ConversationalGeek®

Conversational Email Security for MSPs

By Nick Cavalancia (Microsoft MVP and CEO of Conversational Geek)

In this book, you will learn:

- How to explain the real cost of cyberattacks to SMB owners
- The different types of attack SMBs need to defend against
- Why a layered approach works for both SMBs and MSPs

3rd Edition

Sponsored by
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.

For more details visit
www.barracudamsp.com

Conversational Email Security for MSPs

By Nick Cavalancia

ConversationalGeek®

Conversational Email Security for MSPs

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Nick Cavalancia
Project/Copy Editor:	Ian Whiteling
Content Reviewer(s):	Morgan Pratt
	Doris Au

Note from the Author

Thank you for downloading this eBook.

At Conversational Geek, we know that helping to protect their customers' is a key priority for MSPs. However, getting the message across to SMBs that they need to invest in additional layers of protection to do this, can be a significant challenge – either they think they don't need it as they don't see themselves as a target or they think they can't afford it.

In *Conversational Email Security for MSPs* we'll look at why email security lies at the heart of any data protection strategy, and how MSPs can provide a comprehensive layered email security strategy.

The idea is that this eBook isn't just another book about email threats and security… it's a guide to MSP success. In the following pages you'll learn how you can not only package different layers of email security, but also how you can position it and sell it to your customers effectively. Ultimately, this is about helping you to not only protect your customers' data but also grow your business.

Nick Cavalancia
4-time Microsoft MVP and
CEO of Conversational Geek

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Greetings. Within these boxes I can share just about anything on the subject at hand.

Read ’em!

Email Security and the MSP

"Don't click that! Your name isn't even Pete!"

Managing cybersecurity has always been a challenge for your customers. With small and medium-sized businesses (SMBs) experiencing nearly 3.5 times the number of email-based attacks as the enterprise[1], SMBs have unsuccessfully attempted to defend against increasingly sophisticated and more frequent attacks on their own – all while bad actors put their efforts into developing techniques and malware that can bypass the very solutions that were put in place to keep them

[1] Barracuda, *Spear Phishing: Top Threats and Trends* (2023)

out. On top of this, for many companies, security budgets have shrunk, which is further restricting their ability to effectively fight back.

Unsurprisingly, cybercriminals capitalize on this "opportunity". Last year, the SMB saw a more than 50% increase in the number of experienced attacks, resulting in 36% of all SMBs having been a target[2].

As a result, security has become an even bigger challenge for businesses.

A problem shared…

And it isn't just a problem that is exclusive to large organizations. Cyberattacks can – and do – happen to businesses of all sizes and industries. Although the big companies tend to grab the headlines, SMBs shouldn't be lulled into a false sense of security and assume they're not a target. The reality is that couldn't be further from the truth; on average, 51% of SMBs feel that cyberattacks are becoming more frequent[3], with 94% of them having experienced an attack[4].

Cybercrime is big business and a massive (and rapidly growing) global problem. When the total cost of cyberattacks around the world is added to the financial outlay of putting security measures in place, the cost of cybercrime by 2025 is expected to be more than $10.5 trillion[5].

---

[2] Hiscox, *Cyber Readiness Report* (2023)

[3] VadeSecure, *SMB Cybersecurity Landscape Report* (2023)

[4] Vanson Bourne, *The State of SMB Cybersecurity in 2024* (2024)

[5] Cybersecurity Ventures, *Cyberwarfare in the C-Suite* (2024)

Why SMBs need to take note

SMBs are attractive to attackers for two key reasons:

1. **They can be financially rewarding** – SMBs often have access to valuable information, which can be lucrative for hackers – whether that is personal data (anything from credit card numbers to people's personal information, or from personal emails to access to someone's log-on credentials). They can also act as the gateway to bigger organizations.

It doesn't matter how big or small your company is, money talks for cyber criminals. The 2023 Verizon Data Breach Investigations Report found that financial motives were behind 97% of attacks on SMBs of under 1,000 employees.

2. **They are often an easy target**
   SMBs lack resources and skillsets to implement a proper cybersecurity strategy as 76% of SMBs admit they don't have the skills in-house to properly deal with a cyber-security incident[4]. This is exemplified by the fact that only 45% of SMBs have a written incident response plan![5]4 This may be due to only 45% of SMBs believing their businesses are a likely target for cybercriminals[4]. On top of this, those that do get hacked aren't getting any better at remediating the problem, as 75% of SMBs hit by a ransomware attack would only survive between 3 and 7 days[6].

[6] CyberCatch, *SMB Ransomware Survey* (2023)

3. Email makes it easy
   The bad guys know the value of email both as a delivery mechanism for malicious content and as a means of gaining access to a victim's network – as demonstrated by 80% of all data breaches involving a combination of phishing and credential misuse[7]. The massive adoption of Microsoft 365 (despite Microsoft's efforts to keep it free of cyberattacks) makes it an obvious target for attacks that involve malware payloads that still find their way to a user's Inbox, as well as those attacks that focus on compromising online credentials as part of a larger attack effort.

The problem is being further exacerbated for SMBs by the fact that IT infrastructure is becoming more complex as most of them are going through a digital transformation to accommodate the changing working landscape. For many SMBs, managing the security infrastructure is becoming almost overwhelming. Bad news for companies but a great opportunity for MSPs to jump in and help.

The cost of ignoring cybersecurity

The harsh reality is that there are serious financial implications for SMBs that think they can run the cybersecurity gauntlet. Remediating cyberattacks comes with a material price tag, regardless of how small the SMB is, the average cost of all cyber incidents and/or breaches experienced by an SMB is material. Some 20% of SMBs report a cost of over $100,000, 54% report a cost of between $10,000 and $100,000, and 11% report a cost of less than $10,000[4].

But it doesn't stop there, a successful attack can have a tremendous impact on the SMB beyond the obvious financial one. Of the SMBs that have experienced a cyberattack, 46% of

[7] Verizon, *Data Breach Investigations Report* (2024)

them suffer downtime that disrupts the business, 30% experience financial loss, and 12% reputational damage[4]. Indeed, the impact can be so bad that it can drive companies out of business. Breaches also have an impact on MSPs themselves both in terms of the time taken on clean-up operations to get systems back up and running, as well as potential for having their reputation damaged by association.

The answer of course is to try and stop the bad guys from getting in.

And how are the bad guys getting in? *Email.*

Email should be front and center for security

Email remains the single most popular initial attack vector. Whether you're talking about ransomware, data breaches, business email compromise, digital fraud, or espionage, no other attack vector gives a threat actor internal access to a victim network with a compromised endpoint to act as their foothold.

And it makes perfect sense – it's estimated that roughly 322 billion emails will be sent and received this year. Not only does the sheer volume of correspondence make email an obvious first point of attack, it's also the perfect delivery medium for malware as it can get malicious content, code, links, and attachments directly to a specific employee inside the proverbial "walls" of an organization.

Email has always played a critical role in business communications and operations – and possibly even more so now given the distributed nature of our working conditions. So, it's equally critical that as part of any security service you offer to customers there should be a strong email security strategy.

While you very likely already have your customer's email on one of the major cloud email platforms, (such as Microsoft 365 or Gmail), this doesn't mean their email (and, therefore, their

organization) is fully protected from cyberattack – it only really addresses one part of the problem. I'll look at that in more detail a little later.

In today's rapidly evolving environment, traditional email gateway security solutions aren't enough to protect businesses anymore. You must also effectively defend against sophisticated email threats that are often able to bypass many defenses by using malware-less techniques, including impersonation, social engineering, and fraud, to penetrate networks and wreak havoc.

With email security, there is not really one box you can check.

To protect your SMB customers, you must deploy an email security strategy that is layered in approach that protects email data at the gateway, the endpoint, the email client, and when it finally reaches the user.

To craft an appropriate strategy, let's first take a look at the various types of threat tactics and methods that are used as part of an email-based attack.

Too many threats, too little time

The email and phishing threats faced by organizations today vary greatly in complexity, volume, and the impact they have on businesses and their employees. One of the biggest problems for SMBs and MSPs is that they have so many email-born threats that they need to defend against.

These threats can be broken down into several distinct categories:

1. Spam

Spam email is probably the most basic and most common threat that companies face, but it's also one of the most pernicious. It's often an unsophisticated attack sent without

regard to the recipient's identity. The email is used to get people to either download infected attachments or drive the recipient to click on an infected phishing link. And it does this at huge scale. The impact of spam comes at an estimated cost of around $20 billion per year in losses, due to the reduced productivity created by flooding inboxes with junk mail and the impact on server traffic to process messages.

2. Malware

Malware is the malicious software that often represents the starting point for any cyberattack. It is specifically designed to cause damage to technical assets, disrupt operations, exfiltrate data, or otherwise gain access to a remote system. Some of the most common forms of malware include viruses, Trojans, spyware, and worms. However, the most common form of malware is ransomware, whereby the attacker immediately locks data and other critical files on a user's computer or company network until a ransom is paid. Ransomware can cripple day-to-day operations, cause chaos, and result in financial losses from downtime, ransom payments, recovery costs, and other unbudgeted and unanticipated expenses.

3. Data Exfiltration

Data exfiltration (also referred to as data extrusion, data exportation, data leaks, data leakage, data loss, and data theft) describes the unauthorized transfer of data off a computer or other device. This type of attack very often requires the attacker to dupe a user into either handing over their access credentials or downloading a piece of malware. While some ransomware attacks are indiscriminate, data exfiltration attacks are typically highly targeted, with the objective of gaining access to a specific network or machine to locate and gain access to certain kinds of data. Email can serve the purpose of initial infection and providing malicious access, as well as the vehicle by which data is exfiltrated.

4. Phishing

Phishing refers to emails that attempt to trick an end user into believing the message is from a trusted person or organization to get them to take an action such as disclosing credentials, wiring money, or logging into a legitimate account on an attacker's behalf.

As previously mentioned, 80% of data breaches experienced involve phishing[11]. Phishing has also remained one of the top initial attack vector in ransomware attacks over the past 5 years[8]. Phishing can just as easily lead to a significant number of security incidents that may not actually result in data breaches, but cause network damage and/or downtime.

Phishing is a broad category and can be broken down further into a series of sub-categories:

- *URL Phishing* – In this type of phishing attack, cybercriminals try to obtain sensitive information for malicious use, such as usernames, passwords, or banking details. They do this by directing their victims to a spoofed website – for example, one that looks like a legitimate Microsoft 365 logon page – to trick them into entering sensitive information.

- *Scamming* – With scamming phishing emails, cybercriminals attempt to steal the victim's identity by tricking them into disclosing personal information. Some classic examples of scamming emails include fake job postings, investment opportunities, inheritance notifications, lottery prizes, and fund transfers. It's also common for scammers to try to

[8] Coveware, *Quarterly Ransomware Reports* (2024)

monetize tragedies, such as hurricanes, the COVID-19 crisis, and other disasters.

- *Spear Phishing* – Spear phishing is a highly personalized and targeted form of attack. Cybercriminals will research their targets and craft carefully designed messages, often impersonating a trusted colleague, website, or business. The ultimate goal of these attacks is to steal sensitive information, such as login credentials or financial details, which are then used to commit fraud, identity theft, and other crimes. It is also very common for cybercriminals to use social-engineering tactics in their spear phishing attacks, including urgency, brevity, and pressure, to increase the likelihood of success.

- *Lateral Phishing* – In a lateral phishing attack, the bad guys use recently hijacked accounts to send phishing emails to all the contacts on that account, such as colleagues and contacts at external organizations. This enables them to spread the attack more broadly. Because these attacks come from a legitimate email account and appear to be from a trusted colleague or partner, they tend to have a high success rate. As you can imagine, these attacks can be extremely damaging to a business's brand reputation, especially if they lead to additional widespread attacks in other organizations.

5. Impersonation

Impersonation has been going on for decades. Confidence tricksters have long tried to get people to part with money and information under false pretenses. Email has just made this much more wide-spread and much easier to do at scale. Similar to phishing, it's a broad superset of attacks – in fact they normally go hand in hand with phishing. Impersonation can be broken down into a number of sub sections:

- *Domain Impersonation* – This refers to cybercriminals using a lookalike domain to fool people into believing they are visiting (or receiving emails from) a real brand, vendor, or partner's website. Domain impersonation is often used by hackers as part of a conversation-hijacking attack (see below). In preparation for an attack, cybercriminals register or buy the impersonating domain, often these will have one or more letters changed from the legitimate domain and are often really hard to spot (e.g., citíbank.com or microsofts.com).

- *Brand Impersonation* – Brand impersonation is designed to masquerade as a company or a brand to trick email recipients into responding and disclosing data, such as their personal log-in details or other sensitive information like credit card details or social security number. They tend to focus on big brands with huge customers bases, and some of the most high-profile brand impersonation campaigns have included Microsoft, UPS, Netflix, Amazon, and Apple. Often these emails can be very difficult to spot as their content is well-crafted to keep up the pretense and fool the recipient. Similar to spear phishing attacks, they can also use social-engineering techniques to worry the recipient and increase their chances of being successful.

- *Service Impersonation* – Service impersonation is similar to brand impersonation, but focusses on common services that people use. Microsoft is the most impersonated brand in these types of attacks, probably due to Microsoft 365 credentials being high value because they allow hackers to penetrate a wide range of different organizations and launch additional attacks.

- *Extortion* – Extortion scams, including sextortion, are becoming increasing frequent and more sophisticated, and are bypassing email gateways. In these scams, cybercriminals leverage older usernames and passwords stolen in data breaches to contact and try to trick victims into giving them money. The scammers often claim to have a compromising video, allegedly recorded on the victim's computer, and threaten to share it with all their contacts unless they pay a ransom. Understandably, these types of attacks are often left unreported due to the intentionally embarrassing and sensitive nature of the threats.

- *Business Email Compromise (BEC)* – In BEC attacks, the bad guys send emails impersonating an employee in the organization with the specific intent of defrauding the company, its employees, customers, or partners. In most cases, attackers will focus their attention on employees with access to the company's finances or personal information, tricking individuals into performing wire transfers or disclosing sensitive information. Again, these attacks will often use social-engineering tactics and compromised accounts, and don't tend to include attachments or links making them hard to detect.

It may be easy to think you're too savvy to be caught in a BEC scam, but the list of victims is pretty extensive, and a quick search of the FBI's Internet Crime Compliance Center shows that in 2023, BEC cost just over $2.9 billion!

- *Account Takeover* – In this form of attack a malicious third party successfully gains access to a user's account credentials. Often this will come as the result of a

brand impersonation, social engineering, or phishing attack where the intent is to get the user to provide their logon credentials. Once the account is compromised, the bad guys monitor email communications and track business activity to learn how the company operates, the email signatures they use, and the way financial transactions are handled. They can also harvest additional login credentials for other accounts by using the initially compromised email account to send malicious emails to co-workers. Ultimately, any information they gain can then be used to help them launch other attacks to gain financial benefit – see Conversation Hijacking below.

- *Conversation Hijacking* – In this type of attack, the bad guys insert themselves into existing business conversations or initiate new conversations based on information they've gathered from compromised email accounts, often as the result of an account takeover attack. Then they go on to use this information to steal money or personal information. In one well-publicized example, Shark Tank's Barbara Corcoran lost nearly $400,000 due to a phishing scam. Scammers tricked her bookkeeper using email-domain impersonation, and by sending a bill that appeared to come from her assistant. By the time Corcoran's team realized something was wrong, the money had already been transferred to the scammers.

The Rise of AI in Cyberattacks

The practical execution of any of the threat types mentioned has only become faster, easier, and more impactful for the cybercriminal through the use of AI in a number of ways:

- More Credible Content – the simple use of AI tools like ChatGPT have empowered attackers to write

believable and professional-sounding content in a target victim's native language.

- Faster Creation of Malicious Tools – new AI-based toolsets like *FraudGPT* and *WormGPT* make writing malicious code, creating undetectable malware, creating phishing pages, and building hacking tools as simple as writing query prompts.

- Creation of Deepfake Content – What started a few years ago as technology designed to mimic someone's voice now has become its own malicious industry, with AI being used to generate deepfake audio, video, social media posts, and more used to convince victims that the content is actually created by a celebrity, their boss, etc. in an effort to motivate the victim to perform a desired malicious action on behalf of the attacker.

Multiple layers for multiple types of attack

As you can see, the web of threats that companies must deal with is extensive. Of course, it would be a lot easier to defend against email attacks if we always knew which attack vectors an attacker was going to use, or even if they were just going to use one type of attack and the time when attacks are to be deployed. The problem is that email-based attacks today simply don't use just one of the threat techniques listed above, or when the attack takes place; they will use a combination of them – particularly for high-value targets. This helps them to establish credibility, build recipient confidence, and ultimately lower the human defenses before making their final move.

As an MSP, it's likely that you already have some form of security service offering in place. But is it enough to stop all these different types of attack? In today's rapidly evolving environment, traditional email security solutions that focus

solely on defending just the gateway or the endpoint no longer offer businesses the protection they need. You need to be able to effectively defend against sophisticated email threats, around the clock that have more often than not been evolved to bypass traditional defenses.

This requires organizations to set up different layers of protection that focus on various levels throughout the email journey. Every business needs to deploy the right combination of technologies and people need to have effective email protection. Deploying a defense-in-depth layered methodology in this way ensures that if one security measure doesn't stop an attack, another one will. This approach allows you to effectively come at the problem from different angles.

For example, focusing on the gateway is a great way to block high-volume attacks. Technologies that focus here are unquestionably the foundation stone of solid email security. Good gateway protection will enable you to detect and block a large number of malicious messages, including spam, large-scale phishing attacks, malware, viruses, and zero-day attacks. If left unchecked, these attacks can go on to wreak havoc inside your organization, impacting productivity and infecting machines.

However, gateway defenses are unlikely to pick up a much more nuanced or targeted attack, like a business email compromise attack that relies solely on impersonation and social engineering to trick its victim. To combat this, you need to look at deploying an API-based inbox defense that incorporates artificial intelligence (AI) and machine learning (ML) that is backed by 24x7 365 SOC support and remediation guidance, enabling you to use historical and internal email communication to spot anomalies in behavior and protect your users against those highly targeted attacks that slip past gateways.

Simply put, to protect your SMB customers, you must deploy a multilayered email security solution that not only protects the customer's gateway, but also their users, their data, and their email environment.

Building a modern layered email security strategy

So, what does all this mean in practice?

Let's look at where your modern email protection strategy should focus in order to provide the most comprehensive protection for your customers. To do this, we're going to break things down in three distinct areas that represent the path taken by malicious email content: the *Gateway*, the *Inbox*, and finally the *User*.

Protect the Gateway

Provide protection against: Spam, Malware, Phishing, and Spear phishing.

The Gateway can refer to an implemented email security gateway or simply the logical perimeter of the path that email takes to be delivered to your customer's environment. At this layer in the defense, the goal is to stop inbound malicious email content from ever getting in. Some of the technologies you could have in place include:

- *DMARC Reporting* – Account Takeover is a rapidly emerging problem for many companies, where legitimate accounts are taken over and then used by bad actors to send out spam and phishing emails. As mentioned above, it's something that is widely used in impersonation attacks. By creating and enforcing DMARC (Domain-based Message Authentication Reporting and Conformance) policies, companies can authenticate and track email traffic and effectively prevent domain impersonation attacks. However, setting up DMARC policies is far from straightforward and is one of the biggest hurdles to its roll out – in fact a recent study of the top 10 million domains, only 12.33% use DMARC[9]. If you can provide and manage this service for your customers, you are taking a big step towards securing them against some of the more sophisticated email attacks.

- *An Email Gateway* – This includes using traditional techniques such as signature scanning defenses as well

9. Spam Resource, *DMARC Adoption Rates* (2024)

as other more advanced technologies like a virtual sandbox for analysis and detonation of attachments, checking malicious links, and virus scanning attachments.

- *AI-based Detection Technologies* – Gateways should be employing tools that leverage AI to enhance detection capabilities, helping to improve detection rates and mitigating the risk of attack.

Protect the Inbox

Provide protection against: Malware, Domain Spoofing, Phishing, Spear phishing, Brand impersonation, BEC, Blackmail, and Data Exfiltration.

You should assume some small percentage of malicious email will get through your gateway defenses. So, there needs to be a number of different technologies deployed at the inbox level if you want to provide a well-rounded email security offering for your customers. These include:

- *AI-based Detection Technologies* – In addition to AI at the gateway, server- and endpoint-based solutions leveraging AI can be used to provide a behavioral baseline that can predict how likely an email is to be from the person it purports to be from. This technology provides MSPs with a powerful tool in the fight against sophisticated, socially engineered and targeted attacks like Business Email Compromise and Account Takeover.

- *Resiliency* – As an additional layer of protection, should the worst happen, MSPs need to provide customers with protection against both accidental and malicious

deletion of email data, as well as the ability to securely backup and archive emails. This ensures that not only can you recover lost data if an account is compromised but also meet compliance requirements in terms of being able to access old emails, without having a major impact on storage requirements.

- *Continuity* – Although connected to resiliency, I've broken out continuity as a separate issue as it is an important category in its own right and should certainly be considered as such when looking at email protection. In the event of any sort of outage – whether that is triggered by a security event or an external event such as server downtime – businesses need to be able to continue to operate. If, as an MSP, you can provide your customers with what effectively amounts to a backup email system you are able to ensure they can continue to send and receive email in the event of their main service going offline. Naturally, this system should provide the same level of security (from encryption to scanning) as their existing email system.

Protect the User

Provide protection at all levels of attack.

You see the news stories about successful cyberattacks that leveraged email as the initial attack vector. That means a malicious email got past any gateway and inbox defenses. It also means it was convincing enough that a user fell for impersonation and social engineering tactics. Your customer's users represent the last line of defense against malicious emails. So, it's critical to turn them from a liability into a security layer. If you can elevate the end users' vigilance

and understanding about what to look out for in any sort of email-borne attack, then you can make them a part of the security solution.

This can be done through security awareness training, which focuses on explaining what email-borne threats are and why users need to be able to spot them (often, end users will assume that security is someone else's problem). If they know what to look out for and be aware of – for example, a request coming in from someone that seems out of the ordinary or emails that appear atypical in terms of language or spelling – they can at least check before actioning them or clicking on any links contained within the email.

This sort of education is also best followed up with phishing testing, where you as the MSP can launch your own dummy phishing attacks on the business – obviously with customer buy-in – to see which users fall for the faux-malicious email content and take action based on the email's contents. Any users actually caught out by this can then be re-educated by looking at what they did wrong and helped to understand how to better detect malicious emails in future.

Building out a service

Again, this probably all sounds great in principle, but as an MSP where do you start if you want to put it into practice?

As I mentioned earlier, think about this in layers – both from a security *and* a service perspective. How you apply those very same security layers to an offering can depend on the nature of your customer's business, the sensitivity of their data, and their likelihood to be the target of an attack. While this may seem like it's contradicting what I said right at the beginning of this book, if your customer works for a bunch of government clients or handles investment data for high-net-worth individuals, then they are going to want to deploy the deepest level of protection to secure their data.

Having said that there are obvious places to start.

Remember most attacks start with an email. This means that if your customers are serious about security and protecting their data, having a solid gateway protection in place is essential.

Beyond that, the most obvious thing that companies understand is the importance of being able to recover in the event of an attack, or indeed any sort of outage. Resiliency and continuity are going to be a relatively easy sell.

A third area of what you might refer to as email essentials, revolves around empowering the user to be part of solution and not part of the problem. This means ongoing security awareness training – the emphasis here is on "ongoing". Security in any of its incarnations is not a set-and-forget process, it requires continual reinforcement as well as updating in light of new threats. End users should not simply be given an email security questionnaire as part of their onboarding and then left to get on with it. Things like regular quizzes, online learning tools, and email updates are important parts of the equation. As are phishing simulation attacks, as I mentioned

earlier. These can be a crucial tool for helping you and your customer understand exactly who within the organization is putting your data at risk and, therefore, needs more training.

With the essentials in place, you can then look at some of the more complex and cutting-edge technologies that can be deployed to provide a deeper level of email security protection. This can include advanced AI technologies for behavioral benchmarking and DMARC reporting and authentication, as well as advanced technologies at the gateway level, such as sandboxing.

To capture this, you should consider offering email security in tiers within your managed services provision. Here's an example of how this could play out.

- Bronze-level service
  Include the basics, such as virus scanning and filtering, spam filtering, backup, archiving, continuity, and impersonation protection

- Silver-level service
  Everything in the Bronze level, plus domain fraud protection with AI defense and DMARC reporting, and comprehensive user awareness training.

- Gold-level service
  Everything in the Bronze and Silver levels, plus 24/7/365 global Security Operations Center for complete security coverage.

Mind you, this is just *one* of a myriad of ways you could choose to package your services; it will depend on your customer's needs, your industry focus, the typical customer size, etc. By splitting things out in a logical way, you are providing yourself with the best opportunity to effectively manage your customers' email security challenges. On top of this, with SMBs being very cost sensitive, you're providing a solid and relatable platform from which to sell your services.

The Big Takeaways

Email represents the single biggest security threat to SMBs, yet they are often least prepared for these attacks. And with the security landscape changing and becoming more sophisticated on an almost daily basis, it's not difficult to see why so many companies in the SMB market are tempted to sweep email security under the carpet and either ignore or, or at very least not give it the attention it deserves. Yet, with such a high proportion of cyberattacks starting with an email, email security really deserves to be front and center for any security strategy and, therefore is an opportunity for you as an MSP.

But it can be difficult to know where to start. With so many different email-borne threats in the wild, operating at various levels of sophistication, the only way MSPs can provide ample protection against such threats is to take a multi-level approach to email security. With your approach comprehensively addressing email-based threats from the gateway to the inbox, and ultimately the end users themselves, you'll be in the perfect position to help these companies understand the threats (and real-world impacts) they face, as well as to provide them with a structured approach to email security that augments your customer's overall security stance.

Sponsor Chapter: Ensuring your customers' email is protected with Barracuda MSP

In the face of growing cybersecurity threats to SMBs, today's MSPs need a multi-layered email security strategy to help support their customers in protecting their data. To streamline service delivery, maximize profit potential, and boost overall growth, MSPs should consider consolidating vendor relationships where possible. This simplifies training, implementation, support, and troubleshooting, among other benefits.

Barracuda MSP, the MSP-dedicated business unit of Barracuda Networks, provides industry-leading security and data protection via its purpose-built MSP management platforms. A core part of this is its comprehensive email protection solutions, which enable MSPs to secure their customers' email and safeguard end-users with a range of different tools, from email security awareness training to powerful AI-based spear-phishing protection solutions.

This is the driving force behind Barracuda MSP's email protection solution.

By taking a holistic view of email protection, Barracuda MSP's layered email security solutions provide MSPs with an all-encompassing suite of solutions that gives them the power to detect, prevent, and remediate email-borne attacks.

Modern email protection, the Barracuda way

In today's hybrid work environment, email security must extend past protecting just the mailbox to the user and their data as well. Barracuda's cloud-based email protection solutions work together to tackle the challenge of helping MSPs secure their customers' email from a mailbox, user, and data perspective.

It all starts with the mailbox. Whether you've got your customers on a cloud service like Microsoft 365 or Google Workspace, have them running a dedicated on-premises solution, or even a hybrid configuration, the reality is the same: built-in security measures are often good, but not enough to ensure complete protection. This is why Barracuda MSP's email security solutions look at the different layers of email security, including gateway defenses, resiliency, API inbox defense, access, and awareness, and tackle them individually.

- Gateway defenses
  At the gateway, Barracuda MSP deploys inbound and

outbound security, including traditional signature defenses and advanced techniques like sandboxing, domain fraud protection, and link/URL protection. It also provides encryption, data loss prevention (DLP), and archiving; this helps protect customers against accidental and malicious data loss, as well as providing support for compliance and enhancing storage capabilities.

- Resiliency
  Resiliency focuses on ensuring that MSPs can recover and re-establish their customers' systems as quickly as possible in the event of a data breach. This is achieved by including Cloud-to-Cloud Backup to protect against accidental or malicious deletion of data, and also providing a continuity service so that critical emails can get sent during an outage.

- API inbox defense
  As the threat landscape evolves, hackers continue to find ways to bypass the gateway. To catch these attacks, Barracuda MSP offers an artificial intelligence capability that can predict how likely an email is to be to or from the person it purports to be. Implementation and management of DMARC standard at this level also provides another useful barrier, as it helps ensure that bad actors aren't sending spam and phishing attacks using your domain and brand. This also helps defend against the growing problem of account takeover.

- Compliance
  Different industries may have different regulatory requirements. Whether it is to retain information, including email communications, for a set amount of time, or to ensure Personal Identifiable Information (PII) is not stored in an accessible location such as a SharePoint, Barracuda MSP's Cloud Archiving service

and Data Inspector can ensure seamless compliance to various regulatory and data privacy regulations.

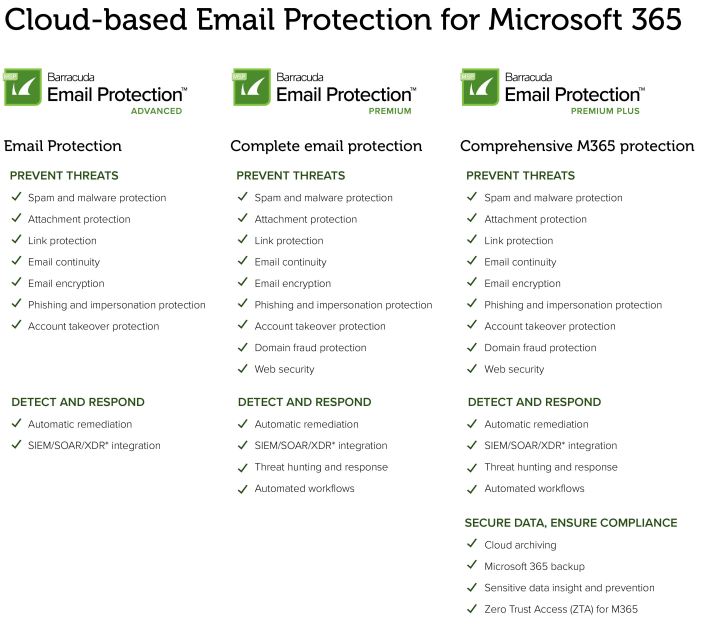
- Access
  In some cases, users are directly interacting with Microsoft 365, rather than from a client that receives its email via a gateway or API access. To ensure the same levels of security, Barracuda MSP also offers Zero Trust Access to Microsoft 365, helping to eliminate compromised access to applications and data within the Microsoft 365 cloud.

- Awareness
  No solution is 100% effective, and some malicious emails are still going to get through to the end user, especially today's most sophisticated attacks which are designed to bypass traditional security measures. To protect against these threats, Barracuda MSP focuses on turning your users from a liability into a control. They do this by providing phishing simulation and email security awareness training to help build your customers' resilience.

- Incident Response
  Social engineering attacks are meant to bypass technologies and target users. Attacks can reside in a user's inbox undetected. Respond to attacks and stop damage in minutes. Slash the time between detection and remediation with powerful delivered email search and rapid deletion from all user inboxes. Proactively identify security threats with threat insights. Identify anomalies that may indicate threats, based on insights gathered from analysis of previously delivered email and community-sourced intelligence.

- **Extended detection and response (XDR) backed by a 24/7 security operations center (SOC)**
  Provide a 24/7 proactive monitoring, detection and response service to top attack vector. Barracuda's SOC offers best-in-class threat detection mapped to the MITRE ATT&CK framework. This allows the team of security analysts to detect threats early and even predict their next move, helping them take effective actions to protect your customers' valuable assets.

The Barracuda MSP Email Solutions Portfolio



The above graphic demonstrates how Barracuda MSP's products map against the layered approach to email security set out on the previous section. The company's product set is created to be totally modular, so that you, the MSP, can layer in defense where your customers need a boost, or use all of the different components to provide the ultimate email security protection.

Barracuda Email Gateway Defense

The first level of the company's offering enables you to provide your customers with gateway defenses and resiliency, wrapped up in an easy to use and managed cloud-based solution. It includes Email Security Service, archiving for compliance, and data protection.

How does it work? The Email Security Service filters and sanitizes every email before it is delivered to your customers' mail server in order to protect them from email-borne threats. Its secure, cloud-based archiving will help ensure your customers can meet their compliance requirements and also address e-discovery requests at the same time.

As an added bonus, by including Barracuda's Cloud-to-Cloud Backup, MSPs can also protect customers' Microsoft 365 emails and files – whether they're in Exchange Online, SharePoint Online, Teams, or OneDrive for Business data.

Barracuda Impersonation and Domain Fraud Protection

Barracuda Impersonation and Domain Fraud Protection is designed to stop brand hijacking and catch social engineering attacks using artificial intelligence.

How does it work? By combining email protection tools with an artificial intelligence engine and domain fraud visibility, Barracuda Impersonation and Domain Fraud Protection can be a serious weapon in an MSP's armory when it comes to protecting against spear phishing, impersonation attacks, business email compromise, and other advanced email attacks.

It integrates directly with Microsoft 365 to protect personalized attacks in real time, with zero impact on network performance. Importantly, when it comes to protecting against socially engineered attacks or account takeover attacks, Impersonation and Domain Fraud Protection uses an API-based architecture that allows it to access historical email data, so that it can learn each user's unique communication patterns.

To provide a further layer of protection, specifically targeting domain fraud, Barracuda Impersonation and Domain Fraud Protection leverages DMARC reporting, analysis, and visibility. DMARC authentication can be quickly and easily set up using an intuitive wizard. Once properly configured, this provides

granular visibility and analysis of DMARC reports. This ensures that only your customer is the one sending emails from their domain and prevents damage to the customer's brand and reputation.

Barracuda Email Encryption and Data-Loss Prevention

Ensure compliance and security by encrypting emails in transit or at rest while stored in the cloud.

How does it work? Emails can travel through many different servers which can be vulnerable. Ensure only the destinated recipient receives and has privilege to reading the email with Barracuda Email Encryption. Data in motion is secured via Transport Layer Security (TLS), while data at rest is secured via AES 256-bit encryption.

Barracuda Cloud-to-Cloud Backup

Production data in the cloud is not immune to corruption, accidental data deletion, or cyber incidents. This is why Microsoft recommends that businesses should use a third-party backup for their Microsoft 365 data.

How does it work? Barracuda Cloud-to-Cloud Backup offers unlimited storage and retention for Microsoft 365 email, SharePoint, and OneDrive data, including the folder structure, attachments, calendars, contacts, and more. Recover individual files and email accounts with point-in-time accuracy either to the same location or to a different account and location.

Barracuda Cloud Archiving

Requirements for regulatory compliance and e-discovery may vary based on the industry. However, all organizations need to implement sound information governance practices, that is not based on backed up data.

How does it work? Barracuda Cloud Archiving is a cloud-based, indexed archive that allows for granular retention policies, extensive search, role-based auditing/permissions, legal hold, and export. Easy compliance with e-discovery requests and regulatory and policy-retention requirements.

Barracuda Zero Trust Access for Microsoft 365

Microsoft 365 accounts are a cybercriminal favorite. Ensure this business-critical application is protected using a modern cybersecurity solution, Zero Trust Access.

How does it work? Security starts with access. Barracuda's Zero Trust Access model establishes unparalleled access control across users and devices — from remote to hybrid, and from company-owned to employee- and contractor-owned. It provides remote, conditional, and contextual access to resources and reduces over-privileged access risks. With Zero Trust Access, employees and partners can access Microsoft 365 applications without creating additional attack surfaces.

Barracuda Web Security

Protect users from clicking the on malicious websites and links in an email with advanced web security.

How does it work? Through flexible controls, administrators can create policies based on 150+ content categories to prevent users from accessing websites deemed inappropriate for employees to access.

Barracuda Managed Security Awareness Training

Managed Security Awareness Training provides an additional line of defense when it comes to helping your customer protect their emails, by training end users to spot and thwart phishing attacks. It can also help your customers meet regulatory requirements, such as HIPAA.

How does it work? Barracuda MSP's team will configure and deliver regular phishing campaigns, and then provide reports to show their efficacy. This information can then be fed into a tailored security awareness campaign to ensure that you are getting the right training to the right people in your customers' organizations.

Barracuda Incident Response

As any cybersecurity professional knows, attacks are still successful, so as an MSP you need to be able to respond quickly in the event of a successful attack to prevent damage and limit the spread of an attack in your customer's network. However, responding to attacks manually is time-consuming and inefficient, and can allow threats to spread.

How does it work? Barracuda Incident Response automates these processes to ensure that MSPs can quickly identify the nature and scope of an attack, immediately eliminate malicious emails, and rapidly carry out remediation actions to halt an attack.

Barracuda XDR Email Security

Cybercriminals don't take vacations, and they will attack when you least expect it. To protect your customers, you need 24/7/365 monitoring.

How does it work? Barracuda XDR Email Security provides a proactive monitoring, detection, and response service to quickly identify threats, predicts their next move, and helps MSPs create and implement effective remediation tactics.

In addition to paid-for solutions, Barracuda MSP also offers a powerful, free tool that can be used to demonstrate the need for a more advanced email solution beyond the gateway, and effectively drive sales for MSPs.

Using AI and API integration with Office 365, the Barracuda Email Threat Scanner quickly and effectively finds social engineering attacks currently sitting in your customers' mailboxes. It's fast, free, and safe—with no impact on email performance.

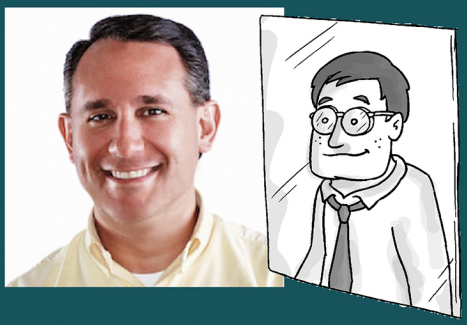
The scan can find threats such as spear phishing, business email compromise, conversation hijacking, brand and domain impersonation, scamming, and URL phishing. It also provides a comprehensive report of your customers' cybersecurity risk profile.

You can begin your scan here:
barracudamsp.com/ets


MSP
Barracuda
Your journey, secured.
FIND OUT WHAT'S HIDING IN YOUR CUSTOMERS' INBOXES.
98% of organizations with Office 365 harbor malicious emails inside their mailboxes.
Run a free email threat scan
barracudamsp.com/ets

Quickly become conversational about managing email security for SMBs

SMBs are increasingly being targeted in cyberattacks because they are financially rewarding for the bad guys and are often an easy target, because they lack the resources to defend themselves. With more than 90% of cyberattacks starting with phishing attacks, email should be front and center in their defenses. This ebook looks at how MSPs can help protect their SMB customers and at the same time build on their own success by offering layered email protection services.



About Nick Cavalancia

Nick Cavalancia is a technical evangelist, 4-time Microsoft MVP, and CEO of Conversational Geek. He has over 30 years of enterprise IT experience, 10 years of executive-level marketing experience, is an accomplished consultant, speaker, trainer, writer, and columnist, and has achieved industry certifications including MCSE, MCT, Master CNE and Master CNI.