Cloud security: Your Zero Trust Future

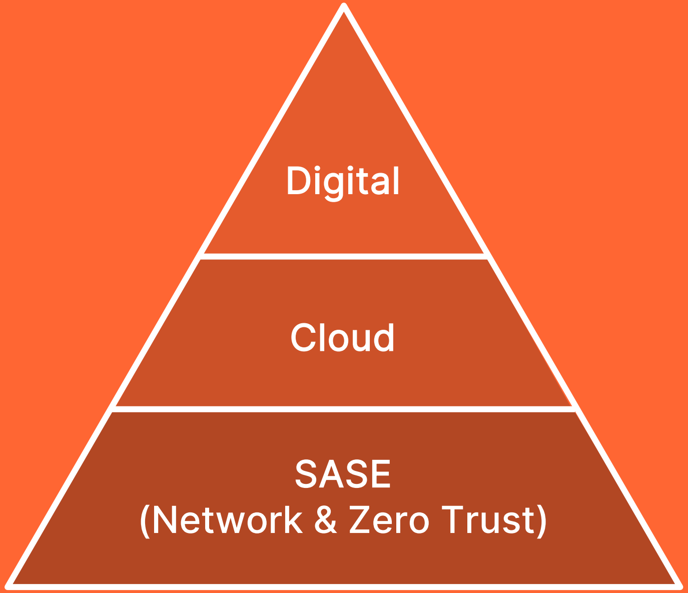
Shimri Vachter
CEERI Regional SASE Sales Lead
CISSP, CCISO, MSc. Management, Keynote, Podcaster,
Future of Business Evangelist

What we are seeing at Cloudflare in 2023

1. Attackers are hitting applications from multiple angles
2. Ransomware is still on the rise
3. Distributed work and cloud-based apps are here to stay
4. Cloud development platforms limit developer velocity
5. Privacy regulations are being passed worldwide

Business Transformation

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



CIO & CISO Initiatives

Transformation is must to accelerate cloud, digital journey & its value to the business

Secured multi-cloud connectivity

Enable hybrid workforce

Cyber risk reduction

Network & Security modernization

Visibility and ease of management

CXO Challenges & Priorities

Rising cost & recession head winds

Business transformation (cloud & digital)

Supply chain resilience

Digital pandemic

Skills gap, talent retention

Case Study: Cisco Breach – A Cautionary Tale of Mismanaged Credentials & Privileged Identities

Attack Group : **the Yanluo Wang ransomware group**

Result : stolen 2.75GB - around 3100 files, including NDA and engineering

Method : 3 key stages

Step 1 : Acquiring the credentials = compromised personal (Google) account

Step 2 – Authenticating to the Cisco VPN

- **Voice phishing** - faking TRUST
- **MFA fatigue** - Triggering MFA push notifications repeatedly

Step 3 - Conquering the target

- **LogMeIn + TeamViewer** = remote access/Persistence
- **Cobalt Strike & Mimikatz** = exploitation, credential harvesting + lateral movement.

https://sec.cloudapps.cisco.com/security/center/resources/corp_network_security_incidents
August 2022, Beyondtrust

Case Study: Conclusions

- MFA are not safe by its own - Use FIDO 2 MFA
- Prevent Lateral movement and C&C -NO MORE VPN
- “Never trust, always verify” - ZERO TRUST
- Least Privileged access by default

Zero Trust is a mindset shift

Never trust, always verify

Assume risk & reduce impact

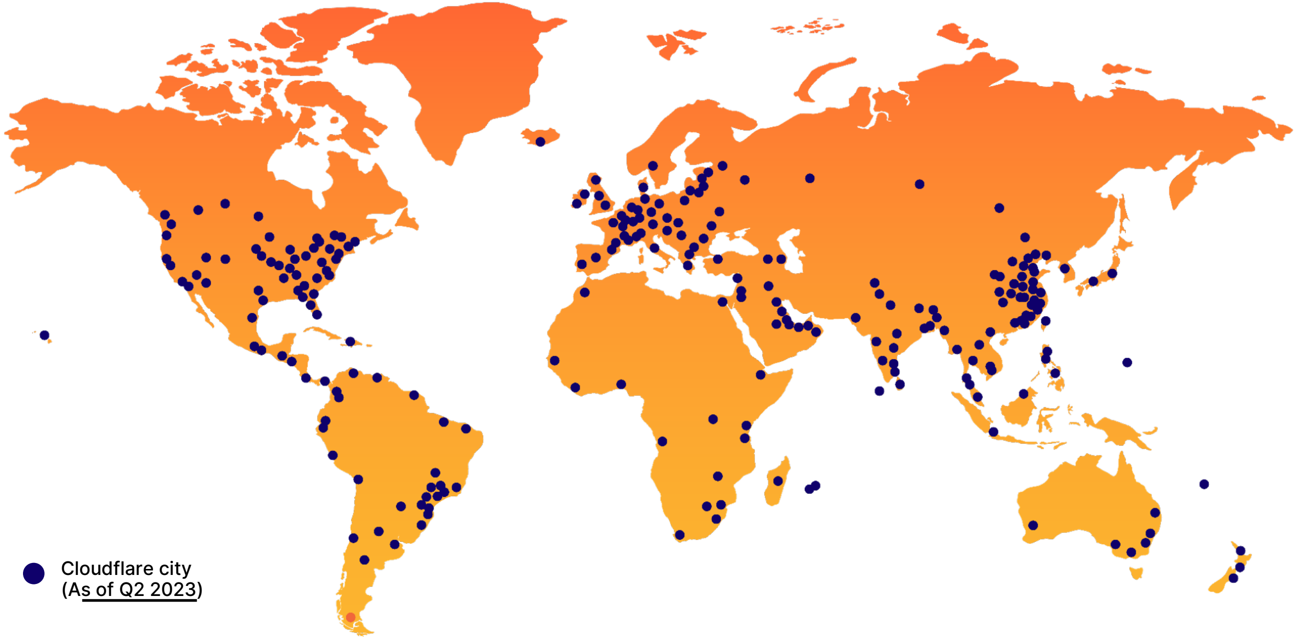
Default deny + least privilege access

Context based (identity, posture etc)

Prevent lateral movement

Cloudflare is the only composable, Internet-native platform

that delivers local capabilities with global scale and with…



● Cloudflare city
(As of Q2 2023)

300

cities in 100+ countries, including mainland China

12,500

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

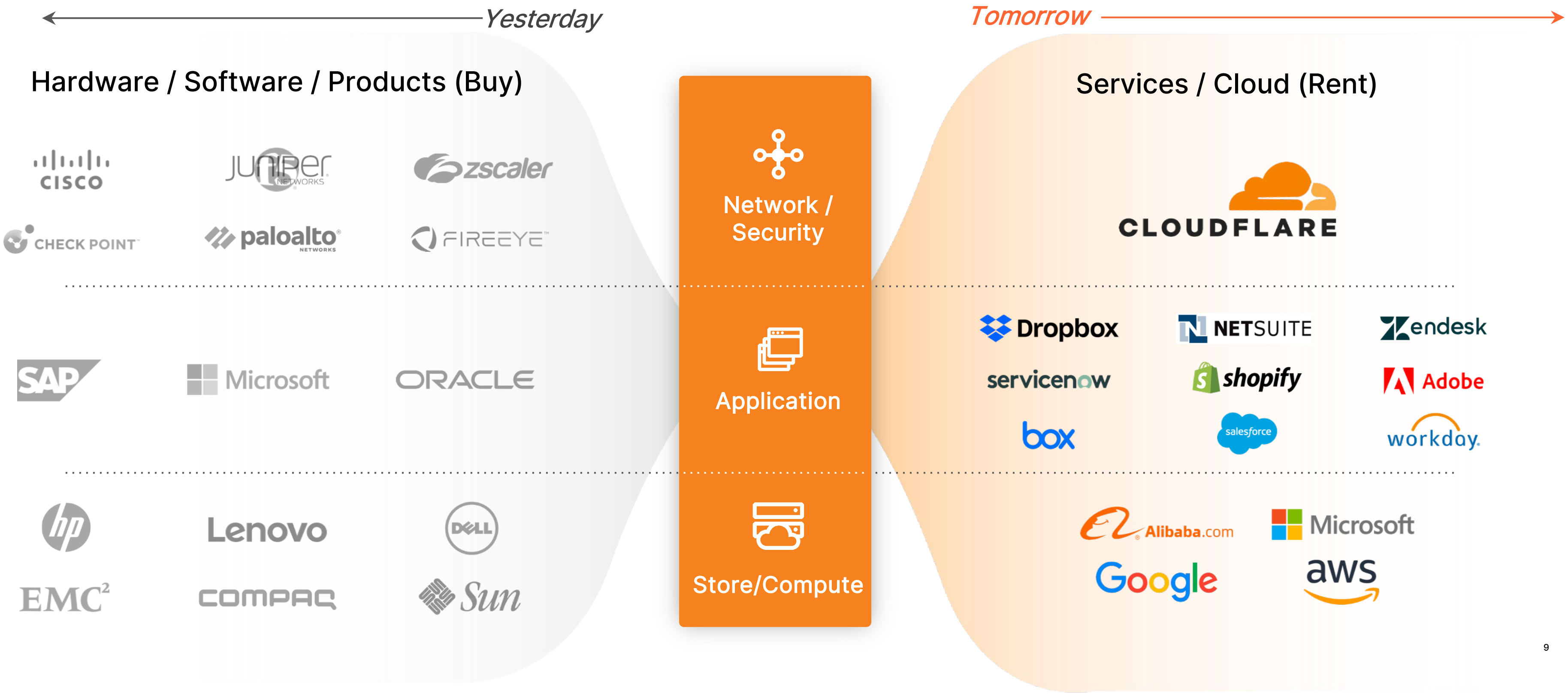
209 Tbps

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

~50 ms

from 95% of the world's Internet-connected population

Cloudflare was built for what's next



Yesterday

Tomorrow

Hardware / Software / Products (Buy)

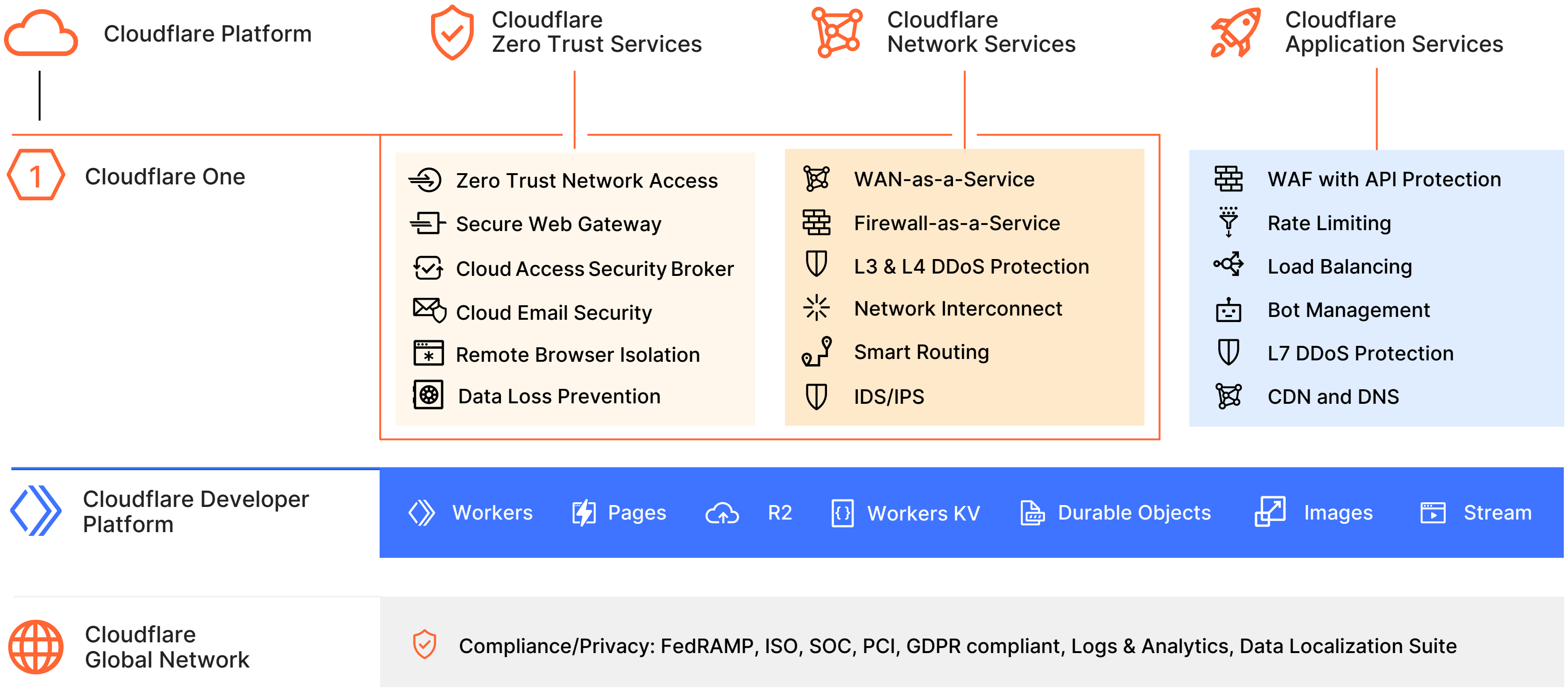
Network / Security

Application

Store/Compute

Services / Cloud (Rent)

Integrated Global Cloud Platform



Cloudflare Platform

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
- IDS/IPS

- WAF with API Protection
- Rate Limiting
- Load Balancing
- Bot Management
- L7 DDoS Protection
- CDN and DNS

Cloudflare Developer Platform

Workers · Pages · R2 · Workers KV · Durable Objects · Images · Stream

Cloudflare Global Network

Compliance/Privacy: FedRAMP, ISO, SOC, PCI, GDPR compliant, Logs & Analytics, Data Localization Suite

> “Cloudflare is a growth enabler for DHL Parcel. Cloudflare provides security out-of-the-box that helps alleviate my team’s workload and allows us to focus on the business.”

– Jan de Groot

Vice President Digital and
Business Optimization, DHL

“Cloudflare was the only provider that ‘just worked’ like you said it would when we hooked everything up.”

Network Security Engineer

The Road Map to Zero Trust

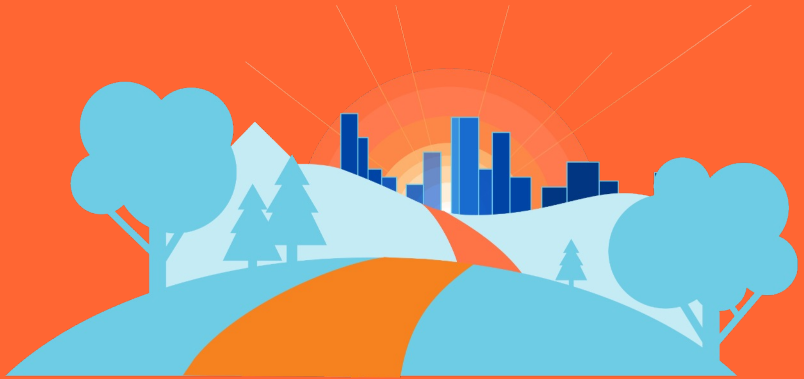
- **many comprehensive steps** in the Zero Trust roadmap

- **Quick WIns map to Early Zero Trust Adoption**

- **The Zero Trust SASE Future Architecture**

- How to **initiate an adoption roadmap** for your organization

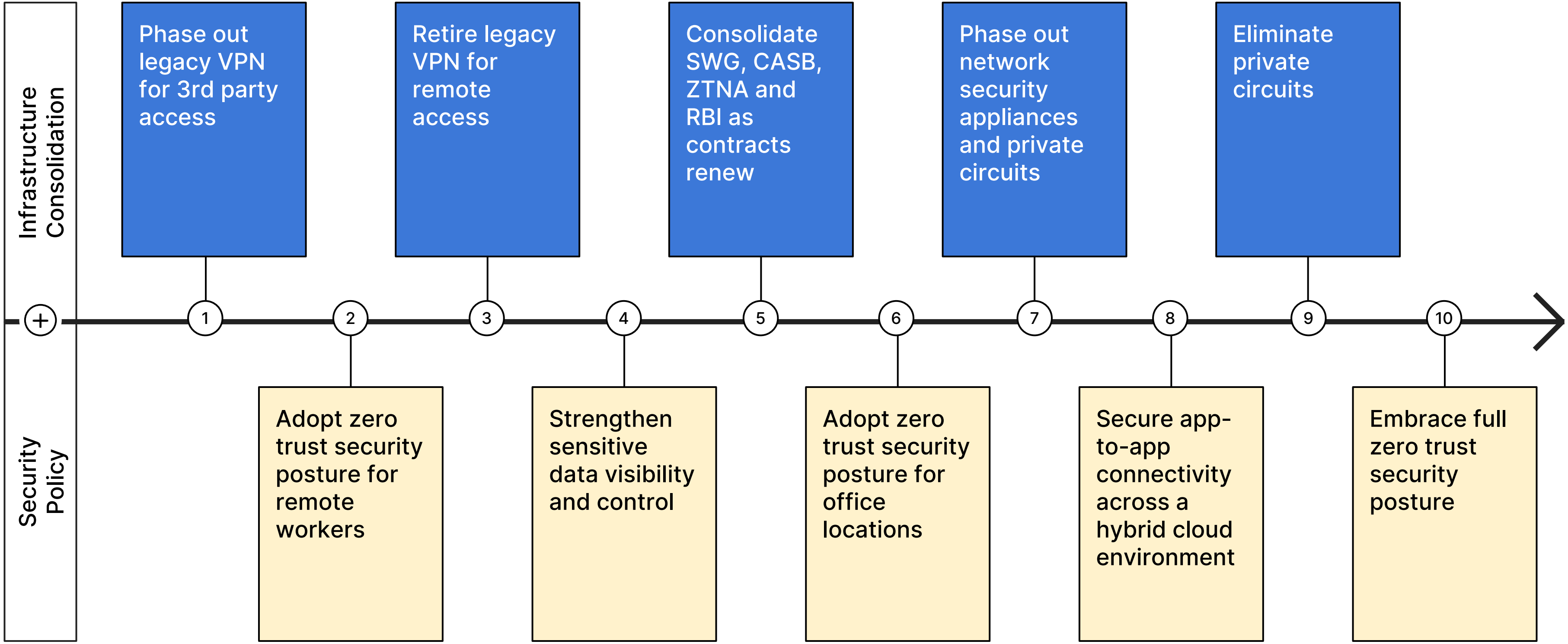
Roadmap to Zero Trust architecture



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	▮▮▮

Quick Wins to Zero Trust: optimize your network at your own pace



Infrastructure Consolidation

Security Policy

1 Phase out legacy VPN for 3rd party access

2 Adopt zero trust security posture for remote workers

3 Retire legacy VPN for remote access

4 Strengthen sensitive data visibility and control

5 Consolidate SWG, CASB, ZTNA and RBI as contracts renew

6 Adopt zero trust security posture for office locations

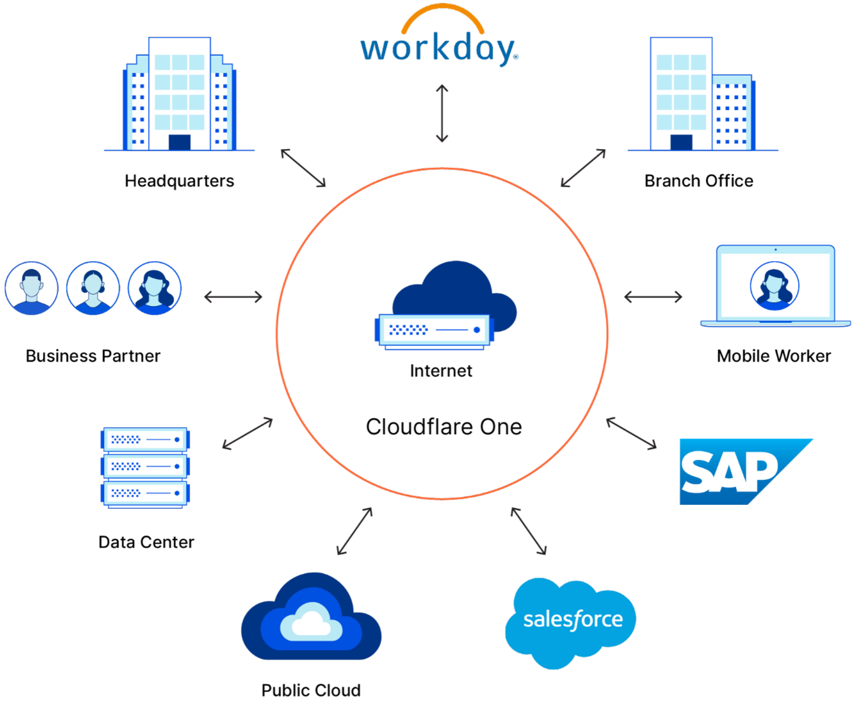
7 Phase out network security appliances and private circuits

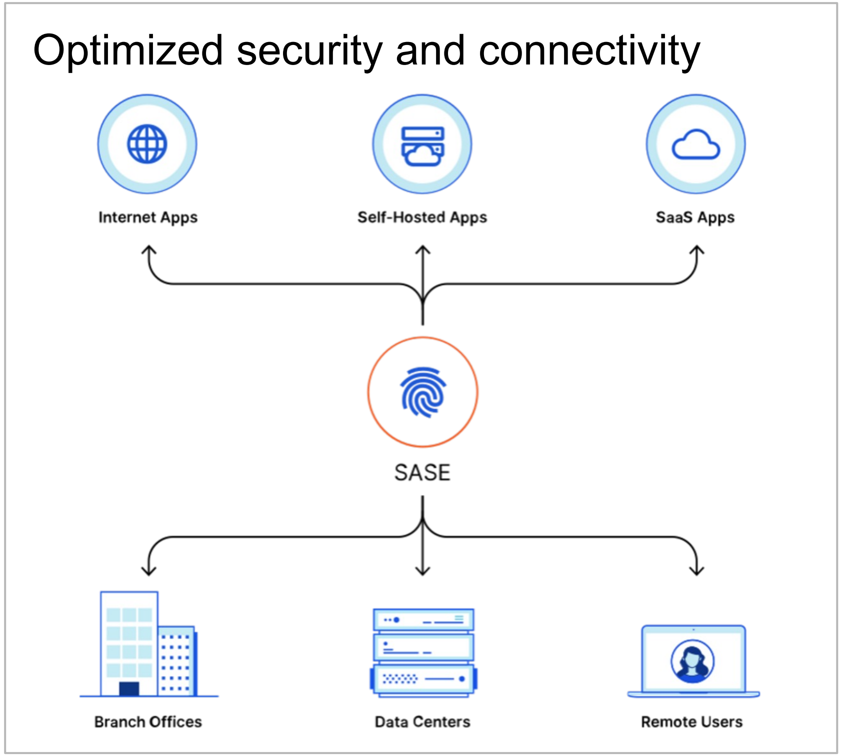
8 Secure app-to-app connectivity across a hybrid cloud environment

9 Eliminate private circuits

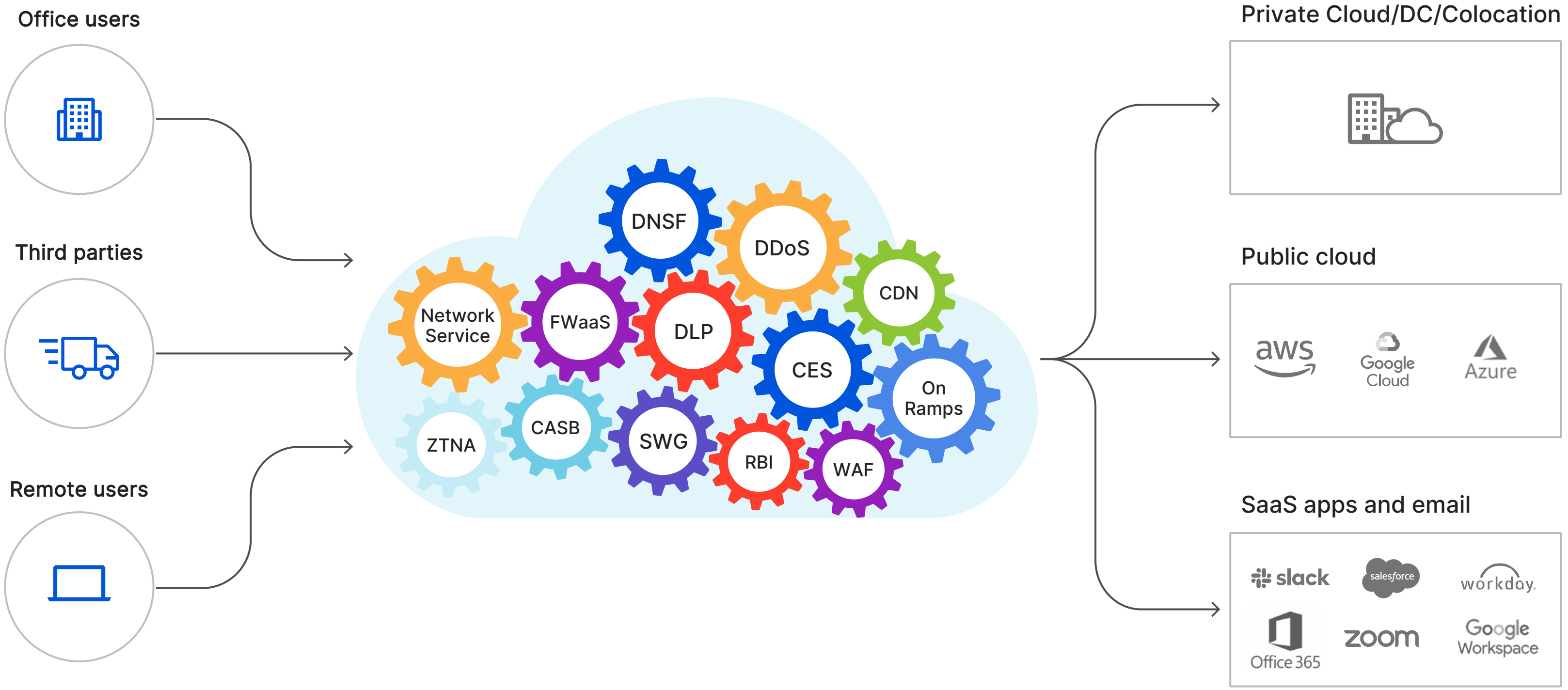
10 Embrace full zero trust security posture

Journey to SASE: End state



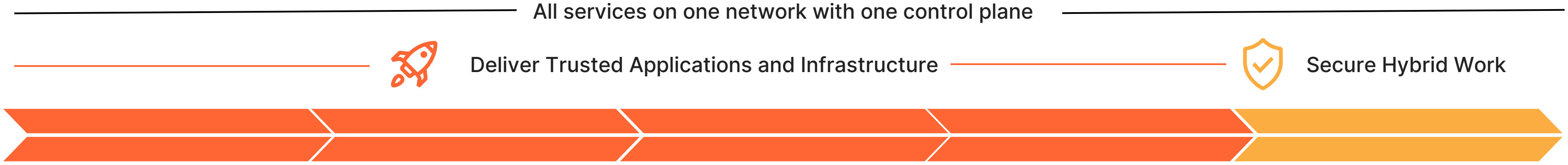


Any-to-any, end-to-end fabric, composable



ANALYST RECOGNITION

Leader in 16 major analyst reports



All services on one network with one control plane

Deliver Trusted Applications and Infrastructure

Secure Hybrid Work

DDoS

2019 IDC MarketScape for DDoS

2020 Frost Radar for Holistic Web Protection

2022 GigaOm Radar for DDoS Protection

CDN

2022 IDC MarketScape for CDN

2022 Frost & Sullivan Global for CDN

2023 GigaOm Radar for CDN

WAF

2022 Forrester Wave™ for WAF

WAAP

2022 Gartner® MQ for WAAP

WAAP =

1. WAF
2. API Protection
3. DDoS Protection
4. Bot Mitigation

ZTNA

2022 KuppingerCole for ZTNA

CLOUDFLARE

Leader in 16 major analyst reports

All services on one network with one control plane

Secure Hybrid Work

Build & Deploy Innovations

ZTNA

2022 KuppingerCole for ZTNA

2023 IDC MarketScape for ZTNA

SSE / SASE

2023 KuppingerCole for SASE

2023 IDC MarketScape for NESaaS

SASE =

1. SWG
2. CASB
3. ZTNA
4. RBI
5. FWaaS
6. SDWAN

Email Security

2023 Forrester Wave™ for Enterprise Email Security

Developer Edge Platforms

2021 Forrester Wave™ for Edge Development Platforms

2023 GigaOm Radar for Edge Platforms

Leader in 16 major analyst reports

All services on one network with one control plane

Breaking Boundaries

Secure Hybrid Work

Build & Deploy Innovations

ZTNA

2022 KuppingerCole for ZTNA

2023 IDC MarketScape for ZTNA

SSE / SASE

2023 KuppingerCole for SASE

2023 IDC MarketScape for NESaaS

SASE =

1. SWG
2. CASB
3. ZTNA
4. RBI
5. FWaaS
6. SDWAN

Email Security

2023 Forrester Wave™ for Enterprise Email Security

Developer Edge Platforms

2021 Forrester Wave™ for Edge Development Platforms

2023 GigaOm Radar for Edge Platforms

Move faster with a platform that constantly delivers innovation

2010
- Launch
- TechCrunch Disrupt's Most Innovative Company 2010

2011
- 100 Billion page views

2012
- WAN Optimization

2013
- Firewall

2014
- Project Galileo
- Fast free SSL

2015
- DNS
- Enter China
- Strategic Parnter investments from Google, Microsoft, Baidu, and Qualcomm

2016
- Network spans to 100th city
- Rate Limiting
- Load balancing

2017
- IoT security
- Intelligent routing
- App platform
- Video services

2018
- DNS Resolver
- IBM Partnership
- Serverless Platform
- Multi-protocol network performance and security

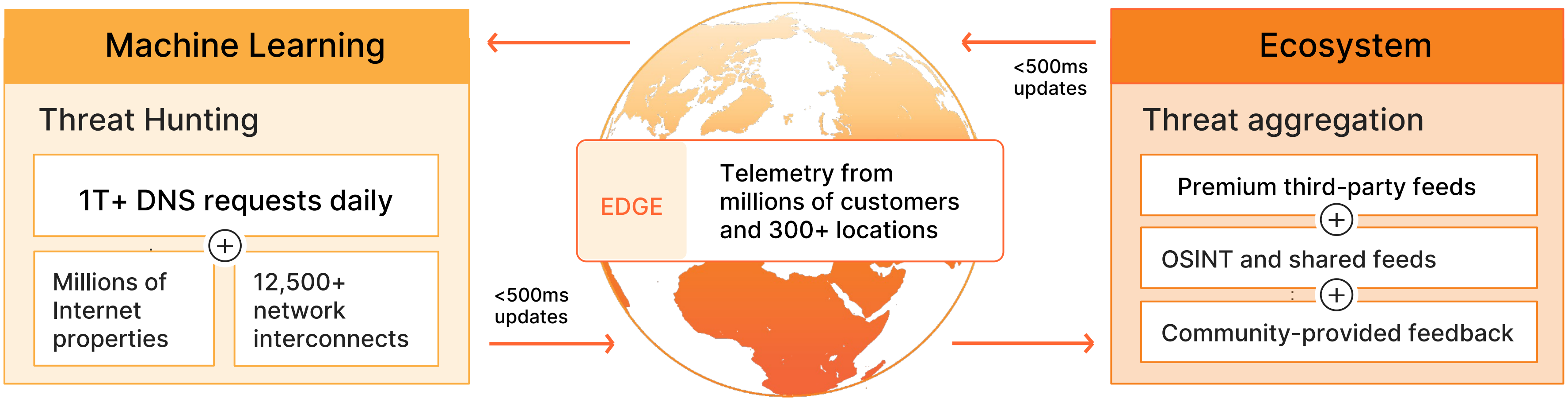
2019
- 1.1.1.1 Mobile App
- Zero Trust Security
- AMP Real URL
- Magic Transit

2020
- Radar
- Workers Unbound
- Data Localization Suite
- Cloudflare for Campaigns
- JD Cloud Partnership
- Network Analytics
- Cloudflare for Teams
- Cloudflare One

2021
- Global Backbone
- Magic Firewall
- FedRAMP Compliant
- Image Optimization
- Signed Exchanges
- Data centers in 250 cites
- Cloudflare for Offices
- Instant Logs & Live Analytics
- 10,000 Network Interconnects

2022
- Logpush for Workers
- Early Hints for Pages
- Relay Workers
- Zero Trust VPN
- Email Routing Insights
- Miniflare
- Unmetered Rate Limiting
- Managed Challenge CAPTCHA
- Hardware Security Keys
- R2 Storage
- $2B Workers Launchpad Fund
- Cloudflare CASB
- API Gateway
- Area 1 Email Security
- Sending Email from workers
- Post-Quantum Cryptography
- Stream Creator management
- Durable Object Alarms
- Cloudflare Queues
- WAF Intelligence Fields
- Backup Certificates
- Dashboard Health Checks

Threat Intelligence: Comprehensive coverage against Internet-borne threats



Machine Learning

Threat Hunting

1T+ DNS requests daily

+

Millions of Internet properties

12,500+ network interconnects

<500ms updates

EDGE

Telemetry from millions of customers and 300+ locations

<500ms updates

Ecosystem

Threat aggregation

Premium third-party feeds

+

OSINT and shared feeds

+

Community-provided feedback

LOG4J — Protecting a full business day faster than leading competitor

Confluence — Protections in place in 30 minutes; attacks began in 3.5 hours

Cloudflare Zero Trust Email Security - Install IT in less than 5 Min !

Phishing risk assessment

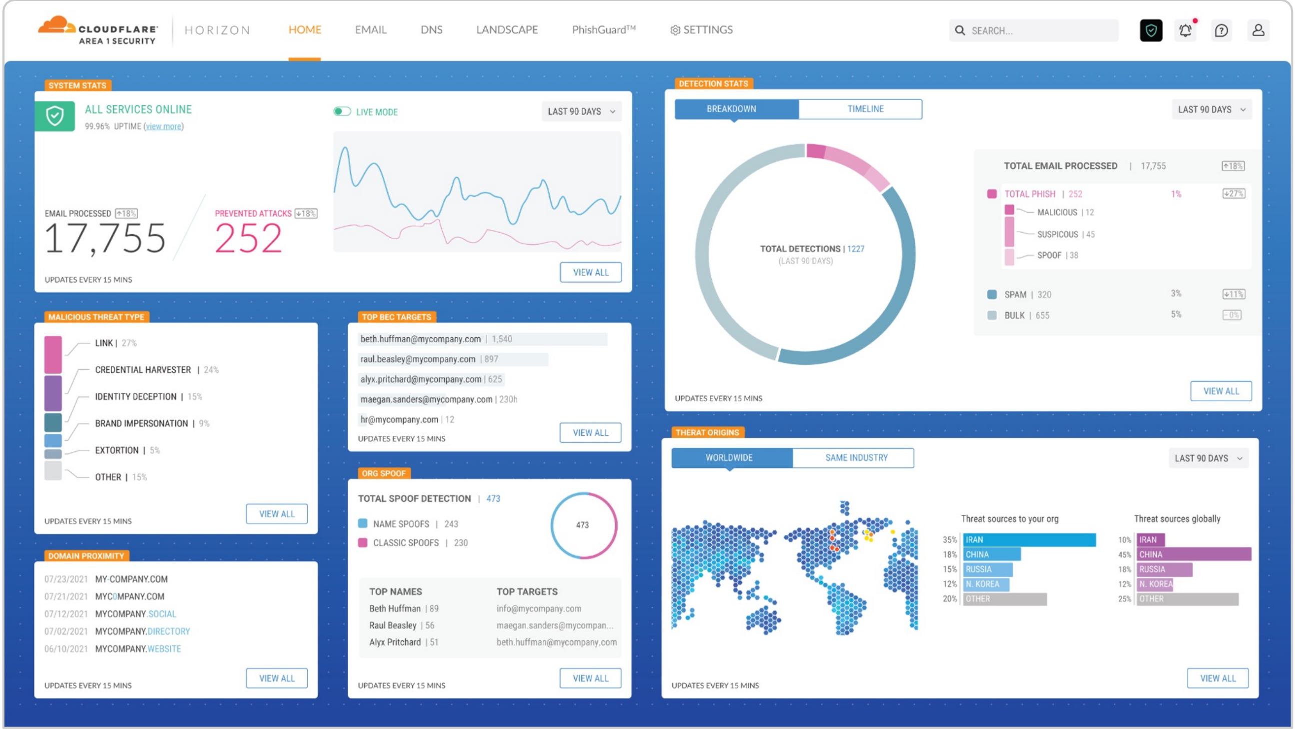
See It.
Believe It.

As little as 5 minutes to set up

(Includes 4 mins for Zoom/Webex/Team)

- Missed Attacks
- Targeted Users
- Fraudulent Payouts
- BEC's
- Contextual Zero day Detection

Attacks, Targets, Trends, Actions…



SYSTEM STATS

ALL SERVICES ONLINE
99.96% UPTIME (view more)

EMAIL PROCESSED ↑18% 17,755

PREVENTED ATTACKS ↓18% 252

UPDATES EVERY 15 MINS

DETECTION STATS

TOTAL DETECTIONS | 1227
(LAST 90 DAYS)

TOTAL EMAIL PROCESSED | 17,755 ↑18%

TOTAL PHISH | 252 1% ↓27%
MALICIOUS | 12
SUSPICOUS | 45
SPOOF | 38

SPAM | 320 3% ↓11%
BULK | 655 5% −0%

UPDATES EVERY 15 MINS

MALICIOUS THREAT TYPE

LINK | 27%
CREDENTIAL HARVESTER | 24%
IDENTITY DECEPTION | 15%
BRAND IMPERSONATION | 9%
EXTORTION | 5%
OTHER | 15%

UPDATES EVERY 15 MINS

TOP BEC TARGETS

beth.huffman@mycompany.com | 1,540
raul.beasley@mycompany.com | 897
alyx.pritchard@mycompany.com | 625
maegan.sanders@mycompany.com | 230h
hr@mycompany.com | 12

UPDATES EVERY 15 MINS

ORG SPOOF

TOTAL SPOOF DETECTION | 473
NAME SPOOFS | 243
CLASSIC SPOOFS | 230
473

TOP NAMES	TOP TARGETS
Beth Huffman | 89	info@mycompany.com
Raul Beasley | 56	maegan.sanders@mycompan...
Alyx Pritchard | 51	beth.huffman@mycompany.com

UPDATES EVERY 15 MINS

DOMAIN PROXIMITY

07/23/2021	MY-COMPANY.COM
07/21/2021	MYC0MPANY.COM
07/12/2021	MYCOMPANY.SOCIAL
07/02/2021	MYCOMPANY.DIRECTORY
06/10/2021	MYCOMPANY.WEBSITE

UPDATES EVERY 15 MINS

THERAT ORIGINS

Threat sources to your org

35%	IRAN
18%	CHINA
15%	RUSSIA
12%	N. KOREA
20%	OTHER

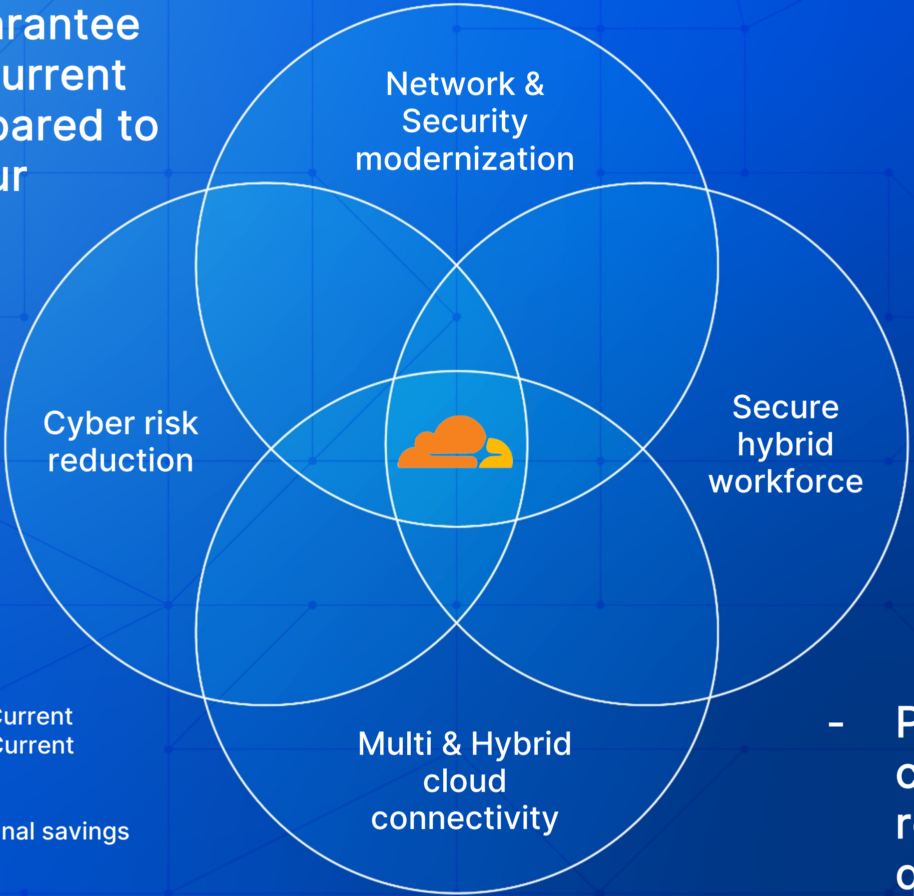
Threat sources globally

10%	IRAN
45%	CHINA
18%	RUSSIA
12%	N. KOREA
25%	OTHER

UPDATES EVERY 15 MINS

- CF1 Deals Ordered during Q4 2023 - We Guarantee reduction of your current TCO by 25% Compared to Renew/Refresh your current platforms

CLOUDFLARE


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

*Depends on : Hardware refresh needed, Current licensing costs, Current operational cost, Current integrations costs.

*ROI assessment is needed to supply the final savings numbers.

- POC install during the conference through remote 15 minutes quick set up.