SOLUTION BRIEF

RESOLVING TAP ALERTS

EFFICIENT RESPONSE WITH THREAT RESPONSE AUTO-PULL

The visibility you get with Proofpoint Targeted Attack Protection (TAP) is critical to triaging security incidents and resolving them. But it’s only the first step in an effective response. With Proofpoint Threat Response Auto-Pull (TRAP), you can quickly contain, quarantine and clean up malicious email before users have a chance to open it.

Email is a business necessity. It’s also today’s top threat vector. TAP detects malicious emails quickly. And when attackers use evasion techniques—such as turning URLs malicious after they’ve been delivered—TAP can still detect the latent threat.

TRAP processes TAP alerts to quickly and easily retract the malicious email and any internally forwarded copies. It also provides a documentation trail of all the protective actions attempted and the results.

RESOLVING EMAIL THREATS

TAP notifies the administrator when it detects email threats through static, dynamic, or predictive analysis. These alerts ensure that you know about malicious messages. But as long as the message is accessible in an end-user’s mailbox, it is a breach waiting to happen—a credential-stealing URL waiting to be clicked or malware waiting to be opened. Responding to these threats can be complex process at a time when every second counts.

To properly mitigate the situation, you need to:

- Prioritize a response based on the recipient, threat information, and situation
- Locate the message using search or message markers for the user, sender and others
- Determine the spread and scope, including whether the email sent to distribution lists or forwarded
- Quarantine the emails
- Document all the mitigation steps taken and their outcome

PRIORITIZE
a response based on the recipient, threat information, and situation

LOCATE
the message using search or message markers for the user, sender and others

DETERMINE
the spread and scope, including whether the email sent to distribution lists or forwarded

QUARANTINE
the emails

DOCUMENT
all the mitigation steps taken and their outcome

WHY DOES IT MATTER?

Attackers know that email is often the easiest way to store files. When you can’t find where you’ve saved a file, a quick email search in email might pull it up — with a malicious URL or attachment included. If not quarantined or deleted, they are ticking time bombs that could result in stolen credentials, malware infections, or data theft.

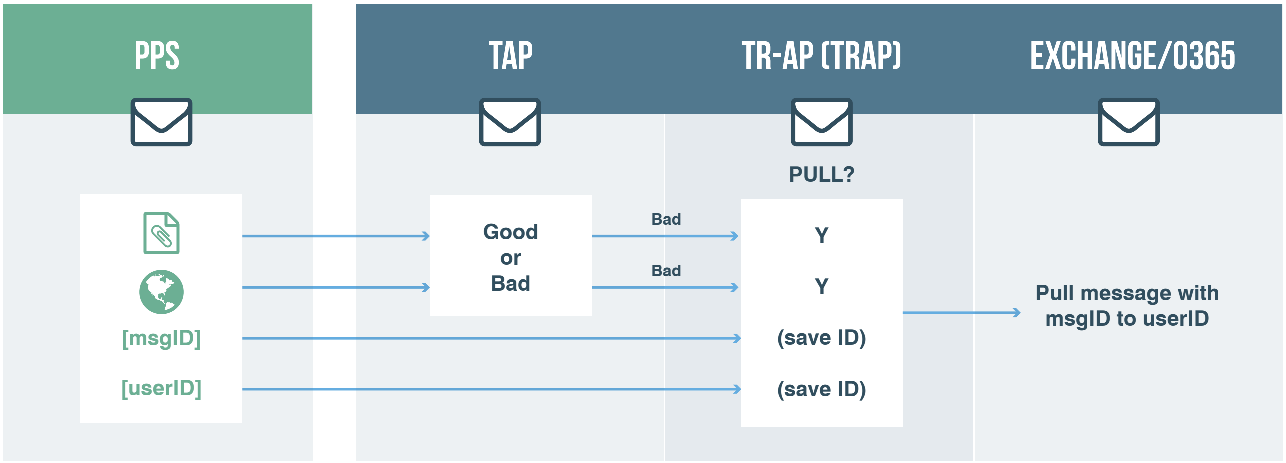
Responding to an already-delivered threat can be time-consuming no matter what your role within an organization. If your focus is security, you know that malicious email is an ongoing risk that could create even more work if not managed quickly. This includes reimaging desktops and servers, restoring backups, and many other steps to bring systems back online and running. Often, this work can extend even further. You might have to conduct deeper forensic collection and analysis to see whether the risk has become a larger threat. That includes whether an infection has led to privilege escalation, lateral movement, or credential theft.

If your focus is enterprise messaging, you're likely tasked with finding and moving the malicious emails to quarantine. The longer the email is in the system, the more likely it will be forwarded, shared, or clicked. Each time the email is forwarded, more work is required to track them down and move them into quarantine. Not every malicious email results in an infection or credential theft. But every email must be cleaned up or quarantined to reduce the risk to users and corporate assets. With a cleanup time of 10-20 minutes per email, the time cost for mitigating the threat can quickly add up, even when using custom scripts.

RAPID RESPONSE WITH THREAT RESPONSE AUTO-PULL

TRAP is a fast, simple solution to clean up malicious emails identified in TAP security alerts. Integration between TAP and TRAP takes only minutes—and the results are immediate.

TRAP automatically captures TAP alerts. It can automatically (or manually) move the email and any forwarded copies from Exchange or Office 365 inboxes into a quarantine accessible only to administrators. In the automatic setting, emails are typically pulled into quarantine before users have a chance to click on the malicious content.



You can add TRAP to your TAP deployment using credentials from your TAP dashboard and Exchange or Office 365 service accounts. Our customers have reported getting deploying TRAP in production environment in as little as an hour—that's a short time to value.

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.