CLOUDFLARE

10 Ways to Secure and Accelerate a Modern Workforce

Modern remote teams are made up of many different kinds of users — including employees, contractors, and partners — collaborating in the same tools. As your team becomes more distributed, how will you protect your company's data without slowing users down?

This E-Book shares 10 best practices that effective organizations can use to protect their global workforce without sacrificing productivity.

1-888-99-FLARE | enterprise@cloudflare.com | www.cloudflare.com

Table of Contents

Introduction

Once upon a time, the office was where work got done. Employees who needed to access internal systems remotely were hamstrung by the sluggish performance and complexity of VPNs, if they bothered at all.

Today, that dynamic has radically changed. As a result of choice and now circumstance, workforces are increasingly mobile and distributed. Where before it was feasible to enforce a perimeter around the corporate network, today's applications and the dizzying array of devices accessing them remotely have rendered traditional security postures obsolete. The modern corporate network is the Internet, and safeguarding it demands a radical new approach.

This guide will give you the foundation to adapt your business's online 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.

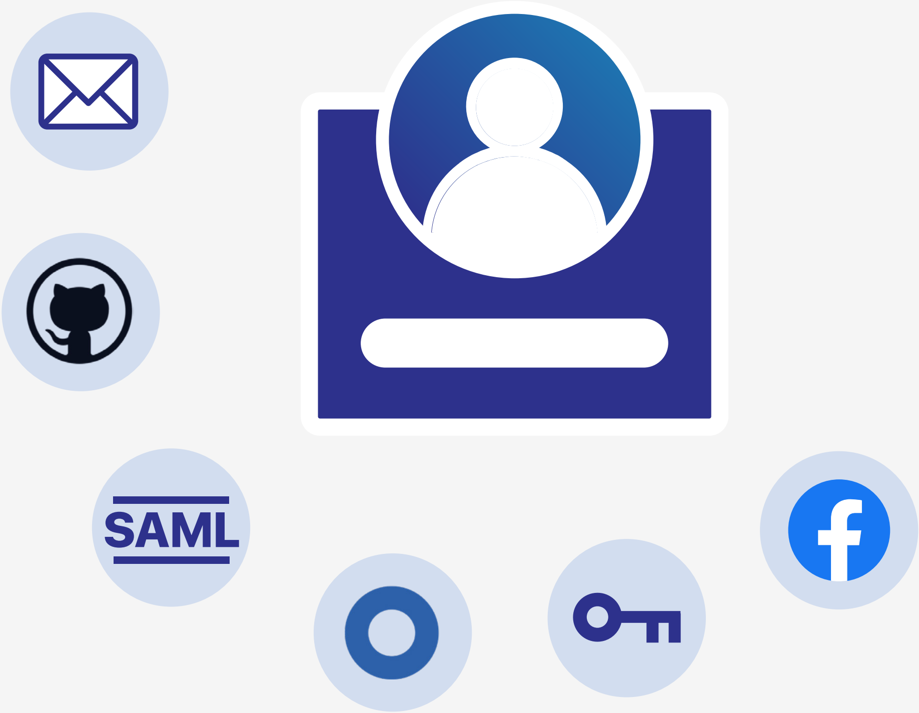
About Cloudflare

Cloudflare is a leading security, performance, and reliability company on a mission to help build a better Internet.

Trusted by over 25 million Internet properties, our integrated cloud platform helps brands and retailers improve the performance of their web properties, while also safeguarding customer data and transactions.

- Network spanning 200+ cities and over 90 countries
- Within 100 milliseconds of 99% of the Internet-connected population in the developed world
- An average of 50 billion daily cyber threats blocked in Q4, 2019
- 35 Tbps total network capacity

Chapter 1: The Changing Landscape



Even before the sweeping rise of remote work, the modern workforce was already evolving to become mobile and distributed. In the past a business could safely assume that connections to their networks would come via work-issued laptops and mobile phones, but it is now far more common for employees to “Bring their own devices” — drafting documents, dialing into video calls, and more from their personal smartphones and tablets.

But while the convenience and productivity gains of BYOD have been a boon in some respects, they are the source of much anxiety for IT departments. It is challenging (or impossible) for administrators to deploy and enforce an effective security policy that spans all of these devices, and employees may be wary of installing security software onto their personal devices.

That's why it makes sense for security to operate at the network level, adopting a model that considers devices to be inherently untrustworthy (because it is so difficult to harden them).

Tip #1

With so many devices out there, it's impossible to secure every endpoint — so conduct your security analysis and enforcement at the network level.

Chapter 1: The Changing Landscape cont'd

Unfortunately these concerns are relevant to businesses of any size. Cyberattacks are on the rise, and malicious actors are looking to take advantage of security gaps that may have been exposed during the rapid shift to remote work, as teams may be distracted by other issues. Indeed, between January and March 2020, attacks increased up to 70% at times.

The rapid acceleration of the shift to remote work, in tandem with the rise of online threats, presents an acute challenge to many IT teams that will likely require new solutions. And while change is never easy, there may be additional opportunities to transform your organization for the better.

Tip #2

As you reevaluate your security posture, consider modern SaaS solutions — many of which are now more robust than their legacy counterparts.

Chapter 2: Building a Toolbox for Everyone

As you transition to embrace remote work, there's a good chance you'll want to reevaluate the tools your team relies on daily. Software that facilitates real-time collaboration will likely be at the top of the list. And it will be important to identify security solutions that work in tandem with the new tools you adopt.

Among your first considerations as you evaluate a new set of solutions should be ease-of use. Your team will have varying degrees of technical familiarity, and any roadblocks they hit will have an immediate impact on productivity and morale — so it's important to develop an approach that is as intuitive and accommodating as possible.

Furthermore, if your security posture gives your team headaches, your IT staff will be feeling a heavy burden. Employees may give up on using internal tools at all (or, worse: try to find a workaround).

A Launchpad to Productivity

As you evolve your team's digital toolbox, there is an additional opportunity to encourage adoption, by putting these tools just a click away. Modern authentication systems will provide your team with a curated selection of tools (namely, the ones they have access to), providing deep links that will take them straight to the appropriate dashboard — no more byzantine bookmarks or lengthy log-in flows.

Embracing Software as a Service

One piece of good news is that there are many mature Software as a Service (SaaS) solutions available that are built from the ground up around distributed collaboration.

The SaaS model differs from the traditional approach of purchasing software in several key ways:

- Rather than host and maintain the tools on your own servers, your team securely accesses them from servers maintained by the software provider. This allows the provider to continually make updates and improvements to the software without additional work on your part.
- Instead of paying a large sum upfront, SaaS providers typically charge a much smaller fee on a recurring basis — putting tools within reach that may have been otherwise unaffordable.

Well-known SaaS tools are available from the likes of Salesforce, Box, and Google's G Suite (including Google Docs and Sheets) — and there are myriad niche tools available. Even if you work in a relatively niche vertical, there's a good chance there's a SaaS app tailor-made to help.

Another nice thing about SaaS tools is that they share many UX conventions with consumer applications, so most of your team will probably be able to navigate them without issue.

Chapter 3: Disconnecting From Your VPN

VPNs have earned their place in the annals of connectivity history. For decades, they've helped keep businesses more secure than they would've been otherwise, 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, VPNs filter all traffic through the same pipe, and when your employees are working remotely every packet has to be routed back to your 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.

What's worse: VPNs employ a security model that no longer makes sense. 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. This makes it hard for security teams to produce logs of user activity for compliance, and makes it very difficult to retrace anyone's steps, should there ever be concern that someone's account may have misused.

Even when your VPN is functioning as intended, it introduces latency that can be anywhere from a mild annoyance to debilitating.

There's also a more fundamental problem with VPNs. In the past a company might expect to host a handful of internal applications on their own servers, and VPNs were designed to connect trusted employees to those resources. But today most businesses rely on some combination of applications running on their own infrastructure, the public cloud, and SaaS applications — which would be impossible to protect with a conventional VPN.

Tip #3

If your infrastructure no longer resembles the castle and moat model — it's time to re-evaluate your options for keeping it secure.

Zero Trust: A New 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 castle-and-model model used by VPNs, with Zero-Trust there is never 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". Since then, Zero Trust has been adopted and deployed by many other leading companies.

This new, decentralized authentication model also readily accommodates configurations spanning any number of applications that straddle on-prem, cloud, and SaaS infrastructure. Which means you can simultaneously leverage the latest cloud software in tandem with the legacy, locally-hosted applications some parts of your business may still rely on — all secured with the latest in encryption technology, and accessible by your team from wherever they are (provided you've considered the ruleset to permit this).

Speaking of which...

Tip #4

Give your team an authentication experience that is familiar and gets out of the way — so they can get back to work.

Give Your Team The Tools & Data They Need — And No More

One of the trickiest things for any company is ensuring 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.

Tip #5

Leverage a modern, zero-trust security solution to ensure every request to your network is fully protected.

Contractors and other third-parties

A related challenge facing many businesses is managing contractors and other third parties. An extended on and off-boarding processes can undermine some of the benefits of bringing on external support (they probably aren't keen on jumping through too many hoops to get started, either). 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, wherein the contractor receives a temporary code via email that grants them temporary access to designated systems. This is another way to streamline your contractor workflows, without compromising on security.

Tip #6

Streamline your contractor accesss on- and offboarding by letting them log in with accounts they already have, or one-time passcodes.

Securing your network

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

Historically, branch offices sent all of their Internet-bound traffic to one centralized data center at or near corporate headquarters. Administrators configured that to make sure all requests passed through a secure hardware firewall. The hardware firewall observed each request, performed inline SSL inspection, applied DNS filtering and made sure that the corporate network was safe from security threats. This solution worked 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 the offices went up. Costs went up, too. In the last 10 years, SaaS spending across all company size segments grew by more than 1615%. 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. The legacy approach to solve this problem is to add MPLS links from branch offices to the headquarters. But MPLS links are expensive, and can take a long time to configure and deploy. Businesses end up spending millions of dollars on legacy solutions, or they remain slow, driving down employee productivity.

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 84% of phishing sites exist for less than 24 hours (source) 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 that rely on static models to filter malicious traffic cannot keep up. As a result, employees remain vulnerable to new threats even when businesses backhaul Internet bound traffic to a single location.

The Cloudflare Solution: Introducing Cloudflare for Teams

Cloudflare for Teams

If the challenges outlined in this book resonate with you, Cloudflare for Teams 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 over 26 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 for Teams harnesses the power of Cloudflare's proprietary technology and empowers you to leverage it to secure your team, network, and data.

Tip #7

Onboard and offboard efficiently and with confidence by utilizing a security solution with granular access controls.

Cloudflare Access

Simple, secure access for internal apps.

One dashboard. All of your internal apps

A single pane of glass to secure your team's applications.

- Secure on-premise applications with SSO in hours, not months
- Standardize access controls across on-prem, private, and public cloud resources
- Manage access to internal apps on a per-user and per-application basis

Zero Trust. 100% Coverage

Extend zero trust security to private applications.

- Minimize exposed application surface and protect your assets from attack
- Implement a software-defined security perimeter without code changes
- Establish discrete perimeters of protection around key applications

Put your VPN on a performance improvement plan

Ditch your corporate VPN for SaaS-like ease of use for all internal applications.

- Authenticate users anywhere in the world with Cloudflare's global network
- Drive adoption and reduce IT overhead with a seamless, familiar login experience
- Improve end user performance with Cloudflare's distributed network and intelligent routing

Tip #8

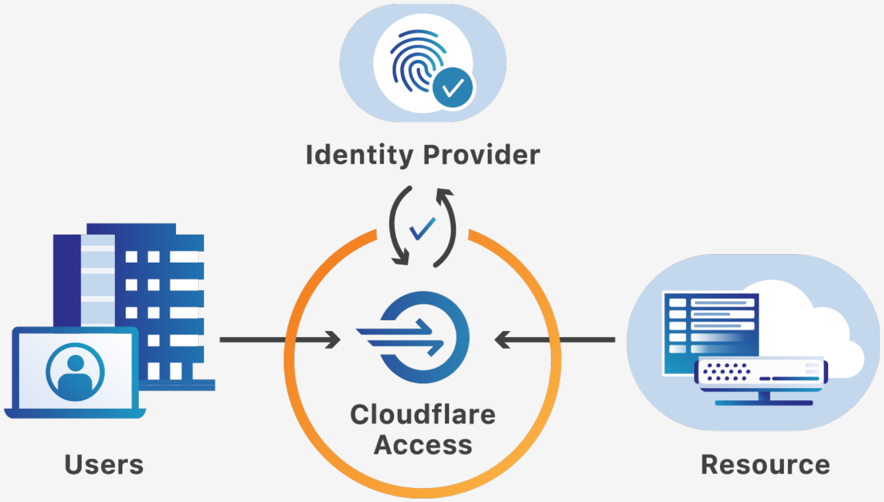
Look for an integrated platform to protect your team.

Cloudflare Access

Third party users? First class citizens

Seamlessly onboard partners and contractors without issuing and managing corporate login accounts.

- Integrate with multiple identity providers simultaneously
- Utilize popular identity provider options for external users, while your employees use your corporate SSO
- Connect securely from any device with no special software agent required



Audit logins, and everything else

Log and review every event.

- Generate logs for logins, access requests and policy changes across all of your internal applications, all in one place
- Search and investigate logs within the dashboard
- Integrate with SIEMs for enterprise visibility

Tip #9

Ditch your corporate VPN for SaaS-like ease of use for all your internal applications.

Cloudflare Gateway

A secure path to the Internet.

A safe harbor on the open Internet

Protect your users as they navigate the Internet.

- Keep malicious content off your network using DNS filtering
- Gain complete visibility into traffic on and off your network
- Stop zero-day threats by moving execution of web code from users' browsers to the Cloudflare edge

Build for the Cloud. Not the 1990s

Reduce your network complexity, spend, and latency with Cloudflare's global network.

- Manage, deploy and monitor your security policies in one place
- Stop backhauling traffic to HQ by sending Internet-bound traffic straight to Cloudflare
- Improve performance of applications on the Internet with Argo smart routing technology

Tip #10

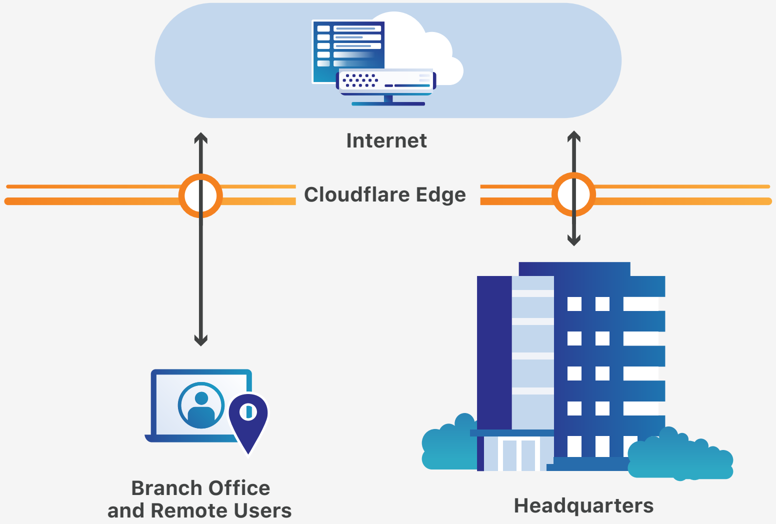
Trade cumbersome firewall appliances for easy-on traffic inspection and filtering.

Cloudflare Gateway

Speed up, costs down

Reduce spending on expensive MPLS links and legacy on-premise hardware.

- Deprecate your next-gen firewall appliance by leveraging the Cloudflare edge for traffic inspection
- Eliminate expensive MPLS fees by removing the need for office backhaul
- Integrate with SD-WAN providers to route traffic securely through Cloudflare's edge



Watch your data like a hawk

Get visibility into all of your Internet traffic with SSL inspection.

- Scan for threats in disguise with deep packet inspection
- Identify devices that are compromised by malware, command & control callback, or other security threats
- Identify unsanctioned SaaS applications
- Visualize all your Internet traffic
- Push logs to your SIEM