proofpoint

PROOFPOINT THREAT RESPONSE

PREVENT SECURITY ALERTS AND INCIDENTS FROM ESCALATING INTO FULL-BLOWN BREACHES

BENEFITS OF THREAT RESPONSE

- Automate collection of forensic data from potentially compromised systems
- Save countless hours confirming infections by comparing system PC data with detection forensics
- Reduce manual collection of data from external devices, intelligence sources and more
- Monitor incidents and processed threats with a visual interface that lets you see what's happening at a glance
- Accelerate response decisions with integrated views of threat activity
- Quarantine and contain threats automatically or at the push of a button for fast protection
- Automatically manage users, hosts, IPs, and URLs on enforcement devices throughout the attack lifecycle to free up staff for other tasks
- Get an auditable history of response actions to boost the ROI of your existing infrastructure
- Reduce dependency on custom-coded software
- Automatically create, track, and manage incident records to reduce the need for manual entry
- Stay current on malicious activity with up-to-the-minute reports of targeted users, systems, groups, and departments

Proofpoint Threat Response™ is the first threat management platform to orchestrate and automate incident response. The platform surrounds security alerts with rich contextual data to help security teams prioritize response actions. It confirms system infections and enforces protections automatically or at the push of a button. And by collecting and analyzing security event context, forensics and intelligence and turning it into automatic or push-button response, it closes the gap between detection and response, multiplying the abilities of your incident response staff.

MANUAL RESPONSE DOESN'T SCALE

At many organizations, security incident response is a slow, labor-intensive process. Responding can take days or weeks depending on your staff. Time-intensive tasks turn into painful bottlenecks, including:

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

Repeating these tasks for every incident can overwhelm already stretched security teams, resulting in skipped steps and cut corners.

The Incident Response Investigation Time Penalty

Incident response investigation requires information from multiple disconnected sources. The information has to be organized and analyzed. Confirming that any systems have been compromised usually requires a series of manual, time-consuming steps. 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 data at risk.

MODERNIZE INCIDENT RESPONSE WITH THREAT RESPONSE

Threat Alert Source Collection and Investigation

Incident response has four main areas of focus:

- Investigate the "who, what, and where" of attacks, including targeted users and systems
- Verify targeted system forensics against sandbox forensic reports
- Stop the bleeding and IP loss with quarantine and containment actions
- Track incident response KPIs to ensure incidents are not missed or forgotten

These focus areas help identify which users are infected and the severity and urgency of a threat. It also helps eliminate false positives and stop the infections from spreading and data from being exfiltrated.

Who, What, and Where with Threat Response

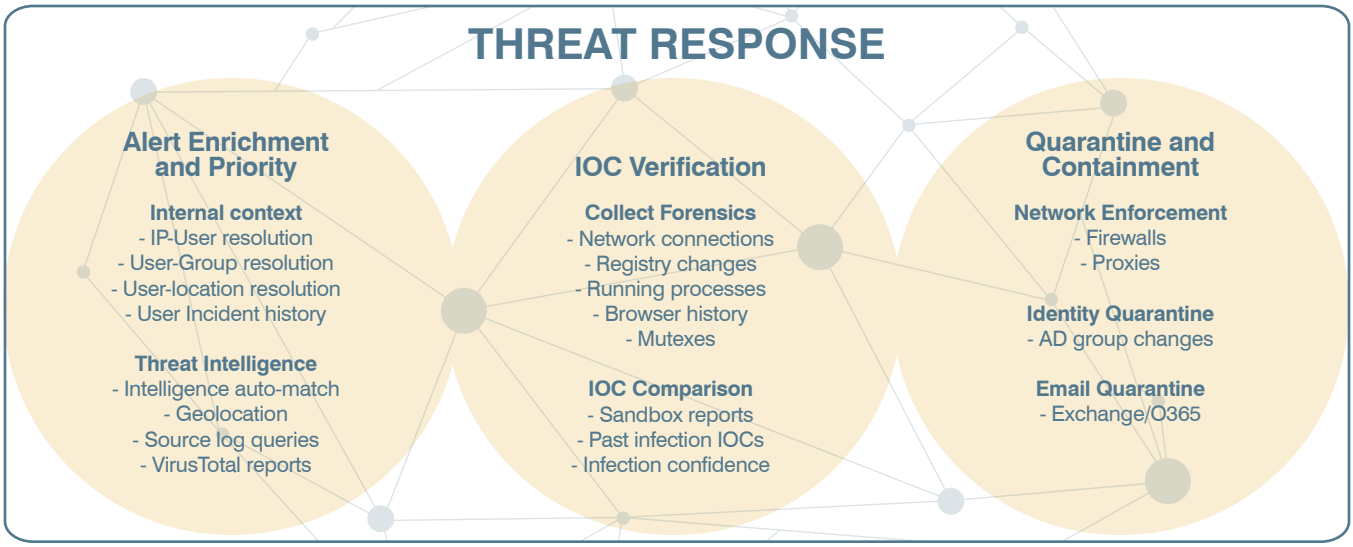
You need to immediately determine which internal users, departments, and groups are affected. Knowing "who" means you can prioritize high-value targets such as the CFO, executive staff and finance systems over the mailroom, for example.

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 further automate analysis.
These key external factors include:

- Domain freshness/length of 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 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 tools and other events to provide insight into the health of the client.



Another key capability is checking attacked systems for past infections. When Threat Response performs an on-demand endpoint collection, it checks for IOCs not only from the current attack, but from past infections seen in your environment. This approach helps quickly and effectively verify whether past infections have spread to the system being targeted now.

Out-of-the-Box Integration with Premium Intelligence and Third-Party Tools

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

Threat Response automatically checks every domain and IP provided in security alerts and sandbox reports against its built-in premium intelligence feeds. This step removes hours of tedious work and manual one-by-one searching against intelligence services to find attacking IPs and hosts leveraging known bad sites.

The analysis yields intelligence that Threat Response puts into action. In addition, Threat Response can automatically or manually import threat intelligence from third parties via STIX and TAXII. This means that security teams can import and automatically match against threat feeds from various Information sharing and analysis centers (ISACs) out of the box. It supports "bring your own intelligence" datasets via upload or by manually adding intelligence items one at a time.

Contain the Threat

Changes at the network level can yield immediate protection, stopping:

- Infections from spreading from one system to another
- Control signals from reaching malware
- Sensitive data from reaching external sites

Threat Response automates containment, using your existing enforcement tools to close the gap between threat detection and protection.

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

SPECIFICATIONS

Event Sources:

- Proofpoint Targeted Attack Protection
- FireEye NX and EX
- Palo Alto Networks (Wildfire, Threat Prevention, Dynamic Lists)
- HP ArcSight
- QRadar/Juniper STRM
- Splunk
- Cisco FirePOWER NGIPS (SourceFire)
- Suricata

Enforcement Devices:

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

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.