at bay

Email Security: A Practical Buyer's Guide for Growing Businesses

How to assess email security solutions, evaluate vendors, and get the protection your business needs

at-bay.com

Table of Contents

Introduction 3

Why Is Email Creating So Much Cyber Risk? 4

An Overview of the 3 Types of Email Security Solutions 6

Questions to Ask Your IT Provider About Your Email Security 9

What Is MDR for Email? 10

Choosing the Right MDR Provider for Your Email Security 13

Making Email Security Work With Your Budget 14

The MDR for Email Buyer’s Checklist for Emerging Businesses 15

MDR for Email: Fortifying Your Inbox 16

Introduction

Email is how most companies conduct business today. From setting up meetings, to sending contracts, to invoicing clients and paying vendors — it all happens over email. But because email is where the majority of business financial transactions are coordinated, cybercrime targeting email is also a booming industry.

In fact, data from At-Bay's 2024 InsurSec Rankings Report shows that email-based cybercrimes are not only among the most common for businesses, they're also on the rise.

Preventing email incidents is increasingly complicated, especially with the advent of AI-driven phishing and sophisticated financial fraud. Unfortunately, the security settings built into email solutions are insufficient against rapidly evolving cybercrime tactics, and even secure email gateways (SEGs) fall short of holistic protection.

Email-related cyber incidents increased by 48% from 2021 to 2023.

Source: At-Bay claims data

Businesses of all sizes now need modern cloud-based security tools coupled with around-the-clock surveillance to secure their inbox.

Managed Detection and Response (MDR) for Email combines modern security technology with a team of experts that provide proactive protection and swift response to email security incidents. This solution ensures vulnerabilities in email systems are addressed and mitigated before they can be exploited, without requiring businesses to build and resource an expensive in-house security team.

In this guide, you'll find everything you need to know about MDR for Email, the threats these solutions protect against, the security technology they employ, and how to shop for the right vendor.

Why Is Email Creating So Much Cyber Risk?

Email attacks are one of the highest-volume threats organizations face because attackers can rapidly send out hundreds or thousands of malicious emails across multiple organizations simultaneously. Unfortunately, small businesses are disproportionately vulnerable. According to data from Symantec, employees at smaller organizations are more than 2X as likely to receive phishing, malware, and spam in their inbox.

Phishing remains the primary vector for email security compromises, preying on human vulnerabilities to manipulate victims into actions like clicking on malicious links or downloading harmful files. The rise of AI has exacerbated the problem. Threat actors now leverage AI language tools to craft highly convincing and context-aware phishing emails, making it increasingly challenging for victims to discern legitimate communications from malicious ones.

AI Has Made Employee Training Less Effective

Traditional phishing awareness training, which focuses on spotting spelling errors and grammatical mistakes, has become less effective as AI-generated content creation removes these telltale signs. Businesses can no longer rely completely on this method of phishing prevention.

Further complicating email security is the increase of sophisticated financial fraud. In these now-common scenarios, attackers mimic known contacts and exploit a sense of urgency to trick employees into completing seemingly legitimate but ultimately fraudulent financial transactions. Such maneuvers include redirecting payroll to attackers' accounts or inducing unauthorized payments through deceptive invoices.

Financial fraud was the most common cybercrime committed via email in 2023, accounting for 61% of At-Bay email claims.

Source: At-Bay claims data

Financial fraud can also come from inside the company network through business email compromise (BEC). In a BEC attack, a hacker breaks into a victim's email (commonly through stolen credentials, social engineering, or another vector) and researches the individual, their company, and the company's vendor relationships to identify an opportunity to intercept a financial transaction. The attacker then uses the hacked email account to communicate with a third-party vendor, diverting communications away from the real user's inbox.

Traditional Security Tools Often Fail to Spot Complex Financial Fraud Like BEC

BEC tactics are highly effective because all communications come from a legitimate email account and discuss an expected transaction. These and other financial fraud attacks are accomplished without the typical red flags of phishing attempts that traditional security tools scan for, like malicious links and attachments, meaning they are unlikely to be identified — much less prevented — by these tools.

The ongoing escalation in complex attack tactics underscores a critical gap in existing security solutions, which is why email continues to create outsized cyber risk — especially for growing businesses without extensive security resources and expertise.

An Overview of the 3 Types of Email Security Solutions

There are three types of email security solutions available: security functions built into your email solution, secure email gateways (SEGs), and modern cloud-based security. Each has its own advantages and limitations.

The foundation of email security is the security built into your email solution, but this does not provide comprehensive protection against modern threats. An additional layer of security is necessary. SEGs are the most common option for added email security. They act as a gatekeeper for the email environment, but they're insufficient in blocking all malicious activity — especially threats coming from inside the network. The better option is cloud-based email security, which can protect from both external and internal threats.

	Native Email Security	Secure Email Gateway	Integrated Cloud Email Security	Managed Cloud Email Security
Protects against well-known threats	✓	✓	✓	✓
Protects against external phishing attempts		✓	✓	✓
Protects against modern email attacks like BEC			✓	✓
Protects against credential theft & account takeover (ATO) attacks			✓	✓
Protects against personal & VIP impersonation			✓	✓
Protects against internal email attacks			✓	✓
Protects against GenAI social engineering attacks			✓	✓
Protects against financial fraud				✓
Actively monitors & investigates your user-submitted phishing inbox				✓
Actively manages your email security for you				✓

Security Built Into Your Email Solution

The built-in security controls included with your email solution can provide a basic layer of protection, but they're often insufficient to protect businesses from evolving attack tactics. These functions focus on identifying known threats, like previously used malicious email addresses or potential phishing links, targeting the 'low-hanging fruit' of email security threats. Built-in security controls may filter suspicious-looking emails into a spam folder or add a banner on emails from unknown senders to alert users of potential risks.

Unfortunately, there's a large difference in the effectiveness of built-in security between different email providers. This means that simply relying on default settings and controls in the most commonly used email providers can leave businesses exposed.

> Businesses using Google Workspace saw 3X fewer incidents in 2023 than those using Microsoft 365.
>
> Source: At-Bay claims data

Google's security measures are typically enabled by default, whereas Microsoft prioritizes user experience over stringent security, even when built-in features are activated. Google also offers better security capabilities in areas like forwarding rules and inbox manipulation — critical defenses against BEC, which is involved in nearly two out of every three financial fraud incidents.

Secure Email Gateways (SEGs)

SEGs act like a vigilant guard at the entrance of your business's email that all incoming messages must pass through before they land in any inbox within the organization. Every incoming email is examined thoroughly for threats like malicious links and attachments before being allowed in.

Unfortunately, SEGs are not infallible. While these tools provide better security compared to built-in functionalities, the amount of protection they offer differs drastically between providers.

In At-Bay's 2024 claims-based analysis of six popular SEGs, only two were associated with better outcomes than the average: Mimecast and Proofpoint. Mimecast was the top performer by far for the second year in a row, with users experiencing 37% fewer incidents than average.

Still, even the best SEGs tend to concentrate primarily on external threats, which means they don't typically monitor internal movements once an email has passed into the organization. This limitation can be significant if a threat does manage to bypass the initial screening or if an attacker infiltrates an organization's network. SEGs are also known for creating some operational friction by occasionally mistaking legitimate emails for threats, potentially delaying important communications and requiring additional administrative oversight to retrieve legitimate emails.

Modern Integrated Cloud Email Security Solutions

Modern cloud-based email security solutions are designed to address the limitations of built-in security and SEGs. These sophisticated systems leverage AI to deeply analyze not only links and attachments but also the content of emails themselves, assessing the tone, intent, and urgency to identify signs of complex attacks like BEC and callback phishing.

Cloud-based email security solutions can even detect impersonation tactics where an attacker pretends to be a vendor or coworker to trick employees into divulging confidential information or making unauthorized transactions. These tactics represent a major threat: In 2023, almost half of all financial fraud occurred as an impersonation. In addition, among those attacks, attackers impersonated a vendor 36% of the time, and they impersonated someone in the business 11% of the time.

Cloud-Based Email Security Solutions Don't Serve the Needs of Small Businesses

Despite their advanced capabilities, standalone cloud-based email security solutions can create new challenges — especially for smaller businesses with limited resources — due to the high volume of alerts they generate. Reviewing each alert means significant work for already-busy IT teams, not to mention taking remediation action when needed.

The 'noise' generated by frequent and sometimes false alerts can lead to alert fatigue, where critical warnings might be overlooked or dismissed by companies without a dedicated email security team. Further, significant expertise is required to properly integrate these technologies into existing IT infrastructures, to fine-tune settings according to the specific needs and threat exposure of the business, to review and assess the alerts generated, and to take action against threats when needed.

Questions to Ask Your IT Provider About Your Email Security

If you already have a SEG provider or an MSP managing your email security, it’s a good idea to check in to make sure that your inbox is as secure as possible. Here are the questions to ask:

QUESTION TO ASK	WHAT TO LOOK FOR
Do we have any kind of email security solution in place today? If so, what solution is it and what does it protect against?	It’s important to have a solution that can protect against social engineering, phishing attempts, and BEC.
If we have a SEG, does it identify indicators of BEC, both from internal and external sources?	BEC is one of the most common types of email threats, and legacy systems may not protect against it.
How is our email security solution configured? Is it using default settings, or has it been customized to our specific needs?	The most effective email security will be tailored to your business’s unique needs and risks.
Who is responsible for monitoring and managing the alerts generated by our email security solution?	If no one is monitoring and managing these alerts, they probably aren’t being addressed in a timely manner.
Do you regularly meet with us to review and adjust our email security configurations based on emerging threats or changes in our organization?	Threat actors adjust their tactics often, so security must remain current to avoid falling behind.
Have we ever experienced a successful phishing attack or email-based security breach?	Phishing attacks are incredibly common. If your business has been attacked, it’s important to understand what happened and what was done about it to prevent future incidents.
Do we have regular phishing awareness training for our employees? How confident are you that our employees can identify and stop phishing attempts?	Any employee can be targeted in a phishing attack. Most phishing trainings track the progress of each employee so you can be sure to provide targeted trainings and education for those who need it.

What Is MDR for Email?

Managed Detection and Response for Email solves businesses' dual problem of security and staffing. It pairs a modern cloud-based email security solution with an expert security operations team to monitor your email environment, maintain proactive email security, identify and investigate potential threats, and take action when needed.

> With MDR for Email, organizations get advanced threat detection and response capabilities without the need to build a dedicated, in-house security operations center (SOC).

The MDR team handles the constant influx of email security alerts that would otherwise strain your team's bandwidth, providing expert guidance, proactive threat hunting, and rapid incident response. Ultimately, MDR for Email enables you to focus your time and energy on your core business operations while knowing that your email environment is secure.

How Does MDR for Email Work?

An MDR for Email service typically does the following:

1 **Deployment and Configuration**

The MDR provider deploys its cloud-based email security solution within your environment, integrating with your existing email infrastructure. The solution is tailored to your organization's specific needs and risk profile.

2 **Continuous Monitoring**

The MDR team continuously monitors your email traffic, leveraging advanced technologies such as AI and machine learning to identify suspicious activity, anomalies, and potential threats.

3 **Threat Detection and Analysis**

When a potential threat is detected, the MDR team investigates and analyzes the incident, leveraging their expertise and threat intelligence to determine its severity and impact.

4 **Threat Mitigation and Response**

If a threat is confirmed, the MDR team takes immediate action to mitigate and contain the threat. This may involve blocking malicious emails, quarantining compromised accounts, or implementing other remediation measures.

5 **Incident Reporting and Recommendations**

The MDR provider provides detailed reports on detected threats, including their nature, impact, and the actions taken to mitigate them. It also provides recommendations for improving your email security posture and preventing future incidents.

6 **Continuous Improvement**

The MDR service continuously adapts and evolves to address new and emerging email-based threats, ensuring that your organization remains protected against the latest attack vectors.

What Threats Does MDR for Email Protect Against?

MDR for Email is designed to protect against a wide range of email-based threats that can compromise your organization's security and lead to financial losses, data breaches, and reputational damage. Following are some of the key threats that MDR for Email can mitigate:

Malicious Payload (Malware and Ransomware)	An attack where an email from a threat actor is crafted and delivered containing a malicious payload or link that can damage a victim's computer or steal sensitive information.
Business Email Compromise (BEC)	An attack where a threat actor gains access to a work email account to trick someone into sending money or stealing sensitive data.
QR Code Phishing (Quishing)	An attack in which a threat actor creates QR codes to redirect victims into visiting malicious sites or downloading malicious content.
Credential Theft Phishing	An attack where a threat actor devises tricks to steal personal credential information like a username, password, and security token combination.
VIP Impersonation	An attack that occurs when a threat actor sends an email to a victim using a compromised or faked email address of a VIP, trusted individual, or legitimate company.
Callback Phishing	An attack where a threat actor sends an email with a phone number to call, typically claiming that there is an urgent issue.

Choosing the Right MDR Provider for Your Email Security

When selecting an MDR for Email provider, it's crucial to evaluate several key features and considerations to ensure it aligns with your organization's specific needs and requirements.

Make sure your vendor...

Includes 24/7 management.

Email threats can strike at any time, so it's essential to have a solution with around-the-clock monitoring and management by a team of security professionals. Look for an MDR provider with 24/7 coverage from a dedicated SOC, ensuring your email environment is continuously protected.

Handles alerts as they come through.

MDR for Email should include a dedicated team of cybersecurity experts who can promptly investigate and respond to email security alerts on your behalf. Ensure that the provider has a well-defined process for triaging, analyzing, and mitigating threats in a timely manner.

Leverages AI to identify anomalous behavior.

Modern email threats are increasingly sophisticated, often leveraging AI and automation techniques. An effective MDR for Email solution should counter these threats with its own AI engine that can identify anomalous behavior and keep up with evolving attacker tactics.

Provides AI decision transparency.

The AI system powering the cloud-based email security solution should be able to explain the logic for each red flag it raises, providing transparency and reliability in its threat assessments.

Manages your dedicated phishing inbox.

A dedicated phishing inbox can be invaluable when multiple employees are targeted by phishing campaigns. It centralizes the reporting and analysis of suspected phishing attempts, allowing the MDR team to quickly identify and respond to emerging threats.

Making Email Security Work With Your Budget

Small businesses have fewer resources to protect their email environment from threats — but they face just as much cyber risk as larger businesses, if not more. One of the primary benefits of MDR for Email is that it can save small businesses time and money by outsourcing email security to a team of experts.

Instead of hiring and training in-house staff to manage email security, small businesses can leverage the expertise of an MDR provider's security analysts and engineers. This not only reduces the need for additional personnel but also eliminates the costs associated with training and maintaining an in-house security team.

MDR for Email can provide further cost savings by reducing the risk of cyberattacks and data breaches. A successful email-based attack can result in significant financial losses, including remediation costs, regulatory fines, and reputational damage. By proactively detecting and responding to email-based threats, MDR for Email solutions can help small businesses avoid these costly consequences.

In 2023, the most common email attack — financial fraud — cost businesses an average of $219K per incident.

Source: At-Bay claims data

Additionally, some MDR providers offer pricing models tailored to the needs of small and medium businesses. Instead of paying for an enterprise-level solution with features and capabilities that may not be necessary, opt for providers that offer a more streamlined and cost-effective service that focuses on the essentials of email security. By carefully evaluating their requirements, exploring pricing options, and considering the potential cost savings and benefits, emerging businesses can make email security work for their needs within their budget.

The MDR for Email Buyer's Checklist for Emerging Businesses

QUESTION TO ASK	WHAT TO LOOK FOR
What is your onboarding process?	Choose a provider that has a relatively simple onboarding process and will guide you through each step on a timeline that works for you.
What experience does your staff have?	The provider you choose should have the expertise to understand the specifics of your business and industry, and the diverse backgrounds to respond to potential threats. Some common analyst skills include digital forensics, incident response, information security, or law enforcement.
What are the terms of the contract?	Your provider should be able to give you the specifics on how the contract is structured, including costs, duration, and termination clauses. Ask if they are aware of any potential benefits or discounts from cyber insurance providers.
What services are provided in your MDR for Email service? Does it include 24/7 coverage?	Email attacks can happen at any time, so you want someone watching and responding to potential issues 24/7. Make sure your MDR for Email provider has around-the-clock coverage so that you can focus on running your business — and living your life.
What insight into up-to-date, real-world cyber claims do you have?	Some MDR for Email providers have access to cyber claims and data from actual security incidents. This insight into real risks allows them to offer more informed advice and deliver solutions that enhance overall security more effectively.
What type of response actions do you take when you detect an issue?	When an incident occurs, it's important to have an MDR for Email provider that will take action to remediate the issues with an immediate response. Some providers limit their role to simply alerting you of issues (via email), rather than actually handling them. The best providers will align with you on when their analysts will respond and when they will escalate to you.

MDR for Email: Fortifying Your Inbox

Investing in the right MDR for Email service can help small businesses strengthen their email security posture through continuous monitoring, expert investigation, swift response, and timely notification.

At-Bay Stance™ MDR for Email leverages AI-powered email threat detection and response technology to find things a SEG might miss, helping enhance customers' cybersecurity posture with 24/7 monitoring of their email environment by cybersecurity experts. It's a key part of InsurSec, which combines At-Bay's insurance expertise, world-class cybersecurity team, and market-leading security software for better security outcomes. With Stance MDR for Email, At-Bay takes enterprise-grade email security and makes it affordable for small businesses.

At-Bay Stance MDR for Email is provided by At-Bay Security, LLC, a wholly owned subsidiary of At-Bay, Inc. At-Bay Security, LLC does not provide insurance services. Insurance placed through At-Bay Insurance Services, LLC is not a condition to purchase At-Bay Stance MDR for Email.

Book an appointment
at-bay.com/mdr-meeting

The information contained is for general guidance on matters of interest only and is not intended to be construed as the rendering of professional services of any kind. If professional advice is required, the services of a professional should be sought.

at bay

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form. At-Bay Insurance Services LLC is a licensed insurance agency and surplus lines broker in all fifty states and the District of Columbia.