

HPE PRESENTS

THE GORILLA GUIDE TO...[®]



Modernizing and Securing IT for Small and Midsize Businesses

Ed Tittel

INSIDE THE GUIDE:

- Why digital transformation is worth pursuing for growth and innovation opportunities
- How HPE solutions help automate the hard work of setup, deployment, configuration and management
- HPE's baked in security model protects SMBs from risk, and lets them get on with business

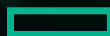
**HELPING YOU NAVIGATE
THE TECHNOLOGY JUNGLE!**



ActualTech Media

www.actualtechmedia.com

In Partnership With



**Hewlett Packard
Enterprise**

THE GORILLA GUIDE TO...®

Modernizing and Securing IT Operations for Small and Midsize Businesses

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

PUBLISHER'S ACKNOWLEDGEMENTS

EDITORIAL DIRECTOR

Keith Ward

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

PARTNER AND VP OF CONTENT

James Green

WITH SPECIAL CONTRIBUTIONS FROM HPE

Robert Checketts

Cole Humphreys

Tim Daron

Heather Leopard

Andrew Dodd

Michael Meek

Lauren Engebretson

Martin Oderinde

Antoinette Gerusa

Jennifer Streck

Victoria Hanrahan

ENTERING THE JUNGLE

Introduction: Maximizing Business Growth and Innovation Opportunities.....	8
Chapter 1: The Challenges of Legacy Technology.....	10
Where Legacy Can Fall Short.....	11
Leaving Legacy Behind.....	12
Legacy or Otherwise, Security Matters.....	13
The Benefits of Automation.....	14
Chapter 2: Setup, Configuration, and Deployment.....	17
About Setup, Configuration, and Deployment.....	18
HPE Solutions Wizard.....	19
HPE Intelligent Provisioning with Rapid Setup.....	22
Start Your Digital Transformation Today.....	23
Chapter 3: Management and Automation.....	25
Management and Automation in the SMB Infrastructure.....	26
Gain AI/ML Insight with HPE InfoSight.....	28
Management Efficiency with HPE Integrated Lights Out (iLO) Facility.....	30
Automate Your Infrastructure with HPE OneView.....	31
Moving from Technical to Cost Controls.....	32
Chapter 4: Cost Controls.....	33
Overcoming SMB Financial Concerns or Limitations.....	33
HPEFS Programs of Interest to SMBs.....	35
Other Options for SMBs.....	37
Equip Your SMB to Tackle Digital Transformation.....	39

Chapter 5: SMB Security Can Be Difficult (and Costly)	40
No Shortage of Security Trouble for SMBs	41
The Ever-Spreading SMB Boundary	42
HPE Security Solutions	43
Baked-in Security at the Edge	45
Chapter 6: New Security Challenges for SMBs	46
Secure Networks Deliver Secure Operations	47
Enable Secure WFH Productivity	51
Secure, Reliable File Backup—and Restore	52
Chapter 7: Business Continuity Is Increasingly Critical	55
The Many Faces of Business Continuity	55
Paths and Mechanisms for Business Recovery	57
Putting Business Continuity to Work	59
Chapter 8: HPE Provides Built-in Security for SMBs	63
What Security Means in 2021	64
Silicon Root of Trust	66
Trusted Platform Module (TPM)	67
HPE's Trusted Supply Chain	68
HPE Covers the Full Range of SMB Security Needs	69

CALLOUTS USED IN THIS BOOK



The Gorilla is the professorial sort that enjoys helping people learn. 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

Maximizing Business Growth and Innovation Opportunities

Welcome to The Gorilla Guide To...[®] Modernizing and Securing IT Operations for Small and Midsize Businesses (SMB)! If you're looking to up-level from your current situation, this book is for you.

To maximize their chances of business success, all companies—including SMBs—must do what they can to grow and innovate to the best of their abilities. In large part, this explains the impetus to digital transformation, which advances and improves an organization's IT infrastructure to support added innovation, boost productivity and profitability, plus shorten sales cycles. The plan is to get more bang from the bucks invested in technology.

To help SMBs get the most from digital transformation, Hewlett Packard Enterprise (HPE) is ready to help. It can assist SMBs in using automation more effectively. This accelerates the time it takes to install, configure, deploy, and manage IT assets and infrastructure. HPE also offers specialized tools to SMBs, such as its Solutions Wizard, which lets them choose new ready-to-run IT systems for their expected workloads. Likewise, HPE's intelligent provisioning pre-stages new servers with rapid setup so they can be deployed immediately upon delivery.

Best of all, HPE's vast technological acumen and experience lets them make its AI-driven management tools, and proactive troubleshooting facilities, directly available to SMBs. HPE's InfoSight technology puts Artificial Intelligence and Machine Learning (AI/ML) in play to develop insights and information from across its total customer base. It can then use what it has learned and determined to make recommendations and forestall potential threats and issues in SMB IT environments.

This Gorilla Guide illuminates the pathway to your own SMB digital transformation. It will help you scope out the costs involved, and the benefits delivered. Along the way, you'll also understand what HPE can do for your business to work through digital transformation with minimal disruption and maximum leverage for the growth and innovation opportunities it delivers.

Strap on your backpack and pith helmet as we forge into the wild for this exploration into growth and innovation opportunities.

Let's enter the jungle right now and get started on a journey of discovery. We'll start with a look at legacy technologies and infrastructures, and challenges they pose to digital transformation. Here we go!

CHAPTER 1

The Challenges of Legacy Technology

In This Chapter:

- Where and how legacy technology can fall short
- Escaping legacy technology, with security front and center
- Understanding and appreciating automation's benefits

Legacy systems involve hardware and software that may have once been widely used, and were even state of the art for their time, but are now passé and have been replaced or enhanced with something newer. Because technology evolves so quickly, it doesn't take long for current technology investments to become outdated.

The real catch is that, over time, older technology becomes less efficient and delivers a lower ROI than equivalent or more capable new technology. Thus, older technology may also not deliver the latest or best user experiences. Perhaps more disturbingly, older technology might hinder a business from delivering experiences as quickly or securely as customers like. In particular, security issues pose additional risks or open companies to fines and penalties when compliance requirements aren't met.

The sorry truth is that many small businesses (and business owners) hang onto legacy systems longer than they should. In fact, keeping outdated technology in service can raise costs and reduce productivity. That's why the benefits of replacing outmoded technology more than offset the risks involved in retaining legacy systems.

Where Legacy Can Fall Short

There are several areas in which legacy systems can pose expensive, sometimes business-crushing challenges. As shown in **Figure 1**, these include:

- **Maintenance** The time, effort, and cost involved in maintaining legacy systems can weigh heavily on small businesses seeking to manage and optimize budgets.
- **Security** While software and hardware vendors routinely provide patches, updates, and fixes to address threats and vulnerabilities, end-of-life (EOL) comes to every program and platform sooner or later. New technologies frequently include security enhancements that can't be added to older technology.
- **Compliance** For businesses that must comply with various regulatory frameworks or regimes (such as HIPAA, PCI, SOX, GDPR, and so forth) technology must be secure and supported, backed up with audits to check and confirm compliance. Compliance failures can lead to civil or criminal penalties, and punishing fines.

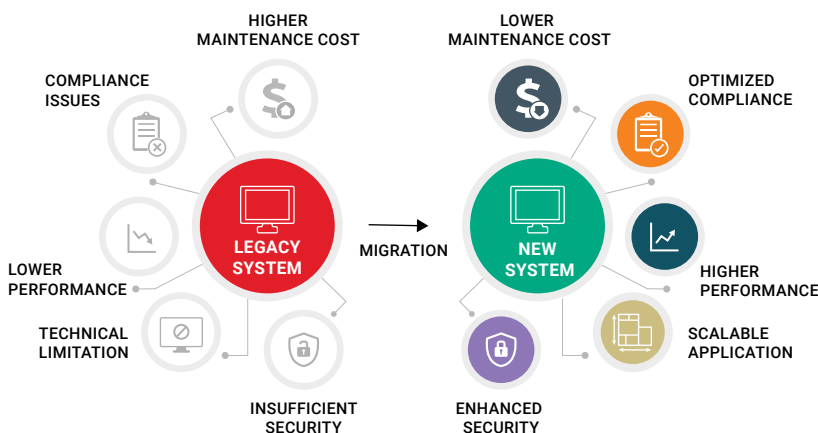


Figure 1: The issues SMBs face with legacy systems

- **Increased Failure Rates** As systems age, they can't help but start pushing the limits on their mean time between failure (MTBF) ratings. This makes downtime inevitable. Its consequences can be severe, including outright loss of customers and revenue if systems become inaccessible or unavailable.
- **Compatibility issues** Legacy systems are often incompatible with newer systems. This locks them out of new technologies and can pose high (if not impassable) hurdles to adopting and integrating cloud-based services and solutions.
- **Limited mobility** For businesses with employees in the field (delivery services, logistics, construction, consulting, and so forth) legacy systems may be hampered in supporting or unable to employ mobile devices to access inventory, accounting, customer data, and other functions. Because mobile devices—especially smartphones and WLAN-equipped handheld and laptop computers—are increasingly essential for effective field operations, this could negatively impact the bottom line.

All in all, SMBs need not look too hard or too far to find plenty of good reasons to update, upgrade, or replace legacy technologies. Ultimately, it's about lowering the TCO, improving reach and productivity, and introducing more opportunities to enhance existing products and services and introduce new ones.

Leaving Legacy Behind

The biggest reason to adopt new technology and to take legacy technology out of the picture comes from the opportunity costs that maintaining and operating legacy technologies impose on a business:

- When IT expends significant time and effort keeping legacy technology working, its people can't tackle tasks calculated to find new customers and new experiences, or make existing customers more satisfied with their current experiences.

- Likewise, when too many resources get allocated to maintaining an aging status quo, there's no opportunity for IT to tackle research and development. This robs them of opportunities to innovate and to seek competitive advantages.
- Growth and improvement come most readily when IT staff has the opportunity to do its current job better (and more quickly). Some might even argue that keeping technology current is IT's job, along with ensuring the best possible ROI on technology investments.

Legacy or Otherwise, Security Matters

To protect themselves from risk, harm, and loss, companies must take security seriously. This is especially important when it comes to managing customer data of many kinds, including personally identifiable information (PII), financial or account data (including accounts, transactions, credit card information, and so forth), and other data subject to compliance regimes or regulatory control.

In today's world, new security threats crop up by the thousands every day. Legacy technology is especially vulnerable to security threats and exploits because it's been around long enough to pile up considerable (and well-documented) avenues and means of attack. In addition, legacy technology may be unable to meet ever-evolving compliance requirements (as with the July 2020 invalidation of the [EU-US Privacy Shield](#)). This exposes companies to potential risks and losses they have no choice but to accept until they can put newer alternative technologies in place. For most businesses, involuntary risk exposure goes beyond what they can tolerate.

The High Costs of Securing Legacy Technology

According to [CSO Magazine](#) (March 2020), 60% of security breaches in 2019/2020 involved vulnerabilities for which a patch was available but hadn't been applied. Too many organizations—of which the

greatest number by statistics and reported breaches are SMBs—experience losses related to theft, downtime, and damage to reputation because they don’t (or can’t) take simple preventive measures to manage and reduce security risks and exposures. This is one area in particular where automation has an outsized influence and impact, as discussed in the following section. Legacy technology can be especially prone to vulnerability and attack, particularly in terms of its pre-boot environments (such as firmware, BIOS, and UEFI) because vendors typically stop patching and updating those environments once devices are more than 5 to 10 years old. When vulnerabilities and exploits target legacy hardware, there’s often no hope for patches or fixes to fend them off.

The Benefits of Automation

Finally, new technology brings added capabilities that act as a “force multiplier” for IT staff productivity. In particular, the automation that new technologies bring to the workplace—such as HPE InfoSight, HPE Integrated Lights-Out, and HPE OneView—provides profound benefits to SMBs that deploy them. Automation helps IT staff turn repetitive tasks over to scheduled, software-based tools that can perform them far more quickly and accurately whenever they’re needed (and such tasks can also be run on-demand or be triggered by specific events).

Though learning automation techniques and tools aren’t trivial, the payoffs are immediate and substantial. Because it can be tested and validated to make sure it works correctly every time it’s used, automation prevents human error from affecting routine tasks and activities, no matter how simple and straightforward they might be, or how time-consuming and complex they often are.



THE MANY WAYS AUTOMATION EASES IT'S BURDEN

Automation works across the entire IT lifecycle to assist at each step along the way. Thus, automation plays a role in defining, configuring, setting up, and deploying IT infrastructures, services, applications, and more.

Further automation can be used to provision virtualized and physical environments, whether on-premises or cloud-based (or as is increasingly the case, some combination of the two). The same automation tools cover maintenance and upkeep, including patches, fixes, and updates (and can even cover pre-OS components such as firmware, BIOS or UEFI elements, along with device drivers, APIs, frameworks, and more).

Automation also helps IT keep up with security monitoring and management, including vulnerability scans, update deployments, and remediation or mitigation tasks when warranted. Likewise, automation helps businesses stay on top of IT assets, related usage and licensing requirements, and cost optimization for IT resource consumption. It truly covers a broad range of IT tasks and activities.

Free Up Valuable Time

The real benefit of automation, of course, is that it frees up time for IT staffers who might otherwise spend their days maintaining legacy technologies. That time can then be better spent on researching and developing new products and services, selecting and deploying new technologies, and thinking of more and better ways to deliver value to

customers, employees, and business owners. The potential gains pose certain rewards to SMBs smart and savvy enough to put automation to work wherever and whenever the opportunity presents.

Once a business owner or IT manager at an SMB starts to understand the potential value of digital transformation, they will want to know exactly where that value comes from. Of course, they'll also want to know how it looks and works for them. In the next chapter, we'll examine a powerful source of value-add from digital transformation—namely the benefits that automation and related tools can provide. In particular, the focus will be on ways to simplify, streamline and speed up the process of new technology introductions. In large part, this comes from HPE's ability to help SMBs move quickly and efficiently through processes involved in setting up, configuring, and deploying new technology, software and systems.

CHAPTER 2

Setup, Configuration, and Deployment

In This Chapter:

- Streamlining new technology setup, configuration, and deployment
- Exploring the HPE Solutions Wizard
- Working with HPE Intelligent Provisioning and Rapid Setup

Digital transformation is the evolution of business activities, processes, competencies, and models to fully leverage the opportunities and capabilities of new digital technologies. Modern businesses, including SMBs, are under considerable pressure to grow and improve by implementing such new technologies. The overall goal is to bring customers, partners, and suppliers together in real time, and empower employees to maximize their productivity.

HPE drives three primary outcomes for its customers: efficiency, agility, and innovation.

- **Efficiency** comes from task automation that drives technology costs down, freeing up funds for other projects and activities.
- **Agility** comes from process orchestration, which improves timely execution and reduces the time necessary to respond to business requirements.
- **Innovation** occurs when the gains from improved efficiency and agility free people, time, and resources to identify, pursue, and implement new or improved business processes and capabilities.

HPE can help SMBs achieve their own digital transformations across the entire technology lifecycle. To that end, HPE can help SMBs deal with issues related to device setup, configuration, and deployment.

About Setup, Configuration, and Deployment

When new technology assets—particularly hardware, but often various software components, as well—are acquired, SMBs must set them up, configure them, and deploy them into their intended use locations. To make sure you appreciate the nuances that distinguish these terms, here are some definitions:

- **Setup:** Assembling the physical pieces and parts that comprise equipment, applying power for basic testing, and ensuring all ordered components are present and working
- **Configuration:** Adding appropriate settings, preferences, and options to make a device and its software ready to function, including network addresses, access to local directory services and admin accounts, proper access controls and filesystem structures, and so forth
- **Deployment:** Staging equipment to its intended use location, making all necessary connections (logical and physical), and testing to make sure that setup and configuration are valid and working and that the equipment and its software are ready to use

Speed Up Processes and Eliminate Errors with Automation

The processes involved in setup, configuration, and deployment that don't involve hands-on assembly or moving equipment are quite amenable to automation. This means that admins can create scripts or make use of tools to perform most of the work. This helps to speed up the process because it replaces tedious, manual, individual entries and

user interface (UI) navigation with a series of well-tested equivalent instructions. It also helps avoid error because it eliminates nearly all opportunities for human operators to make mistakes.

What kinds of SMB scenarios might lend themselves to automation? Consider two brief examples: First, automation can help an SMB select the right server model, equipped with the processing, networking, and storage capabilities to suit its intended purpose. Upon delivery, that server can be readied for use through judicious interaction with provisioning and setup tools designed to deliver working, reliable systems in short order. Second, an SMB might choose to deploy a database or some kind of application service running on a server. The same set of tools—and the same productivity boost—again applies.

As this chapter will explain, HPE offers powerful, usable tools and technologies to help SMBs deal with typical setup, configuration, and deployment scenarios like the ones just described.

HPE Solutions Wizard

HPE has heard from its customers that all too often sizing a business' technology needs can be complicated and overwhelming when trying to find the right solutions. The HPE Solutions Wizard takes your needs into account with a few simple filters and gives you the right solution in as little as two minutes. The HPE SMB Solutions presented are tested and validated configurations that simplify the selection process by providing a complete configuration right-sized for many SMB use cases.

When you visit the Solutions Wizard, you'll find simple instructions to guide you through its typical two-minute process. The Wizard's column headers are intended to give you the most relevant, technical information about related hardware's internal components (see **Figure 2**).

Once you're ready to begin you can see a list of filters at the top that let you refine your solutions search. Start by selecting a use case that fits your business needs.

Welcome to the HPE Solutions Wizard.

In less than **2 minutes** we will help you find the right-sized cost-effective server, storage and network solutions that will solve your business needs and get you prepared for future growth.

Use Case
☐ File
☐ Virtualization
☐ Backup / Archive
☐ Small Office Deployment

Optimization ?
☐ Application
☐ Database
☐ Shared Storage
☐ HCI

Optimization ?
☐ Performance
☐ Balanced
☐ Cost

Expandability ?
☐ High
☐ Medium
☐ Low

Operating System
☐ Microsoft
☐ VMware
☐ ClearOS

Form Factor
☐ Rack
☐ Tower
☐ Micro Tower

Instructions

Reset Filters

Found 50 Offers

SMB Solution Description	Solution Components	CPU # Sockets Installed Frequency # Cores/CPU Brand	Memory Installed (Maximum)	Drive Bays Installed/Available/Maximum* (* Requires Optional Hardware)	Total Data Storage Internal (External)	Networking	Details
ML30 File Solution	ML30 Gen10 85FF Server	1 Socket(s) 1 CPU(s) 3.4 Ghz 4 Cores Intel	32 GB (64 GB)	8 / 2 / 8 Internal 0 / 0 / 0 External	4.8 TB (0 TB)	2x 1GbE	6d
ML30 Archive Solution	ML30 Gen10 4LFF Server	1 Socket(s) 1 CPU(s) 3.4 Ghz 4 Cores Intel	16 GB (64 GB)	4 / 0 / 4 Internal 0 / 0 / 0 External	4 TB (0 TB)	2x 1GbE	6d
		1 Socket(s) 1 CPU(s)					

Figure 2: The HPE Solutions Wizard helps SMBs select the right solution in as little as two minutes with helpful filters that refine the solutions search

From there, select an optimization that fits your need. Performance servers are the best of the best, Balanced finds the sweet spot between performance and cost, and, finally, Cost is focused on providing the most value for your dollar. These optimizations are compared to all other solutions that we offer in the same use case.

Fast and Simple Access

First, navigate to <https://www.hpesmbolutions.com/smb/> to access the Solutions Wizard. When you first arrive, there are simple instructions that guide you through the two-minute process. Working through the Solutions Wizard is fast and simple, and will quickly show you how this tool helps SMBs identify and configure the kinds of hardware solutions they need to meet their IT needs.



Next, choose expandability, which is the degree to which the solution can be expanded from the default Solution configuration. This takes into account CPU, Memory, Storage, and Networking. Generally, more expandable systems have a higher cost than systems with low expandability.

Choose an operating system (OS) and form factor to further refine your selection.

To get more information on your new, sized solution you can select the magnifying glass icon underneath the details header on the right-hand side. Once you click on it you can see what components are included with the server, required additional hardware and software to satisfy the use case, and recommended hardware and software to help you maximize your new solution.

The wizard also gives you the functionality to visit the solution in the HPE store, open the solution in iQuote to work with your favorite distributor, or export the bill of materials (BOM) to send to a colleague or preferred partner.

All SMB Solutions have key resources that help you deploy your use case or view a solution brief that gives a high-level overview of the system. These documents are listed along with a link to QuickSpecs to get more technical information on the server.

In a matter of a few minutes, you can successfully size and select an HPE SMB validated solution that can be fulfilled through [iQuote](#) or the [HPE store](#). When you're ready to start again, reset your filters and refine your ideal settings to see a solution that will best suit your needs. HPE is focused on getting you back to what matters most—your customers.

HPE Intelligent Provisioning with Rapid Setup

Once a server is delivered to your premises, HPE helps automate and expedite the rest of the setup–configure–deploy triad with two highly automated and intelligent tools: [HPE Intelligent Provisioning](#) and HPE Rapid Setup. Following are descriptions of each tool.

HPE Intelligent Provisioning is a single-server deployment tool embedded in the HPE Integrated Lights Out (iLO) management utility of ProLiant servers and HPE Synergy compute modules. It simplifies server setup, providing a reliable and consistent way to deploy servers. HPE Intelligent Provisioning features the Rapid Setup tool described in the next section, but also includes an Always On Intelligent Provisioning facility, maintenance utilities, firmware updates, improved installation wizards, advanced Basic Input/Output System (BIOS) settings, and Enhanced Secure Erase to safely and completely delete all data on hard drives.

The Always On feature allows access to Intelligent Provisioning from the iLO browser UI anytime without having to reboot your server. It provides ready access to advanced BIOS settings to enable, disable, and configure devices at a low level on the server, even before an OS is loaded.

Intelligent Provisioning enables complete custom server setup from start-up to installing the OS. This is ideal when you need special configuration of the server to prepare it for a unique use case. But for common single-server and SMB use cases, Intelligent Provisioning also provides HPE Rapid Setup for even faster deployments.

HPE Rapid Setup now appears as a server and OS deployment option within the HPE Intelligent Provisioning environment (requires 3.31 release or higher and works with all HPE ProLiant 10, 100, and 300 series Gen10 Servers).

Rapid Setup automates server deployment by inventorying the installed components and then presenting a recommended configuration based on best practices. If the recommended configuration is accepted, all that's needed is to provide the OS installation file location and Rapid Setup will automatically configure the server RAID configuration and install the OS, and even update drivers and server firmware if desired.

Of course, if the recommended configuration doesn't meet your requirements, Rapid Setup will provide the opportunity to manually configure the server using a simplified interface that's easy to use.

Rapid Setup also supports or includes the following to help with setup, configuration, and deployment:

- Windows OS, along with Hyper-V and VMware virtualization environments
- BIOS configuration utility
- Hardware validation tool
- Tools for updating software and firmware
- Integrated ability to access HPE support and other on-line resources

Start Your Digital Transformation Today

All in all, HPE Intelligent Provisioning and HPE Rapid Setup make it as simple and straightforward for SMBs to work through the setup, configuration, and deployment processes as modern technology will allow. Seeing is believing: Ask HPE to provide a demo and you'll be able to watch it work for yourself. You can also watch the [HPE ProLiant Gen10 Rapid Setup](#) demo on YouTube. Or, you can check out the [Solutions Wizard](#) for yourself. Then, visit the [HPE Intelligent Provisioning](#) home page for more information, downloads, and resources. It's never been easier to start your SMB down the path to digital transformation.

Once equipment has been purchased, delivered, installed, configured, and deployed, the real IT work begins. More than 80% of the lifecycle for typical IT infrastructure and equipment is spent on maintenance, management, and upkeep. In fact, IT is responsible for all that work. Anything that boosts productivity, speeds task completion, and improves accuracy and reliability during maintenance mode is a huge win—especially for the IT staffs charged with making all this happen and taking care of the business along the way. In the next chapter, we turn our focus to the topics of management and automation, to explain how automation can save IT time and effort, while also ensuring rapid response to issues and problems, and accurate, reliable handling of maintenance tasks.

CHAPTER 3

Management and Automation

In This Chapter:

- Management and automation: keys to SMB infrastructure
- Using HPE InfoSight for AI-driven insights and actions
- How HPE Integrated Lights Out makes management efficient

Set up, configuration, and deployment are relatively easy for IT, because those tasks don't happen terribly often (typically, only when new equipment arrives, or upgrades must be added to existing equipment). But management and maintenance are literally for the life of the solution, and happen every day. HPE understands that even modest improvements in regular, repeated activities can pay big dividends over time. The company also sees that eliminating human error, and speeding task completion add up nicely, too. In this chapter we'll explore the important roles that proper management tools and good use of automation can play to significantly boost IT's capabilities, productivity, and reach. In an era of "doing more with less," management and automation help IT organizations do more, faster, and better than they otherwise could.

Management and Automation in the SMB Infrastructure

Within IT, management means more than simply watching over and taking care of systems, assets, and infrastructure. It covers the entire IT lifecycle from initial determination of needs and requirements; to evaluation and selection of technologies, tools, and platforms; to negotiating purchase and support costs; to installation and configuration; through upkeep and maintenance and ongoing review; all the way to decommissioning and proper surplus operations or outright destruction at end of life (recommended for old storage media used for sensitive data, for example).

In fact, management has been a formal IT discipline for over three decades. That's long enough for the initial management model to become outmoded and be replaced with something newer and more robust. The early model was sometimes called FCAPS: for fault, configuration, accounting, performance, and security, all management categories covered under that model. Modern IT management falls under the heading of IT Service Management (ITSM). These days, ITSM means understanding the IT lifecycle, and how delivering quality IT is itself a service discipline that follows an agile DevOps-inspired approach called CI/CD—continuous integration along with continuous delivery.

In IT, automation generally refers to the use of recorded and repeatable instructions or directives that do programmatically what an IT professional does manually (by entering commands, running a user interface, using tools and utilities, and so forth). Once automated, software tools, frameworks, and appliances can handle tasks with little or no human interaction. IT automation has a broad scope that runs all the way from single actions, to specific sequences of instructions, to full-blown IT deployments whose actions respond to security incidents, user behaviors, or specific event or value triggers.

Proper use of automation tools and frameworks can help IT (and businesses of all sizes and scales, including SMBs) be more productive and responsive to users and stakeholders. First, automation runs much faster than human-computer interactions can. In fact, automation is hundreds to thousands of times faster than manual input, especially for simple, routine tasks. This makes proper automation especially useful for incident response because it can move as quickly to defend as an automated attack can proceed. Second, because automation can (and should) be tested rigorously to make sure it works without errors or issues, it's also more reliable than human input once it's put into production. Given access to results from analytics, cost, or performance monitoring data, automation can also take action to limit resource consumption when costs exceed a preset minimum or when resource consumption spikes.

In general, proper use of automation helps IT (and the businesses it supports) be more productive and responsive to changes in demand or resource requirements. Typical uses of IT automation in SMB operations include:

- Monitoring networks, servers, and clients for health
- Tracking vulnerabilities and update status
- Automated deployment of patches, fixes, and updates

Because automation helps IT do more—and do things faster and more reliably—it's a huge boon to SMB IT teams, which often work under tight resource constraints (especially headcount).

In the sections that follow, you'll learn more about some HPE offerings that can be of particular help and value to SMBs and their IT organizations.

Gain AI/ML Insight with HPE InfoSight

Artificial intelligence and machine learning (AI/ML) can deliver valuable benefits to SMB IT organizations. The intelligence and insights that AI/ML provide often prove particularly helpful in organizations where human resources are tight, and spare bandwidth to cover strategic analysis and planning may simply be unavailable. A management philosophy called AIOps is emerging in IT, whereby insights and information elicited from AI models and analyses is immediately put to work to help organizations make better, more efficient use of the IT assets and resources available to them (both on-premises and in the cloud). And, of course, automation plays a key role in such capability because it provides a reliable, well-tested framework within which speedy, program-driven IT management becomes possible.

HPE InfoSight, a predictive analytics tool that uses AI and ML to address IT issues before they can impact the infrastructure, has over 10 years of collecting telemetry data and retraining ML models. Each second, millions of sensor measurements capture the state of systems, subsystems, and surrounding IT infrastructure within thousands upon thousands of organizations. This data is collected and analyzed across the entire HPE global installed base. More data leads to greater insights and enables HPE InfoSight to make more intelligent decisions and recommendations. A global intelligence engine sits at its heart. This is where cloud-based ML comes into play. From the insights the intelligence engine provides, HPE InfoSight can:

- Make recommendations
- Provide proactive wellness, monitoring, and adaptive behavior through global learning
- Create and apply workload fingerprints
- Apply predictive analytics
- Automate support wherever and whenever possible

By leveraging analytics collected across countless HPE customer platforms around the world, HPE InfoSight iterates through innumerable cycles of observing-learning-predicting-recommending-acting. This process allows advanced visualizations and dashboards for users and supports a fully workload-optimized infrastructure.

For most SMBs, HPE InfoSight lets them optimize IT performance, as the global data patterns let them predict and prevent problems before they become serious. HPE InfoSight also helps make infrastructures smarter and keep improving themselves, based on observation and repetition of what works best for current situations and circumstances. Thus, HPE InfoSight helps SMBs make their IT assets more available and reliable, and assists in optimizing application performance and in planning for growth and expansion of IT resources. When HPE Pointnext Services comes into the picture, its consultants can offer further recommendations to optimize workloads and enhance productivity.



HPE POINTNEXT SERVICES SPECIALIZES IN DIGITAL TRANSFORMATION

HPE's Pointnext Services can help IT organizations plan and do more by tapping the expertise of HPE's own consulting staff (who may have skillsets that are difficult or impossible to develop in-house in an SMB). Pointnext Services helps customers go beyond traditional hardware support to offer recommendations on how to optimize and run their workloads better, cheaper, and faster. All in all, [HPE Pointnext](#) offers SMBs the precious commodity known as "peace of mind," secure in the knowledge that their IT operations are effective and optimal. HPE Pointnext is ready to help SMBs design their own digital transformations with the benefit of expert and insightful IT consulting.

Management Efficiency with HPE Integrated Lights Out (iLO) Facility

The HPE Integrated Lights Out (iLO) facility is a toolset designed to manage servers efficiently, resolve issues quickly, and keep businesses running. Better yet, iLO works from anywhere and provides all firmware, drivers, and tools needed for installations and upgrades. It also makes HPE servers immediately ready to provision and configure, right out of the box.

iLO's integrated system and OS configuration tool simplifies and speeds up server installation and setup, supports rapid setup capabilities, and works with HPE OneView automation. iLO also offers important security features. These include a silicon-based root of trust that prevents malware (especially rootkits) from inserting itself into hardware before the boot process (and OS start-up) completes. iLO provides a server configuration lock to prevent unauthorized changes, and includes a one-button secure erase tool to remove all previous content when a new server image gets installed. In general, HPE iLO supports the world's most secure industry-standard servers (see the "HPE Secure Compute Lifecycle: Building on the world" most secure industry standard servers to optimize your security environment" [whitepaper](#) for more information).

In addition to basic iLO functions built into HPE ProLiant servers, available upgrade options include the following:

- graphical remote console (free until end of 2020)
- multi-user collaboration
- video record/playback
- discover, inventory, and update OS, applications, drivers, and firmware

All this capability makes HPE iLO a real workhorse for SMB server operations. In the following section, you'll learn about HPE OneView, a general IT infrastructure management and automation toolset, which also includes all of the HPE iLO capabilities.

Automate Your Infrastructure with HPE OneView

HPE OneView provides an integrated, general-purpose IT infrastructure management platform. It also supports automation of IT operations through workflows, along with a modern dashboard (**Figure 3**) and a comprehensive partner ecosystem. HPE OneView uses software-defined intelligence to enable automated infrastructure provisioning with repeatable, easy-to-use templates. These templates ensure high reliability, consistency, and control, and can lead directly to lower operating expenses.

HPE OneView also helps to simplify lifecycle management for all common IT resources, including computer, storage, and networking. IT administrators can compose on-premises physical infrastructure quickly and easily, because that physical infrastructure is defined

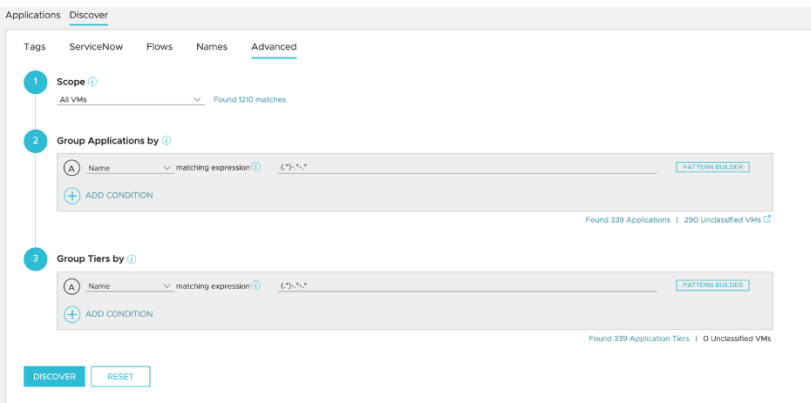


Figure 3: The HPE OneView Global Dashboard helps IT staff troubleshoot alerts and view core inventory data for up to 75 HPE OneView appliances and 20,000 servers in multiple data centers across the globe

using software. This makes the infrastructure directly programmable (and easy to automate), and lets you manage it as you'd manage code—through a single, unified API. Better yet, HPE OneView gives IT administrators the tools they need to connect their software-defined infrastructure from core to cloud by provisioning a turnkey private-cloud infrastructure through its partner ecosystem (including various Microsoft Azure and VMware offerings; see the [HPE Infrastructure Automation Made Simple](#) brief).

HPE OneView supports the HPE product portfolio, including its servers, storage, and networking equipment. For all those IT elements, HPE OneView provides simple and automated management of infrastructure and assets. For more information please visit the [HPE OneView](#) home page.

Moving from Technical to Cost Controls

In modern IT operations, management tools and insights provide information, control, and overview of systems and infrastructure. But SMBs also need cost controls and financing options to put digital transformation to work in their businesses. In the next chapter, we'll examine the various programs and plans that HPE Financial Services offers to SMBs, to let them keep doing business even while planning, implementing, and deploying new IT tools and technologies to make digital transformation both possible and profitable.

CHAPTER 4

Cost Controls

In This Chapter:

- Addressing SMB financial constraints and concerns
- Exploring the many programs available from HPE Financial Services
- Arming your SMB to tackle digital transformation

SMBs, like all business, run on money, and exist—at least in part—to make money. HPE understands that SMBs need funding to pay for digital transformation, and must have means to cover their expenses while that transformation is underway until it starts paying off. HPE Financial Services (HPEFS) offers a number of interesting and innovative programs and payment plans to help SMBs start on digital transformation sooner, and let the funding take care of itself over time. Read on to learn about a plethora of programs designed to let SMBs trade current costs against current and future earnings in a variety of ways, including a form of technology subscription.

Overcoming SMB Financial Concerns or Limitations

HPE can help SMBs accomplish their own digital transformations while controlling costs. SMBs always seek ways to preserve cash flow, defer or reduce expenses, and relieve capacity strains and delivery delays.

To those ends, HPE Financial Services promotes financial vitality with a portfolio approach to IT investments, including financing, subscription, and asset lifecycle management programs.

By aligning tech assets and business objectives, SMBs can:

- Conserve cash and enjoy predictive pricing through a subscription program
- Manage budget across all company priorities and goals
- Find value in legacy assets to fund new technologies to replace them
- Help ensure business continuity and viability by addressing new technology financing needs
- Cost-effectively manage assets across initiatives and their entire lifecycles

HPE Financial Services has a long history of both financial and technical acumen that, when combined, helps customers create an IT playbook with its SMB customers to help them understand the financing options available to them. This IT playbook helps SMBs ensure that they're taking advantage of the best financing solutions available, staying agile and delivering on business goals.



HPEFS PAYMENT DEFERRAL

HPE Financial Services offers a 90-day payment deferral program. This lets SMBs acquire new technology immediately with no payments for up to 90 days, followed by 36 low monthly payments. The full portfolio of HPE servers and systems, networking, and data storage hardware falls under this umbrella.

HPEFS Programs of Interest to SMBs

In addition to industry-standard IT financing options, HPE Financial Services offers a number of finance programs designed to let SMBs cover the costs of a technology refresh or a digital transformation without straining cash flow or threatening business productivity. HPE's programs are designed to bridge the gap between finance and technology, when businesses may need funds to supplement their own resources, as shown in **Figure 4**. Five such programs are described in the subsections that follow.

Generate Cash from Existing Assets

HPEFS helps SMBs free up value from their existing technology assets, which may be converted into capital to purchase new or up-graded technology. Such an incremental capital resource helps close gaps in IT outlays. It also gives SMBs added flexibility to fund other

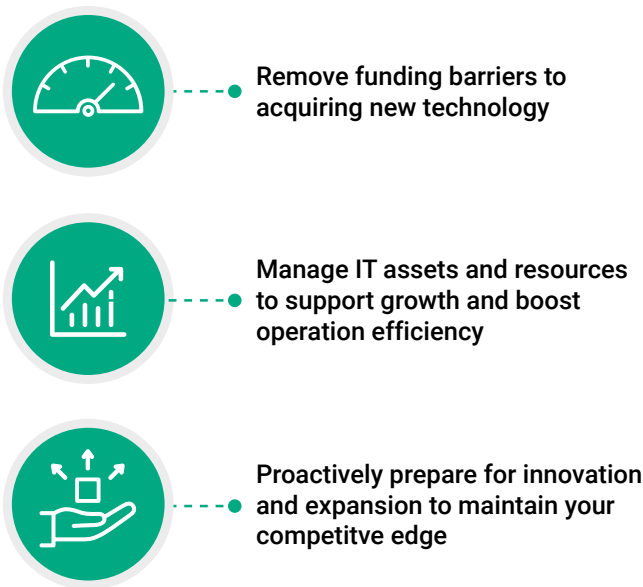


Figure 4: When internal funding isn't enough to cover costs for digital transformation, HPEFS can help!

aspects of their businesses. HPEFS can even buy back an SMB's excess newer-generation technology that it no longer needs or wants. Since 2018, HPEFS has turned such assets into \$642M for its clients and customers.

Subscribe to Complete IT Solutions

To give SMBs an unparalleled opportunity to obtain affordable and timely access to the right IT tools and technologies, HPEFS offers subscription plans for new technology purchases. With delivery and installation guaranteed within a short time after starting a subscription, SMBs can begin using their new capabilities quickly. This program includes seamless upgrades and refresh elements, so SMBs that buy into the program are automatically pricing in upgrades and updates for the foreseeable future.

Match Payments to Production

HPEFS offers SMBs a phased deployment program that lets them acquire compute and storage capacity immediately. They can then take the time they need to configure, test, and deploy systems before making any payment. This allows SMBs to keep their essential business activities up and running, without having a huge impact on their budget cycles and implementation timelines. Under this program, a deployment schedule can extend as long as 12 months, giving SMBs up to a year to pay for purchases they can put to work immediately, paying only when the equipment starts generating income to offset their costs.

Optimize Legacy Environments

HPEFS offers certified, pre-owned HPE technology to address certain typical SMB situations at reduced cost. Such offerings can be worthwhile for SMBs that need to support legacy applications, ensure business continuity, or provide additional capacity and capability to meet peak or seasonal demands for compute, storage, and networking resources.

Short-Term Rentals to Relieve Capacity Strain or Delivery Delays

Finally, HPEFS offers short-term rentals from 3 to 12 months for pre-owned HPE technology, and up to 12 months for new HPE PCs. In this way, HPEFS helps SMBs fill gaps resulting from migrations or unplanned impacts to the business (like those prompted by nearly universal work from home regimes in many or most SMBs, which need PCs suitable for their remote workers). Such technology comes factory-configured to meet the SMB's specifications, includes a standard warranty, and is eligible for HPE Pointnext Services support and further warranty extensions.

Other Options for SMBs

In addition to these programs, HPEFS offers other options that may be of interest to its SMB customers, including:

- **HPE Adaptable Use Models:** HPEFS offers such models to its customers as an investment solution with configurable capabilities. SMBs can choose a monthly payment plan with an option to adjust payments up or down based on pre-planned contingencies or needs. This approach gives SMBs more flexibility in managing an extended deployment schedule. It can also help them cope with uncertainty in forecasting IT demand or in taking on the risks involved in a pilot project.
- **Asset Upcycling Services** SMBs that choose to cash in on existing legacy IT assets to finance acquisition of new technology must make sure their old technology can't be misused or lead to unwanted information disclosures. HPE's Asset Upcycling Services apply secure overwriting to any storage media traded in. It also guarantees environmentally responsible removal and recycling for all technology, whether it's to be repurposed or retired from service completely.

- **Payment Deferral and Pay-as-You Grow** HPEFS offers a variety of payment plan options so SMBs gain flexibility in financing—and paying for—their digital transformations. Payment deferral permits outlays to be delayed by up to 90 days under certain circumstances (talk to HPEFS). Pay-as-you-grow plans allow SMBs to take advantage of graduated payments, which start small as new technology gets deployed and grow bigger as that technology starts paying for itself and generating additional revenue.
- **HPE Pre-Provisioning** This solution lets SMBs obtain quick access to pre-configured, ready-to-run servers, VMs, and other technologies in advance of actual need. A variety of pre-provisioning options for hardware and services are available from HPEFS, so be sure to inquire as to how this might help your business grow as circumstances dictate.
- **HPE Subscription for Servers** This is the name of the HPEFS offering that enables SMBs to select a complete technology package from a set of pre-defined options that includes best-in-class computer, storage, and networking hardware, software, accessories, and HPE Pointnext Services for a predictable monthly fee. SMBs simply subscribe, use, return, and renew as they need to, with the option to add to their subscription for more capability and capacity at any time.

HPE Financial Services stands ready to assist and enable its SMB customers to take advantage of the improvements in efficiency, productivity, and profitability that a digital transformation can bring. When you interact with HPE, be sure to ask HPEFS about how it can help your business do and be its best through careful and considered acquisition of IT tools and technologies. HPEFS can help you find the best way for your business to do what it needs to, at an affordable price, on comfortable terms.

For more information, please visit the IT Financing Solutions for Small and Midsized Businesses or the HPEFS pages.

Equip Your SMB to Tackle Digital Transformation

By now, you should recognize that HPE has the solutions, along with powerful management and automation tools, to make the technology your SMB needs to support digital transformation easy to choose, install, set up, configure, and deploy. In addition, certain HPE offerings—especially HPE InfoSight, HPE OneView, HPE iLO, and more—are designed to make your modern new IT infrastructure easy to manage and maintain.

HPE supports SMBs deliberately and directly with powerful, reliable automation facilities and capabilities designed to make their IT more productive and efficient, and less prone to delay and error. To that same end—digital transformation success for SMBs—HPE offers a broad range of financing and payment plans and programs to get powerful, beneficial new technology to work sooner, rather than later. Above all, HPE wants SMBs to reap the benefits of digital transformation quickly, so the investment required can be recouped as soon as possible.

In the next chapter, we change direction a bit, and start down the seemingly dark and forbidding path of cybersecurity, including threats, vulnerabilities, the possibilities of breach they pose, and the costs and consequences that can come in their wake. Scary stuff, but we'll do our best to steer you past the pitfalls (complete with hungry alligators).

CHAPTER 5

SMB Security Can Be Difficult (and Costly)

In This Chapter:

- Surveying the perilous security landscape and its hazards
- Understanding the expanding SMB security perimeter
- Pondering HPE's security solutions and their "security-first" approach

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 5**).

HPE even addresses security in its own product development and delivery, using a formally documented, frequently audited secure supply chain (see Chapter 8).

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.

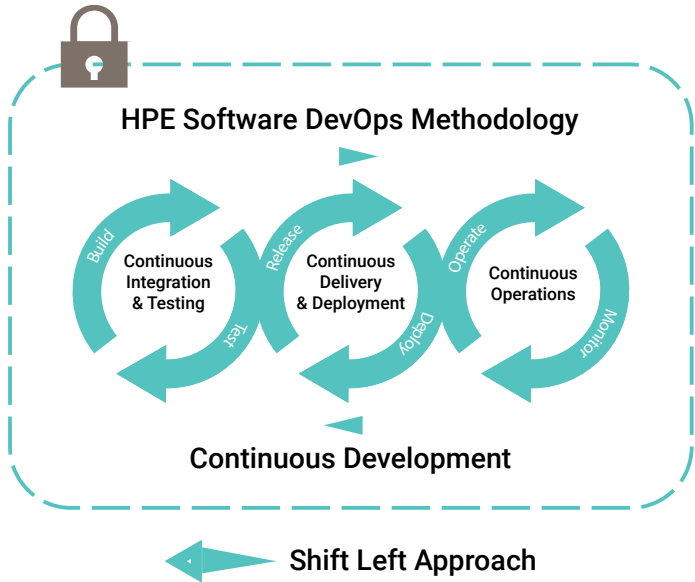


Figure 5: DevSecOps expands on the underlying concepts of DevOps to build the mindset that everyone is responsible for Security

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 5, 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 6

New Security Challenges for SMBs

In This Chapter:

- Work from home (WFH) poses interesting security concerns
- Making networks and their users secure
- Fostering real WFH productivity and innovation

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



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.

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.

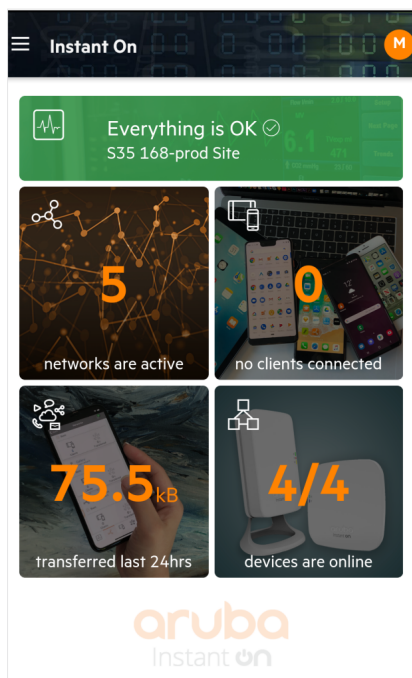


Figure 6: Aruba Instant On allows small businesses to create, modify, and monitor network components from a central location

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.

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 6**). The app offers excellent visibility into access and usage, and can block unsolicited applications or access to disallowed websites quickly and easily (see **Figure 7**). 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.

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.

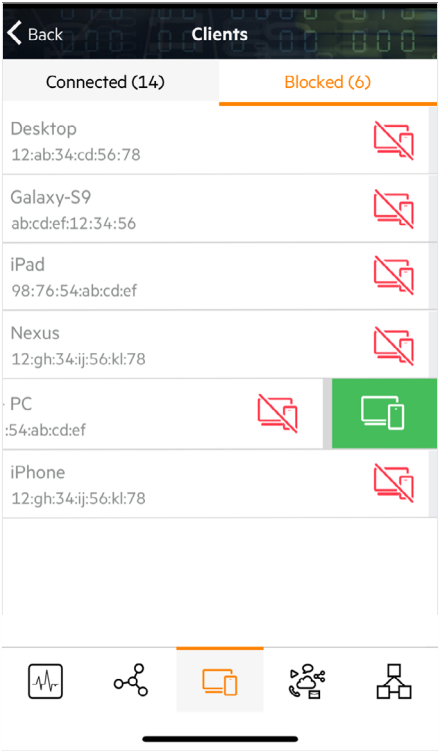


Figure 7: Get visibility into all connected devices and the ability to block specific, unwanted clients from accessing the network

Furthermore, Aruba Instant On can keep your network up-to-date through automatic installation of software updates, ACLs, and black-lists 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 6, 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 7, you'll learn more about the importance of business continuity and the tools necessary to keep your business running without interruption.

CHAPTER 7

Business Continuity Is Increasingly Critical

In This Chapter:

- Understanding why business continuity is vital
- Exploring the many elements involved in business continuity
- Putting modern business continuity to work

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, midsize 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.

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.



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.

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 8 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

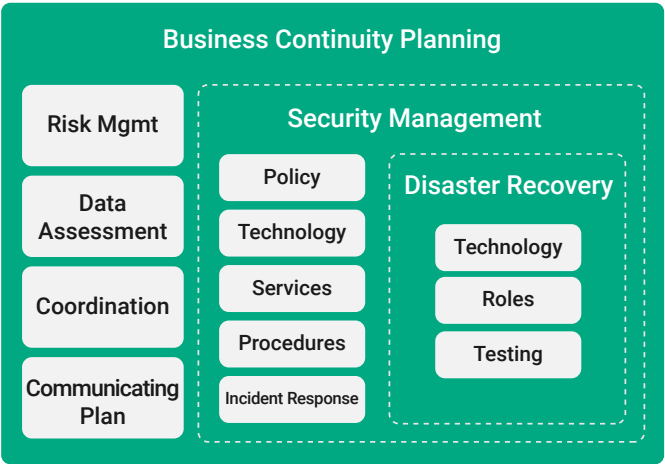


Figure 8: Disaster recovery is a subset of security management, and falls under the general heading of business continuity planning, along with risk management, data assessment, coordination, and creation/communication of the business continuity plan itself

- **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 7, 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 8, 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 8

HPE Provides Built-in Security for SMBs

In This Chapter:

- Everything—including security—starts with hardware
- Mapping out the Silicon Root of Trust and the Trusted Platform Module
- Savoring HPE's Trusted Supply Chain and the security it brings

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

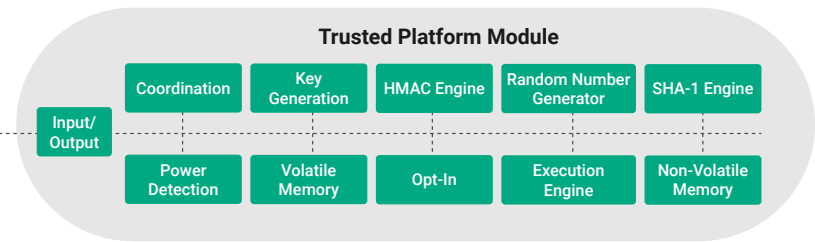


Figure 9: The Trusted Platform Module provides protected, chip-based storage, processing, and encryption tools for use at boot time

As shown in **Figure 9**, 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...® Modernizing and Securing IT Operations for Small and Midsize Businesses.

Hopefully, you can now both understand and appreciate the depth of knowledge and skills that HPE can bring to bear on helping SMBs to plan for, achieve, manage, and finance digital transformation, and then to secure their transformed businesses. HPE offers tools and technologies to escape from legacy challenges, and to streamline deployment (and payback) of new technology investment in digital transformation. By boosting productivity, fostering innovation, speeding up the business cycle and supporting new technology finance, HPE also seeks to improve ROI and boost overall business productivity and profitability.

On the security front, the range and depth of HPE offerings to define, implement, and maintain proper IT security are equally important to business success. 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.

To support all of its solutions, tools, and technologies, HPE also stands ready to help SMBs achieve secure and profitable digital transformation. Be sure to work with HPE Pointnext Services for digital transformation and 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

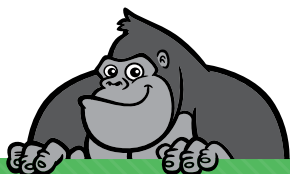
ABOUT ACTUALTECH MEDIA



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.



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/>