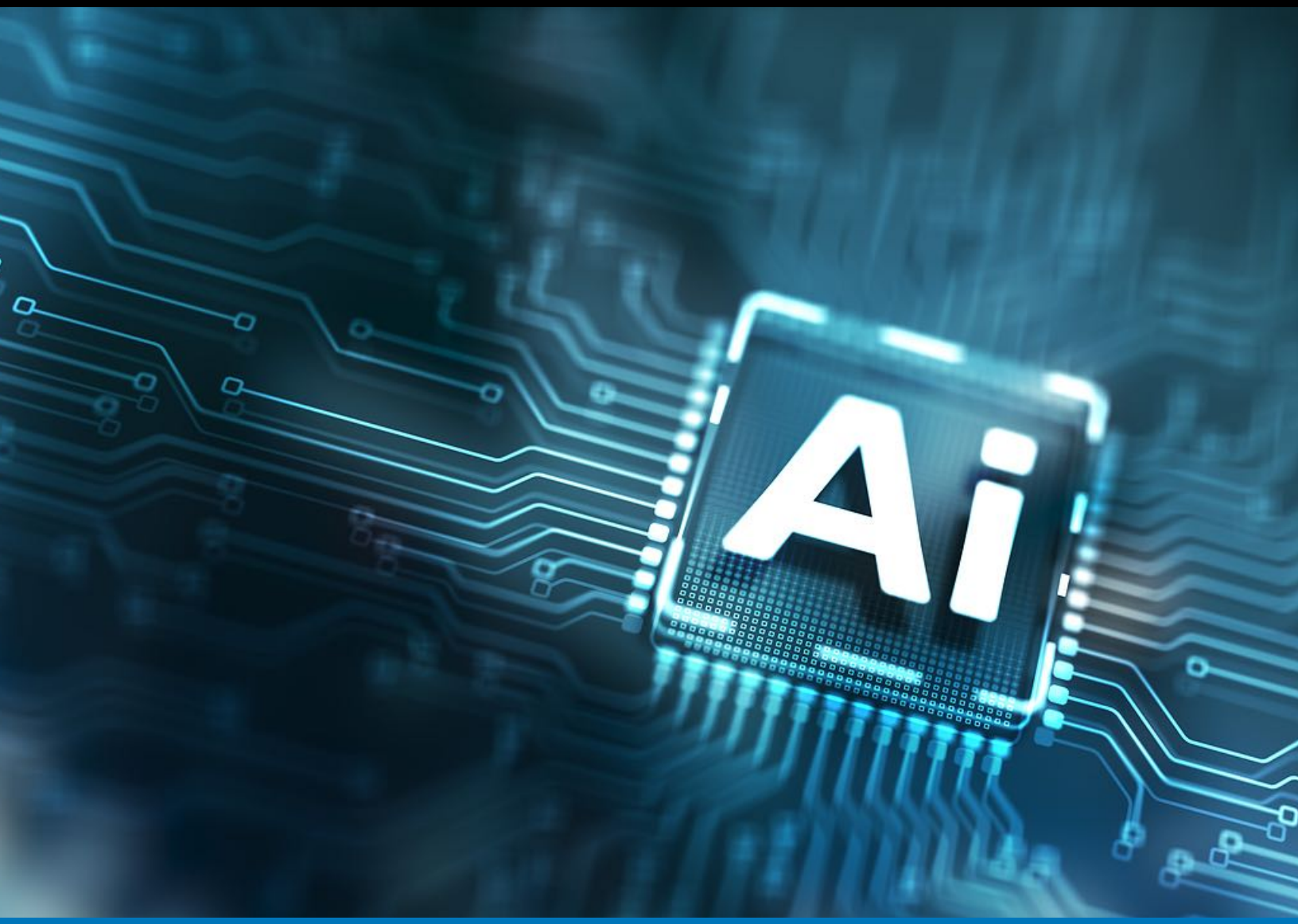
White Paper by Osterman Research



The Role of AI in Email Security

Published **August 2023**

Sponsored by **Abnormal Security**

Executive Summary

Email is one of the most common ingress points into organizations for threat actors. As organizations have implemented email security solutions and trained employees to recognize email attacks, threat actors have pivoted to more advanced methods that bypass protections. They have also embraced artificial intelligence (AI) to make attacks more scalable and personalized while also less detectable.

Email security vendors are using AI in their defensive tools to stop attacks that leverage new and emerging attack methods in email. Many organizations have gained AI-enabled protections by virtue of their incumbent email security vendors adding AI capabilities to strengthen defensive posture. In addition, most have gone shopping for new solutions offering AI to bolster the baseline protections offered by cloud email providers.

When purchasing AI-enabled solutions to strengthen email security, organizations want the ability to protect more than just email, automated mitigation and remediation of identified threats, and next-generation capabilities to safeguard employees, the organization, and its customers, suppliers, and business partners.

KEY TAKEAWAYS

- **Cybercriminals are already using AI in email attacks**
  Threat actors are making higher use of emerging attack methods—many enabled by AI technologies—that circumvent traditional email security defenses and reach the inboxes of their targeted victims. Organizations expect cybercriminals to continue to innovate in how AI is used in email attacks.
- **Organizations are strengthening defenses with new AI-enabled tools**
  With the changing threat environment in email, organizations are implementing new defenses. Nine out of ten organizations have implemented an AI-enabled email security solution beyond what is offered by their cloud email provider.
- **AI capabilities are safeguarding and improving detection efficacy**
  Four out of five organizations indicate that AI-enabled email security solutions have enabled them to safeguard or improve the efficacy of detecting multiple types of threats in email, even as threat actors have changed their attack methods.
- **Organizations want to protect more than just email via AI**
  Buyers of AI-enabled email security solutions want the ability to protect email as well as the other communication and collaboration applications used across the organization, such as Microsoft Teams, SharePoint, OneDrive, Zoom, Slack, and Salesforce. From the buyer's perspective, AI has a role in defending against threats in more than just email.
- **AI-enabled detection without responsive mitigation is misguided**
  Strengthening capabilities for detecting threats in email via AI is an essential first step, but it can't end there. Organizations must train cybersecurity professionals and SOC teams to respond quickly and effectively to identified incidents, leveraging the best of what AI brings to the table.

Organizations expect cybercriminals to continue to innovate in how AI is used in email attacks.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Abnormal Security. Information about Abnormal Security is provided at the end of this paper.

Why AI for Email Security?

Email is a key attack vector for threat actors who seek confidential information, account credentials, and financial gain from their victims. In response, organizations have adopted email security solutions to analyze inbound, internal, and outbound email traffic to identify malicious messages to stop attacks before they become costly incidents. Threat actors are continually modifying their attack patterns to improve the efficacy of their crimes, and organizations their defensive posture to stay one step ahead.

Traditionally, email security solutions have relied on detection methods such as signatures ("we've seen this message before"), rules ("don't allow messages with EXE attachments"), blacklists/blocklists ("always block all messages from this domain") and whitelists/allow lists ("email from these domains is always good.") These methods continue to detect and block many attacks.

The capabilities of these traditional methods have been exceeded, however, by cybercriminals adding new attack methods to long-running attack types. These new and emerging attack methods have created forms of spear phishing, business email compromise, executive impersonation, and other types of attacks that rely on malicious intent (not links or attachments), the compromise of high-reputation email accounts, impersonation, and social engineering. Traditional email security defenses struggle to detect the presence of these malicious signals and markers; without the use of new AI-enabled detection methods, they assume all is well.

Threat actors will never stop wanting to steal account credentials, redirect payroll and invoice payment to bank accounts under their control, and gain access to data for extortion.

HOW CYBERCRIMINALS USE AI IN EMAIL ATTACKS

Threat actors are making higher use of attack methods that circumvent traditional email security defenses to reach the inboxes of their targeted victims. Threat actors are keen to continue stealing account credentials, redirecting payroll and invoice payments to bank accounts under their control, and gaining access to data that can be weaponized for extortion. **This is an enduring dynamic**, and at times, a Sisyphean challenge for organizations.

Cybercriminals are using AI in email attacks in multiple ways, for example:

- **To create unique attacks at scale**
  Polymorphic techniques morph multiple aspects of an email message—e.g., the subject line, sender, wording, sending infrastructure—to create unique attacks that bypass signature-based detection methods. AI technologies offer threat actors the perfect bar for mixing malicious cocktails that are targeted, unique, and generated at scale—think spear phishing and business email compromise attacks on steroids.
- **To mimic the writing style, tone, and mannerisms of the supposed sender**
  AI services can be used to analyze the stylistic and grammatical nuances of any given person, creating near-perfect matches that the person didn't write—but could have. Think high-efficacy executive impersonation, email thread hijacking for pretexting, business email compromise attacks, and more.
- **To improve baseline message grammar quality**
  The presence of spelling mistakes and bad grammar has tipped off many intended victims that an email message is malicious. However, the recent emergence of generative AI services, such as ChatGPT and malicious equivalents such as WormGPT, has enabled threat actors to increase the quality of their writing and decrease the easy giveaways of malicious intent.

Any ethical concerns about AI's use by governments and organizations are not shared by cybercriminals. What cybercriminals do is fundamentally unethical, and AI is but another tool to increase the scale, cadence, and efficacy of cyberattacks.

HOW VENDORS USE AI IN EMAIL SECURITY

Given the changing threat landscape in recent years, established vendors have augmented their solutions with AI capabilities while emerging email security vendors have entered the market with solutions designed around AI and machine learning (ML). As security leaders demand modern security tools to prevent modern attacks, the changing threat landscape demands the use of AI by any vendor wanting to be relevant to current and potential customers.

Vendors are using AI to improve email security capabilities and processes, such as:

- **To understand the behavior and profile of each sender and recipient**
  An AI model is created to profile the sending and receiving pattern of each person in the organization. For individuals: who sends messages to them? What are the messages about? When are these messages sent and from where? Is anyone else normally copied, or is the email sent to a single recipient? What email address or addresses are used by each sender? In other words, AI is used to create a picture of what is normal for each person.

- **To detect anomalous sending patterns**
  A combined analysis of baseline sending patterns (created and maintained using social graphing techniques); derivative and near-match email addresses; messages that contain social engineering triggers; the presence of impersonated logos and other visual brand elements; and the classification of tone, emotion, and style in an email message can be used to detect anomalous email messages that are obfuscated to human sense-making processes. Although employees have been trained through security awareness programs to look for messages bearing these out-of-place signals, AI brings together these disparate analysis strands at the speed of cyber, the only way to ensure consistent and reliable application in the face of growing message volumes.

- **To identify content written by generative AI tools, especially malicious content**
  With threat actors using generative AI tools to create sophisticated and convincing email threats, email security vendors are adding AI models capable of detecting such usage. These models decode the semantic context of the email to identify recurring patterns in generated messages, and especially malicious context and intent.

- **To create derivative training data for ML models**
  AI-based solutions detect messages carrying malicious intent by reference to multiple ML models, which are developed, refined, and updated using training data composed of, for example, messages that have been classified as malicious or benign. Some vendors use generative AI services to create additional message samples off a known malicious message, which expands the known-good training data available to the ML model.

- **To strengthen incident response and remediation processes**
  AI acts as a force multiplier for understaffed and under-resourced incident response and security operations teams by providing improved accuracy, scalability, prioritization, and real-time mitigation of email threats.

The changing threat landscape demands the use of AI by any vendor wanting to be relevant to current and potential customers.

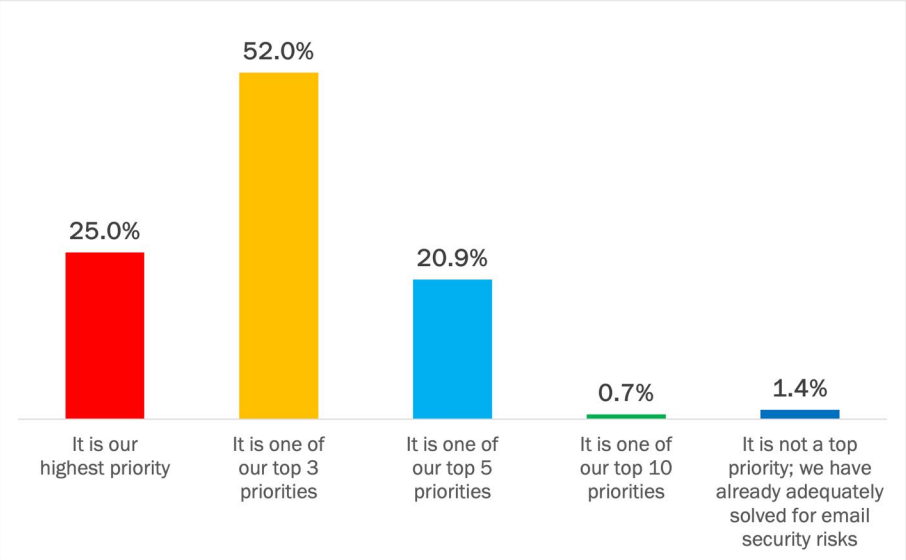
Trends in Email and Email Security

Email is a critical communications system for organizations, and by implication, email security ranks extremely high on the list of security and risk initiatives. AI is being used by email security vendors to protect email and by cybercriminals to compromise and undermine it.

VERY HIGH PRIORITY FOR EMAIL SECURITY

Almost four out of five organizations rate addressing email security risks as a top-three priority for their organization relative to all other security and risk initiatives. This breaks down into 25% indicating it is their highest priority, and 52% indicating it is priority two or three. See Figure 1. For nearly every other organization, it was in the top five priorities, showcasing how prevalent email is for security leaders.

Figure 1
Priority of Addressing Email Security Risks Relative to All Other Security and Risk Initiatives
Percentage of respondents



Source: Osterman Research (2023)

Addressing email security risks is a top-three priority for four out of five organizations.

What is it about email that makes it deserving of such high relative priority?

- **Email is insecure by design**
  Internet email was not designed as a secure channel of communication, but rather an easy and open one. Multiple security schemes have been added to the original design over time, but it largely remains an anyone-to-anyone communication channel. Cybercriminals love that reality.

- **Email provides access to almost everything else inside an organization**
  Compromising email credentials provides a threat actor with access to nearly everything else the victim has access to. For example, email credentials for any victim using Microsoft 365 or Google Workspace provides a threat actor with access to documents, meeting chats, and more. And with email credentials functioning as the dominant identity for a given individual, once compromised, any connected systems are open to the threat actor as well.

- **Email offers direct contact with employees deep inside an organization**
  A threat actor can send an offer, request, or document directly to any employee and their devices with a known valid or ostensibly legitimate email address for the employee.[1] While email is a corporate communications system, employees also feel a sense of professional and personal ownership of their email inbox—it's a personalized space for current work, tasks, and essential duties. What comes into their inbox is for them to handle.

- **Email is a critical communications channel that cannot be turned off**
  Email is the most frequently used tool for sending and receiving external communications, and often for internal communications too, despite the growth in complementary communication and collaboration systems (e.g., Teams, Slack, Zoom, SharePoint, etc.). Many business processes grind to a halt when email goes down.

- **Email offers the ultimate tool for malicious delegation**
  If a threat actor can trick an employee into performing an operation on their behalf, they have successfully weaponized the employee's access privileges for malicious purposes. For example, if a document with embedded malicious code is opened and authorized by the employee, the threat actor can gain access to their device. Alternatively, if a bank account change process is kicked off in response to a fraudulent email, the threat actor can gleefully anticipate receiving payroll or invoice payments that should have been made to someone else.

Among organizations where email security is their highest priority, safeguarding employee productivity is the highest concern.

We asked each respondent to explain why they chose the priority they did (see Figure 1). The common themes for each grouping are:

- **It is our highest priority (25% of respondents)**
  To "safeguard productivity" for employees was the most common answer, e.g., so employees could work without being subjected to security threats and focus on delivering value to customers and partners, and to improve workflow across the organization. Tied for second place were the "increasing threats" seen via email and the need to "protect proprietary information." Other respondents said they wanted to "stop social engineering threats," "stop phishing attacks," and "avoid identity theft" due to the risks and threats delivered to employees within email messages. Good email security is also seen as "fundamental to overall cybersecurity posture."

- **It is one of our top 3 priorities (52% of respondents)**
  "Protecting proprietary information" and "protecting against cyberattacks" tied for first place in this group, followed by email being a "vulnerable channel" and to "stop data breaches" (which is an aspect of protecting proprietary information). Email security was also viewed as being "fundamental to the organization's cybersecurity strategy."

- **It is one of our top 5 priorities (21% of respondents)**
  The most common answer was that email is a "vulnerable channel," which means it must be "protected from cyberattacks" (tied for second) and to "stop data breaches, e.g., stop the leakage of private information" (4th place). The other response tied for second was that "more pressing issues" existed.

The respondents who did not rate email security in the top 5 security and risk initiatives for their organizations also had "more pressing issues" to address.

CYBERCRIMINALS ARE LEVERAGING AI FOR EMAIL THREATS

Cybercriminals have been using AI to craft email threats for several years, although this has been supercharged recently by ChatGPT and malicious derivatives. Respondents show an early awareness of the use of AI in email attacks against their organization and exhibit a growing sense of alarm at what is yet to come, e.g., the use of generative AI tools designed specifically for malicious use. This increasing sense of alarm is evident in Figure 2, where the threat level grows in a stepwise fashion. The five statements divide into two perspectives:

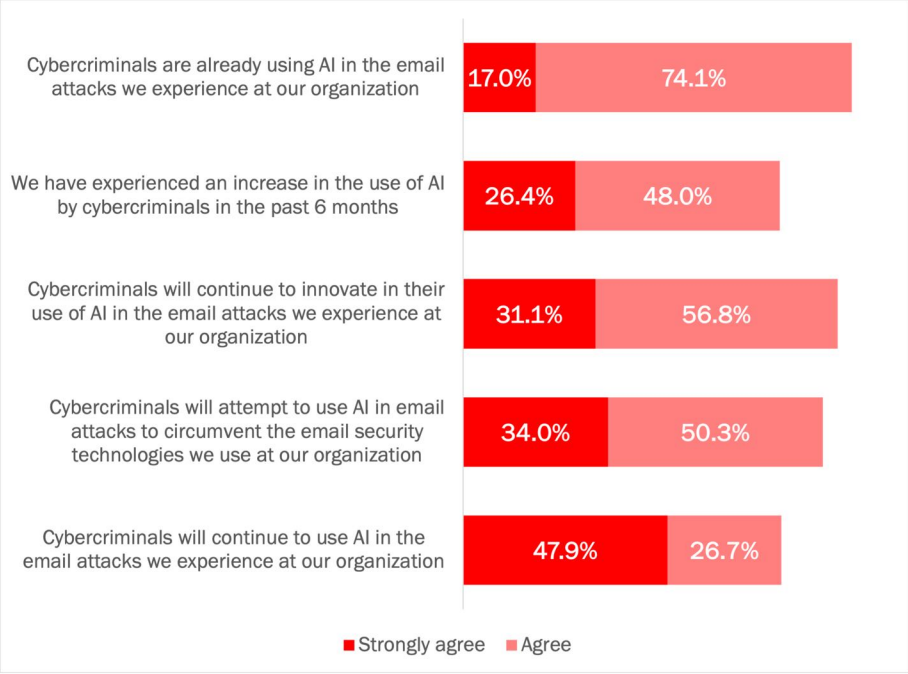
- **The look back: what we know and have experienced to date**
  Respondents indicate that they know cybercriminals are using AI in email attacks against their organization (17% strongly agree). In addition, they have experienced an increase in the use of AI by cybercriminals during the past 6 months (26.4% strongly agree).

- **The look forward: more is yet to come, and we're in the crosshairs**
  Respondents expect continued innovation by cybercriminals in the use of AI in the email attacks directed at their organization (31.1% strongly agree), combined with the use of offensive AI strategies that attempt to circumvent current email security technologies (34% strongly agree). Overall, respondents anticipate continued use of AI against their organizations (47.9% strongly agree). In other words, it is not going away, and it is going to get worse.

The second dynamic evident in Figure 2 is the transition from "agree" to "strongly agree" across the statements. The average variation for the combined values ("agree" and "strongly agree") across the five statements is only +/- 10.5%, yet the intensity of concern shifts to the higher level for the future-looking statements.

Respondents show an early awareness of the use of AI in email attacks against their organization, combined with a growing sense of alarm at what is yet to come.

Figure 2
Experiences and Expectations on Cybercriminal Use of AI in Email Attacks
Percentage of respondents indicating "agree" or "strongly agree"



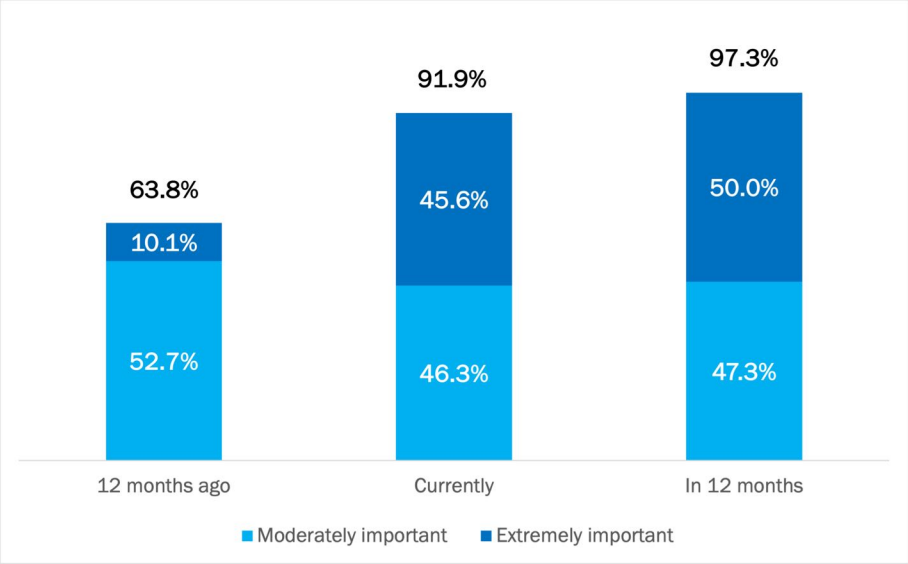
Source: Osterman Research (2023)

AI-ENABLED PROTECTIONS BECOMING MORE IMPORTANT

New and emerging threat methods are expected to grow in email attacks against organizations. Cybercriminals are already leveraging AI in email attacks against the organizations in this research—and are expected to continue doing so. In response, the importance of AI to email defenses is growing rapidly and significantly.

The percentage of respondents ranking AI as "extremely important" to their email defenses has increased more than fourfold over the past 12 months. In the next 12 months, half of respondents expect AI to be "extremely important" to their email defenses, and virtually everyone else says it will be "moderately important." See Figure 3.

Figure 3
Overall Assessment of the Importance of AI to Email Defenses
Percentage of respondents indicating "moderately" or "extremely important"



Source: Osterman Research (2023)

AI's growing importance over the past 12 months aligns with the increasing awareness of the practical application of AI. The power of large language models and generative AI services, led by ChatGPT and Google Bard, crashed into the news cycle during the past year. Although this application of AI is not specifically about email security, it galvanized collective acuity of the game-changing possibilities of AI tools. Weaponization of ChatGPT and its ilk for crafting dynamic and tailored cyberattacks drove specific awareness of the threat of AI among security teams.

In 12 months, virtually all organizations expect AI to be moderately or extremely important to their email defenses.

EMAIL SECURITY VENDORS ARE ADDING AI TO DEFENSIVE SOLUTIONS

The highest-rated reason why organizations have embraced AI-enabled protections for email security is that their incumbent email security vendor(s) updated their technology. As new attack methods are leveraged by cybercriminals, traditional approaches to detecting threats have proven less effective over time. By implication, email security vendors have taken steps to better protect their customers. Respondents may not have necessarily requested an AI-enabled solution but received it as their chosen vendor updated the product.

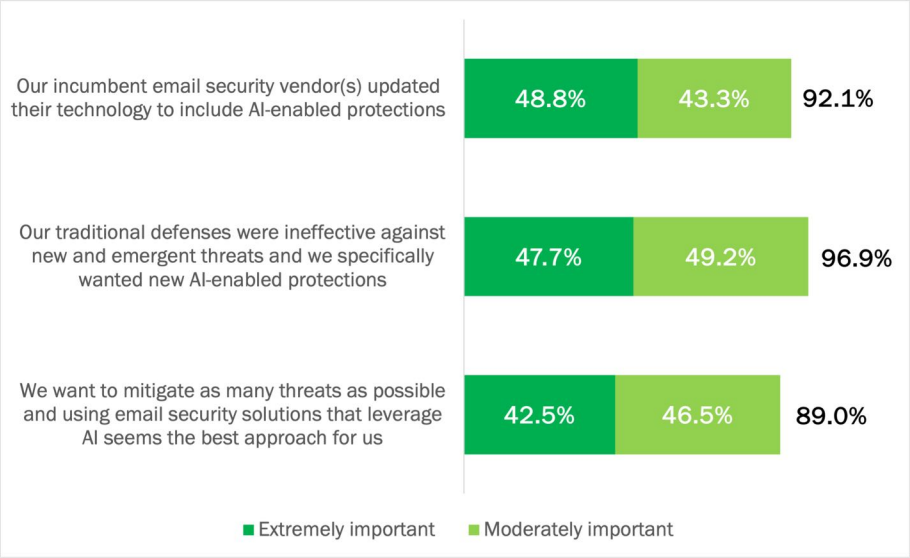
Organizations using Microsoft 365 or Google Workspace for email are protected by baseline email security protections, with emerging AI-enabled protections available in the higher-priced plans. However, in this research, 90.5% of organizations are using one or more additional email security solutions beyond the protections included in Microsoft or Google's email offerings. This is most commonly done to catch email threats that Microsoft and Google miss.

The second highest-rated reason is the ineffectiveness of traditional defenses alone. Virtually all organizations said this reason was "moderately" or "extremely important" in their decision-making process. New threat methods enhanced by AI were getting through to employees across the organization, resulting in lost funds (through BEC scams), lost account credentials (through credential phishing attacks), data breaches, and more—and so the organization acted.

See Figure 4.

Organizations are getting AI-enabled email security protections because their incumbent vendor has added AI to their solution.

Figure 4
Reasons for Implementing AI-Enabled Email Security Technologies
Percentage of respondents indicating "moderately" or "extremely important"



Source: Osterman Research (2023)

Assessing Current Usage of AI for Email Security

Most organizations are already using AI-enabled email security technologies to defend against email-borne threats. In this section, we look at the state of use and what organizations seek from using AI.

MOST ORGANIZATIONS ARE ALREADY USING AI FOR EMAIL SECURITY

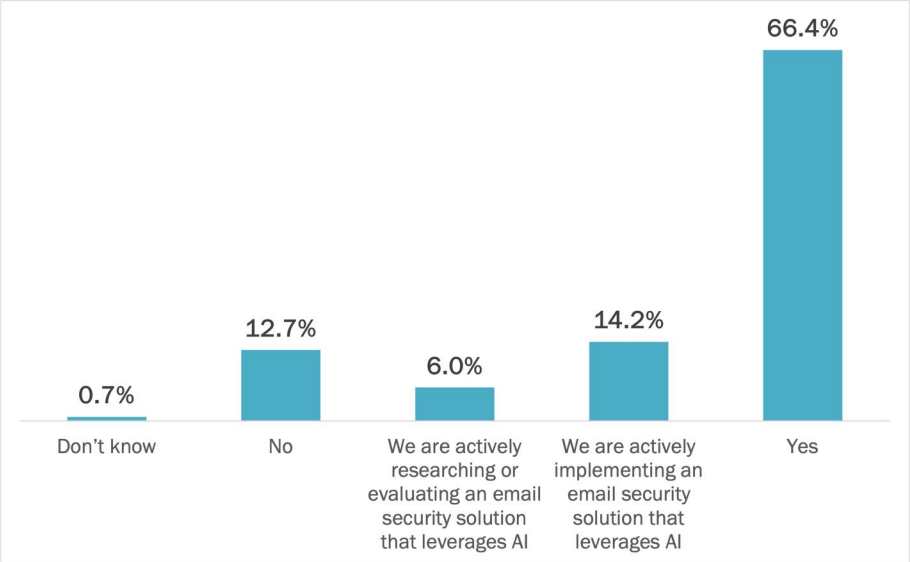
Over the past 24 months, four-fifths of organizations have either implemented or are currently actively implementing an AI-enabled email security solution over and above the protections offered in Microsoft 365 or Google Workspace. As we have previously seen, acquiring AI for email security is driven by two approaches: incumbent email security vendors adding AI protections to their solutions (extremely important for 48.8% of respondents) and by organizations specifically acquiring new AI-enabled solutions (extremely important for 47.7%).

The remaining one-fifth have not implemented such a solution during the previous 24 months (12.7%) or are actively researching or evaluating options (6.0%).

See Figure 5.

Four-fifths of organizations have implemented an AI-enabled email security solution over and above the protections offered in Microsoft 365 or Google Workspace.

Figure 5
Implementation of AI-Enabled Email Security Solutions Over the Past 24 Months
Percentage of respondents



Source: Osterman Research (2023)

AI USED TO PROTECT AGAINST COMPLEX INTERNAL EMAIL THREATS

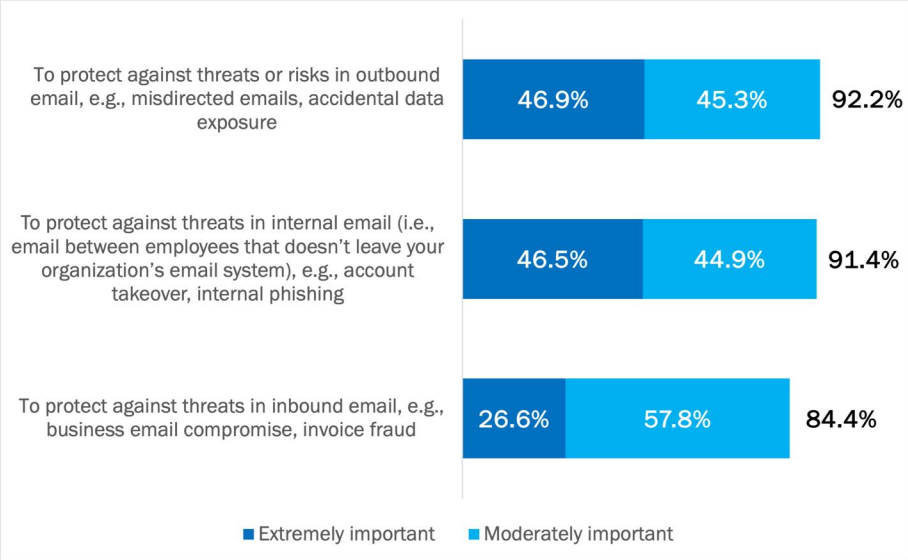
AI-enabled email security protections are viewed as most important in protecting against two types of complex internal email threats (see Figure 6):

- **Outbound emails sent by employees that contain threats or risks**
  Misdirected emails and accidental data exposure occur when an employee unwittingly sends a message and/or attachment to the wrong person, often due to error in using type-ahead addressing. This type of incident is virtually impossible to avoid in all cases, given the message is misaddressed in a moment of error or distraction. AI, on the other hand, can detect that something is amiss due to observing a deviation in the baseline behavioral profile for the individual. For example, if the employee has never sent a given type of document to another person, the first instance could be incorrect—and therefore a warning alert should be shown to the employee to confirm intent.
- **Emails sent between employee accounts that contain threats**
  When a threat actor successfully compromises the credentials to an employee's email account, they gain surreptitious control of a high-reputation account for sending email-borne threats to other employees (i.e., internal phishing) and external parties (i.e., vendor email compromise). Mitigating these threats is the second highest-rated reason for embracing AI.

Protecting against threats in inbound email was rated in third place, behind the two types of threats above. **This is a strange prioritization because organizations cannot ignore the threat conveyed by inbound email, as this is where many multi-stage attacks begin**—and where employees are most likely to succumb.[2] Early detection of inbound threats cancels the whole chain of subsequent malicious activity that would happen otherwise, including threats in internal email.

Organizations cannot ignore the threat conveyed by inbound email, as this is where many multi-stage attacks begin.

Figure 6
Importance of AI-Enabled Email Security Protections Against Threat Types
Percentage of respondents indicating "moderately" or "extremely important"

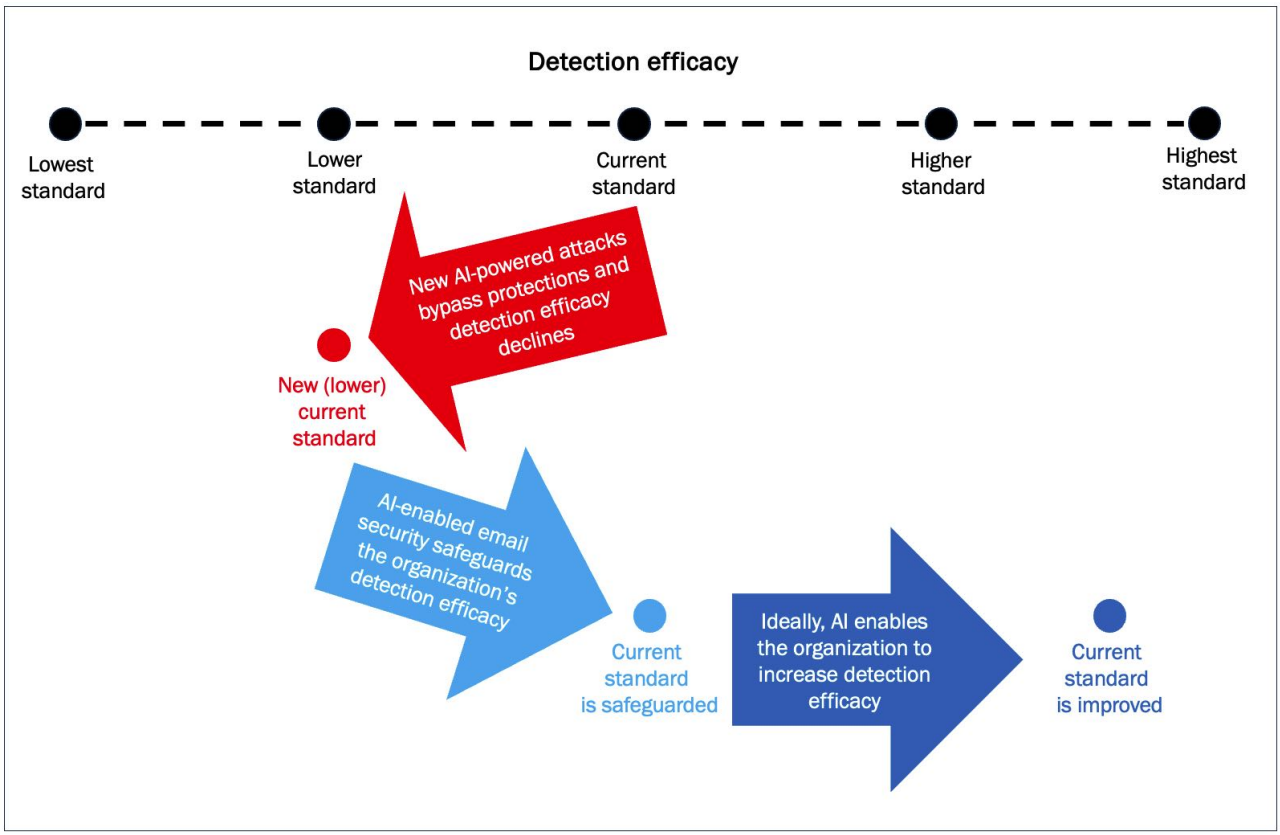


Source: Osterman Research (2023)

AI CAPABILITIES ARE SAFEGUARDING AND IMPROVING DETECTION EFFICACY

Every organization has achieved a defined level of detection efficacy for threats in email before leveraging AI-enabled email security solutions. Due to the change in the threat environment with cybercriminals embracing AI to increase the efficacy of their attacks, the net impact of this change on organizations is a regression in detection efficacy. In other words, in the absence of leveraging AI in email security and where threats are better able to evade an organization's protections, detection efficacy declines. See Figure 7.

Figure 7
Dynamics of Detection Efficacy With AI-Powered Attacks and AI-Enabled Email Security



Source: Osterman Research (2023)

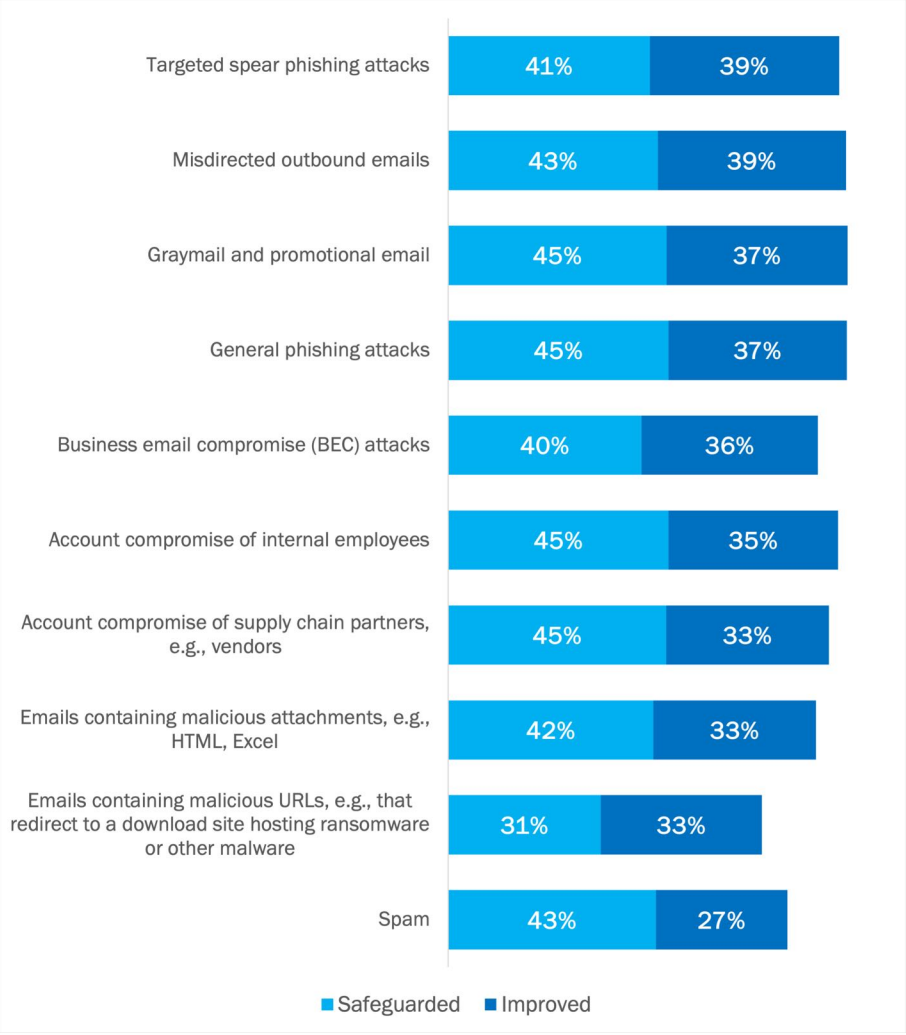
Embracing AI-enabled email security should have two effects for organizations (see Figure 7):

- **Safeguarding detection efficacy**
  AI-enabled email security should safeguard an organization's earlier standard of detection efficacy as the threat environment changes. As threat actors embrace new attack methods to bypass existing protections, these are detected and mitigated by new AI-enabled protection methods.
- **Improving detection efficacy**
  Ideally, organizations should expect to see an increase in detection efficacy enabled by AI over and above where they were previously.

We tested this hypothesis by asking respondents to rate the before-AI and after-AI efficacy of their email security solutions at detecting ten types of email threats. The before-AI rating was used as the baseline detection standard for each organization. We modeled the net effect of adding AI-enabled protections to this baseline. On average, 42% of organizations indicated that AI-enabled protections supported them to safeguard their previous detection standard. In addition, 35% saw an improvement beyond their earlier baseline by adding AI-enabled protections.

See Figure 8.

Figure 8
Safeguarding and Improving Efficacy at Detecting Email Security Threats with AI
Percentage of respondents



Source: Osterman Research (2023)

Respondents are already seeing increased efficacy in detecting most types of email security threats due to the use of AI-enabled email security technologies.

SOME ORGANIZATIONS DON'T REALIZE THEY ARE ALREADY PROTECTED BY AI

As we saw in Figure 5, 13.4% of respondents in this research believe they are not currently using AI for email security. When we dig into the data to understand the profile of the 20 organizations in this cohort, however, almost all are using AI in their email security defenses already—but they don't know it yet:

- **Two organizations rely exclusively on their email provider for email security**
  Two of the 20 organizations in this cohort are currently not using any third-party email security solutions. Both organizations use Microsoft 365 for email, and since Microsoft has added AI to its email security services in Microsoft 365, both organizations already have basic AI-enabled protections available to them. The specific AI-enabled protections available to each organization depend on the Microsoft 365 licenses in use. However, few organizations find native protections sufficient.

- **18 organizations are already using third-party email security solutions**
  The remainder of the organizations in this cohort are already using one or more third-party email security solutions in addition to any baseline protections offered by their email provider. Virtually all say that email security is not the top security or risk initiative at their organization. Since most of the email security vendors that we asked about in the survey have added AI protections to their solutions, the most reasonable explanation for this mismatch is lack of awareness in how current email security solutions have already been fortified with AI.

- **All but two will intentionally embrace AI-enabled security protections within 24 months—and those two will get it anyway**
  Within 24 months, all but two of the organizations in this cohort say they will intentionally embrace AI-enabled security protections. Since the majority already have some form of AI protection without being aware of it, this will be a very simple process. For others who want specific types of protections to cover gaps in detection efficacy, the evaluation and assessment process will be somewhat longer. In 24 months, it will be almost impossible to buy email security solutions that do not make use of AI.

Some organizations appear to have missed the memo that AI protections have been added to their email security solutions.

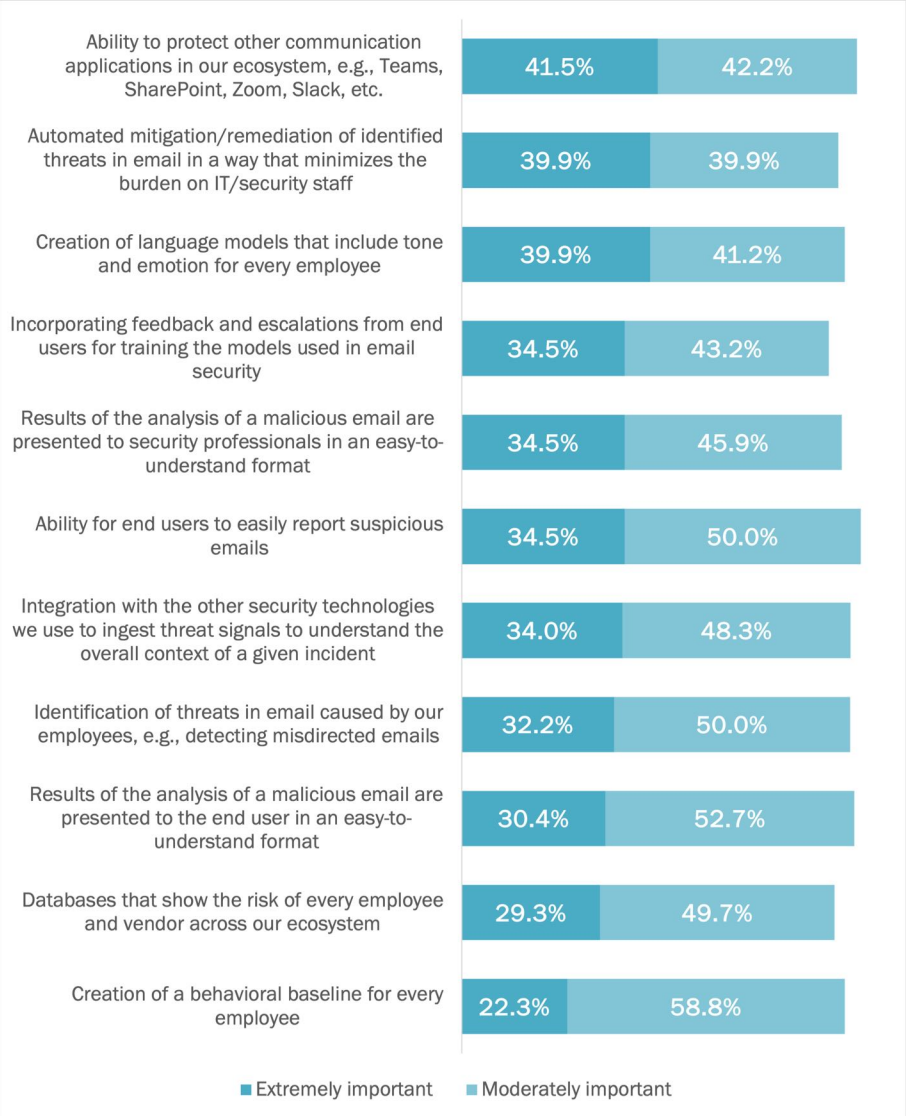
Shopping List of AI in Email Security

When making a buying decision for email security technologies that leverage AI, many features are offered by vendors. In this section, we look at how buyers think about these features.

IMPORTANCE OF FEATURES WHEN SHOPPING FOR AI-ENABLED EMAIL SECURITY TECHNOLOGIES

Organizations seeking email security technologies that leverage AI show a high degree of alignment with the features available from email security vendors. More than four out of five respondents want everything AI has to offer for email security—as well as for adjacent communication and collaboration platforms. See Figure 9.

Figure 9
Buying Decision Ranking of Features for AI-Enabled Email Security
Percentage of respondents indicating "moderately" or "extremely important"



Source: Osterman Research (2023)

Four out of five respondents want everything AI has to offer for email security.

Highly rated features of note from Figure 9 include:

- **Protecting more than just email**
  The top buying factor based on the "extremely important" rating is the ability for a security solution to protect other communication and collaboration applications used across the organization, such as Microsoft Teams, SharePoint, Zoom, and Slack. From the buyer's perspective, AI has a role in protecting against threats in more than just email. While solving changing threat dynamics in email is essential, it is not enough. Employees are working in applications beyond email that are subjected to threats, and protecting employees wherever they work is the emphasis. Buyers want an ecosystem-aligned offering that encompasses all communication applications in use.

- **Simplifying security processes for IT and security staff**
  The second and fifth highest-rated buying factors are about empowering IT and security staff to carry out their duties with greater simplicity. Any new AI-enabled solution should work on their behalf, not dump a load of additional noise and complexity into their already overstretched work queues. The second highest-rated buying factor (39.9% extremely important) is automated mitigation and remediation to minimize the burden on IT and security staff. In other words, the solution should make the right decision on mitigation and remediation as frequently as possible, or integrate seamlessly with the suite of security tools already in place in the environment. The buying factor in fifth place is that the results of the analysis of a malicious email are presented to security professionals in an easy-to-understand format (34.5% extremely important). In cases where an automated approach is not possible, an informed decision context is essential.

- **Train ML models on the organization's context via employee feedback**
  Buyers want the ability to benefit from employee actions in providing feedback and escalation of suspicious messages. The fourth highest-rated decision factor is that these actions are incorporated into the ML training models for email security, thereby capturing data on the organizational context that would otherwise be missed.

- **Continue to enlist employees in the fight against email threats**
  Two of the top three buying factors when combining the "extremely important" and "moderately important" scores focus on including the employee as a critical participant in the fight against email threats. The highest-rated buying factor is the ability for end users to easily report suspicious emails (1st place, 84.5%). The third highest is that the results of the analysis of a malicious email are presented to the end user in an easy-to-understand format (3rd place, 83.1%). Both factors play together, although the lower-rated of the two is the critical input that enables the achievement of the higher-rated one.

- **Underlying technical features are less important to the buying decision, but critical for the highly rated outcomes**
  The underlying methodology and models that enable AI to detect threats are rated lower than capabilities for security teams and users, as would be expected. For example, the creation of a behavioral baseline for every employee is in last place as a buying factor (22.3% extremely important), and a database that shows the risk of every employee and vendor in second-to-last place (29.3% extremely important). However, detection of malicious emails using AI relies on the presence and efficacy of these capabilities—the whole approach collapses without them.

Any new AI-enabled solution should empower IT and security staff via automated response capabilities, not dump a load of additional noise and complexity in their already overstretched work queues.

Best Practices in Using AI for Email Security

While email security is a mature market with a long history, new and emerging threat methods along with AI-enabled protections are shaking things up. This new curve means it is still early days for AI-enabled protections, and what's currently available is not fully baked. Better than what existed before? Definitely. Perfect? Not yet. The organizations in this research are already using AI to strengthen email security. Others who are lagging in adoption and usage should get moving.

Best practices for using AI for email security are:

- **If you can't see new threat methods in email, fix visibility**
  It is a problem when organizations can't see the email-borne threats and emerging threat methods directed their way. When less than a complete picture of threats is available to security decision-makers, they will be caught unaware as new attack methods get through to employees. Fix the question of visibility, and act accordingly. One approach is to set up an evaluation of a solution from an email security vendor offering protections against new and emerging threat methods. This assesses the current efficacy of your email security and the scale and import of unaddressed threats. All organizations should do this assessment once, and most should find a way to regularly assess which email threats are still getting through.
- **Technology plus process plus people is still the order of the day**
  Employees continue to have an essential role in email security. The presence of new AI-enabled protections doesn't set up a win-lose dynamic between the best security technology on offer and people who are informed, trained, and engaged in ensuring email messages are not malicious. It's both/and, not either/or. The organization wins when technology, people, and processes work in harmony to detect, mitigate, respond to, and address threats in email. If an employee sees something out of place that the AI has not detected, reporting the message mitigates the current threat and adds a training data point for the detection model.
- **Take signals for detecting attacks in email from more than just email**
  Attacks that start in email don't always finish there. For example, a spear phishing email written using generative AI requires the victim to do something that appears normal, such as opening an attachment that contains malicious code, starting a process to change a bank account number, or replying with sensitive information. Each of these subsequent processes generate associated signals that can be analyzed for behavioral anomalies. Organizations need the ability to capture and aggregate threat signals from more than just email, creating a holistic picture for end-to-end threat detection across their infrastructure.
- **AI does not eliminate the need for cybersecurity expertise**
  There is a synergistic relationship between AI and cybersecurity professionals. AI is orders of magnitude better, cheaper, and faster at detecting anomalies and creating behavioral profiles than cybersecurity professionals. Cybersecurity professionals, on the other hand, are often better at understanding the intricate human patterns that characterize malicious activities. Leveraging both machine efficiency and human insight recognizes that while AI can process vast amounts of data and detect patterns beyond human capabilities, the human element is essential for interpreting those patterns and making nuanced judgments to help finetune the AI models. Combining human insight and AI-driven analysis in incident response processes or managed services ensures a more robust defense and a faster response to email-borne threats.

The organization wins when technology, people, and processes work in harmony to detect, mitigate, respond to, and address threats in email.

- **More doesn't necessarily mean safer, but one may not be enough**
  Cloud-based email services from major providers already include AI-enabled email security protections, but many organizations find these baseline protections insufficient because threats using new and emerging methods continue to reach employees. To increase overall detection efficacy by extending baseline capabilities, most organizations add complementary solutions from specialized email security vendors. Using multiple vendors allows a layered approach to email security that offers synergistic benefits—assuming the right orchestration and vendor mix—allowing security teams to get a better picture of the threats facing their organization. However, it is possible to have too many vendors, where functionality overlaps to the point of confusion and efficacy isn't enhanced. In the final analysis, counting the number of vendors an organization is using for email security is virtually meaningless. The right answer for a given organization can be a low number or high one, but the proper analysis question is whether the email-borne attacks and threat methods the organization is subjected to are being neutralized as quickly and effectively as possible.
- **Protect more than just email**
  Employees are using a diverse array of communication and collaboration tools to complete their work. Any security solution that uses AI to protect email exclusively is not enough. Look for wider solutions that take an ecosystem view to protect the other communication and collaboration tools used by employees, e.g., SharePoint, OneDrive, Slack, Zoom, and Teams.

Conclusion

Cybercriminals will always seek new ways into organizations to compromise processes, steal information, and capture financial resources they have no right to. Email will continue to be one of the most common attack pathways, and as organizations have strengthened email security protections in recent years, cybercriminals have upleveled their attack methods to circumvent what has been put in place. In this new era of increasingly sophisticated AI-generated email threats, manually driven analysis and mitigation will continue to hinder under-resourced security teams while increasing the threat of email attacks. AI capabilities in email security solutions have become an essential mechanism for organizations to detect, disrupt, and stop new and emerging attack methods, and offer significant protection promise for organizations due to their ethos of continual learning.

Every organization must reassess its email security strategy to ensure the right mix of protections is available to counter new and emerging attack methods. In line with the findings in this research, almost all organizations will need to deploy additional email security solutions that leverage AI to increase security efficacy beyond basic AI-enabled protections offered by cloud email providers.

AI capabilities in email security solutions have become an essential mechanism for organizations to detect, disrupt, and stop new and emerging attack methods.

Sponsored by Abnormal Security

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages in milliseconds—all while providing visibility into configuration drifts across your environment. You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom.

More information is available at abnormalsecurity.com.

abnormalsecurity.com

@AbnormalSec

Methodology

This white paper is based on findings from a survey conducted by Osterman Research. One hundred forty-eight (148) respondents who are familiar with how their organization is leveraging or planning to leverage AI to strengthen email security against advanced inbound, outbound, and internal email threats were surveyed in July 2023. To qualify, respondents had to work at organizations with at least 1,000 employees. All surveys were conducted in the United States. The survey was cross-industry, and no industries were excluded or restricted.

NUMBER OF EMPLOYEES

1,000 to 2,499 employees	22.3%
2,500 to 4,999 employees	62.8%
More than 5,000 employees	14.9%

JOB ROLE IN ORGANIZATION

IT manager or IT team lead	51.4%
IT security manager or IT security team lead	17.6%
Security Operations Center (SOC) manager or SOC team lead	10.8%
Security manager	7.4%
CISO or CIO	6.8%
Email security manager or email security team lead	3.4%
SOC analyst	2.0%
Email security administrator	0.7%

INDUSTRY

Computer hardware or computer software	11.5%
Healthcare	11.5%
Hospitality, food or leisure travel	10.1%
Education	9.5%
Data infrastructure or telecom	7.4%
Energy or utilities	7.4%
Industrials (manufacturing, construction, etc.)	6.8%
Retail or ecommerce	6.1%
Transport or logistics	5.4%
Professional services (law, consulting, etc.)	4.7%
Public service or social service	4.7%
Financial services	4.1%
Life sciences or pharmaceuticals	4.1%
Government	2.0%
Media or creative industries	2.0%
Information technology	2.0%
Agriculture, forestry or mining	0.7%

[1] By default, organizations follow a standardized naming scheme for email addresses, for example, firstname.lastname@domain.com or firstinitial.lastname@domain.com. Once a threat actor can see the pattern, the ostensibly legitimate email address for any employee can be calculated based on their name.

[2] Verizon, 2023 Data Breach Investigations Report, June 2023, at https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf