MSP'S GUIDE TO

Integrating Security

SHUTTERSTOCK

With small and midsize businesses moving their back-end systems to the cloud, managed services providers are expanding their practices to cover security—a market niche that's unlikely to disappear any time soon. **By Scott Bekker**

It's hardly controversial to say that managing servers kept on-premises by small and midsize businesses (SMBs) might not be a sustainable business for managed services providers (MSPs).

More and more companies are moving to the cloud, and with megavendors such as Microsoft redirecting development resources from products like Windows Small Business Server (SBS) to cloud-based solutions such as Office 365, the writing is on the wall.

To be sure, the bread-and-butter business of managing servers for customers could last for a long time. Still, many MSPs are looking around for the technologies that will keep bringing them revenues and profits for the next half-decade or more. Some of them are finding a new niche in security with an eye toward endpoint security, which will continue to be needed even if every SMB in the world were to go to the cloud for infrastructure services.

It's not just good for MSPs to branch out in their practices. It turns out SMBs need to pay more attention to security than they have in the past.

SMBs UNDER FIRE

According to the 2013 version of the annual Symantec Corp. "Internet Security Threat Report," the increased targeting of SMBs was among the most important security trends of the past year.

"Last year's data made it clear that any business, no matter its size, was a potential target for attackers. This was not a fluke. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. In fact, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them," the report stated.

"This is especially bad news because based on surveys conducted by Symantec, small businesses believe they are immune to attacks targeted at them. However, money stolen from a small business is as easy to spend as money stolen from a large business. And while small businesses may assume they have nothing a targeted attacker would want to steal, they forget that they retain customer information, create intellectual property and keep money in the bank," the report continued. "While it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is more than compensated by the fact that many small companies are typically less careful in their cyber defenses. Criminal activity is often driven by crimes of opportunity. With cybercrimes, that opportunity appears to be with small businesses."

RMM VENDORS PUSH SECURITY

Over the last few years, MSP tool vendors have been nudging their MSP partners toward building out security components to their MSP practices.

Recently, for example, Kaseya International Ltd. embraced a freemium model to expand the customer base for its services.

The remote monitoring and management (RMM) tools vendor earlier this year released a set of five Software as a Service (SaaS) IT tools that are free solutions for specific IT headaches.

Kaseya goes to market in two ways—mainly through its 6,000 partners (mostly MSPs), and directly to corporate IT departments. Liz Lederer, senior vice president of Kaseya field marketing channel programs, says the company believes the SaaS tools will help MSP partners add net new customers.

"Having these free tools now is actually a great thing for our partners because our partners can use them as door openers or for planting the seeds with some of their customers. There could be just a particular problem that they're looking to solve. Or there could be a particular piece of our technology that they're looking to add into their portfolio of management solutions," Lederer says.

Gerald Beaulieu, vice president of product marketing at Kaseya, says the five SaaS IT tools are only an initial set—more will be coming.

"Our initial release is focused on auditing and security, because in many ways they kind of go hand-in-hand," Beaulieu explains.

The first batch of tools includes File Share Audit, User Audit, Software Audit, Security Audit and Windows Patch Management. All of the tools require only an e-mail address to set up and can be used to manage up to 1,000 computers.

"We're starting to carve out specific areas of our product that we can deliver to IT professionals or that our channel partners can sell ultimately to end customers that address specific pain points that they're having with those organizations," Beaulieu says.

"They may not need an entire platform to address the one issue," he continues. "So what this does is it says, 'Hey, let's address that pain point through a tool.' It could be a free offering; it could be a paid offering. Get them in the family, let them see the benefits we can offer, and then over time hopefully we can bring them up to our complete solution. And if not, if that one tool solves their pain point forever, then that's fine. So there will be some that will move up the stack and some that will stay."

The free tools use the same agent that Kaseya normally installs for its full RMM and other products, meaning that

DON'T LET YOUR CUSTOMERS BECOME WATERING HOLES

One of the most significant new threats of the last year has small businesses and other poorly secured organizations at its heart—although their data is not the target. The phenomenon is called a watering hole attack.

According to the "2013 Internet Security Threat Report" from Symantec Corp.:

"The biggest innovation in targeted attacks was the emergence of watering hole attacks. This involves compromising a legitimate Web site that a targeted victim might visit and using it to install malware on their computer. For example, this year we saw a line of code in a tracking script on a human rights organization's Web site with the potential to compromise a computer. It exploited a new, zero-day vulnerability in Internet Explorer to infect visitors. Our data showed that within 24 hours, people in 500 different large companies and government organizations visited the site and ran the risk of infection.

"The attackers in this case, known as the Elderwood Gang, used sophisticated tools and exploited zero-day vulnerabilities in their attacks, pointing to a well-resourced team backed by a large criminal organization or a nation state."

To Symantec, small to midsize businesses are increasingly being used as pawns in watering hole attacks. Attackers are leveraging the often-weak security of small businesses to defeat the strong security of their partners and customers. ***–S.B.***

should customers choose to upgrade, it's just a matter of turning on the existing functionality, Beaulieu says.

GET IN ON ENDPOINT SECURITY

What such freemium tools offer, in addition to a way to generate net new business, is a way for MSPs to leverage their experience managing on-premises servers as a bridge to a security practice. Beyond such server-based security practices, many RMM vendors offer specific endpoint security tools, which serve as one potential hedge in a cloudy future.

What such freemium tools offer, in addition to a way to generate net new business, is a way for MSPs to leverage their experience managing on-premises servers as a bridge to a security practice.

Some common areas of endpoint security services that many MSPs are offering to customers include:

Antivirus Protection: The gold standard of desktop protection is still absolutely necessary, and still underused. Many RMM providers contract with top antivirus vendors to use their engines and bolt them into their RMM consoles to protect against viruses at both the e-mail server and desktop levels.

Antispam: Spam is more of a productivity killer than a security threat, although it can be a source of malware or lure users to visit dangerous Web sites. Protection against spam is a common feature of many of the antivirus suites in use by RMM providers—and an added service for MSPs to deliver.

Spyware Protection: This software falls more into the category of protecting users from private attackers installing keystroke loggers and phone-home software in users' desktops, as opposed to the government snooping at the heart of the recent PRISM revelations. Nonetheless, spyware is some of the most insidious malware out there, and scanning for it regularly is a smart move for any organization.

Mobile Device Management (MDM): As mobility infiltrates every organization, managing devices for access and configuration is a vital security step. MDM gives MSPs another way to leverage their server expertise to help SMBs control all the new mobile devices on their networks.

Mobile Security: Some RMM providers are bundling tools and apps for protecting individual devices for the most popular mobile platforms.

Secure Wi-Fi: Special software for securing corporate PCs at mobile hot spots ranges from virtual private networks (VPNs) to other protection schemes that can be handy for organizations with employees who take corporate assets on the road.

Web Protection Tools: Software that helps keep browsers from opening dangerous code on questionable Web sites is especially valuable for customers with less-sophisticated users.

End-User Training: Some savvy MSPs enlist their customers' own users in the effort to keep the organization secure by offering end-user training as a service. Giving users a refresher on the basics that they should already know is important. With the constantly evolving threat landscape, though, end-user training is helpful even for users who are already diligent about secure computing practices.

Some of the best opportunities in security right now extend the kind of server-based monitoring that has long been the strength of MSPs. Others fall directly in the category of endpoint-only protection. In either case, most represent a path for traditional MSPs to expand their business into security. All of the services are a way for MSPs to protect their customers, while protecting themselves against a cloud future by expanding their area of expertise. •

Scott Bekker is editor in chief of RCP *magazine.*

Audit
Patch
Monitor
Remote
Antivirus
Backup
Mobile
All in one.

(877) 926-0001
www.kaseya.com/msp

Kaseya empowers you to do more, in less time, with fewer resources—by automating and controlling IT assets remotely, easily and efficiently from one integrated web-based platform. **No commitment, FREE trial or see a live product demo—www.kaseya.com/demo.**

Deploy from a server within your organization or let us host it in our certified cloud environment.

Consider Kaseya and choose the solution hundreds of your peers* already chose:

- 55% of the Top Global MSPs use Kaseya
- 52% of the Top North America MSPs use Kaseya
- 56% of the Top EMEA MSPs use Kaseya
- 72% of the Top AANZ/APAC MSPs use Kaseya

Kaseya