Revamp Your Wireless Network

with These 3 Things

VECTORUSA

The days when employees worked on just one device in just one location are far behind us. In fact, the average employee uses at least two devices for work purposes, often moving from room to room or even location to location in one business day. This mobility requires smooth connectivity to critical business systems and their coworkers.

The technology that enables this productivity, enterprise wireless networking, often goes unnoticed—at least until it is underperforming.

In a time when more and more business is being conducted on the move and security threats are constantly evolving, here's how your organization can revamp its wireless network for the challenges of tomorrow.

> The average employee uses at least two devices for work purposes.

The Role of a Modern Wireless Network

In a word, the goal of implementing a wireless network is *productivity*.

Whether your wireless network is enabling employees to access resources as they move from meeting to meeting or put the finishing touches on that presentation at lunch, or it's helping a visiting customer in the office, everyone needs a secure, fast, and reliable connection.

At the same time, security professionals entrusted with protecting enterprise assets need access to the latest technologies, tools, and security controls to mitigate and prevent cyberattacks and even nonmalicious activity.

Enabling and achieving this balance requires organizations to have modern wireless technology in place. So whether your organization is just building out its wireless network or you're in the process of taking it to the next level, here are some key milestones.

> In a word, the goal of implementing a wireless network is *productivity*.

1

Enable Basic Network Access Protection

At the most basic level, organizations need to protect access to their wireless network in order to prevent unauthorized access to other enterprise systems.

To enable this, organizations should ensure that:

- ☑ They are using wireless network infrastructure to handle 802.1x and WPA3 authentication, allowing for scalable and secure access to wireless local area networks (WLANs)
- ☑ A strong foundation is in place that ensures wireless network device placement and the models used are based on site surveys that incorporate bandwidth and connectivity needs
- ☑ Security and device policies exist to define standards on how users contribute to protecting network and organizational assets

2
Increase Security Without Sacrificing Productivity

As wireless network maturity increases, **organizations can continue to balance security with productivity by:**

- ☑ Incorporating network access control (NAC) to provide administrative visibility into connected devices, handle device authentication, and to define and enforce security policies
- ☑ Implement firewalls to segment wireless networks from wired networks and/or maintain access control based on device, user, or level of trust

> Organizations can continue to balance security with productivity.

3

Add Additional Security Controls

As organizations grow in size, sophistication, and need—especially with the expansion of bring-your-own-device (BYOD) policies—**wireless network maturity can evolve by:**

- ☑ Implementing additional security controls that help to centralize device management, such as mobile device management
- ☑ Incorporating WLAN controllers, which centralize wireless network access point management, provide redundancy, and assist with enterprise-wide patching and device authentication (i.e., to prevent rogue access points)
- ☑ Initiating and consolidating logging of network activity, especially in coordination with other security and enterprise devices like firewalls and active directory

VECTORUSA

Take the Next Step

There is no one-size-fits-all solution when it comes to revamping and securing enterprise wireless networks. However, there is one truth that all organizations must face: It's a matter of *when* and not *if* they will be confronted with a security incident.

Fortunately, with the right tools, planning, and partners, organizations at each stage of the wireless network maturity curve can take the necessary steps to enable their business while also keeping their employees, customers, and data safe.

Ready to get your own customized consultation to create a plan for revamping your wireless network or enhancing your current design?

Let's Get Started