SOLUTION BRIEF

Beyond the Basic Security Considerations for Telework at Scale

Executive Summary

When organizations implement telework at scale, cyber criminals leap at the opportunity to exploit the numerous security gaps that arise. These range from security naïveté among new teleworkers, an increase in the use of personal devices for work, and vulnerable home networks that serve not just the teleworkers but also their family members. Enabling organizations to secure telework at scale quickly and cost-effectively, the Fortinet Security Fabric offers integrated solutions covering three primary areas of concern: endpoint protection, network access control, and cloud access.

Introduction

When business continuity situations require urgent implementation of telework at scale, most organizations first figure out how to boost virtual private network (VPN) connectivity capabilities and enable remote access to corporate applications and data. It takes some stepping back to consider how well the new VPN setup maintains the organization's security posture. But corporate security leaders do not have the luxury of time. Cyber criminals are attuned to massive upticks in telework and stand ready to exploit, not only the new remote workers but also their family members, as attack vectors into corporate networks.

Organizations must act fast to secure whatever endpoints employees are using—whether corporate-owned laptops or personal devices. The on-premises headend must also be secured against unauthorized network access, as must any cloud environment the organization uses. Doing all this while most users are out of reach of corporate IT services—and oversight—means implementing zero-touch, highly automated security that can be monitored and controlled from a single pane of glass.

Several components of the Fortinet Security Fabric help achieve these goals: FortiEDR endpoint detection and response, FortiNAC network access control, FortiClient advanced endpoint protection, and FortiCASB cloud access security broker.

Protecting Remote Employee Endpoints

Traditional on-site workers who find themselves thrust unexpectedly into telework are understandably more stressed. They are less likely to engage in proper cybersecurity hygiene and are thus more susceptible to phishing and other malware attacks.

When their remote workers' devices become infected, IT departments will find themselves in a quandary. The typical remedy of rebuilding and re-imaging infected endpoints is not practical for remote working at scale. The productivity losses employees will incur, both while waiting for loaner laptops to arrive and while working on the less-than-optimal loaners, may last anywhere from several days to a few weeks.

To keep users secure without impacting their productivity, **FortiEDR** delivers advanced, real-time threat detection and mitigation for endpoints. It proactively reduces the attack surface, prevents malware infection, detects and blocks malicious activities in real time, and can automate response and remediation procedures with customizable playbooks. FortiEDR helps organizations stop breaches in real time automatically and efficiently, and enable remote remediation without taking endpoints offline or otherwise disrupting business operations. In short, FortiEDR turns endpoints into self-healing productivity centers.

FortiEDR Use Case: Potentially Unwanted Applications

Remote workers often have admin rights, raising the risk that they might inadvertently install potentially unwanted applications (PUAs) or perform other actions that introduce vulnerabilities. FortiEDR provides admins visibility into applications installed on the endpoint, along with the applications' reputation scores and vulnerabilities. Admins can proactively reduce the attack surface with communication control policies. These allow questionable or vulnerable applications to run, but limit their ability to communicate, thus neutralizing threats such as malware-infected PUAs connecting with command-and-control sites.

Defense in Depth at the Headend

As more employees work from home, the use of personal devices for work is likely to rise. In a business continuity situation, as telework surges, so does the variety of personal devices used, including older and nonpatched devices. When these devices are connected through a VPN tunnel to the corporate network, they become conduits for malware and other threats. Enforcing bring-your-own-device (BYOD) usage policies can be painstakingly difficult.

Therefore, in addition to hardening the endpoints, organizations implementing telework at scale must shore up protection at the headend. Seamlessly integrating with the VPN concentrator and profiling devices as they connect, FortiNAC provides:

- **Control**—full, partial, or no access, based on the device profile
- **Visibility**—across all connections to the network, including IPsec and secure sockets layer (SSL) VPN tunnels
- **Network monitoring**—continuously watching for new connections and changes in connection status, taking automated action against suspicious events

FortiNAC Helps Enforce Patching Policies

If keeping endpoints patched and up to date within an office setting is difficult, it is even more so when much of the workforce is remote. Organizations can leverage FortiNAC to enforce patching policies for remote workers. For example, they can configure a policy to allow only patched machines to connect to the network, while sending unpatched machines to a remediation-only VLAN for updating. FortiNAC can also enforce these policies for machines connecting via VPN tunnels.

Addressing the SaaS Security Imperative

Cloud security challenges compound with telework at scale. If remote workers are required to connect to corporate cloud-based applications through their VPN, the ensuing latency and bandwidth congestion will quickly render these applications unusable.

The better option is to enable users to connect directly from home to their Software-as-a-Service (SaaS) applications. Installed on the endpoint, FortiClient allows split tunneling, so remote workers have a secure (VPN) connection to network resources like email or databases, as well as a direct link to the internet and SaaS applications. FortiClient also provides protections to ensure that internet-based transactions cannot backflow into the VPN connection and jeopardize the corporate network.

Other cloud security concerns include cloud application visibility, compliance, data security, and threat protection. These concerns are typically addressed with cloud access security broker (CASB) tools. If an organization has not implemented CASB yet, it should seriously consider doing so now; SaaS use will increase significantly as teleworkers rely on remote collaboration tools to compensate for the lack of in-person meetings.

The Fortinet CASB solution, FortiCASB, provides policy-based insights into users, behaviors, and data stored in major SaaS applications, combined with a comprehensive set of reporting tools. By placing SaaS security in the cloud, IT security managers can scan provisioned cloud resource configurations and SaaS application data for threats, proprietary information, or sensitive customer records. FortiCASB also ensures that all SaaS users are monitored and protected no matter where they are or what device they are using.

When companies implement telework at scale, they can keep users secure and productive with the self-healing endpoint protection of FortiEDR.

Supplementing endpoint protection, FortiNAC provides a second line of defense at the headend, enforcing access control policies on remote devices that may or may not be secure.

FortiCASB bolsters cloud security for telework at scale through:

- Visibility into SaaS app usage for approved, sanctioned, and unsanctioned, aka Shadow IT
- Extension of existing data-centric security polices to the cloud, shoring up cloud security and protecting valuable data and IP assets
- Threat protection by identifying and addressing risky activity and data, including malware and the risk of malware propagation
- Compliance enablement by ensuring SaaS usage is aligned with critical business objectives and specifically compliance requirements, which can vary by industry and region

Fortinet Security Fabric Facilitates Business Continuity

When disaster strikes, organizations must move quickly to ramp up VPN access for remote workers and ensure security through endpoint detection and response, network access control, and secure cloud access.

However, adding a collection of disparate security tools can create new management and configuration issues when security teams are already stretched thin. As part of the Fortinet Security Fabric, FortiEDR, FortiNAC, FortiClient, and FortiCASB are seamlessly integrated with consolidated management, orchestration, and reporting tools. The broad, integrated, and automated Security Fabric reduces the overhead associated with telework security deployment, configuration, and troubleshooting. All this ensures that the network remains secure, users remain productive, and the organization continues to thrive.

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 6, 2020 11:56 PM

651216-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Teleworker Additional Security\sb-FA-beyond-the-basic-security-consideration-for-telework-at-scale-562020