ActualTech Media

Hewlett Packard Enterprise

SMB Security Can Be Difficult (and Costly)

Ed Tittel

CONTENTS

IN THIS PAPER

HPE helps small to midsize businesses (SMBs) establish and maintain operational security in the face of ever-increasing and more dangerous threats such as ransomware, phishing, data leakage, hacking, and more.

SMBs need expert help to offset staffing shortages and skills gaps, where slow response times can be costly.This paper explores how HPE helps SMBs to address these issues.

Highlights include:

- Switching from reactive, static security to intelligent, adaptive security
- Closing IT security gaps with coverage at the edge, in the cloud, on-premises
- Defining a security strategy to encompass security, compliance, IT continuity, and disaster recovery
- Building security into the SMB fabric

It's a scary digital world out there. All businesses and organizations face the same formidable and forbidding security threat landscape, including small to midsize businesses (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 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.

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.

Thus, 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.

In fact, even a slow response time 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.

The Ever-Spreading SMB Boundary

Once upon a time, SMBs could focus on their organizational boundaries. Securing such boundaries took care of most of their security concerns and addressed most risks. Today, data and apps are everywhere, making everything harder to track and secure. Under pandemic rules, workers are mostly remote, which means that each and every use of each and every device needs protection. With the Internet a vital link in tying users to applications and services, secure communications are more important than ever before. Ditto for secure storage and servers, both on-premises and in one or more clouds (mostly more, nowadays). In short, security and protection get interesting in a hurry when an organization's assets, apps, and people operate from anywhere, anytime, all the time.

HPE Security Solutions

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

- Data-centric security: Uses proven, NIST-standardized methods to protect data in use, at rest, and in motion (which meet U.S. Government and European Union GDPR requirements). It provides strong encryption and tokenization to render stolen data useless to attackers.
- Zero-trust security: Is a philosophical approach to identity and access management, whereby no user or software action is trusted by default. Thus, all users, devices and application instances must prove their identities and authorizations conclusively before access is allowed.
- DevSecOps: Embeds security teams and concepts in a formal development process, designed to ensure security is addressed early and often along the entire app delivery chain (design-build-test-deliver-maintain), not simply bolted onto a "finished" system or service at the end of development. Security is addressed during development and deployment through a set of DevSecOps best practices (**Figure 1**).

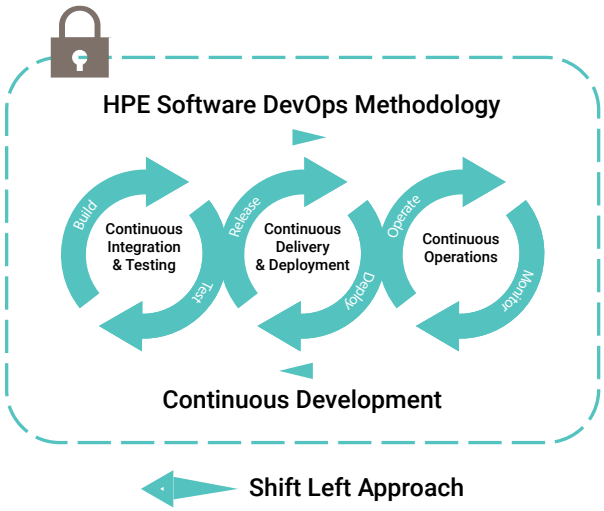

Figure 1: DevSecOps expands on the underlying concepts of DevOps to build the mindset that everyone is responsible for Security

HPE Trusted Supply Chain Initiative

To meet the needs of customers with high security requirements and challenging usage scenarios, HPE operates a Trusted Supply Chain. Such customers include U.S. federal and public sector consumers who prefer U.S.-sourced products with verifiable cyber assurance. Security is baked into the supply chain, by including additional hardened security features and assigning HPE employees to oversee products during the manufacturing process to vet all parts, observe assembly, and make sure packaged devices remain tamper-free until customers accept delivery. HPE includes an exclusive silicon root of trust that embeds silicon-based security into industry-standard servers, and maintains security controls across its entire supply chain to establish and maintain stringent security at the hardware level.

HPE even addresses security in its own product development and delivery, using a formally documented, frequently audited secure supply chain (see: **"HPE Trusted Supply Chain Initiative"**).

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

Baked-in Security at the Edge

All in all, HPE works with SMBs to embed security across the entire organization. This means their 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.

> HPE works with SMBs to embed security across the entire organization.

Visit HPE's Security and Digital Protection Services page to check out security blueprints, the HPE security portfolio, case studies, and more.