proofpoint.

DATA SHEET

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 a malicious email is detected, TRAP will analyse emails and automatically remove any malicious messages. It also moves unwanted emails to quarantine that have reached user inboxes. With TRAP, you get a powerful solution that exponentially reduces the time needed for your security and messaging teams to clean up email.

Over 90% of breaches start with an email, the number one attack vector. As email threats continue to evolve, organisations will be exposed to more malicious messages. Malicious emails can contain phishing links that can be poisoned after delivery. Or it can use evasion techniques, which lead to false negatives that deliver malicious emails to users. Email security teams are often tasked with email analysis and cleaning up to reduce threat exposure and limit potential damages. While email quarantining one message may not require much work and a mere 10 to 15 minutes each, situations where ten emails or more are involved can become tedious, with time requirements quickly adding up.

Cross-vector intelligence sharing with the Proofpoint Nexus Threat Graph

The Proofpoint Nexus Threat Graph provides industry-leading aggregation and correlation of threat data across email, cloud, network and social media. It powers real-time threat protection and response across your Proofpoint products. As part of the Proofpoint platform, there is nothing to install, deploy or manage. You benefit from becoming part of this network and staying ahead of the ever-evolving threat landscape by getting:

- Real-time community threat intelligence from over 115,000 customers.
- Multi-vector visibility from email, cloud, network and social media
- More than 100 threat actors tracked to understand motives and tactics used for enhanced protection

TRAP leverages the Nexus Threat Graph intelligence to build associations between recipients and user identities, revealing associated campaigns, and even surfacing IP addresses and domains in the attack. Based on that, TRAP takes automated actions based on targeted users who belong to specific departments or groups with special permissions.

Also, if we detect an email that contains malicious links, attachments or suspect IPs at a customer site, we will share this information across our entire customer base for future pre-delivery protection. We remove and quarantine any messages that have been delivered to the users inbox.

Identify and reduce phishing risk with CLEAR

An informed employee can be your last line of defence against a cyber attack. With Closed-Loop Email Analysis and Response (CLEAR), the cycle of reporting, analysing and remediating potentially malicious emails goes from days to just minutes. Enriched with Proofpoint Threat Intelligence, CLEAR stops active attacks in their tracks with just a click. And your security team can save time and effort by automatically quarantining malicious messages.

With CLEAR, you get a complete solution. It blends the capabilities of PhishAlarm, the email reporting button, PhishAlarm Analyzer, which categorises and prioritises using Proofpoint Threat Intelligence, and TRAP, which provides message enrichment and automatic remediation of malicious messages.

Reported messages are sent to an abuse mailbox to take advantage of CLEAR and are monitored and processed in the same way by TRAP. Then they are further analysed against Proofpoint Threat Intelligence and third-party intelligences to determine if any of the content matches malicious markers. And messages are automatically pulled from the recipient's inbox.

Out-of-band email management

TRAP also leverages CSV files and Proofpoint SmartSearch. You can upload SmartSearch results, CSV files or use manual incidents with a few key pieces of information to initiate an email quarantine action of one or thousands of emails. In moments, security threats—and policy violating emails—can be pulled out of mailboxes. And you get an activity list showing who read the emails and the success or failure of the attempt to recall them.

Auto-quarantine forwarded messages

Malicious and unwanted emails may be forwarded to other individuals, departments or distribution lists. Attempting to retract those emails after delivery has been a sore point for many administrators. TRAP addresses this situation with built-in business logic and intelligence that understands when messages are forwarded or sent to distribution lists. It then automatically expands and follows the wide fan out of recipients to find and retract those messages. This saves you time and frustration.

Enhanced triage

TRAP provides SOC analysts an enhanced triage process with incidents containing URLs. URLs can be investigated safely by leveraging Proofpoint Browser Isolation technology. This will allow analysts to arrive at an assessment of what the contents of the URL contain while preventing the organisation from risk.

LEARN MORE

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