Proofpoint Remote Working and Business Continuity

PRODUCTS

- Proofpoint Meta
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Cloud Account Defense

KEY BENEFITS

- Provide remote workers with the same levels of security and access as those who are on the network
- Quickly and effectively provide employees and contractors with secure remote access to applications in the datacenter and cloud
- Allow remote workers to browse the web while keeping malicious code execution away from their corporate device
- Educate employees on additional risks faced when working remotely
- Identify and respond to suspicious cloud account activity

Your people are spending less time in the office and more time working remotely. But they continue to be the No. 1 target for attackers. Working safely and securely from remote locations has never been more important. However, legacy methods of remote access can open potential security risks and potentially issues of scale. Combine this with the fact that remote workers are not necessarily behind all the security controls that the organisation has implemented, and the risk can increase even further. We can help you to enable remote working quickly and securely while reducing your risk.

Proofpoint delivers zero-trust networking through client or clientless access for managed or unmanaged devices. We provide granular access to required applications only, regardless of their location. And we ensure security by isolating web traffic to prevent malicious code from executing on the corporate device. This reduces your risk as attackers pivot to personal email accounts.
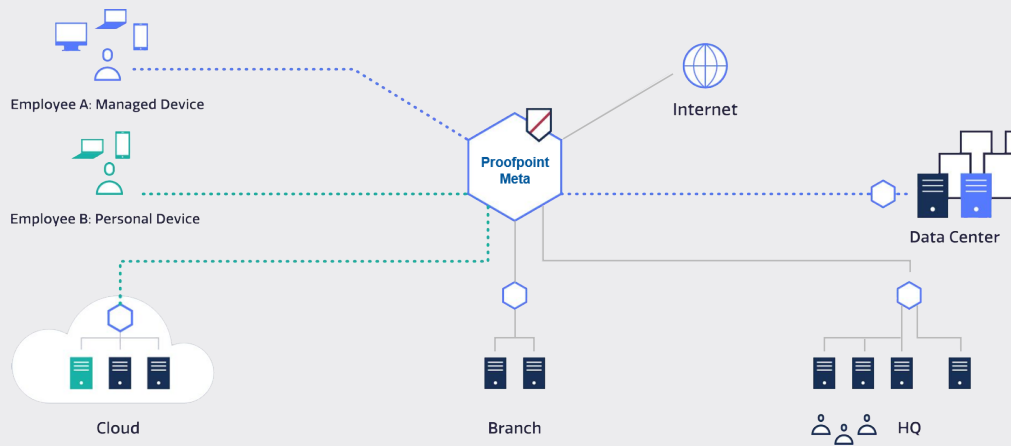
ENABLE REMOTE WORKING

Rapidly Connect Your People To Your Applications Without Location Constraints

Your data and applications are just as distributed as your people. Proofpoint Meta gives you a zero-trust way to quickly connect your remote employees, partners and customers to your datacenter applications and your cloud infrastructure. With tighter security, a superior user experience and reduced IT management, it delivers segmented, verified and audited access for every type of user. This eliminates the many headaches of legacy VPNs. These include overly permissive access, slow connections, and endless administration — not to mention user capacity limitations, traffic bottlenecks, software client requirements and hardware deployment.

Our granular access policy reduces your exposure by granting each of your users explicit access to specific applications. You can enable access to authorised applications wherever they are located—with a single, always-on connection. And our cloud-native, encrypted overlay network features global PoPs in order to optimise performance. What's more, our cloud-delivered secure access solution frees up your IT team. They no longer need to manage rules and troubleshoot problems across appliances in multiple locations.

Prevent Malicious Content From Impacting Corporate Devices

Attackers who target remote workers know they may not be behind enterprise security protection. And they may also be using personal devices and/or have access to their own personal email accounts. Proofpoint Browser Isolation prevents your users from exposing your organisation to additional risk. At the same time, it respects the privacy of your people when they access personal webmail and untrusted sites. Any content accessed inside Browser Isolation is rendered using URL isolation technology. This allows your people to browse the Internet safely and confidently, without risk.

ONLY SAFE CONTENTS
(HTML-CSS)

SECURE CONNECTION
(HTTPS)

HIGH RISK CONTENTS
(.JS, .EXE, ETC.)

ANONYMOUS WEBSITE
TRAFFIC

Browser

Proofpoint Isolation

Public Internet

SECURE REMOTE WORKING

Educate Your Employees on Additional Risks to the Corporate Environment

Your employees face unique security scenarios when working from home or remotely. With Proofpoint Security Awareness Training, you can provide your people with specific training about remote working. These include securing devices, protecting Wi-Fi networks, and understanding the additional security challenges they face when working outside of the office.

Identify and Respond to Suspicious Cloud Account Activity

Today's attackers use a variety of methods to compromise and take over cloud application accounts. And once they do, they can launch attacks inside and outside of your organisation. This impacts your reputation and your finances.

With Proofpoint Cloud Account Defense (CAD), you can protect your people and your organisation from a Microsoft Office 365 and Google G Suite account takeover. It allows you to detect, investigate and defend against cyber criminals trying to access your sensitive data and trusted accounts. CAD is fast and easy to deploy, and it secures Office 365 and G Suite users on any network or device. This allows you to confidently drive your business forward, regardless of the location of your people and security team. And it helps you to make the most of Office 365 and G Suite.

"We have had over 400,000 successful completions of safer web browsing, password security, email security and mobile device security training modules. And more than 32,000 of our users completed the mobile device security training module in two weeks. This is amazing for non-mandatory training. We have now justified the cost of training with just those 4 modules! We are very happy with our investment."

Security awareness and training director, Large technology company

LEARN MORE

For more information, visit **proofpoint.com**.

---

proofpoint.