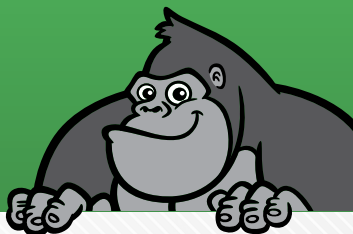


**THE  
GORILLA  
GUIDE TO...**®

**EXPRESS EDITION**



# Secure IT for Small and Midsize Businesses

Ed Tittel

## Inside the Guide

---

- SMB Security Can Be Difficult (and Costly)
- New Security Challenges for SMBs
- Business Continuity Is Increasingly Critical

**THE GORILLA GUIDE TO...**

# **Secure IT for Small and Midsize Businesses**

**Express Edition**

By Ed Tittel

Copyright © 2021 by ActualTech Media

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

**ACTUALTECH MEDIA**

6650 Rivers Ave Ste 105 #22489  
North Charleston, SC 29406-4829  
[www.actualtechmedia.com](http://www.actualtechmedia.com)

# **PUBLISHER'S ACKNOWLEDGEMENTS**

## **EDITOR**

Keith Ward, ActualTech Media

## **PROJECT MANAGER**

Wendy Hernandez, ActualTech Media

## **EXECUTIVE EDITOR**

James Green, ActualTech Media

## **LAYOUT AND DESIGN**

Olivia Thomson, ActualTech Media

## **WITH SPECIAL CONTRIBUTIONS FROM HPE**

Robert Checketts, Group Manager, WW SMB Segment/  
Product Marketing

Tim Daron, Solutions Architect – SMB Segment

Andrew Dodd, WW Marketing & Marcom Manager HPE  
Storage Media

Antoinette Gerusa, Digital Merchandising Marketing  
Manager

Cole Humphreys, Director Global Product Management –  
Cyber Security

Aditi Pandey, Manager Aruba Instant On marketing

Martin Oderinde, SMB Solutions Marketing

# TABLE OF CONTENTS

<b>Introduction: Secure IT Is <u>Not</u> Optional.....</b>	<b>8</b>
<b>Chapter 1: SMB Security Can Be Difficult (and Costly).....</b>	<b>10</b>
No Shortage of Security Trouble for SMBs.....	12
The Ever-Spreading SMB Boundary.....	13
HPE Security Solutions.....	14
Baked-in Security at the Edge.....	16
<b>Chapter 2: New Security Challenges for SMBs.....</b>	<b>18</b>
Secure Networks Deliver Secure Operations.....	20
Enable Secure WFH Productivity.....	25
Secure, Reliable File Backup—and Restore.....	27
<b>Chapter 3: Business Continuity Is Increasingly Critical.....</b>	<b>31</b>
The Many Faces of Business Continuity .....	32
Paths and Mechanisms for Business Recovery....	34
Putting Business Continuity to Work.....	37

<b>Chapter 4: HPE Provides Built-in Security for SMBs.....</b>	<b>42</b>
What Security Means in 2021.....	43
Silicon Root of Trust .....	46
Trusted Platform Module (TPM).....	48
HPE's Trusted Supply Chain.....	50
HPE Covers the Full Range of SMB Security Needs.....	51

# CALLOUTS USED IN THIS BOOK



In the School House callout, you'll gain insight into topics that may be outside the main subject but are still important.



This is a special place where you can learn a bit more about ancillary topics presented in the book.



When we have a great thought, we express them through a series of grunts in the Bright Idea section.



Takes you into the deep, dark depths of a particular topic.



Discusses items of strategic interest to business leaders.

# ICONS USED IN THIS BOOK



## DEFINITION

Defines a word, phrase, or concept.



## KNOWLEDGE CHECK

Tests your knowledge of what you've read.



## PAY ATTENTION

We want to make sure you see this!



## GPS

We'll help you navigate your knowledge to the right place.



## WATCH OUT!

Make sure you read this so you don't make a critical error!



## TIP

A helpful piece of advice based on what you've read.

# INTRODUCTION

## Secure IT Is Not Optional

Welcome to The Gorilla Guide To...® Secure IT for Small and Midsize Businesses, Express Edition. In this Guide you'll find a roadmap to help you assess, establish, and maintain IT security in your business operations.

In today's rough-and-tumble business landscape, IT security isn't just "nice to have"—it's absolutely and positively essential. Just look at recent headlines. For example, in early May 2021, Colonial Pipeline had to turn off deliveries of gasoline, diesel, and jet fuel through its pipelines from Texas to the northeast United States in the wake of a ransomware attack. Good security could have prevented this attack, which put Colonial out of business for more than a week and did undeniable reputational damage.

This Guide begins with a general overview of small to midsize business (SMB) security needs and requirements. It continues with an assessment of key SMB security challenges, with suggestions on how they might be addressed. It also digs into the topics of business



continuity, to explore how and why keeping business going in the face of interruption or outage is key. The book concludes with a discussion of HPE's built-in and trusted security technologies, ready for you to put them to work in your business.

Let's get started!

# CHAPTER 1

## **SMB Security Can Be Difficult (and Costly)**

It's a scary digital world out there. All businesses and organizations face the same formidable and forbidding security threat landscape, including SMBs. As any recent security survey can tell you, organizations at all scales face ever-increasing numbers, kinds, and degrees of threat, and an ever-widening attack surface for bad actors to infiltrate. In this Guide, we won't sugar-coat the situation or gloss over the solutions and their costs. Because security is so important, it's vital for SMBs to understand what they must know and do, what it will cost them, and what risks they can expect to face.

According to Forrester's 2020 State of Security Operations, 79% of businesses have experienced a security breach of some kind in the past 12 months, and data breaches remain a constant concern for all businesses. In addition, security teams and their employers face significant technology challenges, many emerging from complex or siloed tools that create inefficiencies

and produce subpar security outcomes. The same study found that the current top five security threats by type include:

1. **Ransomware:** rogue software that encrypts business data and systems that can't be recovered without paying for decryption—with no guarantee of success
2. **Phishing:** email-, web page-, or social media-supplied links that take unwary users to malicious sites where passwords and credentials get stolen (and more)
3. **Data leakage:** illicit means whereby business data gets past organizational safeguards and into the wrong hands
4. **Hacking:** technical and social engineering attacks on IT infrastructures that aim to gain control; deny access or service; and steal data, intellectual property, or money
5. **Insider threats:** attacks from former or current employees, often disgruntled, who use insider skills and knowledge to go after business data, IP, or financial assets

Most organizations (83%, says Forrester) have 24/7 security coverage of some kind, but too often lack the right kinds of technology and staff to keep pace with

the ever-growing number and severity of cyberattacks. Many businesses, in fact, struggle mightily just to keep up with the volume of security alerts they must handle every day.

## **No Shortage of Security Trouble for SMBs**

SMBs are particularly vulnerable to security woes, given low IT staffing levels where security expertise is either scarce or severely overstretched. In an environment where IT staff struggles to keep up, most SMBs find themselves forced to react to security alerts, rather than to proactively and pre-emptively manage threats and address potential vulnerabilities.

It's the sad truth that even a slow response to a security attack or data breach can spell disaster for SMBs. Opportunity costs for lost business, combined with repair, recovery, and reporting (and potential follow-up audit) costs, and more, weigh heavily on the bottom line. To make a long and painful story short, good security may be expensive and resource-intensive, but the cost of going without or using substandard security can be much, much greater. It can even threaten business viability and survival. That's what makes security both crucial and essential.



## WHAT COULD POSSIBLY GO WRONG, SECURITY-WISE?

In fact, SMBs are at high risk for catastrophic damage or loss. According to the [Ponemon Institute](#), the average cost of a data breach in 2020 was \$3.86M. For a smaller operation, a loss of this magnitude spells the difference between survival and failure.

Moreover, some kinds of attacks, like ransomware, can literally sideline an SMB and render it unable to conduct business at all. Calling such an attack a catastrophe is no exaggeration whatsoever. SMBs need security protection to avoid potential legal and regulatory risks as well, which data breaches involving customer data can also entail, along with substantial financial penalties and damage to the business's reputation.

## The Ever-Spreading SMB Boundary

Once upon a time, SMBs could focus on their organizational boundaries. Securing such boundaries took care of most of their security concerns and addressed most risks. Today, data and apps are everywhere, making everything harder to track and secure. Under pandemic

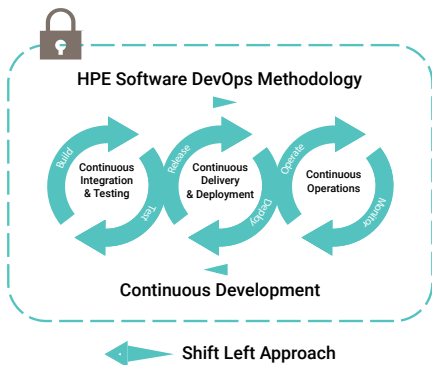
rules, workers are mostly remote, which means that each and every use of each and every device needs protection. With the Internet a vital link in tying users to applications and services, secure communications are more important than ever before. Ditto for secure storage and servers, both on-premises and in one or more clouds (mostly more, nowadays). In short, security and protection get interesting in a hurry when an organization's assets, apps, and people operate from anywhere, anytime, all the time.

## HPE Security Solutions

HPE stands ready to help SMBs make the all-important switch from reactive, static, and siloed security tools and techniques to intelligent, adaptive security platforms that span the digital world. HPE's security solutions allow SMBs to close existing security gaps with coverage at the edge, in the cloud, and on-premises, all under a consistent and coherent security umbrella. To that end, HPE offers the following capabilities:

- **Data-centric security:** Uses proven, NIST-standardized methods to protect data in use, at rest, and in motion (which meet U.S. Government and European Union GDPR requirements). It provides strong encryption and tokenization to render stolen data useless to attackers.

- **Zero-trust security:** Is a philosophical approach to identity and access management, whereby no user or software action is trusted by default. Thus, all users, devices and application instances must prove their identities and authorizations conclusively before access is allowed.
- **DevSecOps:** Embeds security teams and concepts in a formal development process, designed to ensure security is addressed early and often along the entire app delivery chain (design-build-test-deliver-maintain), not simply bolted onto a “finished” system or service at the end of development. Security is addressed during development and deployment through a set of DevSecOps best practices (**Figure 1**).



**Figure 1:** DevSecOps expands on the underlying concepts of DevOps to build the mindset that everyone is responsible for Security

HPE even addresses security in its own product development and delivery, using a formally documented, frequently audited secure supply chain (see Chapter 4).

HPE also offers its [Pointnext](#) consulting services, which can help SMBs audit, define, and refine their security strategy. Expert assistance is on hand to make sure that security policy addresses security needs across the organization, along with compliance requirements for privacy, confidentiality, and data protection. Those same experts can also help SMBs integrate affordable and effective options for business continuity and disaster recovery as part and parcel of whatever intelligent and adaptive security platform they may implement. They can provide your SMB with security blueprints upon which to base your own designs and implementations, and help you see them through test, pilot, and production deployments.

## **Baked-in Security at the Edge**

All in all, HPE works with SMBs to embed security across the entire organization. This means your remote workers will be safe and secure, and that security is embedded and included at the edge, on-premises, and in hybrid cloud environments. This approach builds security into the entire IT infrastructure in all of its implementations and manifestations. Thus,



HPE Edge includes baked-in security to ensure that edge computing capabilities—including intelligent workspaces, IoT environments, virtual desktop infrastructures, and service delivery for Microsoft (Teams, Exchange, Microsoft 365), VMware, Linux VMs and more—start out and remain secure as they're deployed and evolve over time. The same is true for HPE data center and cloud/hybrid cloud solutions, including HPE GreenLake, HPE InfoSight, and much, much more. Visit HPE's [Security and Digital Protection Services](#) page to check out security blueprints, the HPE security [portfolio](#), [case studies](#), and more.

Here in Chapter 1, you've learned about the scope, scale, and potential exposures that security risks can pose, along with a variety of approaches and solutions you can use to address them. In the next chapter, we dig into specific security challenges that SMBs must confront and solve, including network security, secure operations, secure remote access, and matters related to data protection, backup, and recovery.

## CHAPTER 2

# New Security Challenges for SMBs

Beyond the well-studied and widely proclaimed costs of security breaches, ransomware, and other high-visibility exploits, SMBs all face specific challenges when it comes to securing IT, and protecting their information assets from attack, loss, or harm. In this part of the Guide, you'll explore some of the most important challenges that SMBs must face and address, along with suggested tools and technologies to help you handle them properly and expeditiously.

Work from home (WFH) and remote working scenarios are forcing profound changes to the SMB security equation. Businesses must protect users and devices, wherever they may be. At the same time, they must also secure networking, communications, and data integrity—without impeding remote workers' productivity and creativity. This means SMBs must look for comprehensive, holistic security solutions that address backup, acceptable use, and data security while providing safe, usable storage for applications and customer data.



### **Recent studies and surveys provide**

**strong** evidence that employees like working from home—even IT employees—and plan to keep at it even after the pandemic subsides.

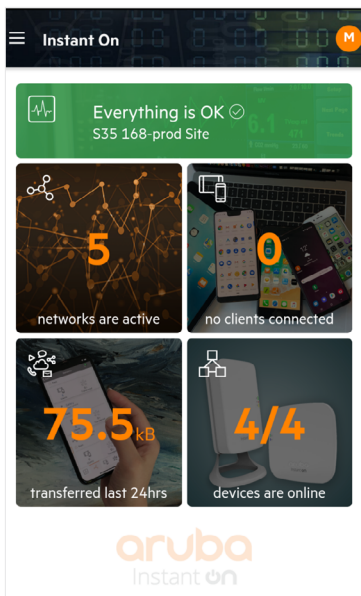
Thus, for example, Microsoft speaks to a [“philosophy and practice of our hybrid workplace.”](#) It recognizes that even as safety concerns abate, and more people return to work, that 54% of workers who opt to return to a “normal” office routine spend only 25% of their time at a company work site. Instead, Microsoft (and many other companies) now speak of “hybrid work” that involves some time in the office (often two days a week or less) and some time working elsewhere (usually from home). This appears very strongly to be the way the world will work from now on, for jobs that don’t require face-to-face contact or access to site-specific facilities and equipment.

Thus, SMBs have lots of interesting security challenges to confront and surmount, as they continue to improve profitability and user experiences.

## Secure Networks Deliver Secure Operations

Ultimately, making remote work connections safe means securing not just end-user devices, but also securing the networks that make remote access possible. HPE subsidiary Aruba's Instant On offers fast, secure, affordable Wi-Fi access points and switches designed for small businesses. Instant On provides easy setup and management and supports blazingly fast Wi-Fi and corner-to-corner coverage designed to keep users connected and comfortable while networked.

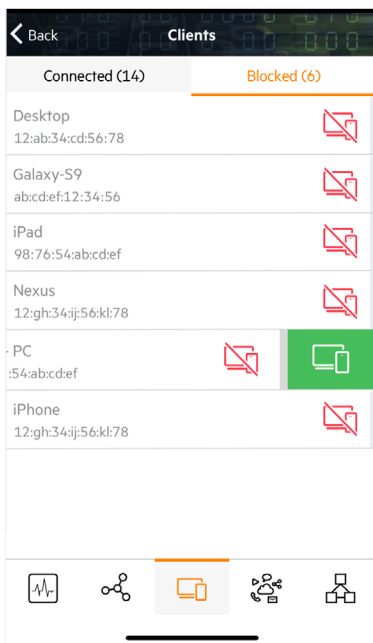
Better yet, Aruba Instant On security is easy to manage. Security is baked into this product family, at no extra charge. Businesses can set up separate networks for business traffic and guest or visitor use. Network access is safe and secure, with a variety of controls over access and usage. They can apply bandwidth limits on a per-client or per-network (LAN) basis. They can also limit duration of use, enforce not safe for work or acceptable use policies, and completely block specific websites or application categories from the network.



**Figure 2:** Aruba Instant On allows small businesses to create, modify, and monitor network components from a central location

The Aruba Instant On mobile app provides a complete toolbox for management and security on Wi-Fi and local networks under its umbrella (see **Figure 2**). The app offers excellent visibility into access and usage, and can block unsolicited applications or access to disallowed websites quickly and easily (see **Figure 3**). Access

controls also include MAC address filtering capabilities that can blacklist specific devices, or simply block all devices not whitelisted for network access and use. In addition, the app offers predefined access control lists (ACLs) to ward off malicious network traffic.



**Figure 3:** Get visibility into all connected devices and the ability to block specific, unwanted clients from accessing the network

Two-factor authentication (2FA) is now available on Aruba Instant On mobile app and web portal, providing HPE business partners and customers with an additional layer of authentication, helping to prevent attackers from remotely accessing your network and securing sensitive customer information. Using 2FA strengthens security by requiring an additional layer of authentication, such as an authentication app, in addition to a username and password.

Furthermore, Aruba Instant On can keep your network up-to-date through automatic installation of software updates, ACLs, and blacklists of known bad sites and actors. In fact, Aruba Instant On supports a variety of other key network security and control capabilities, including:

- Strong authentication with advanced version 3 W-Fi Protected Access (WPA3) support means that authorized users are carefully vetted before they're allowed on the network, and its login controls are more secure and harder to crack.
- Instant On supports the Wi-Fi Alliance's latest security standard for public networks. Wi-Fi Enhanced Open (OWE) provides strong data encryption for open, non-password-protected Wi-Fi networks.

- Enhanced VPN solutions via a trusted online VPN provider (NordVPN) provide communications encryption to secure remote and WFH workers as they connect over the Internet to access your network and its services and resources.
- Immediate notification of critical alerts reports through the app about possible connection issues, device failures, and more. The Instant On mobile app even lets admins tackle repairs and recovery through its friendly, powerful interface. Topology view provides an intuitive map of all Instant On devices deployed in a network, which enables IT admins to identify and troubleshoot network issues more efficiently.
- Every network device has a unique physical Media Access Control (MAC), which can be used to authenticate the device for network access. In addition to 802.1X authentication, Instant On supports Radius MAC-based authentication, providing flexible options for security configuration.

In short, Aruba Instant On offers small businesses the ability to implement and operate wireless and wired local networks on their premises, quickly and easily. It also helps to secure remote access to the networks and resources under its control. The next step is to learn how best to secure the other end of remote connections, to support WFH and mobile work scenarios.



## Enable Secure WFH Productivity

SMBs have ways to make their WFH staffers more productive and secure. These include options for remote desktop services (RDS) and virtual desktop infrastructures (VDI). RDS lets a user device operate a physical computer on the network via the Internet, while VDI lets a user device operate a virtual computer on that network. RDS makes sense when users have their own “work computers” on the company network, and simply make a remote connection to operate that computer from home or while on the road. VDI is much more flexible and powerful and lets users put one or more virtual computers to work whenever they need them. They can turn them on and run them on demand, then turn them off when they’re done, without tying up a physical PC or equivalent virtual resources.

VDI and RDS both let remote users run programs, access data and resources, and get things done using mobile devices (or their own PCs) as they see fit. But VDI lets users scale up and scale down the remote resources, capabilities, and applications at their disposal. RDS, on the other hand, can only offer access to physical computers on the SMB network that the user is allowed to access. Thus, VDI also supports business continuity to keep employees productive through any

disruption (through access to cloud-based resources when on-premises resources are offline or out of reach) whereas RDS does not.

HPE Small Business Solutions for Remote Workers are built around two different VDI implementations. SMBs can choose between Teradici VDI or VMware Horizon VDI offerings, which work with HPE ProLiant Gen10 servers to offer powerful, flexible remote access to virtual desktops preconfigured with the applications and data users need. Sizing and maintaining a VDI environment may be challenging because application demands can vary, while inconsistent performance disappoints users. Plus, there is a risk of costs escalating as VDI deployments grow. VDI requires the storage to handle bursty IOPS (from boot storms, patching, and antivirus scans), read IOPS, and write IOPS. A dedicated shared storage array, like the HPE MSA 2060 Gen 6, can solve these issues by providing fast read and write performance from Flash, while still being easy to set up and manage. Small businesses can further grow their infrastructures beyond the MSA Gen 6 to include hybrid cloud options, as well, including robust solutions built around HPE Cloud Volumes, Microsoft Azure, or another managed service provider's VDI offerings, as they see fit.

Ultimately, HPE is prepared to help SMBs define, deliver, and maintain a safe, secure VDI to support WFH and mobile work scenarios.

## **Secure, Reliable File Backup—and Restore**

Behind the scenes, file backup—and file backup security—play heavily into establishing ultimate security and ensuring SMB peace of mind. Customer data has become a vital asset for creating unique and valuable experiences, but that means losing customer data is a huge risk and a potential liability. Then, too, a secure unimpeachable offline backup is the only sure remedy against ransomware.

Employees must have secure, controlled means for backing up files and application data, so the SMB can fend off or avoid common attacks. HPE file and backup data security solutions enable SMBs to monitor and protect against known and unknown threats so they can concentrate on growth and customer satisfaction.

In fact, backups also provide important protections in the face of loss, failure, and downtime. Consider these exposures: PC can crash, laptops can go missing, and Internet connections can (and do) go down. An upgrade to server-based computing, certainly for file backups, but also for image backups, replication, and more,

provides added protection, as well as failover and recovery capabilities. HPE file and data backup solutions provide SMBs with coverage, which, in turn, helps them save time and money when losses or service interruptions occur.

## **HPE File and Backup Solutions**

HPE offers a variety of ProLiant server bundles that span a range of costs and capabilities, all of which offer a central location for files. In addition, HPE offers automated data backup storage such as HPE StoreEver tape and HPE RDX removable disk to protect key files and data with air-gapped, offline security to protect key files and data. For those who choose additional coverage, image backups can protect client and server operating environments, too. And for customers who want a dedicated appliance for file sharing and storage, or who need more capacity than is available on a standalone server, the HPE StoreEasy network attached storage (NAS) portfolio provides a cost-effective file and backup solution.

HPE bakes virus protection into its backup solutions, to prevent unauthorized access to backup storage (which means that ransomware can't encrypt or exfiltrate backups). HPE Secure Encryption takes a "zero trust" approach to access, so that only authorized users can

see (or change) files under any circumstances. Securing files and backups is essential to protecting the business, and to making sure that even disaster or security incidents won't render files and data inaccessible or damaged. For the most robust safeguards, HPE StoreEver and HPE RDX provide offline data protection, which means data is stored behind an air gap and disconnected from the network. This creates an impregnable barrier against the growing threat of cyberattack that arises as more staff work remotely in less secure IT environments.

Furthermore, HPE file and backup solutions, like HPE StoreEasy, can make files, email, and collaboration tools accessible from any device, when called upon to do so. Thus, employees can share and collaborate more easily and switch among devices as needed. A NAS appliance provides users and applications network-based access to file shares while automatically regulating visibility of sensitive data using Active Directory access controls. And you can also run anti-malware and backup agents from a HPE StoreEasy device. This helps to improve productivity and profitability, while providing protection against damage or loss. HPE is ready to supply the files and data SMBs need to keep working, as well as the systems and services that consume them.

In addition to the HPE ProLiant hardware, HPE also has HPE Cloud Volumes, a suite of cloud data services that unlocks the true potential of a hybrid cloud. This data service allows SMBs to easily back up data to the cloud and back without the exorbitant egress fees, multi-cloud flexibility delivering encrypted backups invisible to ransomware, all while providing pay-as-you-go pricing. HPE Cloud Volumes is an effortless, secure, and efficient solution to cloud backup.

To learn more about HPE's offerings, please check out Aruba's [Instant On wired and wireless portfolio](#), learn more about [HPE WFH productivity options](#), [HPE Cloud Volumes](#), or visit HPE's [File Backup Storage Solutions for Business page](#).

Here in Chapter 2, you've learned more about network security and secure operations, and the tools and technologies that make remote work possible, practical, and safe. You've also learned how essential it is to protect and back up business files and data, with an emphasis on easy restoration and recovery should losses or interruptions occur. In Chapter 3, you'll learn more about the importance of business continuity and the tools necessary to keep your business running without interruption.

## CHAPTER 3

# **Business Continuity Is Increasingly Critical**

Without access to applications and data, the ability for a SMB to operate lands somewhere between difficult and impossible. No business means no customer products or services—it also means no supplier orders or payments. This very quickly translates to zero income. No income, even for only a short period, can spell the difference between a viable, going concern and going out of business. In a nutshell, this nightmare scenario explains why business continuity and disaster recovery are, and remain vitally important to, maintaining an active, healthy, and profitable business. In this chapter, the goal is to help you understand how the right tools and technologies can help your SMB minimize the impact of outages and interruptions, so you can keep doing business in business-like fashion.

# The Many Faces of Business Continuity

Business continuity is a well-understood part of IT. The same is true for the related topic of disaster recovery. Together, business continuity and disaster recovery cover a number of tools, technologies, platforms, and practices. Business continuity is usually part of a bigger set of tools and responses that deals with potential business interruptions and outages, including:

- **Backup and recovery:** Typically uses special software or imaging techniques to permit file-by-file copies and/or snapshotting that can run even while applications or services are busy. This process captures volume shadow or other complete copies of systems, files, logs, and data. Please note that while backup images are usually restored as part of enacting a business continuity or disaster recovery scenario, by itself, backup/recovery is not the same thing as either business continuity or disaster recovery.
- **Archiving:** Archiving differs from backup and recovery because whereas an organization might have many backup copies, typically archives are “one of a kind,” single copies of data preserved for future analysis, compliance, or disaster recovery.



- **Disaster recovery:** Requires specialized steps to bring up an organization's IT infrastructure in a different location. This might occur in the event of a failure, outage, or some natural or man-made disaster that puts the primary IT infrastructure out of action. That location may be located on-premises at a different location, in the public cloud, or at a third-party failover/recovery site.
- **Data security:** Involves a variety of mechanisms and technologies to prevent unwanted access to or disclosure of an organization's data, including breach and exfiltration of private, sensitive, or proprietary data. Data security involves a variety of tools and technologies, from encryption and access controls to monitoring and audit logs.
- **Compliance and governance:** Uses various technical and procedural means to establish, enact, and monitor policy regarding access to systems and data—especially private or confidential data related to personal identification, privacy laws and regulations, financial accounts and monies, and so forth. Organizations that fail to comply with applicable laws and regulations, or fail to meet requirements for governance, are subject to fines and penalties. The responsible officers or officials may also be personally subject to civil and criminal penalties, including

jail time. Proving compliance generally involves producing audit records to demonstrate that data access and use fall within a compliance regime's guidelines.

## **Paths and Mechanisms for Business Recovery**

When business continuity or disaster recovery is needed, such action generally involves initiation of a formal, planned (and practiced) set of activities to re-establish IT operations. In a smaller organization, that might involve having two or three designated individuals who can take charge of coordinating the business's response—almost like fire marshals. In a larger, mid-size company with more resources, following an event that begins with a “disaster declaration,” the first step usually involves calling in a designated disaster recovery team. Once those responsible are at work, they can enact the steps necessary to recover by following the organization's disaster recovery plan.

Business continuity is similar because it is also plan-driven and is invoked when some kind of disruption may endanger (but not actually knock out) an organization's IT infrastructure. Instead of describing how to bring up and run an alternate IT infrastructure, a business continuity plan more generally describes how to keep the business running when possible disruptions appear.



**Recovery Time Objectives (RTO):** Refers to the length of time a system, service, or application may be unavailable or down without causing significant loss or harm to a business or an organization. RTO is not just a time interval; it accounts for the steps that IT staff must take to restore an application and its data. If an organization invests in failover capabilities for high-priority/high-value applications or services, RTO may be a matter of seconds. A four-hour RTO, on the other hand, allows enough time for on-premises recovery—starting with a bare-metal restore and ending with normal application and data access.

**Recovery Point Objectives (RPO):** Where RTO measures maximum sustainable downtime, RPO measures maximum sustainable data loss. Thus, RPO is often expressed as a time measurement, from the time of outage or loss to its most recent preceding backup or snapshot. If an organization backs up all its data daily, a worst-case scenario means that it would lose 24 hours' worth of data. For some applications and services, this is OK; for others, it is emphatically unacceptable. Typical intervals for an RPO in many organizations are between four and eight hours. But for applications with valuable or irreplaceable data, intervals should be shorter.

Two key metrics drive business continuity and disaster recovery. They're known as recovery time objectives (RTOs) and recovery point objectives (RPOs). RTO may be understood as determining how quickly an organization plans to return to operational capability. RPO covers the kinds of capabilities and data are available when that operational capability returns. Recovery objectives apply to the organization and its partners, customers, and other affiliates.

Businesses must understand that setting RTOs and RPOs occurs on a per-application or per-service basis. This requires working with business stakeholders invested in those applications and services to help choose optimal tradeoffs. Such tradeoffs often occur between the higher costs involved in shorter intervals and the greater data losses and opportunity costs that come from longer ones. HPE Pointnext Services can work with SMBs to help them make these important determinations. They can help find the best sweet spots between financial costs on the one side and data losses or opportunity costs on the other.

Eight-hour or longer RPOs will usually work within the typical time frames for restoring backups using an off-the-shelf backup solution. RPOs of four hours or less need scheduled snapshot replication. And near-zero RPOs require special handling—namely, continuous

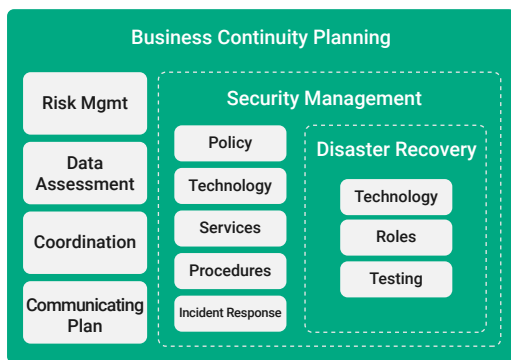
replication. Combining near-zero RTOs and near-zero RPOs means continuous replication with failover services for maximum application and data availability.

When a disaster is declared, or business continuity must be ensured, the relevant business continuity or disaster recovery plan is called into action. Special teams get convoked to undertake the work involved in meeting RTOs and RPOs and bringing up a replacement IT infrastructure sufficient to meet those objectives. The various costs (time, money, opportunity, and so forth) and complexity of these recovery options depend on the value of the data and applications they ensure. They also encompass a variety of storage technologies; each with its own RTO/RPO capabilities.

## **Putting Business Continuity to Work**

The shorter the intervals for RPO and RTO, the more an organization should expect to spend to support its disaster recovery and business continuity plans. So, for example, HPE Nimble volumes are expensive and relatively limited in capacity. Cloud storage offers minimal CapEx with OpEx costs that depend typically on storage consumption and retrieval. The more that cloud-based storage gets consumed, or the more data that is recovered on a regular basis, the higher its costs rise. Here,

again, organizations must watch the tradeoffs between cost, capacity, and capability, to avoid squandering or exceeding CapEx savings on OpEx costs when business continuity or disaster recovery scenarios come into play. Tape storage offers the lowest long-term cost of any storage technology but is potentially the slowest depending on whether tapes are on-premises or off-premises when they're needed. But the offline nature of tapes stored in a vault make them the most secure form of storage to guard against the rising business continuity threat of ransomware.



**Figure 4:** Disaster recovery is a subset of security management, and falls under the general heading of business continuity planning, along with risk management, data assessment, coordination, and creation/communication of the business continuity plan itself

**Figure 4** shows how business continuity planning fits into the overall IT planning context, with special emphasis on security management and disaster recovery. Note that disaster recovery is just a part of security management, which is itself part of the overall business continuity planning process.

Fortunately, SMB customers can choose among (and even combine) these options, including:

- **HPE Nimble Storage:** Flash-based, limited capacity that's extremely fast and the most expensive form of storage for data and applications
- **HPE Modular Smart Arrays (MSA):** Great SMB entry-level alternative, offers a good combination of cost, capacity, and performance
- **Deduplicated storage:** Uses HPE StoreOnce technology and may also be attractive for some SMBs, but is cost- and capacity-constrained when shorter RPO intervals are in the mix
- **Cloud storage:** Can seem compelling from a cost perspective, but comes with variable usage charges and only offers slow recovery times—may not be suitable for shorter RTO and RPO intervals
- **HPE StoreEver tape systems:** Will be attractive for their long-term, low-cost advantage and highly

secure, “airgap” defenses against cyberattack and ransomware. However, tape systems will generally provide slower RTO because of the relatively long time it can take to recover data and applications from tape.

- **Hyperconverged infrastructure (HCI and dHCI) solutions:** Under certain circumstances these offer fast recovery intervals (both RPO and RTO). But they can only protect assets stored within an HCI environment (and nothing from outside it), so they may not fit specific needs or circumstances.

Considering these options, it's easy to understand that most SMBs will require some combination of these solutions. Such combinations help match specific RTO/RPO requirements for specific applications and their data, with custom configured systems and solutions that meet those requirements. So, whatever an SMB's business continuity and disaster recovery needs might be, HPE has all the bases covered. To learn more please visit HPE's [Business Continuity](#) and its [Data Protection Solutions](#) pages. There you'll find information about the full range of business continuity/disaster recovery and other related solutions available to SMBs.



In Chapter 3, you've learned to appreciate the costs and other trade-offs involved in setting recovery objectives, and how an interruption or disaster declaration puts recovery plans and resources to work. In Chapter 4, you'll take a look at security from the hardware level, and learn more about the importance of a Trusted—and secure—Supply Chain that provides such hardware.

## CHAPTER 4

# HPE Provides Built-in Security for SMBs

Security plays into all aspects of IT operation across the entire organization. Thus, security is important not just for system hardware and software, it's also important for the people who use such things. Establishing and maintaining security works best for businesses who choose a vendor who understands that security must be designed into systems and software, built into them from their inception, and maintained as part of a complete lifecycle process. In fact, HPE provides complete security coverage for the whole business, from end to end, for all systems and users alike. As this chapter will explain and illustrate, providing the means to secure and protect the hardware is a key component in ensuring and maintaining overall security. Because the most insidious attacks may seek to bypass operating systems and the security code they run, protecting hardware is the only way to create a secure foundation for computing overall.

## What Security Means in 2021

A good general definition of cybersecurity is a body of technologies, processes, and practices designed and enacted to protect digital systems and assets—including networks, devices, software, and data—from attack, damage, or loss, and unauthorized access. Thus, security is inherently all-encompassing and covers systems, communications, programs, data, and connections. Sensitive data often comes with the requirement for special attention and protection, be it intellectual property, financial data, personally identifiable information (PII), health records, and other kinds of data. If disclosed to the wrong parties, it could result in negative outcomes, both for the organization holding such data, and for the party to which the data refers or belongs.

Security is often applied to specific focuses or concerns and typically includes:

- **Server security:** The collection of tools, technologies, settings, firmware, and software (both inside and outside the server's operating system) that defines and provides security for networked servers belonging to an organization. Often involves access to infrastructure security elements, as well as server firmware plus standalone and operating system software components.

- **Client security:** The collection of tools, technologies, settings, firmware, and software (both inside and outside the client's operating system) that defines and provides security for networked clients belonging or connecting to an organization's networks. Often viewed as synonymous with endpoint security, because clients comprise the bulk of endpoints within most organizations. Usually incorporates threat detection and prevention components, including anti-malware, patch and update management, and more. Also interacts with infrastructure security elements, both local and remote (where applicable).
- **Network security:** The collection of tools, technologies, devices, and software that resides on or monitors and manages network devices (both physical and virtual). Generally involves inspection and filtering of network traffic, primarily at network boundaries to control ingress and egress. May host infrastructure security elements, often in the form of software-defined networking (SDN) for local or wide-area (SD-WAN) network components and services.
- **Cloud security:** The collection of tools, technologies, and software that resides in, monitors, and manages cloud access and use, setup and provisioning, tear down and decommissioning, and traffic/activity monitoring. Intended to protect the underlying

physical infrastructure, cloud security may also extend to virtual infrastructures and services running and data used in the cloud, as well.

- **Infrastructure security:** The collection of tools, technologies, and software used to monitor and manage any and all components of an organization's networks and infrastructure, including client, server, and network devices, as well as cloud components and services accessible to the organization. Infrastructure security provides a big-picture view for entire infrastructures, via dashboards, automation, and other tools used to view, manage, and control their constituent elements and components.

Interestingly, cybersecurity includes all of these various focuses and concerns. It involves software, hardware, and firmware used on clients, servers, and networks directly under an organization's control. It also involves cloud-based components often under a third-party's control (often a cloud platform, services, or Software-as-a-Service [SaaS] provider running a public or private cloud).

Risk management services also play into cybersecurity because they concern themselves with reducing or eliminating sources of risk that could potentially damage an organization's earnings, ability to conduct

business, or reputation using defensive or protective measures. It requires prioritizing and managing digital defenses to offset the potential adverse impacts of threats they pose (small or minor risks get little or no response, whereas large or major risks get big and substantial responses). HPE can help small businesses deal with all of these security focuses and concerns, and ensure that their risk management strategies are in keeping with their business goals and objectives. The sections that follow explain specific HPE technologies used to offset specific security risks, especially for HPE servers and their clients.

## **Silicon Root of Trust**

Silicon root of trust is designed to protect against specific, targeted firmware and BIOS attacks. It works for HPE ProLiant Servers, and establishes a link between custom HPE silicon on those servers and their Integrated Lights Out (iLO) firmware. Essentially, silicon root of trust prevents compromised firmware code from executing. It does so by running integrity checks on firmware code before it's allowed to execute, using special, read-only checksums and comparison tools not directly accessible to the operating system or programs that run atop the OS.

## HPE Pointnext Security Services

HPE Pointnext Services is HPE's support, advisory, professional, and education services organization. HPE

experts work with HPE customers to help them address security and risk management challenges across their digital transformation, IT operations from edge to cloud. HPE is happy to work with SMBs to help them prepare their workforce and re-skill their employees with security training courses and certification. Digital Learner subscriptions package HPE technical training for consumption by SMB teams, and combine access to all the value in training HPE offers—at a better value.

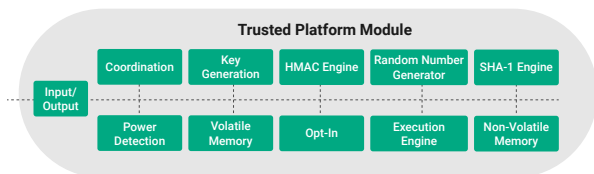


Whenever any evidence of tampering or change is detected, the HPE iLO firmware wipes the potentially (or actually) compromised firmware code. It uses a valid, known-to-be-correct firmware image from a trusted source to replace the code it finds. Then it executes that known, good working copy automatically. HPE iLO integrates encryption with its breach detection tools so that only safe firmware code can ever be executed. If

the server is unable to obtain or run such safe firmware code, it will shut down rather than run potentially compromised firmware. This ensures HPE ProLiant servers are protected from rootkit and other pre-boot attack methods and vectors.

## Trusted Platform Module (TPM)

The TPM comes in the form of a computer chip (microcontroller) that securely stores artifacts used to authenticate a runtime platform, including servers and client PCs (laptops, tablets, all-in-ones, and so forth). Since January 2021, Microsoft requires all new Windows Server platforms to incorporate TPM version 2.0, with Secure Boot turned on by default, and recommends that all servers also use BitLocker encryption for additional protection against potential “rootkit” malware attacks. HPE has backed and supported TPM since it became an



**Figure 5:** The Trusted Platform Module provides protected, chip-based storage, processing, and encryption tools for use at boot time



ISO/IEC standard (11990) in 2009. Today, all available modern HPE ProLiant Servers and HP, Inc. PCs meet or exceed these requirements.

As shown in **Figure 5**, a TPM provides a protected environment where secure credentials such as keys, certificates, passwords, and so forth can be generated, stored, and used securely outside the normal device processing environment. TPM is designed to be highly tamper-resistant, secure, and to provide a silicon-based root of trust to protect against rootkit, firmware, and other pre-boot attack vectors.

On a PC (server or client) a TPM provides secure storage for administrative access and BIOS updates. It also supports drive-level encryption (e.g. Microsoft BitLocker), biometrics data (e.g. Microsoft Windows Hello facial recognition or fingerprint info), and Microsoft's secure boot facility. Thus, a TPM enables and supports low-level, hardware-based security protection against low-level attacks. Microsoft works with all the major chip vendors (AMD, intel, and Qualcomm) to ensure proper integration of TPM functionality at the CPU level. HPE's modern server and HP, Inc.'s client PCs all support TPM 2.0 at a minimum, and offer a solid, protected silicon root of trust to users and organizations.

## HPE's Trusted Supply Chain

To serve customers with higher-than-normal security requirements and highly secure usage scenarios, HPE operates a [Trusted Supply Chain](#). Users of this supply chain include U.S. federal and public sector consumers who must purchase only U.S.-sourced products with verifiable cyber assurance. Buyers from outside the United States can purchase through this Trusted Supply Chain around the globe (except for China, Taiwan, and India). Security is built directly into this Trusted Supply Chain in two specific ways. First, it's accommodated through additional hardened security features in products themselves. Second, it's supervised by HPE employees who oversee those products during the manufacturing process. HPE employees vet all parts, observe assembly, and make sure packaged devices remain tamper-free until customers accept delivery.

Furthermore, HPE incorporates its own exclusive silicon root of trust that embeds silicon-based security into industry-standard servers, and maintains security controls across the entire supply chain to establish and maintain stringent security at the hardware level. HPE's hardening techniques include UEFI secure boot, a reduced attack surface, tamper-proofing at the silicon level, embedded alarms in systems, and physical locks. To learn more, please visit the HPE [Security Solutions](#)

page to learn more about HPE's baked-in, end-to-end security through its silicon root of trust, TPM, Trusted Supply Chain capabilities, and more.

## **HPE Covers the Full Range of SMB Security Needs**

Thanks for taking the time to read and work your way through *The Gorilla Guide To...<sup>®</sup> Secure IT for Small and Midsize Businesses, Express Edition*. Hopefully, you can now both understand and appreciate the depth of knowledge and skills that HPE can bring to bear on helping SMBs secure their businesses, and the range and depth of offerings it provides to help define, implement, and maintain proper IT security. From a silicon root of trust that builds security into its most basic operations at the server level, to a Trusted Supply Chain that makes sure that nothing extra winds up on your equipment, to technology solutions for WFH, remote access, wireless networking, file backup and restore, and business continuity, HPE has your SMB covered. And don't forget its Pointnext Services for security consulting, assessment, design, implementation, and more.

## ABOUT HPE



# Hewlett Packard Enterprise

Grow your business with small business IT solutions that power your key ambitions and help you achieve big goals. Explore how HPE small business IT solutions can best serve your small and midsize business needs.

[www.hpe.com/smallbusiness](http://www.hpe.com/smallbusiness)

# ABOUT ACTUALTECH MEDIA



ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

For more information, visit [www.actualtechmedia.com](http://www.actualtechmedia.com)



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit <https://www.gorilla.guide/custom-solutions/>