# STOPPING MALWARE

## WITH ADVANCED EMAIL PROTECTION

# OVERVIEW

Today's sophisticated threats are changing. They're multiplying. They're morphing into new variants. And they're targeting people, not just technology. As organizations embrace the cloud and go mobile, data is moving beyond the perimeter. So are today's biggest cyber threats.

Ransomware and other advanced malware-based attacks are slipping right by traditional defenses.

To stay ahead of the bad guys, your security teams need proactive solutions. That starts with detecting unsafe content and behavior. But it also includes acting on threats before they cause lasting harm.

## WHAT'S ON EVERYONE'S MIND

### RISKY USER BEHAVIOR

- Clicking on malicious URLs
- Opening infected attachments
- Succumbing to social engineering tactics

### EVOLVING THREATS

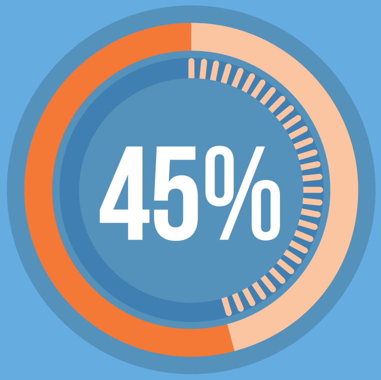
- Advanced threats (ransomware and other malware)
- Non-malware threats (email fraud, credential phishing)

### TOP CONCERNS

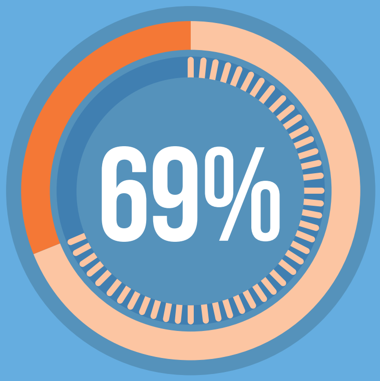
- Theft of sensitive data
- Business disruption
- Direct monetary losses
- Compliance and legal problems
- Damage to brand and reputation

## STATISTICS TELL THE STORY*

Top priority for enterprises: strengthening cybersecurity



of organizations report a **security skills gap**



of organizations are **increasing security spend**

* ESG-Proofpoint Lab Report: "Preventing, Detecting and Responding to Advanced Email-Based Attacks"

# THREAT BASICS

## ADVANCED EMAIL-BASED MALWARE THREATS

Bad actors use a wide variety of sophisticated techniques to bypass security tools. They take advantage of the "human factor" to target people, not just technology. In fact, many advanced threats rely on user interaction as a first step. From there, they steal valuable corporate data. They get victims to send money directly (through ransomware payments or bogus wire transfers). And they get account credentials to gain network access.

### THE THREATS

- Ransomware
- Polymorphic malware
- Email fraud
- Weaponized documents and URLs

### THE ISSUES

- Change and evolve at a breakneck pace
- Volume of variants has multiplied significantly
- Evade traditional defenses, such as whitelists, sandboxes

### HOW THEY WORK

- Delivered through malicious email attachments and URLs
- Exploit technical flaws in business software
- Leverage social engineering

# A MULTI-LAYERED EMAIL DEFENSE IS ESSENTIAL

Most of today’s targeted threats arrive by email. Partnering with technology leaders and dedicated security organizations like Proofpoint can help you stay ahead of threats—now and in the future. Proofpoint Advanced Email Security covers the entire spectrum of known email threats.

**These include:**

- Commodity threats (such as spam and known malware)
- Advanced threats (such as ransomware and targeted attacks)
- Non-malware-based threats that use social engineering (such as email fraud and credential phishing)

# MUST-HAVES FOR ADVANCED EMAIL PROTECTION

According to ESG, here's what security teams need to prevent, defend against, and respond to today's threats:

- Proactive prevention, detection and blocking of threats—before they arrive at their targets
- Tools that improve incident response and effectiveness
- Visibility into threats outside the network perimeter
- Automation to reduce manual effort
- Sharing threat intelligence to protect against future threats
- Regular reporting on security posture and security effectiveness

> “Considering the widening cybersecurity skills gap, cybersecurity resources are being stretched thin. What is needed is a solution focused on quality of data and analytics that can provide visibility into all types of attacks; control and content analysis; protection of employees, customers, and partners; prevention of data loss; and rapid response when needed.”
>
> – ESG Lab

## ESG-PROOFPOINT LAB REPORT: “PREVENTING, DETECTING AND RESPONDING TO ADVANCED EMAIL-BASED ATTACKS”

A recent ESG Lab report commissioned by Proofpoint examines how Advanced Email Security handles today’s evolving email threats. The research firm highlighted the following features of Proofpoint’s multilayered solution:

- Integrated technologies that combat malware and non-malware-based threats
- Complete visibility into email messages and email threats
- Shared threat intelligence for faster, more effective detection, response and remediation

# COMBAT MALWARE FROM ALL ANGLES

## PROOFPOINT ADVANCED EMAIL SECURITY

As ESG Lab points out, Proofpoint combines multiple advanced technologies to tackle today's email attacks. With deep threat analysis and layers of sandboxing, Advanced Email Security:

- Provides clear visibility into email-based attacks
- Uses deep content analysis to classify, monitor and route sensitive data
- Authenticates inbound and outbound email to prevent email fraud
- Protects against data loss— both inadvertent and as the result of a data breach
- Helps your IT and security teams respond to threats more quickly

### PROOFPOINT'S UNIQUE CAPABILITIES

| **Email Protection uses multiple techniques, including:** | **Targeted Attack Protection (TAP) detects and blocks:** | **Information Protection protects against data loss with:** | **Threat Response Auto Pull (TRAP) proactively protects by:** | **Threat Intelligence speeds detection and response by:** |
|---|---|---|---|---|
| • Quarantine of incoming email by type: phishing, impostor email, malware, bulk and more<br>• Detection of non-malware-based threats | • Ransomware and advanced attacks targeting people<br>• Malicious attachments and URLs<br>• Weaponized documents and sandbox evasion<br>• Credential phishing | • Easy management of sensitive content sent through email<br>• Automatic data classification by policies and standards<br>• Transparent encryption and quarantine | • Removing emails with URLs or attachments that are weaponized after delivery – even if emails have been delivered or forwarded<br>• Using automation to do more in less and save hours of manual clean-up | • Gathering intelligence through dynamic threat analysis<br>• Positively identifying malicious behavior<br>• Correlating data across attackers and attack campaigns |

# ESG LAB GIVES PROOFPOINT THE THUMBS UP

| ESG LAB VALIDATION | PROOFPOINT CAPABILITY |
|---|---|
| ✓ | Addresses risks that slip by traditional point solutions |
| ✓ | Remediates threats promptly |
| ✓ | Identifies and prioritizes email-based threats through the TAP dashboard |
| ✓ | Provides at-a-glance information about each threat with one click for details and analysis |
| ✓ | Offers visibility into threats, enriched with insights from a team of 100+ researchers |
| ✓ | Shares aggregated intelligence across other security tools to identify attackers and their campaigns |
| ✓ | Makes the most of limited resources through an integrated approach |

> “Proofpoint’s multilayered approach integrates visibility provided by deep threat intelligence with incident response tools to provide full visibility across the threat lifecycle and reduce the cost and complexity of verifying, containing and resolving threats.”
>
> – ESG Lab

> “ESG Lab validated that Proofpoint’s Advanced Email Security solution provides visibility into all email-based attacks, implements core control and deep content analysis, enables email authentication for both inbound and outbound business email, protects against data loss and enables rapid response to threats and attacks.”
>
> – ESG Lab

# THE PROOFPOINT DIFFERENCE

**Dedicated security and compliance company**

**Protects more than 4,000 organizations worldwide**

**Scans over a billion messages for threats per day**

**Named a leader in the Gartner Magic Quadrant for email protection six years running**

**Trusted by Fortune 100 and Fortune 500 companies**

★★★★★

**96% customer satisfaction rate**

# LEARN MORE

To learn more about how Proofpoint can help you stop malware and other threats including email fraud and phishing read the full ESG Lab Report: "Preventing, Detecting, and Responding to Advanced Email-based Attacks."

## ABOUT ESG LAB REPORTS

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

## ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.