THE IMPACT OF A SECURITY BREACH ON MSPS AND THEIR CLIENTS

SPONSORED BY Bitdefender®

The volume and sophistication of malware has skyrocketed. According to AV-Test.org the number of new and unique malwares identified, per day, has grown from 32,000 in 2009 to over 260,000 in 2014 (more than 10,500 per hour). In today's interconnected world of increasingly sophisticated vulnerabilities, managed service providers can no longer rely on an incomplete or sub-par security strategy to protect their customer from malware that targets an enterprise's diverse array of endpoints.

Rather, MSPs need best-of-breed malware protection as part of a multi-layer approach to safeguard their client's hybrid environments. Without a specialized malware security solution for their physical and virtual technologies, MSPs leave themselves more exposed to the types of malware that last year crippled huge retailers such as Target and Home Depot. Indeed, researchers soon discovered other POS malware, and pundits predict a slew of new ransomware, mobile malware, hard drives, and malware attacks on Internet of Things devices during the next 12 months alone.

Security tools that claim to protect all areas of a network from all points of attack cannot expend the specialized resources necessary to combat hackers focusing on developing next-generation malware. And since malware accounted for 94% of attacks in 2014, it's vital that MSPs choose the best malware protection available rather than rely on a bundled package that tries to do everything.

"There are two types of MSPs," said Terry Hedden, CEO of Cloud Guru. "There are those that keep their service lines very simple that use one or two security products to protect against everything – and deal with the consequences of that approach. And there are those that use layers of security. Think of it like dressing for the cold: You can have one really, really thick layer of clothing or you can put on multiple layers of clothing. Everyone knows the inherent properties of layering of clothing for keeping warm and the same applies to security. Layers keep you more secure than one coating of technology."

Of course, what MSPs put in those layers is critical, Hedden added, since malware creators keep themselves aware of security developers' advances and products. These black hats communicate online, sharing insights and selling tools to circumvent vendors' products, he said. Therefore, in his opinion, MSPs must use solutions specifically designed to combat malware at the endpoint to ensure they're accessing the most sophisticated, current, and tested security technologies. A developer that focuses all its re-

> Think of it like dressing for the cold: You can have one really, really thick layer of clothing or you can put on multiple layers of clothing. Everyone knows the inherent properties of layering of clothing for keeping warm and the same applies to security. Layers keep you more secure than one coating of technology."
>
> — Terry Hedden, CEO of Cloud Guru

sources and intellectual property on protecting the endpoint from malware is more proficient at defending this otherwise vulnerable element than a vendor that spreads its research and development budget across the entire network, he said.

Relying on one vendor for security is perilous. "Having one robust layer of security means you have a single point of failure. If there's a functionality problem or a virus patch that's not deployed as fast as another, you have a situation where customers are vulnerable," said Hedden. "When you have multiple layers, you're not putting all your eggs in one basket. You're deploying across multiple vendors and spreading the risk."

Damage Dangers

While enterprises like Target, Sony, and Anthem typically garner headlines, small and midsize businesses are more likely to be hit – and irreparably damaged – by malware. Approximately 81% of all breaches occur in SMBs. The effect on these smaller organizations, a group that generally includes most managed service providers, can be widespread and devastating.

It costs a business $145 for every lost or stolen record that contains sensitive or confidential data, according to Ponemon's 2014 study, 9% more than the prior year. Given the number of records each MSP oversees via its technology infrastructure agreements, a malware-created disruption, loss, or destruction of internal or client records could quickly add up to millions of dollars. Business for an MSPs unaffected clients could also come to a grinding halt, as investigators – insurance, state, and perhaps federal – research the situation, potentially causing the loss of these unaffected clients, due to service slow downs and/or bad publicity damaging the MSPs reputation. Star employees may move on, seeking to remove themselves from the taint of an affected MSP. Following the breach, an MSP may well be forced to slash fees, advertise heavily, and become involved in extensive – and expensive – public relations initiatives to try and recoup its losses and rebuild the company.

In 2014, the cost a company incurred in lost business following a data breach averaged $3.2 million. Typically, expenses included lost clients, credit monitoring for customers, investigation costs, insurance, and discounts to encourage clients to remain or return. Labor costs represented more than one-fourth of breach recovery costs; employees spent a lot of time recuperating, not serving clients. In addition, cash outlay accounted for 22% of costs, productivity loss represented 21%, and indirect labor 14%.

On average, it takes a business 45 days to resolve a breach at more than $35,000 per day. If employees leave following a breach, it could take longer. HUB International, formed by a group of insurance brokerages, offers a data breach calculator to help companies determine the costs they face after a breach. Elements include the number of affected records; whether the data was centralized; if a class action suit has been filed, and the type of data breached.

Sadly but perhaps unsurprisingly then, six in 10 SMBs that have been breached went out of business.

That was the case for Code Spaces, a code hosting and project MSP that closed its doors in mid-2014 after a "well-orchestrated" DDoS attack against its servers, *SC Magazine* reported. A phishing attack likely caused the attack by giving hackers access to an administrator's credentials.

"This incident is a not-so-subtle reminder that security controls to monitor and manage privileged access need to be taken just as seriously in the cloud as they are in the data center," CEO Ofer Hendler told the publication. "That means limiting access to sensitive systems and data, both IT and business applications, to only those that need it."

Diverting Damage

With free, or more accurately freemium, malware products, MSPs often find costs accrue later, not up-front – but those costs can be heavy. If a business uses a freemium security solution that does not detect a new malware variant that was attached to spam, the company easily could lose confidential or important files, said Liviu Arsene, senior e-threat analyst at Bitdefender, in *InformationWeek.*

"Although a free security solution does have its perks (well, it's free), it might cause more problems than it solves. There's no such thing as a comprehensive and free security solution," Arsene wrote. "Any company, regardless of its size, needs to tackle problems associated with the security of its infrastructure and data. Everything from sandboxing to application whitelisting might be costly and could require some integration work, but at least you'll sleep better at night knowing your company will prosper another day."

MSPs can also sleep better because better endpoint security means better profitability. Providers that use carefully crafted security layers and choose a vendor partner that specializes in malware protection for their endpoints safeguard their organizations and their customers – and improve their bottom lines, said Cloud Guru's Hedden. His recommendation? Implementing Bitdefender's solutions to safeguard the MSP and the client, then marketing this technology as a value-add differentiator.

“Bitdefender gives you a solution you can leverage as a point of differentiation,” Hedden said. “It’s easier to compete with your competitors because your security, your solution, is better, stronger, and different than your competitor’s offering. You cannot compare apples to oranges. Endpoint security is a very substantial portion of the spend an MSP makes to sell its services. Anything you can do to reduce that piece pays for itself in spades. It’s a great way to secure your customer but also reduce your expenses. You’re buying a better solution for your MSP business, then selling the extra security and extra value to your clients so the return on investment is fast and ongoing – in dollars and customer loyalty.”

The End Point Security Answer: Bitdefender for MSPs

When it comes to protection, MSPs have the opportunity to choose a solution that provides the highest level of security for their clients. In the independent AV-Test trials, some of the strictest in the industry, Bitdefender has had the highest average score for protection, performance and usability of all the solutions evaluated. Additionally, no other security vendor integrates with more MSP platforms than Bitdefender, including specialized products for Kaseya, LabTech, N-able and Navarisk.

Bitdefender’s core MSP solution, Cloud Security for MSPs, utilizes a cloud-based console and an advanced set of features:

- Multi-tier and multi-tenant cloud console
- Antimalware, antivirus, two-way firewall, device control, URL security and web control
- Integration with ConnectWise
- Monthly usage based licensing – MSPs are invoiced only for the number of seats protected each month
- Protects physical and virtual endpoints
- Protects Windows desktops, file servers and Macs
- Optimized bandwidth consumption, minimizes external traffic
- Remote deployment and uninstall of competitive solutions
- Service provider can customize branding for the console and reports

“The products easily integrate in our Microsoft environment, they detect unprotected endpoints and clean up malware instantly, and the centralized management makes our job very easy. We can structure it in a way that allows us to manage and train our support staff very easily,” said Rob Bosch, president of iPremise, an MSP that uses Bitdefender.