proofpoint.

BUYER'S GUIDE

Choosing the best email security for your organization

Key capabilities

Here are the key capabilities you should look for when evaluating a modern email security solution:

1. Protection against the widest variety of threats
2. Automated detection and response
3. Flexible deployment options
4. A great user experience
5. Threat protection beyond email

Overview

Email remains a primary vector for cyber threats. However, in recent years, the attack surface has expanded beyond email as people communicate and collaborate across multiple digital channels. Not surprisingly, cybercriminals are adapting to take advantage of this trend. In fact, they're more successful than ever at distributing a wide range of human-centric threats across all digital channels.

In response, organizations are cobbling together a patchwork of best-of-breed point products to address these threats.

Unfortunately, this creates gaps in their defenses and leaves many risks unaddressed. What's more, managing and integrating different security tools is complicated and costly. To avoid these pitfalls, organizations need a comprehensive email security solution that can defend against current and emerging human-centric threats in a single platform.

In this guide, we'll outline the key capabilities that you should look for in a complete email security solution. We'll also explore why these capabilities are important.

Figure 1: Breakdown of the threat types delivered through email.

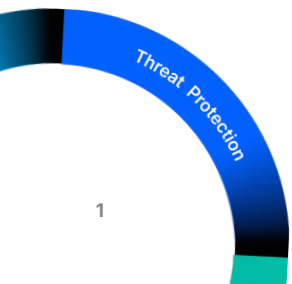


Figure 2: A comprehensive view of email-borne threats prevented by Proofpoint Core Email Protection.

$55B

Losses worldwide due to BEC scams from 2013 to 2023[2]

60 seconds

Average time it takes for a user to fall for a phishing email[3]

1: Protection against the widest variety of threats

The average cost of a data breach caused by a phishing or business email compromise (BEC) attack is $4.88 million.[1] This is the second-highest breach cost, trailing only that of malicious insiders. But every threat that slips through the cracks can be costly in terms of financial losses and brand damage.

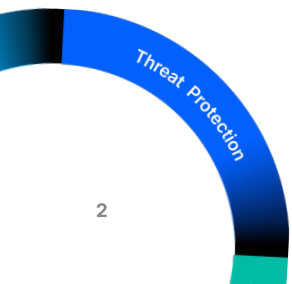
Security teams want to reduce their organization's risk exposure as much as possible. The only way to do it effectively is to stop the widest variety of threats.

Here's what to look for in an email security solution:

- **Uses real-time threat intelligence.** Up-to-the-minute threat intelligence helps identify emerging threats. However, threat intelligence is more than just data. Highly trained threat research teams also need to be involved. When a solution has both, it can analyze trends on a global scale faster and more efficiently. This includes detecting and tracking advanced cybercriminals and nation-state actors as well as identifying shifts in the threat landscape.
- **Harnesses AI for threat detection.** To stop email attacks that rely on manipulation with malicious payloads, a multilayered, AI-driven detection stack is essential. Look for large language modeling, relationship and behavioral graphs, machine learning, and the ability to parse images. These features will help ensure that threats are stopped at scale.
- **Monitors for threats continuously.** The ability to sandbox URLs and attachments is important. But *when* you sandbox them matters just as much. To catch missed or time-delayed attacks, look for a solution that detects and stops threats throughout the entire threat lifecycle. That means pre-delivery, post-delivery and at the moment users click.
- **Provides visibility into targeted users.** You want to know who's being attacked, how they're being attacked and whether they act. It's also important to know how they're being targeted, what data they have access to and whether they tend to fall prey to attacks. With this information, you can enable the right protective measures at exactly the right moment.

When threats are caught early, your organization will be safer. Plus, your security and IT teams won't have to spend their valuable time responding to incidents and remediating them.

1. IBM. *Cost of a Data Breach Report*. 2024.
2. FBI. "Business Email Compromise: The $55 Billion Scam." Sept. 2024.
3. Verizon. *Data Breach Investigations Report.* 2024.



2: Automated detection and response

Malicious messages delivered to inboxes or reported by users can bog down security teams and reduce their productivity. It takes a lot of time to analyze and remove these threats manually. It's essential to detect and respond to threats quickly. Doing so can mean the difference between a minor incident and a full-scale breach.

Here's what to look for in an email security solution:

- **Provides an AI-powered abuse mailbox.** User-reported suspicious messages should be handled as quickly as possible. When these messages are automatically directed to a machine-monitored inbox, they can be analyzed by AI and condemned without being reviewed by your security or IT teams. An automated response system should also let users know their reports have been received. This closes the feedback loop and reinforces positive behavior.
- **Automates orchestration and remediation.** Malicious emails shouldn't be allowed to sit in users' inboxes. Instead they should be removed automatically from inboxes across your organization. Also, make sure that the solution integrates easily with your existing SIEM/SOAR tools. That will provide you a more unified view of your security ecosystem.
- **Simplifies workflows.** Security tools should make analysts' jobs easier. For example, analysts can work better with intuitive workflows and clear, AI-generated threat summaries. Features like integrated search and priority-based alerts can help them quickly hunt for threats. They also benefit from tools that accelerate any remaining remediation after automation.

When the efficiency of your security team goes up, your organization's defenses get stronger. You also get the most value from your existing security resources and investments.

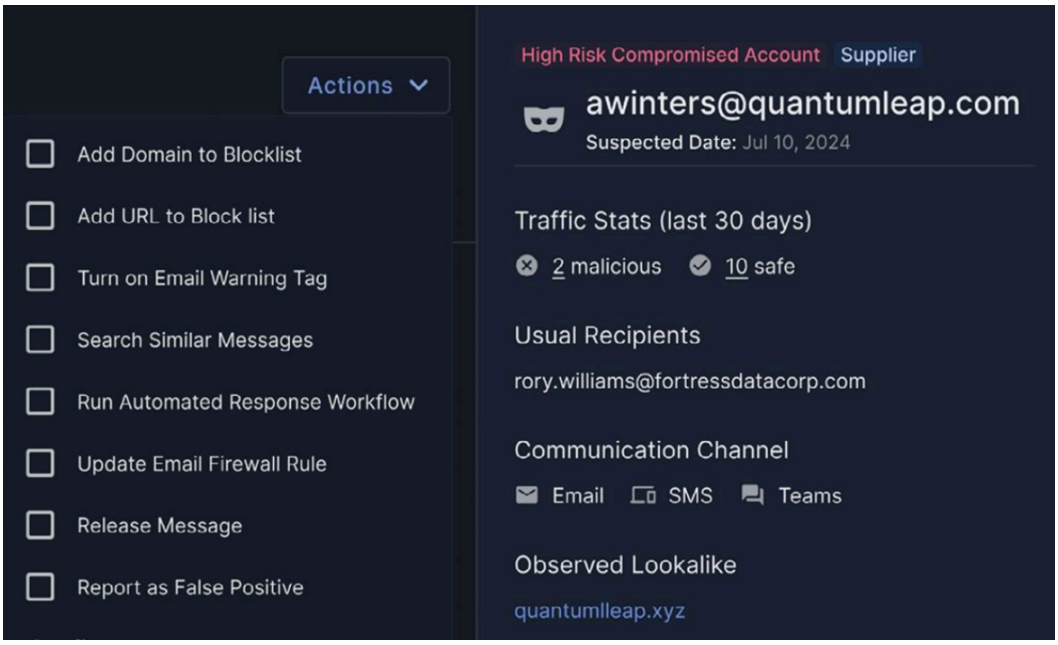
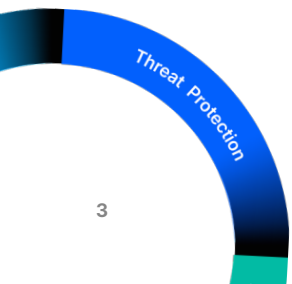


Figure 3: Example of automated detection and response workflows in Proofpoint Core Email Protection.



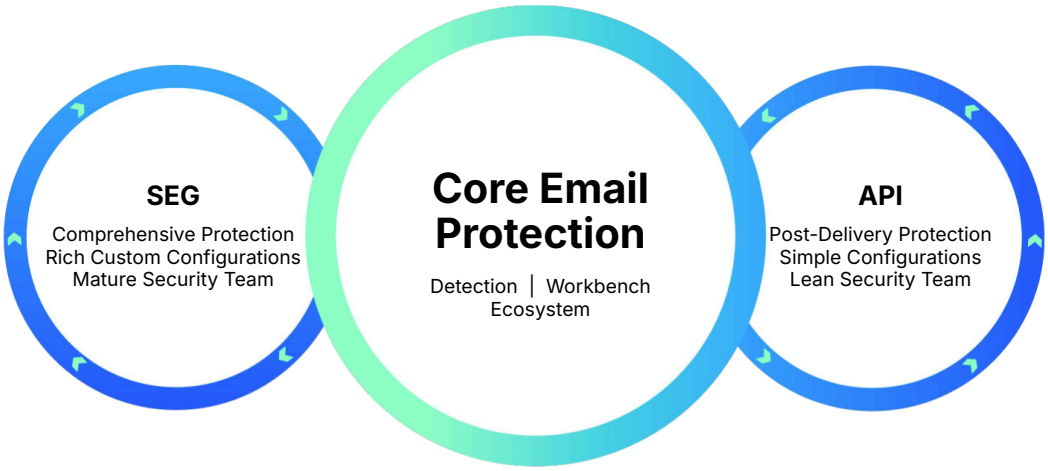


Figure 4: Benefits of SEG and API deployment with Proofpoint Core Email Protection.

3: Flexible deployment options

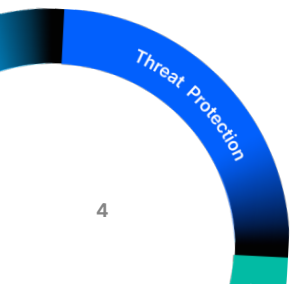
Your architecture, security priorities and compliance requirements are constantly in flux. An email security solution should be able to grow and change with you. Even if an API-based deployment is the best approach now, it might not be as your business evolves and vice versa. Not being locked into a single deployment approach ensures that you can optimize your coverage based on your risk.

Ultimately, when you have a choice, your security and IT teams are empowered to scale and build your defenses for long-term success. And your organization can maintain robust protection as it grows.

Here's what you should consider:

- **Secure email gateway (SEG) deployment.** SEGs offer complete protection for a wide variety of environments. This option is best if you need highly customizable email security. SEGs allow you to maximize your end-to-end protection with pre- and post-delivery and click-time protections. They provide flexible configuration options as well as visibility into people risks.
- **API-based deployment.** This option provides easy onboarding and preset controls within cloud platforms like Microsoft 365. Deployment can be completed in minutes. It's the right choice if you need powerful but low-touch email security and are looking for a "set-and-forget" admin experience with easy-to-understand threat insights and automated remediation capabilities.

By choosing a vendor with flexible deployment options, you get the detection that you need. You also help ensure your security is future-proof.



74%

Percentage of CISOs who believe that people are their company's biggest vulnerability[4]

40%

Security awareness can decrease employee clicks on real-world threats by more than 40% in less than six months[5]

4: A great user experience

There's a saying that your biggest risk and best detection occupy the same space: between the chair and the keyboard. If you want malicious messages stopped, people need to have the right tools.

When they are overwhelmed, they're more likely to ignore real threats or make mistakes. Spam, graymail or constant false alarms increase risk. Employees need clear, actionable warnings, intuitive reporting tools and well-designed phishing simulations to reinforce positive security behaviors.

Here's what to look for in an email security solution:

- **Detects spam/graymail.** Spam and bulk messages clutter inboxes and distract users. Even graymail, like unsolicited sales emails, can chip away at their productivity. Email security that keeps inboxes clean and focused improves the user experience and helps employees stay on task.
- **Nudges users about suspicious messages.** Suspicious emails might be malicious, or they might be legitimate—only a user can say. Contextual preview notifications tell users about the threat signals found in messages. At the same time, they automatically defang malicious URL links or attachments that are associated with the suspicious message, requiring the user to interact with the notification before they interact with the actual email.
- **Provides click-time protection.** Even well-intentioned employees can slip up and click on a threat during a busy moment. Click-time protections like warning banners help users pause and think before engaging. Meanwhile, virtual browsing windows add an extra layer of defense by blocking credential theft and malware downloads.
- **Personalizes security awareness training.** Often, phishing simulations and awareness training are the primary ways that employees engage with email security tools. The most effective tools deliver real-time learning to users when they click on a phish. They also offer interactive, bite-sized modules that are tailored to each user's level of knowledge. This personalized approach builds stronger awareness and better long-term behavior.

A harmonious user experience can empower your employees to stay aware while still staying on task.

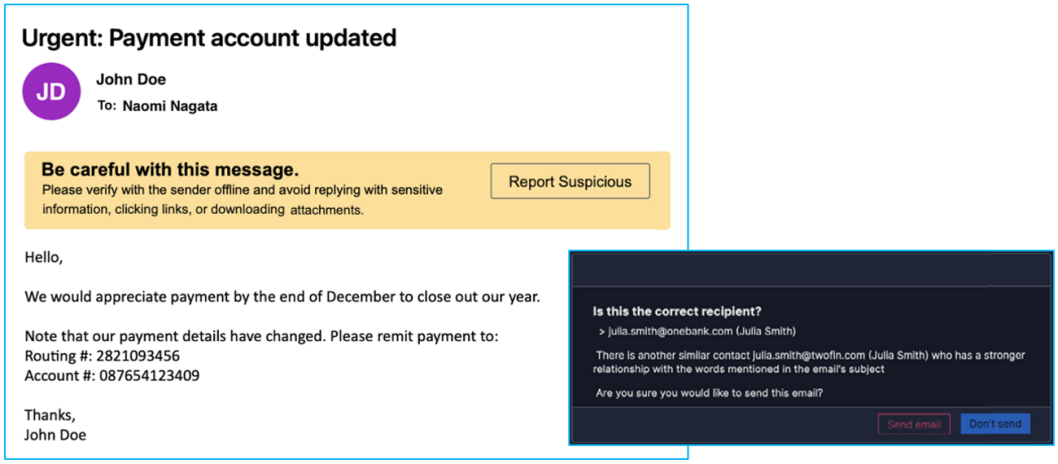


Figure 5: Example of a misdelivered message alert and an email warning banner.

4. Proofpoint. *Voice of the CISO.* 2024.
5. Proofpoint ZenGuide research.

2,524%

Increase in URL threats delivered through SMS-based phishing over the last three years[6]

5: Threat protection beyond email

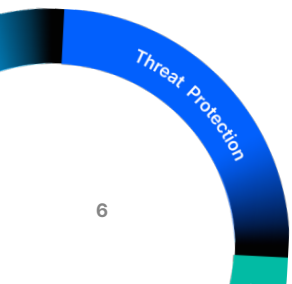
As the digital workspace expands, it's important to have an adaptable platform. It should be able to protect not just email, but also newer digital communication channels. Cybercriminals no longer limit their attacks to email. They have followed users to platforms like Microsoft Teams, Slack, Zoom, LinkedIn and WhatsApp, which are new attack vectors.

For a solution to be future-proof, it should include additional advanced protections, like DMARC-based email authentication, high-fidelity detection of compromised cloud accounts and visibility into supplier-based email threats.

Here's what else to look for:

- **Streamlines email authentication.** One of the most effective ways to stop spoofed messages is with email authentication for both inbound and outbound messages. To help ensure brand protection, look for a vendor offering hosting or managed services to streamline authentication deployment. Expert guidance can be invaluable when it comes to DMARC.
- **Detects compromised accounts.** Combining email threat visibility (like real-world clicks on phishing messages) with cloud access broker alerts delivers more accurate detection of compromised accounts. This reduces false positives and enables automated responses like forcing password resets or unsharing sensitive files.
- **Protects against phishing beyond email.** Malicious URLs are now the most common delivery method for attacks, partly because they can be sent to users anywhere, including through messaging, collaboration and social media apps. Choose a solution that can inspect URLs in real time so malicious links are blocked anywhere and anytime users try to access them.
- **Reduces supplier risk.** It can be challenging to identify threats in your supply chain without the right visibility. Email security solutions with built-in supplier risk capabilities can assign risk scores and detect compromised supplier accounts, helping prevent email fraud. When paired with authentication, this proactive approach can strengthen protection against one of the most difficult attack vectors to spot.

With these capabilities, your teams can stay ahead of new and emerging threats wherever they originate.



6. Proofpoint research.

Conclusion

More than 94% of the threats that target your employees are initiated through email.[7] That's why a strong defense for this primary vector is essential.

To maximize your threat protection, look for a comprehensive email security solution that includes basic and advanced protections. It should detect and respond to threats automatically. And it should offer an excellent user experience. Ideally, you want the solution to have flexible deployment options to adapt to future changes. It should also secure digital channels beyond email, including collaboration tools, messaging platforms and cloud applications.

Do you rely on fragmented, best-of-breed point solutions? If so, you have room to improve your email defenses. Now is the time to assess how well your security protects against all human-centric threats for email and beyond.

Proofpoint delivers human-centric security

Proofpoint Core Email Protection empowers your organization to reduce risk everywhere your people interact—today and in the future.

Core Email Protection stops 99.99% of email threats before they become compromises. Powered by our industry-leading Proofpoint Nexus AI-driven detection stack, it identifies and remediates advanced email threats including phishing, BEC, malware, ransomware, account takeover, impersonations, social engineering and more. With a modern and intuitive console, security analysts work efficiently with comprehensive threat visibility and automated remediation workflows. Our solution's architecture is future-proof for tomorrow's threat landscape, offering flexible SEG and API-based deployment options.

That's why more than 2 million customers, including 85 of the Fortune 100, trust Proofpoint to protect their people and business with human-centric security.

To learn more, contact our sales team at sales@proofpoint.com.

7. Proofpoint research.

proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyberattacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →

0203-010-01-02