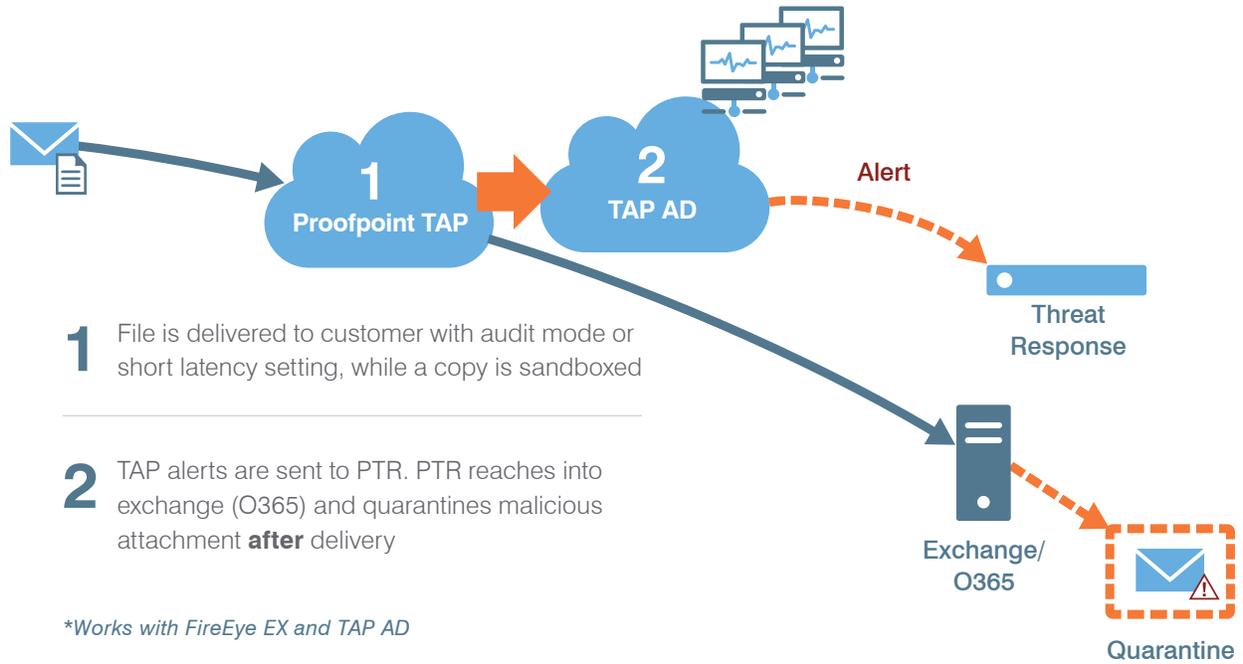


THREAT RESPONSE EMAIL QUARANTINE



THE PROBLEM

Documents are a common, yet critical element in everyday business, but that also means that documents are a potential point of risk for organizations. One obvious risk becomes more visible when documents are exchanged with business partners and customers. Email and email attachments are the method of choice for delivery of business documents, and as such, are equally valuable as a means to attack individuals and their organizations.

USE CASE

Cyber criminals use a variety of tools, technologies, and even cloud services to weaponize files, turning PDFs and office documents into tools in an attack. The weaponized files are sent via SPAM or phishing campaigns with any number of compelling subject lines. A fraction of recipients click and get infected.

Infections occurring through this method are a security issue for the company, but the first line of defense is the Exchange or email administrator. Once a malicious attachment is detected, the email administrator is tasked with finding not only the email message that triggered the alert, but also every other email that may have been delivered in a campaign with the same or similar malicious attachments.

The process of finding, moving, or removing each and every message with a related malicious attachment can easily take one or more hours and can be fraught with errors and often requires double-checking and history documentation.

“My email admin can spend 1 to 3 hours a day cleaning up emails with malicious attachments”

CISO national hotel chain

A BETTER APPROACH

Proofpoint Threat Response Email Quarantine brings smart automation to this scenario. When alerting systems tell Threat Response about a message with a malicious attachment, Threat Response will can automatically, or on-demand, connect to the Exchange server and move the message with malicious attachments into quarantine. Each email quarantine action can also create a task history showing that the protective action was taken.



Email administrators can set their own rules or policies on what happens once these emails are quarantined. Typically, administrators create a policy where the emails are retained for a short period, then automatically deleted. Before deletion, however, administrators can, with caution, retrieve and review the message.

RESULTS

Benefits from applying this technology is immediate:

- The time between the detection of malicious attachments by Proofpoint Targeted Attack Protection Attachment Defense or by FireEye EX and the email quarantine is measured in seconds
- Each quarantine action is automatically documented
- Email administrators can save hours for each incident or attack, and can refocus time on more pressing operational or security issues.

REQUIREMENTS

Threat Response Email Quarantine is included with each Threat Response license in version 2.5 and higher. Connectors to Microsoft Exchange and Office 365 are built-in and require a service account capable with the appropriate administration permissions.

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.