Deep Discovery + HP TippingPoint
Advanced Threat Protection Solution

Real-time detection and blocking of targeted attacks

Targeted attacks and advanced persistent threats (APTs) have proven their ability to evade conventional security defenses and remain undetected while exfiltrating sensitive data and intellectual property. Trend Micro and Hewlett-Packard are working together to help customers prevent these attacks with an integrated solution to detect and block attackers before damage is done.

**Detecting the Attacker with Trend Micro Deep Discovery Inspector**

Deep Discovery Inspector is an advanced network protection appliance that monitors virtually all network traffic to identify and analyze malware, command-and-control (C&C) communications, and evasive attacker activities that are invisible to standard security. Unlike standard security solutions, Deep Discovery Inspector:

- Scans all network ports and over 80 network protocols for broad coverage
- Accurately detects advanced malware by using custom sandbox images that precisely match system configurations
- Uses multiple techniques to identify attack signals across a range of endpoints and mobile devices including Microsoft Windows, Apple OSX, and Android.

**Key Benefits**

- **Targeted Attack Protection**
  - Detects and blocks threats invisible to standard security products
- **Comprehensive Network Security**
  - From the leading products in FW, IPS, Advanced Threat Protection, and SIEM
- **Enterprise Risk Management**
  - Central investigation and reporting across the enterprise

**Detect**

- Detection of zero-day malware, C&C, attacker activity
- Sharing Indicators of Compromise with HP Tipping Point products

**Block**

- Advanced inline attack protection
- Blocking of new threats detected by Deep Discovery

**Investigate**

- Centralized alerting & reporting
- Enterprise-wide incident investigation

---

[Image of Trend Micro Deep Discovery Inspector]

[Image of HP TippingPoint NG FW]

[Image of HP TippingPoint NG IPS]

[Image of HP ArcSight SIEM]
Blocking Attackers with HP TippingPoint Next-Gen IPS and Next-Gen FW

TippingPoint NGIPS and NGFW deliver high-performance inline protection against a broad range of attack elements including malware, C&C, and vulnerability exploits. The TippingPoint Security Management System (SMS) provides central management, policy control, and ArcSight SIEM integration to enable enterprise-wide investigations.

When integrated with Deep Discovery Inspector, NGIPS and NGFW can block newly discovered C&C paths identified by Deep Discovery sandbox analysis. Deep Discovery Inspector maintains a real-time link with TippingPoint SMS to convey Indicators of Compromise (IoCs) that SMS broadcasts to all TippingPoint devices per explicit policy management configurations. The devices can then block all subsequent C&C to/from the C&C location for any host on the network.

Investigation, Reporting, and Remediation with HP ArcSight

Deep Discovery Inspector provides full investigation of incidents discovered, and also enables a full range of direct management and investigation capabilities for ArcSight. And by combining intelligence from Deep Discovery, TippingPoint, and other sources, ArcSight can offer the customer comprehensive investigation and reporting across all enterprise events.

A Comprehensive Cyber Security Solution

By combining Trend Micro’s advanced detection technologies and threat intelligence systems with Hewlett-Packard’s advanced IPS and firewall capabilities, and with its ArcSight system for investigation and reporting of incidents, this integrated solution delivers unmatched defensive capabilities against today’s most aggressive, elusive, and advanced attacks and intrusions.

©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo 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. [SB01_Deep_Discovery_HP_140904US]