AimPoint Group
high-impact marketing

2022 EMAIL SECURITY TRENDS REPORT

MANAGING RISKS AMIDST THE CHANGING THREAT LANDSCAPE

As enterprises shift their email environments to the cloud, attackers are inventing new and more sophisticated ways to circumvent legacy defenses. What challenges are today's email security tools facing? And what capabilities do organizations need? We surveyed 300 security leaders to discover what matters most to them when it comes to email security in the current threat landscape.

SPONSORED BY Abnormal

Contents

Today's Workforce Needs Advanced Email Protection

In the past two years, the prevalence of email-borne cyber threats—which was already high—soared to unprecedented levels. According to data from the FBI, both business email compromise (BEC) and ransomware attack volumes swelled to record highs, as did the number of reported phishing attacks.[1]

BEC is a particularly expensive scourge. The FBI reported that losses attributable to business email compromise attacks increased by 65% from July 2019 to December 2021. Around the world, victims have incurred a total of more than $43 billion in exposed losses since 2016.[2]

Gartner estimates that 70% of organizations had already adopted a cloud-based email solution by late 2021.[3] As enterprises shift to the cloud, many are experiencing a mismatch between their legacy security architecture and the needs of their cloud email environment. Secure email gateways, in particular, were engineered for an on-premises world rather than today's cloud email ecosystem.

Meanwhile, major cloud providers including Microsoft and Google have made considerable investments in improving the native capabilities of their offerings. Gartner predicts at least 40% of enterprises will use built-in capabilities from a cloud email provider in place of a SEG by 2023.[4] That said, advanced features and controls are typically only available as an add-on or part of a higher-priced licensure tier from some vendors—and not at all from others. Further, these native security solutions tend to operate by blocking known threats, which means organizations that rely on these capabilities alone may remain vulnerable to never-before-detected threats or sophisticated social engineering and account compromise attacks.

Even as enterprises adopt more of cloud providers' built-in email security capabilities, large numbers of email-borne attacks are still circumventing enterprise defenses. This reality makes it abundantly clear that it's now essential to implement email security solutions that are more effective and efficient than those of the past. It also requires security teams to shift their mindset, away from a rules-and-policies based approach to preventing attacks, and toward a reliance on human and behavioral analysis. Increasingly, this will mean turning to email security solutions that were designed for a cloud-first world.

Integrated cloud email security (ICES) is an emerging market category that was first described by Gartner in 2021.[5] ICES products are cloud-native solutions that analyze email content via API connectivity so that there's no need to change the MX records. These platforms leverage technologies like natural language processing (NLP) and behavioral artificial intelligence (AI) to detect and block the malicious emails that legacy solutions miss. To combat tomorrow's increasingly sophisticated cyber threats, enterprises will need this sort of innovation–either in addition to, or in place of, their current tools.

Top 5 Stats from This Survey

93%
of organizations have already adopted a cloud email solution or plan to do so in the future.

92%
of respondents experienced at least one email-related security incident within the past year.

78%
of stakeholders believe that secure email gateways (SEGs) are largely incapable of protecting modern cloud email environments.

79%
of respondents think the native security capabilities of cloud email solutions offer insufficient protection on their own and that they need an advanced solution to detect advanced threats.

90%
of survey participants agree that a combination of a cloud email provider's native security capabilities and an integrated cloud email security (ICES) platform can replace the full functionality of a SEG.

1. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), Internet Crime Report 2021.
2. Federal Bureau of Investigation, Public Service Announcement, "Business Email Compromise: The $43 Billion Scam," May 2022.
3. Gartner, Market Guide for Email Security, October 2021.
4. Ibid.
5. Ibid.

SECURITY OPERATIONS EFFICIENCY AND MODERN EMAIL SECURITY

In enterprise security operations, the persistent talent shortage is a perennial challenge. With an estimated 2.72 million unfilled cybersecurity positions worldwide, security leaders continue to feel the impact of the scarcity of skilled professionals.[6] According to the (ISC)² Cybersecurity Workforce Study, 30% of security leaders say there's not enough time to properly assess and manage risks, and 27% believe they're not able to keep tabs on all the active threats against their employees and network.[7]

Naturally, the skills shortage impacts email security as well. When management capabilities are fragmented across multiple dashboards and there's a need for extensive tuning and technically complex maintenance, the challenges often compound themselves. Today's email security teams have a pressing need for solutions that are effective against modern threats as well as simple to control and administer.

Automation can help here. In particular, it can save time by applying machine learning (ML) to processes like investigating and remediating the contents of the abuse mailbox or by making it so that there are fewer manual policies and detection rules to write or update. Of course, these capabilities will also benefit end users, who currently waste time and experience frustration when their organization's inbox management solution doesn't work as well as it should.

STATE OF EMAIL SECURITY TODAY

We conducted this survey in order to understand the challenges and opportunities that today's enterprise email security teams face. We wanted to know whether security leaders and practitioners understand the severity of the threats they currently confront, as well as investigate what they're doing to stop them. We also wanted to see how effective (or ineffective) current email security solutions are, and glean additional insight into how leaders are thinking about evolving their email security strategy for the future.

In a world where the time and expertise of security professionals will remain in short supply, where the migration of email to the cloud will continue or accelerate, and where ransomware attacks, business email compromise scams, and other advanced email-borne threats will persist, it's essential to adopt a multi-layered approach—one that's suited to modern IT ecosystems and architectures. To get ahead of increasingly sophisticated attacks, it will also be necessary to harness technologies like natural language processing and artificial intelligence to increase efficiency, all while centralizing visibility and control to stay ahead of evolving attacks.

For many organizations, this will mean replacing the legacy SEG with a combination of modern cloud solutions. Adding the capabilities of an integrated cloud email security (ICES) solution to cloud vendor-supplied native features may be the optimal approach. This can improve detection accuracy and ease the administrative burden while simplifying processes within attack triage and response to keep the organization safe.

THE NEED FOR ICES IS URGENT AND GROWING

With the number of impersonation-based attacks like BEC and attacks from compromised accounts still increasing, email security strategies must advance beyond the reactive blocking of known threats. Instead, security leaders should look to innovative emerging solutions that use AI to analyze communication patterns in order to detect conversational anomalies (like an unsolicited request for a wire transfer) within email content. Advanced solutions might also leverage computer vision to inspect suspicious URLs or natural language processing to discover messages written with an unusual tone of urgency. For example, a request to pay a past-due invoice immediately, despite the fact that the invoice contains new and different bank details.

Because these hard-to-detect threats continue to proliferate, security awareness training for employees remains a valuable investment. Some advanced email security products include context-aware banners that help users remember the finer points of their anti-phishing training. It's also vital to implement standard operating procedures for handling financial transactions since these processes are often the target of impersonation attacks. Employees should be discouraged from acting on impulse—or relying on ad-hoc processes—when responding to an email.

Furthermore, integrations are key for simplifying management while enhancing efficacy and visibility. An ICES solution that relies on direct API access to the cloud email provider to analyze email content will be much easier to implement than one that requires the mail exchange (MX) record be changed or email servers be reconfigured. APIs can also serve to integrate the email solution into a broader extended detection and response (XDR) ecosystem or with security information and event management (SIEM) and security orchestration, analytics, and reporting (SOAR) solutions. These integrations enable defenders to perform

6. (ISC)², (ISC)² Cybersecurity Workforce Study, 2021.
7. Ibid.

comprehensive threat analysis and identify the role email plays within attack sequences, as well as create custom email notification or ticket-generation workflows.

WHAT THE DATA SHOWS

As enterprises move their email systems into the cloud, implementing automation to increase efficiencies and support the modern workforce is increasingly important. But how many of today's security leaders and practitioners recognize this fact? This survey explores how email security strategies are being adapted for modern computing environments, and what's still needed to mitigate risk.

Key Findings

- **Modern email systems are in the cloud or headed there.**

  Survey results show that the vast majority of respondents (93%) either have already adopted a cloud email solution such as Microsoft 365 or Google Workspace for their enterprise or have plans to do so in the near future. This is slightly less true for the largest organizations (those with 10,000 or more employees), which may be hobbled by technical debt, outdated policies, or the complexity that's inherent to having thousands of employees. However, even among this group, 91.5% of survey participants said they either already have a cloud-only email solution in production or are planning to implement one.

- **SEGs are losing ground to ICES solutions and the native email security capabilities offered by cloud email providers, but they're still prevalent in the marketplace.**

  Nearly 63% of respondents report that they're now using native features and functions from their cloud email provider. Meanwhile, ICES adoption is on the rise, with a full 50% of survey participants having already implemented an advanced cloud email security solution like Abnormal Security. However, almost 60% of respondents still have a traditional SEG in place. A growing number of organizations are relying on a combination of these solutions and, while it's possible for this combined approach to work well, it also increases complexity and administrative overhead. Much depends on which specific solutions and functionalities are in use and how well they work together.

- **The email security solutions currently in use are, by and large, inadequate to stave off the torrent of advanced threats.**

  The vast majority of survey participants (92%) had experienced at least one security incident in which email was the primary attack vector within the past year. And a remarkable 72% of respondents had experienced more than five email-related security incidents. The lesson is clear: the email security solutions (or combinations of solutions) in place in today's enterprise security environment aren't stopping all of the threats.

- **Phishing attacks continue to consume far too much time and too many resources.**

  Email security teams currently spend as much as thirty minutes on a single user-reported phishing email. When dozens of these are reported each day across the organization, the situation is unsustainable. There's a clear need for automated solutions that can accelerate investigation and remediation, so that tasks that would take minutes or hours if performed manually can be completed in seconds.

- **Awareness of the need for change is on the rise. Respondents understand that SEGs are incapable of protecting modern cloud environments.**

  A robust 78% of respondents believe that SEGs are largely unable to protect cloud email environments or prevent advanced email threats like BEC from causing harm. Further, 79% of respondents do not believe that cloud email solutions' native capabilities offer adequate protection. However, nearly 9 in every 10 respondents agree that a combination of cloud email's native features and an ICES platform can replace a SEG's full functionality—showcasing how security leaders are thinking about the move to modern email security.

Enterprise Email Security in a Changing IT Landscape

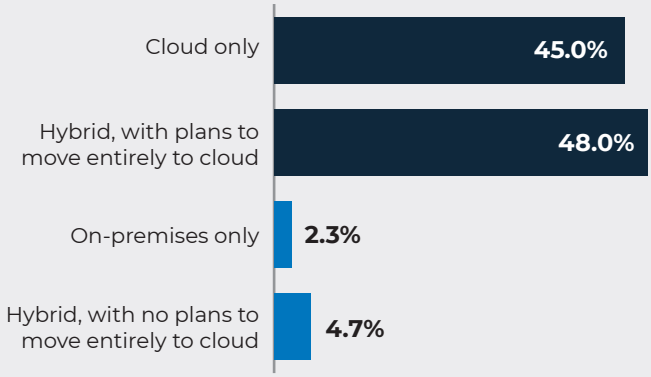
As organizations move ever greater portions of their applications and IT infrastructure to the cloud, they're increasingly adopting cloud email solutions as well. And cloud email needs cloud email security.

HOW FAR ALONG THE PATH TO THE CLOUD ARE TODAY'S ENTERPRISES?

Cloud adoption is clearly on the rise. Not only have nearly half of organizations (45%) embraced a cloud-only solution for their production email environment, but more than nine out of ten either have already moved to the cloud or have plans to do so.

FIGURE 1: THE MOVE TO THE CLOUD IS UNDERWAY

Which choice best describes your organization's production email environment?



Among the respondents to this survey, the largest enterprises tend to be laggards, with a greater percentage of these organizations not yet having made plans to move entirely to the cloud than is the case for any other group. However, even among larger organizations (those with 10,000 employees or more) 91.5% either already have a cloud-only production email environment or are planning to implement one.

The smallest organizations had the highest rates of cloud-only email adoption, with 48% having already moved their entire production email environment to the cloud. Conversely, the largest organizations had the highest rates of using on-premises and hybrid email systems, with 65.9% currently having at least one production email system that is not in the cloud. That said, the high number of respondents indicating that they plan to move entirely to the cloud shows that on-premises-only solutions are unlikely to be the only option for much longer.

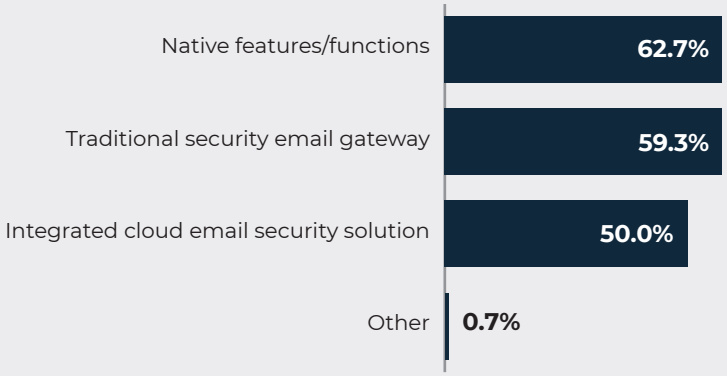
We see organizations of all sizes seeking to capitalize on the benefits that adopting a cloud email solution can bring. These include cost advantages, ease of administration, and readiness to support hybrid and remote workforces. The largest enterprises may be inhibited by technical debt, legacy policies, or the inertia that's an all-but-inevitable consequence of the complexity that comes with size. Still, even these organizations, by and large, have begun the process of cloud email migration.

HOW ARE TODAY'S ORGANIZATIONS SECURING EMAIL ACCOUNTS AND COMMUNICATIONS?

It's no surprise that different companies rely on different solutions. In general, though, traditional SEGs are losing ground to the built-in email hygiene capabilities offered by cloud providers like Microsoft and Google. More than 60% of respondents are now using native features and functions from their cloud email provide, though only 16.1% are using those functionalities without supplementing them with a SEG or ICES solution.

FIGURE 2: THE EMAIL SECURITY TOOLS AND TECHNOLOGIES THAT ENTERPRISES RELY ON

What are the primary tools/technologies your organization uses for email security? Select all that apply.



ICES adoption continues to grow as more stakeholders realize that SEG and/or cloud email solutions' built-in capabilities aren't enough to counter today's sophisticated email-borne threats. A full 50% of respondents have already implemented an ICES solution, with 38% combining ICES capabilities with native features, a secure email gateway, or both.

The traditional SEG retains the largest market share among the largest enterprises. This technology is in use by 66% of respondents in organizations with more than 10,000 employees, perhaps due to the same factors that are slowing these companies' progress to the cloud.

ICES adoption also lags slightly among survey participants in this group, with only 42.6% having implemented this technology. Still, we anticipate that ICES adoption will continue to grow in the future as stakeholders re-evaluate their need for solutions to block advanced but difficult-to-detect threats like business email compromise and supply chain compromise, as well as attacks sent from legitimate but compromised accounts.

That said, stakeholders should exercise caution about implementing multiple solutions with overlapping capabilities. While some, like certain ICES solutions, were purpose-built to work together with cloud vendor-provided functionalities, others are not. Adding a SEG to a cloud email solution's native capabilities may require security teams to disable at least some of the native features, resulting in cost duplication without the benefit of doubled defenses. Security teams will also need to ensure that functions such as URL rewriting, file inspection, content filtering, and similar are neither inadvertently performed *twice* nor accidentally omitted from the workflow. This process can contribute to administrative complexity and frustration.

Email-Borne Threats, Attacks, and Incidents Across the Spectrum

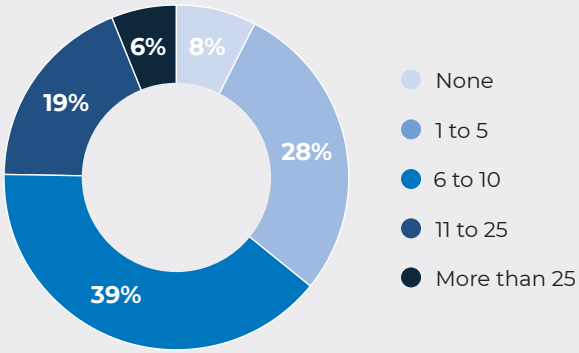
Enterprise security teams continue to be challenged by email-borne attacks, with legacy threats such as spam, graymail, and malicious attachments still posing problems—even as more sophisticated threats grow in prevalence.

ARE EMAIL-BORNE THREATS MAKING IT PAST THE EMAIL SECURITY SOLUTIONS THAT TODAY'S ORGANIZATIONS HAVE IN PLACE?

Unfortunately, the answer is a resounding "yes!" As many as 92% of respondents say their organization experienced a security incident within the past year whereby the attackers leveraged email as the primary attack vector.

FIGURE 3: ABILITY OF CURRENT EMAIL SECURITY SOLUTIONS TO BLOCK INBOUND THREATS

In the past 12 months, how many security incidents at your organization were the result of email-borne threats?



Overall, the prevalence of these types of incidents among survey participants is high. Not only had more than nine in every ten respondents experienced at least one email-related security incident within the past 12 months, but a remarkable 72% of respondents had experienced more than *five*.

This sobering result ties in with other industry experts' findings: sophisticated account takeover attacks have grown more common and more lucrative for cybercriminals over the past few years. In the Verizon Data Breach Investigations Report (DBIR), for instance, email was among the most common action vectors observed in both incidents and breaches, playing a role in more than 35% of data breaches. Making matters worse, 82% of those breaches involved a human element where threat actors used tactics like social engineering, impersonation, and fraud to deceive their targets.[8]

Ransomware attack volumes are up as well, with Verizon reporting a 13% increase in the number of ransomware-related breaches, for a total number larger than what took place in the last five years combined.[9] And according to research conducted by Deloitte, phishing emails are now the number one delivery vehicle for ransomware. In Deloitte's study, 91% of successful cyberattacks began with a cybercriminal sending a phishing email to an unsuspecting victim.[10]

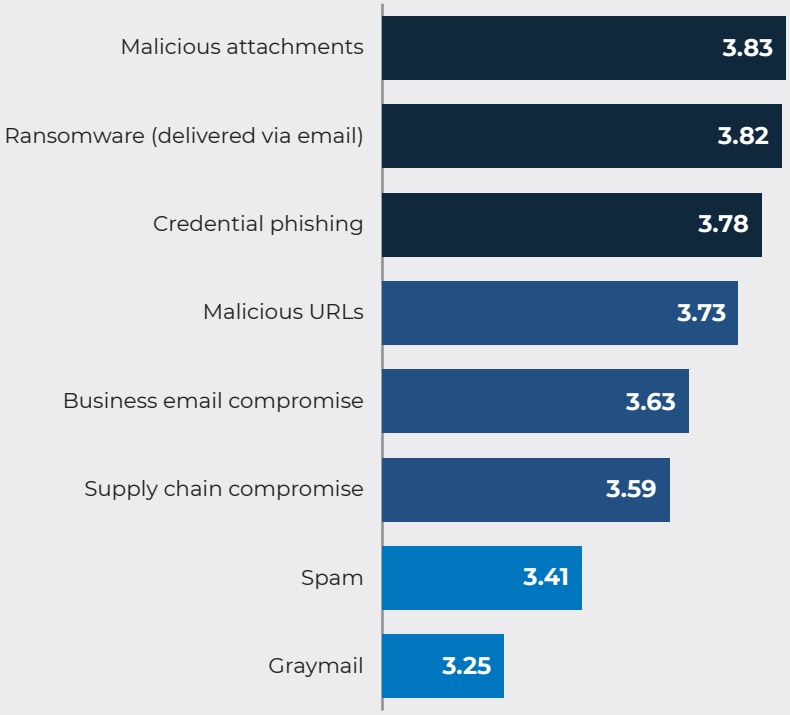
8. Verizon, 2022 Data Breach Investigations Report.
9. Ibid.
10. Deloitte, "91% of all cyber attacks begin with a phishing email to an unexpected victim," Jan 2020.

WHAT'S KEEPING EMAIL SECURITY STAKEHOLDERS UP AT NIGHT?

Survey respondents have a broad array of concerns, nearly all of which seem to be equally pressing. They're worried about malicious attachments, they fret about email-delivered ransomware attacks, and they're anxious about credential phishing, among other things.

FIGURE 4: GREATEST EMAIL-BORNE THREATS TO TODAY'S ENTERPRISES

On a scale of 1 (lowest) to 5 (highest), rate your concern for the following types of email-related threats.



Aside from spam and graymail, which seem to be viewed as more of a nuisance than a significant threat, the email-related threats were perceived similarly. Responses were fairly tightly clustered, with most threats ranked between 3.5 and 3.9 on a five-point scale.

Nonetheless, malicious attachments, often thought to be the easiest type of email-borne threat to detect and block, remain a significant concern for enterprise security teams. Perhaps this is because they're still bypassing legacy solutions, or perhaps it is simply due to the fact that ransomware has been a hot topic across the industry over the past few years.

It's also possible that there's a lack of awareness about the severity and frequency of BEC and supply chain compromise attacks. Like nearly all types of cybercrime, the prevalence of BEC increased sharply in 2020 and 2021, with the FBI receiving a staggering 19,954 complaints about BEC attacks during 2021 alone. These attacks resulted in adjusted losses of approximately $2.4 billion in 2021,[11] while total exposed international and domestic losses exceeded $43 billion between 2016 and 2021.[12]

11. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), Internet Crime Report 2021.
12. Federal Bureau of Investigation, Public Service Announcement, "Business Email Compromise: The $43 Billion Scam," May 2022.

Meanwhile, credential phishing remains the most common method that attackers leverage to gain entry into victim environments, according to research conducted by Verizon.[13] As we've noted, phishing is also commonly employed in ransomware attack sequences and is the first step to launching attacks from legitimate user accounts. Once a threat actor has access to the account itself, there's no telling what information they can glean to run additional attacks—both inside the organization and against its vendors and customers.

The bottom line: in today's world, every one of these threats is serious, and organizations need effective protection against all of them.

Financial Supply Chain Compromise: A Worrisome New Attack Trend

Vendor email compromise, a subset of financial supply chain compromise, is a relatively new attack type that's quickly grown into a significant security threat for organizations of all sizes. In this type of attack, a cybercriminal gains access to an email account and then uses that account to launch attacks against the partners and vendors of that organization. Criminals commonly request payment for a fraudulent invoice, change banking details for upcoming payments, or otherwise try to extort funds.

According to research conducted by Abnormal Security, the prevalence of these vendor impersonation attacks has steadily grown over the last year, surpassing the number of executive impersonation attacks for the first time in January 2022, and increasing every month since.[14]

13. Verizon, 2022 Data Breach Investigations Report.
14. Abnormal Security, From CEO Fraud to Vendor Fraud: The Shift to Financial Supply Chain Compromise, June 2022.

Current Capabilities and Confidence Levels

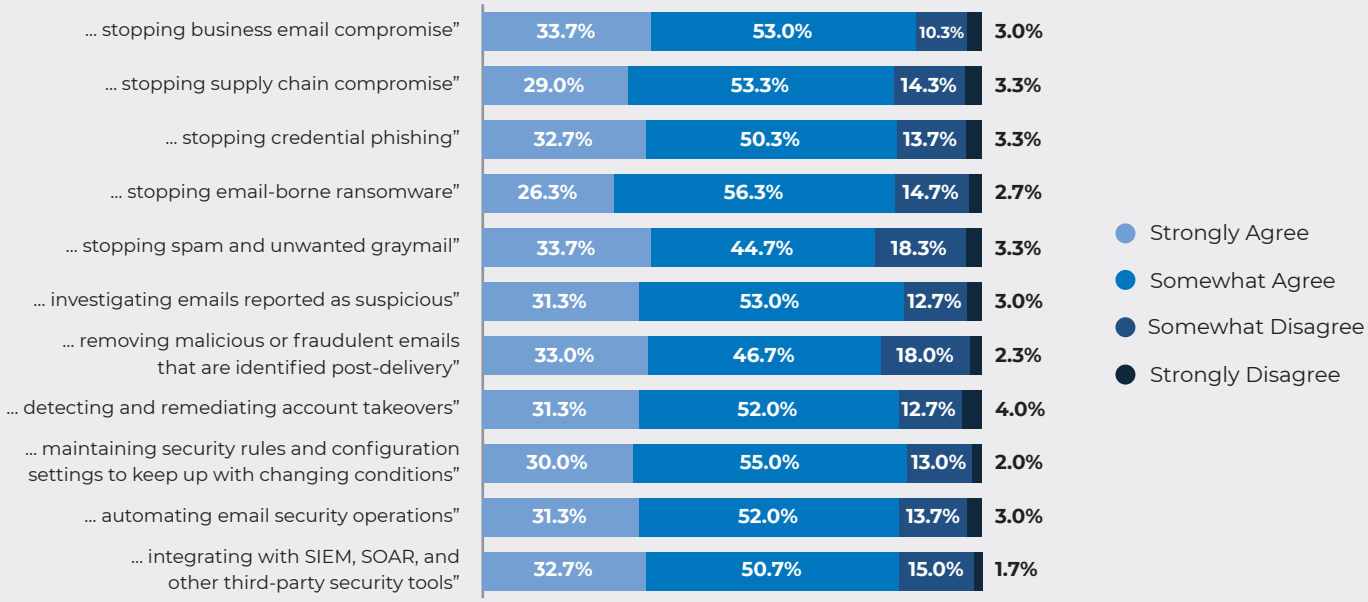
Although there's growing awareness among stakeholders regarding the need for security improvements, there's also a significant degree of overconfidence in both the ability of employees to recognize threats and in the ability of security teams to respond at speed.

COULD THE EMAIL SECURITY SOLUTIONS BE DOING A BETTER JOB?

It's clear that they certainly could. Approximately one-third of respondents strongly agree that there's a need for improvement in *all* capabilities listed, and approximately one-half either agreed or strongly agreed with every statement.

FIGURE 5: ADEQUACY OF CURRENT EMAIL SECURITY CAPABILITIES

Describe your agreement with the following statements as they pertain to your current email security solution: "There is significant room for improvement when it comes to..."



Respondents are apparently aware that there's a need for improvement across the board, which reflects the fact that *all* attack types are important to defend against. Keep in mind that a single successful BEC or supply chain compromise attack could result in millions of dollars lost, which may be why business email compromise was the attack type where the most respondents saw room for improvement. These results also show increasing awareness of the need to protect against vendor fraud. In fact, the largest supply chain compromise attack observed by Abnormal Security used a fake invoice to request an astonishing $2.1 million.[15]

The findings also suggest that respondents may struggle to prioritize since there's a fundamental need to cover all the bases. After all, more than 78% of respondents generally agree that there's room for improvement in all areas. As a result, security professionals may be concerned that they lack knowledge of or visibility into the environments they're charged with protecting.

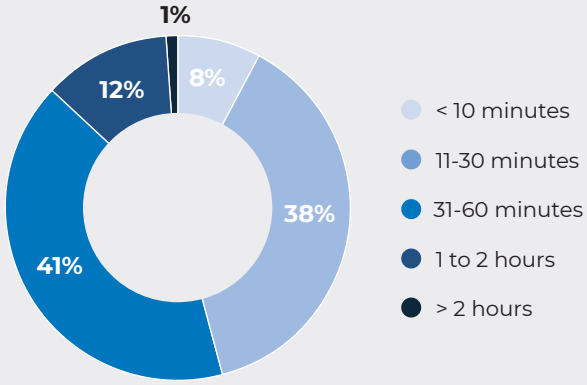
15. Abnormal Security, From CEO Fraud to Vendor Fraud: The Shift to Financial Supply Chain Compromise, June 2022.

HOW MUCH TIME IS BEING LOST TO INEFFICIENCIES IN THE TRIAGE, INVESTIGATION, AND REMEDIATION OF EMAIL ATTACKS?

Far too much. The survey results show that phishing remains a massive problem that continues to consume enormous amounts of time and other resources.

FIGURE 6: TIME LOST TO PHISHING ATTACKS

On average, how long does it take your organization to investigate and remediate a user-reported phishing email?



More than half of survey participants (54%) reported that they require more than half an hour to fully remediate each phishing email reported by an end user within the organization. More than one in eight (13%) need more than an hour to investigate and remediate each phishing attack. The problem is particularly severe among large enterprises, 23% of which need more than an hour to investigate and remediate a single phishing email.

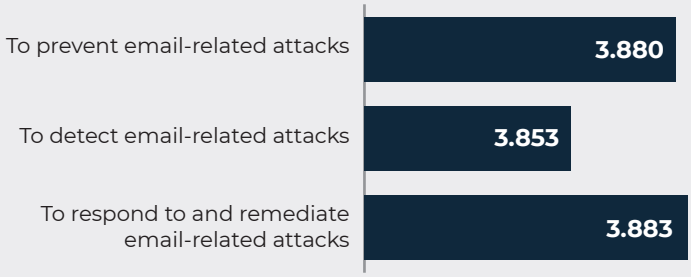
Together, these findings (which are surprisingly high) imply the need for automated solutions that can accelerate investigation and remediation so what would take minutes or hours if tackled manually can be achieved in mere seconds.

HOW WELL DO RESPONDENTS BELIEVE THEY PERFORM ACROSS THE EMAIL ATTACK LIFECYCLE?

Broadly speaking, respondents believe they're equally good at all stages of mitigating email-related attacks.

FIGURE 7: EMAIL ATTACK MITIGATION CAPABILITIES

On a scale of 1 (lowest) to 5 (highest), rate your organization's capability...



There was remarkably little variation across all stages of mitigating email-borne attacks, and there was also little statistically significant variation across geographies or by organization size.

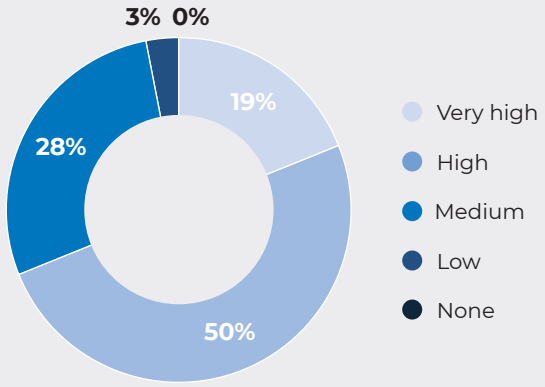
However, there appears to be a disconnect between the medium to high confidence levels voiced here and the far-reaching need for improvement that was articulated in response to the previous question. It seems that respondents assess their own capabilities more favorably when asked to take a broad overview than when invited to drill down into specifics. This could be an indication that security leaders are more likely to think in positive terms about their own security performance, even when the key metrics to measure success—like the number of attacks bypassing security tools or the amount of time it takes to remediate a user-reported email—tell a different story.

IS THERE AN OVERCONFIDENCE IN EMPLOYEES?

It's likely. Participants rated their employees' ability to identify and appropriately respond to malicious emails higher than industry statistics or breach data suggest is actually the case.

FIGURE 8: FAITH IN EMPLOYEES' ABILITY TO RECOGNIZE MALICIOUS EMAIL

What is your level of confidence in your employees' ability to identify and properly respond to a malicious or fraudulent email?



Among survey participants, there's a surprising—and perhaps excessive—amount of confidence in the ability of employees to respond appropriately to malicious emails. Nearly 70% of survey participants expressed a high or very high level of confidence that end users in their organization would be able to identify and properly respond to a malicious email, with only 3% indicating that they had low confidence in their employees.

Unfortunately, this degree of confidence isn't warranted, given real-world incident and financial loss statistics. According to recent Abnormal Security research, as many as 20% of employees will engage with a cybercriminal by responding via email to a BEC attack,[16] and the IC3 report indicates that 28% of all losses to cybercrime are a direct result of business email compromise.[17]

Interestingly, respondents who voiced lower levels of confidence in *their* ability to prevent, detect, and respond to email-borne attacks also said they were less confident in employees' ability to respond appropriately to these attacks.

Overall, it's clear that the confidence respondents have simply doesn't match reality. There's a strong need to implement assistive technologies that can improve the organization's ability to defend against these threats by preventing malicious emails from ever reaching employees' inboxes—ensuring they never even have an opportunity to engage with them.

16. Abnormal Security, CISO Guide to Business Email Compromise, May 2022.
17. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), Internet Crime Report 2021.

What's Needed for Success

In their current state, the email security solutions deployed in enterprise environments aren't effective enough to block the most dangerous email-borne threats. Meanwhile, security operations professionals exist in a chronic state of alert fatigue and overwork. As organizations proceed along their journey to the cloud, it will become increasingly important to invest in agile, automated solutions that were purpose-built for the cloud.

WHAT OBSTACLES ARE KEEPING ENTERPRISE SECURITY TEAMS FROM EFFECTIVELY DEFENDING AGAINST EMAIL-BORNE THREATS?

The usual suspects—alert overload, the talent shortage, technology's complexity—play a role, but so does the fact that many organizations continue to rely on email security solutions that are ineffective.

FIGURE 9: BARRIERS TO EFFECTIVE DEFENSE AGAINST ADVANCED EMAIL THREATS

On a scale of 1 (not at all) to 5 (very significantly), rate how each of the following inhibits your organization's ability to effectively defend against advanced email threats.

Responses to this question were tightly clustered, with all barriers ranked between 3 and 3.5 on a five-point scale. This finding indicates that all the challenges mentioned are of significant concern to survey participants.

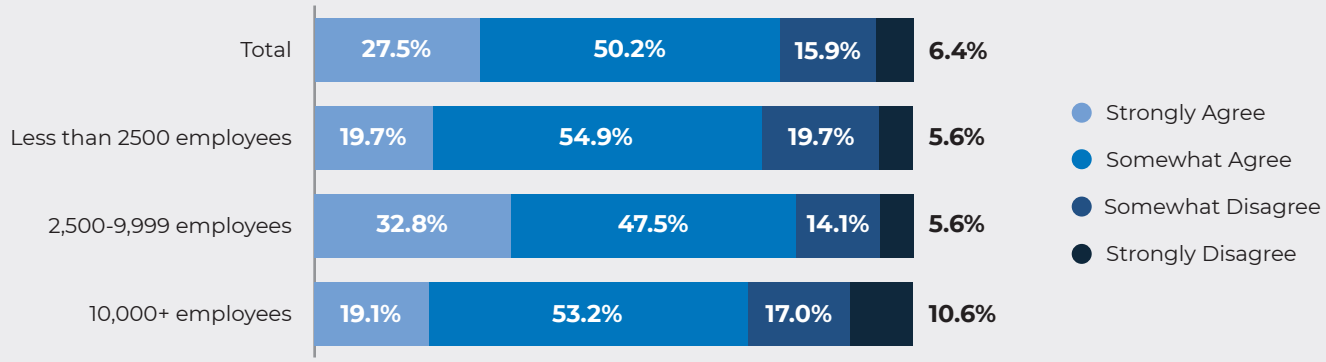
Given the severity of the skills gap in cybersecurity today, it's unsurprising that "lack of skilled personnel" is among the top three responses. Other top responses, including "alert/event overload" and "low effectiveness of email security solutions currently being used," point to the need for more effective security technology. A common challenge for security teams experiencing alert fatigue is that an inability to prioritize means they're not spending an appropriate amount of time on the highest-impact attacks. Machine learning and natural language processing can help identify the highest priority threats, cutting through the noise and helping overworked security teams deliver the most value.

WHICH EMAIL SECURITY SOLUTIONS OR SOLUTION SETS ARE CAPABLE OF SUPPORTING MODERN EMAIL ENVIRONMENTS?

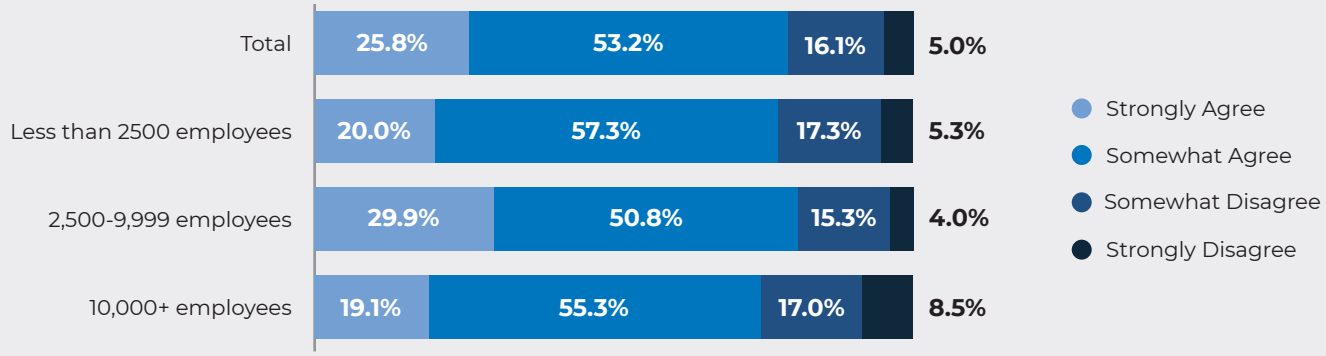
Awareness is growing that neither legacy SEGs nor the native security capabilities offered by Microsoft and Google are adequate for protecting today's cloud email environments against the most advanced threats.

FIGURE 10: CAPABILITIES NEEDED TO SECURE CLOUD EMAIL ENVIRONMENTS

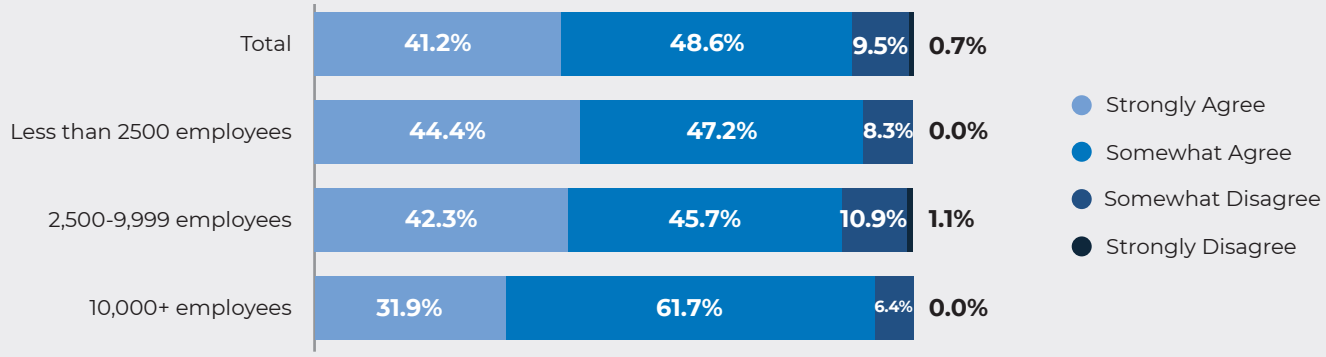
Secure email gateways are legacy solutions that are largely incapable of supporting cloud email environments and thwarting advanced email threats (e.g., BEC, credential phishing).



Alone, the native security capabilities of cloud email solutions (e.g., Microsoft 365, Google Workspace) are insufficient in terms of the scope and/or strength of protection they provide.



The combination of native email security capabilities (e.g., Microsoft, Google) and an integrated cloud email security platform (e.g., Abnormal, Tessian) can replace the functionality of a legacy secure email gateway (SEG).



On this issue, agreement is near-universal: approximately nine out of ten respondents (89.8%) believe that a combination of a cloud provider's built-in security capabilities and an ICES platform can replace the full functionality of a SEG. Furthermore, a robust 77.6% of survey participants feel that SEGs are largely unable to protect cloud environments or defend against advanced email threats like BEC.

While most respondents (78.9%) do not believe that native cloud email security capabilities alone offer adequate protection, the market is growing increasingly confident that, supplemented with the automation, integrations, and advanced functionalities that an ICES solution brings to the table, the combination of ICES and built-in features from a cloud email provider can outperform a legacy SEG. This set of solutions promises a new level of protection—one that's better suited for today's challenging risk landscape.

Among survey participants, there were few differences in opinion across organizations of different sizes. Practically speaking, this near-universal agreement was consistent for everyone, showcasing that this move is likely to occur across the board—no matter the industry, size, or location of the organization.

The Need for Cloud-Native Email Security to Defend Against Today's Advanced Threats

Threat actors have time on their side, as well as the backing of organized criminal syndicates. This gives them ample resources to innovate and develop new email-based attack tactics. They've already honed strategies for circumventing the static rules and policies that security teams have implemented in secure email gateways. Now, they're taking advantage of the cloud's architecture—which is both open and connected—to move laterally from a single compromised account to access other resources. They're also exploiting trusting relationships—such as those between co-workers and partners—to perpetrate email-based fraud that's extremely difficult to detect.

Given that the sophistication and volume of these threats are only likely to increase, the need for more effective and efficient email security solutions is pressing. What's called for is a fundamentally new approach. Leading enterprise security programs are already adopting more intelligent solutions that are far better able to stop the most dangerous attacks.

These are modern, API-driven, cloud-native, integrated cloud email security solutions. They can supplement the built-in capabilities of cloud email solutions to create a deeply integrated and highly effective email security environment. This will drive accurate detection and prevention of email-based threats, saving security teams' time and effort.

With an ICES solution, your email security team can:

- **Protect against *all* types of attacks with precision.** Best-in-class solutions use machine learning and natural language processing to profile known-good behavior and quickly detect anomalies that deviate from this baseline. This deep understanding makes it possible to block malicious emails that bypass other solutions.
- **Deploy the new solution via API in just a few minutes**. Today's leading solutions can integrate with Microsoft 365 and Google Workspaces with no disruption to mail flow. With the right solution, you can get started with just a few clicks.
- **Leverage federated data to protect employees and vendors alike.** The best ICES solutions can automatically identify all vendors in your ecosystem and understand each one's individual risk level. Emails from those at higher risk of fraud can be scrutinized more closely, and when a vendor appears compromised, those third-party attacks can be blocked.
- **Automate email security operations.** Full automation of email triage, remediation, and reporting saves time and makes it easy to rapidly contain missed attacks or reroute misdirected emails.
- **Enhance visibility through integrated insights and reporting.** By centralizing metrics, insights, actions, and the management of global block lists in one place, ICES solutions can provide analysts with a single view of the organization's email security posture—with no need to review multiple tools or dashboards.
- **Improve end user experience.** An ICES platform can help you put an end to spam digests and portals. Leading solutions will learn individual users' preferences and then deliver incoming emails directly into the right folder, removing the need to sort through unwanted mail.

These capabilities will better protect your organization from all types of attacks, and give time back to your security team. As the survey shows, ICES solutions are the future of email security. It's only a matter of time before the market shifts in this direction.

A Word from the Sponsor

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop business email compromise (BEC) and never-seen-before attacks that evade traditional secure email gateways (SEGs). Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA. More information is available at abnormalsecurity.com.