WHITE PAPER

Key Considerations for Implementing Secure Telework at Scale

Identifying the Security Risks and Advanced Requirements of a Remote Workforce

Executive Summary

The ability to rapidly transition an organization's workforce to telework is an essential component of a business continuity plan. However, remote workers create additional security requirements and different security challenges than on-site employees.

Remote workers often connect to the enterprise network over insecure or untrusted networks, potentially enabling eavesdropping, and use devices in insecure areas, where they may be lost or stolen. Advanced users may have requirements that cannot be met by a standard virtual private network (VPN) client.

Beyond these basic requirements, teleworkers may use untrusted devices to access company resources and are more likely to fall prey to social engineering during a crisis, creating more security risks. Additionally, these employees must be able to access cloud-based resources without significant network latency. It's for these more advanced requirements that basic security controls won't offer adequate security for a majority-remote workforce.

Introduction

Every organization's business continuity plan must include the capability to rapidly transition most or all of the workforce to remote work. Natural disasters, pandemics, or terrorist attacks are just some of the events that can make this necessary.

A secure, seamless transition from "business as usual" in the office to a fully remote workforce requires planning and careful consideration of the requirements of teleworkers, such as access to network resources, ample bandwidth, and technical support. The transition also amplifies the security risks of telework, due to home network and personal device vulnerabilities, as well as the challenges of supervising and enforcing good cyber hygiene.

54% of IT professionals believe that remote workers pose a greater security risk than on-site personnel.[1]

Only 74% of companies require a VPN for teleworkers.[2]

Secure Connectivity and Productivity Challenges

The first step in a secure telework strategy is ensuring that remote workers have the ability to connect securely to the enterprise network. There are challenges both in securing remote connectivity and in maintaining user productivity over the remote connection. These have to do with the home networks, the users themselves, and the network equipment at the corporate office.

Home networks are vulnerable

For employees, the most straightforward way to connect to the enterprise is through their home network and the public internet. The employee's home network, however, is likely less secure than the enterprise network, making it more vulnerable to attack.

Traffic between the remote worker and the enterprise network could be intercepted, and potentially modified, by an eavesdropper. Additionally, the network traffic that does not pass through the enterprise network is not protected by an organization's on-site security solutions, making them more vulnerable to malware.

Teleworkers may not be who they seem

Under normal circumstances, many organizations rely upon a perimeter-based security model. Under this model, anyone inside the network is considered trusted, while outside parties are potentially malicious. This enables an organization to identify anomalous connection attempts based upon the location and timestamp (since most workers operate during normal business hours).

With a fully remote workforce, this traditional model is no longer applicable since both legitimate users and potential threats connect to resources from outside of the network and may work at odd hours. Additionally, when employees are working remotely, the probability of an unauthorized user gaining access to and control over an employee's devices is higher.

VPN headends lack scalability

During "business as usual," many organizations do not have telework policies. In fact, only 41% of businesses allow remote work.[3] As a result, many organizations lack the infrastructure necessary to support a fully or mostly remote workforce.

Under normal circumstances, a significant percentage of a user's traffic is internal to the network, accessing internal file shares, databases, and other resources. However, when employees work remotely, all their traffic passes through the perimeter firewalls, increasing the load on these devices.

The use of VPNs only exacerbates this problem. Encryption and decryption of VPN traffic is computationally expensive and can rapidly exhaust the CPU resources of a next-generation firewall (NGFW).

One-size-fits-all telework does not work

For the general worker, a secure connection to the enterprise network and cloud-based resources is sufficient to perform their job duties. However, some employees have additional requirements when working remotely.

Power users, such as network administrators and security personnel, require persistent connectivity to the network. These users may require the ability to connect multiple devices to the network, which can be difficult to manage manually via VPN clients, or connections that last longer than the standard session timeout length of VPN clients.

Super users, including executives and other management personnel, regularly process highly sensitive data and need to be able to do so while working remotely as well. These employees require a higher level of protection than that provided by most VPN clients.

Enforcing Cybersecurity Policies in a Crisis

Beyond the basic needs of a remote workforce, telework creates additional security challenges for an organization. Considerations include the use of insecure devices for work, an increased probability of security incidents during a crisis, and teleworkers' need to efficiently access cloud-based applications.

Incident response is more challenging for remote workers

Situations that force an organization to transition to a remote workforce are often chaotic and emotional for employees. In general, humans are prone to making poor security decisions in these situations, and cyber criminals regularly capitalize on these emotions to perform their attacks.

During times of crisis, employees are more likely to fall for phishing attacks, and an organization is likely less prepared to respond to the incident. With a remote workforce, the help desk is less immediately available to an employee, and an organization's incident response plans may not cover contingencies where a teleworker experiences a security incident. As a result, the cost to the organization, in both employee productivity and remediation efforts, can be much higher during remote work.

Remote workers may lack vital security patches

Organizations without an established telework policy often do not have sufficient company-owned devices to support a fully remote workforce. As a result, employees working from home may be using unapproved devices, including personal laptops or tablets.

Only 15% of organizations have completed a transition to a zero-trust security model, which does not automatically assume that anyone inside the network perimeter is trusted.[4]

75% of IT professionals believe that the risk of a data breach is higher for remote workers.[5]

The remote desktop protocol, used by system administrators for remote device management, is ransomware's primary infection vector in 70-80% of cases.[6]

42% of remote computers receive security patches within three days, compared to 48% of on-site machines.[7]

The ability to enforce bring-your-own-device (BYOD) policies is essential when employees are working from home. Devices used by remote workers historically have lower patch rates than on-premises devices, even if all devices are owned by the company.[8] These delays in patching can be expensive, since 60% of data breaches are caused by an unpatched vulnerability for which a patch was available.[9] An organization must be able to perform pre-connect scans for patching compliance to ensure that remote workers are not exposing the enterprise network to additional cyber risk.

Teleworkers require efficient, secure cloud access

When employees are working on-site, securing their connections to cloud-based resources using on-site security appliances is logical since traffic already passes through the network perimeter. However, remote workers are connecting from outside the network with traffic bound for the cloud.

Backhauling teleworkers' cloud-bound traffic to the enterprise network for security scanning increases network latency. This can create performance issues for latency-sensitive Software-as-a-Service (SaaS) applications and negatively impacts teleworker productivity.

As organizations become more reliant upon SaaS solutions as part of remote work, they become a greater target for cyber criminals. Misconfigurations in security policies and configuration settings on SaaS applications could be the cause of a data breach or enable cyber criminals to use them as an infection vector for malware.

62% of companies allow BYOD for remote workers.[10]

Organizations rapidly deploying cloud-based solutions to support remote work are more likely to misconfigure security settings.[11]

Basic Telework Security Is Not Enough

Transitioning most or all of an organization's employees to remote work creates significant security challenges for an organization. An organization's business continuity plan should take these challenges into account and include solutions to address these new risks.

Deploying basic security controls for telework, such as VPN connectivity and strong user authentication, enables an organization to support intermittent remote work by a fraction of its employees. However, business continuity means an organization should be capable of maintaining normal levels of productivity and security with a mostly or wholly remote workforce. Accomplishing this requires securing the endpoint and ensuring high-speed, reliable access to vital SaaS applications.

[1] "Remote Work Is the Future—But Is Your Organization Ready for It?," OpenVPN, accessed April 29, 2020.

[2] Ibid.

[3] "The Modern Workplace: People, Places & Technology," Condeco, May 2019.

[4] "2019 Zero Trust Adoption Report," Cybersecurity Insiders, November 2019.

[5] "Data Protection Report 2019," Shred-it, June 17, 2019.

[6] Lawrence Abrams, "FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips," Bleeping Computer, February 27, 2020.

[7] Robert Lemos, "Patching Poses Security Problems with Move to More Remote Work," Dark Reading, March 31, 2020.

[8] Ibid.

[9] "Costs and Consequences of Gaps in Vulnerability Response," ServiceNow and Ponemon Institute, October 29, 2019.

[10] "Remote Work Is the Future—But Is Your Organization Ready for It?," OpenVPN, accessed April 29, 2020.

[11] Liam Tung, "Microsoft Office 365: US issues security alert over rushed remote deployments," ZDNet, April 30, 2020.

May 12, 2020 8:53 AM
D:\Fortinet\Work\2020\May\051220\wp-teleworker