proofpoint

Proofpoint Threat Response™ (PTR)

Automated Incident Response Designed for Security Operations

Automatic Threat Context | Containment & Quarantine | Single Pane of Glass | Built-In Device Connectors

Automatic Threat Context and Infection Confirmation

- PTR automatically collects, connects, and organizes internal and external threat context and intelligence.
- Real-time information availability enables security teams to analyze vs. do manual research such as IP lookups, reputation checks, malicious file history investigation, etc.
- Infections on endpoints can be confirmed without sending out service desk personnel.
- PTR customers report reductions in incident investigation time and effort by over 50%.

Containment and Quarantine

- Security analysts can enable automatic containment or semi-automated responses.
- Typical response actions include updating firewall groups, updating proxies, updating Active Directory group membership, increased logging, packet captures, or network isolation of an infected system.
- Response actions are automatically recorded for future review or escalation
- Users report accelerating containment and quarantine times by up to 20x.

Integrated Visualizations

- Analysts are overwhelmed by multiple alerts and dashboards from Advanced Malware Detection tools, IDS, SIEMS, and other detection tools.
- PTR scores and prioritizes incidents to help analysts focus on the most pressing issues.
- Security analysts can increase efficiencies and provide more consistent response results.
- Automatic reports for incident lifecycle management spanning threats, analysts, targeted users, targeted hosts, and more

Connectors and Adapters

- Built-in security alert source connectors for leading advanced malware detection, SIEMs, and IDS providers
- Built-in enforcement and quarantine adapters for all major firewall providers and proxies to enable rapid setup and response for an organization.
- No need for custom coding to experience the benefits of automated incident response and containment.

Proofpoint Threat Response provides automated incident response to close the gap between threat detection and containment. By enabling security operations to understand high value targets and threats in incident, confirming infections, and containing and quarantining threats, the platform prevents data loss and protects against future infections of other users.

World-Class Support

- Customer Satisfaction Scores: **95%**
- Customer Renewal Rate: **90%**
- Average Call Answer Time: **24 seconds**
- Cases Resolved with L1 Support: **90%**

Value to the Business

- Decrease investigation time by >50%
- Accelerate containment speed by 20X
- Reduce exposure and risk from advanced attack with less effort.

For more information, please visit:
www.proofpoint.com/solutions/products/threat-response

proofpoint

For more information, please visit:
www.proofpoint.com/solutions/products/threat-response

Questions to Ask	Relevant Information
How do you confirm and respond to security alerts from TAP or other detection tools?	Customers who take multiple steps and > 15 minutes to respond to TAP or other alerts may be more open to Threat Response. Bottom line – if a customer sees an alert from any source, they should review it. Threat Response makes reviewing and responding to alerts easy and efficient.
How do you confirm high value targets or threats are involved in an incident?	Identifying high value targets and threats can take 15 to 45 minutes and be error prone. Threat Response can increase accuracy and slash the time to 1 to 2 minutes.
How do you verify that a user has been infected with malware?	Most detection tools tell you what happened in a sandbox and cannot confirm that a system was actually infected. Threat Response will verify the infection, check for past infections, and help eliminate false positives, saving hours to days worth of work.
Do you have an IDS, Advanced Malware Detection tool, or SIEM? How many?	If a customer has at least two supported detection tools, they are much more likely to respond to the value of Threat Response. PTR has many pre-built connectors and adapters with more in development, and analysts report configuring devices with PTR in as little as 20 minutes .
Are you concerned that manual response processes leads to inefficiencies or delays?	While security analysts are reviewing the incident information, valuable data may be leaking from infected devices. The ability to automatically contain and quarantine risks stops the bleeding and IP loss.

Homegrown Solutions

- Customers may have developed their own customized scripts to deal with threat remediation.
- This method is difficult to maintain over time and doesn't adapt to new technologies quickly.
- Proofpoint provides the technology and support for PTR.

SIEM Vendors

- Customers tell us is that they're using their SIEMs for log aggregation & compliance, not correlation & response.
- SIEMs allow post-incident review but no visualization.
- PTR is not a SIEM; we provide incident context integration versus aggregation.

New Competitors You May See

Homegrown solutions are the most common, but a few competitors recently entered this market:

- Co3 Systems
- Access Data
- CSG Invotas
- Endgame
- Click Security
- Hexadite

Mandiant / FireEye

- Mandiant is an endpoint agent, which requires every system to have Mandiant installed to be effective.
- Does not do network containment and quarantine.
- Does not update enforcement devices to block traffic to and from malicious sites.