Cloudflare Zero Trust & SASE

G-Cloud 15

CLOUDFLARE

GCloud 15 Service Definition for Cloudflare Zero Trust & SASE

Cloudflare at a Glance

CLOUDFLARE

Cloudflare One

Cloudflare Zero Trust Services

- Zero Trust Network Access
- Secure Web Gateway
- Cloud Access Security Broker
- Cloud Email Security
- Remote Browser Isolation
- Data Loss Prevention

Cloudflare Network Services

- WAN-as-a-Service
- Firewall-as-a-Service
- L3 & L4 DDoS Protection
- Network Interconnect
- Smart Routing
- IDS/IPS [1]

Cloudflare Application Services

- WAF with API Protection
- 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:** 335+ cities, 95% of population within 50ms, 12,000+ interconnects, 197 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

[1] Contact us to request access

Section

Cloudflare One
SASE / Zero Trust

CLOUDFLARE | PARTNER NETWORK

Cloudflare One is the SASE Solution that offers...

Fastest path to safe AI

Accelerate and secure AI adoption
with visibility and controls across generative and agentic AI

Easiest to use

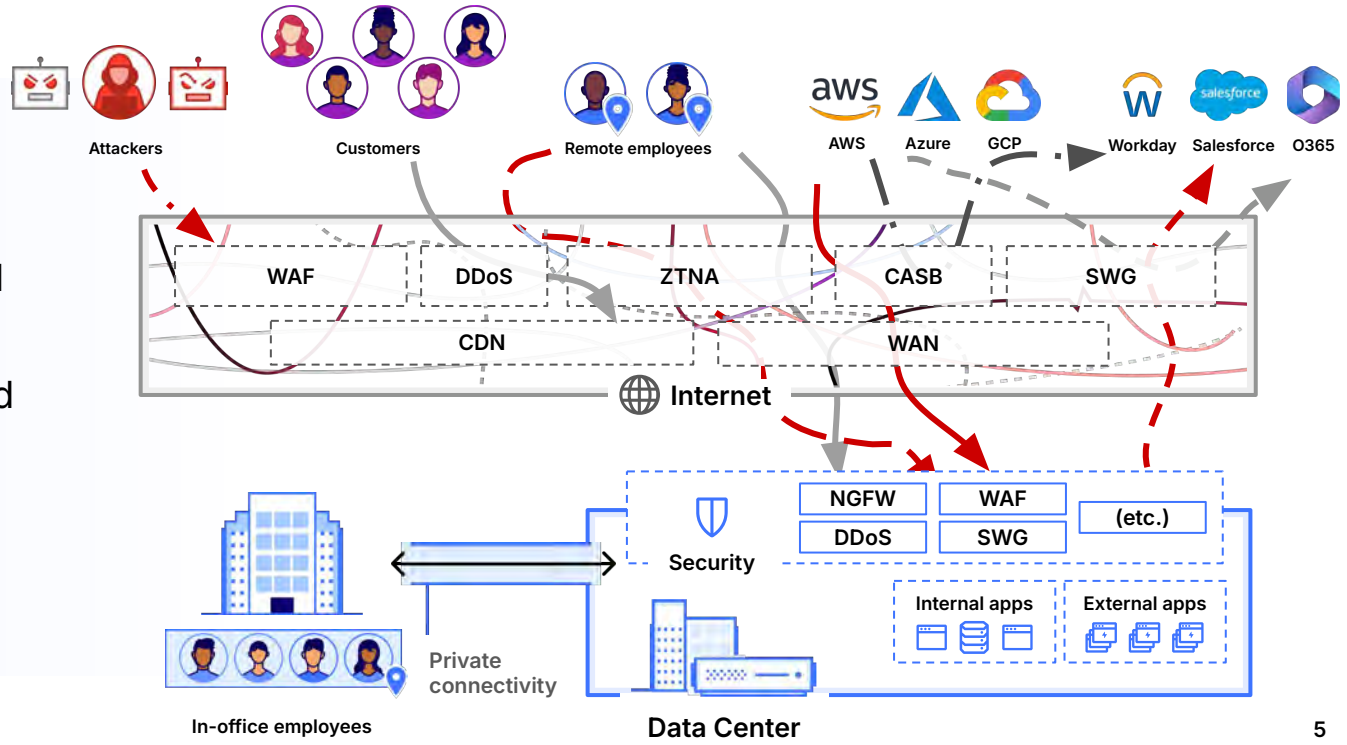
Simplify your SASE journey
with the easiest platform to deploy, manage, and scale

Only composable & programmable platform

Adapt to change with agility
on an unified architecture built for infinite customizability

Legacy networks and point products
hold back digital progress

- Missing visibility or control in infrastructure sprawl
- Ballooning cost of managing legacy and cloud-based, point-product solutions
- Lack of scale and flexibility/agility

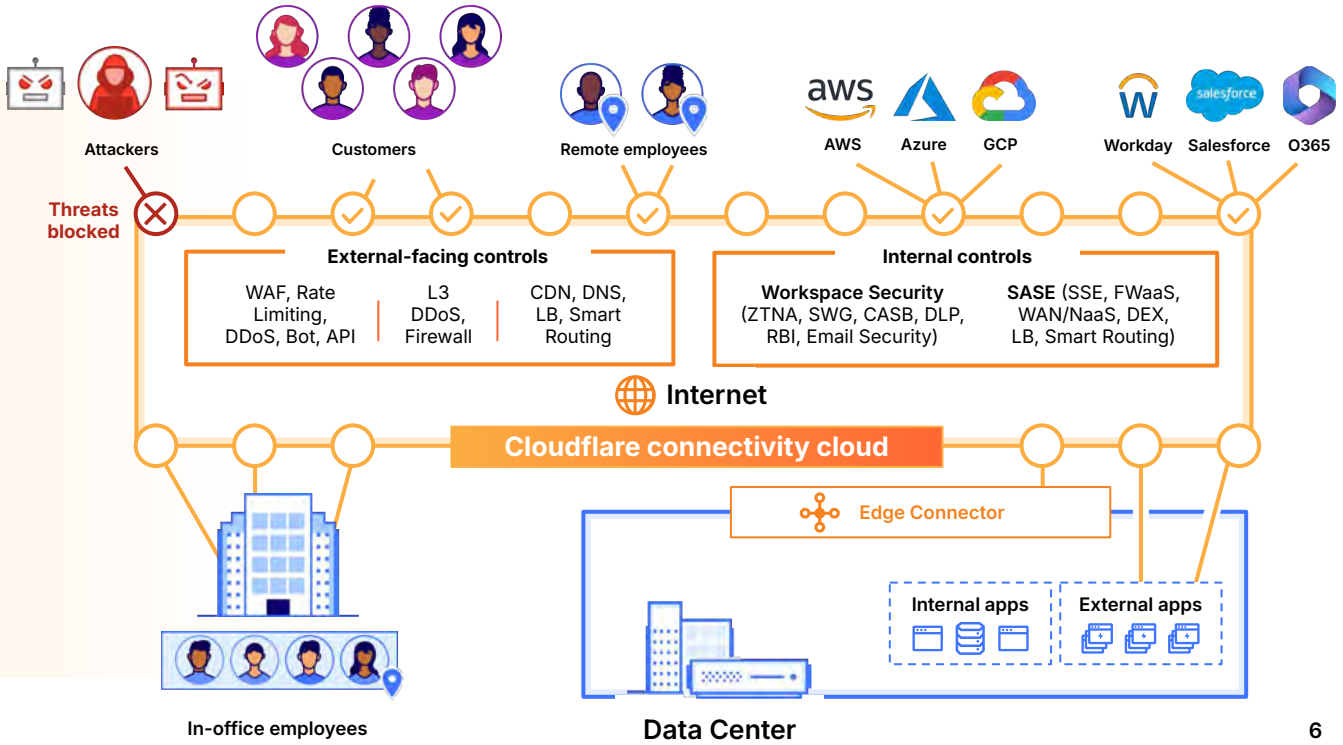


Cloudflare is the only composable, programmable platform that delivers local capabilities with global scale

This enables orgs to...

- ✓ regain control,
- ✓ lower costs, and
- ✓ reduce the risks

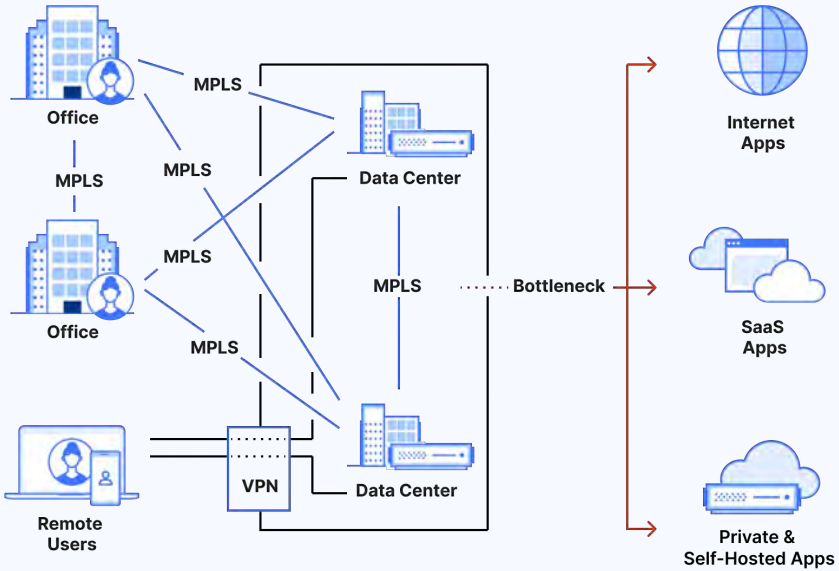
...of a complex and disjointed IT environment



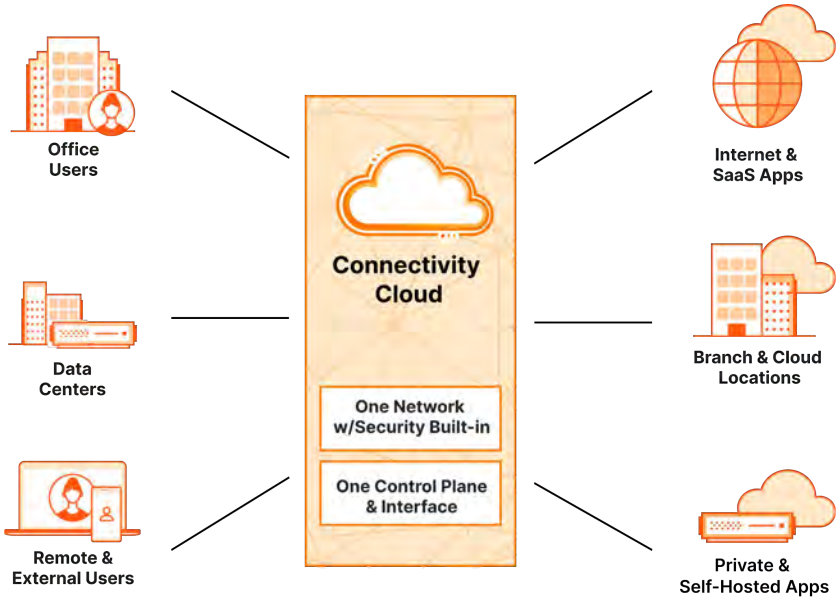
SASE is an architecture design for Zero Trust

CLOUDFLARE

Today's corporate network

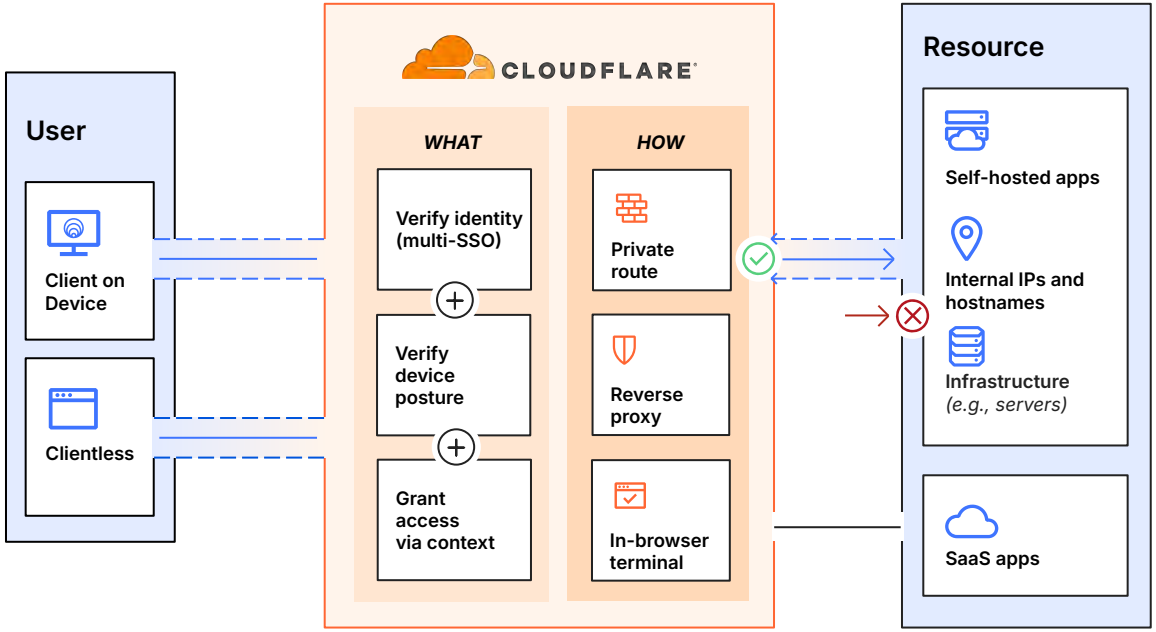


Composable IT



CLOUDFLARE

Simple, secure access



Zero Trust Network Access

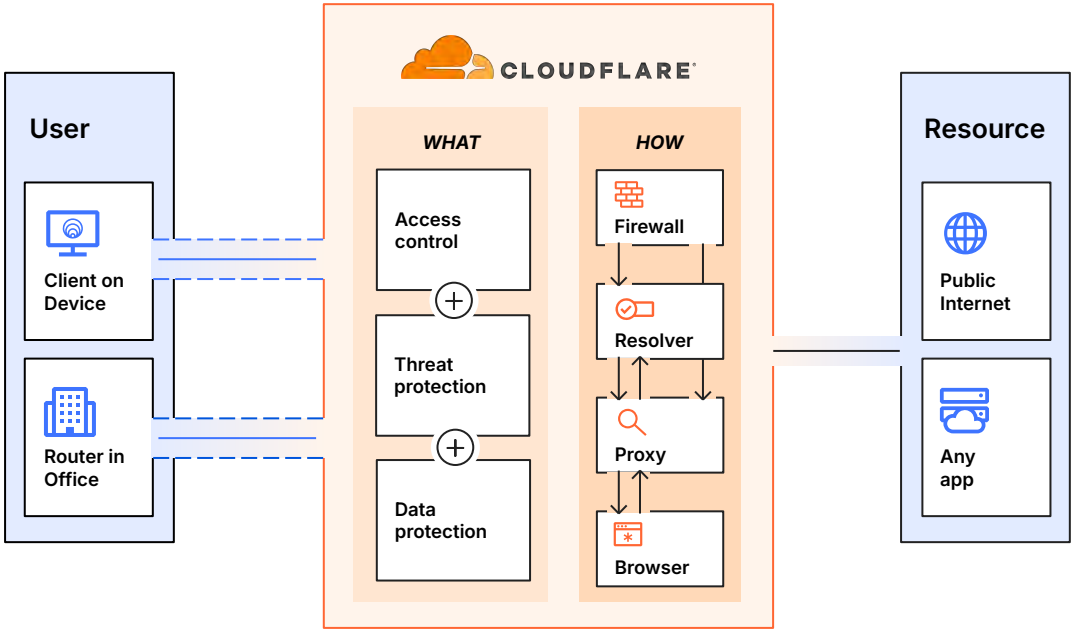
Simplify remote access; augment or replace VPNs

Improve user experience for all (contractors, developers)

Reduce IT / help desk tickets & eliminate lateral movement

CLOUDFLARE

Cyber threat defense



Secure Web Gateway

Simplify policy compliance

Stop phishing

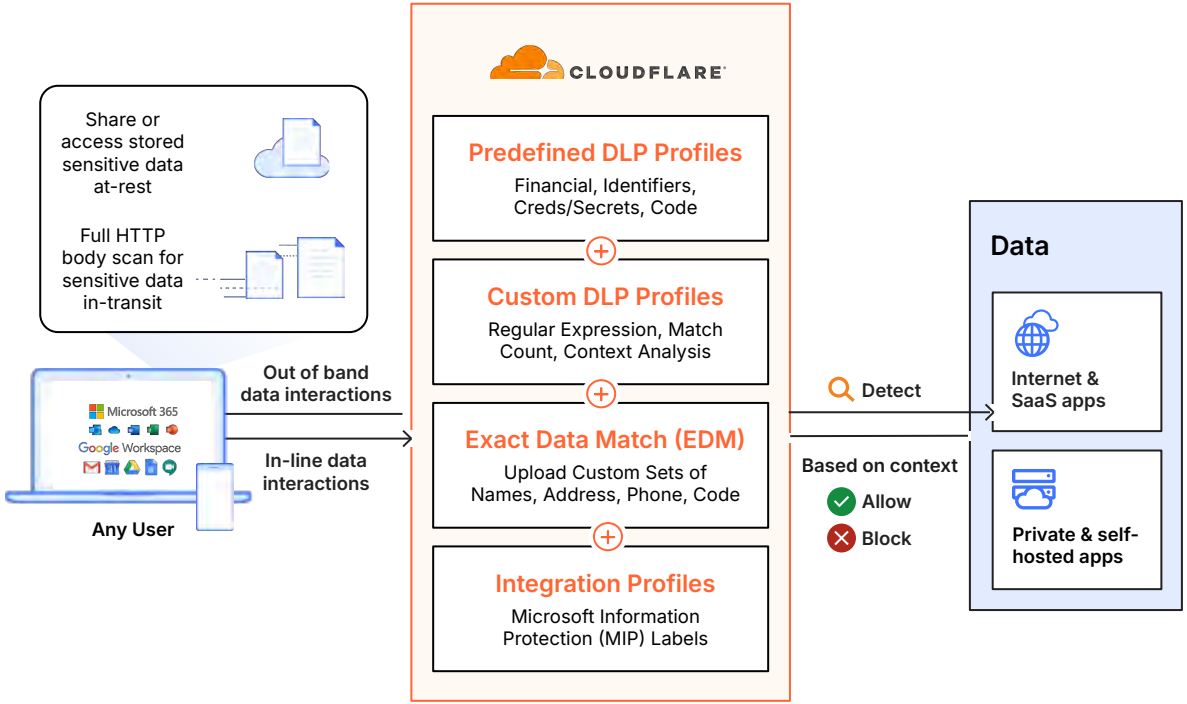
Stop ransomware

Surface Shadow IT

Stop unknown threats

CLOUDFLARE

Data protection



Integrated Data Loss Prevention

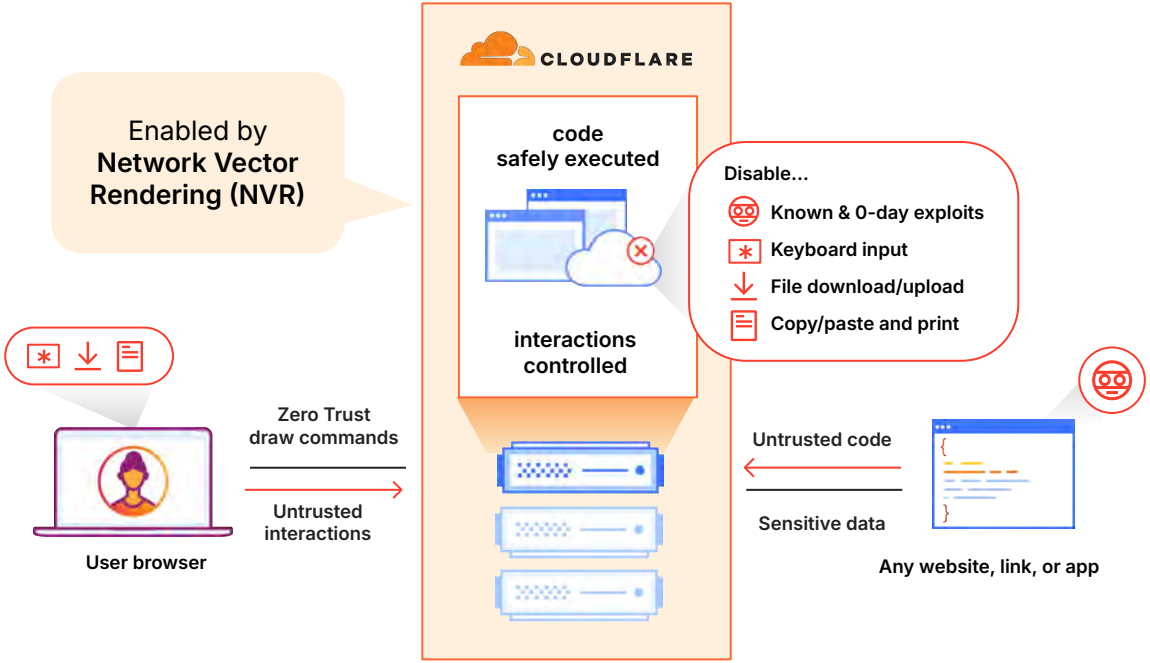
Simplify regulatory compliance

Reduce risk of data leakage and breaches

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

CLOUDFLARE

Simple, secure access with threat & data protection



Remote Browser Isolation

Zero trust web browsing and email links

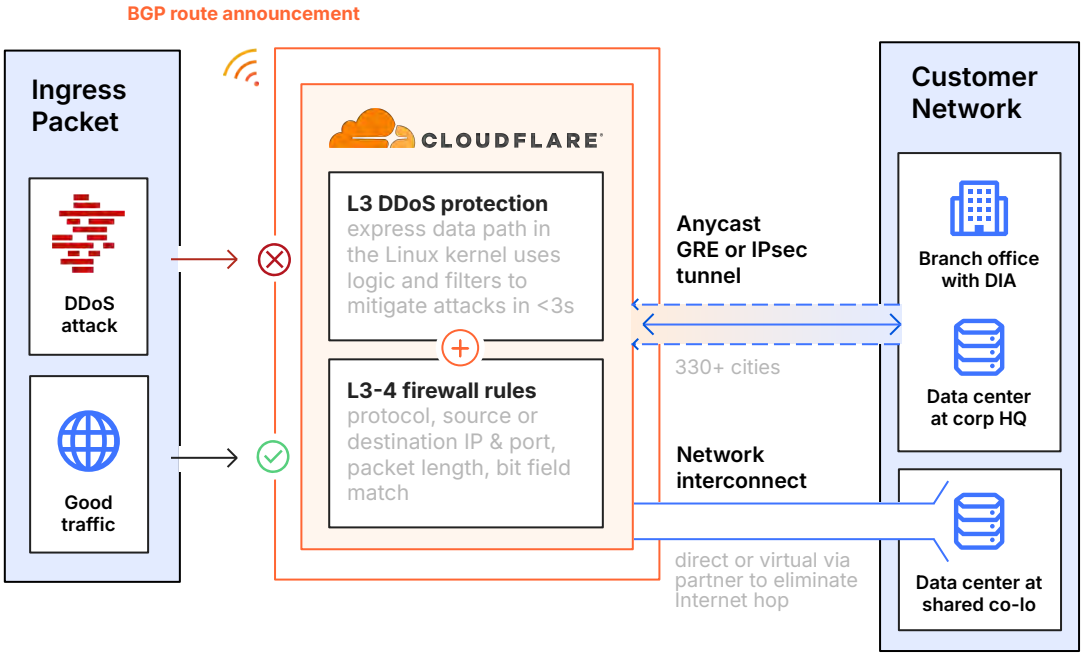
Protect data-in-use

Lightning-fast UX

Compatibility w/all browsers

CLOUDFLARE

Simplify branch connectivity with security built-in



Firewall as a service

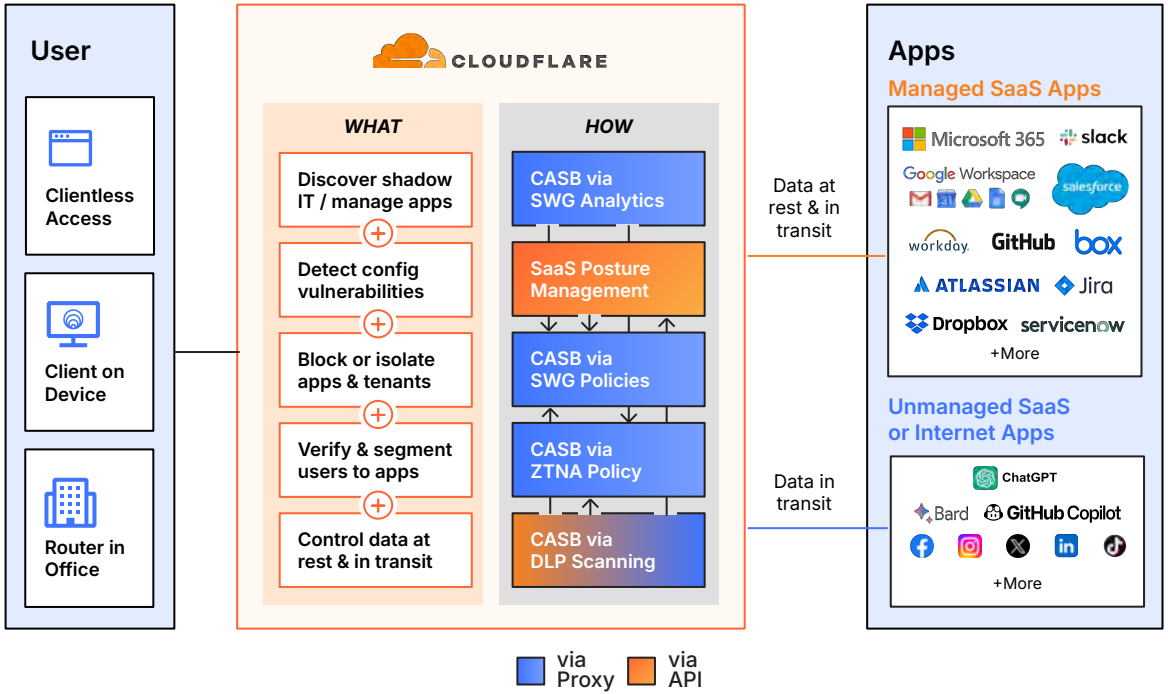
Shifts your network's attack surface to Cloudflare

Stop L3 ransom DDoS and intrusion attacks

Control traffic flows in, out and across your network

CLOUDFLARE

Data protection



Cloud Access Security Broker (multimode)

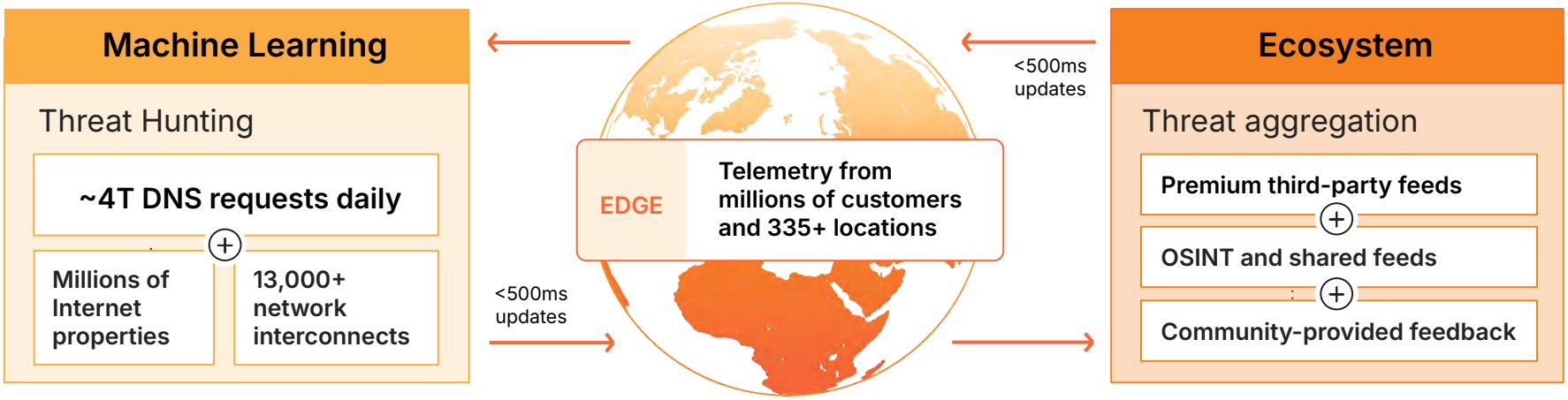
More visibility, less config

Prevent data exfiltration

Quickly identify new risks

CLOUDFLARE

Cyber threat defense with Cloud*force* One



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

Package add-ons

Customer success and support services

Success packages
Maximize value and Cloudflare experience

Standard
Included with every Enterprise subscription and provides the necessities, such as on-demand onboarding modules and priority support.

Premium
Available upgrades for organizations with complex technical environments, or that require high priority support SLAs.

Learn more

Professional services
Advise and assist with planning, configuration, and best practices to accelerate deployment

Quickstart
A solution SME works alongside your team to guide configuration with proven best practices, helping you deploy confidently.

Migration
Expert migration assistance when moving from legacy providers such as Akamai, Fastly, or Zscaler.

Expert
Project managers, consultants, and architects assist with custom, unique use cases, such as highly regulated organizations.

Learn more

Ongoing support services
Focused technical and security operations add-ons

Technical account management
Single point of contact to provide centralized technical support management.

SOC service
Cloudflare-managed SOC providing 24/7 monitoring, detection, and mitigation across yout environment.

Incident response services
On-demand access to incident response experts, helping organizations contain attacks and accelerate recovery.

Learn more: TAM | SOC | IR

WITH YOU, EVERY STEP OF THE WAY

CLOUDFLARE

Ensuring your success

 Community	 Docs	 Resource Hub	 Help Center	 Discord
 Blog	 theNET	 Cloudflare Radar	 CloudflareTV	 YouTube

Roadmap to Zero Trust architecture

cfl.re/zero-trust-roadmap-wp

Then, review our SASE reference 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	

CLOUDFLARE

Service Product Definitions

Application Services Definitions

Application Services	The **Cloudflare application services portfolio** keeps applications and APIs secure and productive, thwarts DDoS attacks, mitigates bots, detects anomalies and malicious payloads, and encrypts data in motion, all while making everything you connect to the Internet private, fast, and reliable. These services run on every server in every data center over our global Anycast network, and all are easy to manage directly from the Cloudflare dashboard.
WAF	Our **Web Application Firewall (WAF)** blocks attacks heading towards applications - including L7 DDoS attacks - and offers better security with sophisticated, layered rulesets.
API Management	**API Management** takes it beyond basic analytics (e.g. viewing the # of exposed APIs or % of API traffic) by including authentication through mutual TLS and a preview of discovery — for instance, identifying the number of endpoints found and showing top X.
Advanced Rate Limiting	**Rate Limiting** provides the ability to limit the rate of requests and gain valuable insights into specific URLs of websites, applications, or API endpoints.
Load Balancing	**Load Balancing** improves application performance and availability by steering traffic away from unhealthy origin servers and dynamically distributing it to the most available and responsive server pools.
Bot Management	**Bot Management** stops malicious bots connecting to web sites, and uses machine learning on a curated subset of hundreds of billions of requests per day to create a reliable bot score for every request.
Advanced DDoS	In addition to protecting against Layer 3 and 4 attacks, including TCP/UDP, Cloudflare **Advanced DDoS** automatically detects sudden changes in traffic and protects against layer 7 DDoS attacks, so they never reach the origin server.
CDN	A **CDN** helps address the challenges customers face around latency, performance, availability, redundancy, security, and costs. A CDN's core goal is to decrease latency and increase performance for websites and applications by caching content as close as possible to end users or those accessing the content.
DNS	**DNS** resolution involves converting a hostname into a computer-friendly IP address. An IP address is given to each device on the Internet. When a user wants to load a webpage, a translation must occur between what a user types into their web browser and the machine-friendly address necessary to locate the example.com webpage.

Application Services Definitions

CLOUDFLARE

Payload Inspection	**Payload Inspection,** is an available feature of the WAF, looks at request body data and headers to determine if they are malicious.
Managed IP Lists	**Managed IP Lists** are WAF managed rulesets created and maintained by Cloudflare and are built based on threat intelligence feeds collected by analyzing patterns and trends observed across the Internet.
Sensitive Data Detection	**Sensitive Data Detection** is a WAF managed ruleset that was created by Cloudflare to address common data loss threats. These rules monitor the download of specific sensitive data — for example, financial and personally identifiable information.
API Shield	**API Shield** helps to identify and address API vulnerabilities and comes with a dedicated certificate authority (CA) to provide strong encryption for mobile applications and IoT device traffic.
Images	**Cloudflare Images** provides an end-to-end solution to build and maintain your image infrastructure from one API.
Stream	**Cloudflare Stream** offers end-to-end video encoding, accelerated global delivery and player for pre-recorded and live content all handled by Cloudflare.
Waiting Room	**Waiting Room** limits the number of users to the origin while placing excess traffic into a Waiting Room to provide a great user experience. This protects customers infrastructure, reduces the number of errors served to users, and acts as an extension of the customer's brand; thereby maintaining a seamless experience.
Account Level WAF	**Account Level Configuration** enables users to configure all application security products (e.g. WAF, Rate Limiting, API Shield) at the account level. This does not remove the granularity of zone-level configuration.

Zero Trust Services Definitions

CLOUDFLARE

Zero Trust Security

Cloudflare Zero Trust is a security platform that raises visibility, eliminates complexity, and reduces risks as remote and office users connect to applications and the Internet. In a single-pass architecture, traffic is verified, filtered, inspected, and isolated from threats. There is no performance trade-off: users connect through data centers nearby in 330+ cities in over 10020
Other providers offer multiple point products to protect from every threat vector, but leave customers to manage their attack surface. Cloudflare's platform stops more attacks by isolating applications and endpoints from the attack surface by shifting it to our edge, and applies threat defenses to shield that edge.

Zero Trust Network Access

Zero Trust Network Access augments or replaces corporate VPN clients by securing SaaS and internal applications. Access works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules limiting access to corporate applications, private IP spaces, and hostnames.

Secure Web Gateway

Secure Web Gateway is our threat and data protection solution. It keeps data safe from malware, ransomware, phishing, command and control, Shadow IT, and other Internet risks over all ports and protocols.

Cloud Access Security Broker (CASB)

A **Cloud Access Security Broker (CASB)** gives customers comprehensive visibility and control over SaaS apps to easily prevent data leaks, block insider threats, and avoid compliance violations.

Cloud Email Security

Cloud Email Security solution crawls the Internet to stop phishing, Business Email Compromise (BEC), and email supply chain attacks at the earliest stage of the attack cycle, and enhances built-in security from cloud email providers.

Remote Browser Isolation

Web browsers are more complex and sophisticated than ever, but represent a large attack surface for businesses. **Remote Browser Isolation** makes web browsing safer and faster, running in the cloud away from your network and endpoints, insulating devices from attacks.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) enables customers to detect and prevent data exfiltration or data destruction. Analyze network traffic and internal "endpoint" devices to identify leakage or loss of confidential information, and stay compliant with industry and data privacy regulations.

Network Services Definitions

CLOUDFLARE

Network Security	The **Cloudflare network security portfolio** exists to secure the networks of modern enterprises, helping to mitigate DDoS attacks, identify malicious traffic patterns, and monitor new and emerging threats. Our solutions offer unified, layered security and can be applied across all endpoints and users — no matter where they're located. Our network solutions are delivered from our global network which operates at massive scale. Every network service - like every Cloudflare service - runs on every server in every data center over our global Anycast network. All are easy to manage from the Cloudflare dashboard, the one pane of glass for all our services.
Magic WAN	Extends the benefits of our network to customers' private networks. **Magic WAN** enables IP level connectivity as well as a full suite of virtual network functions, including IP packet filtering and firewalling, load balancing, and traffic management tools.
Advanced Magic Firewall	**Magic Firewall** is a cloud-based firewall enabling administrators to set policies for all traffic entering and leaving the network.
Magic Transit	Cloudflare **Magic Transit** provides near-instant mitigation of network-layer threats (L3 DDoS attacks) from the Cloudflare global network, alongside next-generation firewall and traffic acceleration.
Network Interconnect	**Cloudflare Network Interconnect** allows our customers to interconnect branch and HQ location directly with Cloudflare wherever they are, bringing Cloudflare's full suite of network functions to their physical network edge.
Smart Routing	**Smart Routing** improves Internet performance by intelligently routing end users through less congested and more reliable paths over the Internet using our network.
Intrusion Detection Systems	**Intrusion Detection Systems (IDS)** is an Advanced Magic Firewall feature you can use to actively monitor for a wide range of known threat signatures in your traffic.

Network Services Definition

CLOUDFLARE

Access	**Access** determines who can reach your application by applying the Access policies you configure.
Gateway	**Gateway**, our comprehensive Secure Web Gateway, allows you to set up policies to inspect DNS, Network, HTTP, and Egress traffic.
Advanced Browser Isolation	**Browser Isolation** complements the Secure Web Gateway and Zero Trust Network Access solutions by executing active webpage content in a secure isolated browser. Executing active content remotely from the endpoint protects users from zero-day attacks and malware.
Cloud Email Security	**Cloud Email Security** solution crawls the Internet to stop phishing, Business Email Compromise (BEC), and email supply chain attacks at the earliest stage of the attack cycle, and enhances built-in security from cloud email providers.
CASB	Cloudflare's **Cloud Access Security Broker (CASB)** service gives comprehensive visibility and control over SaaS apps, so you can easily prevent data leaks and compliance violations. With Zero Trust security, block insider threats, Shadow IT, risky data sharing, and bad actors.
Data Loss Prevention	Cloudflare **Data Loss Prevention (DLP)** allows you to scan your web traffic and SaaS applications for the presence of sensitive data such as social security numbers, financial information, secret keys, and source code.

Matt Johnson
Head of Public Sector

CDS, Yorkshire House, Greek Street, Leeds, LS1 5SH
Email: bidteam@cds.co.uk

Telephone: 07939 866831

Website: www.cds.co.uk