The MSP's Guide to Strengthening Managed Security Services with Security-Centric RMM

MSP Barracuda

BarracudaMSP.com

Table of Contents

Why you need to take a security-first approach

Your managed service is running like a well-oiled machine – every system under management is inventoried and up-to-date, you have an ability to support each one remotely, and you already use automation to address minor issues. In essence, you have a predictable and profitable managed service offering that works.

But the rise in cyberattacks targeting small and medium sized business (SMB) – which we define as businesses with less than 250 employees – demand that SMB organizations (and, therefore the MSPs they outsource their IT to) proactively protect against cyberattacks. The good news is that you already have some security components built into your offering (e.g., patch management), but simply addressing one or two aspects of security is not an effective means of keeping cybercriminals out of your customer's networks.

MSPs need to start taking a security-first approach to every service they offer. This goes beyond the security services you offer to your customers — it needs to start with your remote monitoring and management (RMM) solution. An RMM is essential for you to deliver services to your clients, and the right solution can ensure that security is woven in your daily activities.

If you choose to create a separate security offering, there are three primary reasons why you should have security embedded into your RMM.

1. Cyber threats are only getting worse for the SMB

You read the headlines and hear about high-profile cyberthreats that have resulted in hefty ransoms being paid, massive numbers of records being stolen, or millions of dollars spent on remediating attacks. But the question is always raised, what about the SMB?

In 2018, an average of 34 percent of SMB organizations reported being the target of a cyber incident and **in 2019, and that number rose to 52 percent**[1].

And, if you ask the SMB themselves about their perception of cyberattacks in 2019, the majority of them will tell you that attacks are becoming more targeted (69 percent), are becoming more sophisticated (60 percent), and have more severe consequences (61 percent)[2].

Despite the perception that the SMB isn't an interesting target for cybercrime, the truth is, your customers are just as much at the front lines of the battle as any of their enterprise counterparts.

Despite the perception that SMBs aren't an interesting target, the truth is, your customers are just as much at the front lines of the battle as any of their enterprise counterparts.»

1 Hiscox, Cyber Readiness Report (2019)

2 Ponemon, State of Cybersecurity in Small and Medium Size Business (2019)

2. SMBs are ready to do something

Many MSPs have had the experience that their customers don't want to spend their budget on security initiatives. While it's true that the SMB may hold their wallet a bit more tightly than larger organizations, they are starting to understand that with every attack, there are tangible costs associated. Cyberattacks now present a question of when they will happen, not if – **this shifts the conversation around security from an "insurance policy" to a necessity**.

The average cost an SMB pays to remediate a single cyber incident is just slightly over $11,000[1]. While that's not news-worthy, it's a material amount of your customer's revenue that isn't going to turn into profit. In response, SMBs are now actively setting aside a portion of their budget to improving their security posture. **On average, SMBs devote $98,000 of their budgets toward cyber security**[1]. The breakdown of SMB spend by employee size is as follows[1]:

[1] Number of Employees	[2] Average Annual [3] Cybersecurity Spend
[4] 1-19	[5] $7,000
[6] 20-49	[7] $37,000
[8] 50-99	[9] $115,000
[10] 100-249	[11] $436,000

To add to this good news, **on average, 62 percent of SMBs are planning to increase their spend on their cybersecurity initiatives**[1], with nearly one-third of them seeing both security outsourcing (30 percent) and security consultants (31 percent) as being top priorities in the coming year[1]. In addition, nearly one-third (32 percent) of SMBs report that they are already using an MSP to support their company's IT security operations[2].

A material percentage of your customer base is ready to address cyberattacks; they just don't know what to do about it. And that's where you can come in.

3. Your RMM solution already provides some security

Whether you are looking into offering security services separately or incorporating it into your core offering, because you have already sold your customers on services that utilize an RMM, you already have a few advantages:

- **You're already touching every system** – The presence of an RMM provides you with the necessary visibility into what's happening within your customer's network. It also means you have administrative ability to monitor, manage, update, and safeguard your customer's desktops, laptops, servers, and even cloud-based systems. In many ways, an RMM is a necessary foundation for any kind of security offering.
- **Security is already part of your vocabulary** – Most RMMs have some form of either built-in or third-party integrated patch management that ties in with a rudimentary form of vulnerability scanning of systems and applications. There isn't an MSP who goes without putting in some form of anti-malware solution. So, in essence, you have the basics down; you just need to build out a set of security solutions that create a *multi-layered* security strategy for your customer.
- **Your customer already trusts you** – This is key; you've built up the customer relationship where you provide them with advice, vision, direction, and execution for their technology. Who better than you to add security to that list?

There's an obvious opportunity here – one that you're somewhat already teed up to offer. So, what should you do about it?

You have the basics down, you just need to build out a set of security solutions that create a multi-layered security strategy for your customers.»

Going "security-first"

The idea here is to incorporate security-mindedness into every service, beginning with RMM. It's a way of thinking that identifies cyberthreats as yet another operational risk that needs to be addressed on a continual basis. We'll look at three specific steps you can take to begin adding in security services that integrate with your existing RMM offering.

The following high-level steps will help you establish a security-centric approach, powered by your RMM, that can evolve into a separate security services offering later.

- **Define your managed security service** – Here, you'll establish what your security service offering looks like, what parts of your customer's environment you will be protecting, and how you will leverage the automation found in your RMM solution to simplify service delivery.
- **Find solutions that meet your service needs** – You'll need to identify the software solutions that help deliver your service, the integrations that are key to delivery, and how automation can be used across all the solutions involved.
- **Look for ways to leverage automation to get the job done** – Many security-related tasks don't require human intervention regularly; unless there is an issue to remediate. Leveraging automation will be a key component to your service delivery; one that can heavily lean on your existing RMM to deliver.

Leveraging automation will be a key component to your service delivery; one that can heavily lean on your existing RMM to deliver.»

Defining your managed security service offering

Adding security to your existing services, or creating an entirely new service offering, isn't as simple as choosing a piece of software and building around it. In the case of providing cybersecurity to your customers, **MSPs must take a multi-layered approach** – and, therefore, need to **leverage multiple solutions** that need to be a part of the service – to ensure that they can deliver something that actually provides protection.

It's a delicate balance. Too light of an offering and your customer will be riddled with attacks and be very unhappy with you. Too heavy of an offering, and customers may pass entirely because of the cost, complexity, and perceived misalignment with their needs. From your perspective, you want to offer a security service that accomplishes a few things:

1. **It's cost effective** – Despite your customers' need for security, even they have a price in mind.
2. **It's effectual** – Your service offering needs to successfully secure your customers' environments.
3. **It leverages your RMM** – In one way or the other, most attacks involve the endpoint; the very same endpoint your RMM is already monitoring and managing. Offering security that ignores the obvious benefits an RMM brings to the table is a disservice to you and your customer.

This chapter will help you look at the security components in your service offering from a strategic standpoint and provide advice on what services your offering should include.

What should be a part of your offering?

There's an important differentiator that needs to be outlined before getting into specifics. There are MSPs that offer security services, and there are Managed Security Services Providers (MSSP) – they are not the same thing. Your security offering will put protective security layers in place that help to prevent, detect, and respond to cybersecurity incidents. MSSPs go beyond that, offering advanced services such as intrusion management, threat hunting, compliance monitoring, and more.

There are some overlaps in specific services. However, we're making the assumption that you'll simply be attempting to offer a basic – yet effective – set of services as part of your security offering.

Without jumping into various types of security software and hardware solutions you could employ, let's first look at your offering from a service standpoint. What should you be securing as part of your service?

For MSPs wanting to add security services, but not going as far as to become an MSSP, there are five service areas where vulnerabilities need to be addressed to properly secure the environment without needing a tremendous amount of expertise to get started. These areas form a layered security strategy for your customers, and helps you prevent cyberattacks.

The areas of your customer's network that MSPs can most-easily address from a security standpoint are:

- **Perimeter** – This should be looked at as the logical horizon of your customer's network, where firewalls and gateways reside to separate the Internet from the internal network. In more recent years, this has also come to mean the dynamic perimeter that is delineated by users' interaction with the outside world. Remote users, personal devices, public Wi-Fi, cloud-based applications and data, web browsing, and email all have an impact on defining exactly where the edge of the network is. **Today, that perimeter includes the remote worker surfing the web from a corporate device** in a coffee shop somewhere halfway around the world – and you're going to need to secure that user, device, and connection.

- **Network** – Every device on the network has the potential to be exposed to attacks. MSSPs think of the network in advanced terms like penetration testing, and packet sniffing, but there are still things the MSP can do to ensure devices on the network are secure.
- **Endpoint** – Attackers need a foothold within your customer's network and malware needs an environment in which to reside. That's why **the endpoint is a primary target; it gives attackers undetected access from which they can launch the remainder of their attack.** On average, attackers reside 146 days within a network before being detected[3].
- **User** – Phishing and social engineering are the number one attack vectors against SMBs[2]. **The success of these attacks is almost always dependent on user interaction.** Simply put, a user must click a link or open an attachment for an attack to work. But, as part of your security strategy, think about the user as both another point of vulnerability and an opportunity to further the security of your customer's environment.
- **Data** – As part of most cyberattacks, there is a number of ways data can be leveraged to assist the attacker. In ransomware attacks, data is encrypted. Attacks involving lateral movement or island hopping involve directory access, with user accounts often being created, modified, and granted permissions, all in an effort to establish persistent access to your customer's network and resources.

Building a defense using these parts of your customer's network creates a layered security strategy – one where each layer works to strengthen the security stance by addressing cyberattacks using a different method.

Automating your offering with RMM

As you plan out your new security service offering, consider different ways to leverage the automation found in your RMM solution to secure your customer in three ways:

1. **Provide** visibility to the current state of your customer's security
2. **Proactively** ensure the environment is as secure as possible
3. **Automatically remediate** issues that put the customer at risk

Depending on the specific functionality your current solution provides, there are a number of ways automation can assist with your layered security offering. This table shows just some of the ways RMM automation can assist.

3 Microsoft, Advanced Threat Analytics (2019)

Security Layer	Ways to use RMM automation
Perimeter	• Apply and enforce firewall settings to protect laptops when on public Wi-Fi
Network	• Monitor for new devices, and alert IT on potentially malicious ones in the network • Address known OS vulnerabilities used as part of many network based attacks on Internet-accessible servers and endpoints • Apply and enforce sanctioned IP configurations
Endpoint	• Identify potentially unwanted applications (PUA) using software inventory • Address known OS and application vulnerabilities used to infect endpoints with malware • Review device configurations against security recommendations • Enforce secure OS configuration settings
User	• Apply application settings to protect users from becoming a victim of phishing attacks
Data	• Monitor log ins for lateral movement as part of both ransomware and data breach attacks

Defining automated security

The goal is to **devise a service offering that you can predictably deliver**. So, as you formulate what your offering will look like, it's important to bring automation to the forefront to achieve levels of predictability that will breed profitability. An RMM is the foundation for your service offering, and you can layer other security solutions on top of it, which we'll cover in the next chapter: *Choosing security solutions beyond your RMM.*

Leverage the automation found in your RMM to secure customers.»

Choosing security solutions beyond your RMM

In the last chapter, we talked about your new offering as a layered strategy that includes five areas: perimeter, network, endpoint, user, and data. For each of these layers, there are a number of ways you can use your existing RMM solution to address each.

But, an RMM will only get you so far in securing your customers' environment, because its focus is more broad than just security. That's why your RMM is going to need some assistance from other solutions.

In this chapter, we'll discuss different solutions you should consider putting in place to create and deliver a robust and effective security offering.

What other solutions do you need?

While an RMM tool can offer some functionality that can assist with securing your customer's environment, security isn't exactly a core focus for most tools. You need some additional security solutions to round out the offering. The obvious question revolves around what kinds of solutions are needed.

There are many solutions out there to choose from – so many that it can become confusing as to which types of solutions are necessary. To break this down, we will continue to use a layered security model as a way to help you strategize which solution types you need.

Each of the five layers below represents a specific place where there's an opportunity to prevent an attack from continuing – which should be the basis for your selection.

Perimeter

Attacks can take the form of automated scans of your Internet-facing systems and applications. **Putting a next-gen firewall, a web application firewall, and intrusion detection/prevention in place can block malicious scans and access, and stop an attack before it starts**. Attacks that successfully make their way inside a customer network nearly always need to "call home" to a command and control (C2) server. Any kind of malicious outbound traffic can often be thwarted by implementing **domain-based message authentication, reporting & conformance (better known as DMARC) and DNS/URL filtering** to identify and block access to malicious domains and systems on the web.

Network

There are a few ways you can leverage the customer's network to provide better security. **Restricting access** to critical systems and applications by using network segmentation, can limit the potential risk of attackers accessing critical resources. **Performing vulnerability scans** of the network can augment patch management efforts to help proactively identify systems and applications that may be vulnerable to attacks. And lastly, having the ability to **monitor network traffic for anomalous and known-malicious traffic patterns** can assist in blocking attackers from continuing malicious actions.

Endpoint

If an attack has made it through all the previous layers, you need **endpoint-based anti-malware and endpoint detection and response** solutions in place to monitor and block potentially malicious operating systems and applications behavior.

User

In a lot of ways, the user is your weakest link; they are the ones that open malicious email attachments and click on malicious links without giving it a second thought. So having web and email scanning solutions in place that proactively checks for malicious content before the user can interact with it, helps protect the user from themselves. But, users can also be a part of your security strategy by putting them through **continual security awareness training**. This trains them to have a vigilant mindset while working, and what kinds of tactics and methods of attacks are commonly used in attacks.

Data

The previous layers are all designed to keep attackers from getting to your data. Should they succeed in gaining access, ransomware attacks will potentially result in encrypted data and data breaches that may include the manipulation of user and group accounts in the Active Directory to facilitate access. So, **backups should become a part of your security offering** to be able to **recover the environment** back to a known-good and known-secure state. It's also important to note that some ransomware specifically looks for backup files on on-premises systems, so having cloud-based backup should be a priority for your MSP.

The table lists out recommended solution types that are specifically designed to counter attack measures at each step of a cyberattack.

Protection layer	Solution type
Perimeter	• Next-Gen/Cloud-Gen Firewall • Web Application Firewall • Intrusion Detection/Prevention • DMARC • DNS/URL Filtering
Network	• Network Segmentation • Vulnerability Scanning • Network Monitoring/Packet Inspection
Endpoint	• Anti-Malware • Endpoint Detection and Response
User	• Email Scanner • Web Scanner • Security Awareness Training
Data	• Cloud-based Backup/Recovery

Another layer that has not been listed that you should consider is **identity**. Protecting user credentials with **multi-factor authentication** is a simple and effective means to establish that a user is who they say they are. Additionally, protecting privileged identities by using some kind of password vault for privileged accounts (generally referred to as privileged access management) may also be of use.

All of this can sound a bit daunting to an MSP that has limited experience in offering security. Don't let the list scare you; software vendors focused on MSPs have already figured out ways to simplify the implementation and integration of these kinds of solutions, so that you don't feel like you're drowning on day one.

Putting the solutions all together

When possible, look for ways to **leverage both automation and integration to improve service delivery**. As you work to select the exact solutions to use, identify similar relative functionality that elevates intelligence, improves security, and reduces risk.

In our next chapter, we'll discuss the value automation and offer up practical ways it can be used.

Protecting user credentials with multi-factor authentication is a simple and effective means to establish that a user is who they say they are. »

The value of automation in security

Over the years, many managed service businesses have grown from just one IT pro that did all the work themselves to larger businesses who deliver multiple services to their customers. The challenge for MSPs now, is to find new methods, tools, and processes that allow them to grow. But with most services, there's still an option to manually address problems. Even with an RMM solution in place that can deliver automation via scripting, many MSPs still prefer to let their techs do the work. For some services – namely RMM and backups – it is possible (to a degree) to deliver services manually. When it comes to security, it's just not possible.

There are a number of things that make it difficult to deliver security services manually. They include:

- **The increasing sophistication of attacks** – Cybercriminals are making huge investments in methods to ensure a successful attack. Phishing attacks now use advanced social engineering methods – and even go as far as investigating a specific individual target, creating spoofed websites that look like their legitimate counterpart designed to steal credentials, and using evasive infection techniques to keep malware from being detected by security solutions.
- **The availability of Crimeware-as-a-Service** – Today, anyone wanting to get into the "business" of cyberattacks can do so. For example, developers of ransomware offer it "as-a-Service," with no up-front costs to a cybercriminal (creating an ease of entry to cybercrime), and being compensated via a percentage of the ransoms collected.
- **The constant changing of tactics** – Cybercriminals are continuously testing their methods, both against security solutions and in practical use. They are looking for what works and what doesn't, and are changing methods of attack to avoid detection, increase infection, and improve the success of attacks.

- **The unpredictability of attacks** – MSPs don't have the ability to know when, where, how, and what the scope of an attack will be. This makes remediating difficult at best.

In essence, establishing and maintaining the security of an SMB is a constantly moving target. The threat landscape keeps changing at a blinding rate, so it's very difficult for an MSP to stay abreast of every new attack, every system's security configuration, etc.

To create an offering that truly puts forth a best effort to secure the customer, automation becomes a necessity – from its use in protecting the customer environment, to preventing attacks via vulnerabilities, to detection of attacks when they occur, to remediation activities. In short, security services need automation to be successful.

The benefits of using automation

Automation offers you more than just the benefit of having something done without manual intervention. There are a number of ways automation benefits the MSP in delivering a security services offering. These include:

- **Consistency** – Consistency is vital to knowing the entire environment is being managed in the exact same way. If you've decided to implement a given security configuration or want to apply some patches, you can't have some systems configured only partially. Automation ensures every system and application that needs to be managed is.
- **Accuracy** – When deploying, managing, reporting, and remediating security, manual efforts can be riddled with human error. While consistency is about ensuring all systems are configured the same, accuracy is about ensuring the specific configuration on a per-system or per-application basis is correct. Automation provides the ability to deploy, configure, and update without deviations in your security policy's design.

To create an offering that truly secures the customer, automation becomes a necessity.»

- **Up-to-date security** – Automation isn't just about running scripts to perform tasks. It should be a well-thought process that enables you to keep all your solutions up-to-date as the threat landscape changes. For example, as new malware or malicious domains are discovered, the automatic updating of the respective solutions to block these means of attack is a tremendous value to your offering that you never need to worry about.
- **Faster response** – The goal of a managed security service offering is for you to maintain a secure environment that protects the customer. But issues can arise, such as identifying an unpatched system. Automation can be used to scan, identify, and remediate these kinds of issues without human intervention, lowering your delivery costs.
- **Scalability** – As your business is asked to take on more devices, you can conceivably grow the service through automation, without needing to take on more staff.
- **Predictability** – Automation delivers this in two forms. First, the delivery of your offering is accomplished in a much more predictable manner because of the consistency and accuracy of delivery. Second, the previous benefits of automation add up to a more predictably secure environment, where your confidence in the environment's security is high.
- **Profitability** – Predictability yields profitability. By automating the effort that goes into securing a customer, it's much easier to get your offering to a profitable state.

Delivering better security through automation

Let's take a few examples and look at how automation (whether as part of your RMM or other security solutions) might be used to improve service delivery. The table on the following page highlights a few methods of how automation can be used practically within three different stages of security: prevention, protection and detection, and response.

Service stage	Automation example	Solution
Prevention **Purpose:** Keep an attack from coming to fruition by creating a secure environment	Monitoring the network for new devices	RMM
	Monitoring systems for potentially unwanted applications	RMM
	Updated definitions and machine learning algorithms	Intrusion Detection/Prevention DNS/URL filtering Web Scanning Email Scanning
	Review, update, and enforce security configurations on network devices, operating systems, and applications	Firewalls RMM (OS, Applications)
	Vulnerability, scanning, and patching	RMM (OS, Applications)
	Ensure proper backups through job monitoring and remediation	Backup/Recovery
Protection/Detection **Purpose:** Monitor for and identify indications of potentially malicious activity	Updated definitions and machine learning algorithms	Anti-Malware EDR
	Test and verify attachments	Email Scanning
	Monitor for suspicious OS behavior	EDR
	Monitor for suspicious or inappropriate configuration changes	RMM
Response **Purpose:** Respond to leading or active indicators of attack	Quarantine malicious files and code execution	Email Scanning Anti-Malware EDR
	Run remediation scripts to address detected issues	RMM

Achieving security through automation

MSPs, by definition, are seeking to deliver services that are predictable in nature. But the nature of cyberattacks make it difficult to achieve. Automation makes security far more attainable; from establishing and maintaining a secure configuration, to identifying when attacks are attempted, to quickly taking action to remediate successful attacks.

MSPs already using RMM tools are off to a great start with a platform that could provide custom automation. By adding on other solutions that utilize relative measures to address their part of a layered security strategy, MSPs can quickly create a service delivery model that is effective, responsive, scalable, and predictable.

By utilizing automation, MSPs can create a service delivery model that is effective, responsive, scalable, and predictable.»

Security services start with a security-centric RMM

It's evident that even the smallest organizations are still susceptible to – and are even hand-selected targets of – cyberattacks. So, it's imperative that MSPs begin to formally offer managed security services to protect, prevent, detect, and respond to cyberattacks.

As you work to develop, define, and eventually offer a security service, it's important to incorporate the security features already found in your RMM solution into the service offering. In some cases, RMM features can be the foundation of one aspect of the new security service (e.g., patch management), or can be used to augment both proactive and reactive security measures using automation (such as monitoring for, and remediating, unsanctioned endpoint configuration changes). Even as you put a multilayer security strategy together, consider how each part of your strategy can leverage the RMM that already has its' proverbial hands on endpoints and servers within your client's environments.

RMM represents a powerful foundation for a security offering. MSPs already offering managed services that utilize RMM solutions have the potential to easily begin offering a base service that can be augmented over time, providing your RMM solution has security-centric features and automation already built in.

As an MSP, the path towards offering security services is inevitable. Your customers are becoming increasingly aware of the need and will either look to you to address their security concerns or an MSP that will. So, start by looking to see what functionalities can be leveraged, define the scope of your new service, choose any additional security solutions needed, and use your RMM's automation as the foundation for a new means of generating service revenue.

Key takeaways

An RMM tool should be:

- A near-mandatory, bare-minimum that MSP clients are utilizing to protect their business and end users
- Clearly communicated and emphasized as part of the MSP's services offering to clients, as well

The security-centric image an RMM tool projects for an MSP signifies how:

- Vital cybersecurity is as a core of the MSP company's services
- Seriously the MSP treats the security of its customers

Other security solutions and services can be added or built on top of an RMM tool to:

- Allow the RMM tool to serve as a solid starting point of a security services portofolio
- Strenghten the overall value of a security services portofolio of an MSP
- Attract more clients

Automating security offerings, will:

- Simplify tasks and increase efficiencies
- Reduce the burden and make life easier for both the MSP and its clients.

About Barracuda MSP

Barracuda MSP is the MSP-dedicated business unit of Barracuda Networks. Our mission is to drive the success of our IT service provider partners, delivering industry-leading security and data protection via a purpose-built MSP platform, steadfast commitment to partner success, and a wealth of channel expertise.

We believe in the managed service provider model. We understand your challenges. And, we are champions for your success.

Our Partners are also distinctly positioned to grow their recurring revenue and margins and scale their business profitably, thanks to a unique business model and MSP-friendly pricing structure.

About Barracuda RMM

Barracuda RMM is a powerful, security-centric remote monitoring and management tool for MSPs that offers several features to strengthen an MSP's security posture, including comprehesive reporting to share with SMB clients, a centralized dashboard, task automation, PSA ticketing, and support for third party app integrations, among others.

Barracuda RMM is built to help MSPs:

- Grow your business
- Automate service delivery
- Reduce operational costs

Visit our website to learn how Barracuda RMM equips your MSP with the tools and insight needed to deliver high-quality remote security and support services to your clients.