Proofpoint Threat Response Auto-Pull

Automatically quarantine malicious email post-delivery

Key Benefits

- Automatically quarantine malicious emails that bypass perimeter solutions
- Exponentially reduce time for security and messaging teams when going through mail security orchestration and response
- Leverage Proofpoint Threat Intelligence for message classification
- Automatically monitor abuse mailbox for threats
- Quarantine messages forwarded to individuals or distribution lists
- Track down partially reported phishing campaigns and remove wasted time from misreported messages

Proofpoint Threat Response Auto-Pull (TRAP) enables your messaging and security administrators to streamline the email incident response process. When malicious emails are detected, TRAP will analyze and automatically remove them. It also moves to quarantine unwanted emails that have reached user inboxes. Proofpoint TRAP reduces the time that your security and messaging teams need to clean up email.

Email is the No. 1 attack vector. It is responsible for more than 90% of data breaches. As email-based threats have become more advanced, organizations are facing a growing number of malicious messages. These emails may contain phishing links that are activated after delivery or they might use advanced techniques to evade detection, which can lead to false negatives and allow the emails to reach end users. To reduce the risk of threats and minimize the potential impact of a breach, email security teams must analyze and clean up these malicious emails. Handling a small number of them might not be too time-consuming, but incidents that involve hundreds or thousands of malicious emails can quickly overwhelm security teams and become too tedious to manage.

Forward-Following and Distribution List Expansion

TRAP helps administrators handle malicious or unwanted emails that are forwarded to others. It has built-in logic that can detect when a message is forwarded or sent to a distribution list. And it automatically expands the list of recipients to locate and retract the message. Automatically handling the process of retracting forwarded emails can save administrators a lot of time and effort.

Flexible Deployment Options

TRAP can be deployed in the cloud, hosted by Proofpoint. Or it can be deployed on-premises through VMware and AWS. This flexibility allows TRAP to be used with various email systems, such as Microsoft 365 or Exchange and Google Workspaces. The more modern and convenient option is cloud deployment. It requires less effort to set up and it saves on maintenance because of its automated software updates.

Out-Of-Band Email Management

TRAP lets you quarantine emails that may be security threats or violate company policy. It does this using CSV files, Proofpoint Smart Search or manual incident reports. Provide a few key pieces of information, and TRAP will quickly remove the specified emails from users' mailboxes. It also provides an activity list that shows who read the emails as well as the status of any recall attempts. This helps to ensure that potentially harmful or inappropriate emails are quickly identified and removed from circulation.

Cross-Vector Intelligence-Sharing With the Proofpoint Nexus Threat Graph

The Proofpoint Nexus Threat Graph aggregates and correlates threat data from multiple sources, like email, cloud, network and social media. It provides real-time protection and response for all Proofpoint products. And it is integrated into the Proofpoint platform. So, it requires no additional installation or management.

When you become a part of this network, you can access the following benefits:

- Real-time community threat intelligence from more than 115,000 customers
- Multivector visibility across email, cloud, network and social media
- Information on more than 100 tracked threat actors to understand their motives and tactics

TRAP uses the intelligence from the Nexus Threat Graph to associate recipients with user identities. It also uncovers associated campaigns and identifies IP addresses and domains used in attacks. Based on this information, TRAP can take automated actions against targeted users who belong to specific departments or groups with special permissions. When we detect malicious emails with links, attachments or suspect IPs at a customer site, we share this information with our entire customer base for future protection and to quarantine any delivered messages in the user's inbox.

Enhanced Triage

TRAP's ability to investigate URLs safely using Proofpoint Browser Isolation technology enhances the incident triage process for analysts. The technology allows the analysts to assess the contents of a URL without exposing the organization to risk. This helps them to quickly and accurately evaluate incidents that involve URLs, which allows them to take appropriate action to protect the organization.

Closed-Loop Email Analysis and Response

Closed-Loop Email Analysis and Response (CLEAR) helps users quickly identify and address potentially malicious emails. It combines the capabilities of PhishAlarm, PhishAlarm Analyzer and TRAP to provide a fast and effective response to reported messages. With CLEAR, reported emails are sent to an abuse mailbox. They are then automatically analyzed against Proofpoint Threat Intelligence and other sources to see if they contain malicious content. If a match is found, the message is removed from the recipient's inbox and quarantined. This helps to prevent active attacks and protect your organization. Informed employees are an important line of defense against cyber threats. And CLEAR helps to empower them to report and address potential threats in just minutes.

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 75 percent of the Fortune 100, 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**.