Problem: Complex & disjointed IT

Infosec chaos creates opportunities for attackers

Most IT architectures are too complicated or outdated to enforce security everywhere it should be. Security teams are forced to stitch together siloed tools manually with limited visibility and imprecise controls across environments, slowing down your business.

All this complexity had led to overworked teams, widening vulnerabilities, more damaging attacks and an unsustainable level of resources just to keep up with yesterday's threats.

Solution: Everywhere Security

Simplify your approach with one unified platform

Regain control, lower costs and reduce risks by converging security onto Cloudflare's intelligent platform of programmable, cloud-native services.

Protect your organization everywhere...

- throughout IT environments
- across the attack lifecycle
- and around the world.

Innovation outpaces security

89% of CISOs say digital transformation, which includes experimenting with AI and building new apps, introduces new data risks.

Attack surfaces are expanding

75% of the Fortune 100 operate with hybrid work. New norms like this, plus modern API-first app development, are creating more entry points for attackers.¹

Security teams are struggling

40% of IT & security staff say they are losing control of their environments, while juggling larger workloads and more challenging responsibilities.²

Risks are escalating…

- Protect The Internet
  - WAF/API Security
  - DDoS Protection
  - … more

- Protect Employees
  - SSE Services
  - Email Security
  - … more

- Protect Networks
  - L3 DDoS Protection
  - WAN/FWaaS
  - … more

All services on one network with one control plane
Lifecycle of a cyber attack

Traditional security with point solutions and a flat network architecture makes it easier for cyber attacks to target your IT environment and progress through their lifecycle.

① Discover Attack Surface
Attacks begin by discovering some vulnerability in your expanding attack surface.
As IT environments sprawl, these entry points multiply, including exposed IPs and IT assets with misconfigurations or vulnerabilities in a FW/VPN, self-hosted app/API, SaaS app or web browser.

② Initial Compromise
Attackers then exploit that entry point to gain a foothold in your IT environment.
Tactics include phishing credentials from users or exploiting apps via API abuse or credential stuffing.
Outdated tooling typically leaves more vulnerabilities and security gaps for compromise.

③ Lateral Movement
Once inside, attackers often move laterally and escalate privileges within your environment to reach their desired target.
Flat, unsegmented architectures with default-allow access to resources make this phase easy.

④ Exfiltration & Extortion
Typically, attackers end their campaign by stealing your money or data or by leaving your business in disarray via sabotage.
Other times, they communicate outbound to command-and-control servers to execute additional attacks.
Everywhere Security neutralizes the attack lifecycle

Via a single platform, Cloudflare helps neutralize cyber attacks everywhere, across every stage of the attack lifecycle and for any endpoint, infrastructure or resource.

1 Minimize Attack Surface
When you connect networks and apps to Cloudflare, you minimize your attack surface by hiding IP addresses, configurations and IT assets. Isolate web browsing on our network edge to insulate users and devices from threat or data risks.

2 Prevent Initial Compromise
Protect the entire corporate network and everything you connect to the Internet with L3-L7 services to mitigate inbound risks. Inspect all encrypted traffic, where most threats lurk — even when the latest cryptography is used.

3 Eliminate Lateral Movement
Eliminate lateral movement with Zero Trust best practices of default-deny and least-privilege. Progressively adopt identity- and context-based controls to secure access across environments.

4 Stop Exfiltration & Extortion
Regain visibility and controls over your data to stop exfiltration or fraud and to mitigate exposure risk. Adapt to risks with agility by extending Zero Trust principles with composable capabilities across web, private, and SaaS apps.

4 Stop Exfiltration & Extortion
L7 data protections • Data in transit & in use controls
Data at rest visibility

3 Eliminate Lateral Movement
L4-7 secure access • Default-deny privilege
Log & segment granted access
Benefits

By reducing complexity and delivering security everywhere, Cloudflare helps CISOs accelerate their strategic priorities and modernize their business with tangible results.

CISO AGENDA

Reduce Cyber Risk
Digital Transformation
Control Operational Costs
Innovation and AI

OUTCOMES WITH CLOUDFLARE

Improve posture 90% reduced malicious traffic
Regain operational control 73% Reduced time spent managing security tools
Vendor & platform consolidation 50% Total cost of ownership (TCO) reduction
More productive user experiences 95% of world’s Internet users within 50ms of our network

The Cloudflare difference

Unified & composable platform
Converge web app & API protection (WAAP), security services edge (SSE), email security and more security domains on one platform and control plane.
Limitless interoperability between all services and flexible integrations with third-party tools, so security can adapt quickly to new risks.

Mass scale threat intelligence
Cloudflare’s threat intel is based on a high volume and variety of global traffic, including:
- 20% of the Internet
- 2TB DNS queries / day
- 8B+ pages crawled every two weeks
This unique real-time visibility powers AI/ML-backed models to defend against emerging and zero-day threats.

A network built to scale
Deliver local capabilities with global scale:
- 310+ network locations
- 120+ countries
- 228 Tbps capacity
- 13K+ interconnects
Every security service is available for customers to run in every location, such that single-pass inspection and policy enforcement is always fast, consistent and resilient.
Customer stories

How Cloudflare helps organizations **protect their attack surface**

- **Homeland Security**
  
  **100+**
  
  U.S. civilian agencies with office locations secured with Cloudflare's DNS filtering
  
  Learn more

- **GPC**
  
  **450M**
  
  Threats blocked in one year across 900+ web properties
  
  Learn more

How Cloudflare helps **stop zero-day threats**

- **HTTP/2 Rapid Reset zero day**
  
  In Aug. 2023, Cloudflare helped to discover CVE-2023-44487 and mitigated the largest DDoS attacks on our record.
  
  **201M** requests per second peak. 3x previous record.
  
  Learn more

- **Ivanti Connect Secure zero day**
  
  Cloudflare's AI-enabled WAF proactively defends against attacks on two recently discovered zero-day vulnerabilities affecting Ivanti products.
  
  **<24** hours after CVEs published, new WAF rules are available.
  
  Learn more

How Cloudflare helps organizations **adopt Zero Trust**

- **Fortune 500**
  
  **100K+** hybrid workers protected.
  
  Fortune 500 telecom secured Internet and app access with Zero Trust and replaced Cisco.
  
  Learn more

- **Bouvet**

  Scandinavian IT consultancy

  “We depend on Cloudflare to reduce our attack surface by securing our ports, filtering threats, and cleaning up our traffic.”

  — Victor Persson, Security Operations Lead

  Learn more
The Cloudflare cybersecurity portfolio

Unify your security approach with web app and API protection (WAAP), security services edge (SSE), email security & many more domains. Adopt new capabilities at your own pace.

**Protect The Internet**
Defend sites, apps & APIs across self-hosted, SaaS, and cloud environments
- WAF
- API Security
- Bot Management
- L7 DDoS Protection
- Client-Side Security
- Attack Surface Mgmt

**Protect Employees**
Secure any worker anywhere, with a fast, consistent experience
- Secure Access
- Internet Gateway
- CASB
- Email Security
- Browser Isolation
- DLP

**Protect Networks**
Safer and faster connectivity across data centers, offices, and clouds
- WANaaS
- FWaaS
- L3 DDoS Protection
- Network Interconnect
- Smart Routing
- IDS/IPS

All services on one network with one control plane

Cloudflare Global Network

**Simplify security.**
Consolidate vendors to reduce complexity and enterprise risk.

**See more, protect more.**
Leverage real-time threat intelligence from a massive global network.

**Scale everywhere.**
Resilient protections across any location around the world.

---

1. [BuildRemote.com](#)
2. [Forrester Consulting](#)
3. [Salt, State of the CISO 2023](#)
4. Based on average across 4 case studies
5. Based on customer survey data collected through TechValidate (June-August 2023)
6. [TechValidate survey](#)