Closed-Loop Email Analysis and Response

Identify and Reduce Phishing Risk

PRODUCTS

- PhishAlarm
- PhishAlarm Analyzer
- Threat Response Auto-Pull (TRAP)

KEY BENEFITS

- Find malicious messages and stop attacks that target your organization.
- Users can report suspicious messages with a single click—and these messages are then automatically analyzed.
- Save time with automation. Pull malicious messages from the sender's mailbox. And track messages forwarded or sent to distribution lists to retract and quarantine.
- Use exclusive Proofpoint Threat Intelligence to enrich messages, and streamline the remediation process—right out of the box.
- Reduce abuse mailbox clutter so your response teams can stay focused on the messages that are likely to be malicious.
- Empower your users to be your last line of defense.

Over 90% of breaches start with an email, the No. 1 attack vector. As email threats continue to evolve, end users will be exposed to more malicious messages. Many organizations train their end users to identify and report suspicious email activity. But sometimes end users report harmless and bulk email because they think they are malicious. This creates false positives for the security team. And it uses up the team's limited time. Security teams have to prioritize and sift through all reported messages to identify and remediate truly malicious threats. Proofpoint Closed-Loop Email Analysis and Response (CLEAR) streamlines email threat reporting, analysis, and remediation. The result? Your phishing risk is reduced.

Streamline Reporting, Analysis, and Remediation of Phishing Emails

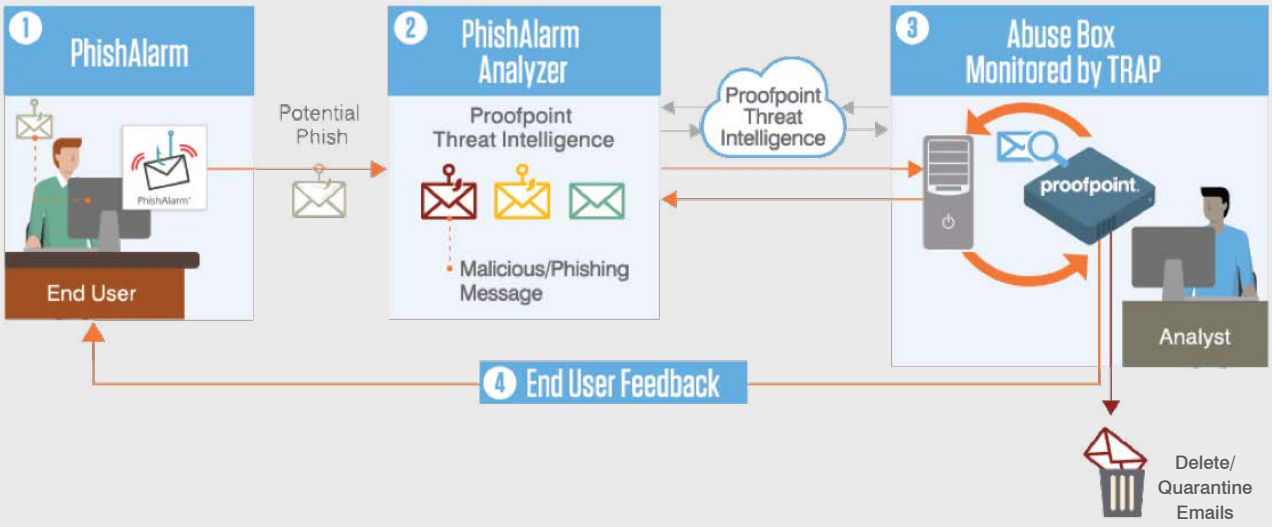
An informed employee can be your last line of defense against a cyber attack. CLEAR reduces time spent on reporting, analyzing and remediating potentially malicious emails from days to minutes. Enriched with our world-class threat intelligence, CLEAR stops active attacks in their tracks with one click. And it saves your security team time and effort by automatically quarantining these malicious messages.

CLEAR is a complete solution that blends these capabilities:

- PhishAlarm, the email reporting button
- PhishAlarm Analyzer, which uses Proofpoint Threat Intelligence to categorize and prioritize email threats
- Threat Response Auto-Pull (TRAP) for message enrichment and automatic remediation

Leverage Enterprise-Class Threat Intelligence

Proofpoint Threat Intelligence spans many threat vectors: email, social, mobile, cloud and network. This gives us unique visibility into the latest threats and tactics that threat actors are using today. With CLEAR, you can leverage Proofpoint Threat Intelligence. CLEAR integrates our proprietary URL and attachment sandboxing technology and our unique email classification engines. So after an end user reports a message, it is automatically processed, analyzed and enriched by Proofpoint Threat Intelligence. This gives you the most accurate classification on reported messages. Your security team no longer has to



CLEAR Workflow

manually investigate each reported message. Instead, they can focus on other tasks.

Track Down Partially Reported Phishing Campaigns

Some end users do not report malicious messages at all. This means a phishing campaign is only partially identified. CLEAR inspects, scores and categorizes each reported message by leveraging Proofpoint Threat Intelligence stack and sandboxing environment. This score helps TRAP prioritize and process messages. TRAP then uses security automation and orchestration to automatically locate other instances of that malicious email across your enterprise.* TRAP continually checks the abuse mailbox where suspicious emails are reported. It retracts and quarantines all malicious messages from users' inboxes after they are delivered. This helps identify a specific phishing campaign that is targeting your organization.

Eliminate Time Wasted on Misreported Messages

Sometimes end users will report clean and bulk email because they think they are malicious. When they do that, they create false positives for the security team. This wastes your team's precious time. CLEAR identifies most bulk and clean messages. This automatically removes the burden from your security team. They no longer have to look into them, since CLEAR automatically resolves these incidents. This closes the loop for harmless emails.

Reported messages marked for "Manual Review" go to the Proofpoint Threat Operation Center for deeper analysis. And they are then scored, prioritized and handled based on this analysis.

Close the Email Reporting Loop

CLEAR provides users with feedback on all messages they report, whether they are malicious, scored as bulk, or clean. This process closes the email reporting loop. Users get the reinforcement they need to continue to report messages. And your organization stays secure.

For more information, visit proofpoint.com/us/products/threat-response-auto-pull or contact your Proofpoint Sales Representative.

* Requires Proofpoint Targeted Attack Protection to locate all instances of malicious emails across your enterprise.

LEARN MORE

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