eBook

The Big Book of Layered Security

N-ABLE™

The Big Book of Layered Security

Your business leaders sit at the dinner table. They're scrolling through the news, and they see a story on high-profile cyberattacks aimed at organizations in their industry. They get worried and ask what you're doing to help them.

In times like these you can shine as a guardian of the business. The key to protecting them lies in having several defensive security layers. Especially with the current threat landscape, it's imperative to have strong defenses at multiple levels to help prevent increasingly sophisticated attacks.

All too often, businesses skimp on their cybersecurity budgets. However, if something bad happens, they expect the IT department to shoulder the burden of bringing them back up and running (and often look in their direction when placing blame).

So what's an IT team to do?

In this eBook, we'll talk about:

- What you're up against in the current threat landscape
- How to demonstrate the need for protection at multiple layers
- What tools you need in your arsenal (at three levels)
- How to approach these conversations with leadership

What You're Up Against

No one ever said security was easy. But departments potentially face greater challenges than other organizations. Your department often has smaller budgets and may not want to spend on security. A knowledge barrier can exist as well—some companies may understand the importance of cybersecurity, but not truly understand the depth of the risk or the technologies and steps required to remain secure. Beyond that, with a roster full of priorities, you can't always devote the time and attention to your security postures that a larger enterprise could.

Yet SMBs often fall victim and really need the help. In 2019, Verizon found that 41% of cyberattack victims were SMBs.[1] This number may be conservative: large companies can detect and report attacks, while SMBs may lack the resources to even know, for a long time, that they've been compromised. According to the 2020 "Cost of a Data Breach Report" by Ponemon Institute, it takes an average of 207 days to even identify a breach and 280 days to identify and contain it fully.[2]

1. "VDBIR: Summary of Findings," Verizon. enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/ (Accessed December 2020).
2. 2020 "Cost of a Data Breach Report," Ponemon and IBM. ibm.com/security/data-breach (Accessed December 2020).

Attackers are growing more sophisticated. Worse, they often share sophisticated tools with less technically skilled criminals, who can use them in their own attacks. This makes for an extremely dangerous threat landscape.

This is a pretty broad overview, but here are some recent developments:

- **Ransomware:** Ransomware has long been a major problem. While traditional ransomware encrypts data on a victim's device or server and demands payment to unlock the data, attackers have started breaching the data as well. For example, with Maze ransomware, the attackers breached the data and then threatened to publish it if the organization didn't pay the ransom. Companies might assume that paying the ransom will be less punishing than paying a compliance fine and taking a reputational hit. This puts more pressure on organizations to respond. If you get breached, please report it. Don't try to sweep it under the rug; transparency is the best policy after a breach.
- **Attack vectors:** Email remains a top attack vector. However, we've seen a major uptick in other channels, namely remote desktop protocol (RDP) attacks. A hacker can scan for open ports and tunnel in via RDP without the end user interaction required of a phishing campaign. The shift in 2020 to remote work likely exacerbated this problem, with many organizations working remotely for the first time. Notably, some dedicated remote support tools do not use RDP and offer multiple security features like session timeouts, advanced key agreement schemes, and strong encryption.
- **Fileless attacks:** We've seen a major uptick in fileless attacks that run in system memory and don't drop a file on a system like malware traditionally does. This makes it hard for antivirus (AV) products to catch since there isn't a file to scan or quarantine. A fileless attack may leverage admin tools that are preapproved by most systems like PsExec or PowerShell® to gain persistence or cause damage. For example, someone may use a fileless attack to create a new user with admin privileges on a computer, then use that foothold to perform reconnaissance against the network. Fileless malware can be hard to detect, so you'll often have to go beyond AV to defend against it.
- **Attacks on IT managers:** Over the past couple of years, cybercriminals have increasingly turned their sights on IT managers and executives. You have the keys to the kingdom for multiple businesses; if they compromise you once, they can compromise several systems. Therefore, working on your own internal security is extremely important. You may even want to hire a managed security services provider (MSSP) to watch over your systems. We'll talk more about MSSPs later in this eBook.

While this is a very high-level overview, the bottom line is this—security has become more complicated, and what was once acceptable protection now falls short. IT professionals need to persuade their businesses to take on more defenses to remain safe in the current environment.

For the rest of the eBook, we'll consider how to think about these new levels of protection and give information to help demonstrate the return on security investments.

Layers of Protection

You may be aware of some frameworks for understanding and analyzing cyberattacks like the Lockheed Martin® Cyberkill Chain and the Mitre Att&ck framework. These models help teams understand an attack, break it down into stages, and understand the tactics used by cybercriminals.

While these models can help you understand an attack, they also point out an important truth—attacks often occur in multiple stages. This gives you multiple chances to stop them.

For the purposes of this eBook, we'll use a layer-based model to show how you can stop attacks. The layers are as follows:

- **Device**
- **Application**
- **People**
- **Network**
- **Internet**

Each of those layers works to prevent or detect threats. It's also important to have a recoverability layer via backup and data protection solutions. We'll cover this more later.

When you implement technology at each layer, you help protect data, which lies at the center of the model. While there are exceptions, most cybercriminals attack companies to get data. They may want to destroy the data, encrypt it and hold it for ransomware, or steal it and resell it on the dark web. Regardless of the end goal, data is usually the jewel they're after.

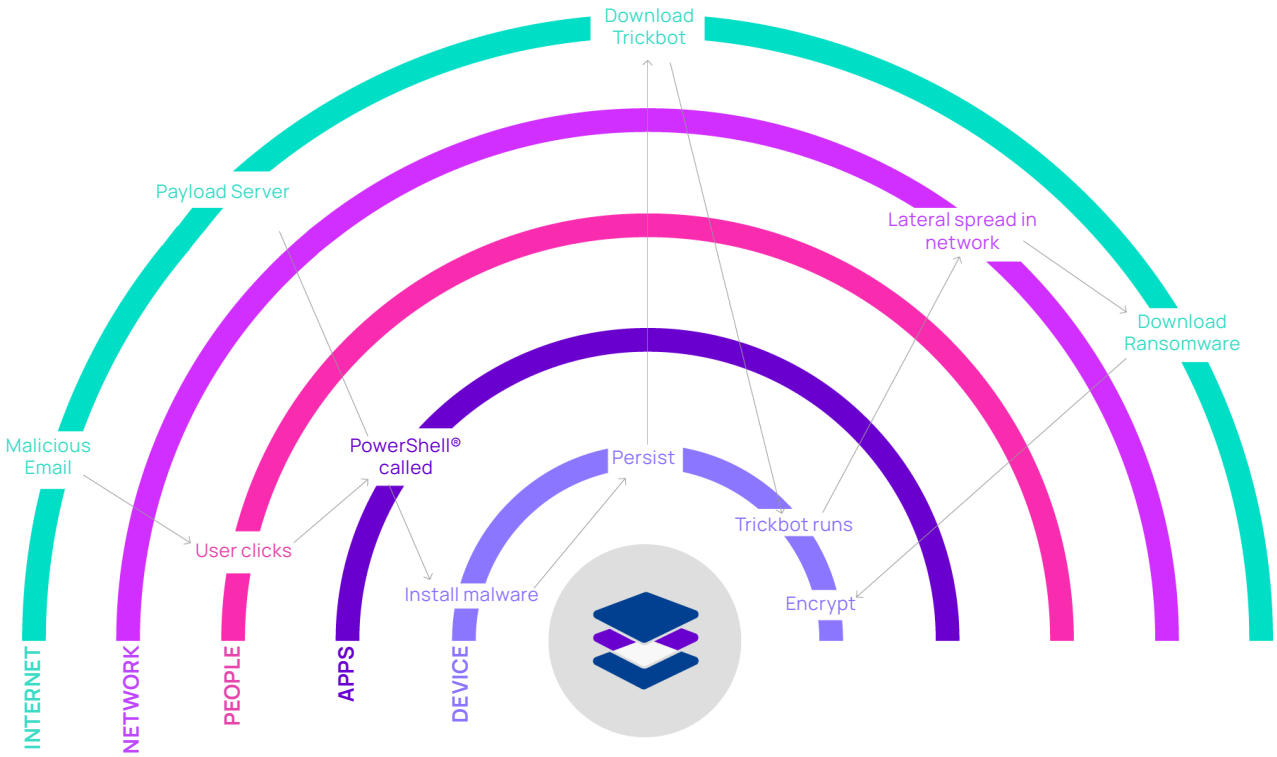
As a result, we recommend trying to stop the attack as far away from the data as possible. For example, preventing a potential ransomware attack from even entering the network by blocking a malicious email will help more than catching it at the device level, when it's already in the middle of encrypting files.

Example: Ryuk Ransomware

An example such as Ryuk ransomware may help illustrate this better. Ryuk is a fairly sophisticated ransomware attack that usually crosses each layer of the model. Some reports from SonicWall® have claimed that up to a third of reported ransomware incidents were due to this pernicious threat.[3]

Different attacks using Ryuk may have slightly different steps, but this is one of the documented attack chains from the past year.

3. "Ryuk Ransomware Responsible for One Third of All Ransomware Attacks in 2020," Security Magazine. securitymagazine.com/articles/93769-ryuk-ransomware-responsible-for-one-third-of-all-ransomware-attacks-in-2020 (accessed December 2020).



Here's how the attack could play out:

- **Internet:** An email comes in as the initial attack vector, with a malicious attachment or a link to a malicious document.
- **People:** A user opens the attachment, likely because they don't recognize a malicious email or the message is particularly convincing. Even trained users can sometimes fall victim to a well-crafted malicious email. The message states they must enable macros to see the content, so they comply. This triggers a script in the document.
- **Apps:** The malicious script calls PowerShell on the user's machine. Because PowerShell is a trusted tool on devices, this doesn't raise red flags and isn't detected by traditional endpoint protection solutions.
- **Internet:** PowerShell reaches out to the command and control server to grab the malicious payload and return it to the machine. If safeguards aren't in place that know to look for calls to the payload server, this will go undetected.
- **Device:** Emotet, a banking trojan, gets installed as the first stage. Emotet uses evasion techniques designed to make detection by AV products extremely difficult. It also reports back where it's installed, so the threat actors can decide what actions to take next.
- **Device:** Once Emotet is installed, it gains persistence on the machine. By persistence, we mean it sits on the device and can be activated even if it is turned off. In some cases, attackers gain persistence and can sit on networks or devices for months, gaining information on intended victims if they're aiming for a targeted attack.
- **Internet:** From here, the machine reaches out to a server to download Trickbot, another type of malware. Trickbot started as a banking trojan but has recently been used for lateral movement. In fact, Trickbot has evolved to spread through an environment and find saved passwords and authentication to report back to the attackers for future attacks.

- **Network:** Trickbot spreads laterally across the network, looking for other devices to compromise. At this point, the entire network is at risk. Trickbot reports back to the threat actors, and now they have a decision to make. Do they continue exploring the network to gain access to data, or do they simply deploy ransomware to make some quick money? In this example, they decide to ransom the victim.
- **Internet:** Next, Trickbot reaches out to a server to download Ryuk ransomware to machines.
- **Device:** Once on the machine, Ryuk finally begins encrypting data. It typically also tries to kill local AV processes and block and remove backups. At this point, it's attempting to remove your defenses. With all the extra damage, it will leave you in the lurch when you try to recover unless you have off-site backup copies. This makes it very likely you'll have to pay the ransom.

One question you may have here—why go through all these steps? In particular, why would a cybercriminal use multiple pieces of malware? Well, for starters, each malware variant offers different "features" in the same way a product might. In this example, Emotet gains persistence on a machine, while Trickbot finds other endpoints in a network. But perhaps more important, having multiple malware infections in a given attack can make it harder to detect and remediate by dividing labor, increasing the likelihood of a payout. Cleanup becomes harder as well. You may remove one infection from the device while not realizing the attacker left another piece of malware on the system, giving them another way to get in.

While Ryuk doesn't always operate in the same manner, this example demonstrates how complex an attack can grow. But it should also offer some hope. If you have your security layers set up appropriately, you have multiple chances to prevent the final damage—from blocking the initial email to shutting down any of the malware samples to recovering from an off-site, cloud-based backup (if all else fails).

Protection at Each Layer

With attacks like Ryuk out there, SMBs and IT professionals need to increase their protection to include multiple layers. In this section, we'll cover what to do at each layer.

We've broken our suggestions into three levels of protection:

- **Core:** These are table stakes. You need these in place. If you don't have them, work on these first.
- **Advanced:** Address these after you've built the core foundations. In many cases, these are optional but highly recommended. Be aware that these technologies are rapidly approaching the point at which they will be the norm. You can be ahead of the game.
- **Comprehensive:** These techniques and tools are built for super-advanced groups that use specialized security tools and functions like 24/7 network security monitoring. Setting up a security operations center (SOC) is cost-prohibitive for many IT departments. Plus, most SMBs won't need them unless they're in a regulated industry or are very security conscious. We do recommend partnering with an MSSP who may already have the firepower to handle most of this.

The following section will cover core and advanced offerings. Comprehensive coverage will have in its own section.

Device

Core

Start with a good AV solution. Traditionally, AV solutions used virus signatures to catch malicious files. But this is less than ideal. You have to wait for a virus to be discovered, then wait for a signature to be created for it, then you'd have to update your virus definitions before the AV solution can catch it. This leaves a gap in protection. Additionally, many modern viruses shift their behavior, so it's hard to develop a signature for them (these are called polymorphic viruses). Because of this, modern AV solutions usually offer heuristic scans that run files in a sandbox and flag them if they behave similarly to viruses (say, creating new user accounts or changing the registry). Additionally, your solution should include some behavioral monitoring, which also looks for odd behavior from files but does so in real time. Any AV solution worth its salt needs to have all three at a minimum to help prevent malware.

Additionally, set up rules in your monitoring tool to look for any services disabled in bulk. Often, malware attempts to shut down detection and recovery mechanisms so you can't stop the malware or recover once you do. It's like disabling the home alarm before breaking into a house—if you see services across your network being disabled, take a close look and try to respond accordingly.

Advanced

At the advanced level, we have endpoint detection and response (EDR) tools. These tools can overcome many of the limitations of AV solutions, and are particularly important during an era of fileless malware. Instead of only inspecting files, EDR looks for anomalies on an endpoint that could be malicious, then helps the team stop them. It uses AI and machine learning on endpoints and can often do a lot more than traditional AV solutions. Since it doesn't require a file to scan, it can catch more than malware (although it does catch that as well) like RDP-based attacks or scripts run from Microsoft 365™ documents. Some solutions can even automatically roll back endpoints to safe states after a ransomware incident.

One important note—AV and EDR solutions often compete for resources on an endpoint. They aren't built synergistically—you really want to choose one or the other for a given endpoint. If you have resistant team members, you can at least prove the value by deploying EDR to the highest-risk employees while sticking with AV for the rest of the users.

Next, start working on endpoint vulnerability management. A good vulnerability scanner can pick up at-risk devices on a network—perhaps some you may be unaware of. Scanners often look for out-of-date software but can search for other vulnerabilities like misconfigurations, default passwords, buffer overflows, OS flaws, or open services and ports. They can also help you make sure appliances and firmware are up to date, which can be a common blind spot in a network. While this is labelled advanced, most scanners are very accessible to anyone with some IT knowledge, so don't feel intimidated if you haven't used one before. There certainly are more advanced scans for which you'll likely want to partner with an MSSP if you choose to perform them.

Application

Core

At the application level, your first goal is to patch. Patch regularly. And automate as much of the patching as you can so you don't neglect anything. Some of the largest attacks—like the WannaCry attack from a few years ago—can be prevented by keeping up with major patches (and quickly pushing out high-priority security updates). If a worried leader or staff member reaches out to you about an attack and you can confidently say you've already patched a vulnerability, it can go a long way in earning trust and building confidence. This has long been a security recommendation, and while advanced security tactics may get a lot of press, many attacks can be prevented with the simple basic blocking and tackling of security like patching. Try to schedule patching during off-hours. That way you'll minimize disruption to the business while still allowing enough time to fully update servers and workstations.

Second, be careful about what types of software you allow staff to use. Avoid any end-of-life software as it often becomes littered with security flaws that have to be regularly dealt with.

Advanced

Employees often install their own software without your team knowing. This introduces risk because unsupported software could open vulnerabilities. You can reduce your attack surface by limiting the applications an organization can use. Consider looking into an application allow/deny list solution like AppLocker® to minimize the chaos shadow IT can bring. However, be aware this is not a silver bullet—often, it still requires some handholding.

Also, investigate mission-critical software before users start using it. Examine the software's website to see what security practices it has in place and make your decision accordingly. Many reputable cloud vendors publish their security policies so that you can make a more informed decision. Think twice before choosing a vendor that doesn't include a trust center.

People

Core

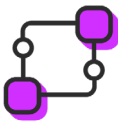
Almost all security breaches have some human involvement. Employees can be the weakest link in a security posture, from having poor password hygiene to clicking a malicious email link to accidentally deleting important data. Because of this, you should enlist your end users as part of your security services. They have to do their part.

User security training is a must. During any training sessions, teach users the elements of strong passwords, the signs of malicious emails like misspellings or unusual requests with urgency (like "please sign this invoice in the next two hours"), and make them aware of any security or personnel policies like locking doors and not allowing nonemployees into the building unaccompanied. Don't focus exclusively on email for social engineering either—voice phishing over the phone, social media phishing, and tech support scams can lead to a full-scale attack as well. You can do your own training but consider adding in commercial-grade training as well. Don't forget to do these trainings regularly—whether semiannually or quarterly—so people retain info. You can also send out monthly reminders on security topics to keep things fresh for end users. Plus, all of these are excellent opportunities to remind your leadership of the value and ROI of you, your team, and investing in security.

Advanced

While training users on password complexity can build a foundation, it's still up to individuals to comply. When security brushes up against ease-of-use, people revert to what's easy. One workaround involves offering a password-management-as-a-service to your users. Particularly with the shift to the cloud, cybercriminals increasingly focus on passwords as the main point of attack. When you implement a password manager, users can automatically generate strong passwords and not have to remember anything other than their primary password. It satisfies both the ease-of-use requirement and security. Plus, password managers offer additional features to help you manage password hygiene across the board. You can set password reset schedules, so users don't use stale passwords—which means that if their passwords were stolen in a data breach, hackers only have a specific time window to use the credentials. You can also revoke users' access if you detect something fishy from an account. This is important when someone leaves an organization as well. Even if the employee doesn't seem like they have an axe to grind, they can still use old access to attack companies. It's better to be on the safe side.

Beyond that, use multifactor authentication (MFA) on all important systems and accounts. The practice offers an additional safeguard against password compromises, and alerts users to false login attempts or password reset attempts when they receive a message. Text or email-based MFA works as a first step; however, third parties can intercept these messages. For that reason, we recommend implementing an authenticator app for users. In this case, a bad actor would need access to someone's phone rather than simply intercepting an SMS message.



Network

Core

At the core level, you have your basic endpoint firewalls. If an attacker does get into the corporate network, these can help prevent movement throughout the rest of the network if the firewalls are properly configured. Windows® Firewall works well for most purposes.

We won't cover much more in the network section. You may want to implement next-generation firewalls for advanced network protection, but we'll cover that in the next section. A lot of network security tools, such as security information and event management (SIEM) tools, require specialized knowledge and dedicated personnel. We'll cover this in the comprehensive section.

Internet

Core

Finally, we have several technologies to help keep out cyberthreats. Remember our earlier comment—it's best to protect as far away from the data as possible. If you can stop an attack from even reaching the network or device layer, you'll have a much easier time.

One crucial technology is email protection. While you'll still need to conduct user training on email phishing signs, adding a secure email gateway offers a lot of additional power. It's helpful to get a product that's specifically designed for email security, rather than relying on native email security in other services like Microsoft 365 or Google Workspace®.

There are a few settings to configure. First, block macros. Many threats come from weaponized documents, where a downloaded Microsoft document will launch a malicious macro. Blocking these can potentially shut down this common attack. Second, set up scanning for link extensions. Often, emails will link out to a legitimate site but then start a malicious download after that. Scanning for link extensions can help. Finally, block password-protected documents and files. Attackers often do this to prevent scanning and detection, so cut them off at the pass. If someone needs to send documents securely, there are plenty of other ways, including cloud-based file sharing like Dropbox®. Allowing password-protected documents simply poses too great a risk when other options are available.

Next, set up proactive DNS filtering on the network and the endpoint. Thousands of malicious domains are created each day[4], so protecting against these new sites is critical. If an attack lands, it will likely reach out to a malicious server or domain to download a payload. Having real-time AI-based domain categorization coupled with machine learning protects the endpoint from accessing the malicious payload. Custom popup blockers can also keep users from navigating to new phishing sites that crop up frequently.

Advanced

For more protection, consider implementing next-generation firewalls. These are like traditional firewalls but add several security features like intrusion-prevention systems, application firewalls, and potentially antimalware protection.

If you're going this route, look at firewalls that can also do SSL inspection. Malware often gets hidden within encrypted traffic via HTTPS. SSL inspection decrypts incoming traffic and then scans for potential viruses. It then re-encrypts the traffic and sends it to the server if all looks good. This gives you far more visibility into network traffic, which is a vital step in reducing potential threats. It's also worth getting a next-generation firewall that uses some level of threat intelligence to keep up with the latest threats.

Additionally, consider looking at cloud-based firewalls. These shift the focus away from just the network perimeter (which still needs protection but isn't the wall it used to be) to users and access. Since so many users work remotely, these protect access externally. Push the control to where the information gets accessed, even if it's remote.

Finally, while this not a security product, we recommend closing any internet-facing ports unless absolutely needed.

Backup and Data Protection

Backup is essential for your security. This is particularly true in the age of ransomware, as you can use it to recover data, devices, or applications.

We recommend at least having a good, cloud-based backup in place since ransomware often deletes local backups. Having data and even full systems off-site means you can recover much faster. Ransomware isn't the only issue backup can help address. Many fileless attacks seek to escalate privileges on endpoints to gain persistence (and do damage). Insider attacks may occur when someone attempts to delete a host of important files; having a backup in place helps you restore files.

Remember, online storage systems have their place, but they're not backup. For example, Dropbox can expand your file storage and help foster collaboration, but it doesn't offer versioning to allow you to recover important files at points in time. Plus, some backup solutions offer standby systems to enable you to get customers up and running on a virtual machine while you recover any other issues. You can't get that from an online storage solution.

4. "Vast Majority of Newly Registered Domains Are Malicious," SC Magazine. scmagazine.com/home/security-news/malware/vast-majority-of-newly-registered-domains-are-malicious/ (Accessed May 2021).

Finally, it's worth looking for a solution that offers automated recoverability testing. This lets you know your backups are ready to go in the event of a disaster so you can get customers moving as fast as possible. The last thing you want is to face a ransomware attack and find out your most recent backups have been corrupted, causing you to lose a lot of data for the client and miss your recovery point objectives.

Comprehensive Coverage: Working with an Managed Security Services Provider (MSSP)

Some businesses require comprehensive security coverage. These organizations often fall under compliance requirements that dictate a base level of security. Some simply are larger and take security very seriously. You should consider partnering with an MSSP, or working with a compliance partner rather than taking it all on yourself in these cases. There are several reasons to consider partnering.

First, unless you live and breathe security day in and day out (and your technicians do, too), it'll be very challenging to keep up regular duties and advanced security services at the same time. In most larger organizations, security and IT teams sit separately anyway, and there's some logic to this. A network administrator will focus on something entirely different when looking at network traffic than a SOC analyst at a security operations center (SOC) would. Even when it comes to threat intelligence services, it's often hard to know the quality of these feeds without some specialized security knowledge and without really understanding the threat intelligence provider's reputation.

Second, building comprehensive security (beyond the core and advanced levels), can become cost prohibitive. You'll need a set of new tools and may need to build out an entire SOC and a team (that could include SOC analysts to watch network traffic and interpret threat indicators or incident responders to help further analyze incidents' attack chains and recommend remediation steps). Getting into this isn't for the faint of heart.

But on the plus side, partnering with MSSPs offers a lot of benefits. For starters, they should have the tools available to monitor networks via a SOC and often alert you to potential issues for your customers (without you having to build the infrastructure for this yourself). You look like the hero to your business when you take the actions to fix things. Second, they can do active threat hunting based on known indications of compromise on your behalf. They use specialized knowledge gained from following the security industry and having the latest threat intelligence to know what signs of compromise to look for. This can be time-, labor-, and knowledge-intensive to do, so it's probably not a fit for someone who isn't deep in the trenches here. Third, they can also run external network vulnerability scans to help close the front door to advanced hackers. Compared to internal vulnerability scans, external scans look for services or areas that may be open or vulnerable on the web that would allow attackers to worm their way into a network. Often, crimes of opportunity happen because a cybercriminal scans for victims using publicly available data on openings (which SMBs are particularly at risk for); external vulnerability management helps close these holes.

The benefits don't stop with your users. As mentioned earlier, IT professionals have increasingly come under attack from cybercriminals. If a criminal can compromise one IT professional, they can compromise their entire business' data in the process. This can even put them out of a job. As a result, some IT departments retain the services of an MSSP to make sure their own internal security is up to snuff. These companies can monitor network traffic, run penetration tests, or help limit the damage and recover after an incident. It's easy to focus so much on

your users you take some shortcuts internally; hiring an MSSP to help you stay vigilant can really reduce your risk. Nothing's bulletproof, of course—anyone can get hit any time. But hiring security specialists reduces your risk drastically.

Demonstrating Security Investment ROI

All the information in the world can't help if the business and its leaders aren't on board. In this section, we'll talk about some of the realities of "internal selling" of security investment—and how to knock your next presentation out of the park.

For starters, most organizations know they need security. They see the same headlines we all do. They probably know people who have been personally affected by ransomware. However, they may not necessarily understand what proper protection entails. Many smaller businesses may think AV is enough. And frankly, most organizations don't want to think about the details of security at all—but they do want to keep their budgets down. Beyond this, they may prefer to stick to the status quo rather than upgrading to deal with the current environment (especially if they're unaware of what you're doing on their behalf).

When presenting to leadership or finance, it's crucial to start by outlining the current risks in the threat landscape. They may not speak the language of security risk, but their ears will perk up when they hear about the risk to their business itself. If you want, consider walking them through a potential cyberattack like Ryuk that touches the various layers of security to illustrate a real-world example of a multistage, multifaceted attack. You may see an "aha" moment when the stakeholder sees the various stages in a kill chain, demonstrating that attacks have grown more sophisticated and beyond the point where AV and a firewall are enough. As with the adage, "show, don't tell," you may want to cite the statistics on downtime and costs of data breaches, so they understand what's at stake.

Then, point out any gaps in coverage you have and show how you plan to resolve them. For example, if stakeholders are already meeting the core guidelines, suggest upgrading them to an EDR solution and password management as a critical next step to further reduce their risk.

Once you have buy in, make sure to regularly review their security postures and try to help them upgrade as new technology and practices become critical for keeping bad actors out of the system. Make sure to cover this at any quarterly business reviews you do—it's a perfect opportunity to help keep security top of mind and reduce business risk.

One important note—try to avoid using fear in your presentations. While it's important for prospects to understand risk, your presentation should reassure them that you'll be able to handle things for them. Try to end on a positive note: it makes a difference.

The Risks and Rewards of Security

Let's face it—**security's hard.** Your defenses must be strong enough to keep cybercriminals at bay each day, but cybercriminals often need to get lucky once or twice to really do serious damage to a business.

That's why updating your defenses is critical. Cybercriminals evolve frequently.

Whether it's new threat types or twists on old threats like breaching data as part of a ransomware attack, it's crucial to try to stay on top of the latest threats and implement threat protection that meets the moment. Failure to do so can be very risky both you and for your business' bottom line. However, as cybersecurity continues evolving, the rewards for IT professionals grow as well. When you up your security game, you can earn more and stay miles ahead of your peers.

So as you face the current threat landscape, make sure to remember you're the expert for your business. It looks to you to keep it safe—so help your business realize the risks of skimping on security and help step up protection.

> For more information on security technologies to help you secure your business, visit **n-able.com**.

About N-able

N-able empowers IT departments and managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein.

The N-ABLE, N-CENTRAL, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

© 2021 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.