WHITEPAPER

THE CASE FOR MANAGED ENDPOINT SECURITY

How to achieve breakthrough growth for your managed services business

CONTENTS:

Introduction and Objectives

N-able Technologies is the global leader in remote monitoring and management (RMM) Automation software for Managed Service Providers (MSPs) and IT departments. Our ongoing work with a worldwide base of more than 2,000 MSP partners confirms that customer acquisition is the overwhelming top business priority for any IT service provider working in the managed services space. Specifically, MSPs report they are looking for new strategies, platforms and solutions for acquiring new small and midsize business (SMB) customers and converting more customers to a managed services model.

The urgency of this need is underscored by the fact that only about 10% of the addressable SMB market has opted for a fully managed services contract. Part of the problem is that many MSPs have found it difficult to package and market managed services engagements to many of their prospective clients. Clients don't understand the "MSP value proposition" or they need to see tangible returns before "buying in" to the fully managed services solution.

What MSPs urgently need is a less costly and less complex value proposition that enables them to demonstrate immediate value to SMBs while moving them towards a true managed services relationship. The ability to provide Managed Security that is part of a Remote Monitoring and Management (RMM) Automation platform is the breakthrough opportunity they need.

While every customer from the smallest SMB to the biggest enterprise requires anti-virus – and many of them already buy it through their VAR / IT Reseller / MSP – managing this anti-virus and security software has long been a challenge for many MSPs. Most notably, MSPs have not been able to centrally control and manage anti-virus software in an efficient way as a true managed service.

By integrating endpoint security into a single, centrally controlled, RMM Automation platform, MSPs can standardize security applications deployment, configuration and management across all customers using the same management platform they trust to deliver managed services. This enables them to realize important new efficiencies and significantly reduce the cost of winning and maintaining a managed services client.

Managed security reflects a shift from selling a price-sensitive, commodity-based security tool to providing a differentiated, high-value, managed service. How and why MSPs need to incorporate managed endpoint security into their practice is the focus of this whitepaper.

WHY ANTI-VIRUS AND SECURITY IS A PROBLEM FOR MSPS

Disparate point solutions

- MSP has to manage or clean up a jumble of anti-virus, anti-spam and malware products deployed into the SMB infrastructure

Commoditization

- A wide and ever-changing variety of choices and many free offerings makes it difficult for the MSP to sell security products profitably

Lack of integration

- The MSP must use an outside vendor's security solution in parallel with their managed services platform – creating a host of billing, reporting and management challenges

Multiple consoles and customer views

- The MSP must manage separate consoles for every customer with multiple log-ins and passwords – and no central reporting

No standardization

- The MSP is managing different AV and security products for different customers, resulting in complexity and operational challenges

Specifically this paper will show how MSPs can use a managed security solution to establish an easier, simpler point of access into the SMB market, win more business – and finally deliver on the promise of fully managed services. Key topics include:

- » Why anti-virus and security is a problem for MSPs
- » The critical distinction between anti-virus, endpoint security and managed endpoint security
- » What to look for: essential features and attributes of a managed endpoint security solution
- » How to motivate SMB customers to make an immediate change with their current approach to security
- » Key benefits of a managed endpoint security solution
- » Why MSPs need a flexible, a-la-carte approach to services to take full advantage of the SMB managed services market

This paper will be invaluable to any IT service provider or MSP who wants a new strategy for spearheading SMB markets and achieving the promise of fully outsourced managed services clients.

Anti-virus and Security: Hoping for the Best

SMBs are well aware that viruses and malware can cripple their business: most ensure they have some form of protection. Unfortunately the approach many SMBs take to anti-virus impedes many MSPs from being able to easily deliver a true managed services solution.

PROLIFERATION OF ANTI-VIRUS PRODUCTS

Over time, most MSPs discover that "small" businesses deploy a disparate mix of anti-virus, firewall, anti-spam and spyware solutions throughout their infrastructure. Efficiently managing this hodgepodge of products is hugely challenging. Whether the SMB has three employees or 100, it eventually becomes motivated to standardize around a single security solution. Typical drivers for this change include excessive and time-consuming complexity, real or perceived risks and vulnerability, or a catastrophic failure resulting in lost productivity and revenue. Regardless of the trigger, the SMB reaches out to an IT service provider for guidance and recommendations.

CRITICAL BUSINESS OPPORTUNITY

For the MSP this is a critical business opportunity to deepen the relationship with an existing client or demonstrate great value to a new customer. Unfortunately, traditional anti-virus and security solutions make this a double-edged sword for MSPs: they present both opportunity and many challenges.

Although anti-virus is considered essential by most SMBs, it is also seen by many to be a commodity. One reason is the sheer number of anti-virus and security choices available. Also many anti-virus and "real-time" security products are offered at low cost or "free" by many major vendors as part of other bundled security services or applications. The challenge for MSPs is to find an approach to delivering anti-virus and managed endpoint security in a way that enables them to profitably service their customers within a managed services model.

STANDARDIZATION: A STEP IN THE RIGHT DIRECTION

Standardizing security tools is one way for MSPs to achieve quicker time to resolutions and superior operational efficiency. Without standardization, the MSP must log onto into a different security system for each customer. This results in a highly decentralized approach with every SMB customer having a different way to be managed.

By standardizing an endpoint security tool across all customers, an MSP immediately knows what tool their SMB customers are using. As well, all of the MSP's technicians can be trained on how to use one tool, realizing immediate operational efficiencies.

Although these are important benefits, standardization doesn't assure MSPs the ability to manage anti-virus within a unified managed services platform to efficiently deliver true managed endpoint security. Typically anti-virus is a second interface that requires the MSP to log into a different system.

In a best-case scenario, a standardized anti-virus tool is installed locally by the MSP: when a problem occurs, the MSP's technician logs into that specific tool to troubleshoot. The problem with this familiar scenario is that information doesn't get rolled up to provide a single view in advance of an incident. Nor can the MSP trend information or be 100 percent certain that the tool is functioning properly and doing what it is supposed to: preventing infection and filtering malicious traffic. Management complexity is further magnified when customers have different renewal dates of the same tool. Billing is also problematic – because they are using a separate, third-party vendor solution alongside their own managed services platform.

NEGATIVE IMPACTS

The lack of centralized management and monitoring leads to increased risk of outbreak at the client site. The lack of centralized management, workflow and notification leads to more incidents that negatively impact customer perception, cost money to respond to, and result in higher overall management costs, and lower organizational efficiency for the MSP.

While standardization is an important step in the right direction, it is still cumbersome for the MSP to manage. As a result, many MSPs install an industry leading tool – but struggle to manage it effectively because it is a standalone point solution that sits outside the service provider's central management console.

MANAGED SECURITY

To address these challenges, MSPs need the ability to monitor and centrally manage a standardized endpoint security solution (across all customers). Managed means continuously monitoring a system: if the anti-virus software is not working or updating, it will be noticed and acted upon. In other words, it is an "active" process – even though it may be automated by an RMM system.

With this approach, all tasks – deployment, configuration, management, monitoring, notifications and reporting – are performed through a single user interface – a "single pane of glass" –for all customers. This is the promise and compelling benefit of managed endpoint security. Centralized management through a single RMM Automation console is the critical new requirement that must be added. In this respect, managed endpoint security takes automation, standardization and integration to the next level.

Important Differences:

ANTI-VIRUS, ENDPOINT SECURITY AND MANAGED SECURITY ARE NOT THE SAME

Anti-virus tends to be a pervasive and blanket term used by SMBs to describe a number of elements that make up a security solution. Over the past decade, anti-virus has evolved into security and more recently "endpoint security." Despite these changes, the term "anti-virus" has stuck with SMBs.

Our research with MSPs suggests that smaller SMBs (less than 50 employees) are not yet using the term "endpoint security" and are far less familiar than larger SMBs with the concept of managed endpoint security. For MSPs this means that some education will be necessary when consulting with SMBs – because anti-virus, endpoint security and managed endpoint security should not be seen as synonymous.

Simply put, SMBs will not pay for something – or be motivated to make a significant change if they do not perceive a fundamental difference in a recommended security solution with tangible benefits. The following distinctions may be helpful for framing the differences to your SMB customers.

ANTI-VIRUS – DETECT, PROTECT AND REMOVE

Anti-virus is a software product that represents one component of a complete security solution. The primary function of anti-virus is the detection, prevention and removal of potential computer viruses and malware including Trojan horses and worms. Over the past decade anti-virus software has evolved to include removal of adware, spyware and other malware.

ENDPOINT SECURITY

Endpoint security is anti-virus plus other value-added protection including anti-spam, content filtering and web protection. Moreover, endpoint security introduces the concept that each device – the endpoint – requires its own security rather than relying only on a traditional firewall, central scanners and other intrusion detection devices such as anti-virus software alone. Endpoint security augments these other systems. Anti-virus, while not replaced, in effect becomes the last line of defence in a multifaceted protection chain.

MANAGED ENDPOINT SECURITY

Managed endpoint security is a logical evolution and next step in security protection: it brings security under the control of a single, integrated RMM Automation platform. This includes automation of routine IT tasks, remote control, remote monitoring, remote management and reporting on all applications including security.

The result: endpoint security is seamlessly integrated into a complete managed services solution for MSPs targeting SMBs.

WHAT TO LOOK FOR IN A TRUE MANAGED ENDPOINT SECURITY SOLUTION

- Enterprise-class endpoint security protection
- Endpoint security is integrated seamlessly into an RMM Automation platform to provide a true managed services solution
- Centralized console
- Control and manage anti-virus efficiently with end-to-end remote monitoring, management and reporting
- All configuration, updates, monitoring and reporting for security – and all other applications and devices – is through a single management console

Important benefits to the MSP include:

- Realize immediate operational efficiencies from centralized remote monitoring, management and reporting through a single console – with one log-on, one password, one set of reports and one set of event management for everything
- Generate new revenue from selling security as a managed service versus third-party anti-virus licensing
- Deepen existing customer relationships by delivering a significantly higher-value service that is integrated with other managed services
- Differentiate your MSP services from other service providers that are selling traditional anti-virus and security tools that are not part of a managed service
- Profit from the sale of a higher-margin service rather than reselling a third-party commodity anti-virus product

Requirements for a True Managed Security Solution

The first pre-requisite for a true managed endpoint security solution is the ability to ensure SMB customers get world-class anti-virus protection. This includes:

» Anti-spam
» Firewall
» Anti-virus/spyware
» Intrusion prevention
» Centrally managed quarantine
» Content filtering
» Real-time alerts

CENTRALIZED "ALL-IN-ONE" CONSOLE

Many endpoint security solutions offer enterprise-class protection – that's not new. The critical new requirement that defines a managed endpoint security solution is that enterprise-class security is integrated into an RMM Automation platform with a centrally managed console that can be used to automate and deliver managed services to all SMB customers. Furthermore, the central console must also provide a common management dashboard that seamlessly collects information on all customers and provides real-time information.

PART OF A MANAGED SERVICES OFFERING

When endpoint security is integrated into an RMM Automation platform, technicians can not only control and manage anti-virus in an effective way, they can also provide an end-to-end remote monitoring (supported by notifications), management, and reporting solution with notifications for the entire SMB IT infrastructure. This integration, coupled with remote automation of routine manual IT tasks, is what makes managed endpoint security fundamentally different and extremely powerful.

With this approach, security becomes an integral part of an MSP's integrated, high-value managed services offering rather than the "add-on" of a traditional, price-sensitive commodity tool.

A MANAGEMENT CONSOLE DOES NOT MEAN MANAGED ENDPOINT SECURITY

Many security products lay claim to being "managed" simply because they have a management console. This does not constitute a managed endpoint security solution in the context of true managed services.

From the perspective of an MSP, a security solution that comes equipped with its own console is a single tenant solution that results in one console for every customer. While the MSP may realize some benefits from standardization, day-to-day management is still cumbersome.

For example, consider a situation where the MSP is trying to manage 50 customers with a security solution that comes equipped with its own console. The MSP is effectively managing 50 separate consoles with 50 separate update policies, 50 separate scan policies – and they have to run reports on 50 separate systems. Any gains made from standardizing around a single toolset are quickly lost. The end result is increased operational complexity that translates directly into higher overhead costs, and reduced margins. This is not a true managed endpoint security solution.

Key point: the value proposition for a true managed security solution is one that delivers industry-leading protection through a single integrated management console that is used to manage all customers and all devices as part of a true managed services offering.

> "95 percent of companies nowadays have an anti-virus installed on their network endpoints, but 72 percent are still infected."
>
> *- Panda Labs*

Overcoming SMB Objections to Managed Endpoint Security

USING INDUSTRY RESEARCH AND KEY QUESTIONS TO EXPOSE SMBS' RISKS AND FEARS

One reason for the relatively low deployment of managed services is that current platforms supporting remote monitoring and management – the foundation for any successful managed service offering – are complex, costly and generally available as an all-or-nothing service. It takes considerable time and effort from MSPs to educate SMB customers on the value of a managed services model. This leads to long sales cycles that are difficult for many MSPs to weather and that yield lower revenue than expected.

This is the key reason managed security is such an important break-through opportunity -- it provides the MSP with a less expensive and less complex value proposition while quickly demonstrating the value of managed services.

Success for MSPs hinges on SMB customers recognizing that security should also be a managed service and therefore fundamentally different from existing and largely commoditized anti-virus and security products. In addition to understanding the difference between a managed security solution and traditional security tools, the SMB must realize it has an immediate need or problem.

The most common objection raised by SMBs when an MSP introduces a new anti-virus or security solution is that they "already have anti-virus." This paper has already shown how there are many approaches that an MSP can take to overcome this objection and motivate an SMB to consider a managed security solution.

Reporting third-party industry research that reveals most SMBs are far more exposed and vulnerable than they realize, is one strategy. Put another way, "Mr. SMB customer your current anti-virus product may not be working correctly and providing the protection you are counting on, and you likely have no way of even knowing." Helping a prospective SMB customer to realize their security tool is not working or is inadequate is critical. This is the foot in the door – and where industry facts can help.

MOST SMBS WITH ANTI-VIRUS ARE INFECTED

According to a study carried out by Panda Labs, based on 1.5 million users, 95 percent of companies have anti-virus installed on their networks yet 72 percent had malware on their networks. Many users are infected without knowing it. This means that traditional protections are not enough for meeting an SMB's security needs. Malware has become more complex and much of it goes undetected.

In a 2010 report, Panda also reported that 46 percent of SMBs have been infected by Internet threats[1]. The measurable loss in direct business revenue or lost productivity is a very real concern to most SMBs. According to the in-depth Gartner: User Survey Analysis: IT Security Opportunities in the SMB Market, North America (2007): "Almost 50 percent of SMBs shut down external network access during serious external attacks; for many SMBs, this can cause crippling revenue loss."

For MSPs trying to motivate an SMB customer to embrace a managed security solution, these are compelling facts. While the MSP does not want to resort to fear mongering, these research findings may give a prospective customer legitimate reasons to be concerned about the level of protection they really have and how vulnerable their IT assets are.

KEY QUESTIONS YOU CAN ASK AN SMB PROSPECT OR CUSTOMER

Questions are an MSP's best friend and bring a surgical precision to the task of revealing potential SMB security vulnerability. These questions can plant seeds of doubt that they are well protected from mass-market malware. For example:

1. Who is finding out about any viruses that are detected by your current solution?

   » Do you actually trust your employees to know what to do or call you?

2. Can your users/employees turn off their protection or scheduled scans?

   » Anti-virus cannot detect threats if it has been cancelled by users

3. Wouldn't you feel safer if security information were aggregated centrally?

   » Knowing that security information is being sent to an MSP who knows what to do can bring significant peace of mind

4. Can you afford to have your network shut down to resolve an outbreak or problem?

   » What revenue or productivity losses will you incur if your network goes down for a few hours or half a day or more?

5. What type of reports does your service provider give you?

   » Are you getting regular reports that show threats that were averted, detected or quarantined?

   » Are the reports customized and easy to understand?

[1] **Panda Security Report:** http://www.darkreading.com/smb-security/167901073/security/antivirus/226900214/index.html

6. Are you using a standard anti-virus tool across your organization?
   - If you are using several solutions, how do you ensure these are kept up-to-date?
   - How frequently are these being updated – is this good enough?

7. Are you covered by any regulatory compliance?
   - SMBs in the health or financial industry are mandated by law to show that their network is properly protected – and auditors often like to see third-party outsourced vendors managing networks rather than internal IT departments

8. Have you had a recent infection?
   - If the answer is "yes", this quickly leads to further questions about the cost of downtime, how the problem was fixed, what was the root cause? etc.

9. What would be the consequences if sensitive data or information were stolen from your network?

These and similar questions can help an MSP quickly expose a point of potential vulnerability in the SMB's current anti-virus protection. This effectively becomes the "thin edge of the wedge" into the largely untapped SMB market and opens the door to other MSP services.

A Modular RMM Automation Solution is critical to MSP Success

A Managed Security solution that is part of an "a-la-carte" RMM Automation platform gives an MSP optimal flexibility to meet specific SMB needs – and a compelling value proposition that will be hard to beat. Essentially the MSP can replace a mishmash of unmanaged standalone, anti-virus products with an enterprise-class security solution that also includes 24/7 remote monitoring, management and reporting.

Other standalone services that compliment an MSP's managed security solution can include:

- Audit tools for detecting potential vulnerabilities and helping SMBs in highly regulated industries meet compliancy needs
- Back-up tools for disaster recovery
- IT reporting solutions for assessing the IT infrastructure and generating performance reports
- And others

The ability to offer a security solution, and other tools, that are centrally managed by an RMM Automation platform, enables an MSP to more easily demonstrate the value of a managed services offering. Centralized functionality also enables MSPs to more easily demonstrate value to SMBs through the proactive delivery of all services and the ability to generate customer-specific reports that demonstrate the security activity on the customer's network in a very user-friendly format.

GET N-CENTRAL FREE FOR 30 DAYS

Drive recurring service revenue from all SMB opportunities

Use N-central free for 30-days, with no obligation. This free trial offer:

- Gives you access to the complete N-central toolset
- Allows you to remotely monitor and manage all of your desktops, servers, and network devices
- Enables you to upgrade at any time to our on-premise or hosted software

Remote power at your fingertips – use your FREE N-central software to:

- Manage all of your customers from a single, state-of-the-art console
- Monitor every device for availability and performance
- Control any device anytime, anywhere
- Provide incisive reports to demonstrate your value

Get details and register for your free 30-day trial N-central software by

https://secure.n-able.com/signup/?value=c2lnbnVwaW5mb2lkPTE2YmM5NjZhLTViM2QtNDE3Ni1iNTIzLTEwYTdiM2UwODA4NSZjYW1wYWlnbmlkPTcwMTUwMDAwMDAwN0dvcw==

Conclusion

Managed Security that is part of a RMM Automation platform is an important opportunity that the managed services industry has been waiting for. By seamlessly integrating world-class endpoint security into a leading-edge remote control, remote monitoring, remote management and reporting platform, MSPs can:

- » Realize huge new operational efficiencies and savings
- » Provide a true end-to-end managed services offering that for the first time includes security
- » Differentiate their managed service offering while creating significant new value to SMB customers
- » Use Managed Security as a new point of entry to demonstrate the value of managed services
- » Provide real benefits and reasons for an SMB customer to migrate to managed services

N-CENTRAL 8.0

N-able is meeting these needs and more with N-central® 8.0, the #1-rated Remote Monitoring and Management Automation platform that now includes:

- » **Remote Automation** – easily and quickly automate many routine IT tasks and process including: updating patches, resetting passwords, running defrags, application deployments, updating software, and many other tasks
- » **Remote Management** – tools for securely connecting to and gaining control over any Windows or non-Windows device on the network in seconds
- » **Support Manager** – tools to provide the core functionality required to effectively manage end-users and deliver more than 90 percent of services remotely
- » **Remote Monitoring** – a single comprehensive console to easily monitor the availability and performance of any IP-enabled device
- » **Audit Manager** – a breakthrough tool that enables MSPs to help SMB clients in highly regulated industries, such as the finance and medical markets, more easily meet their compliancy requirements
- » **Tactical Reporting** – a library of built-in real-time reports that provide performance insight to the IT infrastructure including what happened on any machine (transaction and log reporting)
- » **Security Manager** – enterprise class end point anti-virus and security protection to ensure a rock solid, secure IT infrastructure

N-central is the only RMM Automation platform that provides MSPs with an integrated yet unbundled product strategy. An “a-la-carte” approach gives MSPs the ability to map products, services, and technology to the specific needs of their SMB customers. This makes N-central the most flexible and powerful solution for automating tasks, securing an SMB’s IT infrastructure, and remotely delivering high-value IT services.

Find out more about N-central and why this is a breakthrough opportunity by visiting www.n-able.com.

About N-able Technologies

N-able Technologies is the global leader in remote monitoring and management software for managed service providers and IT departments. N-able's award-winning N-central platform and complementary toolsets, backed by best-in-class business and technical services, are proven to reduce IT support costs, improve network performance and increase productivity through the proactive monitoring, management and optimization of IP-enabled devices and IT infrastructure. N-able is 100% channel-friendly and maintains operations in North America, the U.K., the Netherlands and Australia. Get N-central with managed endpoint security free for one year.

Copyright

www.n-able.com
info@n-able.com
1-877-655-4689

N-able®