aruba
a Hewlett Packard Enterprise company

AT A GLANCE

TOP 6 NETWORK SECURITY TIPS FOR MIDSIZED BUSINESSES

Making sure your business is protected from cyber attacks is critical. But how? Follow these tried and tested tips to help ensure your company and your network are safe.

TIP #1. GIVE USERS THE RIGHT ACCESS

Because users roam and IoT devices are being used everywhere, Wi-Fi software with role-based access control is the way to go. It lets you minimize the number of SSIDs being used, while still letting you differentiate access per user or device type, whether it's a guest, a printer or even the Apple TV someone brought in to work.

TIP #2. BUILD APPLICATION-FRIENDLY POLICIES

Apply extra security based on location, application being used and/or traffic type. Automated policy enforcement makes it easy. Now you don't have to worry about guest traffic interfering with an employee's business-critical apps, regardless of location or time of day.

TIP #3. USE THE LATEST WI-FI SECURITY STANDARDS

Protect yourself from unnecessary risk by ensuring the wireless equipment you choose is certified to support WPA3 with Enhanced Open with Opportunistic Wireless Encryption (OWE).

TIP #4. CHOOSE WI-FI ACCESS POINTS WITH BUILT-IN INTRUSION PROTECTION

The fear of intruders and attacks on your network can keep IT up at night. Your network should have built-in threat protection that will identify and contain unauthorized devices and other security risks, and alert IT to any critical issues

TIP #5. MANAGE WEB ACCESS WITH BUILT-IN CONTENT FILTERING

Preventing users from accessing malicious content is difficult, and keeping up with the ever-expanding list of unsafe Internet sites is virtually impossible. A good way to keep your network safe is to choose a Wi-Fi solution that includes built-in web content filtering capabilities that allows you to restrict access from unauthorized sites and types of content.

TIP #6. SELECT A VENDOR WHERE SECURITY IS TOP OF MIND

While its imperative to ensure that your network has built-in role-based access control and policy enforcement, don't stop there. Choose a network vendor capable of providing a broad set of industry-validated security solutions that integrate easily with the core network architecture and can be added on as your security needs grow. Advanced solutions should offer complete visibility to devices on your network, and automated policy enforcement based on combination of variables such as user, device type, location, and applications being used.

ARUBA EDGE SERVICES PLATFORM (ARUBA ESP)
Zero Trust Security from the Start

aruba
a Hewlett Packard Enterprise company

AAG_Top6NetworkSecurityTipsForMidsizedBusinesses_RVK_040721

Contact Us Share