CLOUDFLARE

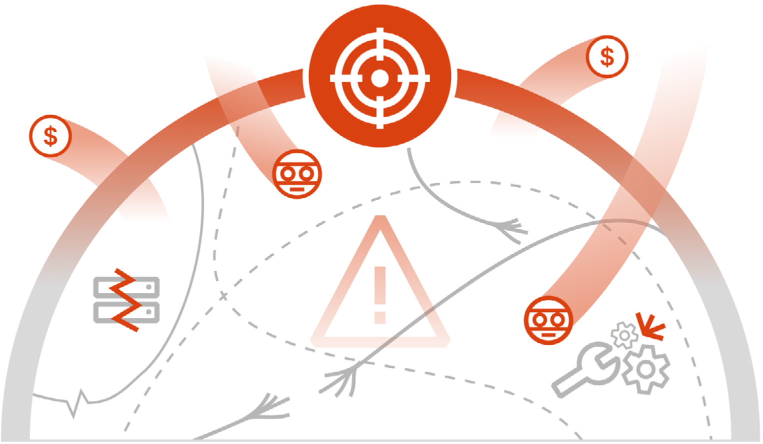
SOLUTION BRIEF

Protect your Attack Surface with Everywhere Security

Discover and manage risks before attackers find them first

The challenges of ever expanding attack surface

While distributed operations and digital modernization initiatives offer greater flexibility and scalability, they also present a complex set of security challenges that require new strategies and controls to ensure robust defense measures across an increasingly insecure environment. Every Internet-connected resource expands the attack surface: instead of relying on a "castle-and-moat" security model, enterprises have to protect employees, apps, data, and networks everywhere.



Examples of security threats point solutions fail to address

Multi-channel phishing attempts to engage victims across multiple communication channels — email, web links, cloud collaboration tools, mobile/SMS, and other Internet-connected tools.

API

Business logic-based fraud exploits how public-facing APIs are designed. Modern apps use APIs to automate certain workflows like account setup, logins, and payment transactions. However, malicious bots can manipulate an API's business logic to steal credentials through brute force attacks, deploy hypervolumetric DDoS attacks, and more.

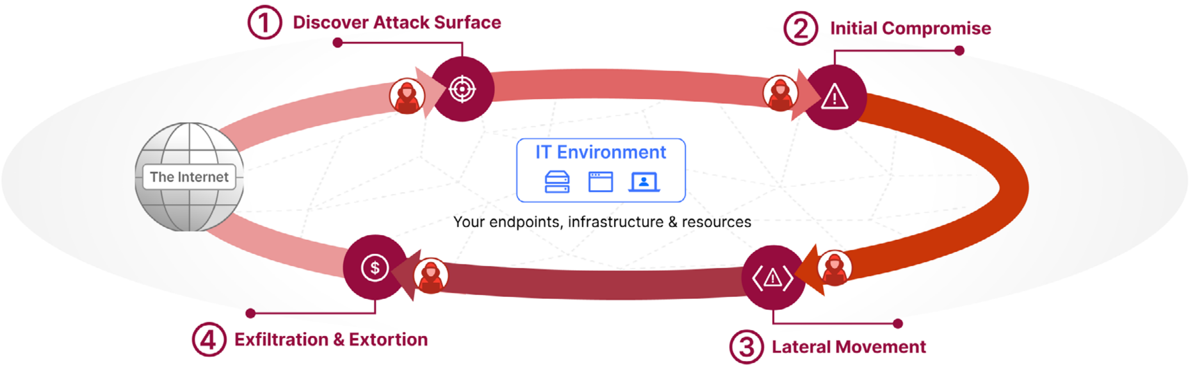
AI-related data leakage, such as when an engineer accidentally uploaded internal Samsung source code to ChatGPT, can increase as organizations increase their AI usage. AI risks can also be malicious; for example, large language models (LLMs) can be hijacked to perform unauthorized actions.

Problem: Hardware based point solutions with traditional flat network architectures have failed to address the needs of modern business

Traditional network architecture with point solutions puts everything within the network – users, applications and devices – onto one flat plane. As cyber threats continue to increase in type and scope, organizations are finding that traditional security approaches are rapidly reaching their limits. Historically, the instinctive response to new threats has been to layer on additional security solutions. Each emerging vulnerability or attack vector would be met with another specialized tool, leading to a patchwork of costly and often complex security controls and workflows.

As cyberattacks become more sophisticated, users work from everywhere, and apps are increasingly in the cloud, these fragmented solutions can lead to operational silos, gaps in visibility and protection, and integration headaches, making it harder for security teams to manage and orchestrate. As a result of gaps in security architectures, attackers are able to breach organizations and inflict substantial harm following four steps:

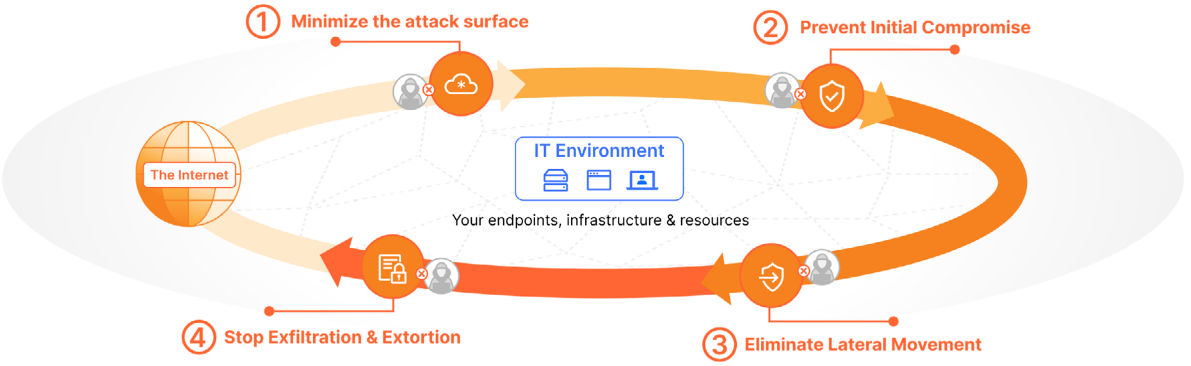
The challenges of ever expanding attack surface


1 Discover Attack Surface
2 Initial Compromise
The Internet
IT Environment
Your endpoints, infrastructure & resources
4 Exfiltration & Extortion
3 Lateral Movement

Solution : Everywhere Security neutralizes the attack cycle and protects the attack surface

To realize the vision of a modern and distributed enterprise, organizations need to move away from complex and disparate security systems and adopt a comprehensive Everywhere Security approach that delivers secured access to its workforce across web and multi cloud environments, while protecting against sophisticated cyber threats, securing sensitive data, protecting public-facing applications and APIs, and simplifying operations.

With a unified platform of programmable cloud-native services , Cloudflare helps neutralize cyber attacks everywhere, across every stage of the attack lifecycle and for any endpoint, infrastructure or resource.


1 Minimize the attack surface
2 Prevent Initial Compromise
The Internet
IT Environment
Your endpoints, infrastructure & resources
4 Stop Exfiltration & Extortion
3 Eliminate Lateral Movement

1. Minimize attack surface

Cloudflare **reduces organizations' discoverable and exploitable attack surface, by:**

- Securing web apps and public APIs, and reducing browser supply chain risk.
- Placing Cloudflare's network in front of applications such that accessing self-hosted apps & private network infrastructure can only happen via Cloudflare's global network. Threat actors cannot impact what they cannot see.
- Shifting **web browsing to the edge** rather than endpoints, insulating users and devices from web-based threats

2. Prevent Initial Compromise

Cloudflare's security makes it harder for threats, whether inbound- or web-based, to compromise any entry point into the organization, by:

- Combining external-facing security services (i.e., a web application firewall, DDoS mitigation, bot management, or API security) with internal-facing security services (i.e., cloud email security, secure web gateway) — everywhere
- Placing the WAF and all external-facing services in front of every internal resource (i.e., self-hosted apps and servers) to protect them from zero-day exploits

3. Eliminate Lateral Movement

To make lateral movement more difficult for attackers, Cloudflare **centrally integrates and manages connectivity and network security** (including Internet-native Zero Trust security) to:

- Require strict identify verification for every user and device trying to access resources on a private network, regardless of whether they are within the network perimeter
- Grant context-based, least privilege access per resource, rather than network-level access
- Reduce or eliminate the need for network DMZs, which are particularly sensitive to zero-day exploitation

4. Stop Exfiltration and Exploitation

Cloudflare help you in regaining visibility and controls over your data to stop exfiltration or fraud and to mitigate exposure risk, by:

- Providing deep, detailed detections with granular controls over what data is protected, and how
- Streamlining customization so that it is easy for IT and security administrators to design flexible data loss prevention (DLP) policies — and apply them anywhere
- Connecting, scanning, and monitoring SaaS applications for misconfigurations, improper data sharing, and sensitive data, as well as preventing data loss from web applications and APIs

> **"With the Cloudflare platform, we're getting very high-powered, very technical cybersecurity detection and protections that take little to no effort to deploy — that's especially important for our organizations that already struggle with limited resources."**
>
> **State of Arizona**

Unified & composable platform

Converge web app & API protection (WAAP), security services edge (SSE), email security domains on 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

Cloudfalre's threat intel is based on a high volume and variety of global traffic, including:

- **20%** of the internet
- **2TB** DNS querie/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+** networks 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.