ENTERPRISE
IRON

Transforming Telework in the Post COVID-19 Workplace

By Sergio DuBois

Firms confronting the "new normal" of a COVID-19 pandemic and economic shutdowns faced unprecedented challenges. Many organizations came to realize that they only had the capacity and licenses to handle a fraction of their workforce working remotely. Even with the drive towards cloud-based applications and data, always-on VPNs (virtual private networks) were suddenly required for the entirety of their workforces' remote access.

Remote access network segments were not originally designed with the load of the entire workforce working simultaneously and required expansion to meet burgeoning remote access performance requirements. Many VPNs were crushed by a demand that was never planned for. Technology portfolios found themselves without the licenses that would be required to support an entirely remote workforce.

Many VPN networks were crushed by a remote workforce demand that was never planned for.

IT Security and Risk management leaders tasked with infrastructure security and remote access had to determine remote access requirements in the context of the once unimaginable requirement that the entire workforce operate remotely:

- **Remote work policies** needed definition or expansion to align with the new normal possibilities of entire workforces working remotely.

- **Portfolios needed rationalization** to determine when cloud-based services could be employed and how on-premise applications would be used remotely.

- Products and **remote access technologies needed performance testing** to ensure that they were capable of taking on the load of an entire workforce relocation to remote access.

- **Unknown devices had to be evaluated** for the security vulnerabilities they present such as for BYOD (Bring Your Own Device).

In the past decades, organizations have evolved from entirely relying on VPN technologies to enable remote access to enterprise applications towards the increasing trend of providing cloud-based services. Yet, many organizations still route all network traffic through a corporate VPN including these cloud-based services.

During emergencies like the COVID-19 crisis, this proved a problematic choice, as the performance of these cloud-based services was choked with the inordinate traffic placed on VPNs. This resulted in many users bypassing their corporate networks and accessing their cloud-based enterprise applications directly from their own personal devices on unsecured networks.

Solutions like a Cloud Access Security Broker (CASB) or Zero Trust Network Access (ZTNA) solution proved vital to address this surge in VPN demand and provide an alternative that retains greater enterprise control on access, while alleviating the performance impacts of funneling all cloud traffic through a VPN.

Opportunistic Phishing Attacks During the Pandemic

With countless employees relying on remote access connections to work from home, bad actors are exploiting remote working to launch attacks. Virtually all attacks require the end users' intervention to work and remote working is increasing that risk. This year companies are seeing a rise in data breaches and so called "Phishing" attacks via text and email.

> *A frightening number of COVID domain names exist solely to serve as phishing lures.*

Bad actors realize that employees are more vulnerable working at home and moving their "lures" to communications that appear to concern COVID-19 often proves irresistible to its threat targets which given society's attention to this subject. Over 4,000 domains have been registered this year that are named under the guise of COVID-19 and a frightening number of these exist solely to serve as phishing lures. They try to get users to click on a link or open a document, either of which exposes your employee's systems to malicious activities.

Remote Access Requirements

Rationalizing enterprise portfolios without understanding Remote Access Requirements leads to platforms that will perform unpredictably when faced with the massive remote access needs imposed during pandemics. Crippled performance and security are on the line, and it pays to have a precise understanding of the needs of an entirely remote workforce:

1. **Itemize users and work functions** – executive remote access requirements will vary wildly from field employees on specific granular work functions.

2. **Itemize devices and owners** - Security and the controls applied to mitigating vulnerabilities vary widely based on the kind of device and who owns the device.

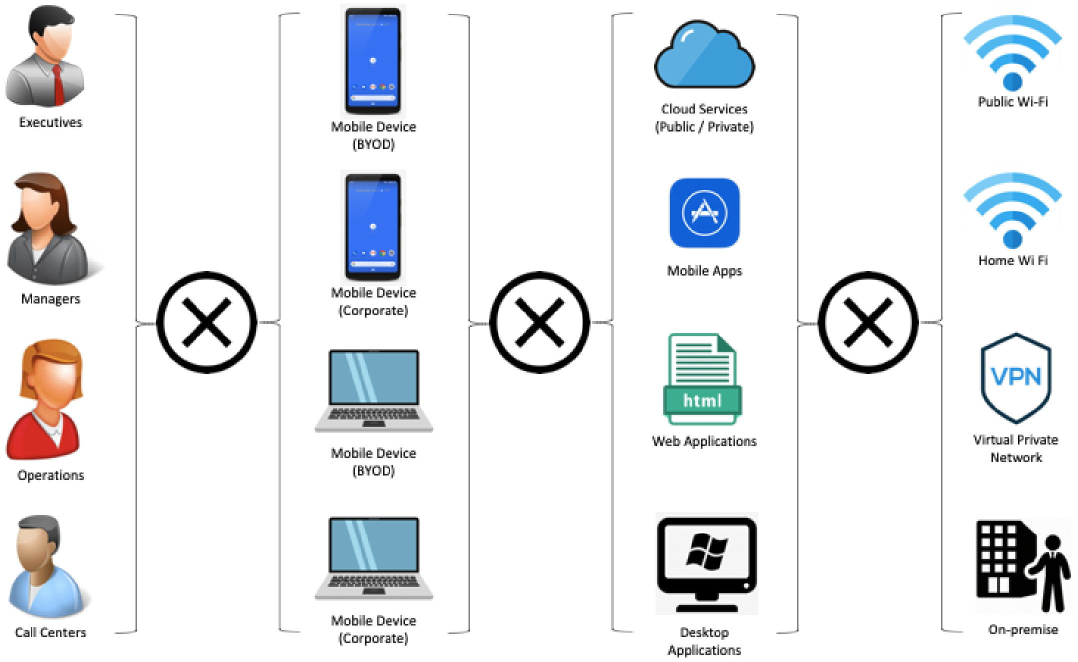
3. **Itemize applications and data** - on premise applications and data will have vastly different requirements than SaaS (Software as a Service) applications

4. **Itemize workplace locations** - where users are located is a factor that must consider a wide array of data privacy laws across national and local jurisdictions that could impact remote access strategies.

Based on these four parameters, each combination defines a distinct use case that must be mapped to a use case specific remote access solution pattern as part of a comprehensive strategy to align with the needs.

A Threat Model for Scaling Telework

Threat modeling in Telework identifies resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources. The model then quantifies the likelihood of successful attacks and their impacts. Finally, threat model analyzes this information to determine where security controls need to be improved or added. Threat modeling helps organizations to identify security requirements and to design the remote access solution to incorporate the controls needed to meet the security requirements.



Lack of Physical Security Controls

Telework client devices are used in locations outside the organization's control, such as employee homes, coffee shops, hotels and at conferences. The mobile nature of these devices makes them more likely to be lost or stolen, which places the data on them at increased vulnerability. When defining a telework strategy, security policies and controls, companies should *assume* that client devices *will* be acquired by malicious parties who will either attempt to recover sensitive data from the devices or leverage the devices to gain access to the enterprise network. The primary mitigation strategy for the threat of device loss or theft is to encrypt the client device's storage so that it cannot be recovered by unauthorized parties, or to not store sensitive data on client devices.

Even if a client device is always in the possession of its owner, there are other physical security risks, such as an attacker looking over a user's shoulder at a coffee shop and viewing sensitive data on the client device's screen. Organizations can mitigate threats involving device reuse, such as an attacker gaining remote control over a device or impersonating a user, by using a strong multi-factor authentication for enterprise access.

Unsecured Networks

Nearly all remote access happens over the Internet, organizations have no explicit control over the security of the external networks used by telework clients. Communications systems used for remote access include broadband networks such as cable and wireless mechanisms such as IEEE 802.11 and cellular networks.

Internet communications systems are susceptible to eavesdropping, which places sensitive information transmitted during remote access at risk of compromise. **Man-in-the-middle (MITM) attacks** may also be performed to intercept and modify communications. Organizations should plan their remote access security on the assumption that the networks between the telework client device and the organization cannot be trusted.

Risk from use of unsecured networks can be mitigated, but not eliminated, by using encryption technologies to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints.

Infected Devices on Internal Networks

Telework client devices, particularly BYOD and third party-controlled laptops, are often used on external networks and then brought into the organization and attached directly to the organization's internal networks. An attacker with physical access to a client device may install malware on the device to gather data from it and from networks and systems that it connects to.

If a client device is infected with malware, this malware may spread throughout the organization once the client device is connected to the internal network. Firms should assume that client devices will become infected and plan their security controls accordingly.

In addition to mandating use of appropriate **anti-malware technologies**, such as antivirus software on laptops, organizations should consider the use of network access control (NAC) solutions that verify the security posture of a client device before allowing it to use an internal network. Organizations should also consider using a **separate network segment** for all external client devices, including BYOD and third party-controlled devices, instead of permitting them to directly connect to the internal network.

External Access to Internal Resources

Remote access, including access from BYOD and third party-controlled client devices attached to an organization's wireless BYOD networks, provide external hosts with access to internal resources such as servers. If these internal resources were not previously accessible from external networks, they can be exposed to new threats particularly from untrusted client devices and networks when they are made available via remote access.

Each form of remote access that can be used to access an internal resource increases the risk of that resource being compromised. Firms should carefully consider the benefits of providing remote access to additional resources in terms of the potential impact of compromise. They should also ensure that any internal resources chosen to make available through remote access are hardened appropriately against external threats and that access to the resources is limited to the minimum necessary through **web application firewalling** and other access control mechanisms.

Guiding Principles for Telework Strategy

- **Threat modeling** - Before designing and deploying telework and remote access solutions, organizations should develop system threat models for the remote access servers and the resources that are accessed through remote access.

- **Plan for loss and theft of devices** - When planning telework security policies and controls, organizations should assume that client devices will be acquired by malicious parties who will either attempt to recover sensitive data from the devices or leverage the devices to gain access to the enterprise network.

- **Zero Trust** - Organizations should plan their remote access security on the assumption that the networks between the telework client device and the organization cannot be trusted.

- **Harden Internal Resources** - Organizations should ensure that any internal resources they choose to make available through remote access are hardened appropriately against external threats and that access to the resources is limited to the minimum necessary through firewalling and other access control mechanisms.

- **Tailor controls to the remote access use case** - When planning a remote access solution, firms should carefully consider the security implications of each of the various remote access methods possible as applied to combinations of users, devices, applications and workplaces.

- **Isolate BYOD network segments** - When considering permitting BYOD devices within the enterprise, strongly consider establishing a separate, external and dedicated network for BYOD use within enterprise facilities. Such a network may also be used for third party-controlled client devices if desired.

What Can Be Done?

Enterprise Iron has a rich history of helping our customers through trying times with a high degree of competency and success. In addition, we have introduced and scaled a world class VPN for our own staff. Given the specter of a potential round two of the pandemic, it is critical that the "new normal" - a secure, scalable, remote working environment with a reliable backbone be part of your business plan.

Our Subject Matter Experts can assess your infrastructure and devise a strategic and tactical roadmap that will best lead you to address whatever challenges lie ahead, COVID-19 related or not. We understand that time is of the essence, given the whirlwind of political, legal, technical and compliance activity that seems to morph on a regular basis. We can assess and produce an actionable roadmap in a compressed timeframe and our SMEs are at the ready to provide the expertise and guidance you need.

To learn more about how Enterprise Iron can help, please contact us at: eim@enterpriseiron.com