The New Must-Have for MSPs:
Managed Email Security Services

MSP
Barracuda
Your journey, secured.

BarracudaMSP.com

Table of Contents

Introduction

When it comes to cyber security, there's a simple reason why email is the number one threat vector — and will likely remain that way for the foreseeable future. People open emails. **All it takes is for one person in the organization** to download an attachment or click on a link that takes them to a website infected with malware for **the entire organization to be impacted.**

There are now countless incidents of ransomware requiring organizations to either pay money to cybercriminals to regain access to encrypted files or incur substantial costs recovering data. Most of the time that malware was delivered within an email attachment, cleverly crafted using social engineering techniques capable of tricking the savviest end users into downloading that attachment.

Managed email security services are now table stakes for MSPs. You won't be able to provide your customers with complete protection without it.

> You can't have an email offering that stands still — and neither can your vendors. The threat landscape is simply too dynamic."
> — Brian Babineau »

Understanding email-borne attacks

There are millions of emails sent every day that might contain hidden malware. In 2019, ransomware costs may have hit $170 billion. This number includes not only ransoms paid out but loss in productivity, data and other damages caused the attack. The average amount of ransom more than doubled from $41,198 in Q3 2019 to $84,000 in Q4 2019. Most of those attacks are split evenly between social engineering and reliance on external exploits.

These attacks generally have two primary goals. The first is to deposit malware on an endpoint from which it can spread laterally. The second is a little more insidious. If cybercriminals can trick end users into **revealing their credentials,** it then becomes possible to start sending out email laden with malware **from a legitimate end user email account**.

Ransomware is, of course, the most crippling form of malware shared via email. The ransom being demanded is usually minimal, but at times can be substantial. **The more immediate cost to the business is the downtime** that occurs regardless of whether the ransom is paid. The threat of ransomware is only growing, with recent estimates showing that a ransomware attack will take place every 11 seconds by 2021.

A ransomware attack will take place every 11 seconds by 2021.»

Sizing the MSP opportunity

Most email today is delivered via the cloud, so given what's at risk, it's not surprising to see the cloud-based email security market is expected to reach a value of $1.1 billion by 2023, registering a CAGR of 7.81% during 2018-2023. Obviously, a significant percentage of that revenue is going to be generated by managed service providers (MSPs) that have the expertise required to secure email.

The unemployment rate for cybersecurity is a negative number. Small to medium-sized organizations are especially hard pressed when it comes to finding and retaining cybersecurity expertise. With email the most critical form of business communication there is, most of these organizations will be looking to rely on external expertise to secure their email systems.

The cloud-based email security market is expected to reach a value of $1.1 billion by 2023.»

New email expectations for MSPs

The primary mission of any MSP focusing on cybersecurity is to protect and serve. Organizations of all sizes now expect their MSPs to be able to secure their environment as part of a larger portfolio of services. When it comes to email, that means being able to not only secure messages, but ensure they're **backed up and archived.**

MSPs are specifically being asked to **filter inbound email to identify viruses, prevent phishing attacks, and eliminate spam.** Outbound filtering extends those capabilities by both preventing data leakage and automatically encrypting sensitive data. **Advanced Threat Protection (ATP)** blocks advanced zero-hour attacks from cybercriminals.

Critical capabilities required include sender virus scanning, spam scoring, real-time intent analysis, URL link protection, reputation checks, sender spoof protection, and multiple domain validation techniques. MSPs are also expected to be able to block outbound spam and viruses, preventing end users or other infected clients from inadvertently sending malicious email in addition to keeping mail server IP addresses and domains from being listed on spam block lists.

Additionally, machine learning and behavioral analytics combined with a CPU-emulation based sandbox to provide the most comprehensive threat prevention possible without introducing any latency will soon be viewed as table stakes.

Compliance requirements

Finally, MSPs are being asked to create and enforce compliance policies to prevent sensitive data such as credit card numbers, social security numbers, HIPAA data, customer lists, and other private information from being sent by email. Policies should also be able to automatically encrypt, quarantine, or even block certain outbound emails based on their content, sender, or recipient.

New regulations such as the **General Data Protection Rule (GDPR)** put in place by the European Union make being able to manage and, when required, delete all personally identifiable information (PII), are critical capabilities that present new compliance challenges, including reporting breaches to relevant authorities within three days of their occurrence.

The challenge doesn't stop there. **Cloud-based archiving** makes it possible to comply with any number of regulations or court orders that may require an organization to prove what message was sent when.

Cloud-based backup is now needed to not only protect data from being accidentally or maliciously deleted, but also provide a pristine copy of the data that can be stored in the event of a ransomware attack, and that encrypts an organization's data.

Organizations now expect their MSPs to be able to back up and archive messages in their email inbox.»

Building a unified defense

Customers today expect cybersecurity and data protection to be unified. If a breach involving ransomware is detected, they want a recovery process to implemented with all due haste to prevent as much data as possible from being potentially lost.

Delivering those services requires investments in security and network operations centers that are beyond the amount of capital most MSPs can ever hope to raise. And, even if they can raise the capital, chances are high that IT infrastructure is not the best use of those funds when cloud services that MSPs can provide under their own brand are readily available. The only thing more challenging than initially being able to provide that level integration is **maintaining it on a 24 x 7 basis.**

Customers will want to be certain that whoever is managing their business communications —regardless of whether they are relying on Microsoft Office 365, Microsoft Exchange, or G Suite from Google—has the **technical and financial resources required to deliver** on that promise both today and well into the future. Alas, the skills needed to integrate security and data protection services are not easy find, so MSPs need to prioritize investments.

Customers today expect cybersecurity and data protection to be unified by their MSP.»

Training-as-a-Service

One of the most overlooked aspects of providing a managed security service is the **investments made in personnel training and awareness can pay for themselves.** Every piece of malware that doesn't get downloaded is one less incident an MSP needs to investigate. The opportunity to **train end users to recognize phishing attacks creates a unique win-win situation for the MSP**. The MSP can charge for a service that effectively lowers the risk associated with delivering a managed security service.

In fact, **end-users are now the first line of defense in a layered approach to providing cybersecurity.** Making sure end users can effectively play that role requires training using, for example, a Software-asa-Service (SaaS) application through which MSPs can generate multiple types of messages that mimic a phishing attack.

MSPs can rely on either a click-rate metric employed to track cyber-resiliency by counting how many times employees click on a URL or download a piece of content they shouldn't, or they can use more advanced gamification techniques to provide a series of incentives to employees that identify the highest number of attacks. The latter approach reduces the level of hostility that often exists between end users trying to perform a task and the cybersecurity teams trying to protect them.

Regardless of the approach used, end-users that click on links in fake messages or download attachments via bogus links clearly need more training. MSPs can then **provide that training** to improve the **overall cybersecurity resiliency of the organization** in a way that also increases the overall revenue generated.

Additional security opportunities

Email security and associated training opportunities are only one element of a layered approach to cybersecurity. Once an MSP starts securing email, it's only a short leap to also **managing firewalls and endpoint protection software**, along with a broad range of other cybersecurity technologies.

MSPs are also going to be in a unique position to **leverage security intelligence applications** to proactively engage in **threat hunting**. Because of the increased sophistication of cybersecurity attacks, MSPs should assume that malware is lurking somewhere in the applications and systems they are managing on behalf of their customers.

Threat hunting technologies make it simpler to proactively locate malware before it gets activated. Security intelligence services, meanwhile, scour the Internet to not only identify new and emerging threats in the Dark Web, but also find out if an organization's data is for sale somewhere that it shouldn't be.

There is almost no end to the number of additional managed security services that can be provided. Each MSP will need to carefully balance **the cost of acquiring the expertise** required to deliver those services against the **potential revenue they generate.** But whatever services an MSP decides to ultimately provide, any effort to offer cybersecurity services needs to start with email threat vectors that are the most widely exploited.

Challenges and considerations

Providing a managed security service is not for the faint of heart. There is no such thing as perfect security, so it's inevitable there will be no shortage of incidents to investigate and, unfortunately, malware infestations to clean up.

All those activities are time-consuming, so savvy MSPs need to factor in the **cost of labor** associated with performing those tasks. Finding IT professionals that have the appropriate level of expertise to implement a cybersecurity service and remove malware when necessary is not easy, especially when all the nuances associated with servicing various vertical industries is factored in. Not only is cybersecurity expertise scarce, technicians that have it rank among the **highest paid professionals** in the channel and industry.

MSPs in many cases will need to be prepared to **assume the cost of training their own** cybersecurity professionals simply because the cost of hiring and retaining someone with existing skills will be prohibitive. For that reason, MSPs need to carefully evaluate the services being provided. The more functionality that is baked into the platform they employ, the greater the chance there is for a mere IT mortal to be able to manage it.

> Not only is cybersecurity expertise scarce, those with it rank among the highest paid in the industry.»

It's not all bad news

The good news is **advances in automation are steadily lowering the cost and complexity** of providing Cybersecurity-as-a-Service. But, automation also comes at a cost. Going forward, it's already apparent that next-generation cybersecurity solutions are going to make extensive use of machine and deep learning algorithms to drive artificial intelligence.

Those algorithms, however, are only effective when they have a massive amount of data to analyze, which creates another compelling reason for MSPs to **partner with a vendor that has built a cloud service.** Most MSPs on their own are not likely to be able to aggregate the amount of data required to build an effective AI model capable of automating cybersecurity processes.

In fact, AI is emerging as a primary reason why MSPs should rely on a **cloud service to provide an email security service**. It's already complex and costly enough to set up an email security service using on-premises software and hardware. Collecting and storing that data is much simpler and less costly for a vendor that provides email security services optimized to meet the **specific needs of an MSP**.

MSPs need a vendor to help them build an effective automated cybersecurity process.»

Demonstrating value of email security services

Finally, MSPs need make sure they can **show value for the cybersecurity services they provide**. Dashboards infused with advanced analytics are critical because they can be used to **generate reports that demonstrate scale** of the services being provided to their clients.

Too often, customers evaluate the quality of a service solely on the **number of negative experiences** they've had. That can be problematic when it comes to cybersecurity services because the value of the service is inherently tied to preventing something from happening. In the absence of tangible evidence of the amount of activity being executed on their behalf, there's a natural tendency to not value that service. Inevitably, things that are not valued become subject to downward pricing pressure.

It's critical for MSPs to **set expectations** and then be able to back up their claims with **hard evidence**. Given the nature of human foibles, there will always be some form of cybersecurity incident that needs to be addressed. The critical thing is to make sure those issues are not only promptly addressed, but also that they are **not the only thing the customers remember** about the quality of the services being provided.

MSPs must take care

MSPs should also be selective when it comes to engaging a customer in the first place. Organizations that rely on, for example, older versions of Windows are going to be much more expensive to support than those that have invested in modern applications and IT equipment. Older versions of applications are subject to many more known vulnerabilities that result in the MSP taking on a lot of responsibility for patch management.

Most malware infestations can usually be traced to older applications and systems that have not been properly maintained. In fact, organizations relying on older versions of applications and antiquated systems would be indicative of an organization that doesn't really value IT as a strategic investment worth protecting.

Chances are high in those circumstances that the customer is going to continually look to reduce the cost of cybersecurity services by demanding more resources to be delivered at an increasingly lower price point. Rather than being put in the awkward position of firing that client one day, MSPs should pass on those types of opportunities in the first place.

Most malware infestations can be traced to older systems that have not been properly maintained.»

Conclusion

It's hard to think of any new IT project that is being launched without addressing cybersecurity issues to one degree or another up front. If MSPs expect to be considered relevant going forward, they need to be able to **include managed security services as part of their offerings** by either providing that capability themselves or partnering with another service provider that does.

Customers are not going to ask MSPs that can't secure communication processes—around which their business operates—to manage business processes that are wrapped around their emails. That's especially true when so many organizations are now focused on digital business transformation. Given how much of their daily business is conducted via electronic messages these days, most organizations would prefer to lose phone service before having email offline.

To gain the expertise required to provide email security services, MSPs need to partner with an **IT vendor that regularly demonstrates that they are making the right cybersecurity investments** on their behalf. The fundamental name of the cybersecurity game is **prevention.** The less malware that finds its way into an IT environment, the higher the margins a managed service provider is going to enjoy. Every minute spent remediating a vulnerability or, worse yet, cleaning up after a malware infestation directly impacts the bottom line.

They say an ounce of prevention is worth a pound of cure. In the case of cybersecurity, that pound of cure is worth thousands of dollars in both costs to the MSP and potential losses for their clients. If MSPs want to remain competitive and successful, they need to **address their customers' cybersecurity needs,** particularly around **email protection**.

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.

MSP Barracuda®
Your journey, secured.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.
@BarracudaMSP | LinkedIn: BarracudaMSP | smartermsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com