Proofpoint Targeted Attack Protection

Gain advanced threat protection and visibility

Key Benefits

- Detect, analyze and block advanced threats before they reach your inbox
- Gain unique insights to identify your Very Attacked People™ and overall security risk
- Leverage Proofpoint Threat Intelligence to protect against threats and receive detailed forensics on attacks
- Provide adaptive security controls through URL isolation and security awareness training
- Enable VAPs to confidently browse unknown websites through corporate email while protecting them from URL and web-based attacks. This feature is part of our solution bundles

More than 90% of attacks start with email[1]—and these threats are always evolving. Proofpoint Targeted Attack Protection (TAP) provides an innovative approach to detect, analyze and block advanced threats targeting your people. It also offers unique visibility into these threats so you can optimize your response.

TAP stops both known and never-before-seen email attacks. It detects and blocks polymorphic malware, weaponized documents, credential phishing and other advanced threats. It monitors cloud app activity to identify suspicious logins, broad file sharing, risky third-party applications and more. And it gives you the insight you need to identify and protect your most targeted people.

Defend Against BEC, URL-, Attachment- and Cloud-Based Threats

TAP uses both static and dynamic techniques to continually detect and adapt to new attack patterns. We analyze potential threats using multiple approaches that examine behavior, code and protocol. This helps detect threats early in the attack chain, potentially before they do damage.

TAP defends against business email compromise (BEC) and supplier account compromise threats. These types of attacks often do not have malicious payloads, so identification requires sophisticated detection techniques that go beyond sandboxing. Proofpoint Nexus Threat Graph — our threat intelligence — powers TAP. It collects, analyzes and correlates a trillion data points across email, cloud, network, endpoint and social networking sources. The Advanced BEC Defense engine is built and trained on rich threat data. It learns in real time and can quickly react to changes in the threat landscape.

1 Verizon, "Cost of a Data Breach Investigations Report." July 2019

We use sandboxing to study a wide variety of attacks. Attacks include the use of malicious attachments and URLs to install malware or trick users into sharing sensitive information. We also leverage analyst-assisted execution to maximize detection and intelligence extraction.

To help you better understand cloud attacks, TAP detects threats and risks in cloud apps and connects them to credential theft and other email attacks. Our technology doesn't just detect threats, it also applies machine learning to observe the patterns, behaviors and techniques used in each attack. Armed with that insight, TAP learns and adapts so it can catch future attacks more quickly.

Advanced BEC Defense

Advanced BEC Defense protects against BEC and supplier account compromise threats. It conducts a comprehensive analysis of every detail within a message, including:

- Header forensics
- Originated IP address
- Sender and recipient relation
- Reputation analysis
- Deep content analysis

Advanced BEC Defense also provides detailed visibility into attacker techniques, threat observations and message samples. It helps you understand how your users are being targeted.

URL Defense

TAP URL Defense provides protection against URL-based email threats, including malware and credential phishing. It provides unique predictive analysis that identifies and sandboxes suspicious URLs based on email traffic patterns. All URLs that reach inboxes are transparently rewritten. This protects users on any device or network. Real-time sandboxing is also performed every time a URL is clicked.

Attachment Defense

TAP Attachment Defense delivers protection against known and unknown threats that are delivered through attachments. It protects against threats hidden in a large range of file types, password-protected documents, attachments with embedded URLs and Zip files.

TAP Account Takeover

TAP Account Takeover provides visibility and defenses across the entire email account takeover attack chain. Its graphical attack sequence timeline helps speed up investigations of compromised accounts and suspicious activities. You can see what kind of mail threats target accounts. If an attacker accesses an account, you can take corrective action to protect it. It also remediates malicious mailbox rule changes, abused third party apps and data exfiltration across email and cloud environments. TAP Account Takeover is compatible with Microsoft 365, Google Workspace or Okta.

SaaS Defense

TAP SaaS Defense brings to light suspicious login activity. This includes unusual login locations and excessive login attempts and failures. It also flags when there are too many connections from known malicious IP addresses. You get visibility into internal and external high-exposure file sharing events. This lets you see when sensitive data could have been leaked during the previous 30 days. TAP SaaS Defense detects critical and high-severity third-party applications being used by your organization. It is compatible with Microsoft 365 or Google Workspace.

Isolation for VAPs

TAP URL Isolation for VAPs is designed to protect your Very Attacked People™ (VAPs) from URL and web-based attacks. It provides real-time phish detection and helps protect users and permitted clicks against unknown and risky URLs. Using our isolated browser solution, VAPs can confidently access websites from their corporate email knowing that the organization is secure.

Gain Deep Insight and Visibility Into Threats and Targets

Proofpoint has visibility into multiple threat vectors, such as email, cloud, network and social media. We derive this visibility from our global base of over 115,000 customers. Our gathered data is passed to Proofpoint Nexus Threat Graph. Here it is correlated together for increased visibility into the threat landscape. You can see this and gather other important insights with the TAP Threat Insight Dashboard, which provides detailed real-time information on threats and campaigns. You can understand both widespread and targeted attacks with this data. Details about threats, like impacted users, attack screenshots and in-depth forensics, are available.

Very Attacked People

The Proofpoint Attack Index helps identify your VAPs so your security teams can identify the top targets in your organization. The index is a weighted composite score of all threats sent to an individual in your organization. It scores threats on a scale of 0 to 1,000 based on threat sophistication, spread and focus of attack targeting, type of attack and overall attack volume. By better understanding your VAPs, you can prioritize the most effective ways to stop threats.

Company-level Attack Index

The Attack Index can also be applied at the company level and compared to other industries to give you an overall company-risk comparison. This report helps your CISO and security team understand how attacks on your company compare to attacks on peers across industries. It covers frequency of attacks and types of threats. With this insight, you can prioritize security controls based on your unique attack landscape.

Threat actor insight

As people continue to be the target, it becomes ever more critical for customers to have a holistic picture of the threat actors executing the attacks. Our threat researchers have been curating data around actors for many years, and this intelligence is manifested in the TAP Dashboard. Customers can see which threat actors are targeting them, who is being targeted, the tactics and techniques being used and any trends forming over time from the threat actors. This helps organizations prioritize additional security and remediation controls to better protect their people.

LEARN MORE

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