

2022

Cybersecurity
INSIDERS

EMAIL SECURITY:

The Confidence Game



FORTINET®

Introduction

IT and Security pros are increasingly confident that their email security defenses are up to the challenge of successfully guarding against today's email-based threats. From email security solutions like secure email gateways and API-based tools to security awareness training and phishing simulation, our respondents are thinking in terms of multiple layers of defense directly related to email.

But it's also obvious that these same respondents are thinking even more broadly to connect their email security to the rest of their security infrastructure to share indicators of compromise across security layers, to connect the dots to get the fullest context on threats in seconds, and to automate workflows including their response that create greater efficiencies across their security operations.

Key findings include:

- 75% of respondents cited their ability to connect their email security tools to their broader security infrastructure as “Very Important” to “Extremely Important.” Cybersecurity professionals are turning to platform strategies to solve larger-scale security challenges without accompanying increases in budgets or team resources.
- 76% of respondents indicated that their organizations have not experienced a breach with email as the threat vector in the last 12 months.
- 88% of respondents are moderately to extremely confident in the ability of their employees to spot malicious emails.
- 83% of respondents cited their email security solution as “Very Important” to “Extremely Important” to their strategy against email-based ransomware threats.

Meanwhile, we do see some cracks in the facade:

- Despite high overall confidence in their ability to protect against email-based threats, cybersecurity professionals still graded their current email security solution with a low rating of 7.8 out of 10.
- Though 66% of cybersecurity professionals cited ransomware as their top concern, just 53% indicated that they were “Very Confident” to “Extremely Confident” in their capabilities to counter ransomware.

We would like to thank Fortinet for supporting this important industry research project. We hope you find this report informative and helpful as you continue your efforts to secure your organization against email-based threats.

Thank you,

Holger Schulze



Holger Schulze

CEO and Founder
Cybersecurity Insiders

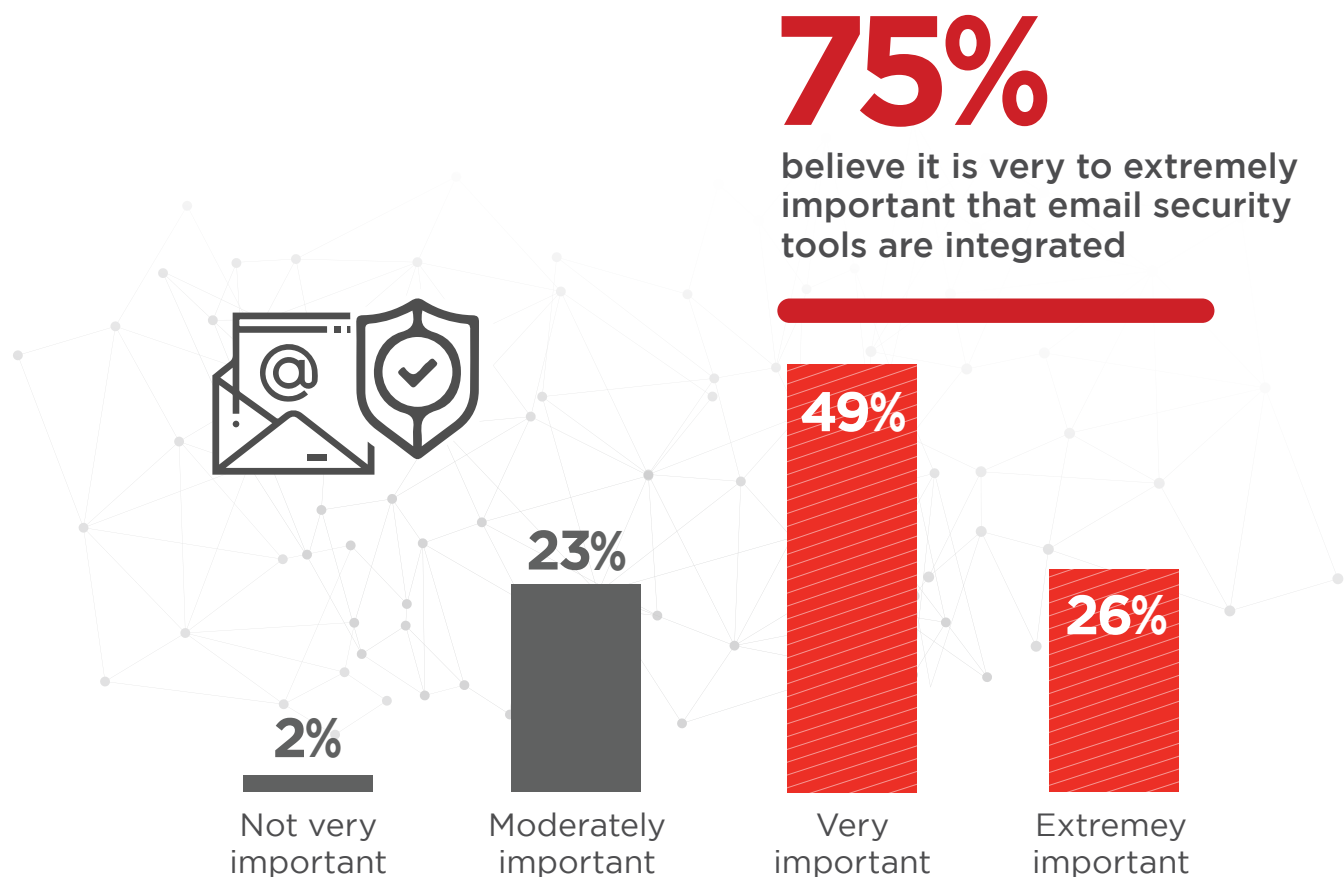
Cybersecurity
INSIDERS

Email security goes **beyond email**

If there is one statistic above all that jumped out in our survey, it was the importance placed on the integration of email security tools with broader parts of organizations' security infrastructure. In fact, 75% of our respondents cited this as "Very Important" to "Extremely Important."

As you'll see with the high confidence organizations currently have in their ability to combat email-based threats, we believe that confidence is in no small part predicated on the ability of organizations to bring broader capabilities and efficiencies to bear when it comes to their email security. In other words, we're talking about the importance of platforms or emerging cybersecurity mesh architectures to help teams enhance their organizations' security, drive automation, and further achieve scale.

- ▶ **How important is it that your email security tools are integrated to work together with other parts of your broader security infrastructure (rather than non-integrated point products)?**



Concern **VS** Confidence

As we cited earlier, confidence is running high and we're pleased as long as this confidence is well-placed. Respondents overwhelmingly indicated they have higher confidence in both their ability to counter email-based threats and in their employees to spot malicious emails should something get through.

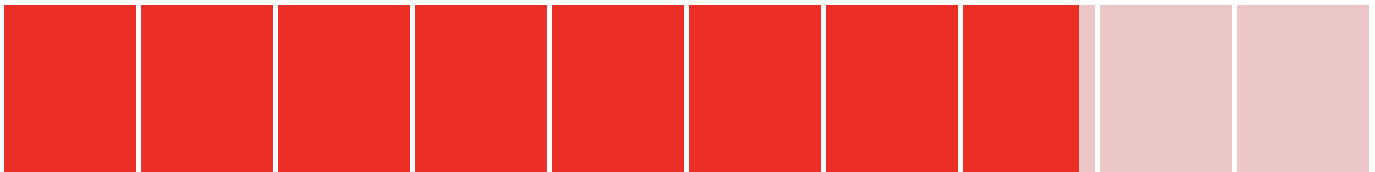
However, we also saw some fractures in that confidence. When asked about their confidence in their current email security tools, respondents gave their current solutions only a 7.8 score out of 10. That's significantly lower than we would have liked to see. What it tells us is that organizations are still seeing spam and malicious emails getting through more than they deem acceptable. It also tells us that their current email security solutions are not performing at a level we deem acceptable.

► **How would you rate the effectiveness of your email security solution or tools today?**



7.8
out of 10

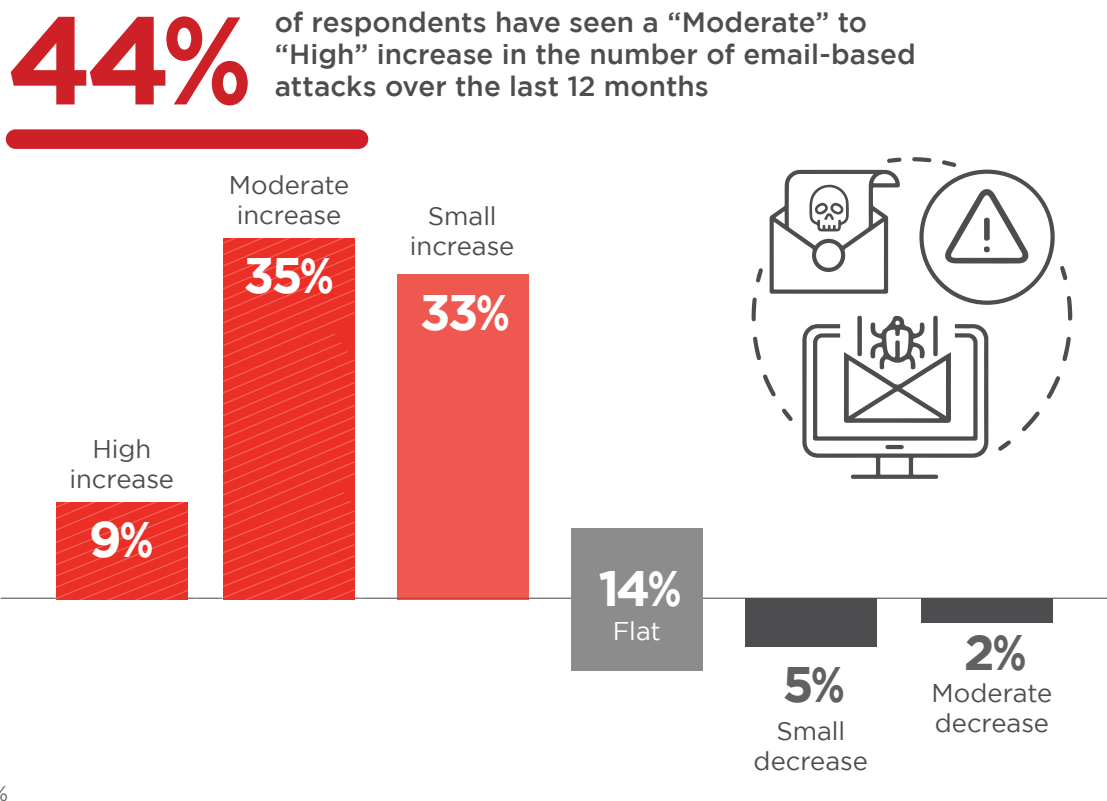
respondents' rating of their
current email security tools



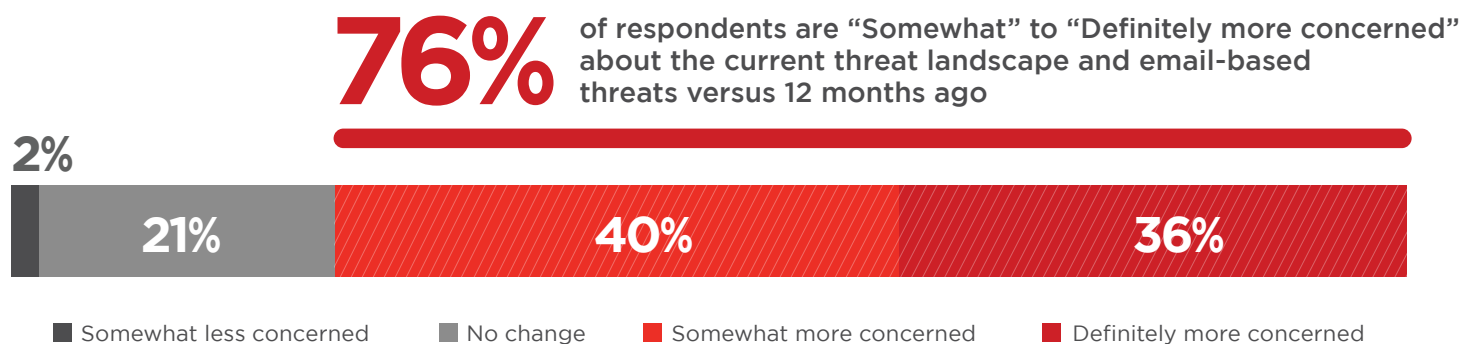
/Concerns

We wanted to know how much IT and Security pros were seeing any intensification of the threat landscape and gauge their sentiments for how they are handling it.

- At your organization, have email attacks increased, decreased or remained unchanged over the past 12-months?



- Compared to 12 months ago, how concerned are you about the current threat landscape and email-based threats?

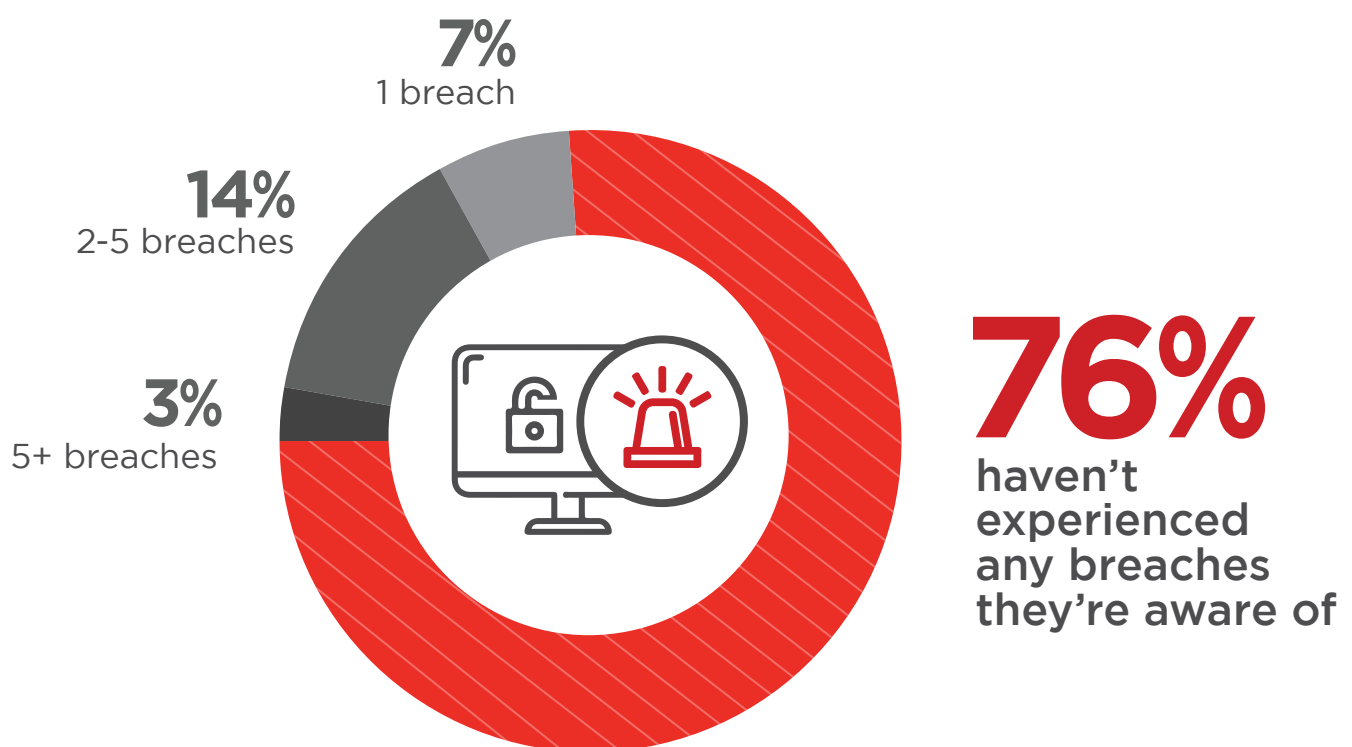


Confidence in posture

Confidence appears to be winning the tug-of-war over Concern. IT and Security pros are simply feeling good about their ability to defend against email-based threats even with the escalation in volume and sophistication we've seen since the COVID-19 pandemic began.

With 76% of respondents citing that their organization hasn't suffered a breach in the past 12 months, it should be no surprise that organizations are feeling more positive about their email security postures. Especially given the large increases in email-based threats we've seen in the last 18 to 24 months.

► **Has your organization experienced a breach(es) in the last 12 months involving email as a threat vector – If so, how many?**



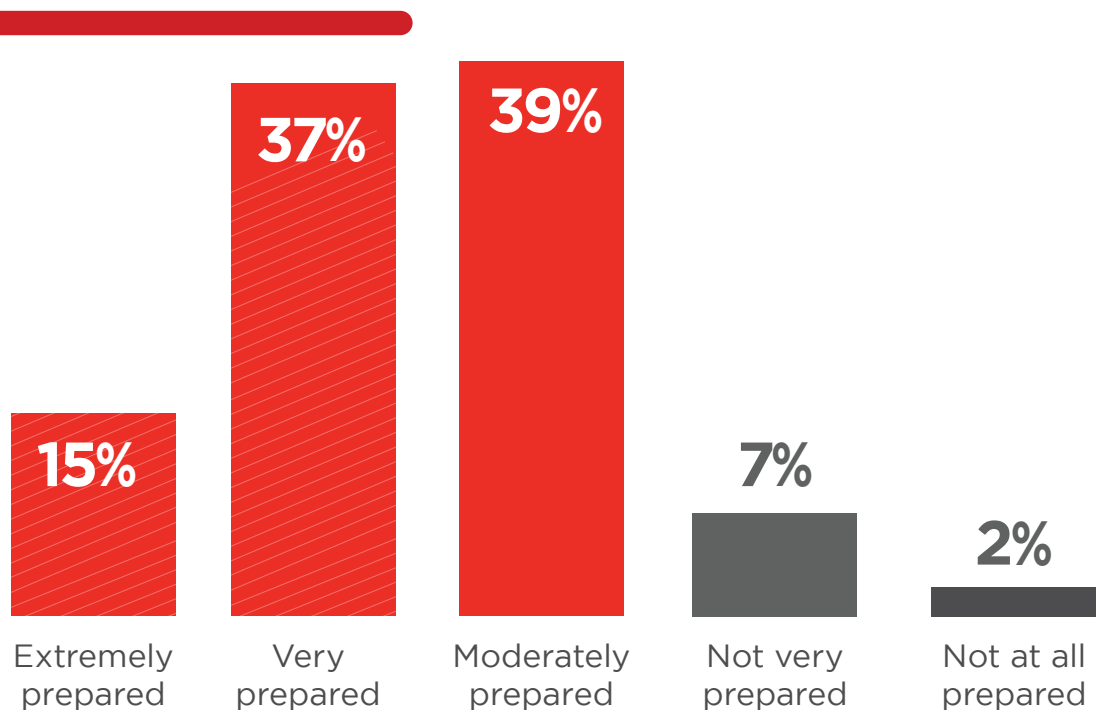
Confidence in preparation

When we asked respondents about mitigating targeted email attacks, here we again see some cracks and room for improvement. Though 91% of respondents cited being at least “moderately prepared” against a targeted email attack, we’d like to see a higher level of respondents citing that they are “very prepared” or “extremely prepared.” In our minds, the stakes are high here - even for the smallest organizations - and so should your preparation.

► In your opinion, how prepared is your organization to mitigate a targeted email attack?

52% 

of respondents are “very prepared” to “extremely prepared” to mitigate a targeted email attack



Confidence in people

For those organizations that have a layered approach to their email security where employees play a role in guarding against email-based threats, confidence is again high. We can't remember a survey result that reflected such a high confidence in employee vigilance.

A surprising eighty-eight percent of respondents are "moderately to extremely confident" in the ability of their employees to spot malicious emails.

► What's your level of confidence in your employees ability to identify a malicious email?




88% of respondents are "moderately to extremely confident" in the ability of their employees to spot malicious emails



Extremely confident

Not at all confident

■ Extremely confident ■ Very confident ■ Moderately confident ■ Not very confident ■ Not at all confident

66% 

are now "somewhat to definitely more confident" in their employees being able to identify malicious emails versus 12 months ago

32% 

see no change in their employees being able to identify malicious emails versus 12 months ago

Confidence in best practices

When we talked earlier about the importance placed on email security tools being integrated with other aspects of organizations' broader security infrastructure – what platforms or cybersecurity mesh architectures help do - we could see how that integration could play a role in IT and Security pros' higher confidence.

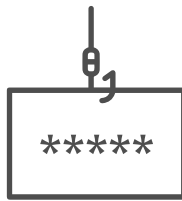
Here's where we also see other practices coming in to play to contribute to that positive outlook. Our takeaway: IT and Security pros are seeing positive, tangible benefits from security awareness training and phishing simulation practices in helping them detect and stop email-based threats.

► Does your organization use any of the following to educate, train and test employees on spotting malicious email?



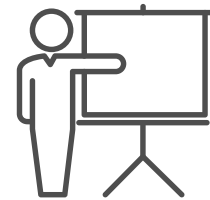
63%

Online security awareness training



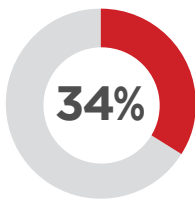
59%

Phishing simulation or testing

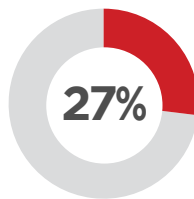


49%

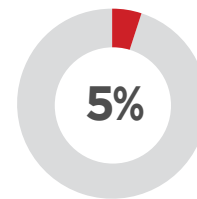
In-person security awareness training



Use a dedicated email for reporting phishing



Use a dedicated button in Outlook/email for reporting suspicious email



Don't use any of the above tools or practices today

Other 2%

Ransomware **menace**

Ah, the menace of ransomware. With 1/3 to nearly 1/2 of ransomware attacks being vectored through email at any time, we wanted to know how IT and security professionals were dealing with the exponential growth in ransomware attacks. In fact, our FortiGuard Labs threat research team saw a 10.7X increase in ransomware attacks hitting our sensors over the July 2020 to July 2021 timeframe. Ransomware has gone well past media attention and hype to a very real cause for concern.

► Which of the following email threats do you see most often?



1 in 5

indicated they see ransomware threats

► Which of the following email threats is you and your business most concerned about?

66%



of respondents who cited ransomware as the email-based threat they worry most about



46%

Impersonation
(where the attacker is posing as a false identity)



41%

Spear phishing
(where the attacker is targeting executives and leaders)



37%

Malicious links

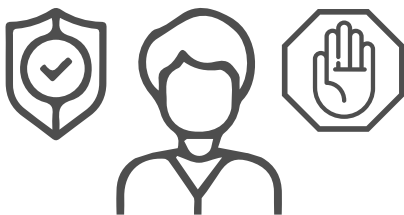
Business Email Compromise (where the attacker impersonates leadership with the common aim to get an employee to wire funds or divulge sensitive data) 29% | Malware (not including ransomware) 24% | Volumetric phishing 12% | Other 7%

Ransomware: **semper paratus?**

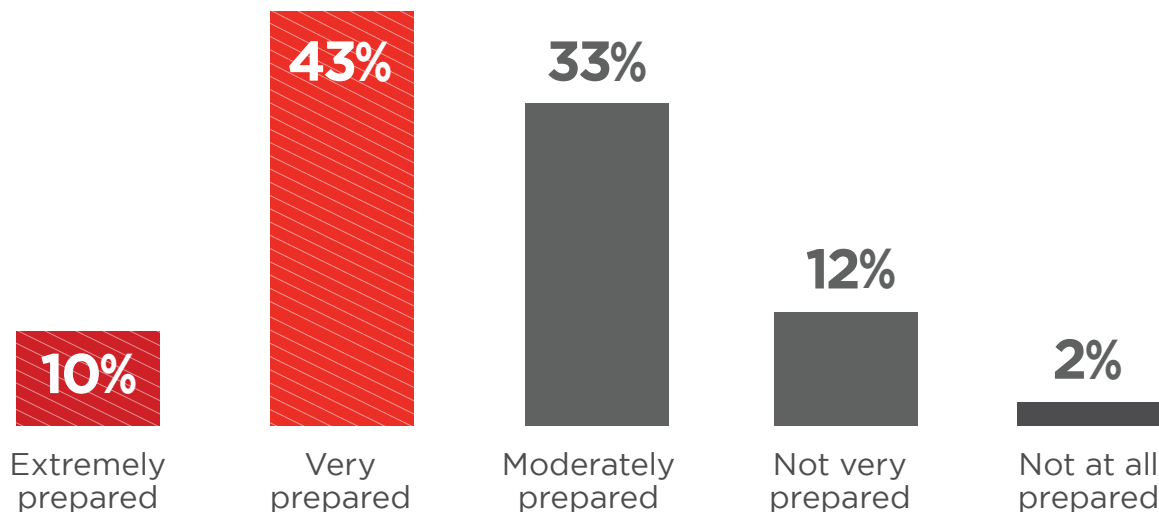
Again, our respondents are telling us they are confident when it comes to combatting email-based threats and in particular, ransomware, despite it being their chief concern. Confidence across respondents is high – though lower than confidence in combatting targeted threats.

Given the increasing frequency of both ransomware threats and successful breaches this past year, we suspect this confidence will be sorely tested in 2022. As a result, we hope IT and Security pros will continue to place high importance on preparation and testing of their defenses against ransomware threats.

► How prepared is your organization for a ransomware attack?



53% of respondents are “very prepared” to “extremely prepared” to combat a ransomware attack



Ransomware: strategy & tactics

IT and Security pros are clearly taking concern and turning it into action when it comes to ransomware. 63% of respondents indicated their Incident Response Plan includes some level of detailed planning and/or specific playbooks and tactics for dealing with a ransomware incident. Meanwhile, organizations have deployed an array of technologies and controls to guard their networks, systems and data from ransomware. Given the growing involvement of ransomware in reported breaches over the past 18 months, we'd like to see higher levels of planning that adequately account for ransomware as organization appears to be affecting organizations of all sizes across all industries.

- In terms of email security and the ability to prevent, detect and respond to email-based ransomware threats, how important of a role does your email security solution and related tools play in your overall ransomware strategy?



83%

of respondents cited their email security solution as “very” to “extremely important” to their strategy against email-based ransomware threats

- How is the threat of ransomware addressed in your Incident Response Plan?

We have fully detailed planning and/or specific playbooks and tactics for how to respond to a ransomware attack

17%

We have some detailed planning and/or some specific playbooks and tactics

46%

We have very limited planning and/or specific playbooks and tactics

27%

We don't have ransomware specifically addressed in our IR plan

7%

We don't have an IR plan

2%

Ransomware: **mitigation**

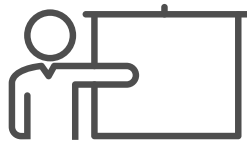
Ransomware is a complex challenge, one not solved by email security tools alone. Besides prevention and detection capabilities, organizations have in place a toolbox of technologies and practices to mitigate the risk and cost associated with a ransomware attack.

► Which of the following does your organization conduct or have in place to prevent, detect and mitigate the impact of a ransomware attack?



79%

Offline
backups



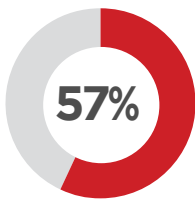
71%

Employee
cyber training

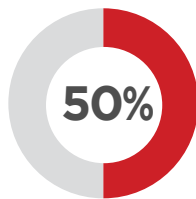


67%

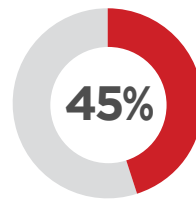
Business
continuity
measures



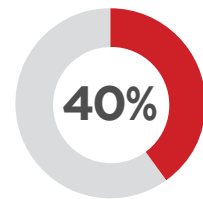
Network
segmentation



Remediation
plan



Risk assessment
plan



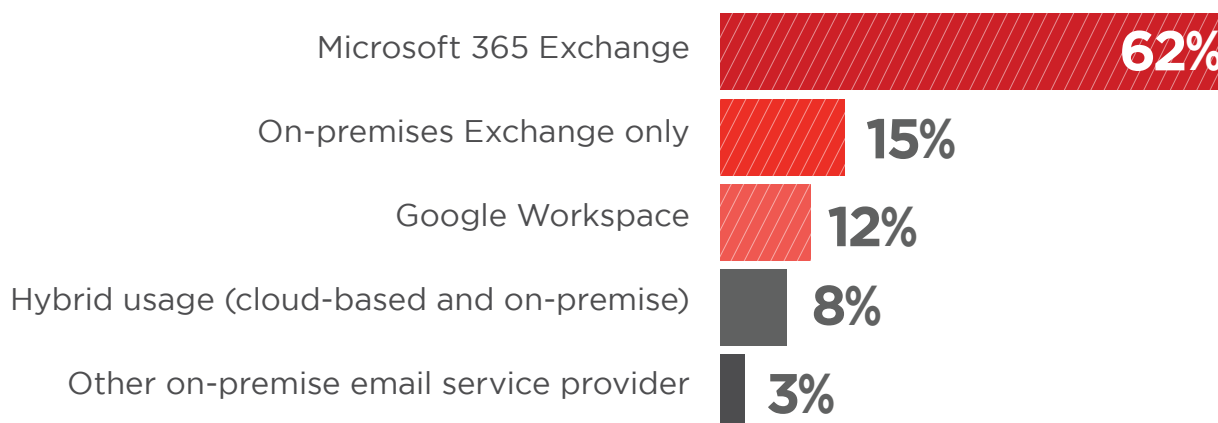
Cybersecurity/
ransomware
insurance

Forensics abilities 31% | Testing of ransomware recovery methods, technologies and policies 29% | Incident response vendor on retainer 26% | Red or blue team exercises 12% | Ransom payment guidance 10% | Other 2%

Cloud-based email adoption

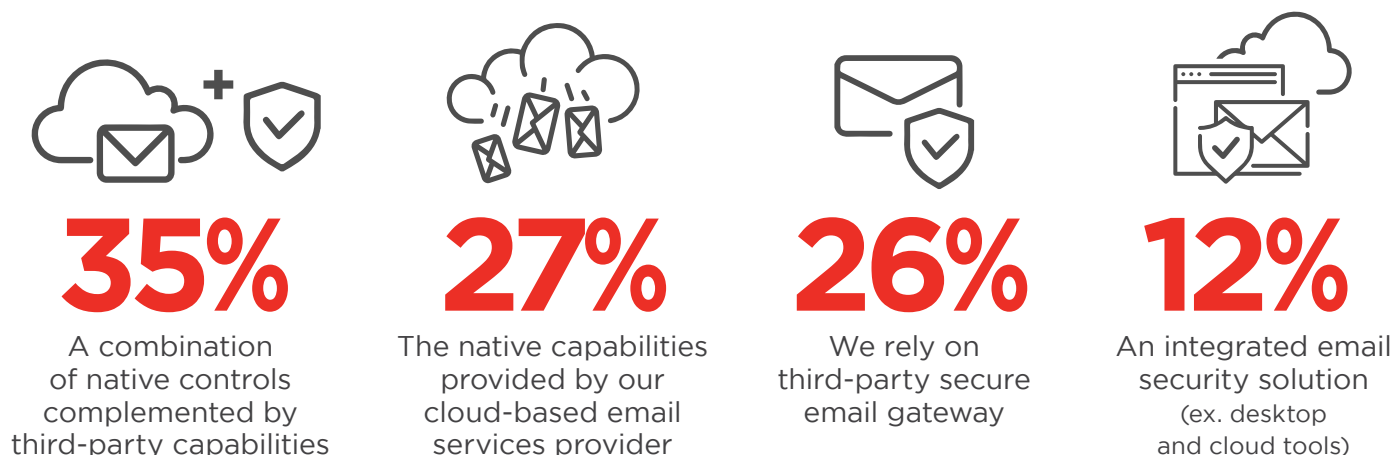
Organizations are clearly moving away from on-premise instances for their email services to capitalize on advantages SaaS the cloud offers. When it comes to adoption of cloud-based email services, Microsoft Office 365 has the lion share of the marketplace.

► What email services does your organization utilize?



Larger and more complex organizations are likely to utilize a combination of email security capabilities.

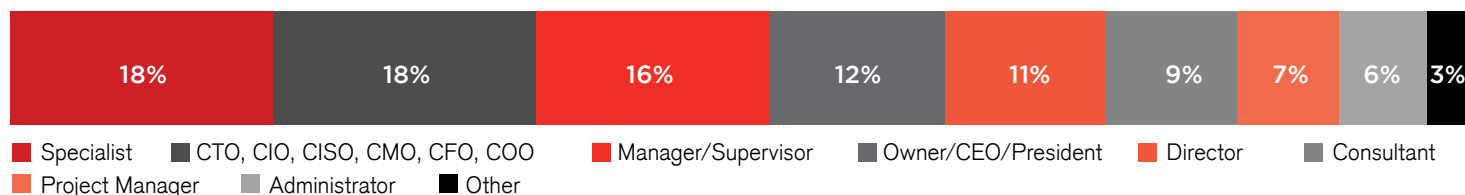
► What tools or services do you use to secure email today?



Methodology & demographics

The Email Security in 2022: Confidence Game report is based on the results of a comprehensive online global survey of 294 cybersecurity professionals, conducted in Fall 2021, to gain deep insight into the latest trends, key challenges, and solutions for email security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

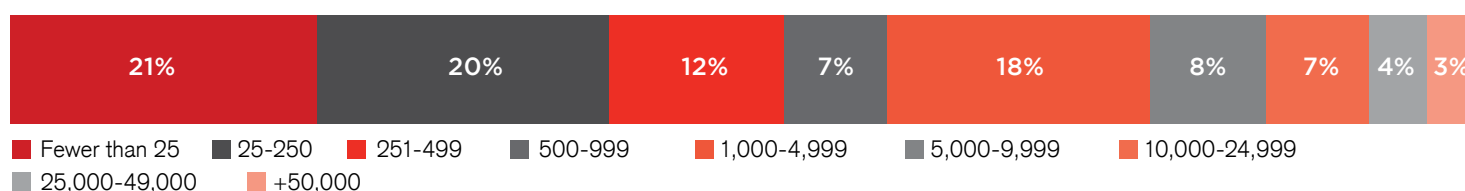
CAREER LEVEL



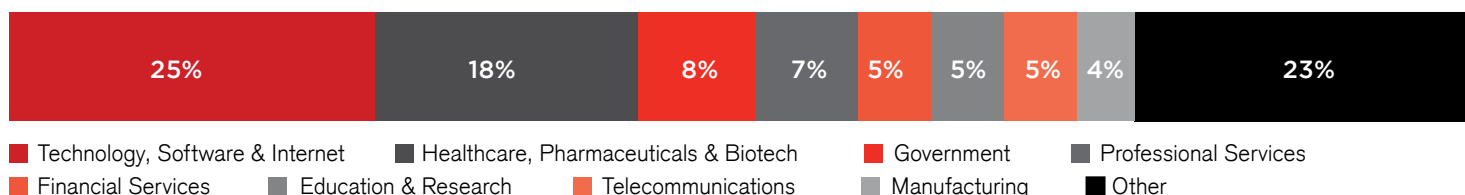
DEPARTMENT



COMPANY SIZE



INDUSTRY





Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as the company with the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.

[**www.fortinet.com**](http://www.fortinet.com)