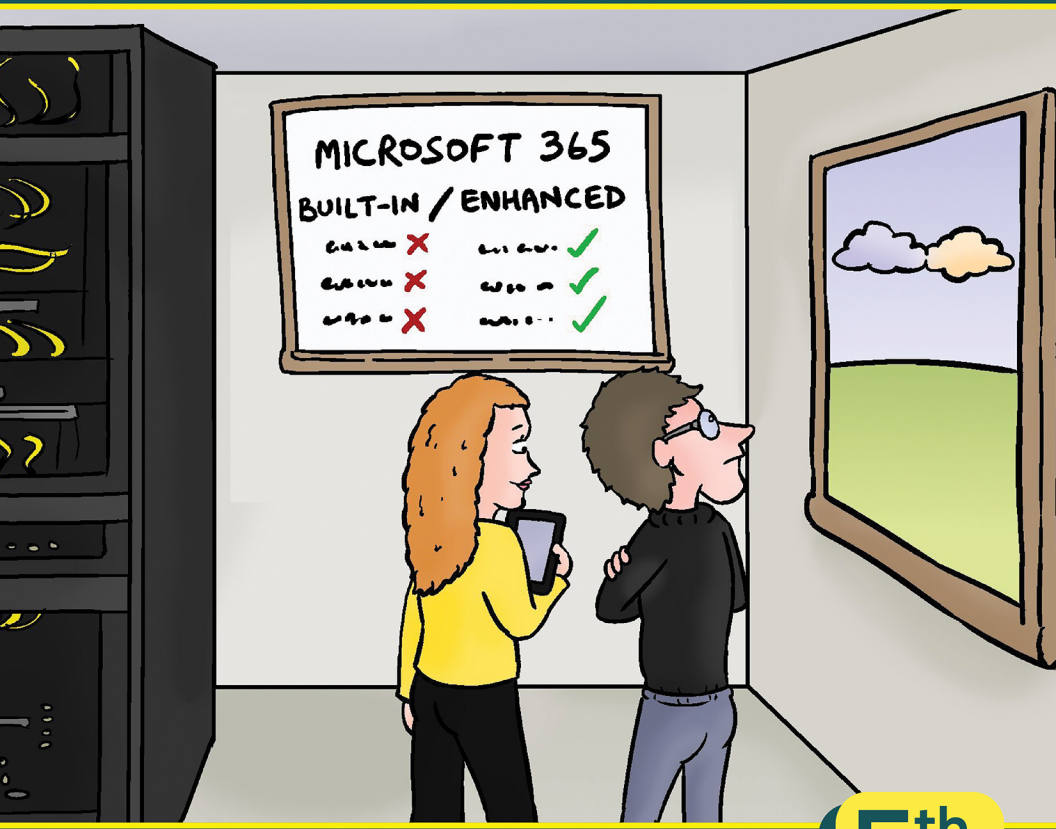
ConversationalGeek®

Conversational Microsoft 365 Cyber Resilience

By J. Peter Bruzzese (8-time Microsoft MVP for Exchange/Office 365)



5th Edition

In this book, you will learn:

- The value of a cyber resilience strategy for Microsoft 365
- The potential security gaps that exist in Microsoft 365
- How a third-party solution like Mimecast can reduce risk and add resilience

Sponsored by

mimecast®

Sponsored by Mimecast

Mimecast: Work Protected™

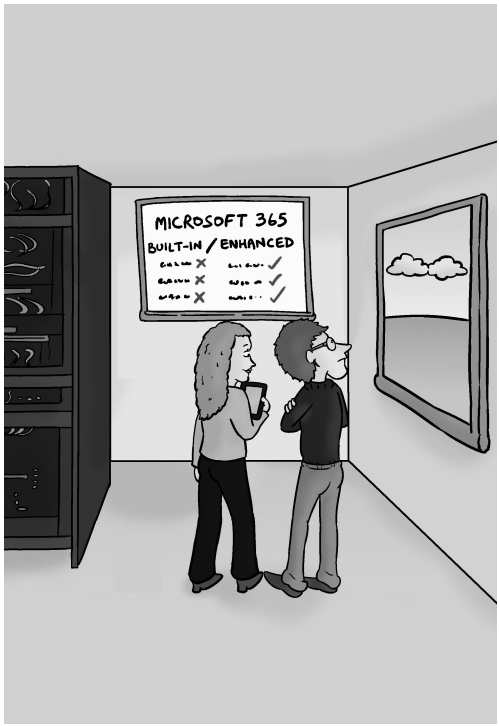
Since 2003, Mimecast has stopped bad things from happening to good organizations by enabling them to work protected. Mimecast empowers more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide.

mimecast™

www.mimecast.com

Conversational Microsoft 365 Cyber Resilience (5th Edition)

By J. Peter Bruzzese



ConversationalGeek®

Conversational Microsoft 365 Cyber Resilience

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:	J. Peter Bruzzese
Project Editor:	Hope Crocker
Content Reviewers:	Orly Bar Lev

Note from the Author

Greetings! From the earliest of times … no, not the beginning of the physical universe itself … the earliest of my time working with Exchange, I have always bolted on a variety of different solutions to enhance what Microsoft gave us. Exchange, despite being the best solution to come out of Microsoft (and yes… I'm somewhat biased here), has always left some gaps for third-party vendors to plug. For example, backup and recovery, archiving, monitoring, malware protection, and so on. The talk around the IT water cooler was all about what solutions you used to fix <insert the gap>, especially when dealing with Exchange Server and email services.

Microsoft 365 started off with the same need for all of those bolt-on additions, but over time Microsoft has worked hard to build some of these features within their platform. However, I'm still a huge advocate for bolt-ons for a variety of reasons, not the least of which is that I don't believe in "good enough" security. I think security is one area where you just cannot afford to stop at "good enough".

Honestly, just from a technology standpoint, companies need to seek out solutions that not only protect against attacks but also act faster to limit attack impact. That's not to say you should be buying everything on the market and bloating your security situation with tools that are disconnected and redundant, without enhancing, efforts. It's balance between risk and total cost and business impact.

Microsoft 365 isn't ready to go it alone.

J. Peter Bruzzese

Email Deserves More

You've heard it said many times, I'm sure. 90+% of all cyberattacks start with email. Email is the number one attack vector.

Email, arguably the most mission critical application, has always been at the intersection of a massive amount of risk. With on-premises Exchange servers, we mitigated that risk by surrounding our Exchange server(s) with an ecosystem of solutions from third-party vendors. We "bolted on" rather than making do with what was "built-in". The objective? *Security* and *resilience*. Out-of-the-box was never good enough.

Exchange admins would deploy a security solution(s) with an email security component to stop spam and phishing. For compliance and e-discovery we might have an archive solution. Perhaps a monitoring solution to ensure services are up. A must-have backup and recovery solution for DR and point-in-time restore capabilities. And the list continues.

We could choose a different vendor for each solution, or a single vendor if they had multiple solutions bundled together that met the criteria we were looking for (i.e., best of breed, best in class, personal favorite, Gartner magic quadrant, etc.). What we didn't do was deploy Exchange alone. You never saw that in an enterprise environment. An Exchange server (or servers) and nothing else.

Moving your email to the cloud with Microsoft 365 (specifically Exchange Online) doesn't eliminate risk. Cybercriminals are still doing their thing and technical failure is still lurking. One might say the risks not only remain but are expanded by moving services to the cloud. What increases accessibility for you increases it for attackers too! Email continues to be the number one attack vector for the bad guys.

How do organizations address the challenges associated with changing infrastructure and ever-growing attacks?

My advice is to go back to what you know! Back to what works… but with a twist.

Looking at Microsoft 365 from a security perspective, it makes sense to ensure your security is layered. A defense-in-depth approach that considers:

- The budget limitations you have
- The number of solutions you can reasonably manage
- The top risks addressed first and foremost

Budgets vary, as does the number of solutions you can reasonably manage. As for top risks, some may think this is debatable within the cyber kill chain (the gateway? the endpoint?) and yet over and over it's been confirmed, as I stated at the outset of this chapter, that majority of all modern-day attacks start with email.

No matter the exact percentage, it gives us a focus point… it's a lot. We must do our best to place defenses that give our people a chance against ransomware/malware, spear phishing, impersonation attacks, and the like.

"Good enough" mentality has led some to do more than just trust Microsoft 365 out-of-the-box. Many aren't even taking advantage of what comes "in-the-box". A lack of initiative in turning on built-in features like multi-factor authentication have all led to the Department of Homeland Security's cybersecurity division (CISA) putting out warnings and recommendations for Microsoft 365.

goto.cg/CISA-M365

But we cannot have a prevent-only strategy. In addition to email security components we should be considering how to strengthen our people who have consistently been labeled the weakest security link (and rightly so).

We need solutions that will help people be more vigilant to bridge the awareness and understanding gap. And you know what? There will still be breaches, outages, and human error.

The Revival of the IT Admin

I imagine some of you are reading these past pages like a superhero that has been put out to pasture, all of a sudden feeling needed again. You've been told your skills are no longer needed in a SaaS, cloud-service world. You've been told that a "power user" can do the job now, it's so easy. You've been told the built-in solutions are "good enough" now… leave it be. Are you ready to put the super suit back on yet? Keep reading.

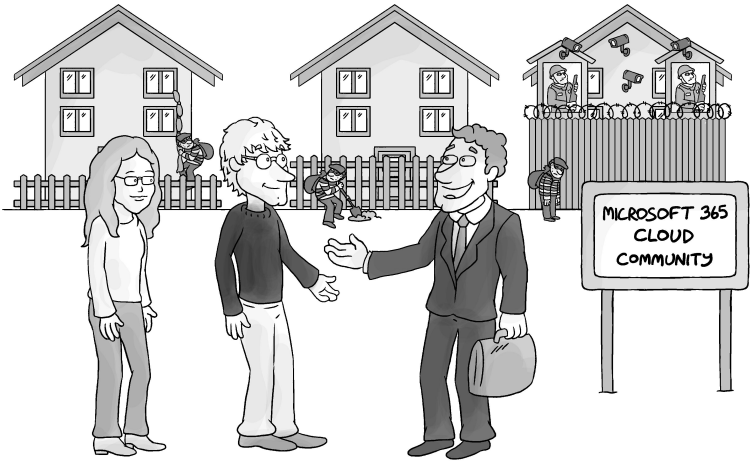
Deciding the Future of Your Microsoft 365 Cyber Resilience

Microsoft provides a solid suite of solutions (with email at the forefront) in Microsoft 365. Within Microsoft 365, Microsoft provides a measure of security, compliance, continuity (or availability), and recoverability as part of their service level agreements to customers. However, it's up to you to guarantee the overall security of your entire email environment. Just like we've done with on-premises servers in the past.

In the on-premises days, we bolted on enhancement solutions to ensure resilience. With on-premises you could bolt on different solutions to address your needs… however, in a cloud-based world you want and need an all-in-one security and resilience *ecosystem*. You don't want to daisy chain multiple solutions on to the front end of Microsoft 365. That will lead to multiple points of failure and added latency. No… you need a solution that can wrap itself around Microsoft 365 and provide true cybersecurity and resilience… *especially* for your mission-critical email.

It's time for IT admins to rely on their experience to provide thought-leadership on which solutions can fill existing gaps.

Cybersecurity Resilience and Microsoft 365



"We have homes with an EOP fence… and an MDO365 fence… and… if you like you can go with an outside security company called Mimecast"

Although I'm a supporter of Microsoft 365 as a communication and collaboration solution, I don't believe a single-cloud approach is either sufficiently secure or resilient. Two clouds are better than one. But there are reasons behind that thinking. It's not simply a matter of "well, I've always used third-party solutions to fill the gaps and so I will continue to do more of the same." Obviously, the cloud brings change and I'm not averse to positive change. I'm not buying the hardware or doing the upgrades, which is great. But is Microsoft 365 the be-all and end-all of security and resilience? I don't believe so and what I find odd is how many organizations are simply closing their eyes and sleepwalking into Microsoft 365.

Sleepwalking into Microsoft 365

As mentioned, with our on-premises experience we rarely (ahem… never) saw a greenfield or long-term deployment of Exchange that simply used what Exchange had to offer without

using ecosystem partners to provide improved services to surround and support it, or even to enhance it.

So why is it that when we move to the cloud, and move to Microsoft 365, many close their eyes and just accept what is provided or built-in? *Why are so many sleepwalking into Microsoft 365?*

There are things Microsoft can do with a multi-tenant cloud-based version of hosted Exchange they couldn't do with the on-premises flavor. Because they have full control of the infrastructure, they can provide high availability using 'native data protection' that provides multiple passive (and lagged) copies of your databases across datacenters to deliver a high availability offering that would cost a company time, money, and personnel to provide in-house. That's one of the many reasons I encourage folks to move to Microsoft 365.

However, there are still gaps in the services provided that require a third-party solution (ideally an all-in-one solution) to help ensure the type of one-to-one experience that is typically seen on-premises.

Key Areas for Concern

We're not going to pick apart every little thing about Microsoft 365 and Exchange Online. There is no point in doing that. It's a great solution and priced right. I'm only going to hit the risk areas that make people like me nervous about "naked" Microsoft 365. I'll explain what is built-in and why third-party software will enhance the overall solution.

Security

Exchange on-premises (2013/2016/2019/2021) includes an anti-malware solution and anti-spam agents. These offer very basic protection, so most enterprise deployments of Exchange look to a third party, on-premises appliance or cloud-based

solution to really cover themselves against all the bad stuff: spam, malware, phishing, spear phishing, impersonation attacks, ransomware attacks, and so on.

Spear phishing is becoming a focal point for attackers looking to breach organizations' defenses, and it is very treacherous. It's targeted against a specific company or person, and has led to some major, high-publicity breaches, because there were no solutions in place to help block the attack.

Exchange Online Protection (EOP)

Exchange Online comes with a free solution called Exchange Online Protection (EOP). It's enabled by default and provides basic anti-spam, malware, and spoofing protection. Does it work? It does… and the EOP dev team is aggressively seeking to improve the solution.

However, the last thing you want is to live in a *security monoculture*. The term *monoculture* is defined as a community of computers that all run identical software and have similar vulnerabilities. Microsoft 365 might be considered a SaaS Security Monoculture if used without a third-party layered security solution approach. It certainly is big enough to draw the focused attention of cybercriminals.

On-premises, every company handles security a little differently, with a combination of vendors involved, layered with multiple locks to pick and each company its own unique target. With Microsoft 365 all tenants live together under the identical security controls, providing a very target-rich environment.

Dan Geer, a risk management specialist and cybersecurity expert, has repeatedly pointed out the problem of a security

monoculture, especially with regard to Microsoft. His primary focus was on the number of Microsoft workstations connected to the Internet. But an even greater threat is to have a multi-tenant email solution, near monopoly (which is inevitable at this point), with a single security solution protecting all the tenants.

Think of the saying "don't put all your eggs in one basket". Well, with Microsoft 365 you're putting all your eggs – and everyone else's eggs – in one big basket. Am I the only one who gets nervous about that? Talk about a juicy target!

EOP on its own doesn't protect against some of the more sophisticated attack types with weaponized attachments and links that make it through the first line of defense and into an end-user's mailbox. So, Microsoft offers an extra cost solution called Microsoft Defender for Office 365. Defender for O365 is included with an E5 plan or can be purchased per user (Plan 1 or Plan 2).

Microsoft Defender for Office 365 (MDO365)

MDO365 offers several additional protection features called Safe Attachments, Safe Links, and Anti-Phishing. The concept is simple. Besides easy-to-spot spam and known virus attachments, there are three ways the bad guys get to your end users: attachments (that may appear suspicious but aren't KNOWN to be bad), URL links that lead to sites that are "ok" when they first come through, but may become harmful later, and with social engineering-based impersonation.

- Safe Attachments: Safe Attachments uses a sandbox 'detonation chamber' to check if the attachment is harmless. During the scan the users can view the attachment through 'dynamic delivery' if supported for

that attachment type. Sandboxing offers the promise of zero-day detection capabilities (meaning it can spot a new malware threat if done properly). Sandboxing has its place, but it has a few weaknesses as well. For example, malware may figure out when it's in a sandbox and remain dormant. Microsoft's sandbox solution uses virtualization with Azure VMs to check for weaponized attachments. Software-based, virtualized sandboxing is easier for malware to evade whereas full system emulation is a better approach to catching evasive malware.

- Safe Links: When a user receives an email, MDO365 analyzes URLs against a block list as part of a URL reputation check. At the time-of-click, it will perform a URL scan within a virtual detonation environment to check before allowing the user to continue to the site. However, it doesn't do a deep inspection of web page content, for example, chasing down URLs off the main site to ensure connected pages are also safe.

- Anti-phishing: Detects impersonation attempts and custom domains. However, it doesn't have homoglyph similar domain spoofing detection. Google that word if you don't know what it means.

The threats that keep me up at night include spear phishing, ransomware/malware, and impersonation attacks. And in my opinion both EOP and MDO365 aren't good enough to allow me to sleep easy. I need more.

Long story short, Exchange Online Protection (with or without the Microsoft Defender piece) is lacking against today's threats. And it's lacking not just due to features as compared with third-party options, because over time the gap in features may close (although that, too, is a moving target). BUT… it is and will continue to be a single lock to pick, a security monoculture, and that is why a complementary solution should be seriously considered. Don't just hope you're safe, know you're safe. PLAN to be safe.

I believe in defense-in-depth and the wisdom of a layered security approach. I promote end-point protection, DNS level web protection, user behavior analytics etc. And I'm a huge proponent of a third-party cloud-based email security component with Exchange/Microsoft 365. Especially if you're in a hybrid environment where many security features don't span multi-platform/vendors.

Opportunistic Attacks (Low Hanging Fruit)

Imagine you're a thief looking to rob a home and you're looking at two big, beautiful houses. The first sits on a wide-open property with no gates, no security system signs, no "Beware of Dog" (or "Beware of Owner") signs – really nothing to indicate protection. And the second has a massive gate and fencing system with security cameras, a sign for a security solution that is noted as the best around, a "Beware of Dog" sign out front, and a "No Trespassing" sign. Now, which would you try and rob?

It's the same with attackers going after an organization. Unless the motive is revenge (a disgruntled former employee perhaps) or corporate espionage/attack (competitive cyber warfare) many attackers are just looking for low hanging fruit. An easy target for money.

Some have asked, “if I pay for third-party security, am I not just paying twice for the same thing if I have EOP? Or EOP and MDO365?” Well, if you are calling all three options “fences” then yes, you’re paying for the same thing. But fences vary in size, strength, and effectiveness. EOP is like a two-foot fence that helps keep the anti-spam/malware critters out. MDO365 is more like a five-foot fence that will help prevent mass malware/ransomware-type attacks, opportunistic attacks, and such. But if you want a 10-foot fence with security cameras and sentinels and such you will need to seek a third-party solution.

It's not that difficult to do a little bit of research to find what a company is doing with regard to email security. Basic research, combined with a little social engineering will yield a clear view of what tools they are or aren’t using. And with a little effort you can discover what they are or are not doing. That’s important. What are they NOT doing? Are they NOT training their end users? Do they NOT have other solutions to protect themselves? For lack of a better word, they are looking “tasty” to you as a cybercriminal.

Recreate the Vault

Another factor to consider is the ability of the cybercriminal to recreate your environment should they wish to test their attack methods out before hitting their target. I call it recreating the vault.

Have you ever seen Oceans 11? In the beginning of the movie George Clooney and Brad Pitt steal the plans for the vault. To rob it? Well, yes. But not at first. First, they recreate the vault in a warehouse so they can practice robbing it first. See?

If you're using straight out-of-the-box EOP/MDO365, it costs less than $100 to register a domain name and set up a portal to play with. And that includes multiple account types (E3, etc). Now you can toss stuff at it and see what makes it through.

Efficacy: One Drop of Poison

It's not *what your security solution can stop* that matters. It's *what it lets through* that you really need to worry about. The efficacy (aka effectiveness, usefulness, or value) of a solution cannot be determined by looking at a list of check boxes. "Does your solution do a, b, and c?" Answer: "Yep! We can do a, b, and c!" Check! Rather, the efficacy of a solution must be determined by genuine testing and impartial solution review.

EOP and MDO365 do work. They DO stop stuff: spam, malware, ransomware, and malicious links or impersonation attacks. They do check some of the security boxes. But in testing and in real-life scenarios, I've seen results that demonstrate that they miss way too much for my comfort level. Are you ok with that? Are you ok with having your people, a key target of many cybercriminals, be your last line of-defense against a steady flow of modern security threats?

My advice would be to run a trial of a third-party solution at your organization for a period of time to see what's being missed.

In other words, are you ok with a glass of water that isn't *filled* with poison, but has just a drop or two? Drink up! Ahem… probably not. A third-party solution is a key necessity to mitigate security risks with Microsoft 365. Those of us in cyber security like to say it's the end user that is the weak link but we often forget that we, too, are end users. Even we have the unfortunate lapse or mistake where we click a link in a phishing email or find our search results have been "poisoned" or simply browse to the wrong site. We might get coerced into giving up credentials or get hit with a drive-by download scenario. Here is where some form of browser isolation can help to keep your organization safe.

Understanding the Stakes

It's easy to talk about the gaps in security, but that keeps the conversation focused on the technology. I think it's important to also grasp the impact of a data leak or a security breach.

A data breach, for example, can have all sorts of consequences. It can trigger regulatory violations from one of the scary regulatory acronyms like GDPR, FINRA, CCPA, and others. In addition, it can cause loss of reputation for the organization that leaked the data, reputational damage (or job loss) for the C-level folks who are often blamed (or become the scape goats). It can cost the company money either through loss of customer confidence (sales are down), or a stock hit.

Either way, the stakes are high. Because the potential impact is deep. A significant breach can change your company's entire trajectory. When you think about it that way, is good enough, good enough?

The Big Takeaways

Microsoft 365 is a fantastic solution, especially Exchange Online. Increasingly organizations of all sizes and types are making the move to Microsoft 365, with email a key driver.

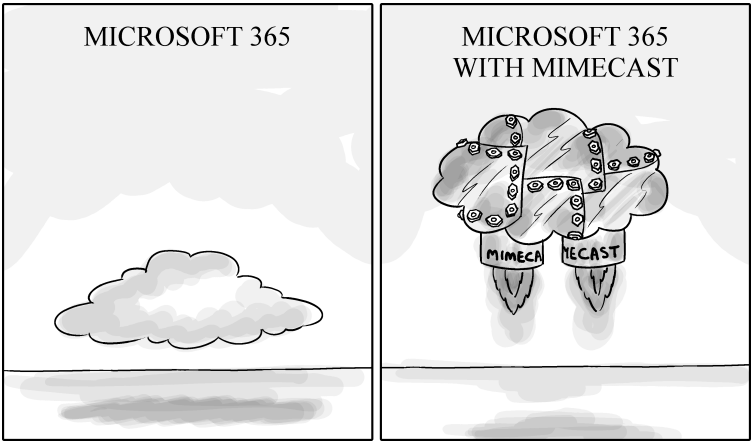
Although Microsoft has more control over Exchange Online because it's hosted in their cloud and they can enhance, improve, develop, and tweak it all day long… there are still gaps. There are security risks, as we've discussed.

It's obvious these risks can cause fear, uncertainty, and doubt (FUD). But they don't have to. My advice to any Microsoft 365 current customer or potential customer is to look once again to the surrounding vendor ecosystem to find ways to mitigate these risks. Look for a complementary solution that can address the pain points and enhance what Microsoft provides.

A "two-are-better-than-one" complement is the key here. A solution that strikes the balance between risk and total cost and/or business impact. But does such a solution exist?

Sponsor Chapter:

Work Protected with Mimecast



Work Protected

The multi-dimensional problem described above deserves a multi-dimensional solution.

Most information you read about when it comes to a third-party solution is written by the third-party. They tell you:

"*We're awesome! And here is a document that proves it! <cough><cough> written by us <said in a whisper>.*"

Even if it is true, it certainly does cause an eyebrow to rise and the cynical side to us comes out. Doesn't it?

That's why I told my friends at Mimecast I wanted them to let me write this up in my way. I want you to see their solution how I see it. I won't be able to give you every last bell and whistle of their solution, but I will certainly be able to tell you how it will add value to either your Microsoft 365 Exchange Online, hybrid, or on-premises environment.

Mimecast was founded in 2003 by Peter Bauer and Neil Murray. These were regular people (albeit super geniuses), IT/Dev admins that saw a problem and went to work fixing it. The problem they saw was that email was becoming more and more complex to handle, while simultaneously becoming more strategic. They built a cloud-based solution to the problem that provided email management and risk mitigation – and the solution took off. And while the solution has dramatically grown over the years, the philosophy of having a single integrated cloud-based service has never wavered. And they decided this way back in 2003! Since that time Mimecast has been helping their customers by enabling them to work protected. Ultimately you can't work if you aren't safe. And I don't mean if you don't "feel" safe, because security theater can create the illusion of safety. Rather, if you aren't mitigating genuine risks that arise from malicious cyberattacks, human error, and technological fallibility, you're not work protected.

Mimecast focuses on three areas of protection: *Communications*, *Data* and *People*. Let's explore those a bit further.

Protect Communications

At the heart of protected communications is email as the top attack vector. Email protection can mean so many things, so what is it REALLY that Mimecast provides? Well, for starters, anti-spam and anti-malware. Keeping the junk from ever reaching your users inboxes. And Mimecast can do this through its AI-powered email security with a gateway (called *Cloud Gateway* or CG) or without (called *Cloud Integrated* or CI).

Email Security, Cloud Gateway (CG)

With Mimecast's Secure Email Gateway in the cloud solution, Mimecast sits between your email environment (Microsoft 365, Google Workspace, hybrid, on-premises) and the Internet and provides solid protection from spam, viruses, malware,

impersonations, zero-day attacks, ransomware, phishing, spear phishing, and data leaks. Setting this up requires an MX record change so that you point to Mimecast and email goes through Mimecast and then to Microsoft (or other email solution) before being delivered to end users.

Mimecast uses several detection engines for a multi-layered approach. It includes the ability to deploy policies that assist with data leak prevention (DLP) and content control, a serious sore spot for most organizations. So, Mimecast keeps the company data confidential while keeping the bad guys out at the same time. And it does this no matter where the person is connected (LAN/Wi-Fi/Internet) and no matter the device (desktop, laptop, mobile, or tablet).

Mimecast also rewrites every inbound URL for on-click protection. And identifies emails that use impersonation and/or domain spoofing to try and steal money, data, or credentials. Safe-file conversion of file attachments (which I think is brilliant) converts incoming documents to PDF. So rather than send every document through a sandbox detonation chamber (i.e., a virtual machine to open that document and see if it will do harm) it will convert it to PDF and strip out any active content, thus rendering the file harmless. And then if the person WANTS the original document it can be rigorously inspected (using full system hardware emulation-based sandboxing and static file analysis). A very creative approach to eliminate the latency of trying to sandbox every single incoming document.

With either solution Mimecast helps defend your organization from sophisticated attacks. Phishing, ransomware, social engineering, payment fraud and impersonation, and more.

One Mimecast solution I consider cutting edge… better yet, bleeding edge… is their static file analysis. It's file agnostic and looks at the bits and bytes of a file (image/pdf/Office doc) for executable code. No sandbox latency involved. Absolutely brilliant, and something Microsoft simply doesn't offer.

Email Security, Cloud Integrated (CI)

As an alternative to the traditional cloud gateway approach that sits in front of your organization there is an option for Microsoft 365 where email is first scanned by Microsoft and then scanned by Mimecast before hitting the user's mailbox. It's a faster, less complex setup using a simple install wizard that uses Microsoft 365 mail flow rules to inspect the emails after Microsoft's native detection engine. Email Security CI is architected to protect a single Microsoft tenant (which may have multiple domains).

This cloud-integrated approach empowers organizations to deploy email-based protection literally in a matter of minutes with lower costs than CG. Using pre-configured, optimized settings, email is protected immediately, with AI-powered detection kicking in the moment it's implemented. Emails are scanned and warning notifications are sent to internal email recipients to instantly provide value, lower risk, and increase the security of the organization.

This is especially valuable for organizations with limited resources. As small to midsize businesses (SMBs) face the same level of cyber threats as large enterprises, it's crucial for Mimecast to provide them with the same level of security as their enterprise counterparts. Additionally, administrators can

test the solution on partial domains before full implementation.

Social Engineering Defense and AI Cybersecurity

Malware-less, social engineering attacks have become more sophisticated than ever, using homoglyph attacks to make it even harder for detection solutions to fully protect users. Homoglyphs are two or more characters that look very similar and there are online generators that make it easy for crooks. Mimecast offers homoglyph/homograph detection along with impersonation attack protection through their product *CyberGraph*.

CyberGraph's AI is continually learning to catch more sophisticated threats. Using human behavior analytics, it can detect anomalies in behavior. It uses color-coded email warning banners that help users with at-a-glance threat notification that updates automatically for all employees across all devices; according to Mimecast's *State of Email Security 2023* report (goto.cg/SoEMR), nearly half (48%) of security decisionmakers agree their organizations would derive huge benefit from these warning banners. CyberGraph also removes embedded email trackers.

Browser Isolation

We discussed earlier how the savviest of end users might find themselves clicking a link or going to a site that ends up being trouble. With Mimecast's Browser Isolation, Mimecast uses a virtual environment to "open" uncategorized URLs to make sure they aren't a threat, adding another layer of protection. So, the browser is running in an isolated container on a server in the Mimecast cloud and then the pages are streamed from the Mimecast cloud to the user's browser.

Protect People

Security Awareness

They call the end user the weakest link. How do we move the needle on that side of the story when a threat makes it past the goalie and into their inbox? How do we eliminate human error? Well… eliminate is a strong word. But we can make them security savvy through training.

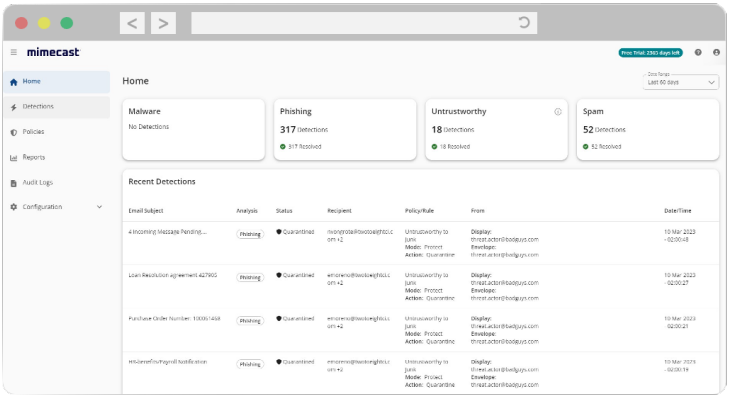
I know what you're thinking. Death-by-PowerPoint security awareness training? No thanks! I thought the same thing when I heard Mimecast had awareness training and phishing simulation tools. But this is a really engaging approach. Unique compared to other training solutions. It's clear that when your users aren't engaged, they don't pay attention to the training, never learn, and become somewhat dismissive toward security in general. So, how do you engage folks? Humor.

Mimecast uses short videos (three to five minutes) usually delivered on a monthly basis, that are quite funny. And while they are designed to make you laugh, they're also designed to make you think and internalize the risky situation. Users get an email reminder to watch the lesson. They get a single question at the end of the module to ensure they got the point. A risk score is determined based on how your users do and you can locate your riskiest people and provide them more help *before* they make a mistake (or *another* mistake).

Feel free to try them out yourself at goto.cg/MimecastSA.

The Big Takeaways

Despite the risks of moving to the cloud, by solution like Mimecast you can mitigate those risks, eliminate the FUD, and plan for success rather than just hoping for it.



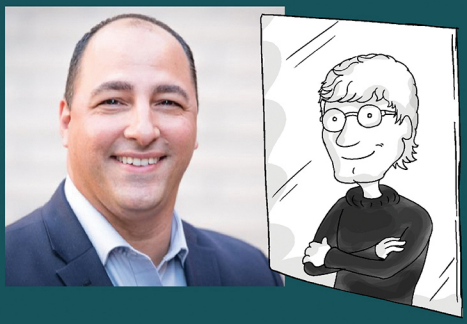
The Mimecast Email Security CI Console

So, that's my personal opinion on Mimecast's security enhancement solution for Microsoft 365. I recommend you check them out. The added value you will receive at such a reasonable price point is unbelievable.

www.mimecast.com/mimecast-and-microsoft-365

Get conversational about cyber resilience for Microsoft 365

If you are moving to or already using Microsoft 365 then it's essential to formulate a plan to create a risk-free cyber resilience experience. Doing so will protect your organization from security threats, compliance concerns, unplanned outages, and more. To mitigate concerns and form a resilient strategy you have to first KNOW the risks. This book will ensure you do in no time.



About J. Peter Bruzzese

J. Peter, an eight-time awarded Microsoft MVP (Exchange/Office 365), is an internationally published author, global tech speaker, journalist, and cyber security advisor.

ConversationalGeek®

For more content on topics geeks love visit

conversationalgeek.com