# 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

Over 90% of breaches start with an email, the No. 1 attack vector. As email threats continue to evolve, organizations will be exposed to more malicious messages. Malicious emails can contain phishing links that can be poisoned after delivery or use evasion techniques which lead to false negatives and delivered to end 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.

### Automatically Quarantine Malicious Email

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 analyze emails and automatically remove any malicious messages. It also moves unwanted emails to quarantine that have reached end 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.

### Leverage Enterprise-Class Threat Intelligence

Proofpoint Threat Intelligence spans across many threat vectors; email, social, mobile, cloud and network. This gives us unique visibility into the latest threats and tactics the threat actors are using today. With TRAP, you can take advantage of leveraging Proofpoint Threat Intelligence as well as third-party threat intelligence such as STIX/TAXII feeds, WHOIS, VirusTotal, Soltra and MaxMind. All of this helps you understand the “who, what and where” of attacks, quickly triage and prioritize incoming events, and off-load repetitive tasks.

After an email is detected, it is enriched with the above-mentioned intelligences. And associations between recipients and user identities are built, related campaigns are revealed, and the IP addresses and domains in the attack are even surfaced. This gives you the most accurate classification on messages. And it allows your security teams to focus on other tasks and not have to manually investigate each detected message.

## Identify and Reduce Phishing Risk with CLEAR

An informed employee can be your last line of defense against a cyber attack. With Closed-Loop Email Analysis and Response (CLEAR), the cycle of reporting, analyzing 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 categorizes and prioritizes 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 analyzed 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. Users 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.

## LEARN MORE

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