Remote Working Security Readiness Quick Guide

To support remote working many businesses need more than collaboration tools to function, such as existing applications and cloud services. Organisations may also unwittingly introduce vulnerabilities into their information environments in the rush to enable remote working which exposes business information to new threats. This guide will introduce four basic ideas about how to ensure that your employees and customers can securely access services and information securely from any location without relying on traditional on-premises security tools.

Cloud and On-Premises Information

Cloud workloads (such as Office 365) may have been hastily deployed without consideration for security. Access to line-of-business (LOB) applications that only exist on-premises may not be easily supported, secure or even possible. The risk of exposing legacy applications to the Internet to enable remote working could be high, especially if the application is not supported, has vulnerabilities or doesn't support modern authentication.

The corporate network perimeter has vanished

The perimeter we once relied on has rapidly evolved into what is now more like a distributed digital footprint.

Staying on top of all of the following, it's no easy task:

- Ensuring your new newly extended information landscape stays available, engaging and responsive.
- Being able to combat attacks & stay ahead of digital threats.
- Maintaining a level of security like no other using industry leading identity and access policies, encryption and communication protocols.

Devices that were previously behind the perimeter of the business network are now operating on untrusted networks.
On-premises security solutions for security are often less effective or cease to function when employees work from home.

New threats to remote workers

Like any time of global uncertainty, with enough attention the wrong crowd can be drawn, and this goes the same for the threat-actors on the internet. In the past month, an alarming rise in phishing emails related to COVID-19 and a new form of ransomware (Pysa) has started circulating out of France.

Our own cyber threat intelligence has shown us over 320 new domains registered that relate to the pandemic in New Zealand alone in last half of March, many of which are malicious and designed to trick people into thinking they are legitimate. In the rush to enable a distributed workforce we have also detected over 1 million new RDP ports opened with critical vulnerabilities.

Trusted devices on untrusted networks

Nearly every data breach in history had two things in common; a firewall and an anti-virus that failed to detect and prevent the attack. Now devices are operating outside of the firewall and likely with an anti-virus that may not be able to be updated so the risk to your data, identities and business operations is now much higher. Ensuring that your remote workers use devices that are trusted, protected and free from vulnerabilities and security misconfigurations will add an important layer to your defences.

Security of your remote workforce does not have to add friction or complexity. In fact, the best security is tied to a seamless user experience because happy users are less likely to try to circumvent poorly designed or prohibitive security controls. The IT systems that support remote, mobile and secure communication have never had so much riding on them. VPNs might solve some remote access issues but require additional configuration, identity and access management and can impact the user experience. Without the corporate firewall and in some cases without any form of control on the endpoints, it's integral to consider modern mechanisms of ensuring security without compromising on user-experience.

Actions to secure your remote workforce

Secure your cloud

Ensure you have implemented best practice for your cloud solutions such as Office 365. This includes protection of your identities using multi-factor authentication, but also removing default configurations that can easily allow hackers to exploit emails and documents and business functions.

Shield your apps and data

Allow secure remote access to your on-premises applications using an application proxy, single-sign-on or cloud shielding service that supports modern authentication, encrypts data in transit yet making them invisible to hackers without the need for a VPN

Minimise the risk of remote access

The rapid transition to remote working may have introduced new risks such as opening ports or exposing vulnerable services that should not be directly exposed to the Internet. Understanding what your newly distributed business now looks like to an adversary on the outside is important to reduce or remove the options to deliver an attack against your business.

Use trusted devices

Now that your devices are outside the network or that your employees are using their own devices, it is increasingly difficult to protect the device they use to access your on-premises applications or cloud environments. Build trust into remote devices by ensuring they remain fully patched and only use secure means to connect without burdening the user with additional tasks, passwords or VPNs.

? Security questions to consider:

- Do you know which cloud services your business is using and who can access it?
- Are your devices able to receive updates and patches outside of the office?
- Are your endpoints adequately protected outside of their usual environment?
- Do you still have a level of control of your assets and identities about who is accessing information and from where?
- What risks do vulnerable applications create to your business information when being accessed remotely?

Contact us to find out more and let us help keep your organisation secure.

PREDICT. DETECT. PREVENT. RESPOND

Better cyber security starts here