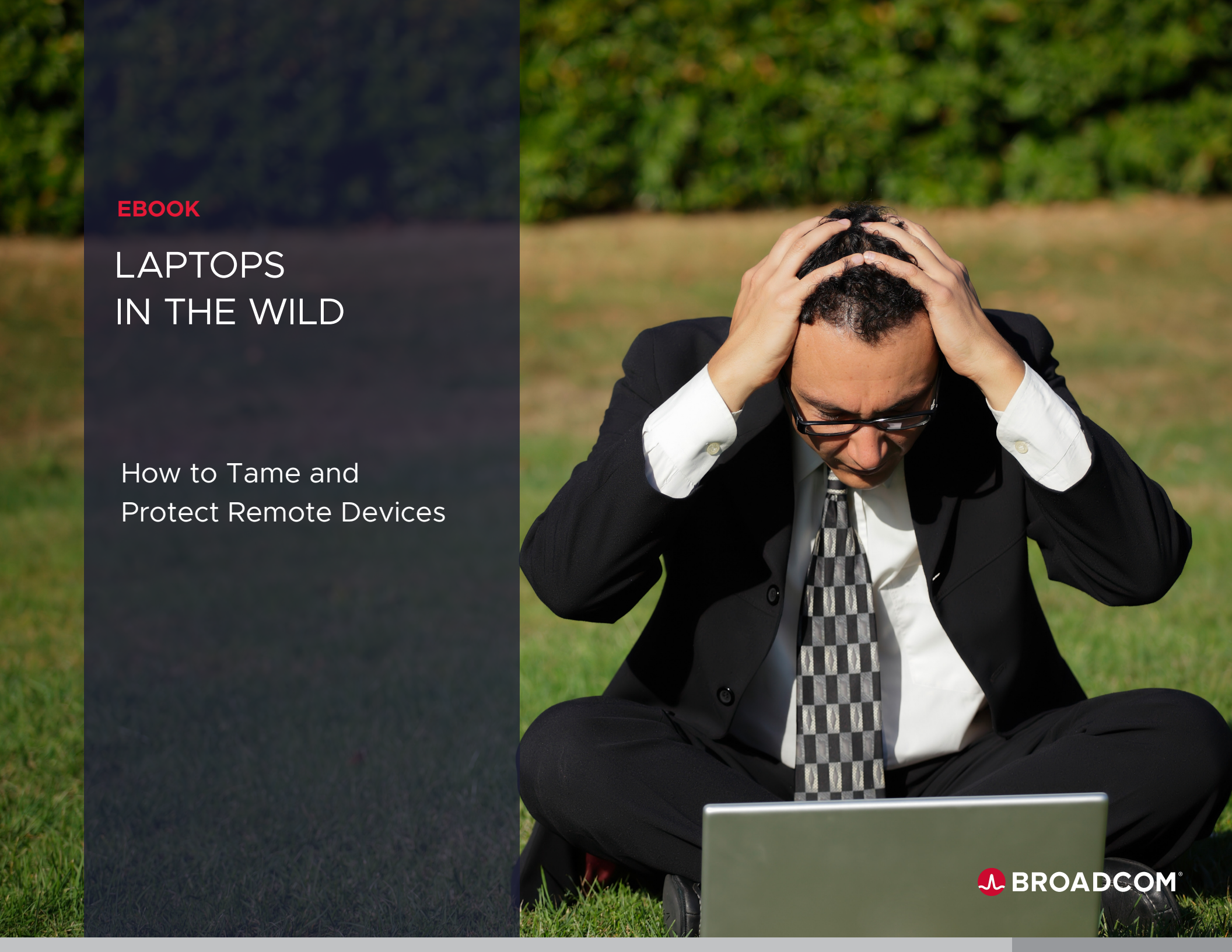
EBOOK

LAPTOPS IN THE WILD

How to Tame and Protect Remote Devices



BROADCOM

Anywhere Workforce: Passing Fad or Here to Stay

During COVID, we witnessed a massive shift in the number of employees working from home, but now many businesses are trying to bring workers back to the office.

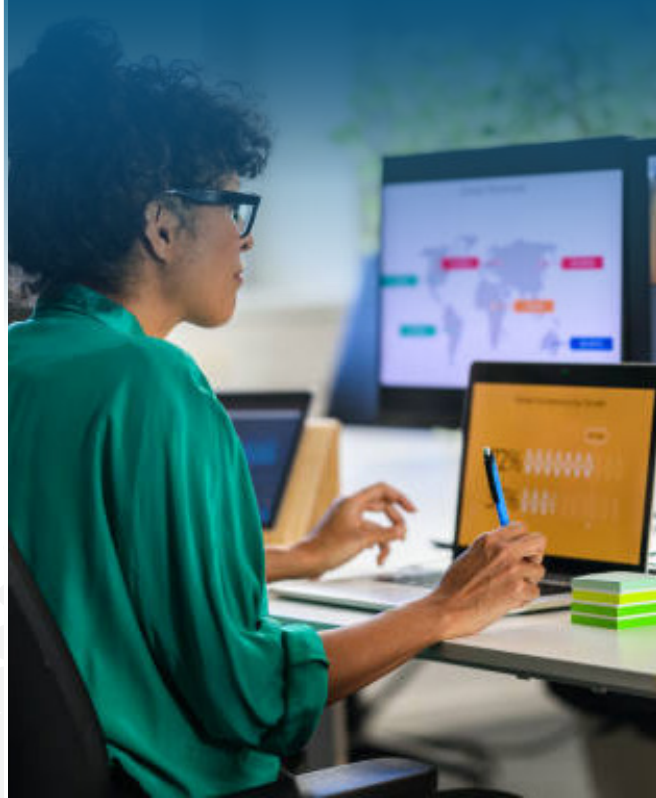
This is being met with fierce opposition. About half of U.S. workers who work in a fully remote or hybrid capacity say that a return-to-office requirement would definitely or probably cause them to search for a new job, according to recent SHRM research.[1] CNBC reported that some employees who choose to stay will rebel against the mandates by only making brief appearances in the office. Or they may stay but be less engaged in their work, which translates to lower productivity and performance.[2]

It is understandable why employees prefer working from home. It provides flexibility in their schedules. Without the need to commute daily, employees save both time and money. This combined makes remote workers feel less stressed and more focused. However, there are also benefits to businesses who continue to support an anywhere workforce, thanks to reduced costs for real estate and utilities. Additionally, providing remote work opportunities can attract top talent from around the globe, secure employee loyalty, and diversify company culture.[3]

1. SHRM, *Remote Work Isn't Going Away—and Workers Don't Want It to*, March 25, 2025
2. CNBC, *5 years into the remote work boom, the return-to-office push is stronger than ever—here's why*, March 23, 2025
3. Business.com, *Why Remote Work Makes Good Business Sense*, January 23. 2025

BROADCOM

About half of U.S. workers who work in a fully remote or hybrid capacity say that a return-to-office requirement would definitely or probably cause them to search for a new job.



Whether your organization is willingly embracing working from home or not, several IT challenges need to be addressed.

Managing the Unmanaged: IT in the Anywhere Era

The top IT Operations and Security challenges facing organizations with remote workers:

- **Endpoint Provisioning & Management.** How do I manage diverse laptops that are not always connected to the corporate network?
- **Email Security.** How do I protect remote workers from increasing the risk of email-based malware, ransomware, and phishing attacks?
- **Endpoint Detection & Response.** How do you detect and prevent attacks on remote endpoints outside your corporate defenses?
- **Secure Access & Identity Management.** How do you identify legitimate users from fraudulent ones without impacting user convenience?
- **Data Leakage & Protection.** How do you protect data stored and created on an endpoint if the device is lost or stolen?
- **Remote Access for Privileged Users.** How do you prevent unauthorized access and use of privileged credentials and accounts from remote endpoints?

This eBook highlights how Broadcom enables and secures the remote workforce.

Challenge 1: Endpoint Provisioning & Management

IT teams struggle to manage a diverse fleet of laptops that are not continuously on the corporate network. Here are the top 5 IT concerns with remote workers:

- **Provisioning Devices:** Shipping and configuring devices without local IT assistance.
- **Inconsistent Configurations:** Risk of misconfigured machines affecting performance or security.
- **Patch Management:** Ensuring remote endpoints remain secure and up to date.
- **Reduced Visibility:** Limited insight into device inventory, health, and compliance.
- **Limited IT Resources:** Smaller teams supporting larger, geographically dispersed user bases.

Symantec® GHOST® Solution Suite assists with deploying laptops, desktops, and servers, providing support for Windows, Windows Server, and various Linux distributions. From a central management console, organizations can provision new devices as part of an onboarding process or PC refresh project, restore end-user or lab computers to their original state, and migrate devices to the latest operating system version.

Symantec IT Management Suite strengthens endpoints by detecting and remediating known vulnerabilities. The solution also reduces costs by automating the deployment, software installation, and inventory collection processes for laptops, desktops, and servers, whether inside or outside the firewall. Finally, the solution maximizes productivity and satisfaction through user self-service.

BROADCOM

84% of companies have high-risk vulnerabilities, of which half could be resolved with a simple software update.[1]

1. Get Astra Blog, January 9, 2025

The 2024 IBM Cost of a Data Breach Report found that "the share of breaches caused by ransomware grew 41 percent in the last year and took 49 days longer than average to identify and contain."

Challenge 2: Email Security & Threat Detection

Remote workers connect from unsecured networks and personal devices, increasing the risk of malware, ransomware, and phishing attacks.

According to a 2025 blog, 92% of malware is delivered through email.[1] Additionally, the 2024 IBM Cost of a Data Breach Report found that "the share of breaches caused by ransomware grew 41 percent in the last year and took 49 days longer than average to identify and contain."

Symantec Email Security.cloud (ESS) offers a comprehensive solution for protecting both cloud-based email platforms (Office 365, Google Workspace) and on-premises systems (Microsoft Exchange). Utilizing a multilayered defense, Symantec ESS blocks advanced threats such as ransomware, spear phishing, and business email compromise (impersonation) attacks while enhancing visibility into attack campaigns with advanced analytics and integration with the Symantec Global Intelligence Network.

This comprehensive email security solution provides end-to-end protection, by integrating advanced detection technologies such as cloud-based sandboxing, click-time URL protection, Office365 clawback, and web browser isolation. Symantec ESS also delivers a robust solution to detect, prioritize, and remediate sophisticated email threats. It also emphasizes user preparation and training, interoperability, and compatibility to streamline the security stack and maximize return on investment.

1. Astra, *160 Cybersecurity Statistics 2025*, January 9th, 2025

Challenge 3: Endpoint Detection & Response

Endpoint Security is still one of the most critical lines of defense in preventing cyber attacks from compromising devices.

Prevention matters as global cyber threats are more aggressive than ever and can have a staggering impact on a business. It is critical to prevent attacks as early as possible, as a modern attack's detection and reaction window is very short. A comprehensive and integrated endpoint security solution protects traditional and mobile endpoints, providing interlocking defenses at the device, application, and network levels.

Symantec Endpoint Security (SES) delivers Adaptive Protection, an innovative approach to helping organizations shift left and focus on enhancing protection across the entire attack chain, emphasizing reducing the attack surface. Beyond the basics—antivirus, spam, and malware protection—the solution also leverages the Symantec Global Intelligence Network and AI to identify and disrupt LOTL attacks and other cyber threats before damage can occur.

Carbon Black App Control is perfect for protecting laptops. It protects laptops from ransomware through email or web downloads and can defend against insiders launching apps that should not be running. It can enforce policy whether on or off local area networks. With Carbon Black App Control, organizations decide which applications can run on an endpoint regardless of regional or domain admin rights, ensuring that only trusted software can run. It can also minimize the risk that trusted software might run maliciously by stopping malicious commands from running.

BROADCOM

Endpoint Security is still one of the most critical lines of defense in preventing cyber attacks from compromising devices.

Identity is the universal glue that ties everything together and must exist everywhere.

Challenge 4: Secure Access & Identity Management

As organizations migrate to the cloud, most applications and data run in someone else's infrastructure.

At the same time, employees work from home and access these resources across the Internet. Under this scenario, an enterprise's only tangible assets are the user identities, the access they are given, and the information they interact with. Identity is the universal glue that ties everything together and must exist everywhere.

Ensuring the right people access the right systems becomes complex. A crucial step in enforcing zero trust access for remote workers begins with distinguishing legitimate users from fraudulent ones, but implementing multifactor authentication can hinder productivity.

Symantec VIP is a leading cloud-based, strong authentication service that protects networks and applications by verifying the identities of users and devices to prevent unauthorized access. VIP's core capabilities strengthen security and enhance the user experience across four key areas: multifactor authentication; a contextual risk engine; user adoption and onboarding; and interoperability with popular VPNs, cloud and web applications and user directories that follow popular standards.

Challenge 5: Data Leakage & Protection

Laptops and removable media devices capable of storing gigabytes of data have provided the freedom to work from anywhere.

With this freedom comes an increased risk that lost or stolen devices will result in a costly data breach, particularly as cloud "sync and share" services allow employees to carry a large amount of sensitive information unknowingly. Additionally, shared file servers have emerged as central collaborative tools in the modern workplace, enabling users to access shared information anywhere. This shared data presents an easy target without proper controls.

The Symantec PGP® Encryption Suite offers comprehensive capabilities to encrypt data at rest and data in motion for endpoints, including:

- Endpoint Encryption, which provides robust full disk and removable media encryption
- Desktop Email Encryption, which encrypts internal employee communications
- File Share Encryption, which automatically encrypts data when it is created byselected applications or sent to specific folders.

Symantec PGP Gateway Email Encryption automates email encryption using customizable rules, eliminating the need for client-side software installation, while ensuring sensitive data is securely transmitted before it leaves the organization. This helps prevent accidental and intentional data leaks via email, while addressing compliance with government and industry regulations such as CDM, PCI DSS, HIPAA, and GDPR.

BROADCOM

The Symantec PGP® Encryption Suite offers comprehensive capabilities to encrypt data at rest and data in motion for endpoints.

Symantec PAM is designed to protect administrative credentials and other secrets while controlling privileged access across cloud, physical, and virtual environments.

Challenge 6: Remote Access for Privileged Users

Many data breaches and insider attacks exploit privileged accounts or credentials. This is not surprising, considering that privileged identities have elevated access to the most sensitive resources and data in your environment.

This risk is magnified in a work-from-home environment because managing privileged access securely is harder with distributed teams.

Symantec PAM is designed to protect administrative credentials and other secrets while controlling privileged access across cloud, physical, and virtual environments. The solution delivers five core services: privileged credential vault, session management and recording, behavioral analytics, fine-grained access controls, and secrets management from a single platform.

Symantec PAM provides several key capabilities to support remote access for privileged users working from home:

- Implementing two-factor authentication before granting access to a privileged credential ensures that users are who they claim to be.
- Enforcing policy-based controls over which credentials a privileged individual can use to ensure least privileged access.
- Providing visibility to audit all privileged activities and link these activities back to an individual user to improve accountability and record those activities as forensic evidence.

Introducing Anywhere Workforce Security by Symantec

Enable and protect the remote workforce with comprehensive security from Broadcom.

ARE YOU DOING ENOUGH TO ENABLE AND PROTECT YOUR REMOTE WORKFORCE?

Broadcom can help you answer that question with a confident yes.

Why Partner with Broadcom?

Broadcom offers three differentiators over the competition when considering a vendor to help protect your data.

MOST SECURITY

Broadcom cybersecurity solutions safeguard data at every stage of their lifecycle.

MOST COVERAGE

Broadcom cybersecurity bridges the hybrid environments to safeguard data everywhere.

MOST TRUSTED

Broadcom cybersecurity has protected the world's largest customers for over 50 years.

BROADCOM®
connecting everything®

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

Laptops in the Wild May 29, 2025