proofpoint

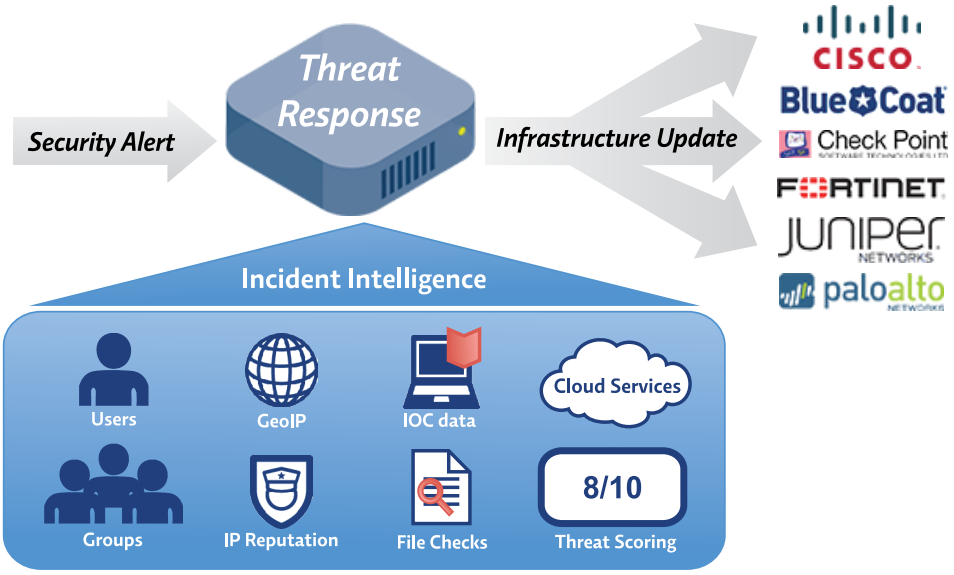
Proofpoint Threat Response

Benefits of Threat Response

- Reduced manual collection of data from external sites
- Automated collection of IOC data from suspected systems saves time and speeds response
- Infection confirmation saves countless hours by comparing system PC data with detection forensics
- Consistent analysis insures consistent response
- Visual monitoring of incidents and processed threats
- Integrated views accelerate decisions
- 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

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 and turning it into rapid response, the platform closes the gap between detection and protection by containing threats and preventing infections from spreading.



Manual Response Doesn't Scale

Increasingly sophisticated security attacks, often in the form of Advanced Persistent Threats (APT), have led enterprises to invest in threat detection solutions that identify security breaches in real-time. Knowing that a breach has occurred is an important step in threat response, however, it is only half the battle.

Once security events have been detected, IT security teams need to decide which events target high value users and systems. These events are urgent and high severity, requiring an immediate response. Some alerts may even be false positives, requiring no action, but how is an IT security team to know the difference?

At many organizations, security incident response is a slow, labor-intensive process that can take days or weeks depending on the available staff.

> "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*

The Incident Response Investigation Time Penalty

Incident response investigation requires information collected from multiple disconnected sources, organizing that data, analyzing it, as well as another series of 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
2. Verify that targeted systems have been compromised
3. Stop the bleeding and IP loss
4. Track incident response KPIs

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

Who, What, and Where with Threat Response

Internally determine which users are impacted on the network, which groups or network segments are affected. Knowing "who" means you can prioritize high value targets like the CFO and finance systems over the mailroom.

Externally determine the source domains and IPs which are hosting the malware, acting as a command and control server, or receiving data.

Some key external factors to look at:

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

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 include 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.

File Analysis

Using VirusTotal, 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.

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

Enforcement Devices:

- Cisco ASA
- Palo Alto Networks
- Check Point
- Cisco IOS
- Juniper SRX (JUNOS)
- Fortinet FortiGate
- Blue Coat

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