ActualTech Media

Hewlett Packard Enterprise

New Security Challenges for SMBs

Ed Tittel

CONTENTS

IN THIS PAPER

These days small to midsize businesses (SMBs) must protect users and devices, wherever they may be. But 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.

Work from home (WFH) and remote working scenarios are forcing profound changes to the small to mid-size business (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.

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.

> Ultimately, making remote work connections safe means securing not just end-user devices, but also securing the networks that make remote access possible.

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,

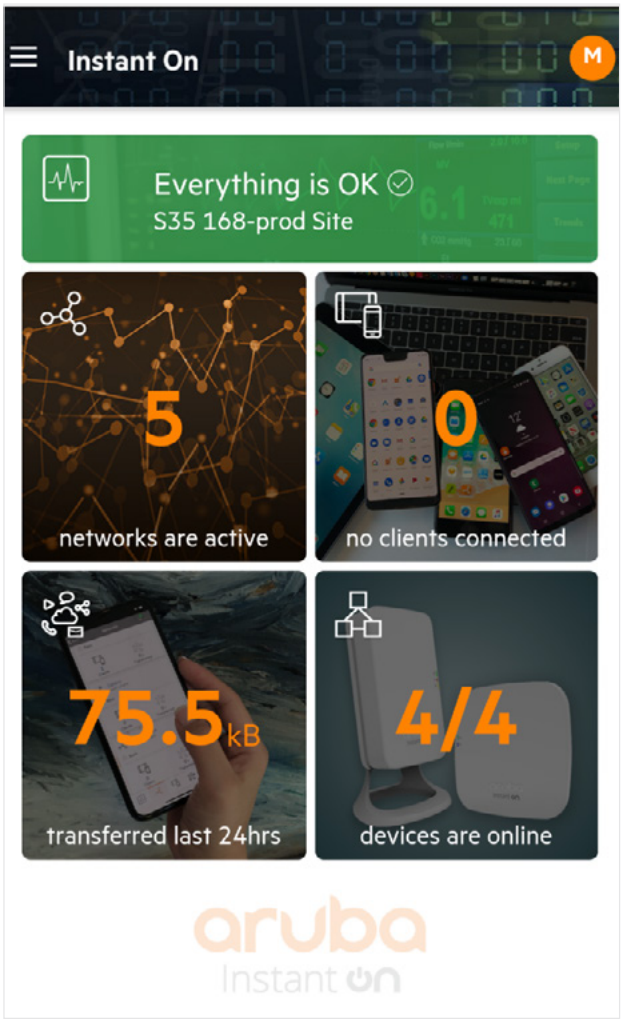

Figure 1: Aruba Instant On allows small businesses to create, modify, and monitor network components from a central location

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 1**). The app offers excellent visibility into access and usage, and can block unsolicited applications or access to disallowed websites quickly and easily (see **Figure 2**). Access controls also include MAC address filtering capabilities that can blacklist specific devices, or simply block all devices not whitelisted for network access and use. In addition, the app offers predefined access control lists (ACLs) to ward off malicious network traffic.

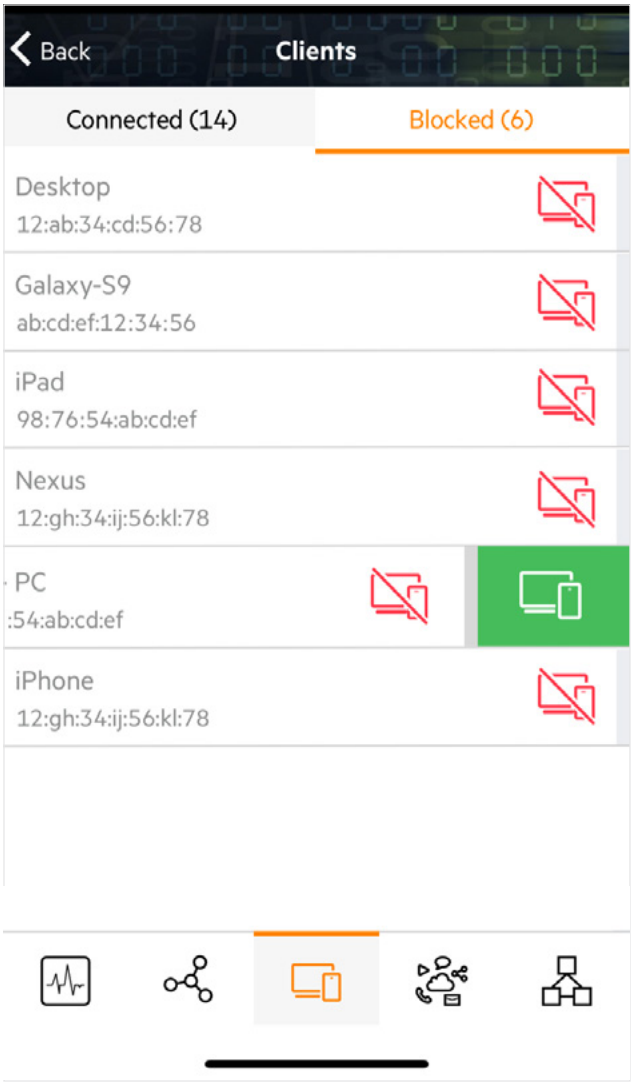

Figure 2: Get visibility into all connected devices and the ability to block specific, unwanted clients from accessing the network

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

- Strong authentication with advanced version 3 W-Fi Protected Access (WPA3) support means that authorized users are carefully vetted before they're allowed on the network, and its login controls are more secure and harder to crack.
- 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.

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.

> Aruba Instant On offers small businesses the ability to implement and operate wireless and wired local networks on their premises, quickly and easily.

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 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.

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.

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

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 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.

Get started today. Check out Aruba's Instant On wired and wireless portfolio, learn more about HPE WFH productivity options, or visit HPE File Backup Storage Solutions for Business page.