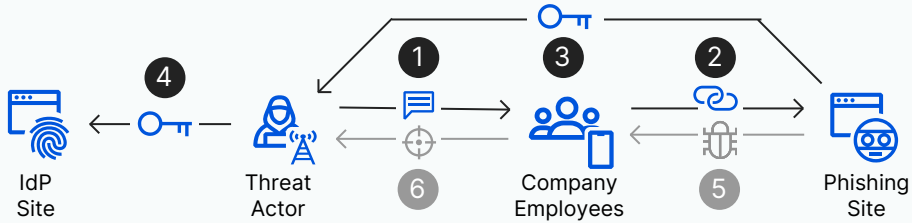
#	What happened
1a	Threat actor sent legitimate-looking malicious SMS
1b	Company employees and family members received SMS on personal & work phone #s
2a	Message included a legitimate-looking newly registered domain (cloudflare-okta.com)
2b	Clicking link opened a legitimate-looking phishing site (Cloudflare Okta login page)
3a	Victim's entered credentials were immediately relayed to the threat actor
4a	Threat actor enters credentials received into actual identity provider (IdP) login site; sending TOTP codes to victims via SMS or mobile app
3b	Victim enters TOTP code on the phishing site, and it too would be relayed to the threat actor
4b	Threat actor enters code in IdP site before it expires
5	Phishing site initiated download of a phishing payload (may have been due to a misconfigured kit)
6	Once software installs, threat actor controls victims' machine remotely

Despite threat actor technical sophistication, Cloudflare was protected as we do not rely on TOTP codes

[1-2] Targeted text messages

[3-4] Sophisticated real-time phishing

[5-6] Remote access payload



#	Technical details
1	● 100+ messages sent from four T-Mobile-issued SIM cards ● 76+ employees received in <1 min
2	● Domain registered via “Porkbun” <40 min before phishing campaign to avoid automated detection ● Site had a Nuxt.js frontend, a Django backend, and was hosted on DigitalOcean
3	● Telegram messaging service provided real-time relay ● 3 employees reached this step, but did not go further as security keys don’t use TOTP
4	● Okta generates a TOTP code sent to the employee via SMS or mobile app ● Defeats most 2FA implementations
5	Included AnyDesk remote access software
6	n/a

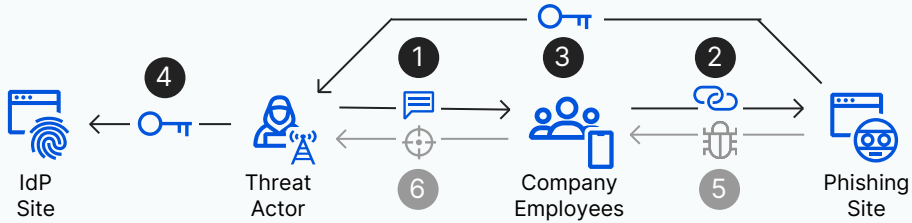
Cloudflare's Zero Trust platform played a role in mitigating this and similar attacks

CLOUDFLARE

[1-2] Targeted text messages

[3-4] Sophisticated real-time phishing

[5-6] Remote access payload

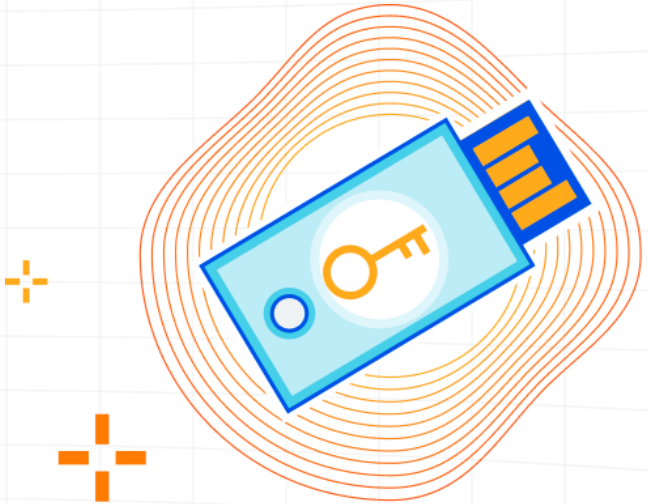


#	Our response
1	● 1 min after attack, SIRT was informed; no evidence of compromise via directory provider logs ● 9 min after attack, SIRT sent an internal warning to all employees across chat & email
2	● 3 min after attack, SIRT added domain to SWG to block access. Later, isolated access to all newly registered domains and seized control of domain. ● 37 min after attack, DigitalOcean shutdown the attacker's server via our collaboration
3	● 1-37 min after attack, SIRT killed active sessions via ZTNA, plus 48 min after attack, SIRT reset credentials & initiated scans for the identities & devices with unverified 2FA per our activity logs
4	● Intel from server indicated actor was targeting other orgs, including Twilio, and SIRT shared intel ● SIRT blocked IPs used by threat actor from accessing any Cloudflare service
5	n/a
6	Note: Endpoint security used by Cloudflare would have stopped the installation

Reinforced the importance of what we're doing well, and everything you can do, too

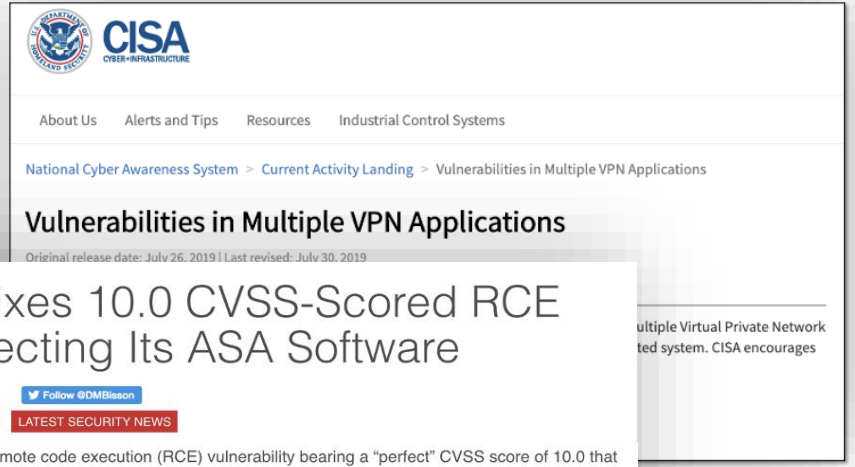
CLOUDFLARE

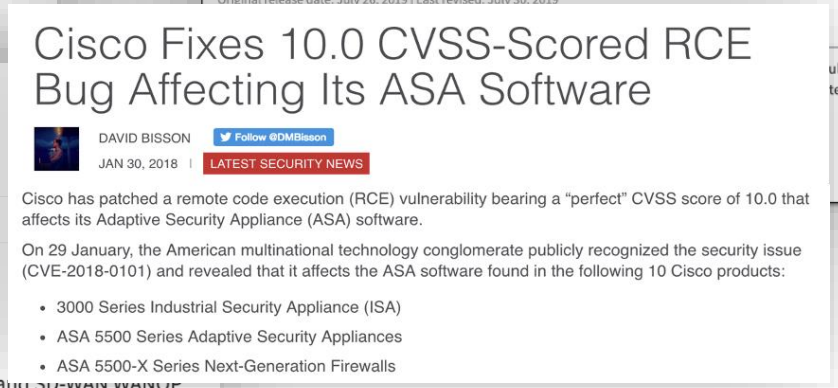
1. **Adopt a phishing-resistant MFA**
   Not all MFA provides the same level of security
2. **Implement selective enforcement**
   with identity- and context-centric policies
3. **Enforce strong auth everywhere**
   All users and apps; even legacy non-web systems
4. **Adopt Zero Trust via one platform**
   Easier, faster operations & improved security posture
5. **Establish paranoid, blame-free culture**
   Report suspicions early and often



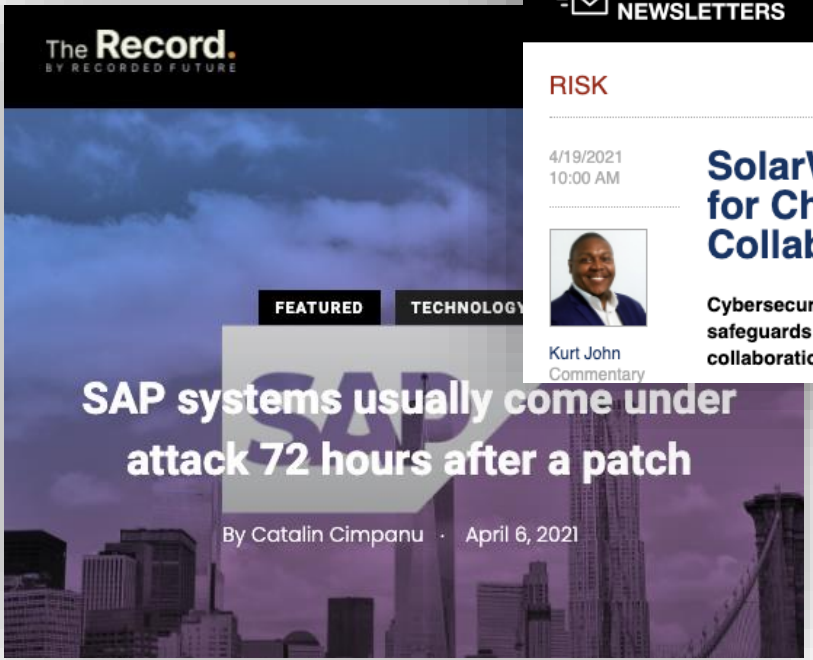
The Perimeter as we know it, is **under Attack**...

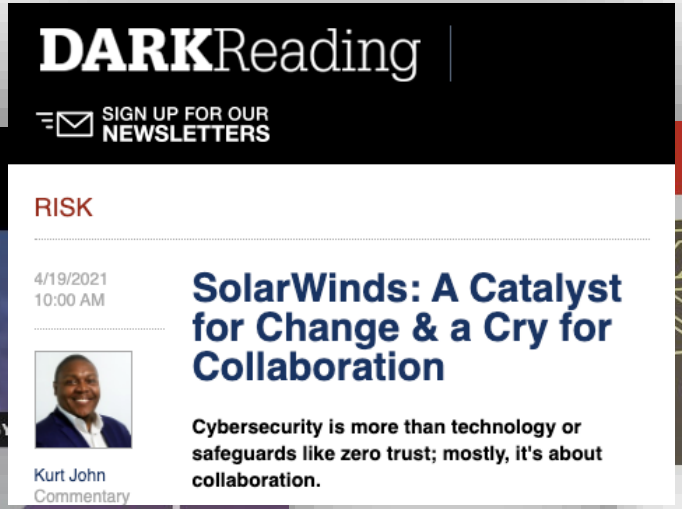
CLOUDFLARE

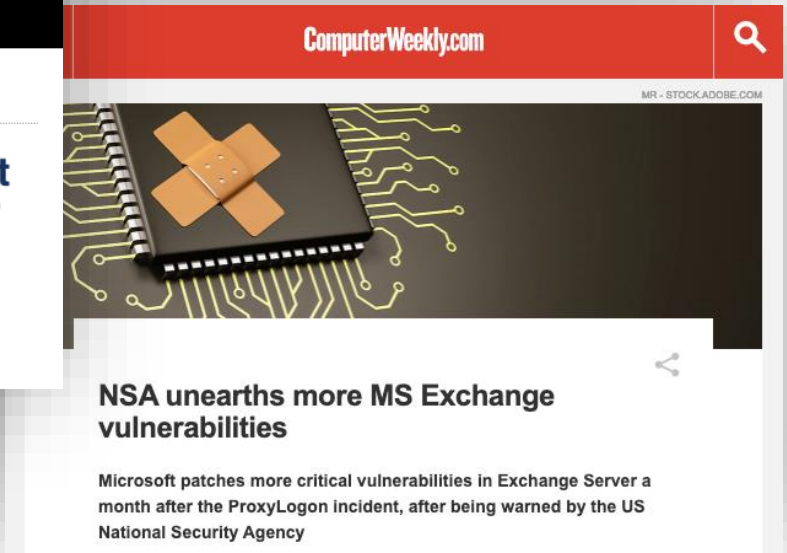




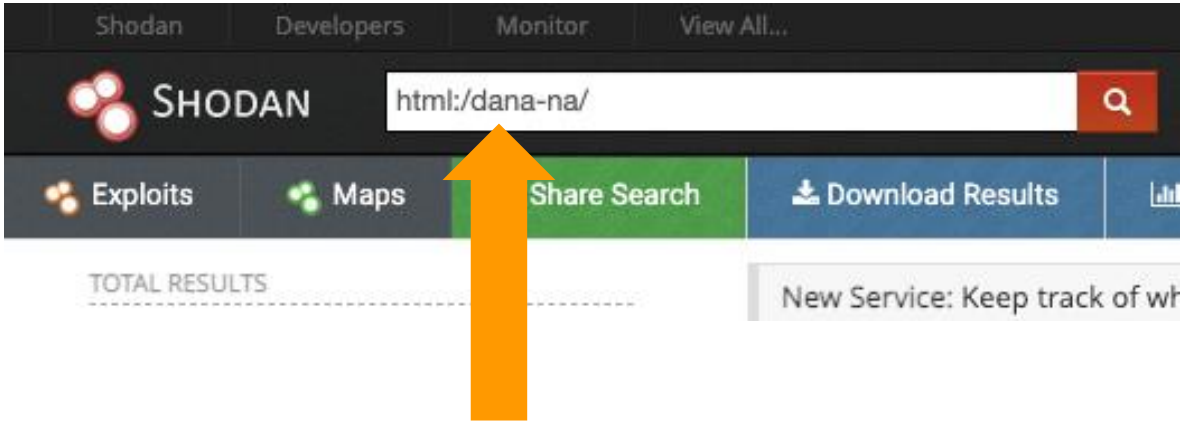
… and so are the apps **inside the corporate environment**







In most cases, you **become a target by accident**...



Sample Query for Pulse Secure

TOTAL RESULTS

40,773

TOP COUNTRIES

United States	11,531
Japan	3,455
Germany	2,634
United Kingdom	2,361
France	2,021

TOP SERVICES

HTTPS	40,048
HTTP	106
HTTP (8080)	56
Qconn	40
HTTPS (8443)	32

In most cases, you **become a target by accident**...

CLOUDFLARE

Patching Vulnerabilities **takes TIME**...

9.8

CVSS Score

7% Australia

12% USA

13% Singapore

23% India

% of devices still vulnerable **5 months after patch released**

CLOUDFLARE

Zero Trust is a mindset shift

Never trust, always verify

Assume risk & reduce impact

Default deny + least privilege access

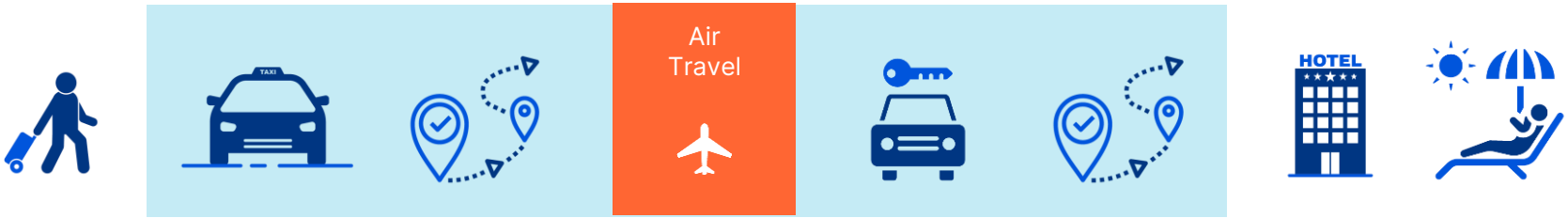
Context based (identity, posture etc)

Prevent lateral movement

CLOUDFLARE

Air Travel	Security	Security	Security	
				
	● Purpose ● Identity	● Baggage ● Traveler	● Boarding ● Seat	● Fun ● Recharge
	✓ Validate/ Verify	✓ Posture Check	✓ Authorize	✓ Objective
Zero Trust	● Context ● Identity (requestor)	● Posture check ● Isolation	● No lateral movement ● Micro segmentation	● Enables Any-to-Any ● Protect Users Device & Apps

For analogy purpose only



Security Service Edge (SSE)

Secure Access Service Edge (SASE)

Drop bags in the taxi, Get it at Hotel	Fastest route to airport. Traffic intelligence	Express Entry at airport	Pre-Identity authorization	Early boarding	Best seats	Rental Car	Navigation, Toll pass	Easy hotel check-in	Customized excursions

Exceptional vacation experience(safe, fast, reliable)

One portal, friction less travel, safety first, direct flights, customized restaurant, excursions & many more

Cloudflare

For analogy purpose only

The Cloudflare global network

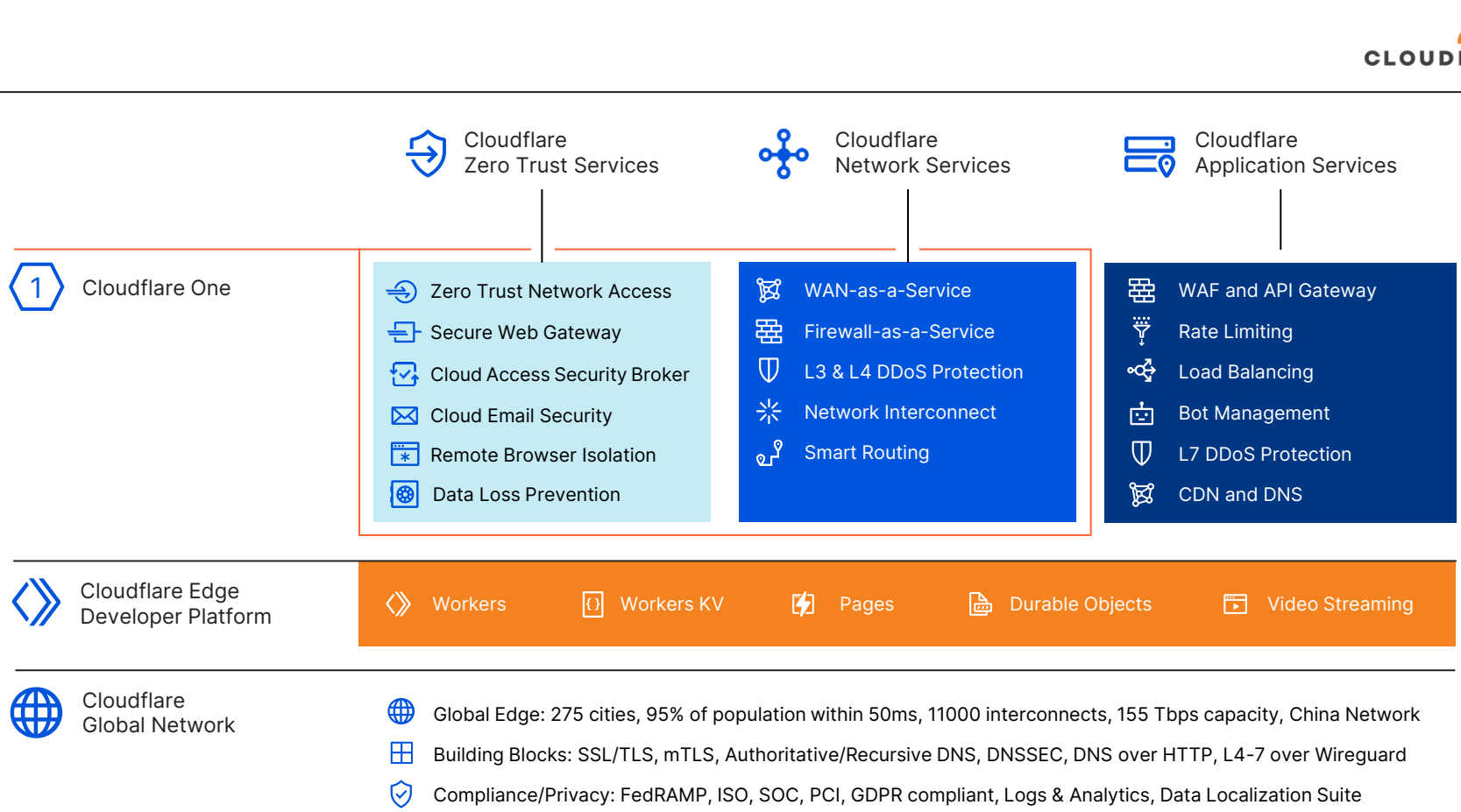
CLOUDFLARE

275+
cities in 100+ countries,
including mainland China

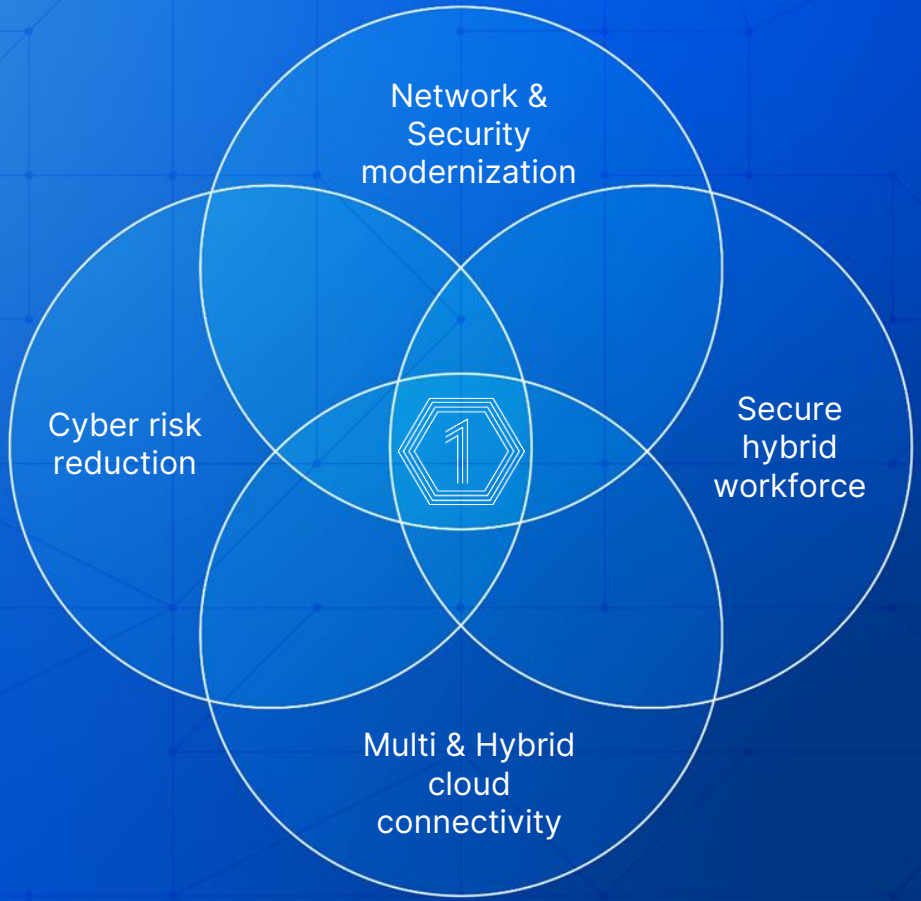
11,000+
networks directly connect
to Cloudflare, including ISPs,
cloud providers & large enterprises

155 Tbps
of network edge capacity
& growing

● = Cloudflare city (Map data as of December 15, 2021)

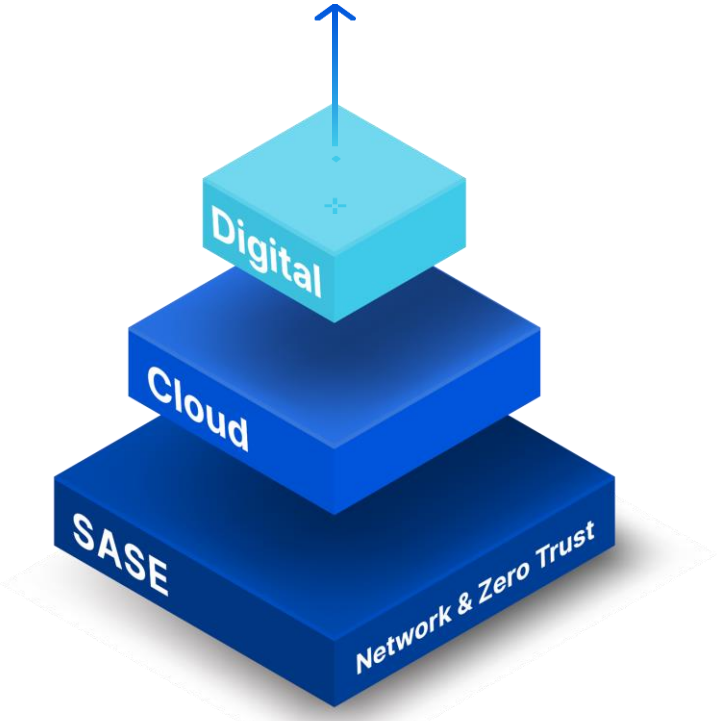

CLOUDFLARE
Cloudflare Zero Trust Services
Cloudflare Network Services
Cloudflare Application Services
Cloudflare One
Zero Trust Network Access
Secure Web Gateway
Cloud Access Security Broker
Cloud Email Security
Remote Browser Isolation
Data Loss Prevention
WAN-as-a-Service
Firewall-as-a-Service
L3 & L4 DDoS Protection
Network Interconnect
Smart Routing
WAF and API Gateway
Rate Limiting
Load Balancing
Bot Management
L7 DDoS Protection
CDN and DNS
Cloudflare Edge Developer Platform
Workers
Workers KV
Pages
Durable Objects
Video Streaming
Cloudflare Global Network
Global Edge: 275 cities, 95% of population within 50ms, 11000 interconnects, 155 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

CLOUDFLARE


Network & Security modernization
Cyber risk reduction
Secure hybrid workforce
Multi & Hybrid cloud connectivity
1

CLOUDFLARE

Business Transformation



There is no longer a business & technology strategy.
There is a strategy & technology is driving it.

Network

Optimize business operations

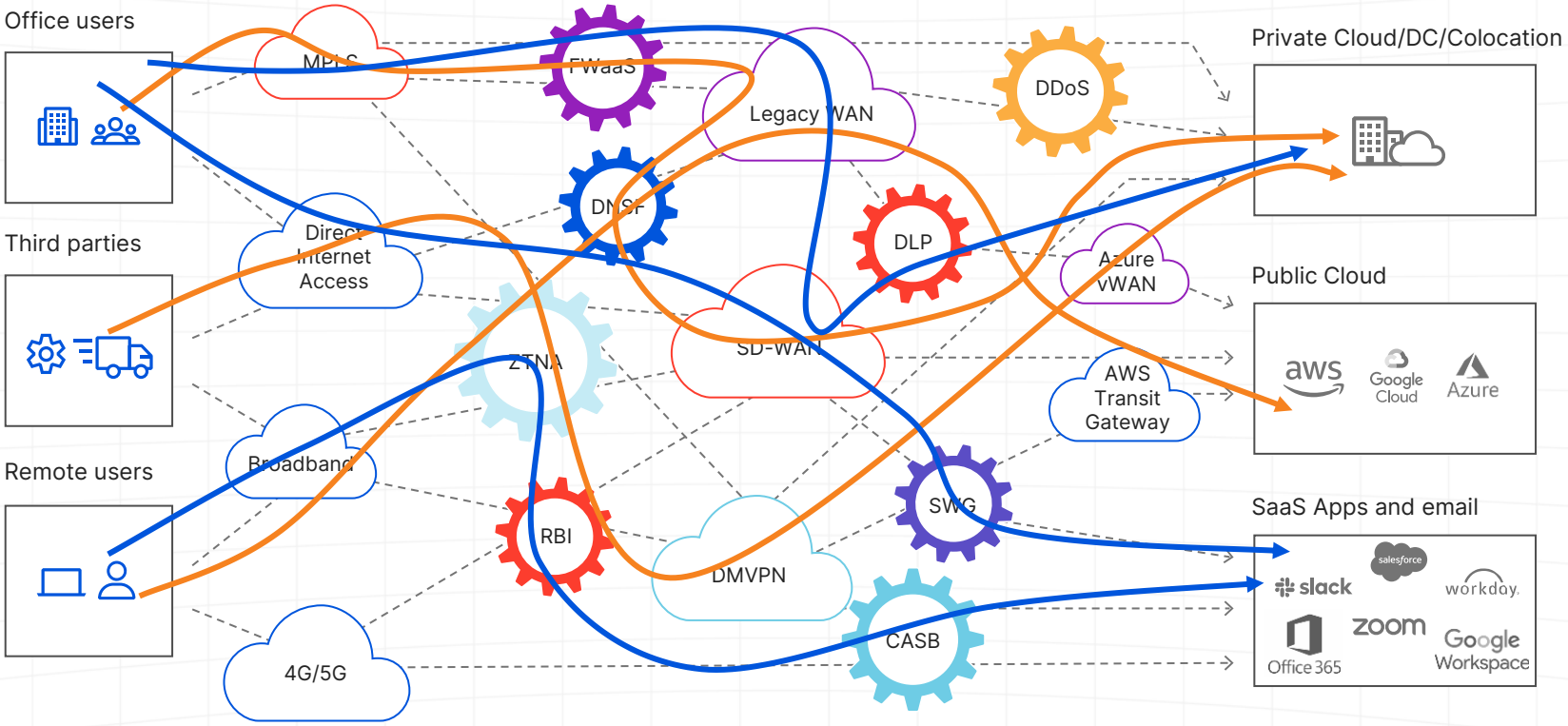
Increased speed to market

Re-imagine user experience

New revenue streams

CLOUDFLARE

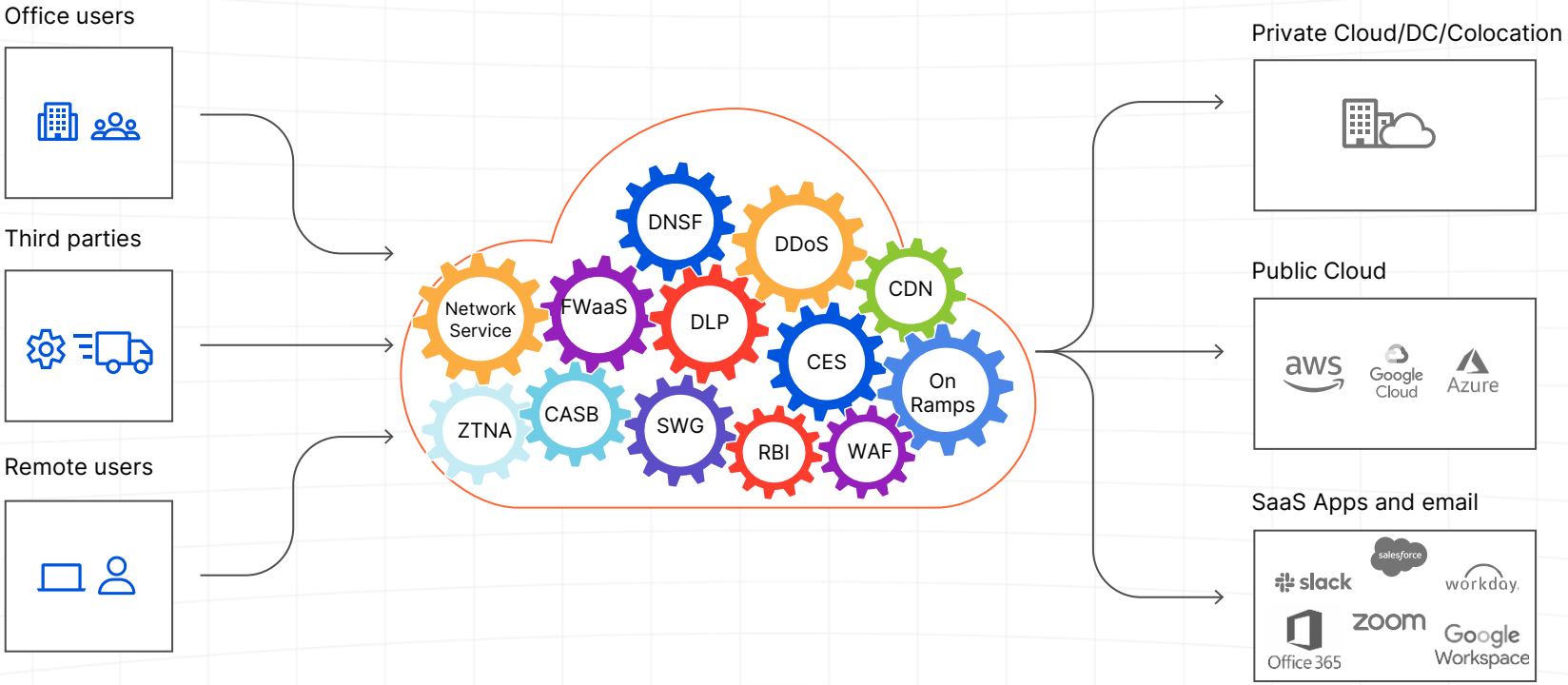
Legacy networks & products are not built to support your digital future



Cybersecurity fatigue is a growing concerns

CLOUDFLARE

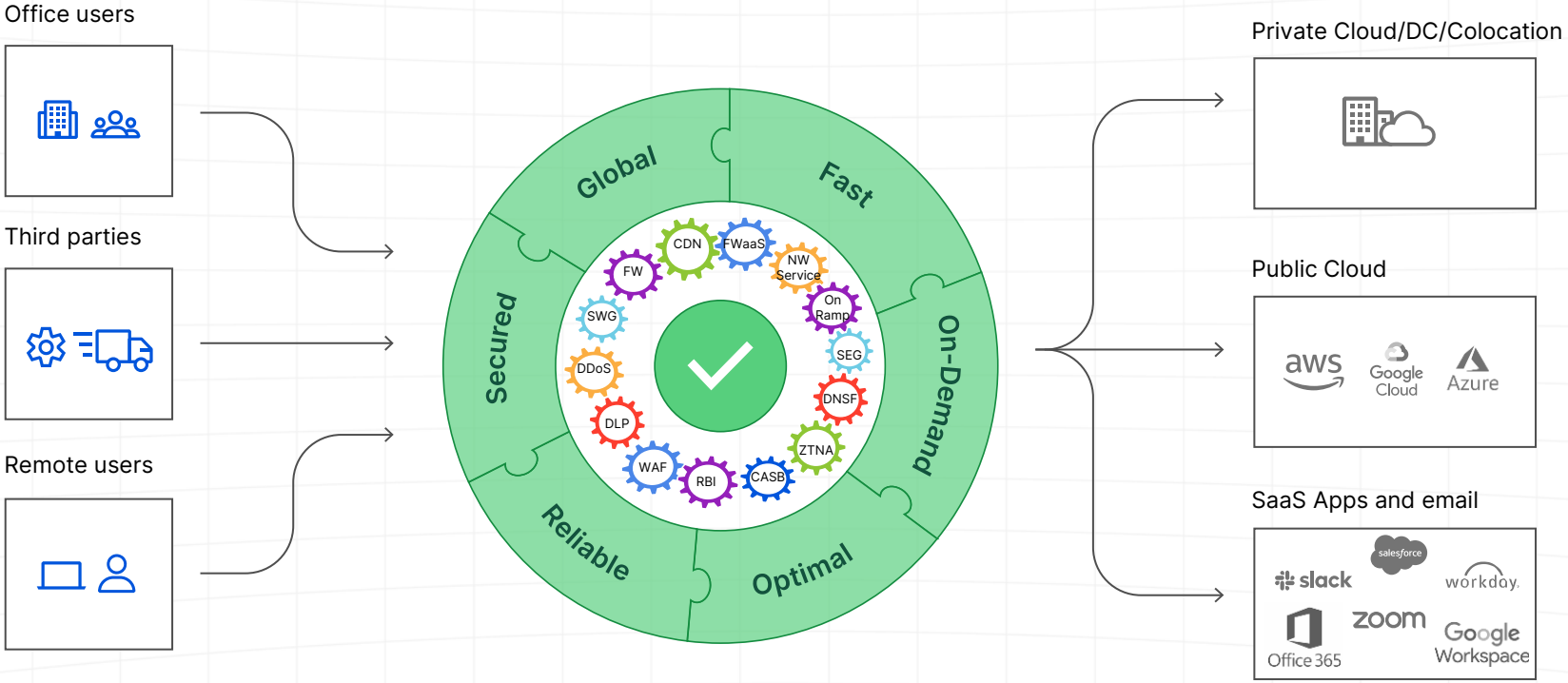
Solution for future success?



Any-to-Any | End-to-End | Internet Native | Single Platform | Composable Services

CLOUDFLARE

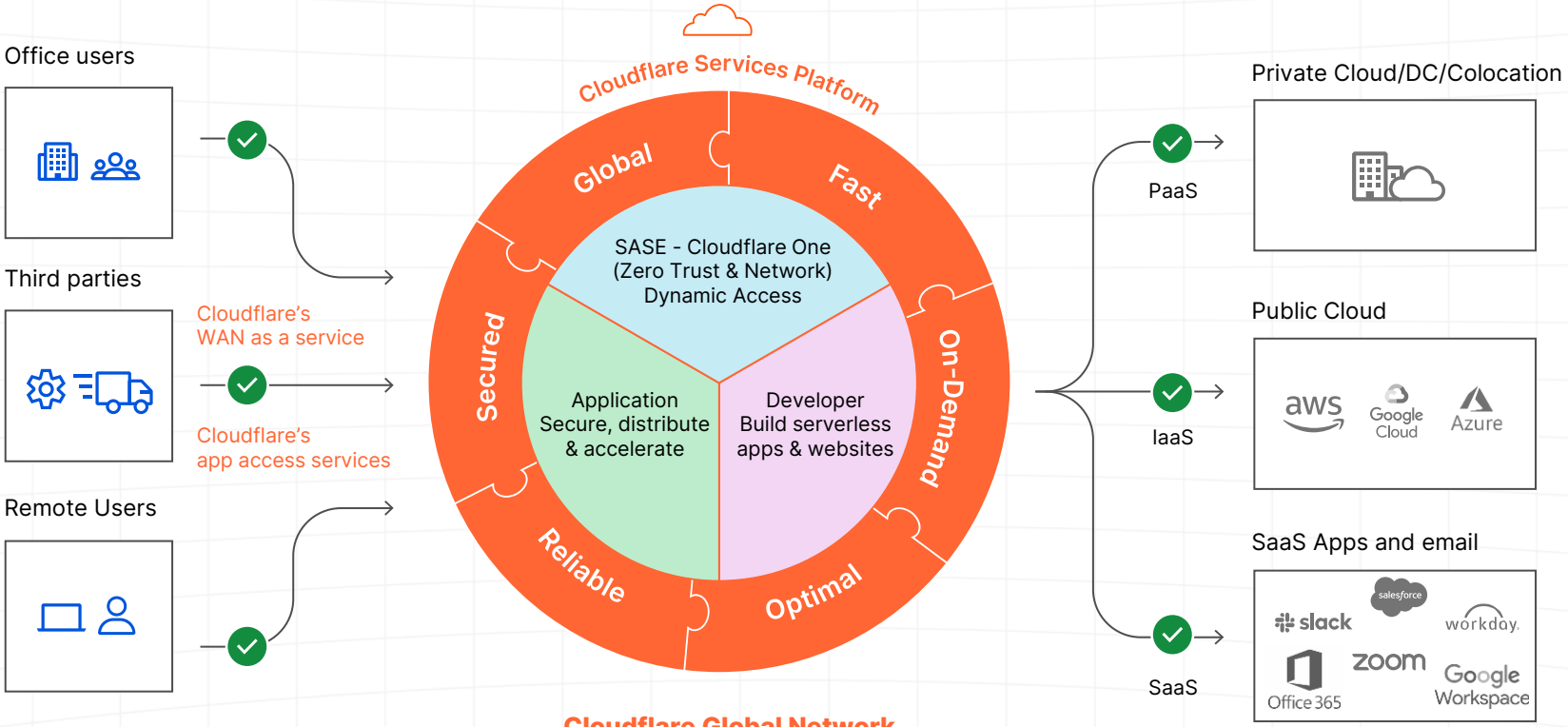
Solution for future success?



Path to the cloud needs to have same characteristics as the cloud

Cloudflare is secure, fast, reliable, any-to-any & end-to-end, composable

One management plane, One control plane to one data plane with single-pass inspection

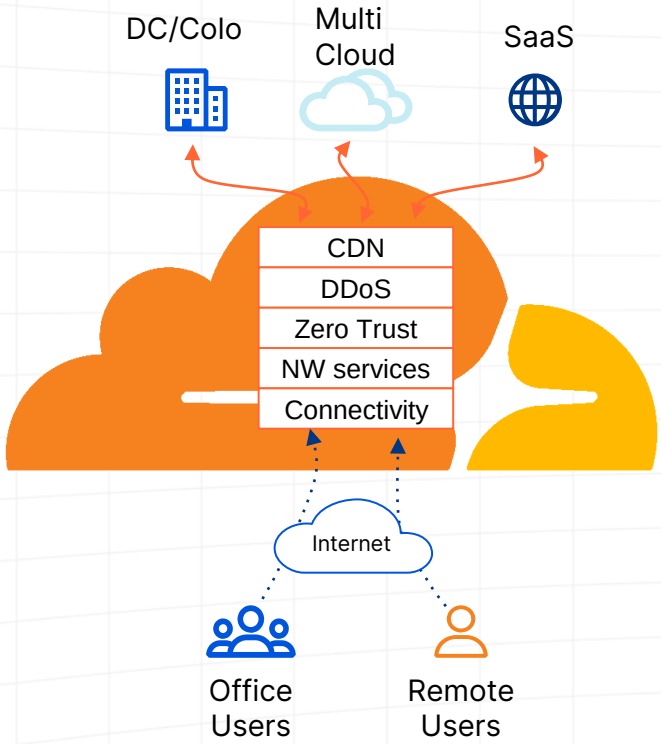


Cloudflare Global Network

275 cities (100 countries) • ~50ms from 95% of Internet population
11,000 interconnects •155 Tbps capacity network onramps

CLOUDFLARE

Cloudflare enables cafe experience for corporate apps



Simplify application access

Distribute(CDN) & protect applications

Apply consistent ZT based policies

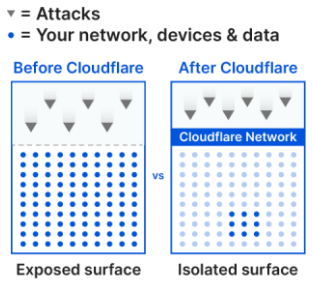
Protect users and endpoints

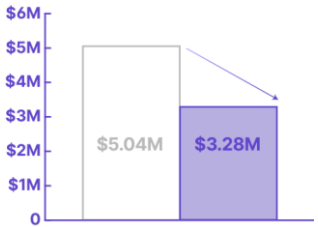
Enhance end user experience

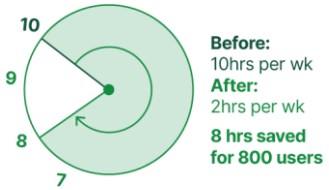
Business drivers and Zero Trust outcomes

CLOUDFLARE

Discover & monitor attack surface	Authorize access based on context, reduce blast radius	Ensure plug & play infrastructure	Manage IT fatigue	Improve customer experience
1. **Reduce attack surface** **91%↓**	2. **Reduce incident costs** **35%↓**	3. **Accelerate onboarding** **60%↑**	4. **Reduce IT tickets** **80%↓**	5. **Reduce latency** **39%↓**



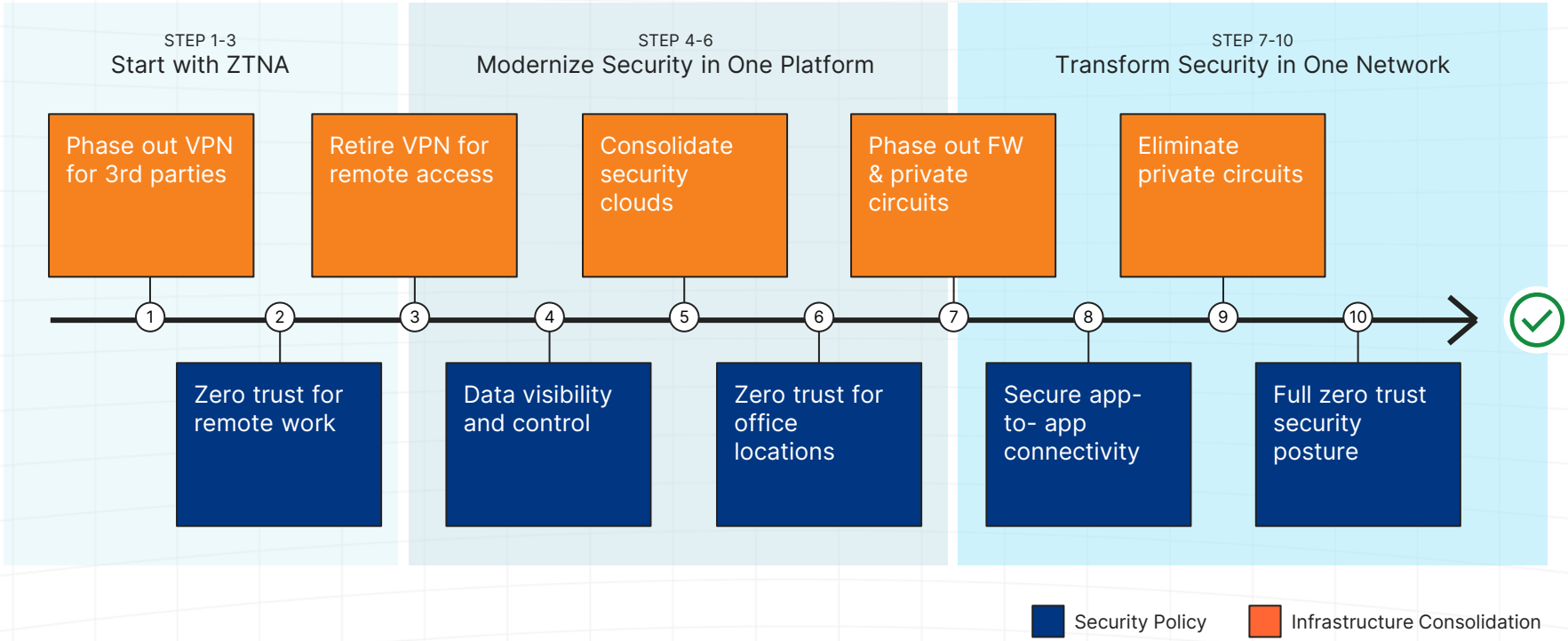




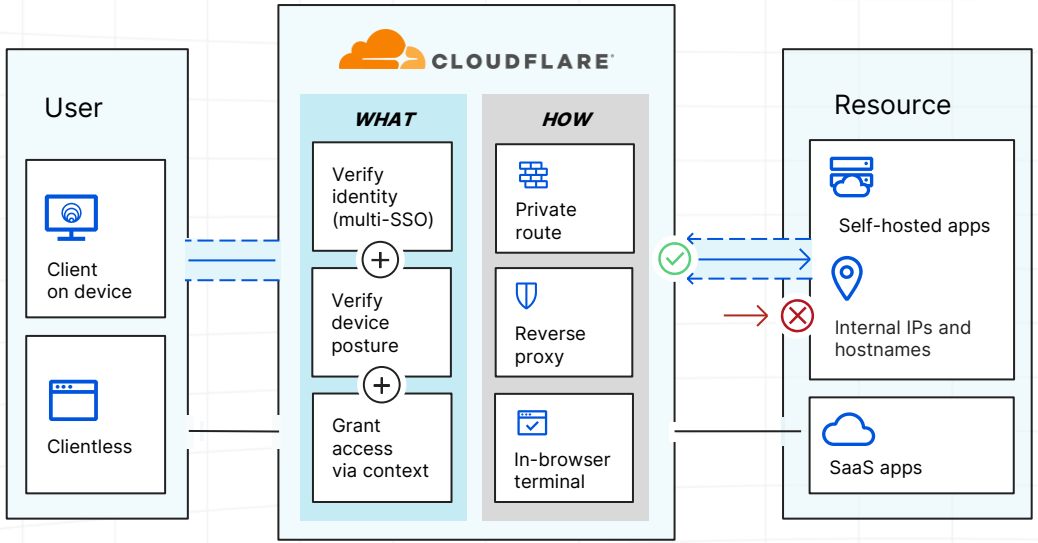
CLOUDFLARE

Recommendations for a successful Zero Trust journey

A common roadmap to Zero Trust, and eventually a complete SASE transformation



VPN replacement and augmentation



Zero Trust Network Access

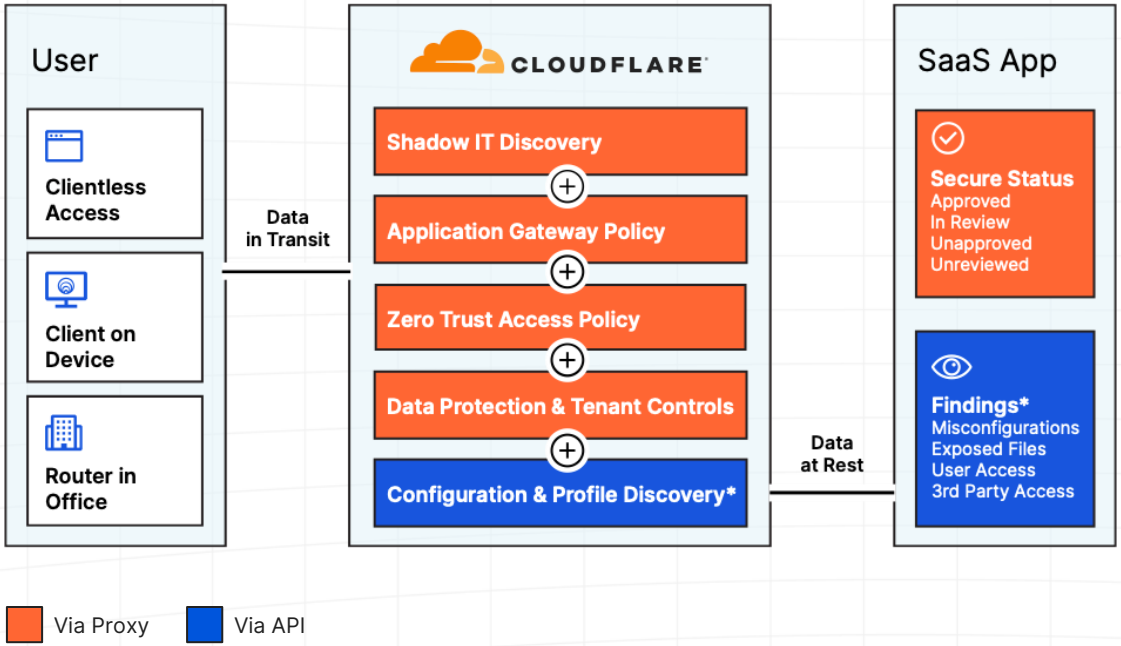
Simplifies remote access

Improves user experience

Eliminates lateral movement

Built-in DDoS & FW protection

Streamline SaaS security



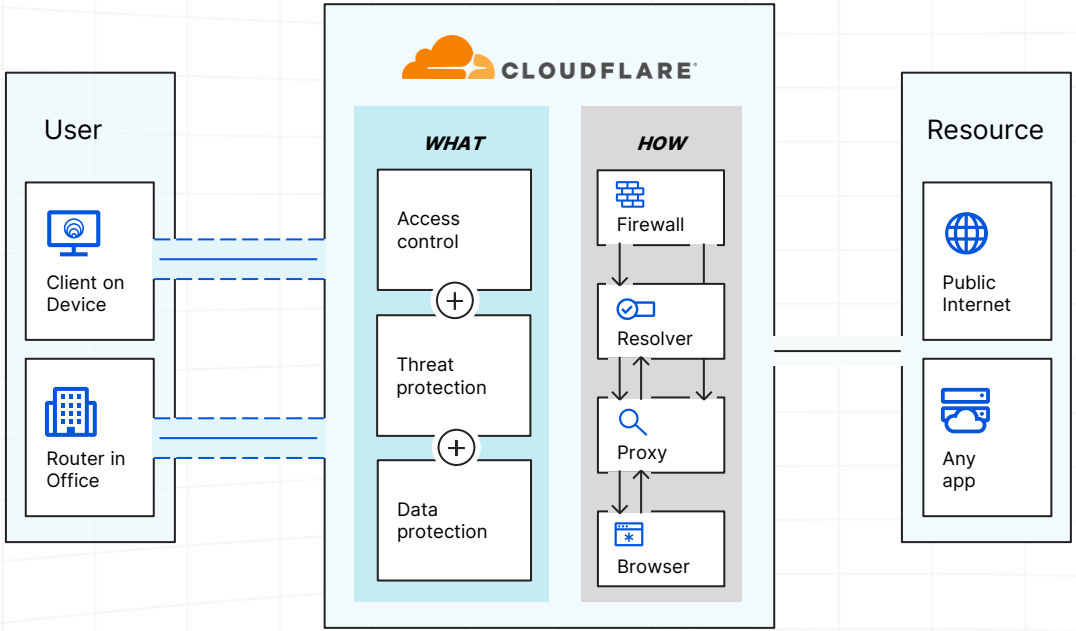
Cloud Access Security Broker

More visibility, less config

Prevent data exfiltration

Quickly identify new risks

Internet threat and data protection



Secure Web Gateway

Simplify policy compliance

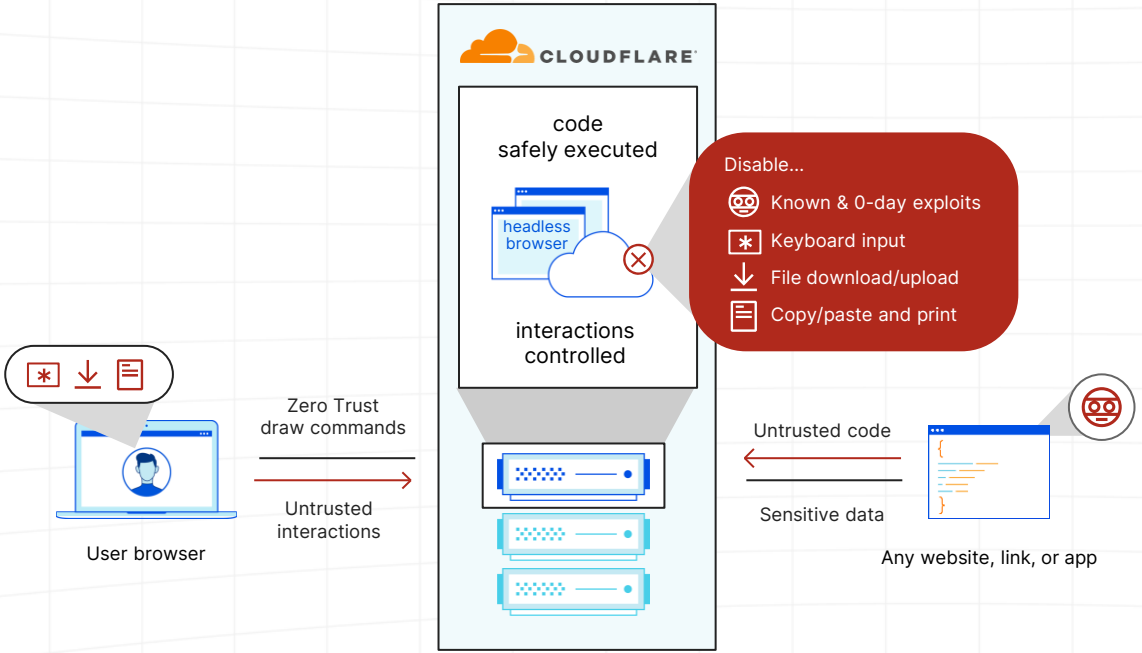
Stop ransomware

Stop phishing

Stop shadow IT

Stop unknown threats

Perfect and simplify protection



Remote Browser Isolation

Zero trust web browsing and email links

Protect data-in-use

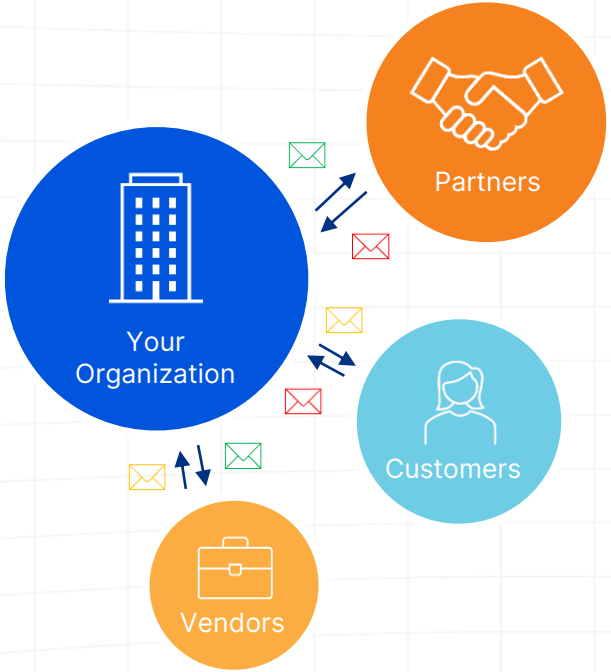
Lightning-fast UX

Compatibility w/all browsers

Extending Zero Trust principles to email

Too much implicit trust in email communications

Email makes everyone an insider; no network intrusion or malware needed



Cloud Email Security with RBI integration

Stop multi-channel phishing attacks pre/at/post-delivery

Stop BEC attacks using contextual relationships

Eliminate lateral movement across inboxes

CLOUDFLARE

Zero Trust for all internal and external network, web and email traffic

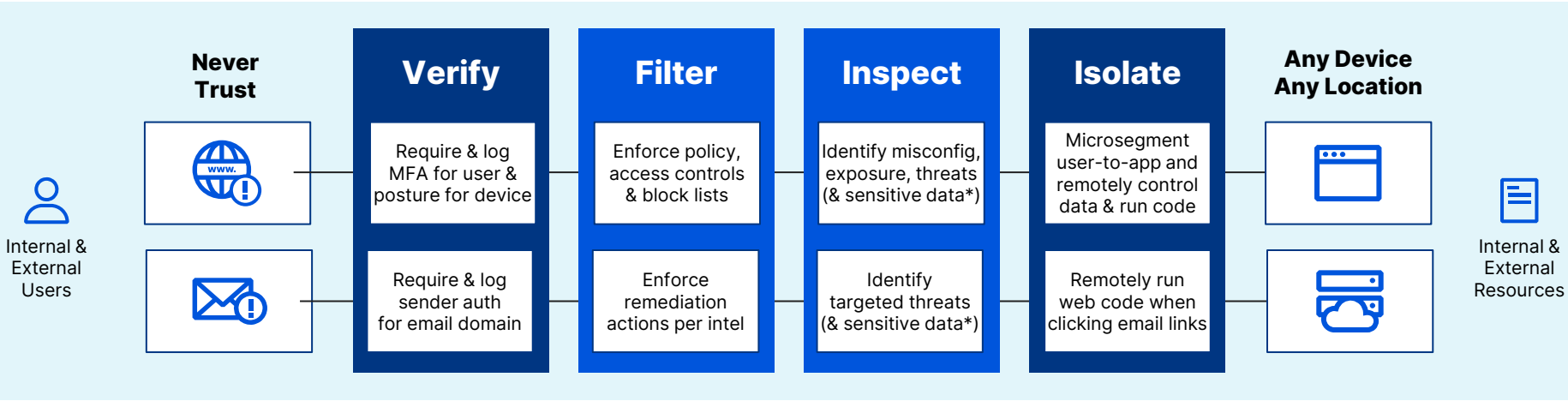
Built-In App & Email Security

\+

API-Driven SaaS Security · CASB · CES

\+

Proxy-Based Network Security · ZTNA · SWG · RBI



Roadmap to Zero Trust architecture

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	

Details @ zerotrustroadmap.org

CLOUDFLARE

Thank you!