



EBOOK

Everywhere Security

Protecting modern organizations from threats
without stifling innovation



Complex, disjointed security creates opportunities for attackers



The pursuit of innovation creates risks that ripple throughout an organization.

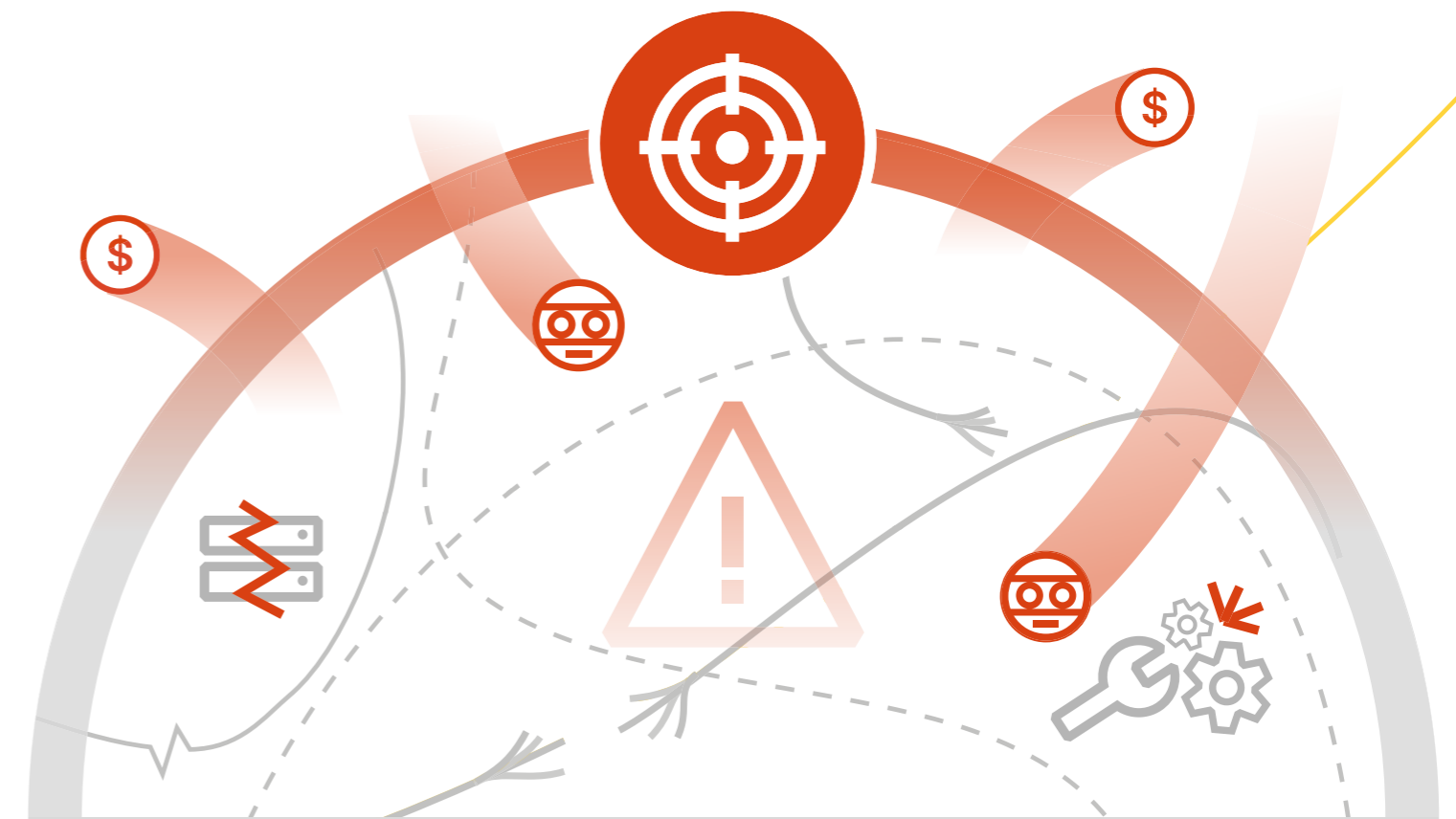
Driven by digital transformation goals, enterprises build new web apps, extend integrations with customers and partners through APIs, and experiment with emerging technologies like AI. These investments improve customer experiences and generate revenue but also represent new targets for attackers.

The traditional corporate network has also dissolved due to a variety of factors synonymous with business today: hybrid work, bring your own device (BYOD) policies, the popularity of SaaS apps, and sprawling IT environments consisting of hybrid and multi-cloud cloud architectures.

With attack surfaces expanding so rapidly, threat actors are taking advantage and expanding their arsenal of techniques to deal more damage with supply chain attacks, multi-channel phishing, and even AI-enabled social engineering.

Unfortunately, many organizations are struggling to evolve their security in the face of these changes. Too often, IT and security teams rely on disjointed and inflexible point solutions that lead to more security gaps, more management overhead, and more incompatibilities between technologies. Overall, this complexity makes it hard to extend visibility and controls throughout all environments, making organizations more vulnerable and holding back business growth.

This ebook describes a strategy — **“Everywhere Security”** — for reducing all of this complexity and confusion, without limiting an organization’s ability to innovate.



Challenges facing modern organizations



Security risks are escalating for organizations across industries, regions, and maturities:



Expanding attack surfaces create more entry points

75% of the Fortune 100 operate with hybrid workforces.¹

98% of enterprises have adopted or plan to adopt multi-cloud infrastructure.²

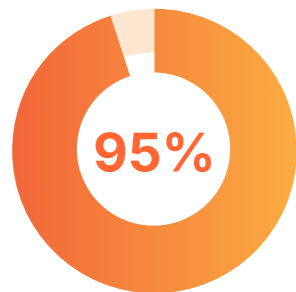


Complex and disjointed defenses widen security gaps

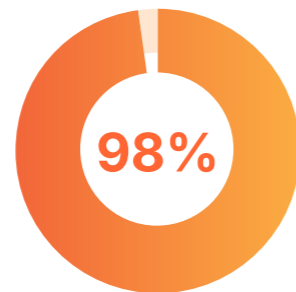
Security teams typically deploy **20 to 50** discrete cybersecurity solutions.³

40% of IT security teams feel they are losing control over their environments.⁴

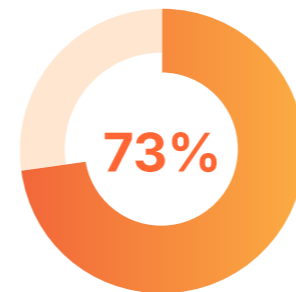
These trends increase risks, which result in dire consequences:



of breached organizations experienced more than one data breach.⁵



of organizations have a relationship with a vendor that experienced a breach within the last two years.⁶



of all organizations fell victim to a ransomware attack in 2023.⁷

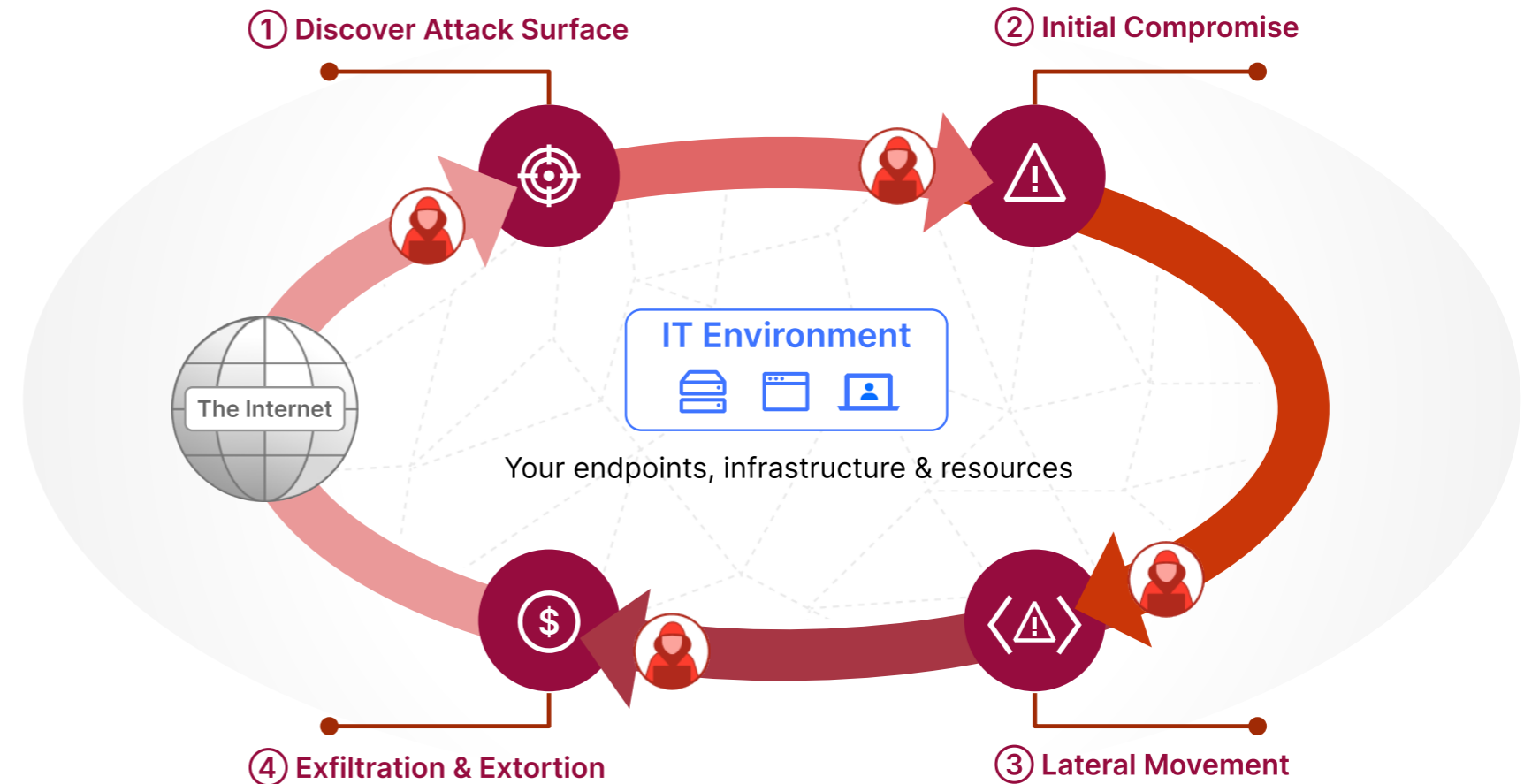
The lifecycle of a cyberattack in 4 phases

The chaos of running a modern business creates opportunities for cyber attacks.

The risks these attacks pose can be categorized into three main categories:

- **Inbound risks** that attack your organization externally (e.g. API abuse, email phishing, DDoS, bot attacks, etc.)
- **Browsing risks** that users encounter on the Internet (e.g. drive-by malware, threats in encrypted traffic)
- **Outbound risks** posed by traffic leaving your organization (e.g. data loss/exposure, noncompliance)

Although the specific techniques and actors involved can vary enormously, all cyber attacks tend to follow the same lifecycle — a sequence of events that breaks down into four phases:







- Phase ①** Attackers begin by discovering vulnerabilities and exposures in your IT environment — all the technologies your organization needs to operate — including your corporate network, cloud instances, applications (SaaS, public, private), physical locations, and users.
- Phase ②** Attackers exploit unpatched vulnerabilities and security gaps, leveraging tactics such as stealing credentials from users or exploiting APIs to access apps.
- Phase ③** Attackers move laterally within your infrastructure and escalate privileges to reach their target systems and data.
- Phase ④** Attackers typically end campaigns by stealing money or data. Other times, they will sabotage your IT to leave your business in disarray or communicate outbound to command-and-control servers to execute later attack stages.

How traditional security empowers attackers



Managing disjointed point solutions and a traditional, flat network architecture put extra strain on each stage of the attack lifecycle:

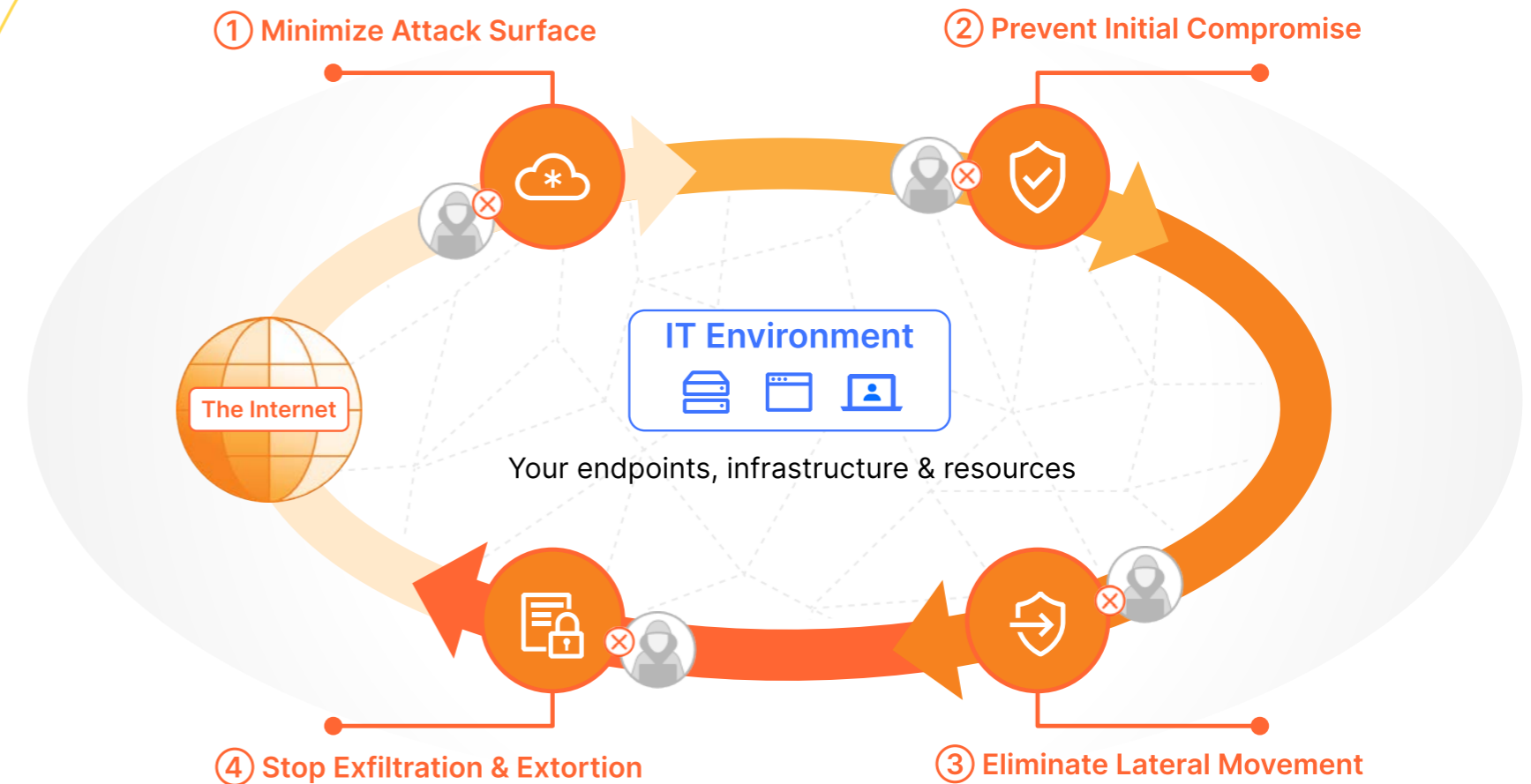
Attack Phase	Complication	Consequences
 Discover attack surface	IT sprawl multiplies entry points for attackers. Disparate, perimeter-based security services make it hard to even identify what IT assets pose the most risks.	<ul style="list-style-type: none">• Higher likelihood of exposed IT assets or unpatched vulnerabilities.• Poor visibility or controls across IT environments.
 Initial compromise	Outdated tooling typically leaves more unpatched vulnerabilities and security gaps for compromise.	<ul style="list-style-type: none">• Slower time-to-mitigation.• Legacy security tools themselves become targets for compromise.
 Lateral movement	Perimeter-based, unsegmented security with default-allow access to resources make lateral movement easy.	<ul style="list-style-type: none">• Attackers traversing the network remain in the network or application for longer.• Harder to track attacker movements.
 Exfiltration and extortion	Limited visibility and controls across environments make it difficult to prevent exfiltration and extortion.	<ul style="list-style-type: none">• Attackers have more time to locate and exfiltrate sensitive data.• Teams struggle to understand the attack's impact.

Everywhere Security: Protecting organizations from threats

An Everywhere Security model neutralizes attackers across all phases of the attack lifecycle. In this model, an organization unifies protections across IT environments and geographies onto a using a single platform:

- Unites point solutions across multiple security domains (e.g. network security, application security, data security, and more).
- Provides flexible design with composable services that are interoperable with each other and with any piece of third-party infrastructure.
- Incorporates real-time threat intelligence based on a large volumes of high-quality data.
- Scales automatically to deliver consistent protections across locations without backhauling traffic to specialized data centers.

An Everywhere Security approach simplifies protection at every stage:



Phase ① **Minimizes attack surfaces** by hiding IP addresses, configurations, and assets from discovery and by isolating web browsing to insulate devices from threats.

Phase ② **Prevents initial compromise** with L3-L7 protections spanning the corporate network and anything connected to the Internet while also inspecting all encrypted traffic, where most threats lurk.

Phase ③ **Eliminates lateral movement** by extending Zero Trust principle of default-deny and least privilege to enforce identity- and context-based access controls.

Phase ④ **Stops exfiltration and extortion** by providing controls over data across all environments.

Everywhere Security facilitates strategic priorities



An Everywhere Security approach simplifies the path to achieve key goals:



Protect attack surface

An Everywhere Security approach helps organizations enforce protections across attack vectors, which span employees, networks, websites, apps, and APIs connected to the Internet. In this way, organizations can feel secure in diversifying their digital footprints.



Stop zero-day attacks

An Everywhere Security approach helps organizations quickly detect and automatically mitigate zero-day attacks on web apps and APIs based on threat intelligence. Enforcing these protections before vulnerability patches are available augments the productivity of security teams.



Adopt Zero Trust

An Everywhere Security approach offers the fastest path to Zero Trust adoption, enabling organizations to simplify how they secure hybrid work while reducing their attack surface.

How Cloudflare delivers Everywhere Security



A unified and composable platform

Cloudflare converges security services across web application and API protection (WAAP), security services edge (SSE), email security, and more onto a single platform and network control plane.

With limitless interoperability among all services and flexible integrations with other third-party tools, security teams can adapt quickly to new risks and simplify key workflows.



Unique threat intelligence visibility

Cloudflare generates threat intelligence by analyzing a high volume and variety of global traffic seen by our global network, such as ~20% of all Internet traffic and ~3TB of DNS queries every day.

This real-time visibility powers AI/machine learning models that help us identify and stop billions of cyber threats each day, including zero days.



A network built for scale

With a network that spans 310+ cities in over 120 countries and has 13K+ interconnects, Cloudflare provides local security capabilities at a global scale.

Every service is available for customers to run in every location, such that single-pass inspection and policy enforcement are always fast, consistent, and resilient everywhere your organization needs protection.

Delivered on one network and one control plane

The benefits of Everywhere Security with Cloudflare



Regain operational control

Cloudflare restores visibility and controls to defend against threats throughout all phases of the attack chain.

Our unified platform connects and protects the Internet, employees and networks across all endpoints and infrastructure in any location. Composable services with flexible integrations enable you to extend protections at your own pace.



Improve security posture

Cloudflare protects the most critical entry points into your organization with best-in-class threat intelligence backed by AI/ML threat hunting models.

Moreover, the platform makes it easy to adopt security best practices like Zero Trust across your distributed environments to further minimize risk.



Accelerate vendor and platform consolidation

Cloudflare reduces operational overhead by converging multiple security capabilities onto a single platform and control plane.

In this way, organizations can reduce reliance on (and even eliminate) multiple, overlapping tools that introduce redundancy, security blind spots, and hidden costs.



Enhance end user experiences

Cloudflare makes it easy to layer rigorous controls with single-pass inspection across environments to ensure business continuity without security getting in the way.

Protections are enforced close to protected users and resources so the experience is fast and frictionless.



Deliver security at scale

Cloudflare scales with the growth of your digital footprint — without sacrificing connectivity and performance.

As the volume of users and the need for new apps increases, we ensure scalability with consistent, fast and seamless experiences along with increased visibility to simplify operations and troubleshooting.

Cloudflare from the customer perspective



Customer surveys compiled by TechValidate demonstrate the value customers realize by relying on Cloudflare for Everywhere Security:

- Reduces unprotected API endpoints by **57%**
- Improves response times to application security incidents by up to **75%**
- Increases incident response time for network attacks by up to **75%**
- Improves average time to recover from security and performance incidents by up to **50%**

“Our busiest website is hit by approximately 57 million threats each and every month. And Cloudflare blocks all 57 million every month. I know this because Cloudflare’s security insights technology shows me exactly what’s happening across the entire digital footprint.”

Damien Apone
Global Director of Governance, Risk, Compliance, and Security
GPC

Customer successes

- ✓ **Genuine Parts Company (GPC), a Fortune 200 automotive parts company,** collaborated with Cloudflare to create a cohesive security posture across its global e-commerce footprint of 900+ sites. Blocking 450 million threats (including millions of bots) in the first year reduced latency and improved customer experiences. In addition, the discovery of screen scraping by a competitor enabled the blocking of malicious competitive activities and access to private company information.



- ✓ Cloudflare empowered **NCR Voyix, a leading retail technology company,** to fight sophisticated payment fraud and protect customers from bad bots, fraudulent transactions, and business disruption. The company consolidated five security services onto Cloudflare to increase operational efficiency by freeing up critical IT team time. These security improvements have also reduced payment card chargebacks.

NCR VOYIX

Getting started with Everywhere Security



Cloudflare offers composable, scalable Everywhere Security to help reduce complexity and accelerate business innovation. Our cloud platform unifies many security capabilities and harnesses real-time threat intelligence to enforce low-touch, high-efficacy protections across the Internet, employees, and corporate networks.



[Explore how to enforce security without compromising innovation](#)



[Contact us today for a consultation](#)



Unified Global Security Platform

Protect The Internet

Defend sites, apps and 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

Citations

1. [Fortune 100 Return To Office Policy Tracker](#), by Henry O’Laughlin, Buildremote, February 2024.
2. [98% of Enterprises Using Public Cloud Have Adopted a Multicloud Infrastructure Provider Strategy](#), Oracle, February 2023.
3. [2023 Review: Reflecting on Cybersecurity Trends](#), by Greg Young and William Malik, Trend Micro, December 2023.
4. [Regaining control with a connectivity cloud](#), Forrester Research, August 2023.
5. [Cost of a Data Breach Report 2023](#), IBM.
6. [SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party](#), SecurityScorecard, February 2023.
7. [Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023](#), Statista, by Ani Petrosyan, Statista, October 2023.

© 2024 Cloudflare Inc. All rights reserved.

The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.