ProofID

Ping Identity

5 WAYS TO MAKE WORKING FROM HOME SECURE AND PRODUCTIVE

With a global shift to working from home employees require a secure and productive environment. If employees can't access applications and information securely from remote locations, their productivity will decrease and the security of key corporate assets will be at risk.

Together with our partner Ping Identity, we are prepared to help IT organizations with the following immediate steps to ensure employees can be productive anywhere in the world.

1. Put multi-factor authentication everywhere

52% of data breaches are due to hacking, and of those, 80% are due to weak or compromised passwords.[1] Multi-factor authentication (MFA) can reduce password risk by 99.9%.[2] Putting MFA everywhere is a no-brainer, especially on VPN connections and for employees that use personal devices (BYOD) when they work from home.

2. Leverage intelligence so that added security doesn't add friction

As more employees work outside the corporate network, intelligent authentication helps you make better decisions about who should have access to resources. Continuously evaluate risk scores based on user behavior and location to better understand when to grant access, when to step-up authentication or when to deny access—all without impacting employees' productivity.

3. Being on the network shouldn't automatically grant access

Organizations enable VPNs for remote access, but this often allows employees to access more than they need. Since 23% of sensitive data breaches are caused by internal employees,[3] someone shouldn't have access to everything just because they're on the network. To mitigate risk, enforce least-privileged access and establish Zero Trust security for apps, APIs and data.

4. One password is not only more secure, it's more productive

On average, employees spend 10.93 hours per year entering and resetting passwords.[4] This slows down remote employees as they sign on to applications to get their work done, like collaboration apps for instant messaging and video conferencing. Federated single sign-on (SSO) and self-service password reset gives employees back all those hours and lets them get back to work. Better yet, strong authentication methods, such as biometrics and FIDO2 keys, can make passwords a thing of the past.

5. Put digital business resources at workers' fingertips

There's a streamlined app for just about every business task. But employees may struggle to find all these tools—or just forget to use them now that they're not in their usual work environment. They may also find them difficult to access, since some are on-prem and some are in the cloud. With a dock for SSO to all digital resources in one place, employees can easily find, access and use apps to get more work done from anywhere.

We want to help you get your work-from-home workforce secure and productive, right now. **Click here to Get fast, free, cloud SSO and MFA for unlimited apps and unlimited identities.**

[1] Verizon 2019 Data Breach Investigations Report
[2] Microsoft Security Intelligence Report, 2018
[3] Forrester Analytics Global Business Technographics Security Survey, 2019
[4] Ponemon 2019 State of Password and Authentication Security Behaviors Report