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.