GUIDE

Bitdefender

Security

Bitdefender Email Security Guide For MSPs

STRENGTHEN CYBER RESILIENCE AND REDUCE CUSTOMER RISK.

www.bitdefender.com/msp

Contents

Introduction

It's easy to get the impression that email is slowly dying due to the increased adoption of social media platforms and collaboration tools. But email is not going anywhere anytime soon. It's still the most widely used tool for businesses. Even more so now that many employees are working remotely and relying on email and collaboration platforms to get their jobs done. Email remains an essential part of nearly all online subscriptions, platforms and services used through the internet. Radicati predicts businesses and consumers will send more than **347 billion emails per day by 2023**[1].

The pandemic last year spurred a major increase in the use of cloud solutions like Microsoft 365 and G-Suite to support remote working without harming productivity. Many organizations are moving away from on-premise networks and fast-tracking digital transformation plans. While these solutions offer clear collaborative benefits, cloud and hybrid environments can also bring some risk if security and user training is neglected, leaving your customers' businesses vulnerable to social engineering and sophisticated malware attacks.

In short, the threat landscape has changed drastically in terms of attack surface, threats and challenges brought forward by the global Coronavirus pandemic and working from home. MSPs need to learn to adapt to these new trends and assess whether their technology meets the needs of customers in the current climate. On the flip side, it opens opportunities to increase customers' cybersecurity and strengthen their business continuity – with your MSP security stack.

Email is at the forefront of strengthening cyber-resilience. It is notorious as the #1 attack vector - **96% of data breaches are a direct result of phishing and pretexting**[2], and remains a vulnerability due to the human element.

Businesses can reduce risk by strengthening email security and practicing frequent user training. This eBook covers the current email threat landscape, steps you can take to help reduce your customers' risks and the benefits of providing email security for you as an MSP.

Top Email Security Concerns

78% of users say they're familiar with the risks of unsolicited links in emails. Still, around 30% click on the links anyway

Business Email compromise accounts for **over 1% of all traffic**, at an average cost of $37K to an organization

96% of data breaches stem from phishing and pretexting

62% of organizations fell victim to ransomware in 2020

1 "Email Statistics Report 2019 – 2023,"Radicati Group. https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf (Accessed February 2021)

2 "2018 Data Breach Investigations Report," Verizon. enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (Accessed February 2021)

Email Threat Landscape

Cybercriminals target email – it's easy to access and vulnerable due to the human element - 94% of malware is delivered via email[3]. In this section, we take a look at some of the most common threats in today's market.

Among the most popular attacks are CEO fraud and Business Email Compromise (BEC). These attacks are well-known, but their sophistication and personalization are ever-evolving.

Email campaigns crafted around the coronavirus pandemic became the new norm, Bitdefender telemetry found[4]. "Attackers dress-up their threats with a cloak of panic, fear and information manipulation. Bitdefender telemetry has actually revealed that during peak of the pandemic, four in 10 emails on the Coronavirus topic are fraud, phishing, or malware."

Business Email Compromise, Phishing and Impersonation

Business Email Compromise (BEC), CEO/CFO executive whaling and sender impersonation are here to stay. Cybercriminals rigorously research the individuals and organizations they target and craft highly tailored emails. When sent in such low volumes, the emails are much harder for anti-spam and anti-virus solutions to detect.

BEC scams mainly trick email users into sharing confidential information or into transferring money to fraudulent accounts. The FBI reported around **$12 billion in losses over the last six years due to BEC scams[5].**

With remote working, many employees don't have the same security mindset they had at the office. In the past, it was easy to walk over to a colleague and ask for confirmation when an email looked suspicious. Now, verifying the legitimacy of an email is sometimes skipped because it's more of an effort. One of the biggest challenges of the past months has been employees falling victim to phishing and spear-phishing attacks.

Employees might use both their private email account and business emails on their work devices. When added to the need to balance meetings, video conferences, the home-based education of children and the need for information regarding the pandemic, this creates the perfect conditions for cybercriminals to launch their attacks.

"The pandemic has proven to be a strong catalyst for opportunistic coronavirus-themed spam emails which spiked considerably throughout the first half of 2020. Bitdefender telemetry shows that four in 10 coronavirus-themed emails have been classified as spam, phishing, or malware, suggesting that remote employees and average users have been constantly at risk of opening up tainted emails." Remote work has potentially exposed businesses to more business email compromise (BEC) attempts, risking employee and company data.

Business email compromise evolved over the past couple of years in terms of approached themes, ranging from wage and tax statements in 2016 to human resources and gift cards in 2018. While the main BEC topics revolved around healthcare and payroll diversion in 2019, 2020 seems to have been all about COVID-19 and healthcare, according to HHS[6]. BEC scams can be extremely damaging. The Federal Bureau of Investigation (FBI) estimated the average loss

3 "2019 Data Breach Investigations Report," Verizon. enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf (Accessed February 2021)

4 "The 'New Normal' State of Cybersecurity', https://www.bitdefender.com/files/News/CaseStudies/study/378/Bitdefender-Whitepaper-2020-Business-Threat-Landscape-Report.pdf

5 "Introducing BEC: The great white shark of social engineering", https://www2.infosecinstitute.com/l/12882/2019-06-05/drch5b (Accessed February 2021)

6 Business Email Compromise in the Health Sector," HHS Cybersecurity Program. https://www.hhs.gov/sites/default/files/business-email-compromise-in-the-health-sector.pdf (Accessed February 2021)

per complaint at nearly $75,000 in 2019[7]. The expectations is that BEC financial losses in 2020 far exceeded that number due to the pandemic.

BEC emails seem to be short and personal, and are always phrased as if the victim needs to perform a quick action or a favor for a coworker.

"2020 Popular MITRE ATT&CK® Techniques and Sub-Techniques Bitdefender's business telemetry on identifying the most commonly used attack tactics and techniques used by sophisticated hackers has revealed that phishing remains one of the most common tactics reported for initial access." Infosec research showed 30% of spear-phishing campaigns succeed[8].

Other examples detected are more generic, and use the same style as internal IT teams or automated platforms to trick users into responding or engaging with the threat actors or downloading files that contain malware.[9]

The most popular phishing emails in the current threat landscape:

- Spear-phishing attempts related to services, platforms or tools used by employees such as Microsoft 365 or Google Cloud Services (i.e., spam about bonuses via fake SharePoint email accounts).
- 'Fake' emails from shipping services like DHL, FedEx, DPD, TNT and Amazon
- False email account alerts about 'pending messages', 'unauthorized login notifications' or 'storage full notifications'
- Netflix phishing campaigns
- Covid and vaccination-related phishing campaigns
- Extortion campaigns that ask for payments and cryptocurrencies
- Financial phishing campaigns using PayPal or banks to create a sense of urgency

These emails generally include phishing or malware attachments and look very real.

Display Name Spoofing

Be aware of the CEO. CEO fraud or C-level impersonation is a popular method used by hackers, where they create a fake CEO email account using a nearby domain. This technique, also referred to as Display Name Spoofing, involves forging a sender's name to make it looks like it comes from a legitimate source. Using the name of someone in executive-level management of the company adds additional urgency for users to act on the request. Typically, cybercriminals attempt to get an 'invoice' paid, a direct wire transfer completed or sensitive data.

Account Takeover (ATO)

Account takeover (ATO) is a form of identity theft where a cybercriminal gains access to a victim's email account. ATO attacks are often targeted at a specific organisation. Typically, the higher-profile the target, the more tailored the phish. For prime targets, such as government or financial organisations, an attacker may spend significant time researching their mark by collecting information to personalise the approach. The result can be anything from locking users out of their accounts, to vast data breaches.

7 "2019 Internet Crime Report", Federal Bureau of Investigation (FBI),https://pdf.ic3.gov/2019_IC3Report.pdf

8 "The Trends in Spear Phishing Attacks", Infosec. https://resources.infosecinstitute.com/topic/the-trends-in-spear-phishing-attacks/#:~:text=At%20least%2030%25%20of%20the,the%20return%20is%2040X%20greater. (Accessed March 2020)

9 "The 'New Normal' State of Cybersecurity', https://www.bitdefender.com/files/News/CaseStudies/study/378/Bitdefender-Whitepaper-2020-Business-Threat-Landscape-Report.pdf

Malware

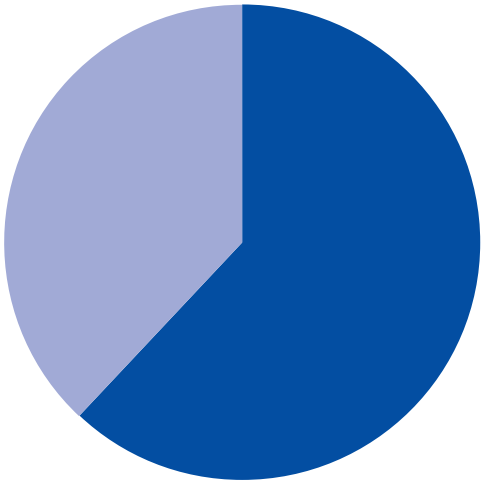
Cybercriminals often use other techniques to spread malware. Evasive malware has been rising in recent years and poses a great risk to MSPs and their customers because it is hard to detect and can evade signature-based antivirus solutions.

Emotet is still active, dubbed “the most dangerous malware” by Europol. It is a malware strain first detected back in 2014 and originally designed as a banking Trojan. It has remained active and evolved over time to become one of the most prevalent threats that tries to infiltrate other computers on a network once it has infected a device. Emotet most commonly appears in spear-phishing as email attachments (mostly Word documents) or downloadable links. When users open the files they are asked to “enable macros,” which installs Emotet malware on their computers.

Ransomware

Ransomware is one of the top cyberthreat concerns for organizations. This form of malware is commonly downloaded or installed by a threat actor after compromising and gaining access to a system. With the cloud expanding and hosting more data, it’s no surprise that ransomware attacks are increasing and more and more victims are willing to pay to recover their data – 62% of organizations were victims of ransomware and 58% of victims paid the ransom in 2020. Getting data back is not a guarantee – 33% of the 58% of victims walked away with zero data recovered. The good part is that majority got their data. The bad part is that it turns into a chain reaction where threat actors launch more ransomware attacks knowing more organizations are willing to pay. The point is, you and your customers don’t want to deal with this scenario. Cybercriminals target managed service providers (MSPs) – as the saying goes, *MSPs hold the keys to the kingdom* and a successful attack on an MSP opens the door to an entire customer base and their data. In 2019, 22 municipalities in Texas got hit by a ransomware attack spread through MSP tools. Exploiting the remote monitoring and management (RMM) software commonly used by MSPs is lucrative for threat actors.

Ransomware Victims 2020



62% of organizations were victims of ransomware

Again, email comes into play. It’s an easy entry point for ransomware. One click on a malicious link or downloading a malicious attachment can take down an entire network.

Spam

Spam is still a thing, though it is a very old method -- the first known spam email was sent in 1978. Today, many companies don't even consider it a threat, but it is still efficient. Modern spam can be a vehicle for more complex and targeted attacks. It was found that, in 2019 – 2020, 42% of CISOs had to deal with at least one incident caused by spam and that 13% of data breaches were a result of spam, as in this blog article, "Are you ready for the post-spam era".

Mitigate Email Security Risks for Your Customers

In this section, we cover steps that can help you evaluate email security and ultimately reduce risks for your customers.

Take a step back, evaluate.

Evaluate the effectiveness of your current email security solution and determine if it truly lives up to the standard of protection required. Consider remote working in your evaluation. Technology must help protect against human error and the vulnerabilities presented by a remote working culture.

Take into account that legacy email security solutions are not designed to tackle the complexities of highly sophisticated targeted attacks or handle complicated mail flow. Most include AV and anti-spam engines, but to deal with today's modern email threats, email security solutions need to go further in terms of the features they offer and the quality of their AV and anti-spam filters.

Deploy strong cloud-based email security

Protecting your customers against today's sophisticated attacks requires powerful and reliable security solutions. Modern, cloud-based email security solutions are generally very fast to react to new spam waves and handling false negatives and false positives – and can help reduce deployment time and costs compared to on-premise solutions.

We recommend to look for a solution that includes layers of algorithmic analysis, threat intelligence, executive monitoring, real-time link scanning and machine learning to defend against advanced email threats. Algorithms are king when it comes to identifying and stopping threats. They are among the most effective ways to protect email from modern threats. Traditionally, email security tools worked using pattern-based approaches, looking at messages for elements that had already been observed in a live spam run, or a previous spam run. This approach is still valuable, although fairly rudimentary. But, as threats have evolved, email security tools have had to as well. A strong solution includes extra spam classification features to emphasize when an email is phishing, extortion or carries malware.

Enhanced image content analysis and improved control over email flow capabilities can further strengthen email protection.

Threat intelligence is becoming increasingly important in many aspects of security. If an attacker sends a simple plain text email from a legitimate server/domain that hasn't just been registered, where the server matches the domain, with an IP address that isn't blacklisted, that has valid MX and SPF record, then there may be nothing to identify the email – algorithmically or otherwise – as malicious. Threat intelligence may provide a crucial additional layer of defense. Domain-based Threat Intelligence will provide a high-risk rating if the registrant has a criminal track record of registering domains and using them to launch attacks or distribute malware.

Support for SPF, DKIM and DMARC are important to help protect against domain-based spoofing emails when used in combination with other technologies and checks, like IP reputation, domain reputation, email reputation, domain and link analysis, RFC alignment, content checks, signature checks, inspection of headers etc.

Email is a vehicle for sharing a lot of sensitive information. Many organizations, especially those in financial, legal or health sectors, require email encryption capabilities. An email security solution with a strong email encryption tool included helps protect sensitive information in transit.

Accuracy is key. Email security solutions should be powerful in terms of delivering clean email to users' inboxes, but it needs to strike a balance and not block important email communication. The last thing you want is to lose out on sales opportunities because an email was incorrectly classified and landed in your junk folder. Review the accuracy and false positive rates of solutions during your evaluation. Most vendors offer free trials, and this is the best way to see if a solution is suited to you and your customers' environments.

Consolidate security

For strong protection, all security tools must talk to one another to share security context, data and events. Combining this data with threat intelligence that provides information on known bad files, security solutions can make decisions based off of real-time information. This can only be achieved with a unified security platform.

A unified security platform that consolidates all security features in one console can also help simplify and automate management of tasks so your teams can focus on billable tasks and strategic priorities. Offering your customers a security bundle with the key security solutions and tools included in one easy-to-use console can simplify management and drive adoption much more effectively than a variety of disparate solutions and tools across your customer base.

Add additional layers of security

Many businesses are moving to cloud solutions like Microsoft 365 and Google Suite to take advantage of the collaboration tools these vendors offer. Forbes predicted that 83% of enterprise workloads would be in the cloud in 2020 and two thirds of IT professionals responsible for managing these changes say that security is their greatest concern.

While both Microsoft 365 and Google Suite include built-in security, it comes with some limitations. Relying solely on one layer of security can leave your customers vulnerable. Layering advanced protection – and choosing third party security solutions complimentary to the Microsoft platform – is an approach advocated by analyst firm Gartner. As an MSP, you should look for an email security solution that is compatible with all email services. It should also seamlessly integrate with Microsoft 365 so you can onboard end-customers easily, helping increase efficiency across your business.

Drive User Awareness Training

While security solutions are essential, it is just as important to take user behaviour and awareness training into account when reviewing security strategies. The boundaries between work and life activities have blurred, and many employees are engaging in non-work related activity on the web, like streaming Netflix or Amazon Prime Video, and reading private email on work devices. All in all, it comes down to helping your customers develop a true culture of security.

According to research by Osterman, employees who consider adhering to an organization's security best practices as part of their responsibilities are more likely to be sensitive to phishing, spear-phishing and business email compromise, and will take additional steps to ensure the security of sensitive company data. They will be more attentive to complying with protocols related to regulations like GDPR. Security will become second-nature to them.

As an MSP, understand the behavior of your customers' employees and where they may need further education.

This topic extends to user processes. Many employees in financial-type roles would previously verify 'urgent bank transfer' requests by walking over to a person's desk. In current conditions, many skip this verification step and employees rely on the authenticity of email credentials that are easily replicated by scammers. This is where CEO Fraud comes in. It is key to review security processes to include not only multiple layers of security tools, but also different layers of checks to compensate for new ways of working, like verifying payment requests above certain amounts using a method other than email.

Choose better protection with third-party research

Independent testing by third parties can help your decision making process and confirm the quality of technologies used in solutions.

Email Security: Part of Your MSP Security Stack

Cybercriminals continue to evolve their techniques and have shifted their mindset from a few years ago where they would only target large organizations. In today's threat landscape, their primary concern is obtaining credentials and personal data regardless of the size of their victims, according to findings by Verizon. The Data Breach Investigations Report 2020 found that threat actors are targeting both large and small organizations – with the top threat actions being phishing, use of stolen credentials, and password dumpers.
Your customers are prime targets.

For MSPs, it's imperative to stay ahead of cybercriminal activity and have their 'own house' in order in terms of security best practices, before rolling it out to customers.

Email security is an essential part of a security strategy that can help you:

1. **Strengthen your customers' security posture:** Your customers are constantly at risk of falling victim to cyberattacks. Quantifying your customers' risks, identifying gaps in their security and increasing their security posture by giving them the right level of protection and combination of security solutions lowers their cyber risk and increases cyber-resilience – resulting in peace of mind for both you and them.
2. **Differentiate your service offering with layered security:** Adding additional security services and tools to your offering can help you stand out among competitors and drive growth.
3. **Grow your business by expanding your service offerings:** Adding email security to your MSP security stack adds more value to your service offering, especially if this is included in one platform or console for ease of access and use. This also opens doors to upselling to existing customers and drives an additional revenue stream.
4. **Drive profitability by reducing time spent on managing email security issues:** Managing issues related to spam outbreaks or phishing attacks is time-consuming. By adding a professional email security solution that can decrease time spent on remedying issues, you free up time for your internal security team to pursue higher-level strategic business objectives.
5. **Support compliance:** Many businesses in regulated industries that need to comply with industry-regulated bodies, like FRCP, SOX and HIPAA, require robust encryption of data in transit. Having email security with strong encryption capabilities can help you better meet your customers' compliance requirements.

Conclusion

Email is vital for businesses to operate, but it's also the #1 attack vector. It's essential to include strong, reliable email security in your security stack to protect against modern threats. Including it as part of a consolidated security bundle is ideal.

Bitdefender GravityZone Email Security is designed for **efficiency** and ultimate **protection**.

Bitdefender offers a multi-layered, cloud-based email security solution designed for organizations and managed service providers. Multiple scanning engines and behavioral technologies protect inboxes against spam, viruses, phishing attacks, ransomware, malware and other email-borne threats.

The solution is available as an add-on as part of GravityZone's unified security and risk analytics platform. The unified risk analytics, hardening next-gen AV, EDR, and MDR, in a single MSP platform with extensive API and RMM integrations can help automate tasks and reduce security efforts and costs. Combining endpoint protection and email security in one easy-to-use console can help you easily strengthen the security posture of your customers and maximize working from home protection.

Grow Revenues, Consolidate Security and Reduce Costs with GravityZone Cloud MSP Security.

Learn more and try the full Bitdefender MSP Security Suite

Go to www.bitdefender.com/msp and fill in the free trial form or create a customer company with Monthly Trial License in GravityZone.

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is the industry's trusted expert* for eliminating threats, protecting privacy and data, and enabling cyber resiliency. With deep investments in research and development, Bitdefender Labs discovers 400 new threats each minute and validates 30 billion threat queries daily.

The company has pioneered breakthrough innovations in antimvalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 150 of the world's most recognized technology brands.

Founded in 2001, Bitdefender has customers in 170 countries with offices around the world. For more information, visit https://www.bitdefender.com.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

*Bitdefender has ranked #1 in 54% of all tests by AV-Comparatives 2018-2021 for real-world protection, performance, malware protection & advanced threat protection.

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-MSP-Email-Security-Guide-cpress53102-210x297-en_EN
12.04.20 April 12, 2021 9:24 am 04/12/21