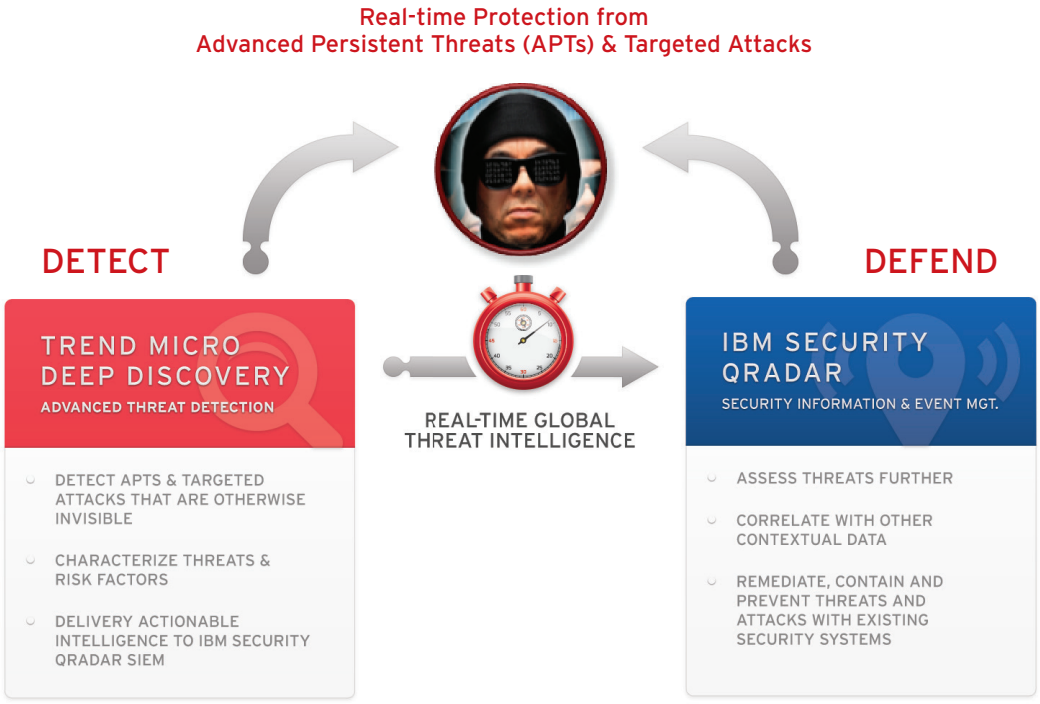
Trend Micro™ Deep Discovery and IBM® Security QRadar SIEM

Real-time Protection from Advanced Persistent Threats (APTs) and Targeted Attacks

Detect and Respond to APTs and Targeted Attacks

Advanced persistent threats (APTs) are stealthier and more sophisticated than ever, using insidious social engineering techniques to quietly penetrate your organization to deploy customized malware that can live undetected for months. Then, when you are least expecting it, cybercriminals can remotely and covertly steal your valuable information–from credit card data to the more lucrative intellectual property or government secrets–potentially destroying your competitive advantage, or in the case of government, even putting national security at risk.

Trend Micro Deep Discovery integrated with **IBM Security QRadar SIEM** enables you to detect and respond to APTs and targeted attacks that are invisible to traditional security systems, or that are easily lost in the "noise" of millions of events.



JOINT SOLUTION VALUE

Trend Micro Deep Discovery threat detection together with **IBM Security QRadar SIEM** provides contextual and actionable real-time surveillance across your entire IT infrastructure. This intelligent, automated and integrated joint solution enables you to quickly and confidently detect, contain and remediate APTs, targeted attacks and threats that are missed by other security solutions.

Over 75% of organizations have found active command and control communications from within their network, 90% have active malware, and over 50% had data-stealing malware.

Why Trend Micro and IBM

Combines best-of-breed threat intelligence and SIEM to detect and respond to the broadest range of APTs and other threats, across the entire attack lifecycle.

Most Intelligent

- Proactive threat detection
- Identifies APTs, targeted attacks and other critical anomalies
- Rapid, extensive threat intelligence and impact analysis
- Containment and remediation recommendations

Most Automated

- Easy deployment and integration
- Rapid time to value (days)
- Operational efficiency

Most Integrated

- Bridges silos
- Highly scalable
- Flexible and adaptive

Premier Business Partner IBM™

Get real-time answers to these critical questions:

- Are we being attacked? By who?
- Is someone stealing our data? Who?
- How are they attacking/stealing?
- What is being attacked or targeted?
- What is the business impact?
- Where do I investigate?
- How can we prevent the attack/theft?
- How can we remediate?

Detect and Respond to:

- **Malicious content:** emails containing embedded document explots, drive-by downloads, zero-day and known malware
- **Suspect communication:** command and control communication for all malware; bots, downloaders, data stealing, worms and blended threats; backdoor activity by attacker
- **Attack behavior:** malware activity (propagation, downloading, spamming, etc.), attacker activity (scan, brute force, service exploitation), data exfiltration

TREND MICRO DEEP DISCOVERY provides organizations with the network-wide visibility, insight, and control needed to combat APTs and targeted attacks. For advanced threat protection, Deep Discovery uniquely detects and identifies evasive threats in real-time, then provides the in-depth analysis and relevant actionable intelligence that will equip enterprises to assess, remediate, and defend against targeted attacks.

IBM SECURITY QRADAR SIEM is an enterprise solution that consolidates log source event data from thousands of devices distributed across a network, storing every activity in its raw form, and then performing immediate correlation activities to distinguish the real threats from false positives. It also captures real-time Layer 4 network flow data and, more uniquely, Layer 7 application payloads, using deep packet inspection technology.

HOW IT WORKS

DETECT THREATS: Once installed in your network at the primary Internet ingress/egress point where it has maximum visibility to all traffic, Deep Discovery is then quickly configured to automatically push the syslog threat or attack event data it collects to QRadar in Log Event Enhanced Format (LEEF). Deep Discovery inspects all types of network traffic in a non-intrusive, listen-only mode to detect malicious content, suspect communication and attack behavior.

THREAT NOTIFICATION: You will be notified of threats that have been identified by Deep Discovery either directly in the QRadar dashboard, or via email alerts. You can then do additional analysis, logging or investigation using QRadar to further understand the attack. You may also then choose to log into Deep Discovery for full details on the event and remediation recommendations.

RESPOND: QRadar provides the actionable and contextual information that is required to block specific breaches. For example, this could mean changing a firewall setting to block all traffic on a specific port, modifying a blacklist on a web gateway, adjusting a router to prevent specific activity, or isolating an infected endpoint on the network.

About Trend Micro

As a global leader in cloud security, Trend Micro develops security solutions that make the world safe for businesses and consumers to exchange digital information. With 25 years of experience, we deliver top-ranked security that fits our customers' needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments.

©2013 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Trend Micro Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

Find out more at:

www.TrendMicro.com/DeepDiscovery
Or contact a Trend Micro sales specialist at:
1-877-218-7363 or sales@trendmicro.com