

# Targeted Attack Protection

## Protect Your People from Advanced Threats in Email and Cloud Apps

### KEY BENEFITS

- Stop threats before they reach the inbox
- Detect known and unknown threats in email
- Respond with end-to-end insight
- Provide adaptive isolation controls for riskiest URLs or users
- Deploy quickly and protect everywhere
- Focus resources on your most attacked people
- Identify and highlight your most attacked users

### KEY FEATURES

**Attachment Defense**—TAP can open and sandbox many Microsoft Office and PDF files—even if locked or compressed.

**URL Defense**—TAP inspects URLs and quarantines messages that link to malicious web pages and attachments.

**SaaS Defense**—TAP inspects files in cloud apps for threats. It also surfaces potentially compromised accounts.

Proofpoint Targeted Attack Protection (TAP) helps detect, mitigate and block advanced threats that target people through email. This includes attacks that use malicious attachments and URLs to install malware or trick users into sharing passwords and sensitive information. TAP also detects threats and risks in cloud apps and connects email attacks related to credential theft or other attacks.

Traditional cybersecurity solutions, using legacy techniques such as reputation and signatures, are no longer enough to identify and stop malicious email and cloud-based threats.

TAP stops both known and new, never-before-seen attacks. It detects polymorphic malware, weaponized documents, credential phishing and other advanced techniques. And it gives you end-to-end insight to identify and protect your most targeted people.

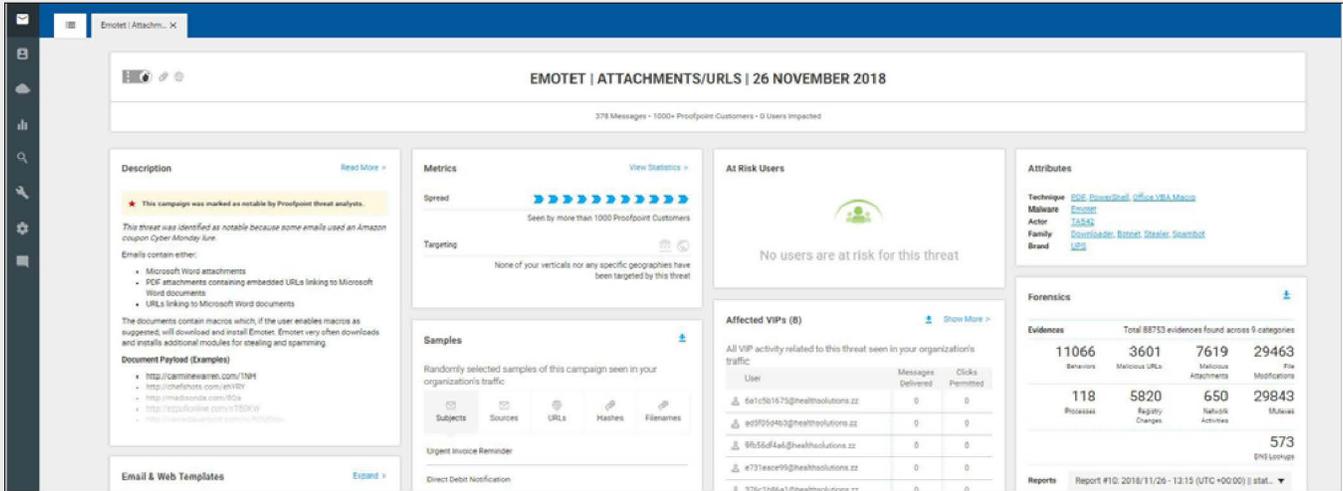
### Stop Threats Before They Reach Your People

TAP provides greater context into how attackers are targeting your executives, your most attacked people and other users. It can extract threat intelligence from attacks and quickly block malicious messages, reducing your attack surface and security risk.

Other threat solutions examine SMTP traffic after it has penetrated the network perimeter. But with this approach, you don't get the context to understand who is affected by the threat, and you can't inspect encrypted network traffic. That means you get only a limited view of the email threat landscape. And because these tools are not in the flow of email, they cannot stop zero-day threats before they reach your people's inboxes.

### Detect Known and Unknown Threats Using Sophisticated, Adaptable Techniques

TAP inspects the entire attack chain using static and dynamic techniques to continually adapt and detect new attack patterns. We analyze potential threats in several stages using multiple approaches to examine behavior, code and protocol to detect threats early in the attack chain. TAP uses unique features, such as multiple machine learning engines and predictive analysis, to identify and sandbox suspicious URLs before users can click on them.



## Respond with End-to-End Insight and Superior Security Intelligence

We are the only cybersecurity company with threat intelligence spanning email, network, mobile apps, cloud apps and social media. Because we can attribute the majority of malicious traffic to attack campaigns, you can then easily discriminate between broad-spectrum attacks and threats targeted at executives or other employees.

We incorporate insight from Proofpoint Emerging Threats (ET) Intelligence, the timeliest and most accurate source of threat intelligence available today. ET Intelligence is the gold standard for threat researchers, offering fully verified threat intelligence beyond domains and IP addresses.

Knowing who the most attacked people are in your organization is critical to providing the highest level of security. The Proofpoint Attack Index within TAP helps identify targeted people and surface targeted or other interesting threats from the noise of daily threat activity. You can then prioritize the most effective way to resolve the threat and receive reporting and metrics to assess and understand the individual and overall risk to your people. And by identifying

your most attacked people, you can provide them with additional adaptive controls, such as isolating their URL clicks in email. For others, you can isolate just the riskiest of their URL clicks.

TAP includes a web-based graphical dashboard that provides data at organizational, threat and user levels to help you prioritize alerts and act on them. You get detailed forensic information on individual threats and campaigns in real time.

## Deploy Quickly and Protect Everywhere To Get Immediate Value

To protect your people, today's defenses must work where they do—at the pace they do. The TAP architecture enables you to deploy quickly and derive value right away. You can protect hundreds of thousands of users in days—not weeks or months. TAP protects your users on any network or device, regardless of where and how they check their email or access their cloud apps. It is easily configured as part of the broader Proofpoint email security platform, which you can deploy as a cloud service, virtual appliance or hardware appliance. We also use the cloud to instantly update our software every day to quickly incorporate new features and help you stay ahead of attackers.

## LEARN MORE

For more information, visit [proofpoint.com](http://proofpoint.com).

### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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](http://www.proofpoint.com).

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. [Proofpoint.com](http://Proofpoint.com)