proofpoint.

SOLUTION BRIEF

Advanced Email Security

Protect against advanced email threats, streamline operations and get actionable visibility into people risk and your threat landscape

Products

- Proofpoint Email Protection
- Proofpoint TAP
- Proofpoint TRAP
- Proofpoint Email Isolation
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense
- Proofpoint Internal Mail Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

Key Benefits

- Block threats that contain malicious URLs, attachments and ransomware or that attempt email fraud
- Automatically remediate messages submitted by users or activated post-delivery with integrated workflows
- Get unmatched visibility into your people, threats and other insights like supplier and cloud risk
- Easily deploy DMARC policies and enforce authentication quickly and safely to block fraudulent emails that spoof trusted domains
- Educate and empower your users to make them a strong line of defense against cybersecurity threats

Email is a fundamental feature of modern business. It is also the No. 1 threat vector. And email attacks—from phishing attacks to business email compromise (BEC), supply chain attacks, ransomware and cloud account compromise—are constantly evolving. So, effectively securing this vector from threats has proven daunting, even for the biggest and most complex organizations. Proofpoint can help.

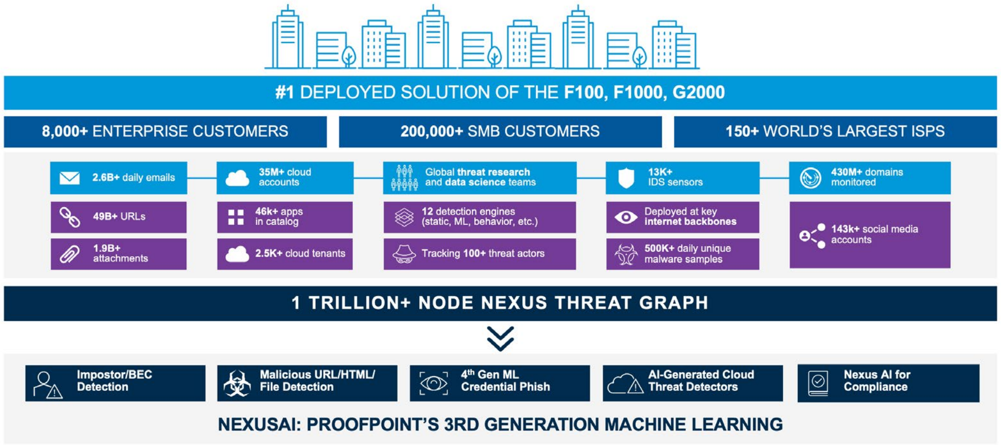
More organizations in the Fortune 100, Fortune 1000 and Global 2000 trust Proofpoint to deal with these threats than any other advanced email security provider. Our solution takes an inline and API approach to meet the challenge. This ensures full protection of all inbound and outbound messages. It doesn't just focus on emails that default security solutions miss. The integrated, layered approach reduces the risk of successful attacks by accurately detecting threats faster. With a leading detection ensemble and a scalable platform, you can improve operational effectiveness. And with actionable insights, you can better understand the risks you face. You'll also be able to take proactive action and respond more quickly and effectively.

Detect and Block Advanced Threats

Get efficacy you can trust

With Proofpoint's threat intelligence and detection, you'll have a stalwart defense against sophisticated threats while minimizing false positives.

We use reputation, URL rewriting, and predictive and click-time sandboxing to detect payload threats, such as those that come through attachments and URLs. Detecting through evasion and obfuscation like CAPTCHA, password protection, render-heavy sites, redirectors and file-sharing sites is built-in.



#1 DEPLOYED SOLUTION OF THE F100, F1000, G2000

8,000+ ENTERPRISE CUSTOMERS

200,000+ SMB CUSTOMERS

150+ WORLD'S LARGEST ISPS

2.6B+ daily emails

49B+ URLs

1.9B+ attachments

35M+ cloud accounts

46k+ apps in catalog

2.5K+ cloud tenants

Global threat research and data science teams

12 detection engines (static, ML, behavior, etc.)

Tracking 100+ threat actors

13K+ IDS sensors

Deployed at key internet backbones

500K+ daily unique malware samples

430M+ domains monitored

143k+ social media accounts

1 TRILLION+ NODE NEXUS THREAT GRAPH

Impostor/BEC Detection

Malicious URL/HTML/ File Detection

4th Gen ML Credential Phish

AI-Generated Cloud Threat Detectors

Nexus AI for Compliance

NEXUSAI: PROOFPOINT'S 3RD GENERATION MACHINE LEARNING

Figure 1: Nexus Threat Graph.

In today's people-centric threat landscape, your users are your greatest asset—they are also your biggest risk.

We also use artificial intelligence (AI) and machine learning (ML) models from Nexus Threat Graph to detect payloadless attacks, such as BEC. The AI/ML models score signals such as supplier risk, user signals from collaboration suites, content natural language processing, receiver relationships and intent. Baseline and contextual data let us quickly spot emails that may be malicious. And they work seamlessly with our threat intelligence and other targeted detection engines. This minimizes false positives.

We analyze email with multilayered content analysis, reputation analysis and sandboxing. This effectively stops advanced email threats, including polymorphic malware and ransomware, before they hit your users. And we provide you with predictive and click-time URL sandboxing to detect and block malicious URLs. Re-writing URLs protects your users on any network and device. It also helps detect if a message has been weaponized after delivery.

Click safely with email and browser isolation

Proofpoint email and browser isolation provide a secure environment for your users to access websites, personal webmail and corporate email safely. Attackers try various tactics and threat vectors to gain access to your systems, like compromising supplier accounts. They can, for example, target your users through personal email or unprotected channels. With isolation, you can disable uploads and downloads. You can also restrict data input while a website is being analyzed in real-time. This takes no more than a few seconds. The technology adds an extra layer to prevent credential theft, malware or ransomware. It is especially useful against phishing emails that contain URLs poisoned post-delivery.

Prevent email fraud with email authentication

Email authentication adds an additional layer of protection. It has proven to be an effective way to stop malware-less impostor threats, such as BEC. However, organizations hesitate to adopt and enforce DMARC standards because of the risk of blocking legitimate email.

Proofpoint helps you fully deploy and enforce DMARC with confidence without blocking legitimate mail flow. It protects against domain spoofing and fraudulent emails using your trusted domains. It stops fraudulent emails at the Proofpoint gateway while protecting your company's email identity. What's more, you can see all impostor threats, including malicious lookalikes of your domain, from a single pane of glass. You have this visibility regardless of the tactic used or the person being targeted. With our Virtual Takedown service, you can proactively prevent fraudulent lookalike domain email attacks before they strike. We simplify your DMARC journey with an experienced consultant who guides you through every step of your deployment. We work with you to identify all of your trusted senders, including third-party senders, to ensure they authenticate properly. Proofpoint has helped more than one-third of the Fortune 1000 through this process. We can work with the most sophisticated configurations.

Protect internal email and quickly contain threats

Protecting internal email is just as critical as protecting inbound email. Attackers use compromised accounts to send phishing, BEC or malware. We scan internal emails for malicious content in the form of URLs and attachments. When we detect a malicious internal email, you can pull and quarantine it automatically. You can do so even if other users already received the email and forwarded it on to others. We also provide reports that show any accounts that may have been compromised. This lets you quickly take action on those accounts.

Get Visibility on Attacks and Your Human Attack Surface

To better mitigate and communicate risk to your management and board, you need to know:

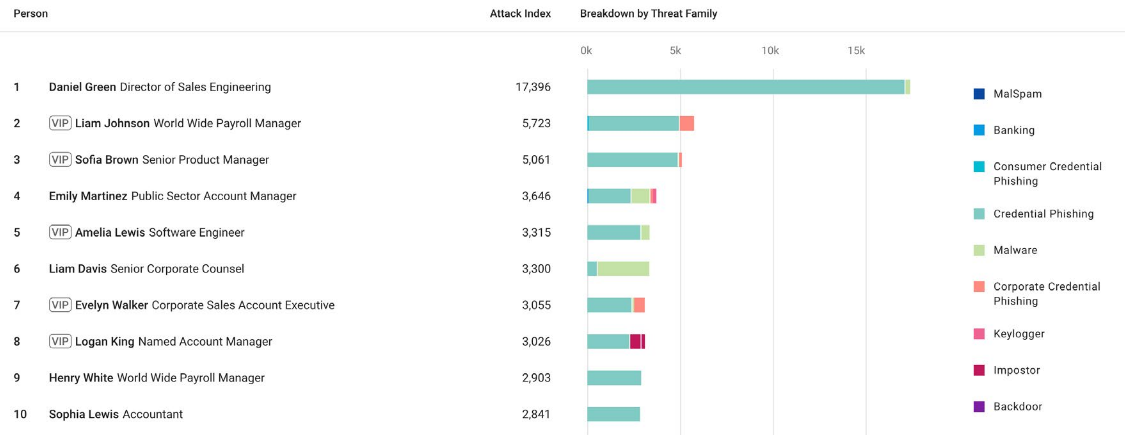
- Users who are most at-risk and how they're being targeted
- Threat landscape insights, objectives, actors and trends
- Other signals like supplier and cloud risk insights

Proofpoint provides all of this and more. And with our platform approach, you get an entire understanding of people-centric risk, without data silos. We empower you to be more proactive against sophisticated threats.

Address risk with people-centric insights

In today's people-centric threat landscape, your users are your greatest asset. They are also your biggest risk. We give you unmatched visibility into targeted attacks and your human attack surface.

We show you who poses the most risk to your organization and why. Our Very Attacked People™ (VAP) report indicates which of your users are being targeted most. And our Top Clickers report shows you which of you users have clicked real malicious messages. You can input and track VIPs in the dashboard. Once you have these insights, you can implement adaptive controls for your risky users to prioritize and mitigate risk. These controls can include targeted security awareness, browser isolation and multifactor authentication.



	Person	Attack Index
1	**Daniel Green** Director of Sales Engineering	17,396
2	VIP **Liam Johnson** World Wide Payroll Manager	5,723
3	VIP **Sofia Brown** Senior Product Manager	5,061
4	**Emily Martinez** Public Sector Account Manager	3,646
5	VIP **Amelia Lewis** Software Engineer	3,315
6	**Liam Davis** Senior Corporate Counsel	3,300
7	VIP **Evelyn Walker** Corporate Sales Account Executive	3,055
8	VIP **Logan King** Named Account Manager	3,026
9	**Henry White** World Wide Payroll Manager	2,903
10	**Sophia Lewis** Accountant	2,841

Breakdown by Threat Family
0k
5k
10k
15k
MalSpam
Banking
Consumer Credential Phishing
Credential Phishing
Malware
Corporate Credential Phishing
Keylogger
Impostor
Backdoor

Figure 2: Proofpoint's Very Attacked People (VAP) report shows the most at-risk users and threat types.

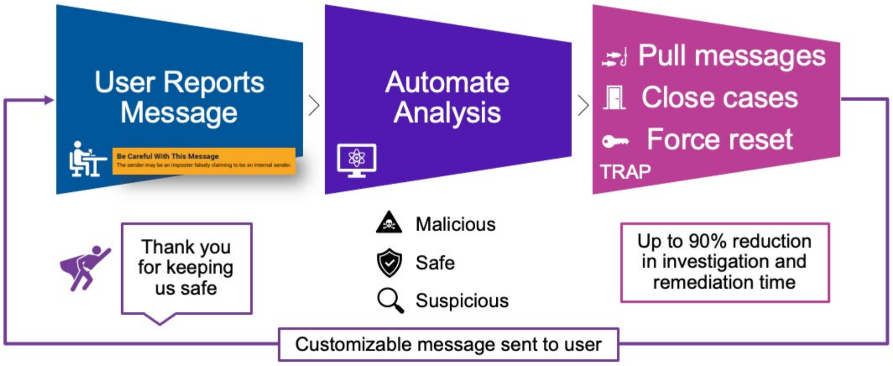

User Reports Message
Be Careful With This Message
The sender may be an imposter falsely claiming to be an internal sender.
Automate Analysis
Pull messages
Close cases
Force reset
TRAP
Thank you for keeping us safe
Malicious
Safe
Suspicious
Up to 90% reduction in investigation and remediation time
Customizable message sent to user

Figure 3: Proofpoint's automated abuse mailbox solution Closed-Loop Email Analysis and Response (CLEAR).

Receive threat-centric insights for context

We provide real-time detailed forensic information on threats and campaigns. Our deep threat analysis shows you everything from who was being attacked, the origin of the attack and what the attack looked like. We also determine the objective of the attack. (We can tell, for example, if it aimed to exfiltrate data, install ransomware, execute fraud and so on.) We connect the dots between email attacks and suspicious logins. This helps you uncover and stop account compromise more effectively. The platform provides comprehensive benchmarking about the types of threats and objectives you're receiving compared to your peers.

Integrate supplier and cloud compromise risk insight

We provide you with visibility into compromise and supplier risk. Visibility across these attack vectors lets you address complex attacks thoroughly. With Nexus Supplier Risk Explorer, we automatically identify potentially compromised suppliers as well as the domains they use to send email to your users. And with our included SaaS defense feature, you can get insight to potentially compromised users, malicious or exposed files and risky third-party applications.

Improve Operational Effectiveness

Many organizations have understaffed or overwhelmed security teams. These teams often must manage multiple security vendors and products that don't always talk to each other. We provide you with an integrated solution that focuses on the threats that matter and that automates threat detection and remediation. This saves you time and money, as your security teams can spend fewer internal resources on remediation compared with if they were using competing solutions.

Auto-pull malicious emails

We take the manual labor and guesswork out of incident response. This helps you resolve threats faster and more efficiently. We remove phishing emails containing URLs that were poisoned post-delivery. And we can remove—with one click or automatically—any unwanted emails from internal accounts that are compromised, even if they were forwarded or received by other users. Also, our Nexus Threat Graph provides alerts and automatically collects and compares forensic data. This gives you an actionable view of threats. You can reduce email remediation time by up to 90% using this approach.

Streamline the abuse mailbox process

We help you streamline the abuse mailbox process and reduce your IT overhead. Users can easily report suspicious messages with one click. They can do so directly from an Email Warning Tag or by using the PhishAlarm® email reporting add-in. If the reported message is found to be malicious, it and other copies can be quarantined automatically. And your users receive a customized email that lets them know the message was malicious. This helps reinforce future behavior to report similar messages. Administrators can get in-depth reporting on user behaviors and accuracy of reporting malicious messages benchmarked against peers.

Change Behavior With Threat-driven Education

Modern email threats often require humans to activate them. But your workers don't need to be a weak link in your cyber security defense. Security-conscious employees, in fact, can be a strong line of defense against cyber attacks.

Proofpoint lets you take action on your VAPs or Top Clickers. Data collected on them is automatically integrated into our security awareness platform. The platform uses this data to run a more targeted, impactful education program. It lets you use real-world phishing simulations from Proofpoint threat intelligence to create timely and relevant educational experiences. Users who fall for a simulation are presented with just-in-time guidance. They can then be automatically enrolled into specific training. We also provide users Email Warning Tags with Report Suspicious capabilities. These provide short customizable descriptions and visuals of the risk associated with a particular email, and they allow users to report messages directly from the tag. This helps the users make more informed decisions. These features work seamlessly on all devices and applications.

Protect Against Data Loss Via Email

Email is the No. 1 threat vector for both inbound threats and outbound data loss. So you must secure your sensitive data and prevent data loss via email. We give you out-of-the box visibility and enforcement to prevent intentional and accidental data loss during email communication. Email data loss prevention (DLP) and encryption are tightly integrated. They can be centrally managed in the Information and Cloud Security platform. With the new unified alert manager, you can customize out-of-the-box data explorations to hunt for and report on DLP violations you care about. Simplify operations with optimized workflows and remediation capabilities. We analyze confidential information within structured and unstructured data. And we provide you with fine-tuned policies and prebuilt dictionaries. These automatically identify data protected by regulatory compliance and data privacy laws. And they help you comply with data protection rules across a range of industries—including PCI DSS, SOX, HIPAA, GDPR and more—while reducing your manual work. When combined with encryption, you can define and customize unique policies to automatically encrypt sensitive data in email. This makes it easy for you to manage and secure sensitive data exchange.

Summary

Proofpoint Advanced Email Security effectively protects against threats that target email. It provides you with actionable visibility into your attacks and your most attacked people. Our solution:

- Blocks advanced threats before they're delivered
- Provides unmatched visibility into your people risk, threats, and other insights
- Improves operational effectiveness with efficacy and automated threat response
- Educates and empowers users to become a strong line of defense
- Protects against data loss via email

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT 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 cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, 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**.

proofpoint.