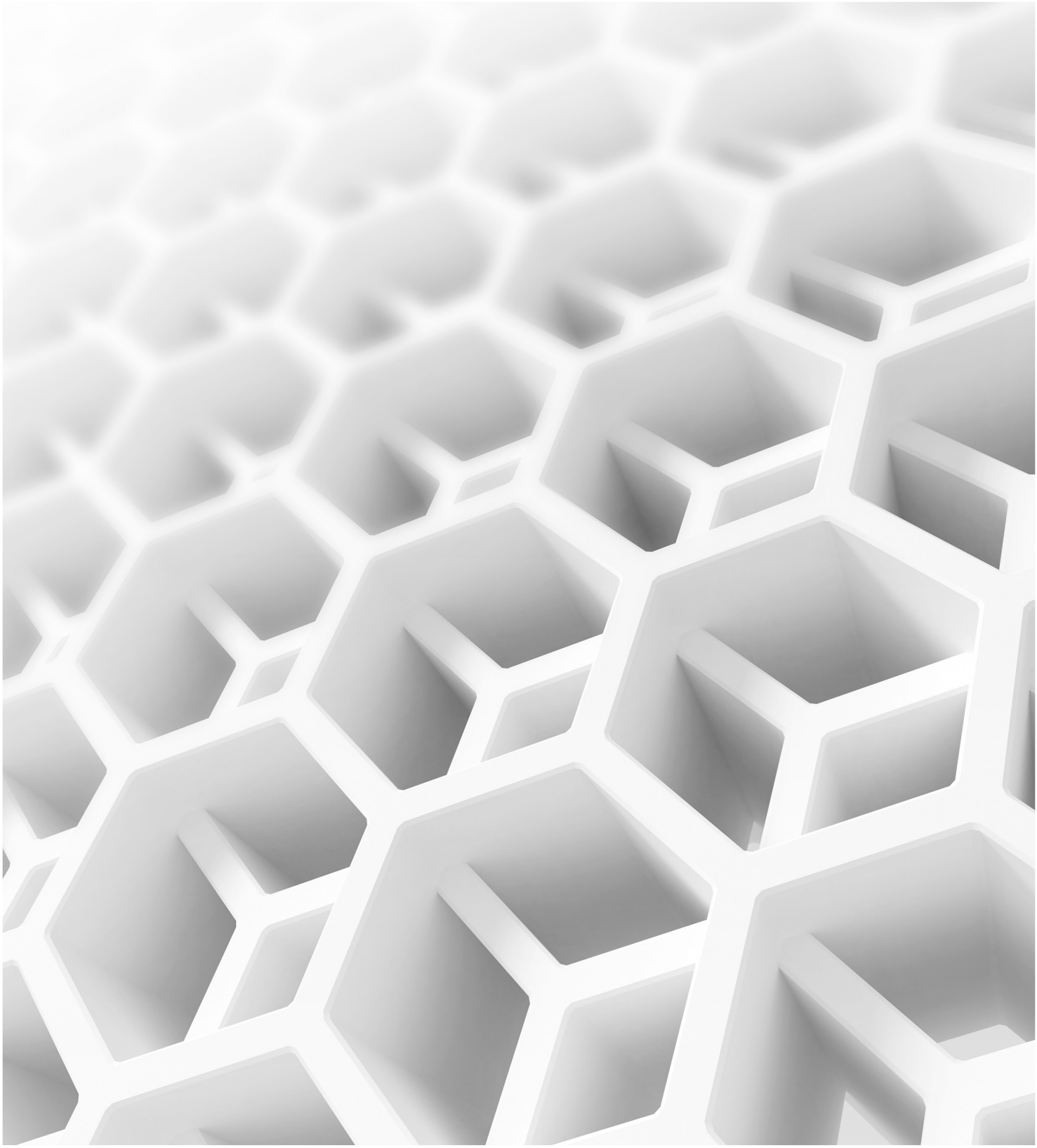


WHITE PAPER

THE CYBERSECURITY BLUEPRINT:
A FOUR-PART MODEL FOR PROVIDING COMPREHENSIVE LAYERED SECURITY

solarwinds msp

INTRODUCTION

Cyberattacks have increased in both number and severity over the past few years. The press has focused primarily on ransomware attacks. It makes sense: some research has shown that ransomware will cost roughly $5 billion USD in 2017 alone.[1] To put that in context, that's higher than the gross domestic product of many small countries and territories, like the US Virgin Islands, the Maldives, or Gambia.

But while ransomware has received the majority of the press, other cyberthreats have grown in their severity as well, threatening both individuals and businesses. Whether it's a distributed denial of service (DDoS) attack taking down a website (or entire portions of the internet), stolen intellectual property due to compromised passwords or improper employee access, or widespread automated attacks against unpatched software, businesses have to stay vigilant against attacks from all vectors.

Organizations seem to be rising to the occasion, with cybersecurity budgets growing at a rapid clip. In fact, estimates show that cybersecurity budgets will total roughly $1 trillion USD during the period of time between 2017 and 2021.[2]

If you're an IT service provider, this gives you a massive opportunity to generate more revenue. However, dealing with the sheer variety of attacks these days—ransomware, malicious insider attacks, and advanced persistent threats, among others—requires that you take a broad, layered approach to security for your clients.

But where do you begin? What tools do you need? And how do you even assess what each client needs to stay protected?

This paper presents a model for providing comprehensive layered security to managed services clients. By working within this framework, you can systematically approach each client's network (or even your own) and know what elements to put in place to provide strong layered security. You'll also have a good sense of where your employees need additional training and what tools and processes they need to master.

CONTENTS

THE FOUR PILLARS OF COMPREHENSIVE, LAYERED SECURITY

Your first inclination might be to think in terms of technical components. However, providing security services to clients goes well beyond the individual components you choose. Instead, think in terms of "what" you're trying to do, rather than "how" you're trying to do it. For example, instead of thinking about what antivirus to use, consider it within the broader context of your threat detection capabilities. Doing so allows you to systematically build defenses for any business.

Use the following four pillars as your framework to approach any layered security project.

1. PROTECT

Your first line of defense involves monitoring both electronic devices and the physical security of corporate offices. This first layer can show early warning signs of cyberthreats, helping you stop attacks before they get off the ground. In fact, some of the defenses in the other pillars would be impossible without this foundational layer. Detecting critical information like personally identifiable information (PII)—especially in hard-to-locate areas like persistent storage—is paramount to limiting the risk if a system is breached.

2. DETECT

This next pillar includes many of the tools and techniques thought of as traditional security mechanisms—like antivirus, patch management, web protection and email protection. They're not enough to cover all problems, but they can deal with quite a few. Just patch management alone would have prevented several major ransomware attacks like WannaCry and Petya.

3. RECOVER AND ENCRYPT

Any defense strategy requires the ability to quickly recover after a disaster. The first two pillars can prevent a lot of attacks, but they're not bulletproof. By having good backup solutions to restore systems quickly, two-factor authentication for account recovery, and strong encryption to prevent unauthorized access to intellectual property, you can provide your clients with a kind of insurance policy against data theft and downtime.

4. ANALYZE AND MANAGE

The final layer involves advanced security tactics and active management. Many businesses require a more in-depth approach than the first three pillars can provide. This step involves penetration testing, security incident and event management (SIEM) systems, and security operation centers. This pillar provides the highest level of protection for businesses, making these some of the most lucrative security services you can provide.

But before you start implementing the practices and technology of the model, you will have to assess the security situation for each client. So we recommend starting with a discovery phase.

DISCOVERY

Whether you're starting out with a new client or you want to review the security state of an existing customer, start by taking stock of existing security defenses. Whether it's out-of-date antivirus with infrequent scans, unpatched software, or inconsistent backups, or "data at rest" scattered throughout the organization, nearly every organization has something you can improve.

Start by going through this list of questions. Asking these questions will help you formulate your plan for implementing the four pillars.

MONITORING

- What general security monitoring do you have in place?
- Do you monitor user activity?
- Do you monitor physical security devices?
- Do you monitor access points?
- Do you monitor IP-enabled cameras?

SECURITY MANAGEMENT

- Do you have an antivirus solution? If so, what kind? How often do you update your definitions and run scans?
- Do you have a patch management solution in place? If so, how often do you update your software?
- Do you have perimeter-level protection, such as mail security?
- What password management controls have you put in place?
- What's the process for when an employee leaves the company?

RISK MITIGATION

- Do you have a defined data management program?
- Do you test the data management program?
- Do you track user access to sensitive data?
- Are you required to adhere to any regulatory acts?
- Do you perform monthly security assessments?
- Do you run vulnerability scans on "data at rest" in all possible locations, looking for PII that could be exploited?

ACTIVE MANAGEMENT & ANALYSIS

- Do you limit employee access to corporate data and select areas of the network?
- Do you have internet content controls in place?
- Are employees trained on security protocols?
- Do you manage the core network to avoid malicious activity?
- Do you have failover/redundancy on the full network?
- Do you have a CTO/CSO you utilize or on staff?

Once you have answers to these questions, you can start implementing the model. However, please view these questions as a starting point—and don't take answers at face value. For example, you may find that user training on security protocols occurs only when a new employee or group of employees start. In this case, you should suggest updating employees on security protocols on a regular basis, both to remind them and to update them on any new processes.

PILLAR ONE: PROTECT

When it comes to the first layer of security, the basics matter. Start by monitoring the access points to your clients' systems (and your building) and ensure that you've "locked every door" so malicious actors have a hard time getting in.

First, add safeguards for physical access to both the office building and devices. For any office space, make sure only active employees have access to the building. Keep an inventory of each keycard so when employees leave the company, you can recover or deactivate the keys.

This applies to physical equipment as well. Unfortunately, many employees try to keep equipment like laptops, smartphones, or tablets after leaving the company. So keep track of each device using a remote monitoring and management (RMM) solution with inventory tracking. Even if you can't recoup the device after an employee leaves, you can use your RMM solution to lock the device or wipe the data on it to prevent ex-employees from stealing or sharing intellectual property.

Next, double check the webcam security. Hackers can get into webcams and spy on employees—or on important meetings in conference rooms. But the threats go beyond simple spying. In October 2016, a distributed denial of service (DDoS) attack took down a host of major websites, including Amazon and Twitter. The culprit? Webcams that were turned into a large botnet to flood traffic to these sites.[3] In short, monitor your webcams—they're an easier access point than you'd expect.

All of this speaks to an important point—monitoring. Find a strong RMM tool to help you monitor traffic in and out of your network. Make sure to cover all internet access points, including firewalls, routers, and switches. However, any internet-connected devices, including webcams or web-connected printers, need to be monitored for any issues.

Finally, we recommend that you perform additional vulnerability scans once per quarter. Look specifically for any unsecured sensitive data including personally identifiable information like customer names, addresses, or credit card numbers, or any protected health information.

TECHNOLOGY FOR STAGE ONE

- Security assessment and testing tool
- RMM tool for in-depth monitoring and management

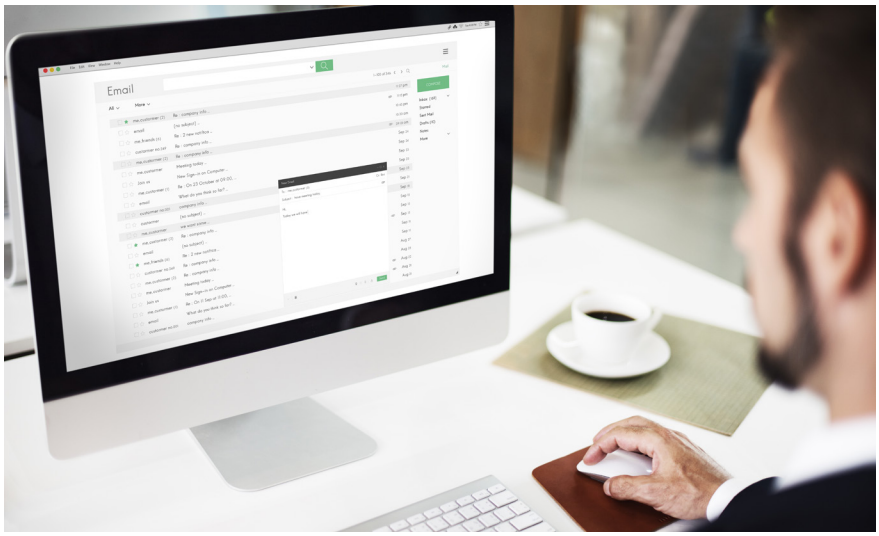
PILLAR TWO: DETECT

The next layer of security covers your detection capabilities. Once a security attack of some kind—whether spear-phishing, malware, or ransomware—gets past your initial defenses, you need to be able to detect it fast and stop it cold.

Start by using a corporate-grade, high-quality antivirus solution. Modern antivirus solutions employ multiple methods of stopping attacks. Traditional virus scans check file signatures against a list of known viruses and malware. This can protect against most issues, but it doesn't protect against new virus strains. Many antivirus solutions have started looking beyond what files are (signatures) and started looking at their behavior. These behavioral and heuristic virus scans will quarantine files that act like viruses—such as those attempting to modify the system registry or delete backups.

Next, you need a strong patch management solution. As ransomware attacks like WannaCry and Petya demonstrated, keeping up to date with the latest critical security patches is crucial. Both ransomware attacks could have been prevented from taking hold in any systems had those affected applied critical updates from their operating systems released just a few months prior. But beyond the OS, it's important to choose a solution that handles patch updates for third-party software, especially for commonly exploited programs like Adobe, Java, and the major web browsers.

Next, you can cut down on a lot of potential threats with perimeter mail protection. From spam to phishing attacks to malware attachments, email is still the largest attack vector. The right mail solution should include multiple antivirus engines and aggressive spam protection. It should also have the ability to scan all email off-site, to prevent malicious emails from even reaching a business's internal servers or computers.



The detection phase can involve a lot of active upkeep. If you're managing thousands (or tens of thousands) of endpoints, updating software with the latest patches or maintaining the latest virus definitions can quickly become unwieldy. That's why we recommend you find tools that can automate as much of the process as possible.

For example, when looking at patch management solutions, you want to be able to set rules like requiring a download, update, and quick reset whenever a critical security patch becomes available for the OS. Any good RMM solution would likely involve some level of automation, but many provide additional scripting capabilities.

TECHNOLOGY STACK

- Automation tools
- Managed antivirus with signature scans, as well as behavioral and heuristic scanning
- Patch management for both OS and third-party software
- Perimeter mail protection service

PILLAR THREE: RECOVER AND ENCRYPT

The next layer focuses on account recovery, system recovery, and data protection. Your previous defense layers can prevent many issues, but they aren't foolproof. It doesn't even take a technical hack—user errors are common and natural disasters can also cause problems (from a small electrical fire to a flood all the way to a major earthquake).

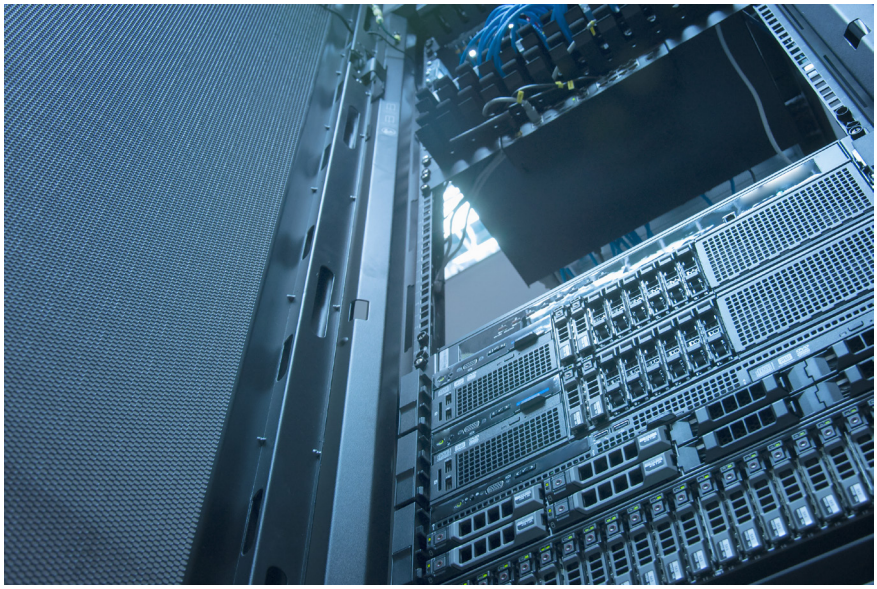
Before you start on this step, consider any regulations your clients may be required to follow. Certain industries—like healthcare, finance, or government—already have clear guidelines around data governance. Make sure that you're familiar with these guidelines if your clients work within a regulated industry.

After regulations, our next piece of advice is to employ two-factor authentication (2FA) for login accounts and devices. Employees may use the same password across accounts, despite your best efforts to train them out of this behavior. If their accounts are compromised elsewhere, this opens the company up to significant risk. The most common method of 2FA involves sending a text message to an account holder's mobile phone when suspicious activity is detected (like a login from a new device). It's unlikely an attacker will have access to the user's phone in addition to their login credentials. Please note that some industries require 2FA for IT systems, particularly government contracts and those governed under the Payment Card Industry Data Security Standard (PCI DSS) standards.

Next, develop a policy on software. Employees often install their own software, and that can open you up to both security and liability issues. You have two options here:

1. Create a "black list" of software to prevent employees from installing them on their systems.
2. Block all software installations unless approved and installed by an administrator. This requires more management, but could be worth it in the long run.

Next, assess the quality of your clients' backup solutions. Look for a backup solution that uses hybrid-cloud technology to back up both servers and workstations—and don't forget key documents! By using a hybrid-cloud version, you not only get faster backup and recovery, you get redundancy from both on- and off-site backup. If Internet access is unavailable, you can quickly restore from on-premises hardware. And if the on-premises hardware is unworkable, you can always restore from the cloud.



Additionally, your solution should allow for rapid and lightweight backups, helping ensure you can run backup more often. You don't want to have out-of-date backups during a crisis. We recommend you look for three key features in a backup solution:

1. Choose a backup solution that employs some form of deduplication to reduce backup file sizes. This makes backup jobs run more quickly, allowing you to back up more often.

2. Make sure your backup system allows you to automate the process as much as possible, preferably with the ability to schedule outside of peak hours.

3. Look for something that gives you visibility into each backup job. When a crisis hits, you want to be able to quickly check your system logs to make sure the data hasn't become corrupted.

Next, you'll need to provide a disaster recovery plan. Developing a disaster recovery plan could be the topic of an entire white paper itself, so we won't go into it here. However, remember that this recovery plan should cover both data and equipment recovery. Also, the plan should go beyond problems arising from cybercrimes, as natural disasters and human error can play a major factor as well. Whether you personally provide the recovery plan, work with your clients' internal IT team, or outsource it to a third party, your clients need a playbook that covers the most likely disasters and the steps to restore continuity (and sanity) to the business. These plans take time and can be in-depth, so don't hesitate to work with a specialized firm for help on delivering this aspect of the service.

At this point, you also want to add data encryption on all devices. Some clients may view this as unnecessary, but this can protect against malicious actors pulling data from a stolen laptop, tablet, or smartphone. It may also be necessary to meet certain regulatory requirements, so again, make sure to double check the laws for your clients' industry.

TECHNOLOGY STACK

- Backup solution
- Two-factor authentication
- Device encryption capabilities

PILLAR FOUR: ANALYZE AND MANAGE

The final pillar consists of both day-to-day management as well as long-term analysis. This stage involves a lot of hands-on work and sophisticated tools that may be beyond the realm of many MSPs; however, becoming familiar with these tools and practices, and outsourcing when necessary, is important for providing complete services to your clients.

First, look at a more robust firewall to protect your clients. A unified threat management (UTM) solution will add a strong, enterprise-grade firewall as well as a number of other helpful technologies, like gateway antivirus, antispam, and network intrusion monitoring.

Next, start inspecting security information and event management (SIEM) solutions. An SIEM involves both a large-scale database and advanced data analysis tools to help you assess security trends. The most robust tools include forensic analysis and searching, threat intelligence that alerts you to bad hosts, monitoring for external devices being added—like USB drives, and even compliance reports. In fact, it's important to note that these SIEM reports can be useful in establishing compliance with HIPAA, PCI DSS, and other regulations.

As you analyze the data from your SIEM solution, start blocking malicious domains and sites you come across. Many web content filtering solutions will come with a default list of known malicious sites that will block users from visiting. However, you can also customize these rules and add more sites to the list, or select from classes of sites like social media or gaming to keep employees productive during the workday. Web filtering solutions help protect against several major issues, including drive-by downloads, phishing sites, and URL hijacking.

The challenge here for many MSPs is that these systems can often be difficult to maintain and adopt. Data analysis and storage are fairly specialized skills as well, meaning this level of service often comes with those with large security budgets. However, as threats have grown more numerous and costly, many mid-sized organizations have begun looking for SIEM providers to help them deal with threats.

To take things to a higher level, consider offering an information security operations center (ISOC) for your clients. This builds on your SIEM system and offers around-the-clock monitoring and defense. However, these solutions can be extremely expensive and unnecessary for quite a few clients and businesses. Yet, some regulations do require the establishment of an ISOC, particularly the PCI DSS standards. In this instance, you may want to consider outsourcing to a specialized firm.

Finally, we strongly recommend periodic penetration tests to help with security readiness. Pen testing software will "war game" out different security scenarios that could arise. These tests show how hackers might attain a goal like accessing sensitive data or taking down a network. Then, you can use the results to address the vulnerabilities and shore up your security. It's worth running these tests at least once a quarter to stay up to date.

TECHNOLOGY STACK

- SIEM Management
- SOC Operation
- Penetration Testing Software

CAN IT SERVICE PROVIDERS AFFORD NOT TO PROVIDE LAYERED SECURITY SERVICES?

Let's face the facts: cybercriminals aren't going away. Their methods will continue to get tougher as they evolve to meet new security protocols and standards. Any business that has sensitive data—and that's all businesses—will always face some level of threat.

What does that mean for the future? Of course, it means a lot of revenue opportunities for those IT service providers that can tackle the new security challenges and help businesses stay ahead of cybercriminals' latest threats.

However, with the severity of cyberthreats over the recent years, many IT service providers may be required to offer security services. When your clients have a problem with their IT—any kind of problem—they're likely to look to their MSP as the party responsible for fixing the issue. It won't matter if your clients crash due to human error or if their systems get locked out due to a ransomware strain, they will simply want their problem fixed.

If you're not currently a full-fledged managed security services provider, the task of taking on more security responsibility may seem daunting. But use the model in this white paper as a guide, and flesh out your layered security strategy as you go. Your clients and your bottom line will thank you.

REFERENCES

1. http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
2. http://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html
3. https://techcrunch.com/2016/10/24/webcams-involved-in-dyn-ddos-attack-recalled/

LAYERED SECURITY COLLECTIVE INTELLIGENCE SMART AUTOMATION

SolarWinds MSP empowers IT service providers with technologies to fuel their success. Solutions that integrate layered security, collective intelligence, and smart automation—both on-premises and in the cloud, backed by actionable data insights, help IT service providers get the job done easier and faster. SolarWinds MSP helps our customers focus on what matters most—meeting their SLAs and delivering services efficiently and effectively.

For more information, visit **solarwindsmsp.com**

COWP00177EN0817

SOLARWINDSMSP.COM

solarwinds msp