the GORILLA GUIDE® to...

Secure IT Deployment for Small to Midsize Business

Maximize Your IT Investment and Productivity with HPE and Its Partners

ED TITTEL

Hewlett Packard Enterprise

POWERED BY ActualTech MEDIA

THE GORILLA GUIDE TO...®

Secure IT Deployment for Small to Midsize Business, Express Edition

By Ed Tittel

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, Sr. Manager, Product Marketing
Andy Fernandez, Senior Manager, Zerto Product Marketing
Cole Humphreys, Director of Security Product Management
Ruben Ramirez, Manager Security Product Marketing
Mark Simpkins, Manager SMB Product Marketing

ABOUT THE AUTHOR

Ed Tittel is a 30-plus year IT industry veteran who's worked as a developer, in various management roles, a technical evangelist, and as a trainer. Ed is the author of over 100 computing books and countless articles, blog posts, white papers, and more. For more info visit edtittel.com.

ENTERING THE JUNGLE

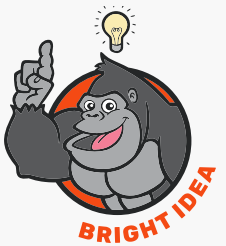
CALLOUTS USED IN THIS BOOK

SCHOOL HOUSE

The Gorilla is the professorial sort that enjoys helping people learn. In this callout, you'll gain insight into topics that may be outside the main subject but are still important.

FOOD FOR THOUGHT

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



BRIGHT IDEA

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

DEEP DIVE

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

EXECUTIVE CORNER

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

With the vast majority of U.S. businesses falling into the small to midsize category (over 99%, in fact), the overwhelming majority of organizations employ 499 employees or less. Worldwide, that number hovers around 400 million total companies. In fact, some 96% of such operations employ 100 or fewer full-time workers, and a great many of those employ 10 workers or less. Given chronic and ongoing cash and human resource constraints, effective deployment of information technology poses all kinds of interesting problems, not least of which is cybersecurity.

In this Gorilla Guide® To... Secure IT Deployment for Small to Midsize Business, we'll explore the hallmarks and characteristics typical of small to midsize organizations, and call out the kinds of technology challenges they face in deploying, maintaining, and securing workable IT solutions. Along the way we'll look at how businesses of various sizes in this spectrum may be characterized and understood and explore the value and insight that Hewlett Packard Enterprise (HPE)—and its partners—can bring to help these organizations maximize their returns on IT investment, while protecting people, systems, assets, and data.

CHAPTER 1

Focus on Your Business

Businesses face extraordinary challenges trying to succeed in an active, competitive, and ever-changing marketplace. Businesses require the confidence, foresight, and clarity needed for success. They don't need to worry about technology management burdens. Rather, their objectives must be to work on achieving long-term goals while meeting and handling near-term business challenges. Their primary focus must be to survive, so they can succeed and thrive in their chosen markets and customer bases.

HPE and its partners are here and ready to help businesses through products, services, and the expertise for companies that range from very small (a single person) to midsize (a hundred or a few hundred employees). HPE even offers financing and buy-back plans to help cash-strapped businesses fund necessary technology upgrades and refreshes.

Action Galore on Both Ends of the Business Spectrum

Businesses of different sizes require different approaches and mindsets. They also face different sets of challenges that vary by size as well. Thus, businesses at one end of the spectrum (1-10 employees) live in a world very different from the one somewhat larger businesses face (100-499 employees, for example).

The bulk of businesses by number across the entire economy falls at the low end of the size spectrum! According to the U.S. Census Bureau, in 2018 there were 6.1 million employer firms in the United States. Of that number, 99.7% had 500 or fewer employees. That puts 6.08 million of those firms in this general category. Drop the size to 100 employees or less, and the total drops to just under 5.3 million. Small is not just beautiful, it's also how the vast majority of businesses may be characterized.

A March 2021 chart (**Figure 1**) from the U.S. Bureau of Labor Statistics shows that across all private industries it tracks, the majority of firms have 499 or fewer employees. In fact, most firms fall into categories ranging from fewer than 5 employees to 20-49 employees.

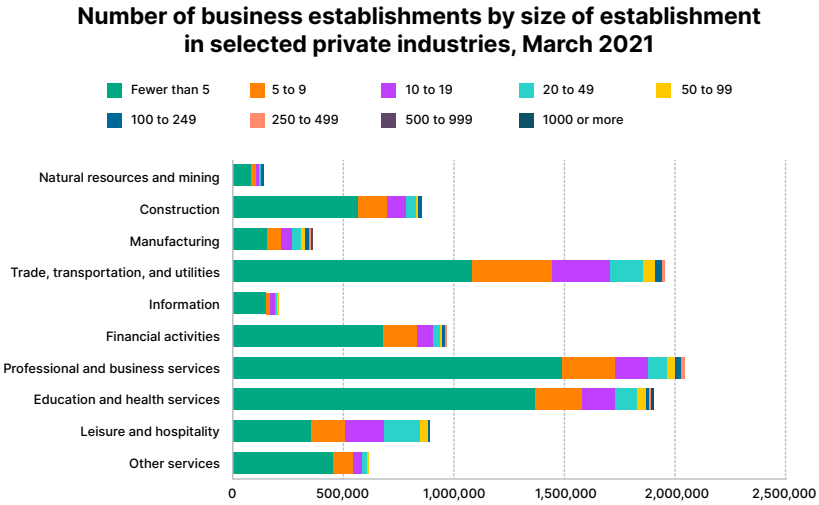


Figure 1: As of March 2021, the vast majority of U.S. companies employ 499 or fewer employees Source: U.S. Bureau of Labor Statistics

Small and midsize companies are laser-focused on the products and services they deliver to their customers. HPE and its partners recognize that different business segments need different kinds of technology solutions—along with associated expertise, assistance, and financing. This means different offerings and approaches based on business size and market focus. The following sections zero in on key segments identified by IDC analysts.

Microbusinesses (Single Employee)

Microbusinesses feature self-employed individuals, and are best understood as "zero employee" firms. Such firms do not yet generate steady income streams, and include start-ups, gig workers, independent contractors, and professional services practitioners. Such businesses generally behave like individual consumers in their research and purchasing. Even so, they have business-grade technology requirements.

Thus, most microbusiness operators have only a consumer-level knowledge of technology benefits and risks. That said, some may have more advanced knowledge based on prior experience at larger companies where they may have overseen IT purchase and deployment as business stakeholders or technology professionals. When such organizations purchase technology, it's either to get their operations going or in response to a specific technology need.

Key challenges for microbusinesses include:

- **Cash-poor:** Only 20% of microbusinesses survive for a year, where shutdowns result from cash shortfalls during early stages of growth.
- **Time-poor:** Microbusinesses must spread their time across all business functions, where the individuals behind the operation do as much themselves as they possibly can.
- **Generalist expertise:** Microbusinesses often don't know what they don't know. This explains why actions and technology use are reactive rather than planned or strategic.

- **Crafting value proposition(s):** Early-stage microbusinesses may be testing value propositions for their products and/or service, making changes to attract new customers along the way.
- **Technology research from free advice:** Microbusinesses invariably get information where they can find it for free, often from sales professionals, service providers, word of mouth, and online.

HPE understands that microbusinesses need simple, straightforward solutions that work out of the box. Pricing needs to be clear and obvious, without added fees lurking in the background. The emphasis must be on business value and bottom-line benefits, because such organizations often can't appreciate technical differentiators or translate them into monetary terms. HPE also understands that timing for technology implementation must be quick enough to prevent lost revenues for microbusinesses, and that it should put them back to work ASAP. In fact, HPE understands that microbusinesses often need business coaching with a focus on business problem solving, and stands ready to work with such customers to make that happen.

Small Businesses (1-99 employees)

According to IDC, small businesses typically accommodate 1-99 full-time equivalent (FTE) employees across all locations. Within this mix, an important subgroup may be characterized as a small office operation, usually comprised of 1-9 employees. Each component of this category, small and larger, has its own technology needs.

Small office operations (SOOs) pop up in every industry, including professional services, retail, hospitality, manufacturing, and technology. According to the SBA Office of Advocacy, 99.9% of all firms in the United States are small businesses. They make up 99.7% of businesses with paid employees and 97.5% of all exporters. In SOOs, 1-9 employees handle day-to-day duties that are usually covered by 3-4 specialist roles in larger organizations.

Bigger small businesses and SOOs generally have flat hierarchies, where employees manage workloads around customer requirements. Typically, there are few if any mid-level managers. Instead, the firms take a team lead approach to train and mentor junior employees and manage workloads.

In small businesses, final technology purchase decisions come from business leaders, not technologists. In fact, only 32.5% of small businesses globally employ one or more full-time IT staff. Such organizations tend to be larger, with 50-99 employees, or are primarily focused on technology. Even then, IT staff in such organizations usually have only generalist IT skillsets, where the persons filling that role are likely junior staffers reporting to a senior manager who makes budget decisions.

Key challenges for small businesses include:

- **Cash-constrained:** As with microbusinesses, matching available cash inflows to outflows can be a significant challenge.
- **Juggling tasks and responsibilities:** The smaller the operation, the more its people must wear multiple hats and constantly switch among them.
- **Better understanding of value propositions:** Small businesses usually include at least one person (often, the owner or operator) who can focus on value for and from the business, and who guides day-to-day activity toward specific goals for revenue and for the delivery of the business's product or service.
- **Technology research still comes primarily from free advice:** As with microbusinesses, small businesses rely on sales professionals, service providers, and other free information sources.

HPE understands that small businesses (from SOOs to those with double-digit headcounts) need short, direct, informative solutions and content that focuses on business value and benefits. HPE also seeks to keep such information free of buzzwords and jargon, so that small

business staff (and managers) can make sense of what the available options can do and how much they cost. Where IT terminology may be essential to explaining a product or service, HPE seeks to provide definitions and examples, so small business readers can relate to that information and use it to their advantage. Above all, HPE and its partners seek to enable small businesses to get on with business, and rely on HPE and partners to arm them with the information and technologies they need to make that happen. Where coaching or guidance can help, HPE and its partners will gladly provide it.

Midsize Businesses (100-999 or 100-499 Employees)

IDC reports that midsize businesses generally support from 100 to 999 FTE employees in the Americas and Japan. For the rest of the world, midsize businesses top out at 499 FTE employees. IDC compares such organizations to teenagers: They need less support than small businesses, but are not yet large enough to gain access to all the resources and capabilities found in larger organizations.

At this point in business growth and development, organizational structures transition from flat to hierarchical. This means that companies get "departmentalized" and that staff roles become more specialized and focused.

Midsize businesses often suffer from accumulated "technical debt." This means that technology already in place might be outdated, or no longer well-suited for increased complexity and technological needs. At this level IT departments grow, with some senior talent in the mix. Job roles in IT start to specialize, but talent remains generalized and less focused than in IT staffs at larger companies. In-demand talent tends to be scarce because larger, better-funded corporations can outbid the midsize ones for limited pools of talent.

Technology purchasing at midsize businesses is often consensus-oriented. Senior staff leads research and selection, working with line-of-business (LOB) leaders to reach consensus. Depending on the size and structure of specific midsize businesses, CIOs may report to CFOs or COOs. This means that for big-ticket items, buy-in or formal approval is likely mandatory. This is especially relevant for end-user technologies such as applications or computing devices. If conflict emerges among stakeholders when choosing best solutions, C-level execs must step in. In such cases, trade-offs among price, functionality, and integration into existing technical architectures typically come first, with future-proofing technology decisions a close second. Organizational conflict can stretch out decision making, increase interdepartmental tension, and dampen user adoption unless strong change management is put in place.

Key challenges for midsize businesses include:

- **Competing priorities for IT and capital budgets:** Different departments have different priorities and goals; strong management and consistent vision are needed to herd all the cats.
- **Growing pains:** Growth often leads to stakeholder misalignment and conflict; new leaders complicate decision making. More time and effort are required to reach consensus.
- **Core processes:** Behavior can become entrenched and cause strong resistance to changes presented by new processes and applications.
- **New technology purchase research:** Such efforts include more active vendor discussions, along with formal and informal advisors. Also, the count of research sources increases to 5 or 6.

HPE understands that information for midsize businesses must remain short and business-oriented, but also provide sufficient product data and details to differentiate its offerings from competitors. The need to explain and define buzzwords and jargon persists because, even though IT teams ingest and interpret product and services information, they

must still share that information with a final decision maker in a high-level business role who may lack technical background and in-depth understanding.

Specialized, Focused Content

Here's the net-net from this market segmentation analysis for very small, small, and midsize businesses: HPE and its partners understand this enormous segment of the business spectrum. They offer specialized, focused content and materials—along with coaching and hand-holding where needed—to make sure that prospective buyers understand business benefits and value, as well as costs and other considerations, when choosing and buying technology to use in their operations, whatever their business size (and growth plans) might encompass.

No matter how small a business might be—be that very small, small, or midsize—it remains responsible for protecting its data and assets, and for meeting data privacy and confidentiality requirements. This puts security squarely in the crosshairs for all businesses, and makes things like data protection, threat intelligence and remediation, and business resilience and continuity essential to business viability. We'll tackle those topics, and more, in Chapter 2.

CHAPTER 2

Cybersecurity Remains Mission Critical

Businesses on the smaller end of the spectrum must struggle to match resources and capabilities to important demands for technology acumen and expertise. Even micro-businesses, with at most one full-timer, remain responsible for securing data, protecting assets, and withstanding cyberthreats and cyberattacks. In this chapter, we'll explore the ins and outs involved in establishing and maintaining security for small to midsize organizations.

The wild and digital world can be scary and challenging, especially for small to midsize businesses. As technologies become increasingly distributed and interconnected, the cyberthreat landscape continues to evolve and gain complexity and danger. Today's threats and vulnerabilities require business operators to take a highly systematic and strategic approach to security. That means they must identify and prioritize protection and defense of their most valued assets. These include their customers, their data, and their sources of revenue, as well as the IT infrastructure and systems that need dedicated, capable cyber defenses.

Security Is Key to Business Success

Given an ever-expanding threat landscape, security has become even more crucial to the effective operation for all business, including even the smallest of operations. Owing to the complex and ever-evolving nature of today's cyberattacks, small to midsize operations must understand what to do and what to watch out for. They must also understand how much proper protection costs, and the kinds of risks that must be prioritized and safeguarded against.

According to Forrester's State of Security Operations 2021, key business challenges include the following across all businesses:

- Security Operations teams struggle to address high alert volumes: less than half of decision makers say their organizations can address most or all the security alerts they receive daily. Teams struggle to triage and investigate threats quickly. Because of alert volume, teams must often ignore low-priority threats that still leave organizations vulnerable to risk so they can concentrate on urgent, high-priority matters.
- Nearly half of firms report difficulties hiring and retaining qualified security staff. Because so much threat detection, investigation, and response occur manually, security teams face high rates of analyst burnout. Teams are starting to automate workflows to alleviate this crunch. Smaller businesses generally face larger challenges finding good people, because bigger businesses can offer better packages (pay, benefits, and so forth).
- Almost 75% of decision makers have started Security Operation Center (SOC) automation—with full automation as a long-term goal. As of April 2021, 70% of organizations surveyed have started down this path. Also, 44% of that survey population expect increased automation in the coming year or two. Those who've adopted automation report more effective and cohesive SOC teams that face a lower likelihood of technical gotchas, including poor visibility into security issues and answers and lack of tool integration.

In general, smaller businesses feel the constraints and impacts related to security matters more keenly than larger ones. Indeed, the smallest of businesses (those with nine employees or fewer) very likely have neither a dedicated security resource, nor much in-house expertise when it comes to dealing with ongoing security issues and concerns. That makes access to security insight, resources, and services something of a must-have to such operations.

Leading Security Threats

Security Magazine reports the five top cybersecurity threats in 2021 as the following (see **Figure 2**):

Phishing: an attack method that presents users with safe-seeming email or social media items that trick them into downloading harmful content. Phishing can look legitimate, and uses apparently safe links,

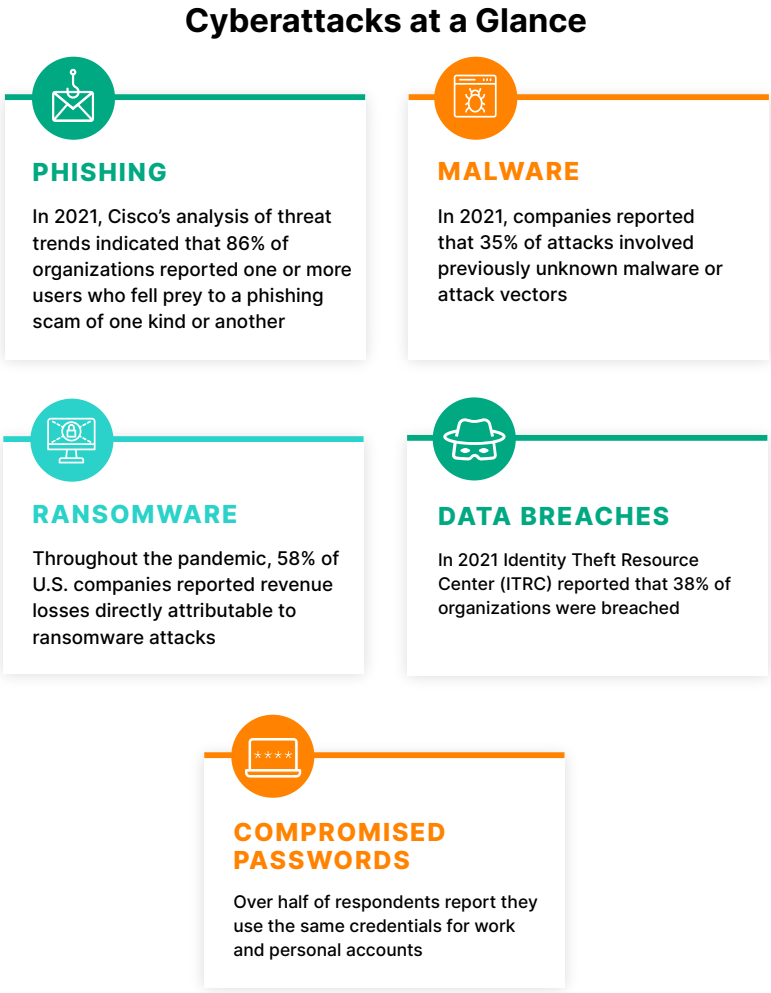


Figure 2: Security Magazine's top 5 cybersecurity threats in 2021

attachments, names, and logos to persuade readers to click embedded links or download files or attachments. Spear phishing targets people who work in specific departments such as Finance, AP/AR, or Purchasing where theft might be possible. Whale phishing targets high-visibility targets (typically C-Level executives whose names and identities are public and known). Smishing uses SMS messages to persuade readers to click malicious links. In 2021, Cisco's analysis of threat trends indicated that 86% of organizations reported one or more users who fell prey to a phishing scam of one kind or another.

Malware: Aka malicious software such as worms, viruses, Trojans, ransomware, adware, and so on, that attack devices to slow them down or stop them from working. Some malware also targets specific kinds of information that it seeks to exfiltrate to a malicious third party, such as accounts and passwords, credit card information, financial accounts, and more. Malware finds its way onto PCs via clicking a malicious link, downloading malicious files or software, clicking pop-up advertising, or opening unsolicited (and unexpected) email attachments. Once it's running on a targeted PC, malware can ransack systems and steal information. In 2021, companies reported that 35% of attacks involved previously unknown malware or attack vectors. That percentage is almost certain to grow as most of the workforce goes remote.

Ransomware: One of the most insidious and visible forms of malware, ransomware encrypts all files on systems it infects. It requires users to pay an often-hefty ransom for a decryption key so they can get their files back. Because not all decryption efforts succeed, the FBI recommends against paying such ransoms, though high-visibility companies like Colonial Pipeline ($3 million of which $2.3 million was later recovered) and a major insurer ($40 million) have found themselves forced to pay to regain access to systems and data. Throughout the pandemic, 58% of U.S. companies reported revenue losses directly attributable to ransomware attacks.

Data breaches: Unwanted and unauthorized disclosure of data, often customer account details and information (such as credit card numbers,

SSNs, names and addresses, contact info, and so on), can occur when cyberattacks succeed, and hackers gain access to company systems and data. Breaches can occur through hacks into company networks or point-of-sale systems. A Q2 2021 analysis from the Identity Theft Resource Center (ITRC) reported that 38% of organizations were breached. If a data breach occurs, businesses must respond immediately to contain its effects and resolve related issues. Failure to act can damage reputations and lead to fines into the millions of dollars.

Compromised passwords: Usually harvested when a user logs into a fake (but real-looking) website, user accounts and information can be accessed when such credentials become known.

In fact, there's a thriving trade in such information, because many users ignore security advice and use the same credentials on multiple (or all) of their online accounts. Over half of respondents report they use the same credentials for work and personal accounts. Companies must therefore teach workers how to create (and preserve) account and password security.

Security Magazine also recommends three general approaches to handling such threats, all of which are eminently sensible and achievable:

Build cybersecurity expertise, internally and externally. For small to midsize operations, working with a freelancer or hiring an outside organization—like HPE and its partners—is a good option. Two advantages of working with an outside company are that they can provide 24/7 monitoring for attacks that can occur anytime, and outside companies can bring in experts who always stay up-to-date on the ever-evolving threat landscape.

Educate your team. Make sure everyone knows what's what and is on the same page. This includes raising general employee security awareness, and training those with security responsibility to work with service providers to recognize and react to threats quickly and directly. HPE and its partners can provide security awareness training and regularly assess employee security awareness with ready access to refresher and

specific remedial training as needed. They can also work with designated members of your staff to handle alerts and fend off potential or actual attacks.

HPE has teamed up with global cybersecurity training champion SANS (an old acronym for System Administration, Audit, Networking and Security, and the name of a leading training provider for three decades) to offer outstanding security awareness training for employees. When used as part of new-hire onboarding, with regular, periodic refresher classes, security awareness helps organizations avoid all kinds of potential security trouble. For more details see HPE/SANS Security Awareness Training.

Create a cybersecurity policy. The basics of a workable security policy should include guidelines on protecting devices, multi-factor authentication, and data protection. This should be a living, constantly updated document that reflects the current state of threats and attacks. Here, again, HPE and its partners can help your organization adopt and maintain such a policy, and make sure it's properly enforced to deliver the protection and peace of mind your organization needs.

Special Challenges for Smaller Businesses

Because they are often cash- and resource-constrained, smaller businesses are particularly subject to security issues and problems. Low staffing levels in general often mean that IT expertise is itself scarce, so that security expertise may either be entirely missing or seriously overstretched. Alas, this too often means that smaller

businesses—particularly those with 100 or fewer employees—will be stuck in reactive mode, mostly unable to anticipate and head off security trouble before it becomes dangerous or poses risks to revenues or outright business viability.

In particular, small and midsize businesses may find themselves saddled with unwanted and unexpected Issues that can present when slow response time to threats or vulnerabilities hamper or restrict their productivity and profitability. When you stop to consider that IBM disclosed the average cost of a data breach in 2021 was a whopping $4.24 million, that could be more cost than many small to midsize businesses could survive intact.

That's why small to midsize businesses should turn to HPE and its partner network to obtain security solutions and expertise. HPE is committed to helping such operations implement affordable and workable security so their businesses can survive—and even thrive—in today's rough-and-tumble digital world. Factoring in the added complications of remote work, and ever more distributed modes of operation and interaction, organizations need the kind of security help, insight, and assistance that HPE and its partners bring to the table.

Beyond the efforts involved in tackling and establishing security, it's equally important to keep up with the ever-changing landscape of security threats and the potential attacks and exposures they can present. Businesses of all sizes, including the smallest among them, must be ready to acquire, digest and proactively anticipate current and zero-day security threats. In Chapter 3, we'll explore what's involved in getting ahead of the security curve through proper prevention, mitigation, and (where necessary) remediation or workarounds.

CHAPTER 3

Staying Ahead of Security Threats

With the understanding that security is a constant and important concern, the only thing that's as important as establishing proper security posture and capability is maintaining those things over time. This means adopting tools and technologies to provide input and insight about current and emerging security issues—known as "threat intelligence"—coupled with an understanding of which of the many potential threats could pose actual risks, and the scale and scope of the risks that are involved.

In fact, when it comes to cybersecurity, the old saying "An ounce of prevention beats a pound of cure" is particularly apt. That's because the costs of a cure—remediating the consequences of a security incident or breach—are high enough nowadays to pose an existential threat to most businesses, especially smaller operations.

That's what makes understanding and anticipating the dangers that security threats and vulnerabilities can pose so important, if not downright essential. Ultimately, it's all about risk management, which means the following:

- As threats and vulnerabilities make themselves known, the first step is to **identify** those that pose actual risks to the business, and to assess their potential impacts and consequences.
- For those items where risk is involved, it's essential to **prioritize** them so that those with the highest costs or most dire consequences are addressed first, and so on, in decreasing order.

- For items with sufficient risk to warrant a response, businesses should set up **risk mitigation and action plans** to address them.

In practice, especially for businesses too small to implement a security team in-house, this means subscribing to a threat intelligence and remediation service of some kind. In fact, HPE and its partners can help with such things, including identification, prioritization, and remediation of risks as part of a comprehensive security service offering.

The Cloud Changes Everything … Including Security

As organizations bring cloud subscriptions and services, new and challenging threat vectors will also come into a business's security picture. This makes it vital to up the security game, and to take steps to improve the organization's security posture and cyber resilience. The following business exercises should be undertaken to help businesses achieve those goals:

- **Align your security strategy with your business priorities:** By understanding the gaps between business and cybersecurity priorities, management and stakeholders can commence aligning both strategies to ensure key priorities are focused, and resources and budgets allocated accordingly. It's important that business leaders reach a state of agreement on the priorities and that risk profiles are understood clearly.
- **Build a security-first culture:** Prioritizing a security-first culture is an important step to thriving in a world rife with uncertainty and risk. Protecting vital assets becomes everyone's business. It's essential to invest in staff awareness training given its prominence as a source of cyber risk, and because a collective effort against cyberthreats will better serve your business.

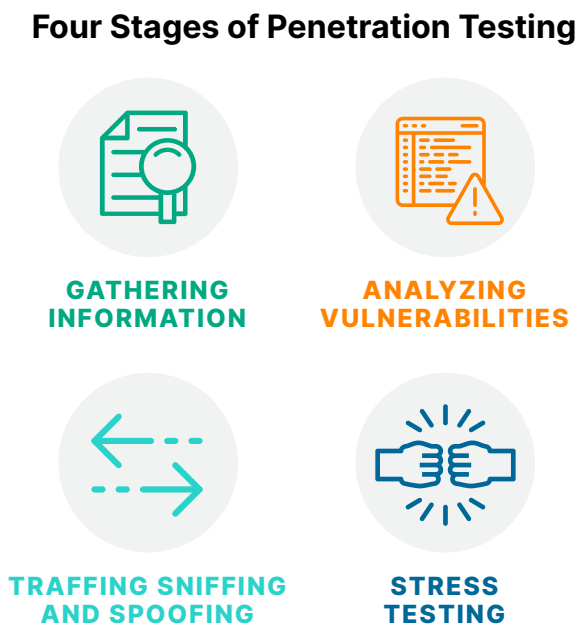


Figure 3: The four stages of penetration testing, also known as pen testing

- **Know your attack surface and fix vulnerabilities before hackers find them:** Cyber vulnerability analysis, also called security testing or pen testing, is a process of testing to assess your organization's security posture (see **Figure 3**). It identifies vulnerabilities before an attacker can exploit them. This process provides insights into the risks that organizational assets face, from external and internal perspectives. It also helps identify potential security gaps prior to formal compliance assessments or audits. To enhance security posture in your organization it's also important to develop actionable mitigation plans. To that end, engaging experienced partners (such as HPE and its partners) can bridge cyber skills gaps in your business and mitigate vulnerabilities.

Disaster recovery: Describes services and systems that permit a business to return to normal operation even in the face of disaster or a total interruption of access and service.

Ransomware: A type of malware that denies businesses access to their systems and data by encrypting everything, so that nothing will function. Crooks claim that paying a ransom will return everything to a pre-attack state, but the FBI recommends against paying ransoms because that isn't always how things turn out.

Virtualized and containerized apps and data: Applications and data that run in virtual machines or containers, often in the cloud, typically as part of a usage- and consumption-based computing model.

Edge to cloud: Refers to computing resources and data that may reside in datacenters or server rooms on-premises at the business core, at the network edge in remote of field locations, or on one or more cloud platforms (e.g. Amazon Web Services, Microsoft Azure, Google Cloud Platform).

Hybrid and multi-cloud scenarios: A hybrid cloud involves integrating local and cloud-based computing resources into a single environment for handling computing tasks. Multi-cloud means the same thing, except it involves two or more cloud platforms. Most modern businesses operate in hybrid multi-cloud environments, and seek to position workloads and data where they make most sense from a cost, security, and performance perspective.

How HPE (and Partners) Can Secure IT

As a quick examination will verify, HPE's cybersecurity solutions are comprehensive, innovative, and robust. Its security capabilities begin at the hardware level and extend all the way to users and systems at the network edge. The overall thrust is to gather and analyze security intelligence to keep up with the threat landscape, to secure systems and services in business use, and to advise (and assist) its customers in managing and minimizing security risks.

HPE Security Starts with Its Servers

HPE is recognized as a purveyor of the world's most secure industry standard servers1. Its ProLiant server family has won numerous awards and accolades, thanks to these specific characteristics:

- **Protect:** Systems avoid hardware- and firmware-level exposure to attack via a silicon root of trust, trusted platform module (TPM) enhancements, multiple levels of tamper-proofing, and added HPE innovations such as "Integrated Lights Out" (iLO) firmware to promote "security-first" capabilities.
- **Detect:** A whole suite of innovations detects and fends off threats during runtime, including boot integrity checks, whereby iLO wipes potentially (or actually) hacked firmware code and replaces it with a known valid copy if possible. If repair proves impossible, systems won't be allowed to boot (provides pre-boot protection against rootkits and other insidious firmware-based attacks).
- **Recover:** Robust capabilities to restore and recover systems back to their last known, good, working states quickly and easily, thanks to tamper-proof, encrypted backups and safe, secure restore mechanisms.

[1] Based on an external firm conducting cybersecurity penetration testing of a range of server products from a range of manufactures, 2020.

Zerto

In 2021, HPE completed acquisition of Zerto, a company that specializes in disaster recovery, ransomware recovery, and multi-cloud mobility solutions. Now part of HPE, Zerto offers continuous data protection and recovery for virtualized and containerized apps and data from edge to cloud. With Zerto, organizations can recover in minutes to a state seconds before an attack, eliminating lengthy and costly disruption and data loss. Zerto brings increased availability with a much lower administrative overhead than legacy data protection solutions. In addition, Zerto's unified, scalable, and automated data management makes workload and data mobility across clouds easy and straightforward. Furthermore, Zerto offers continuous data protection for organizations employing a hybrid-cloud strategy and includes Disaster Recovery as a Service (DRaaS) with a network of over 350 managed service providers. Visit the HPE/Zerto page to learn how your business can avoid data losses and application downtime as close to zero as technology can get.

HPE Security Solutions

HPE's security tools, technologies, and solutions all employ three key approaches throughout their design, development, manufacture, and maintenance. These are best described as follows:

- **Data-centric security:** Security measures seek to protect data first and foremost, particularly data with any kind of sensitivity (personally identifiable information, or PII; accounts and passwords; financial, health, or other legally protected data, and so forth). This ties directly into the next approach, which focuses on who gets access to systems and data, and for what purposes.

- **Zero-trust security:** The National Institute of Standards and Technology (NIST) describes zero trust (ZT) with the epigram: "Never trust; always verify." ZT focuses on data and service protection but should also include all assets (devices, infrastructure elements, applications, plus virtual and cloud resources) and subjects (users, applications, services, and systems). Basically, ZT assumes attackers are always present and active. Thus, it extends no implicit trust to anyone, and always analyzes and evaluates risks to assets and business functions. Verifying identity for all access requests is a key strategy, as is applying the "Principle of Least Privilege" (aka PLP), which means allowing no more privileges than those necessary to subject than they need to do their jobs.

- **DevSecOps:** Simply put, this is an extension of the idea of DevOps, which puts developers (and support personnel such as testers, documenters, and trainers) together with operations staff (administrators, tech support, and field technicians or troubleshooters) into a single organization with shared goals and objectives. DevSecOPs goes one step further and integrates the security team across the entire development lifecycle, so that security is considered during design, construction, testing, maintenance and retirement phases in business IT operations.

Beyond the Solutions: Expert Consulting Help

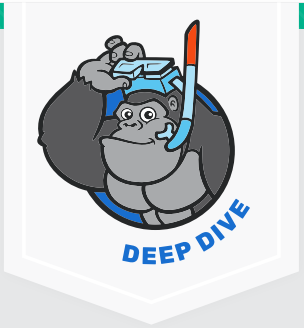
HPE Pointnext Services can help small to midsize businesses audit, define, and refine their security strategies. Pointnext offers expert assistance in formulating security policy, and meeting compliance requirements for privacy, confidentiality, and data protection. They can also help resource- or knowledge-constrained businesses integrate affordable, effective solutions for business continuity and disaster recovery. In fact, Pointnext specializes in helping businesses prepare security blueprints to ground security designs and implementations firmly in reality (and within budgetary constraints). They can also provide end-to-end assistance through test, pilot, and production deployments. Ultimately,

Pointnext can help businesses ensure that security gets embedded across the whole organization: remote workers, at the edge, on-premises, and in hybrid, multi-cloud environments.

HPE and its partners offer a broad range of carefully crafted security solutions to help small to midsize businesses manage risk, protect their systems and data, and cope with today's complex and forbidding security landscape.

Visit the HPE Small and Midsize Business IT Solutions page for all the details. Consider further that HPE and its partners can also offer coaching, consulting, assistance, and services to help smaller businesses stay safe and secure through its Pointnext services organization.

HPE Trusted Supply Chain + Project Aurora



HPE operates its HPE Trusted Supply Chain to serve customers with stringent, higher-than-normal security requirements or usage scenarios. Representative customers from this supply chain include U.S. government and public sector organizations and agencies who must acquire made-in-USA products with verifiable product assurance. Security goes into the HPE Trusted Supply Chain in two important ways. First, such products include hardened security features designed to make them tamper-resistant, if not tamper-proof. Second, HPE supervises the entire supply chain, and approves all parts, observes assembly, and keeps packaged goods secure (and tamper-free) until customers accept delivery.

Project Aurora provides a complete security architecture with new embedded and integrated security solutions starting at the at the silicon level. Learn how Project Aurora is ignited in the supply chain and establishes an immutable chain of trust up through the infrastructure, operating system (OS), software platform, and workloads without requiring signatures, significant performance trade-offs, or lock-in.

Closing the Book: Making IT Workable and Safe

Small to midsize businesses face extraordinary challenges in putting technology to work in their operations. In fact, the smaller that operation, the more challenging it is to identify, obtain, implement, and maintain IT technology to deliver the best possible return on investment.

Establishing and maintaining security is an especially vexing area, because small to midsize businesses are typically under-resourced—both in terms of human and financial capital—to manage the job entirely on their own. That's why HPE (and partners) provide particularly useful, compelling, affordable, and secure solutions for those customers, along with design, consulting, implementation, and day-to-day operations assistance to pull all the necessary pieces together, and keep them working to benefit and secure their buyers and users.

Be safe out there and thanks for reading!

ABOUT HPE

Hewlett Packard
Enterprise

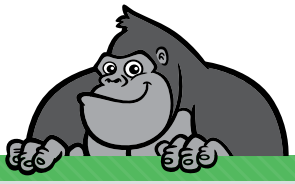
Grow your business with small business IT solutions that power your key ambitions and help you achieve big goals. Explore how HPE small business IT solutions can best serve your small and midsized business needs. www.hpe.com/smallbusiness

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/