WHITE PAPER

Securing the Immediate Shift to Remote Work

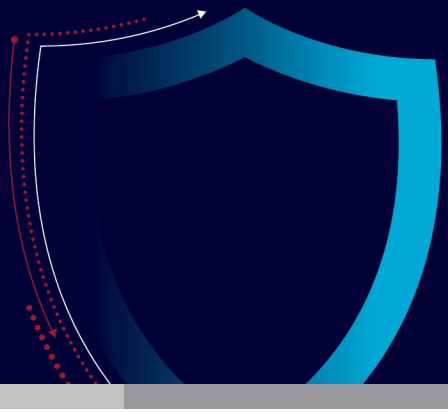

TABLE OF CONTENTS

Introduction

VPN as a Threat Vector

Public Services that Require CAC Authentication

Anatomy of the Modern Attack Landscape

Use Case #1: Standard Operating Environment (SOE) Used Remotely

Use Case #2: Bring Your Own Device (BYOD) Environment Used Remotely

Use Case #3: BYOD Environment Connecting to Government Resources

Use Case #4: Bring Your Own Device (BYOD) Mobile Device Access

Conclusion

Introduction

Securing a network infrastructure has never been a static activity. Adjustments are always needed but are normally related to disruptive technologies that are introduced over time. What we are experiencing now is a massive shift in network architecture in an unprecedented short period of time. The migration of a workforce from inside a network to remote locations has already strained corporate (and government) resources driving the need for upgrades, but this initial wave of IT upgrades is not the only challenge that organizations will face.

We believe that there are three phases of this forced migration:

- Physical IT infrastructure expansion
- Security Incident Identification expansion
- Zero Trust architecture expansion

The physical expansion has already been solved through the expansion of VPN gateways, load balanced firewalls, traffic shapers, etc. Network architects relied on the concept of beefing-up the existing connectivity as a stopgap measure to handle the increased load. The cloud transformation will continue for those organizations that have already committed to those activities. This challenging computing environment will force organizations to be nimble and secure by adopting capabilities like Symantec® Zero Trust Network Access (ZTNA) achieving point-to-point connectivity at the application level, cloaking all resources from the end-user devices and the Internet. The network-level attack surface is entirely removed, leaving no room for lateral movement and network-based threats.

This paper will focus on the threats that will certainly seek to take advantage of the workforce migration. Solution architects demand the use of VPNs for information security, but the location and security posture of the endpoint will be critically important in defending an enterprise as will an evolution of Security Operations Center (SOC) business processes. Finding actors who are living off the land and using built-in system commands is a manually intensive process without the correct toolset, such as the Symantec Targeted Adversary Analytics framework from Broadcom.

The increase in remote users and their transition to home machines which are often less protected than corporate machines will overwhelm many SOCs with additional data from these users, making it much more difficult to identify malicious activity among benign log entries.

The use of Standard Operating Environment (SOE) endpoints verses Use Your Own Device (UYOD) endpoints will be a critical policy decision for leaders to make. We will introduce some threat vectors that may have existed and are under the radar of many organizations not familiar with a remote workforce. We will then offer four use cases and a recommended security posture that will offer state of the art protection and monitoring.

VPN as a Threat Vector

BECAUSE A VPN CAPABILITY IS THE CURRENT DEFACTO STANDARD FOR SECURING REMOTE ACCESS TO A NETWORK, IT IS A FOCUS OF ATTACK FOR AN ADVERSARY

Because a VPN capability is the current defacto standard for securing remote access to a network, it is a focus of attack for an adversary. Much has been written recently about SSL VPNs and the wide use of unpatched flaws that allow actors to attack the infrastructure of an organization. Organizations that are adding VPN concentrators are adding to the workload of their IT staff, but also increasing the surface area that must be monitored for an attack. The user end of the VPN also becomes an increased threat vector, in that machines that connected only via the corporate network are now connecting via a home network. These machines are exposed to additional threat vectors (other compromised machines on the home network, man-in-the-middle attacks against the home network provider, spoofed WI-FI networks, etc.) and if compromised, would provide direct access to the internal corporate network via VPN.

Split tunnels can be used to route corporate traffic into a VPN tunnel with other Internet connections routed to the machine's next hop. The operational benefit of this type of VPN configuration is a reduction in physical load on the VPN concentrators and fewer log entries to be analyzed by the SOC. Split tunnels put the burden on the endpoint and the user to be both technically secure and securely vigilant. If a phishing campaign is successful in a split tunnel configuration, the threat to the organization is real if and when the VPN tunnel is up.

Public Services that Require CAC Authentication

Military organizations use Common Access Cards (CAC) as a means of authenticating to a machine or service. Civilian organizations use Personal Identity Verification (PIV) cards to perform the same function. Utilizing a CAC card to authenticate opens the user to similar threats as they would face using a split tunnel. If the CAC authenticates a user who then gets phished, the threat can be transferred to any other service visited by the user. The Sykipot threat from 2006 did exactly this—stealing the CAC PIN, then authenticating to USG resources as an authenticated user.

Anatomy of the Modern Attack Landscape

Until recently, attacks varied in sophistication but shared a high-level attribute in common. Most were custom software development efforts. This began to shift with the availability of powerful scripting tools like Microsoft PowerShell. Actor Tactics, Techniques, and Procedures (TTP) shifted quickly to this vector, that the industry has labeled living off the land. Now only one successful attack is needed for an actor to be able to move quickly throughout an enterprise.

Use Case #1: Standard Operating Environment (SOE) Used Remotely

This use case has two components that need to be addressed. As noted earlier, the load on a VPN concentrator will need to be addressed before an entire workforce can shift to remote access. The Network Architect can use Split tunnels or Symantec Cloud Secure Web Gateway (Cloud SWG). Cloud SWG is the ideal solution to split tunnels because traffic to web services not under corporate control can be secured by Cloud SWG.

SYMANTEC ZTNA CLOUD MEDIATES A SECURE NETWORK CONNECTION BETWEEN EACH REMOTE USER AND APPLICATION, TO PROVIDE LEAST-PRIVILEGED ACCESS TO AUTHORIZED SERVICES AND REDUCE THE ATTACK SURFACE.

Additionally, Symantec ZTNA mediates a secure network connection between each remote user and application, to provide least-privilege access to authorized services and reduce the attack surface.

An SOE is more likely to have a known endpoint security posture and participate in a Domain Environment. This will certainly reduce the attack matrix but there is always an opportunity for an actor to succeed. If an actor gains access to an SOE endpoint on a corporate network, they will explore the environment to determine what information is available and to move laterally across the network. Symantec Threat Defense for Active Directory (stand-alone version) will provide notification of an adversary enumerating active directory information, and Cloud SWG will provide notification of unusual user behavior accessing cloud resources.

Additionally, an SOE client is more likely to be designed to allow remote access to a corporate network. This should include a Network Access Control (NAC) capability within the VPN of choice. An administrator is likely to perform minimum security checks on the connecting device and can quarantine a device if it is out of compliance.

Use Case #2: Bring Your Own Device (BYOD) Environment Used Remotely

We know that some organizations are asking users to connect to corporate assets from home computers, most likely by installing a VPN. This method of access introduces extensive risk to an organization because the back office has little to no control of the security posture of the endpoint. The endpoint may already have an active threat or could become infected when used for family computing activities.

Symantec Cloud SWG is an indispensable line of defense against modern-day cyber threats. It provides secure web services, enables enterprises to control access, protects users from threats, and secures their sensitive data.

Symantec ZTNA can augment VPN capacity by providing secure connectivity for remote workers to corporate applications and systems without exposing internal networks to attackers. Symantec ZTNA is a cloud-based software-defined perimeter that acts as a trust broker between users and resources. It can be used with a Symantec agent or agentless and can even eliminate the need for a VPN, making it ideal for employees and third parties accessing applications from unmanaged devices.

Additionally, Symantec Endpoint Security (SES) provides visibility and peace of mind by delivering prevention and protection technology to all endpoints, whether corporate owned or UYOD. This includes traditional (desktop or laptop) and modern (mobile or tablet) endpoints across every OS (Windows, MacOS, Linux, iOS, or Android). SES is fully cloud managed and perfectly suited for complex UYOD remote environments like those customers need today.

SYMANTEC ENDPOINT SECURITY (SES) PROVIDES VISIBILITY AND PEACE OF MIND BY DELIVERING PREVENTION AND PROTECTION TECHNOLOGY TO ALL ENDPOINTS

Use Case #3: BYOD Environment Connecting to Government Resources

If a BYOD worker is using a CAC or PIV card to authenticate to web applications within government networks, they are raising the risk to the organization. If their system is infected with sykipot-like malware, the actor can ride on the connection and attack the web service the user is visiting or access the user's sensitive information. The CAC and PIV software does not have an ability to perform Network Access Control over this type of connection. The security posture of the entire network would rely on the protections of that one machine. Symantec ZTNA provides the secure connection that government networks require, even when users access resources on their own devices.

Use Case #4: Bring Your Own Device (BYOD) Mobile Device Access

Desktop utilization is not the only stress point on a corporate network in this migration window. Mobile connections to corporate resources are likely to increase regardless of a corporation's BYOD policy. While solutions have been introduced for securing mobile devices, applying these to BYODs continues to be a challenge due to lack of an enforcement mechanism. On personal devices, as opposed to managed endpoints, the employee is the administrator and essentially decides what goes onto their device. This has made it difficult to achieve widespread adoption of Mobile Threat Defense (MTD) apps on employee BYODs. This was an issue even before the remote migration. We expect this problem to be exacerbated by recent trends.

Conclusion

With the change in the way we work and the speed with which it has changed, Broadcom has done research into best practices on how to minimize threats for your organization. If you would like more data on the research and would like to speak with the team, please reach out to your Symantec account representative to discuss further.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

BC-0581EN_032025 March 5, 2025