EBOOK

CLOUDFLARE

7 ways to work from anywhere

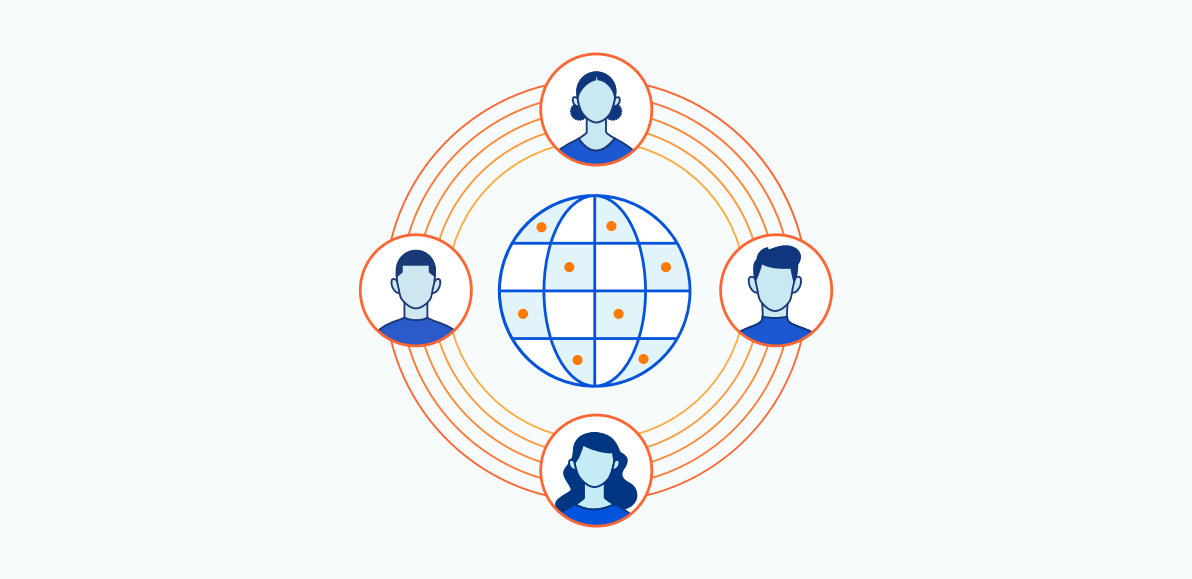
Bring security and speed to the office of the future

Modern teams are made up of many different kinds of users — including employees, contractors, and partners — collaborating in the same tools to get work done. As your business decides where employees will work in the future, your security controls must meet them where they are. How will you protect your company's data without slowing users down?

This ebook shares 7 best practices that effective organizations can use to protect their global workforce without sacrificing productivity.

INDEX

INTRODUCTION



Once upon a time, the office was the primary place work got done. Employees who needed to access internal systems remotely connected to tools over a VPN; a slower experience designed for occasional use.

Today, that dynamic has radically changed. Workforces are drastically more mobile and distributed, with more employees working from home than ever before. Where it was once feasible to draw a perimeter around corporate resources, the rise of SaaS, cloud computing, and remote work has rendered this approach obsolete. The modern corporate network is the Internet itself, and safeguarding it demands a radical new approach.

This guide will give you the foundation to adapt your business's security for today and the future. It will introduce key concepts like the Zero Trust security model, highlight new solutions for old problems, and equip you with the knowledge you need to secure your team in this rapidly-changing landscape.

CHAPTER 1

The changing landscape of network security

Even before the sweeping rise of remote work, the modern workforce was already evolving to become mobile and distributed. The Internet made it possible to form global teams that collaborate across state lines, rivers, and oceans. But for many IT teams, dispersion challenged the foundation of their security programs: the idea that an employee's physical location should define how their traffic is routed and secured.

In the past, security controls were physically defined and enforced at office locations, where an employee was considered to be "on the network," and thus given access to the applications and services they needed to get work done. Onsite firewalls filtered employee traffic and logged inbound and outbound requests through the network. And custom private links provided extra-fast and private connections to SaaS applications like Office 365.

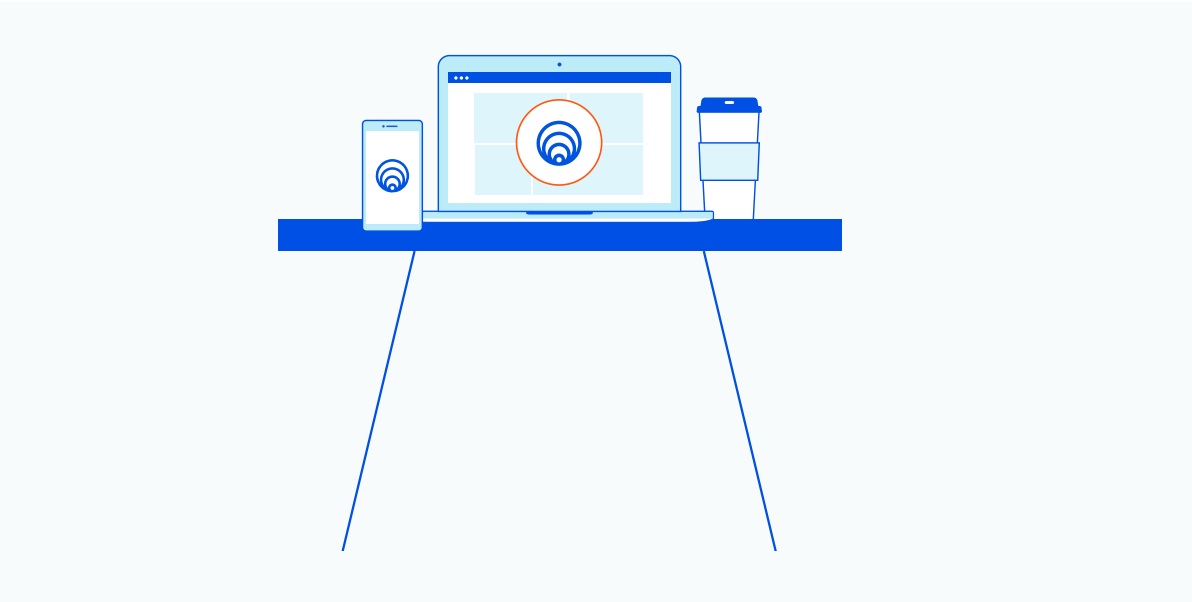
Following a massive global influx of remote work, IT teams have been forced to find new ways to connect employees and customers. A recent study by Forrester Consulting commissioned by Cloudflare found that 52% of security leaders surveyed identified remote work as one of the top factors impacting their IT security programs in 2020.

Today, employers are considering how they will bring employees back to the office. For most, there will be a new normal, where a portion of employees will return to offices, and the rest continue to work from home.

The impending arrival of a hybrid working environment raises new questions for security teams:

- How will we continue to protect remote workers' access to internal resources without slowing them down?
- What security controls do we still need at our branch offices, and which investments no longer make sense?
- How can we retain visibility of employee activity with so many modes of connection?
- How can we achieve consistency in our security model, and route traffic without unnecessary hops?

For many IT teams, these questions present an acute challenge that will likely require new solutions. And while change is never easy, there may be opportunities to transform your organization for the better. In this e-book, you'll learn about new models for corporate security and 7 best practices to implement them.



Tomorrow's office: the Internet cafe

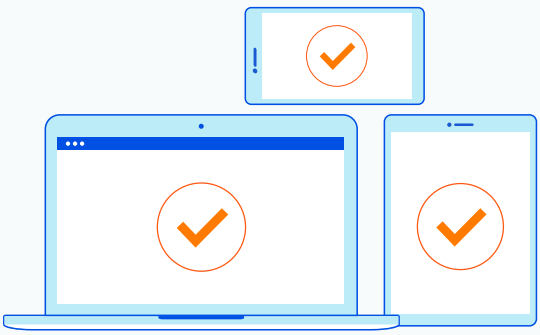
Before the rise of remote work, teams used to consider their physical office locations as hubs for connectivity and security. Simply connecting employees to resources on the open Internet was not considered to be safe or fast enough for corporate use. Thus, it made sense to establish private connections directly from the branch office to the Internet, SaaS apps, and corporate data centers. And it also made sense to install on-premise firewalls for additional layers of protection.

Today, networking and security leaders are reconsidering those investments in favor of a device-centric approach. In this model, individual offices are no longer hubs or spokes of a corporate network, but more like Internet cafes. Connectivity (WiFi) is provided, but security is managed on the employee's device. Employees can now truly work from anywhere and have the same excellent experience everywhere they go.

Creating a device-centric security model

The freedom to work from anywhere safely starts with safe devices. When employee devices are effectively managed and secured, they can benefit from many of the security functions that were once exclusively delivered at the network level.

CHAPTER 1



In a device-centric model, employee devices are connected and secured with the following controls:

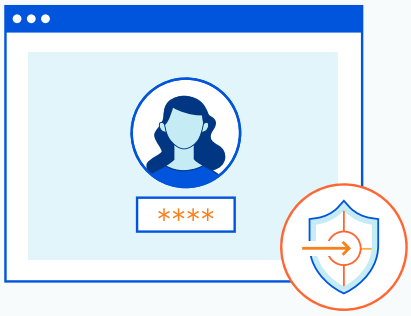
- **Managed**: administrators use a device management platform to enroll devices in a corporate security program. Employees use corporate devices that are bound to specific terms and conditions in exchange for better connectivity. When employees leave the company, the management interface can instantly wipe their device of sensitive corporate data.
- **Patched**: Through a centralized device management program, devices are automatically patched with the latest updates for their operating systems. The newest bug fixes are applied to their machines automatically.
- **Filtered**: Devices send all of their outbound traffic through a secure web gateway (SWG) for analysis and policy application. Corporate policies are enforced at the device level to prevent usage of shadow IT apps or inappropriate sharing of information.
- **Isolation**: Browsing on employee devices is conducted in an isolated container/secure sandbox. Zero day threats, if encountered, never impact the employee device.
- **Anti-virus**: Devices are regularly scanned for malicious files and viruses. If viruses are detected, they are contained and eliminated.
- **Monitored**: All traffic from the device is logged centrally for administrator triage.

Tip 1: Focus your security strategy on employee devices, not office locations.

Corporate device management is the first step to modern Zero Trust security. Harden your devices against threats, and you're one step closer to protecting your network.

When security becomes focused on the employee's device, and not their network location, they can start to work safely and efficiently from anywhere. And the firewalls and security appliances that used to be essential to protect the branch office are no longer important.

If the Internet cafe is the way of the future, how are security teams getting there?



Zero Trust: A model for a new era

Over the last few years, a new approach to online security has transformed how businesses secure themselves in the modern world of connectivity. It revolves around an idea called Zero Trust security.

Instead of employing the traditional security model used by VPNs, which automatically trusts any user that gains access to internal applications, Zero Trust does not rely on an assumption of trust. Every request to every application is digitally interrogated, regardless of where it came from or where it is going.

The Zero Trust model was first popularized by Google in a research paper published in 2016, which explained how the tech giant had reinvented its internal security model such that it "considers both internal networks and external networks to be completely untrusted".[2] Since then, Zero Trust has been adopted and deployed by many other leading companies.

Zero Trust is not one product, nor a collection of products. Instead, it is a mindset that informs security architecture decisions, and at its core is the principle that no user should be trusted by default, even if they are already inside the network.

When shifting to a Zero Trust model, there are best practices to aspire to, but the key is finding the right set of habits that will allow you to achieve specific goals. For example, implementing multi-factor authentication may not prevent every attacker from accessing your applications, but it does set a solid baseline in security hygiene.

Tip 2: Use devices as a key to your sensitive data.

With contextual access controls, you can ensure that only managed devices can access specific apps and data.

CHAPTER 2

Disconnect from your VPN

VPNs have earned their place in the annals of connectivity history. For decades, they've helped keep businesses secure, and many companies continue to rely on them today.

Unfortunately, VPNs come loaded with compromises.

First and foremost is the usability tax: VPNs are notoriously difficult to deploy and use. Between configuration hurdles, reliability hiccups, and clunky login applications, VPNs are a hassle for everyone, which often translates into a tremendous burden for your IT staff.

Even when your VPN is functioning as intended, it introduces latency that can be anywhere from a mild annoyance to debilitating. By design, most VPNs filter all traffic through the same pipe. When your employees are working remotely, every packet has to be routed back to the VPN appliance at corporate HQ before it can begin making its way to the intended destination. That translates to latency and frustration, especially for globally distributed teams.

Tip 3: Replace your VPN with Zero Trust access.

Zero Trust access platforms protect your applications from unauthorized access. Authentication requests are evaluated for identity and context, not just VPN location.

What's worse: VPNs employ a security model that is no longer effective against emerging threats. Anyone who successfully connects to a corporate VPN is considered trustworthy, without any additional checks subsequent to the initial connection. Concerns with this overly-permissive model are exacerbated by the low-fidelity logging supported by VPNs — they can report a user's IP address, but none of the applications or data they've accessed. Not only is it difficult for security teams to produce logs of user activity for compliance, but it is almost impossible to retrace the attacker's steps, should there ever be concern that a user account has been compromised.

46% of organizations experienced latency from their VPN in 2020 last year, according to a research paper from Forrester Consulting.[1]

Replacing VPN connections with Zero Trust network access is a first step in adopting a Zero Trust model. Zero trust network access is a way to overcome these challenges by applying the principle of least privilege to business-critical applications. By applying microperimenters around each application, hiding applications behind encrypted connection tunnels, and logging every request, ZTNA can simplify processes around IAM, free up valuable development time, and significantly reduce opportunities for data loss.

If your company is reliant on a VPN for application access, we recommend starting with a pilot program targeting a handful of applications used by a small group of users.

For instance, a ZTNA pilot might start with:

- Applications that use HTTPS
- Apps that are not protected with existing SSO providers
- Apps only used by 5-10% of overall company base

After a successful deployment, users will note a difference in the experience of logging on to their applications. Capture positive feedback and use it as momentum for your Zero Trust transformation project.

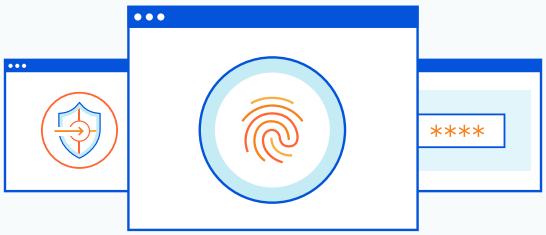
CHAPTER 3

Implement Zero Trust application control

One of the trickiest things for any company is ensuring that everyone has access to the tools and data they need — but no more than that. That's a challenge that becomes all the more difficult as a team scales. As employees and contractors leave, it is similarly essential to ensure that their permissions are swiftly revoked.

Managing these access controls is a real challenge for IT organizations around the world — and it's greatly exacerbated when each employee has multiple accounts strewn across different tools in different environments.

With the right authentication system, onboarding and offboarding is much smoother. Each new employee and contractor is quickly granted rights to the applications they need, and they can reach them via a launchpad that makes them readily accessible. When someone leaves the team, one configuration change gets applied to every application, so there isn't any guesswork.



Extend secure access to third parties

Many businesses also need a secure method of managing contractors and other third parties. Extended on and off-boarding processes can undermine some of the benefits of bringing on external support. And, as with employees, it's key to ensure that your contractors and vendors only have access to the data and tools they need, for as long as they need them.

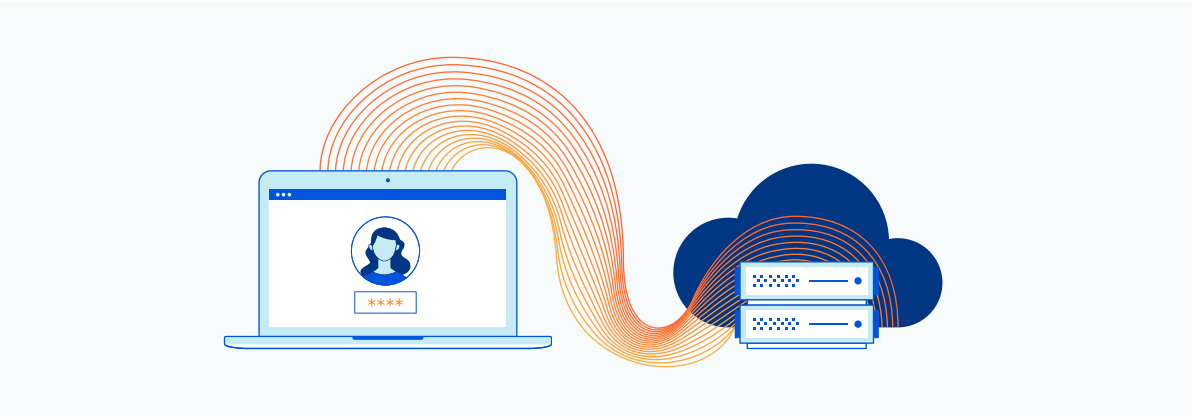
Modern authentication solutions allow your contractors to sign in with accounts they already have — like Gmail, Facebook, or LinkedIn — while still providing the same degree of security, logging, and granular permissions they'd get if you took the time to generate new accounts on your own systems.

Some authentication systems also support one-time passcodes, where the contractor receives a code via email that grants them temporary access to designated systems. This is another way to streamline your contractor workflows without compromising on your security.

Tip 4: Simplify contractor access.

Most IAM systems make 3rd party users difficult to manage. Treat 3rd party users like first class citizens with a platform that simplifies contractor access.

CHAPTER 4



Secure the flow of data — in and out of your enterprise

In addition to adopting a modern authentication system, it's also vital to maintain control over the data that comes into and out of your network.

Historically, branch offices sent all of their Internet-bound traffic to one centralized data center at or near corporate headquarters. Administrators ensured that all requests passed through a secure hardware firewall, which then observed each request, performed inline SSL inspection, applied DNS filtering, and kept the corporate network safe from security threats. This solution worked best when employees accessed business critical applications from the office, and when applications were not on the cloud.

SaaS applications broke this model when cloud-delivered applications became the new normal for workforce applications. As business critical applications moved to the cloud, the number of Internet-bound requests from all offices went up. Costs went up, too. The legacy model of backhauling all Internet traffic through centralized locations could not keep up with the digital transformation that all businesses are still going through.

These issues are exacerbated by geographically distributed offices and remote workers, who wind up having to send their network traffic back to their company's hardware firewall — often located at corporate HQ, sometimes on the other side of the world.

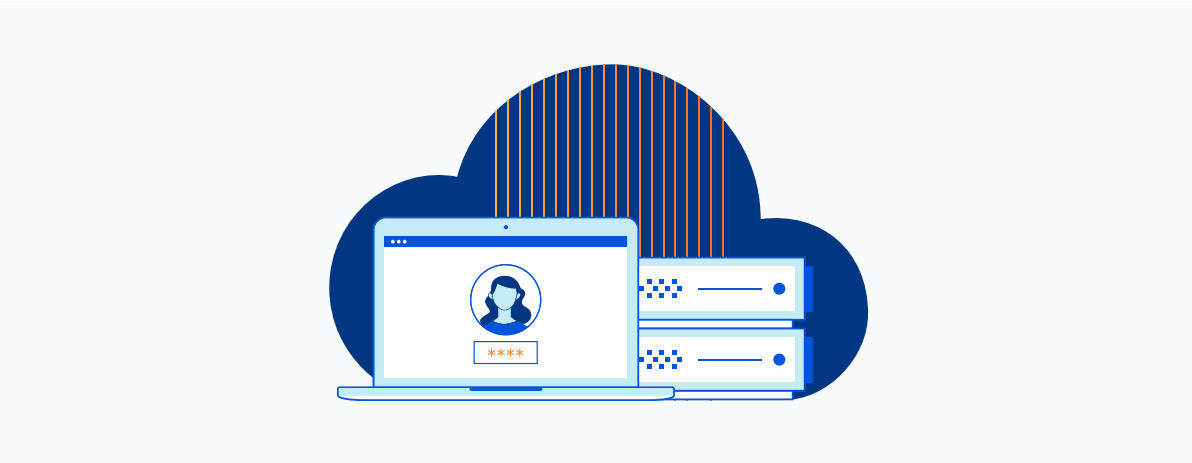
Another issue with legacy hardware firewall appliances is that they were not built for the constantly-evolving threat landscape of the modern Internet.

For example: about 1.5 new phishing sites are created each month[3], and legacy hardware firewalls are not fast enough to update their static rules to thwart phishing attacks. When security threats on the Internet act like moving targets, legacy hardware appliances cannot keep up. As a result, employees remain vulnerable to new threats.

Tip 5: Filter traffic.

Set corporate policies for Internet use and filter out malicious or inappropriate sites.

CHAPTER 4



Secure web gateways have become a popular method to address these fast-evolving threats. SWG's are most often delivered as SaaS security platforms that can intercept traffic from employee devices. Once traffic is intercepted, the gateway applies filtering rules to inbound and outbound traffic.

Instead of relying on a static threat model to capture threats, SWG platforms give administrators the tools to set their own rules on the fly. Equipped with built in threat intelligence and easy-to-use categories, they can easily block new threats as they surface.

Using the same filtering mechanism, administrators can also set policies that control how a user interacts with corporate data.

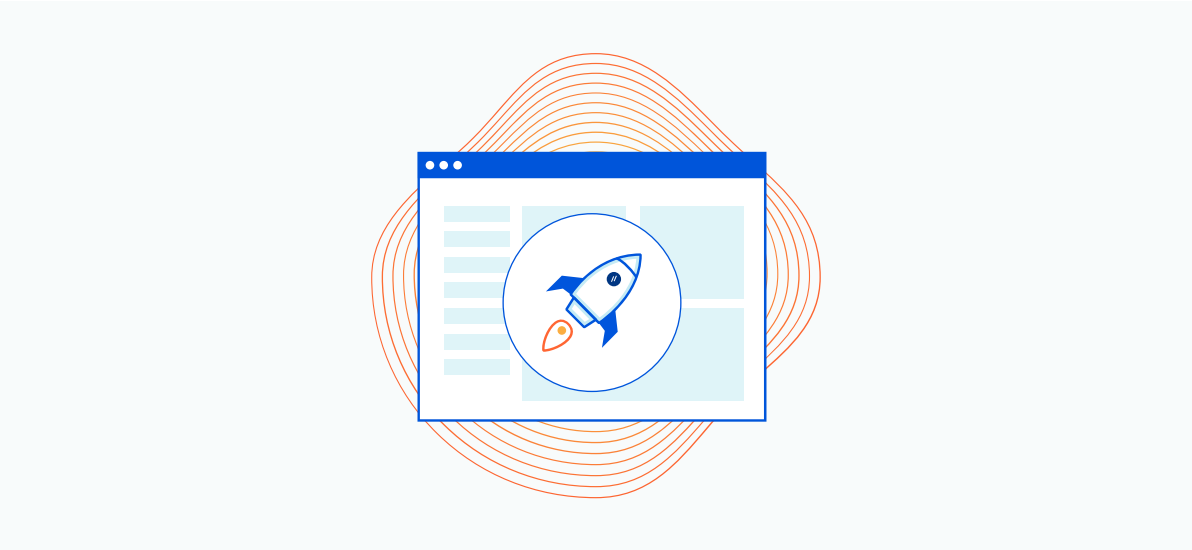
The possibilities are endless. For example, an administrator might set up secure web gateway policies to:

- Block sites that have been flagged as phishing scams
- Log and monitor activity inside SaaS applications
- Prevent employees in the marketing department from visiting the administrative portal of a corporate CRM application
- Limit file uploads and downloads from unapproved cloud storage sites like Dropbox

Tip 6: Log everything.

With activity logs flowing to a centralized SIEM or cloud storage bucket, you can better understand traffic patterns and spot anomalies.

While secure web gateways are powerful, they rely on administrators to configure rules and policies to protect their organization. There is no net big enough to catch every threat on the Internet before it impacts your organization. But for emerging threats, isolated browsing can act as a final frontier of protection.



Enter: browser isolation

A web browser, the same application that connects users to the entire Internet, also connects you to all of the potentially harmful parts of the Internet. It's an open door to nearly every connected system on the planet, which is powerful and terrifying.

We also rely on browsers more than ever. Most applications that we use live in a browser and that will continue to increase. For many organizations, a corporate laptop is just a managed web browser machine.

To secure the data these devices hold or access, enterprises have started to deploy "browser isolation" services where the browser itself doesn't run on the machine. Instead, the browser runs on a virtual machine in a cloud provider. By running away from the device, threats from the browser stay on that virtual machine in the cloud.

Tip 7: Isolate risky browsing.

Prevent browser exploits and mitigate data breaches well before they reach user devices or spread to the corporate network with Browser Isolation.

A Zero Trust security model assumes that even though a user has safely loaded a website 99 times, the website might be compromised on the 100th time. Browser isolation is one way to implement this assumption.

Organizations will likely not need to invest in every Zero Trust technology immediately. But by addressing critical weaknesses first, they can begin strengthening their longer-term security mindset.

CHAPTER 5

The Cloudflare solution: Introducing Cloudflare Zero Trust

Cloudflare Zero Trust

If the challenges outlined in this book resonate with you, Cloudflare Zero Trust may well be the solution you're looking for.

Cloudflare runs one of the world's largest networks — spanning 200 cities in over 90 countries, with approximately 25 million Internet properties running on it. Cloudflare provides a variety of services spanning security, performance, and reliability, and is utilized by many of the world's biggest brands, including 10% of the Fortune 1000.

Cloudflare Zero Trust harnesses the power of Cloudflare's global edge network to secure your team, network, and data.

Embrace zero trust access	Replace broad security perimeters with one-to-one verification of every request to every resource. Enforce zero trust rules on every connection to your corporate applications, no matter where or who users are. Learn more about Cloudflare Access
Secure Internet traffic	When threats on the Internet move fast, the defenses you use to stop them need to move faster. Cloudflare Zero Trust protects employees from threats on the Internet and enforces policies that prevent valuable data from leaving your organization. Learn more about Cloudflare Gateway
Stop zero day threats with browser isolation	Prevent browser exploits and mitigate data breaches well before they reach user devices or spread to the corporate network. Learn more about Browser Isolation

REFERENCES

1. Forrester Opportunity Snapshot: A Custom Study Commissioned By Cloudflare, October 2020
2. BeyondCorp: A New Approach to Enterprise Security - Google Research
3. Webroot Quarterly Threat Trends report - Webroot