proofpoint

Proofpoint Threat Response

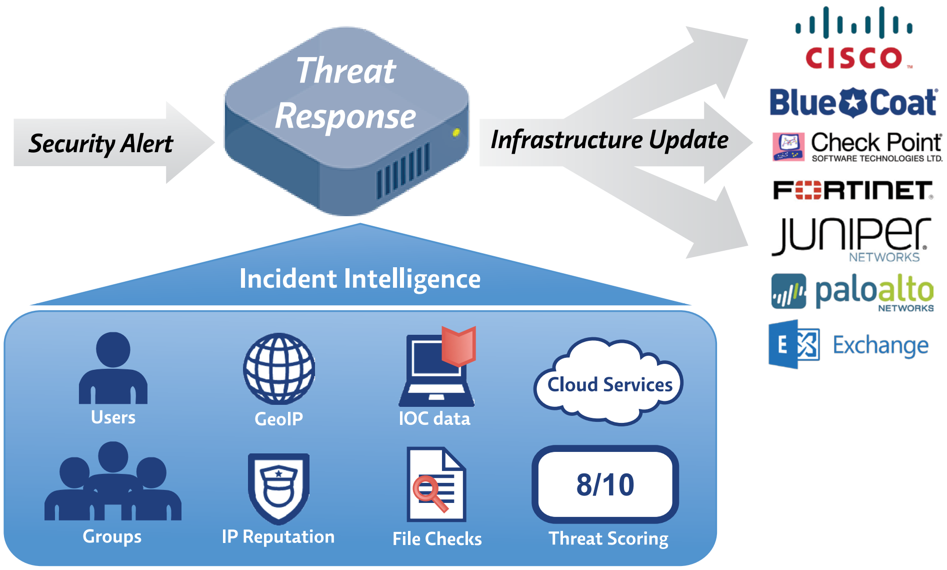
Benefits of Threat Response

- Automated collection of forensic data from suspected systems saves time
- Infection confirmation saves countless hours by comparing system PC data with detection forensics
- Reduced manual collection of data from external devices, intelligence sources, and more
- Visual monitoring of incidents and processed threats
- Consistent analysis insures consistent response
- Integrated views accelerate decisions
- Automatic or push-button quarantine and containment for rapid protection
- Automated lifecycle management of users, hosts, IPs, and URLs on enforcement devices
- Instant audit trail of response actions boosts the ROI of existing infrastructure
- Reduces dependency on custom coded software modules
- Automatic incident creation and incident management tracking reduces manual entry requirements
- Gain up-to-the-minute reports of targeted users, systems, groups, and departments

Prevent security alerts and incidents from escalating into full blown breaches

Summary

Proofpoint Threat Response™ is the first threat management platform to automate incident response by surrounding security alerts with rich contextual data to create actionable intelligence, confirming system infections, and enforcing protections automatically or with the push of a button. By collecting and analyzing security event context, forensics, and intelligence and turning it into automatic or push-button response, the platform closes the gap between detection and protection by containing threats and preventing infections from spreading.



Manual Response Doesn't Scale

At many organizations, security incident response is a slow, labor-intensive process that can take days or weeks depending on the available staff. Time-intensive tasks turn into painful bottlenecks that cannot be avoided:

- Identifying high value targets to prioritize threats
- Identifying high value threats that may be part of larger campaigns or botnets
- Collecting and reviewing endpoint forensics for signs of infection
- Laborious negotiations between security and infrastructure with implementation time for enforcement

Repeating these tasks for each and every incident can translate into more time than a security team has in a day, resulting in skipped steps and cutting corners.

The Incident Response Investigation Time Penalty

Incident response investigation requires information collected from multiple disconnected sources, organizing that data, analyzing it, as well as a series of manual steps to confirm that one or more systems have been compromised. During the investigation phase, valuable data may be stolen from infected systems and attackers may be moving laterally across the network. The quest for a complete investigation often comes at the cost of putting intellectual property at risk.

Modernize Incident Response with Threat Response

Manual Threat Source Collection and Investigation

Incident response has four main areas of focus:

1. Investigate the who, what, and where including targeted users and systems
2. Verify targeted system forensics against sandbox forensic reports
3. Stop the bleeding and IP loss with quarantine and containment actions
4. Track incident response KPIs to insure incidents are not left behind, forgotten, or missed

These focus areas help identify which users are infected, the severity and urgency of a threat, eliminate false positives, and stop the spread of infection and exfiltration of data.

Who, What, and Where with Threat Response

Immediately determine which internal users, departments, and groups are impacted on the network. Knowing "who" means you can prioritize high value targets like the CFO, executive staff, and finance systems over the mailroom.

Besides internal context and intelligence, external factors can provide clues to suspicious IPs or domains in security alerts. These factors are pre-integrated into Threat Response to deliver another level automated analysis for security teams.

Some key external factors to look at:

- Domain Freshness/Recent Registration
- Domain Blacklisting
- IP and URL Reputation
- IP Geolocation

> "Proofpoint closes the gap between threat detection and rapid response by providing our team with deep contextual data for each incident, as well as supporting a variety of network enforcement options. It's our Incident Response analyst 'in a box.' "
>
> *Kevin Moore, Director of Information Technology at Fenwick & West, LLP*

Infection Confirmation by Automatic IOC Verification

Threat Response collects and analyzes endpoint forensics from targeted systems to yield a rich snapshot of Indicators of Compromise (IOC). IOC data includes a list of recent changes on the system (registry and modified files), active processes, and open network connections. This information is compared to changes reported by malware analysis systems and other events that have been received by the system to provide insight into the health of the client.

Another key capability is checking attacked systems for past infections. Each time Threat Response performs an on-demand endpoint collection, it not only checks for IOCs from the current attack, but it also checks for IOCs from past infections that Threat Response has seen at that site. This translates to a quick and effective method to verify that past infections have not perpetuated and spread to the currently targeted system.

Out-of-the-box Integration with Premium Intellience and 3rd Party Tools

Using built-in VirusTotal integration, files can be checked not only once, but over time, to detect how many of 50+ Anti-virus engines detect malicious signatures or properties in files dropped, downloaded, or unpacked during a potential infection.

Premium intelligence feeds built-into Threat Response are automatically checked against each and every domain and IP provided in each security alert and sandbox report. Automatic checking removes hours of tedious work and manual one-by-one searching against intelligence services to find attacking IPs and hosts leveraging know bad sites.

The analysis yields actionable intelligence which enables prioritization, that Threat Response puts into action.

Contain the Threat

To stop the bleeding, changes at the network level can yield immediate protection:

- Stopping infections from spreading from one system to another
- Stopping control signals from reaching malware
- Stopping sensitive data from reaching external sites

Threat Response automates containment using your existing enforcement devices to close the gap between threat detection and protection in real-time.

Specifications

Event Sources:

- Proofpoint Targeted Attack Protection
- FireEye MPS
- Palo Alto Networks WildFire
- HP ArcSight
- QRadar/Juniper STRM
- Splunk
- Cisco FirePOWER NGIPS
- Suricata

Enforcement Devices:

- Cisco ASA
- Palo Alto Networks
- Check Point
- Cisco IOS
- Juniper SRX (JUNOS)
- Fortinet FortiGate
- Blue Coat
- Microsoft Exchange/ O365
- OpenDNS

About Proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com