CLOUDFLARE

EBOOK

Protect your attack surface

Discover and manage risks
before attackers find them first

Table of Contents

Overcome the obstacles to attack surface protection

When it comes to security, digital modernization resembles playing a video game: as a character levels up, the obstacles increase, and enemies get tougher.

In fact, IT and security leaders often think that digital modernization both helps and harms their organizations. For example, a global survey found that 31% of IT and security professionals and C-suite leaders view AI as “equally advantageous” for both defenders and attackers; 25% see it as more beneficial for attackers.

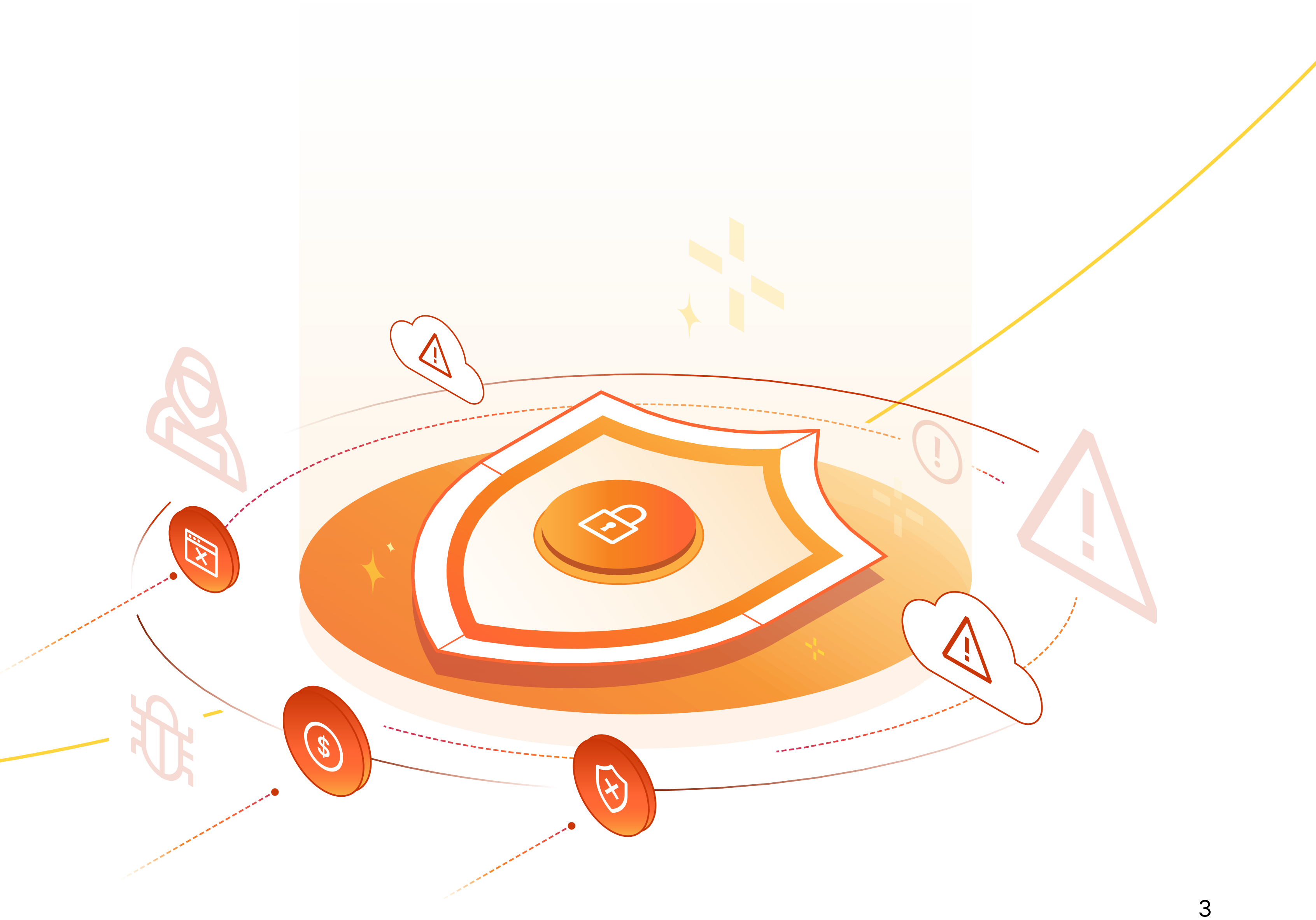
It is true that as businesses innovate and diversify their digital footprints, they inadvertently create additional entry points and vectors for adversaries to exploit. Every Internet-connected resource expands the attack surface: instead of relying on a “castle-and-moat” security model, enterprises have to protect employees, apps, data, and networks everywhere.

Consider, for example, these emerging threats that security 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.
- **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.

Fortunately, in the real world, IT and security leaders do not have to ‘win’ by pursuing every specialized weapon or learning complex battle moves. Instead, they can end the game.

This ebook explores the strategy — “Everywhere Security” — for taking back full visibility and control over your growing attack surface, and how to **end enemy access throughout the entire attack lifecycle**.



The limitations of legacy approaches

Most cybersecurity professionals have thought about digital transformation as adding more “front doors” to their house. More access points, more intruders. And, in practice, they attempt to close the doors by restricting external-facing networks, open ports, IP addresses, and web apps.

However, as everything Internet-connected expands the attack surface, traditional vulnerability management and risk governance programs fail to prevent attacks throughout the attack lifecycle.

1 Discover

- Recon
- Misconfiguration
- Exposed Assets

2 Compromise

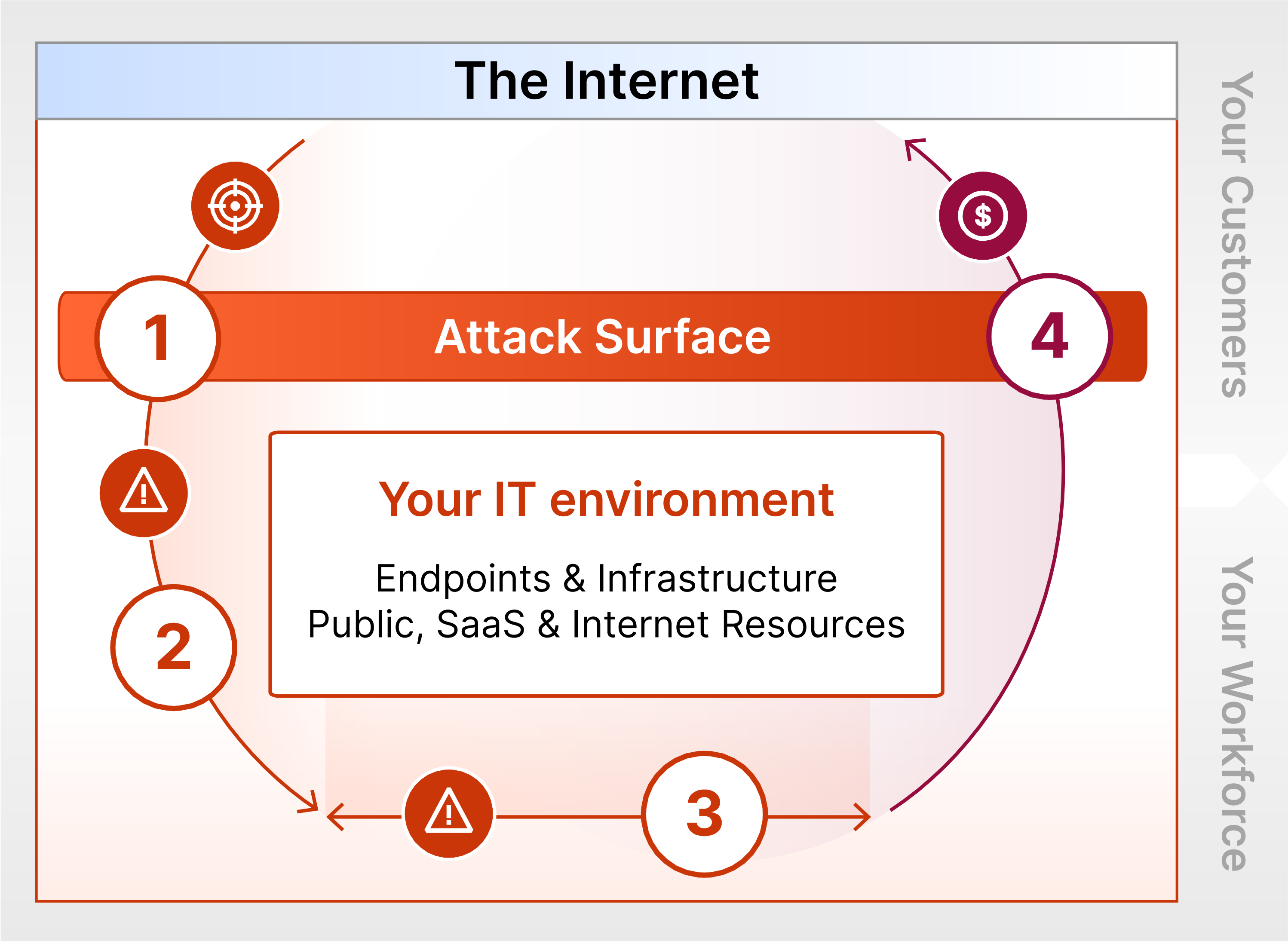
- Phishing
- Malware
- Zero Day Exploits
- Encryption

3 Move

- Flat Network
- Unrestricted Access
- Compromised User

4 Exfiltration / Extortion

- Scams
- Sabotage
- Ransom/Extortion
- Data Loss



The Internet

Attack Surface

Your IT environment

Endpoints & Infrastructure
Public, SaaS & Internet Resources

< Table of contents >

Point solutions with traditional flat network architectures contribute to the problem:

1 Discover

With more users connecting remotely and with apps now hosted across public clouds, data centers, private DMZs, and SaaS environments, attackers can **discover more** vulnerabilities in your attack surface.

2 Compromise

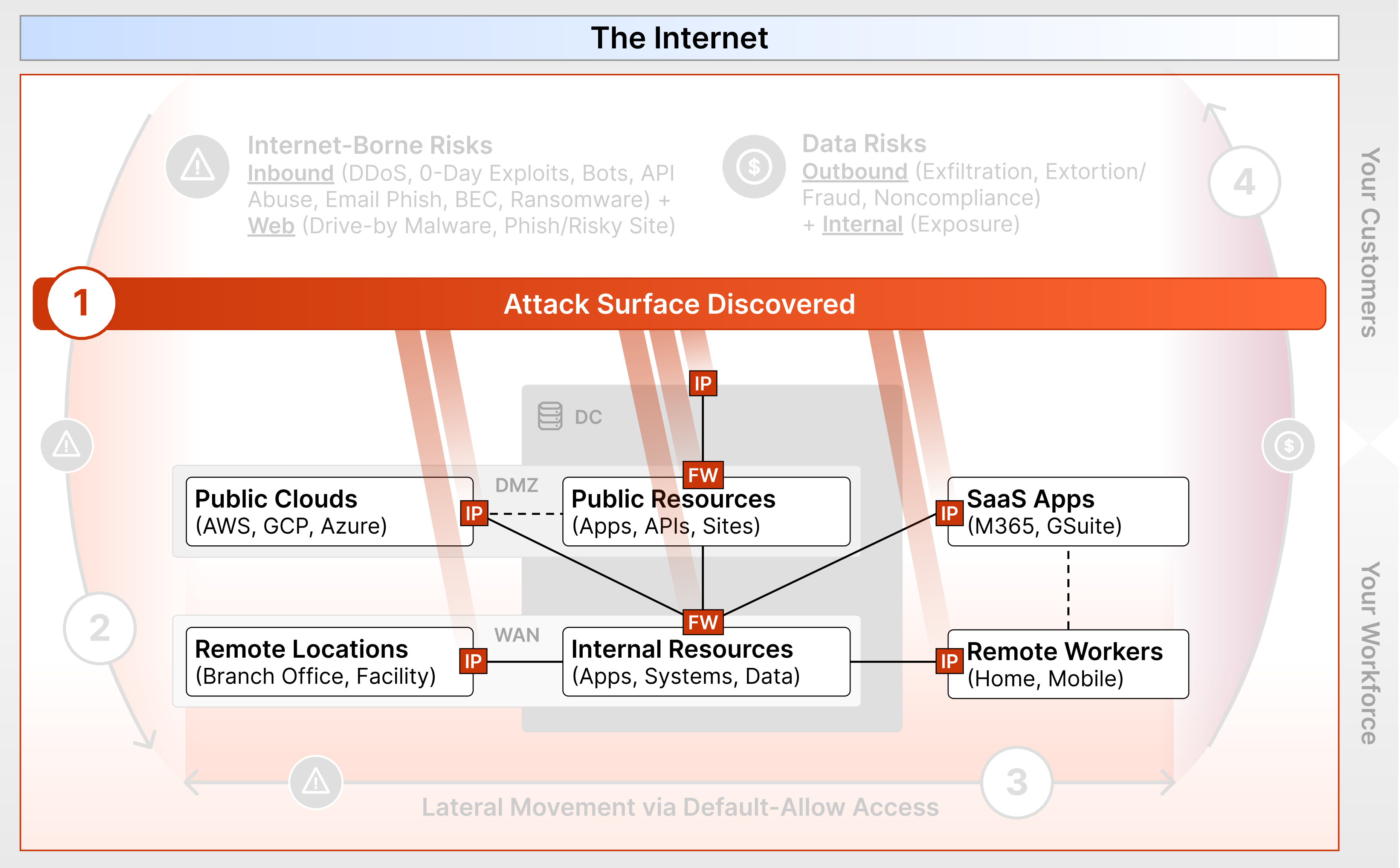
With IT sprawl and legacy network infrastructure/security tools themselves having vulnerabilities, attackers can **compromise more** users, devices, applications, and infrastructure.

3 Move

Traditional, flat IT architectures that follow the 'castle-and-moat' model make **lateral movement easier** with default-allow access to resources across environments.

4 Exfiltration / Extortion

Limited visibility and controls of legacy security tooling make it **harder to prevent exfiltration** (of money or data) and stop extortion.



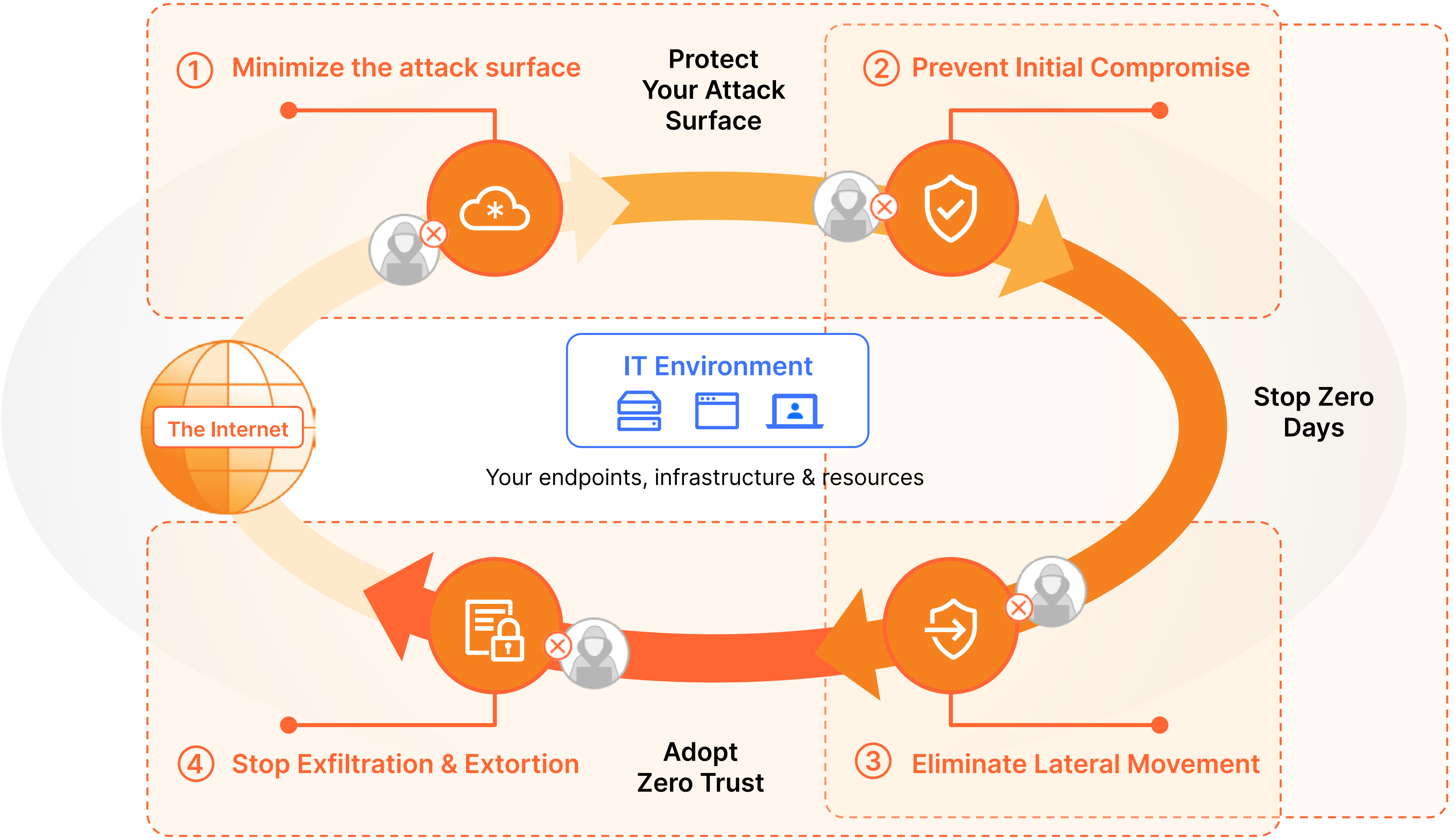
The risk of point solutions with flat network architecture

Protect your attack surface with Everywhere Security

To better protect the growing attack surface, modern and distributed enterprises need to move away from complex and disparate security systems, and adopt a comprehensive Everywhere Security approach.

Unlike traditional security solutions, the Everywhere Security model unifies protection across employees, applications, APIs, and networks.
This significantly increases an organization's IT visibility and control.

The following pages describe what this strategy looks like when applied throughout the entire attack lifecycle.


① Minimize the attack surface
Protect Your Attack Surface
② Prevent Initial Compromise
The Internet
IT Environment
Your endpoints, infrastructure & resources
Stop Zero Days
④ Stop Exfiltration & Extortion
Adopt Zero Trust
③ Eliminate Lateral Movement

1

Minimize the attack surface

In early 2024, the City of New York's payroll website was down for more than a week following a text message phishing campaign targeting employees. "Smishing" (SMS phishing) campaigns, malware-less business email compromise (BEC), QR phishing, and other phishing threats from the Internet are difficult to detect.

When users' email addresses are often public information and account credentials are easily leaked, phishing attempts will continue to occur. The key is to prevent these types of inbound and web-based Internet threats from ever reaching users.

Everywhere Security reduces organizations' discoverable and exploitable attack surface, by:

- Placing a **global cloud network in front of applications** (such as email and those accessing self-hosted apps and private network infrastructure). This makes it difficult for threat actors to discover then exploit IP addresses, configurations, and IT assets
- Managing web apps, and **properly inventorying** all APIs and web app client-side scripts
- Shifting **web browsing to the edge** rather than endpoints, insulating users and devices from web-based threats

2

Prevent initial compromise

The rapid shift to distributed workforces has fundamentally transformed the cybersecurity landscape. Threat actors have been quick to exploit vulnerabilities (for example, unmanaged devices and inconsistent access control enforcement) inherent in this distributed model.

As the corporate perimeter disintegrates, the probability of unauthorized access and initial compromise increases.

Everywhere Security makes it harder for threats (whether inbound or web-based), to compromise any entry point into the organization, by:

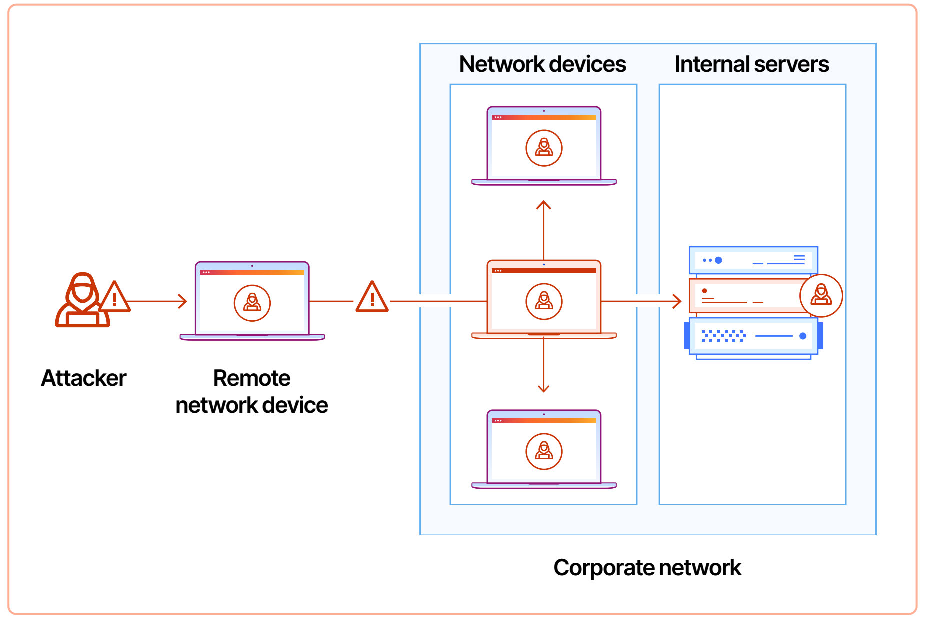
- Combining external-facing security services (i.e., a web application firewall, DDoS mitigation, bot management, API gateway) with internal-facing security services (i.e., cloud email security, secure web gateway) — everywhere
- Putting the WAF and all external-facing services in front of every internal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

3

Eliminate lateral movement

Lateral movement is like a group of thieves entering a mansion through an open window, with each going to a different room in the house. Even if one thief is discovered in one room, others can still escape with stolen items, undetected.

In January 2024, the Cybersecurity & Infrastructure Security Agency (CISA) issued an emergency directive in response to a critical vulnerability impacting the Ivanti Connect Secure product. By exploiting those vulnerabilities, an attacker was able to (among other things):



- Harvest credentials from users logging into the virtual private network (VPN) service
- Use those credentials to log into protected systems in search of even more credentials
- Modify files to enable remote code execution

To make lateral movement much more difficult, an Everywhere Security approach **centrally integrates and manages connectivity and network security** (including Internet-native Zero Trust security) to:

- Require **strict identity 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

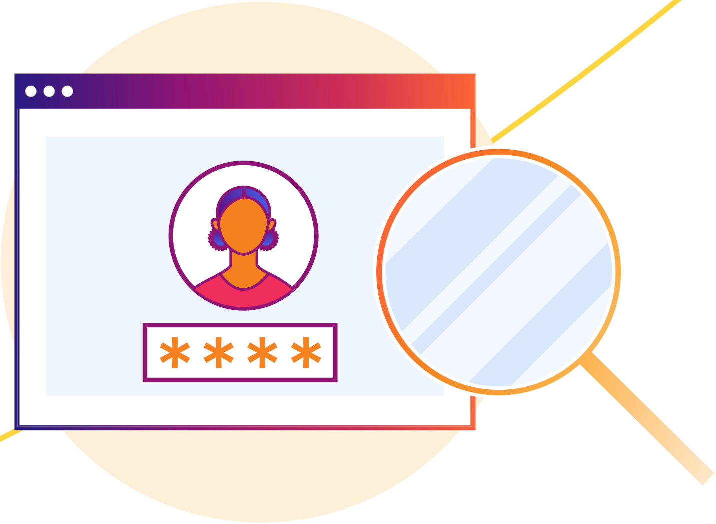
4

Stop exfiltration and extortion

Data continues to explode in volume, variety, and velocity, and security teams at organizations of all sizes are challenged to keep up. Businesses face escalating data loss risk posed by varied SaaS environments, a rise in ransomware, the emergence of generative AI tools, and the theft of valuable source code.

Unifying data protection with Everywhere Security provides:

- **Deep, detailed detections** with granular controls over what data is protected, and how
- **Complete customization** so that it is easy for IT and security administrators to design flexible data loss prevention (DLP) policies — and apply them anywhere
- **The ability to connect to, scan, and monitor SaaS applications** for misconfigurations, improper data sharing, and sensitive data



Use cases for Everywhere Security

USE CASES FOR EVERYWHERE SECURITY

Minimize tool sprawl and complexity to help minimize the attack surface

Tackling inbound and other web-based Internet threats has traditionally involved manually stitching together an expanding suite of traditional and siloed tools across security domains (e.g. email security, application security, data security, threat intelligence). This can lead to security gaps and an unsustainable level of resources just to keep up with yesterday's threats and priorities.

Cloudflare protects ~20% of the web, giving it a unique capability to scan the Internet for attacker infrastructure and phishing campaigns that are under construction. By proactively using that early insight (plus contextual analysis techniques), Cloudflare protects organizations from phishing attacks — before damage can occur.

For example, **Werner Enterprises** (one of the USA's largest truckload cargo carriers) had concerns that its previous email security system wasn't keeping up with attacks against its geographically diverse workforce.

They were also systematically migrating its legacy on-premise applications to the cloud. Werner looked to minimize tool sprawl and reduce the complexity of managing multiple vendor security solutions.

With Cloudflare, Werner:

- Secured its Microsoft 365 inboxes, improved protection for its mobile and roaming users, and implemented a more proactive approach to email security
- Secured its internal and external networks, and gained more granular control over the flow of information between users, cloud tenants, and on-premise systems

> **As we roll out Cloudflare and consolidate into a single platform, our security stack is stronger than ever before."**
>
> **Danny Lilley**
> Vice President and Chief Technical Officer
> Werner Enterprises
>
> WERNER®

Table of contents

Connect app deployment with API defense-in-depth to help minimize the attack surface

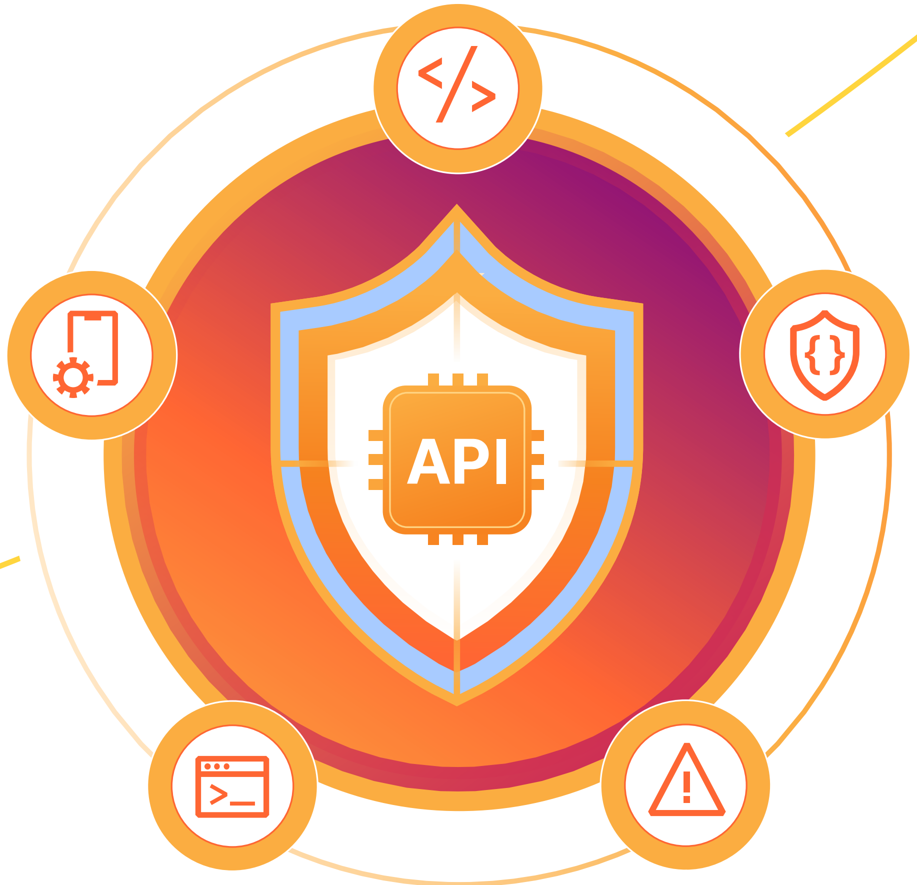
Flaws in API authentication and authorization lead to breaches; for example, an attacker accessed millions of customer records through a telecom provider's unauthenticated API.

The rapid increase in API development also makes it nearly impossible to detect and patch every vulnerability they contain, especially when developers and engineers fail to communicate with security teams before launch.

APIs fulfill such a wide range of purposes — from augmenting application development to connecting microservices and other external functions — it is not uncommon for organizations to rely on dozens, if not hundreds (or thousands) of them.

Cloudflare services provide the connective tissue between app deployment and API defense-in-depth to:

- Automate API discovery and visibility as the crucial first step to improving and implementing API security practices (you cannot protect what you cannot see)
- Build in API authentication and authorization processes from the outset
- Monitor and protect APIs from abuse, vulnerability exploits, authentication loopholes, and data leakage



USE CASES FOR EVERYWHERE SECURITY

Secure web apps and APIs — with no gaps — to help prevent initial compromise

Apps are relentlessly targeted by attackers: with zero-day threats, credential stuffing that leads to account takeovers, browser-based supply chain attacks that compromise third-party dependencies, exploiting API vulnerabilities to steal data — and much, much more.

Therefore, application protections must be part of a broader, unified security posture that also protects APIs, stop bots, and reduces client-side risks.

For example, prior to using Cloudflare, Maricopa County, **the State of Arizona's largest county**, had firewalls in place, but not Layer 7 DDoS protection "or anything to protect against sophisticated attacks that emulate end users."

With Cloudflare services:

- Every organization in Maricopa County can identify and thwart attacks by blocking problematic IP addresses
- The county's online forms are also protected from credential stuffing or brute force attacks
- The State of Arizona secured websites and cloud-based agency applications across more than 80 domains against DDoS, JavaScript emulation, and other website vulnerabilities at the server level

After **boohoo Group**, an online fashion retailer with 13 brands, discovered malicious bots behind credential stuffing, and more than 100,000 fake accounts, they turned to Cloudflare to help protect their applications from DDoS attacks, malicious bots, API abuse, and other attacks.

With Cloudflare, boohoo experienced:

- Up to 90% reduction in bot attacks and abusive traffic
- A reduction in manual responses to fraudulent accounts, bots, and other threats
- Dashboard reporting for more robust governance

Table of contents

Absorb malicious traffic to public-facing infrastructure to eliminate lateral movement

Like other busy global airports, **Melbourne Airport in Australia** must maintain a strong security fabric that covers the entire passenger experience. This includes being very clear about who is on their infrastructure (including its free public Wi-Fi), and how to protect it.

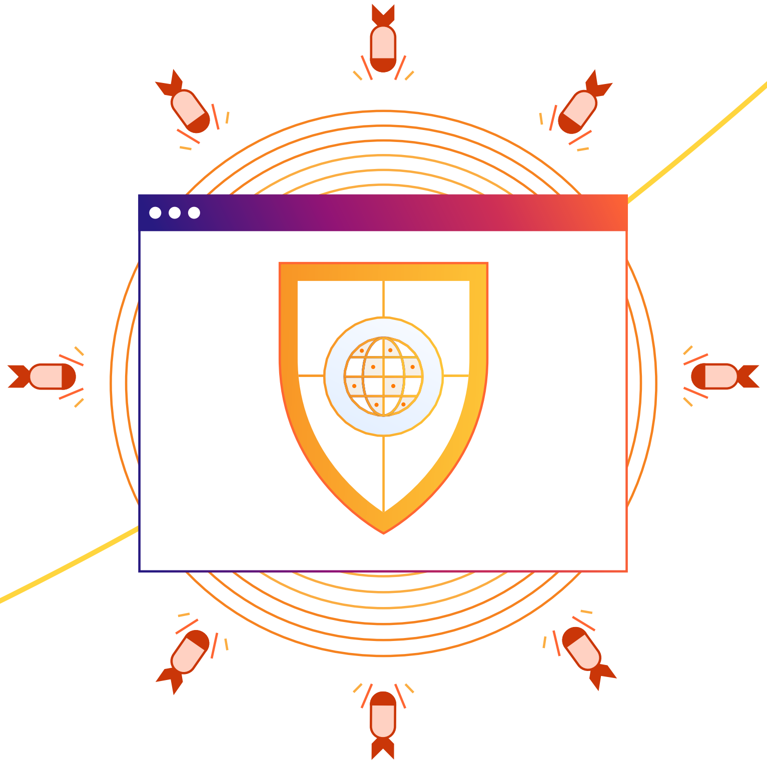
In addition to leveraging Cloudflare for web security, the airport moved its network perimeter to the Cloudflare global network edge. The results included:

- Securing externally exposed URLs and restricted problematic traffic for more than 100,000 daily visitors
- Mitigation of potential international DDoS threats
- Enhanced visibility into network traffic patterns and usage, aiding in continuous security assessments and improvements

The enterprise network and the DMZ are addressable and exposed to the Internet, and require a different security approach (one that isn't built on flat network architecture).

Accepting inbound traffic opens the attack surface to unauthenticated or pre-authenticated traffic — but Everywhere Security absorbs that exposure — and lets organizations **provide simple, secure access without allowing inbound traffic to applications**.

> **“Overnight we expanded our Cloudflare protection from our web applications to our entire network. It was an A+ experience.”**
>
> **George Panagiotidis**
> Technology Project Manager
> Melbourne Airport
>
> MELBOURNE AIRPORT



USE CASES FOR EVERYWHERE SECURITY

Improve visibility and control over data to stop exfiltration

Everywhere Security enables organizations to extend visibility and unify data protection across all apps, users, and devices.

With Cloudflare, organizations can:

- Determine how corporate users are using SaaS, web, and private apps
- Granularly identify which ones they are using
- Then accordingly, apply data controls and identity/device-driven policies to **shrink your attack surface**

Reduce risk of data exfiltration

- Apply DLP controls to what/where data moves into any app
- Isolate threats of data leaving SaaS and private apps*
- Secure access to SaaS and self-hosted private/cloud apps*

Gain visibility over data movement

- Detect inappropriate sensitive data sharing in SaaS apps
- Detect unsanctioned and sanctioned SaaS apps
- Integrate logs with SIEM providers for auditing*

*Using Cloudflare's programmable global cloud network

Learn More

Cloudflare offers composable, scalable security that's tailored to the evolving needs of distributed organizations. Our cloud platform unifies a range of diverse technologies and harnesses network-powered threat intelligence to deliver low-touch, high-efficacy protection across users, applications, and corporate networks.

Cloudflare's security products are well-received by analysts and customers alike.
Check out our library of analyst recognitions today!

Call: 1 888 99 FLARE
Email: enterprise@cloudflare.com
Visit: cloudflare.com