

Securing the Midmarket: The Challenges, Threats and How to Overcome Them

Understaffed and Under Attack

When it comes to protecting your midmarket organization, you know you're in for an uphill battle. Skilled security staff is hard to find and even harder to retain. Mergers, acquisitions, even changes in management have created disparate systems that don't communicate and are incredibly challenging to manage.

With the increased number of attacks, and those specifically targeting midmarket organizations, good enough security won't cut it anymore. You need solutions that can protect against ever-changing threats, but don't add to your day-to-day complexity. In this guide, we review the top challenges facing midmarket organizations and the tools you need to conquer them.

Lack of Skilled Security Staff

According to a 2018 ESG report, 53% of midmarket organizations express a problematic shortage of cyber security skills in 2019. Unfortunately, this skills gap is only expected to get worse with unfilled cyber security jobs reaching 1.8 million by 2020.¹ If you're unable to hire the people you need to protect your business, there can be serious implications and impacts to the rest of your IT organization.

- 1. Increase in existing staff workload** – It's very common for resource-constrained midmarket organizations to assign security tasks to other members of their IT teams. This may work as a temporary solution but can have long-term impact on employee satisfaction and turnover.
- 2. Inability of cyber security staff to learn or fully utilize security technologies** – It's a bad use of staff time and your money to deploy cutting-edge cyber security solutions if your employees aren't able to learn the technology or take full advantage of its capabilities.
- 3. Recruit junior personnel instead of hiring experienced pros** – When you can't find the experienced staff you need, that next logical step is to recruit less-qualified personnel and spend the time and money to train them. This plan can work out well, assuming you don't invest the time to get them up to speed just to have them leave for greener pastures.

What can you do about it?

Since the skills gap isn't expected to go away anytime soon, here are few options you can consider to help with your limited resources:


- Work with a technology vendor or reseller that offers technical training to your team. They should know better than anyone how their products should work, so take advantage of that and any free training they have to offer.
- Considering working with a managed security services provider to augment your internal staff? You're not alone. Over 46% of midmarket organizations worked with an MSSP in 2018. This is a great option to keep your IT team focused on what they need to do, without leaving your business open to attack.

Growing Pains

For IT teams, your day-to-day can be rotating items on your to-do list – yesterday's critical project moving down the list to make room for today's crisis. And while business decisions like mergers, acquisitions and expansions don't require your seal of approval, they certainly increase the workload for your team.

As your business grows, your technology infrastructure will certainly need to evolve. But if you're unable to add the new technologies your business needs due to limited resources, you could create new issues.

¹ <https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#749051af1c30>

- 
1. **Dependence on manual processes** – 28% of surveyed midmarket organizations said they struggle with a dependence on manual or information processes for cyber security. This can complicate your security operations and doesn't scale.
 2. **Disconnected point tools** – All technologies must be tested, piloted, configured and operated on an ongoing basis. But with limited resources, your team may struggle to keep up with disconnected tools that have different deployment processes, management interfaces and reporting tools.

What can you do about it?

You need to make sure that the solutions you implement are scalable and work together to keep you secure. Look for security solutions that can integrate and share data to give you a holistic view of your organization. You should also consider integrations that simplify ticketing, case management and process workflow. Additionally, evaluate solutions that can offer automation capabilities, including generating remediation rules, gathering data for investigations and applying security patches regularly.

"Good Enough" Security

Many midmarket organizations don't see themselves as large enough or important enough to be a target for hackers. By operating under the assumption that they can fly under the radar, they may be remiss in deploying the necessary security solutions or provide the appropriate security training necessary to keep their businesses secure.

1. **Lacking security deployments** – If you don't think you're a target, it's easy to see why you wouldn't be concerned with having robust, layered security defenses in place. But you know your business is under attack – and it's hitting you at every angle.
2. **Limited security training and education** – One of the easiest ways for hackers to gain access to your business is through your employees. It's important to ensure that your employees know how to spot these attacks and how to follow up with you to report it.

What can you do about it?

You have to take the steps to make sure your executive team understands the risk your up against and the uphill battle you're facing. Take advantage of security research tools like the WatchGuard Quarterly Internet Security Report or The 443 Podcast to stay up to date on the latest in threat trends and attacks. Furthermore, look for solutions offering layered security defenses to protect against multiple types of attacks at multiple attack vectors. Some of these solutions even offer refresher phishing education in the moment to help users learn from these attacks so they don't happen again.

Are you ready to protect your midmarket organization?

Maybe it's time to take a look at WatchGuard. We understand the challenges you face, because they're the same ones we do. WatchGuard is a global security organization with over 700 employees and 16 offices around the world. We've completed multiple acquisitions through the past years and have over 100 remote employees globally.

At WatchGuard, we know that you need solutions that are easy to deploy and even easier to manage. We know that you expect your vendors to offer top-of-the-line support and training so you can get (and keep) running efficiently. We know that you expect your security to work and to keep you protected from the attacks of today and the threats of tomorrow.

We build security and simplicity into every product we develop – and that's why we use them ourselves! From Network Security to Multi-Factor Authentication to Secure Wi-Fi, we have solutions designed to meet your specific business needs.

Not sure you want to take this on in-house? Work with one of WatchGuard's MSSP partners and take the stress of managing your security off your to-do list.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit [WatchGuard.com](https://www.watchguard.com).