N-able
by solarwinds

USING MANAGED ENDPOINT SECURITY TO GROW YOUR MANAGED SERVICES BUSINESS

AN MSP'S WORST NIGHTMARE

It was a simple mistake. An employee of one of one of your customers clicks on a link to get some useful information promised by someone they vaguely remember meeting at a networking event. The network is opened to vicious malware. And then the heartache begins. Data is corrupted. The network goes down. The company can't send invoices or fulfill orders. Paralyzed, they make a panic stricken call to their MSP.

What do you do?

The best answer is to ensure you are never confronted by this nightmare scenario. Yet, without the right type of managed security solution, the odds of your small to medium sized business (SMB) customers becoming victims of a nefarious virus, worm or Trojan is extremely high. According to BizTech, nearly one-third of all malware attacks specifically target businesses with fewer than 250 employees.[1]

Cybercrime is on the rise for one simple reason: it seems to pay. The recent outbreak of Cryptolocker is a case in point, nabbing about $30 million in ransom in 100 days.[2] Like most viruses, Cryptolocker gets installed through unwanted attachments or emails or visits to dubious websites. Once installed, information on all computers is encrypted and the owner is greeted with a ransom message: **your files will be lost without payment within 72 hours.**

This paper will show how MSPs can use a managed security solution to establish an easier, simpler point of access into the SMB market, overcome customer objections, win more business – and deliver on the promise of fully managed services.

An MSP confronted by this catastrophic scenario is immediately thrown into damage control. Do they recommend wiping the hard drive and losing their customer's data? Or do they recommend ponying-up the Bitcoin ransom fee and hope they are dealing with "honest" criminals?

Either way, the SMB's trust and confidence in the MSP's security solution is undermined, perhaps irretrievably. Unfortunately preventing security breaches isn't the only challenge facing an MSP. The bigger challenge is demonstrating immediate value to SMB customers while moving them to a true managed services relationship.

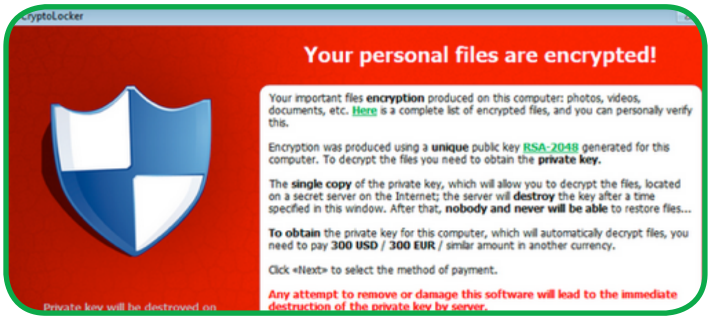
Managed security represents a shift from selling a price-sensitive, commodity-based security tool to providing a differentiated, high-value, managed service. How and why MSPs need to incorporate managed endpoint security into their practice is the focus of this whitepaper.

[1] http://www.biztechmagazine.com/article/2013/04/malware-attacks-targeting-small-businesses-rise-infographic

[2] http://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up-to-30-million-in-ransom.html

A VIRTUAL BATTLEFIELD

While Crypotolocker is considered by law enforcement as one of the worst kinds of viruses, it is but one of many that today's MSP must be able to defend their SMB customers from. Another recent example of vicious ransomware is Reveton, (also known as IcePol). This virus displays a phony message posing as a police service telling the unlucky recipient they have been monitored accessing child abuse websites and issues a fine that must be paid to avoid prosecution. American victims see an image of the U.S. president pointing an angry finger beside the FBI logo for added credibility and a fear factor. In Britain, a similar approach uses a stern, "we are not amused" image of the Queen and a police officer in standard Bobby gear.



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on

In a major 2013 study on cybercrime in the U.S., the Ponemon Institute reported an increase of 26 percent in the cost of cybercrime from the previous year. Perhaps more alarming, the study revealed that the companies in the study experienced 122 successful attacks per week in comparison to 102 successful attacks the previous year.[3]

Not surprisingly, threats of cyber-attacks have been well publicized. In response, there has been a proliferation of anti-virus and security products. For many MSPs, this is the nub of the problem.

"Although anti-virus is considered essential by most SMBs, it is also seen as a commodity," says Bryan Zimmerman, Product Manager, N-able Technologies®. "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," he adds.

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 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

Multiple mobile devices

- Many small businesses professionals use three or more mobile devices to run their business – smart phone, tablet, and laptops are common, all with sensitive data and represent a walking security threat

The need for managed security

Centralized management through a single RMM Automation console is the critical requirement for a managed endpoint security offering. In this respect, managed endpoint security takes automation, standardization and integration to the next level: it brings security under the control of a single, integrated RMM and automation platform. This includes automation of routine IT tasks, remote control, remote monitoring, remote management and reporting on all applications including security.

[3] 2013 Cost of Cyber Crime Study: United States. © 2013 Ponemon Institute, LLC

KEY REQUIREMENTS FOR A MANAGED ENDPOINT SECURITY SOLUTION

To address these challenges, MSPs need the ability to monitor and centrally manage a standardized endpoint security solution (across all customers). Key requirements for a true managed endpoint security solution include the following requirements.

ADVANCED MALWARE PROTECTION

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

- Anti-virus/spyware
- Firewall
- Intrusion prevention
- Centrally managed quarantine
- Content filtering
- Real-time alerts
- Web content filtering
- Web access control
- Application control

What defines a security solution as 'world class' is the ability to detect and block malware from installing in the first place; so that customers are protected. Following extensive research, N-able Technologies selected BitDefender® as the foundation for its managed endpoint solution for this reason. Bitdefender was one of the first mainstream solutions to effectively prevent ransomwear like Cryptolocker from propagating by using sophisticated behavioral analysis and advanced network scan technology – it takes a proactive approach by blocking malware from accessing command and control servers. The ransomware can't retrieve the public key from the server – and it can't encrypt files.

"Your network is only as strong as its weakest link," says Zimmerman. "It's not good enough to have most of your employees protected because once a virus like Cryptolocker infects a single machine, it can't be stopped. You need 100% coverage to avoid potentially catastrophic consequences."

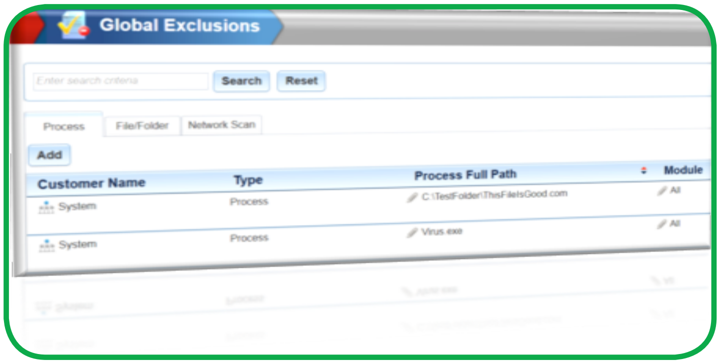
CENTRALIZED "ALL-IN-ONE" CONSOLE

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 a remote monitoring and management (RMM) 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 dashboard that seamlessly delivers real-time information on all customers and devices including mobile."

A true managed security solution is one that delivers industry-leading malware 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.

PART OF A MANAGED SERVICES OFFERING

When endpoint security is integrated into an RMM platform, endpoint security becomes part of the established workflows, with data flowing into dashboards, ticketing, reports, notifications, and more. With this approach, security becomes an integral part of an MSP's integrated, high-value, multi-tenant managed services offering rather than the "add-on" of a traditional, price-sensitive commodity tool. Multi-tenancy is an essential requirement for a scalable, growth-focused managed service solution.



Customer Name	Type	Process Full Path	Module
System	Process	C:\TestFolder\ThisFileIsGood.com	All
System	Process	Virus.exe	All

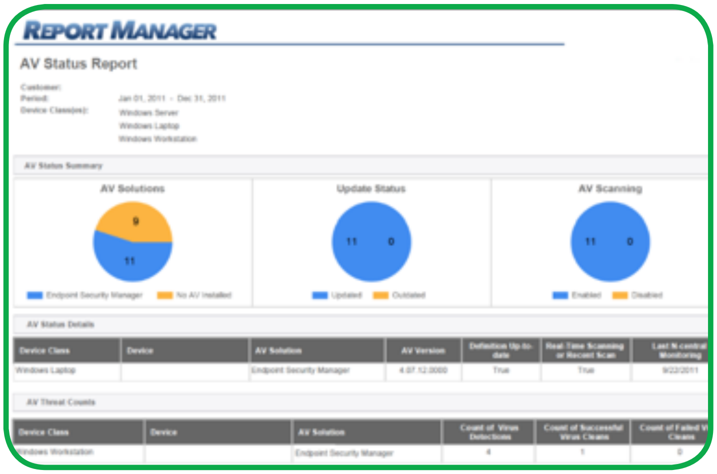
A single, integrated management dashboard with global exclusions provides a powerful method of centrally administering AV exclusions.

REPORTING ON ACTIVITY

A key problem faced by most MSPs is visibility. You may be working tirelessly, 24/7 to protect your clients' network and ensure optimal efficiency. Because the majority of your proactive security interventions and Help Desk activities are delivered remotely; they go unnoticed, un-reported, and often undervalued.

"One of the biggest threats that can occur for an MSP as they enter managed services is that they are doing all of their remediation in the background," says Kevin Kirkpatrick, Senior Manager of Partner Development at N-able Technologies. "They keep their end customer up-and-running and protected. Over a period of time, say six months or a year, the customer says well everything is running great and I never see you. So what am I paying you for?"

This is why the most successful MSPs build standardized checkpoints into their service agreement using monthly or bi-monthly reports that include an AV Status Report.


REPORT MANAGER

AV Status Report

Customer:
Period: Jan 01, 2011 - Dec 31, 2011
Device Class(es): Windows Server
Windows Laptop
Windows Workstation

AV Status Summary

AV Status Details

Device Class	Device	AV Solution	AV Version	Definition Up-to-date	Real-Time Scanning or Recent Scan	Last N-central Monitoring
Windows Laptop		Endpoint Security Manager	4.07.12.0000	True	True	9/22/2011

AV Threat Counts

Device Class	Device	AV Solution	Count of Virus Detections	Count of Successful Virus Cleans	Count of Failed V Cleans
Windows Workstation		Endpoint Security Manager	4	1	0

Figure 1: The AV Status Report quickly scans the network by client, location, or device to provide a summary of all AV solutions with details on what is current and out of date.

Most SMBs have various, multiple AV solutions deployed, often in distributed environments where customers have multiple locations or regional offices. For many MSPs, the deployment of these various AV solutions is a tracking nightmare.

In a worst case scenario, you might miss a deployed AV solution and get caught off guard by your client. This can inadvertently undermine the confidence your customer has in their malware protection and lead to a slippery slope of creeping doubts: does my IT service provider know what is going on? Am I really protected from malware? Can I really trust their advice?

The AV Status report enables you to quickly and easily quantify all AV solutions and their status. It ensures they you aware of exactly what is going on in your clients' environment by summarizing all AV solutions including the updated vs. outdated status and where AV scanning is enabled vs. disabled. Figure 1 illustrates the type of information that is provided by an AV Status report using simple, intuitive graphics to visually communicate key information. This report is usually used in conjunction with many other reports to provide a well-rounded summary of the current IT environment and is a key requirement for a true managed services endpoint security solution.

The key requirement is having access to real-time threat data across all customers and devices. For example, having fingertip access to scan summaries that provide a detailed list of what was scanned and found over the past 90 days. Again, an integrated console is critical to your ability to access this type of report and troubleshooting information – and easily engage your customers in relevant discussions about a range of security and threat issues.

SELLING A MANAGED ENDPOINT SECURITY SOLUTION

One of the challenges faced by many MSPs is that customers don't know what they don't know. Many feel they have deployed so called disparate off-the-shelf malware solutions and they are lulled into feeling protected. Peppering these customers with alarming statistics and examples of horrendous security breaches is unlikely to woo them. In our experience with over 3,000 global partners, the key is to highlight points of vulnerability with the current approach to security protection.

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.

Questions are your 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 and create an opportunity to introduce a managed endpoint security solution. 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?
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 other similar questions can help you quickly expose a point of potential vulnerability in a SMB's current anti-virus and malware protection. This effectively becomes part of your secret sauce – and the "thin edge of the wedge" – for acquiring new customers and opening the door to other MSP services.

CONCLUSION

By integrating endpoint security into a single, centrally controlled, remote monitoring and management (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.

Important benefits to the MSP include:

- Realize immediate operational efficiencies from centralized remote monitoring, management and reporting through a single console
- 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

The N-able advantage

Managed endpoint security (provided by Security Manager - AV Defender – powered by BitDefender) is one component of a unique, multifaceted strategy used by N-able Technologies to help all MSPs go-to-market with confidence, align their sales strategy and products with the needs of all types of SMB customers, and achieve 100% market coverage.

Key planks in the total N-able solution for quickly transforming MSP businesses and giving them an unfair competitive advantage are:

- N-central®, the industry's number one rated Remote Monitoring and Management (RMM) and service automation platform
- Strategic, best-in-class, optional modules for maximum flexibility to meet specific customer needs and generate additional revenue streams
- Unique, industry leading hybrid licensing model designed for maximum business growth
- Comprehensive professional support services to help MSPs go to market with new revenue generating services in the fastest time possible

Learn more about the N-able Advantage and how you can take full advantage of our endpoint security solution to demonstrate breakthrough customer value by visiting. www.n-able.com.

ABOUT N-ABLE TECHNOLOGIES

N-able Technologies by SolarWinds is a leading global provider of complete IT management, Automation and MSP business transformation solutions. N-able N-Central® is an award- winning RMM and MSP Service Automation Platform. N-able has a proven track record of helping MSPs standardize and automate the setup and delivery of IT services in order to achieve true scalability. N-central is backed by comprehensive business enablement support services and a unique freemium licensing model. Thousands of MSPs use N-able solutions to deliver scalable, flexible, profitable managed services to over 100,000 SMBs worldwide. With offices in North America, the Netherlands and Australia, N-able is 100% channel-friendly and maintains strategic partnerships with Microsoft®, Intel®, IBM®, CA®, and Cisco® among others.

COPYRIGHT

This document contains information intended for the exclusive use of N-able Technologies' personnel, customers and potential customers. The information herein is restricted in use and is strictly confidential and subject to change without notice. No part of this document may be altered, reproduced, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of N-able Technologies.

Copyright protection includes, but is not limited to, program code, program documentation and material generated from the software product displayed on the screen, such as graphics, icons, screen displays, screen layouts, and buttons.

N-able Technologies, Inc.'s trademarks, service marks, logos and copyrights are the exclusive property of N-able Technologies, Inc. and its affiliates. All other trademarks or works mentioned herein are used for identification purposes only and may be or are intellectual property of their respective companies. N-able Technologies and SolarWinds Worldwide, LLC are not affiliated with any of the respective companies.