

# PROOFPOINT THREAT RESPONSE AUTO-PULL

## AUTOMATICALLY PULL DELIVERED MALICIOUS EMAIL INTO QUARANTINE

### KEY BENEFITS

- Reduce the time to quarantine and contain email threats
- Reduce exposure time to malicious emails
- Quarantine messages forwarded to distribution lists or individuals
- Receive an auditable history of response actions to boost the ROI of your existing infrastructure
- Reduce dependency on custom-coded software
- Receive email notifications for incident changes or quarantine confirmation
- Set flexible notification content for easy integration into ticketing systems
- Automatically monitor and check abuse mailbox messages for threats
- Restore quarantined messages via 'undo'
- Clean up groups of messages using CSV files or SmartSearch results

Proofpoint Threat Response™ is the first threat management platform to extend orchestration and automation to include the capability to retract malicious emails that were delivered to users' inboxes. Threat Response Auto-Pull is an entry level version of the platform that moves malicious email out of users' hands and implements additional business logic to find and remove internal copies of that messages that were forwarded.

At many organisations, security incident response is a slow, labor-intensive process. Addressing email security incidents can take hours or days as manual email clean-up can be a chore. Dealing with delivered email with malware, bad URLs, or credential phishes involves many steps, including:

- Connecting an email address to an internal identity
- Searching and finding selected malicious messages on the server
- Removing a malicious message out of a user's inbox or other folders
- Identifying which malicious messages were forwarded and moving those to quarantine

Repeating these tasks for every email incident can take hours per day and can overwhelm already stretched security and messaging teams.

### EMAIL CLEANING "GOTCHAS"

Email cleanup for malicious messages is often a manual process that starts with an alert or complaint that a malicious email got through.

On the surface, resolving an email incident seems as easy as looking in an inbox and deleting a message, but that could be a costly assumption. Common missteps in the cleanup stem from an over simplification of the process and ignores the volume of messages and anything beyond a basic case. Other important considerations include:

- Is the email only in the inbox or was it moved to another folder?
- Should you check other folders for copies of the message?
- Has the message been internally forwarded? If so to whom and how many copies?
- Is there an audit trail or record of all the actions taken?

There are other variables which impact how successful an email cleanup can be, which has led to DIY and homegrown email cleanup scripts. These also pose their own risks.

### PERILS OF DIY AND CUSTOM CODE

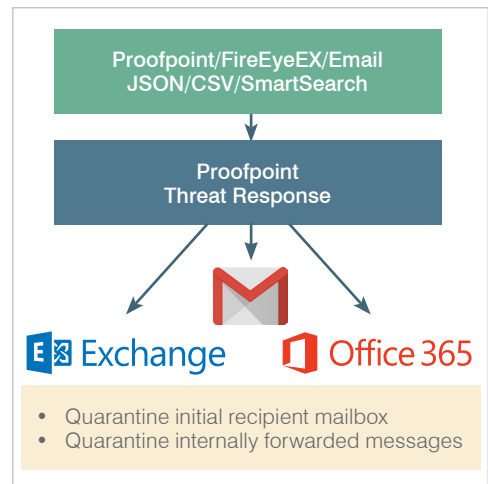
Creating and running custom code to cleanup email has been the defacto solution for malicious email that was delivered.

There is nothing inherently wrong with this path, however, building and running custom code represents a commitment that brings with it standard software development questions:

- Is there a spec or is the custom code performing only one function and doesn't need a full specification?
- How is the script maintained? Is there an owner who can respond to fix an issue? What happens when the developer leaves?
- If the script acts against 3rd party products, who oversees addressing product versioning, testing, interface or API changes of the 3rd party products?

Aside from those obvious technical concerns the business side requires that custom code deliver against business logic and visibility goals. These often include:

- Monitoring ongoing operation of the code
- Measuring or tracking the effectiveness of the code
- Assurance that all malicious versions of the message were handled, even forwarded ones



### CONSIDER THREAT RESPONSE AUTO-PULL

Threat Response Auto-Pull is an entry level version of Threat Response that delivers the Email Quarantine function when connected to Proofpoint Targeted Attack Protection (TAP) and either O365 email or Exchange on prem. TR Auto-Pull also accepts FireEye EX CSV files, SmartSearch, and JSON alerts.

The use case is simple—when malicious email is detected, detecting systems send an alert to Threat Response with information about the message. Threat Response then goes into Exchange, Office 365, and/or Gmail to move the message into quarantine. Auto-Pull will also then look for forwarded copies of the message and distribution list recipients of the message in other mailboxes on the same server and move those to a limited access quarantine as well.

### INTEGRATIONS BUILT-IN

Threat Response Auto-Pull includes adapters to connect Exchange, Office 365, Gmail, CSV, SmartSearch, TAP, FireEye EX, and JSON sources in minutes, so no additional systems or connectors need to be purchased. Admins only need the appropriate credentials, for Exchange and O365 for email retraction. In addition, Threat Response Auto-Pull will monitor abuse mailboxes and automatically check messages sent there for matches against intelligence and reputation.

### AUTO-PULL OR FULL THREAT RESPONSE

While Auto-Pull addresses email security incidents, security professionals should also consider full Threat Response which goes beyond the email quarantine with key capabilities worth considering:

- Security orchestration and automation of incident response
- Adding context and intelligence to shortcut incident triage
- Collecting and verifying endpoint forensics against sandbox forensics
- Accepting and applying 3rd party intelligence against all incidents
- Quarantining and containing threats via Firewalls, proxies, and AD
- Real-time reporting against campaigns, users, incidents, threats, and targets

---

**“...it deployed, integrated with TAP and AD, and already auto-purging messages within a couple hours”**

**Confidential Customer, Healthcare**

---

### SUMMARY

Threat Response Auto-Pull can provide proactive, automated, quarantine and containment for malicious emails that were delivered to the inbox, including the removal of internally forwarded messages. Security professionals should consider full Threat Response to gain time, efficiency, and other capabilities beyond email incident handling.

#### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.