

# Are you prepared for the next cyberattack?

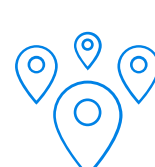
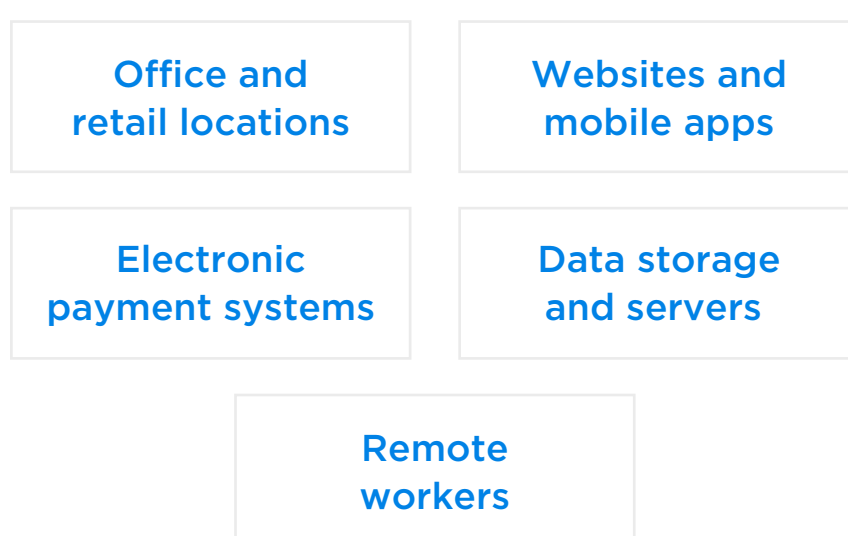
## 4 key steps to fortify your security

Today's retailers face common technology concerns: network security and business disruption. These threats can have a negative impact on everything from the customer experience to your stock price. It typically takes nine months to identify and resolve a data breach and costs \$9.4M, on average.<sup>1</sup> Furthermore, cyberattacks are on the rise — nearly 2/3 of organizations have experienced major security incidents that jeopardized business operations.<sup>2</sup>

### Help keep your organization secure

## 1 Identify which network access points need to be protected

Consider all network endpoints across your enterprise, including:



## 2 Set your goals

Determine your organization and security objectives and then examine all network access points — and where there may be security gaps. Goals could include:

- Strengthening IT security in stores and online.
- Helping to mitigate / prevent fraud.
- Protecting sensitive data and customer privacy, especially data in motion.
- Managing IT complexity / simplifying complex WAN.
- Lowering costs and driving network efficiency.
- Ensuring compliance for card transactions and software-based payments.
- Supporting a mix of private and public network connectivity.
- Deploying a multi-cloud strategy.



## 3 Assess your current capabilities

Ask the tough questions to identify the areas of greatest need. Here are aspects to think about:

### Do you have the right network security? Consider this:

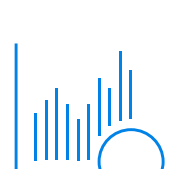
- Cybercriminals are adept at finding the weakest point in your security.
- Know what's at stake. Explore an Intrusion Prevention System (IPS) to monitor for malicious activity.

### Do your employees practice safe surfing?

- Cyberattacks are getting more sophisticated and deceptive.
- Remote and hybrid workers have added more devices (including BYOD) to company networks and from more disparate locations.

### Do you have the staff and resources to manage security on top of other IT needs?

- Cyberattacks require immediate response — can your internal teams “drop everything else” to take action?
- Do they have the bandwidth to keep security up to date?
- Will strategic technology initiatives get deprioritized?



## 4 Consult with a managed security solutions expert.

The right partner can offer a range of valuable services, including:

- ✓ Tailoring, installing and managing security solutions.
- ✓ Implementing new firewalls or layering cloud-based solutions on top of legacy firewalls.
- ✓ Integrating disparate solutions into a single, easy-to-manage portal.
- ✓ Connecting remote users and locations.
- ✓ Maintaining the latest security updates.
- ✓ Serving as an extension of your internal IT staff.



Discover how Spectrum Enterprise solutions can help secure your retail organization.

[Learn more](#)

#### Sources

1. “Cost of a data breach 2022: A million dollar race to detect and respond.” IBM, July 2022.
2. “Security Outcomes Report, Volume 3.” Cisco, January 2023.

