CLOUDFLARE

8 Keys to Securing Your Remote Workforce

Modern remote teams are made up of whatever combination of people can get online and get the work done. That means many different kinds of users are working together in the same tools — full-time employees, contractors, freelancers, vendors and partners. How do you protect your company's data everywhere it's hosted without slowing them down? Here are 8 best practices to secure modern remote teams without slowdown.

1. Secure access to internally managed applications

You may be using a conventional VPN to secure your business's internal apps — but that model tends to fall over as employees connect remotely at scale. What's worse, VPNs are overly permissive, trusting anything that makes it past the front door.

Modern solutions rely on the zero-trust model: digitally interrogating every packet of data, without the frustration or performance degradation of a VPN.

2. Protect your team from threats on the Internet

If you leverage any combination of SaaS applications, your team is potentially exposed to the wilds of the Internet. Historically companies have routed outbound Internet requests back to HQ for threat scanning — but that's slow and untenable at scale.

You need a way to identify and stop the latest threats, without bringing your team to a standstill.

3. Secure your corporate data, wherever it lives

Your businesses' most valuable data may straddle SaaS vendors, internal applications, the public cloud, and more. Ensuring that this data only goes where it should requires protection designed to support any combination of on-prem and cloud-based services.

8 Keys to Securing Your Remote Workforce

4. Leverage tools that anyone can figure out.

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).

Why not use a system that's already familiar to them — one that utilizes the same Google or Okta login they're used to?

5. Fast-track your contractors

The modern workforce is fluid. As contractors and other external partners work with your team, it's important to ensure they have everything they need from day one — but no more. And once the job is done, you need to be confident that their permissions have been revoked.

A modern authentication solution will work seamlessly with a variety of identification providers, including widely-available free services that your contractors are likely already using.

6. Make tools easier to find.

High-performing remote teams make it easy for employees to find the right tool when they need it. App launchpads were designed to be a life-raft in the tools ocean, bringing every application a user can access into one easy, graphical dashboard.

Some launchpads are better than others: make sure yours supports granular permissions, to ensure employees are only seeing tools they have access to.

7. Consider new solutions for old problems

If you've been bogged down by legacy applications, this might be the right time to consider one of the many mature SaaS solutions. Provided you have the right tools to secure them, SaaS apps afford a high degree of functionality, continual updates, and subscription models that are easier for many businesses to handle over extended periods than a lump up-front payment.

8. Get a heads up when something goes down

The dashboards in the office may have gone dark, but that doesn't mean your insight needs to. Ensure you use a solution that supports extensive logging and auditing of every request — with the flexibility to export to security information and event management (SIEM) platforms.

Unlock safer and faster remote work for your team today at teams.cloudflare.com