proofpoint.

TARGETED ATTACK PROTECTION

PROTECT YOUR PEOPLE FROM ADVANCED THREATS IN EMAIL AND CLOUD APPS

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.

Attackers exploit the tools your people use, especially email and cloud apps. They trick people as a way of compromising your endpoints, stealing your credentials and accessing your data. While more than 90% of targeted attacks arrive through email, cloud risks are also rapidly increasing.

Traditional cybersecurity solutions, using legacy techniques such as reputation and signatures, are no longer enough to identify and stop malicious email. Malware techniques are quickly evolving. To keep pace, so must your defenses.

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. No cybersecurity defense is better at stopping today's advanced threats.

TAP provides first and second lines of defense at the email gateway and cloud apps with three key components:

Attachment Defense: TAP can open and sandbox many Microsoft Office and PDF files—even those that attackers have locked with a password or compressed multiple times. Safe emails are delivered, malicious emails are blocked and threats quarantined.

URL Defense: TAP inspects URLs that link to malicious web pages and attachments. Messages containing malicious URLs are immediately quarantined. TAP rewrites all other URLs to track and block clicks. Based on the verdict from sandbox inspection, TAP redirects clicks to the original web page or a customizable block page that prevents access to unsafe sites.

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

When used together, these defenses provide a unique people-centric view into email and cloud attacks that may have led to credential theft.

KEY BENEFITS

- Stop threats before they reach the inbox
- Detect known and unknown threats in email
- Respond with end-to-end insight
- Deploy quickly and protect everywhere
- Focus resources on your most attacked people
- Identify and highlight targeted VIPs

STOP THREATS BEFORE THEY REACH YOUR PEOPLE

TAP is built on our next-generation security platform, which offers clear visibility into all email communications. This means that TAP has 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 advanced 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. Because prevention is critical, our solutions are designed to detect threats as early as possible 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.

Some threats, such as credential phishing and email fraud, do not use malware or leave obvious traces. TAP doesn't just detect malware and non-malware threats. It also learns from them. We observe the patterns, tactics, behaviors and tools of each attack, making the next one easier to catch.

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. Our threat graph of community-based

intelligence contains more than 600 billion data points to correlate attack campaigns across diverse industries and geographies. 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.

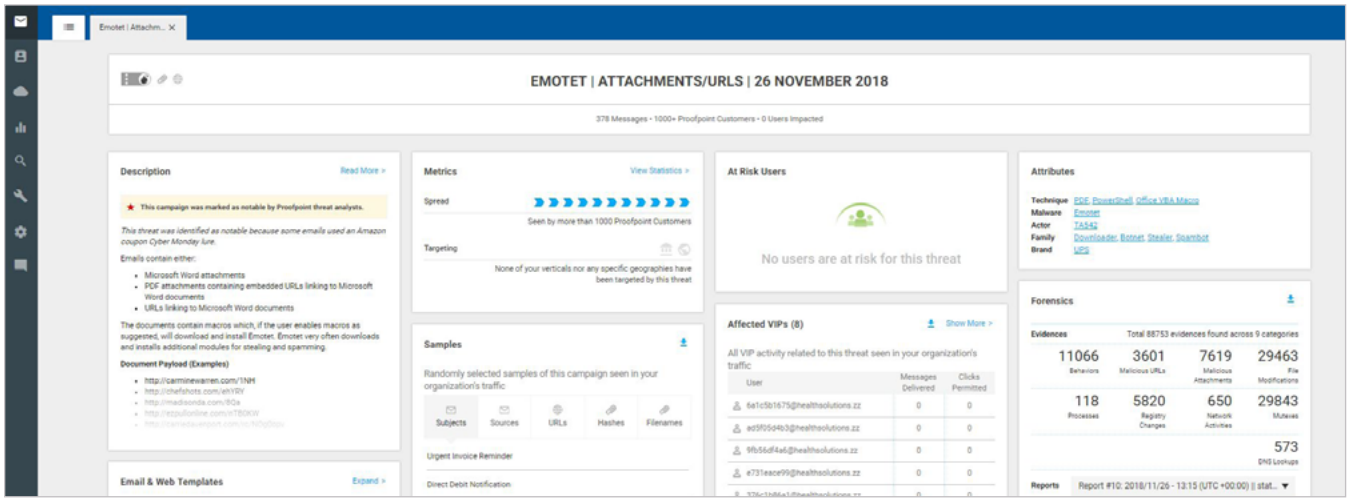
We incorporate insight from Proofpoint Emerging Threats (ET) Intelligence, the timeliest and most accurate source of threat intelligence available today. ET Intelligence is the gold standard for threat researchers, offering fully verified threat intelligence beyond domains and IP addresses.

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 threat activity that you see every day. The Attack Index is composed of four key factors: threat actor sophistication, spread and focus of attack targeting, type of attack and overall attack volume. 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 your people face.

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.

We help answer critical questions, such as:

- What is the threat? Is it part of an attack campaign?
- Who is being targeted? Are any VIPs at risk?
- Who are your most targeted people? What threats are being used to attack them?
- How many messages have been blocked or clicked? And by which users?
- How can I identify whether an endpoint has been compromised?
- What are the potential indicators of compromise (IoCs) from the threat?
- Is the attack targeting a specific region or industry?



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.

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.