Trend Micro™

ENDPOINT SENSOR

Discover, investigate, and respond to attacks on endpoints and servers

Targeted attacks and advanced threats have clearly proven their ability to evade conventional security defenses and remain undetected, while stealing corporate data and intellectual property. Advanced threat protection appliances can detect these attack activities at the network level, but they cannot always verify endpoint infiltration, and they can't single-handedly investigate the details and extent of the attack across the entire enterprise.

Trend Micro Endpoint Sensor is a context-aware endpoint security solution that can discover targeted attacks by continually monitoring behaviors in accordance with attack discovery rules, and collecting suspicious objects for sandbox analysis. Endpoint Sensor is also an advanced forensics tool that records and reports detailed system-level activities, allowing threat investigators to rapidly assess the nature and extent of an attack. Endpoint Sensor uses Indicators of Compromise (IOC) information from Trend Micro™ Deep Discovery™ and other sources to perform multi-level searches across user endpoints and servers.

This capability allows you to:

- Confirm endpoint infiltration alerts from Trend Micro™ Deep Discovery™ Inspector or other security solutions
- Find endpoints with specific IOCs, malware, or command-and-control (C&C) activity
- Analyze actual malware execution behavior and results
- Discover the full context, timeline, and extent of an attack

KEY FEATURES

Endpoint-resident event recording

Endpoint Sensor uses a lightweight client to record significant activities and communication events at the kernel level. It tracks these events in context across time, providing an in-depth history that can be accessed in real time.

Rich search parameters

Endpoints can be queried for specific communications, specific malware, registry activity, account activity, running processes, and more. Search parameters can be individual parameters, OpenIOC files, or YARA files.

Advanced behavior monitoring

The continuous monitoring capabilities can discover known and unknown threats based on pre-defined rule sets or OpenIOC rules. This monitoring can discover attacks based on the relationship and context of behaviors. Attacks can be discovered based on the threat's tactic, procedure or technology.

Centralized search and analysis

Searches can be executed directly from the Endpoint Sensor Manager or within Trend Micro™ Control Manager™—so you can immediately respond to attacks based on real-time IOC and activity data from other products.

Multi-level contextual analysis and results

Interactive dashboards allow you to view and analyze system activities over time, assess enterprise-wide activity timelines, and export investigation results.

Deep Discovery integration

Suspicious objects that are discovered by Endpoint Sensor can be collected and sent to the Trend Micro™ Deep Discovery™ Analyzer sandbox for detailed analysis.

On-premises, remote, and cloud

Endpoint Sensor reports and records detailed system-level activities across Windows-based servers, desktops, and laptops, regardless of location.

A/V Compatibility

Coexists with any endpoint/server antivirus software.

Key Benefits

Threat discovery

Identifies infiltrations using the latest available security intelligence and signatures

Forensic investigation

Uncovers the full context, timeline, and extent of an attack

Behavior monitoring

Discovers suspicious behaviors based on pre-defined and custom defined rules

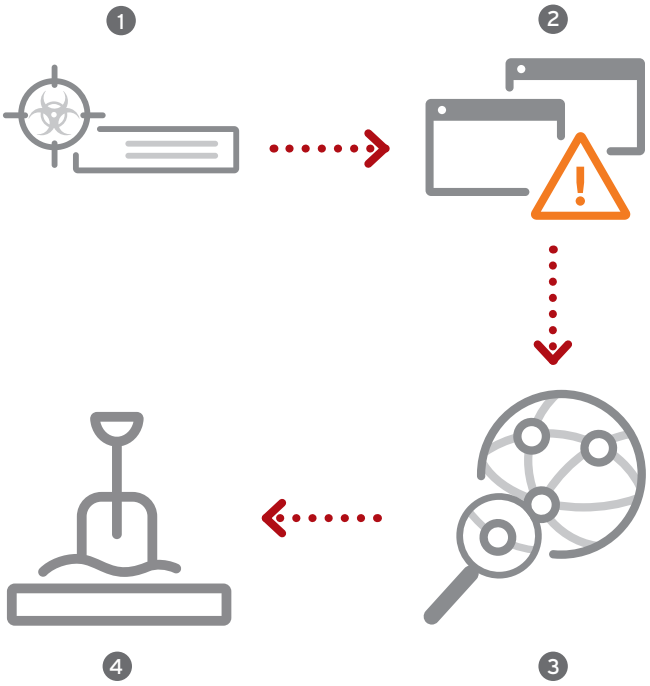
Rapid response

Reduces the time to assess and respond to targeted attacks

NSS LABS RECOMMENDED

RECOMMENDED
Breach Detection System
3 YEARS IN A ROW

99.8% Detection Rate



Discover, investigate, and respond with network and endpoint threat detection

1. Deep Discovery detects a targeted attack on the network
2. Indicator of Compromise sent from Deep Discovery to Endpoint Sensor
3. Endpoint sensor searches for infiltration, scans for similar IOCs, maps the timeline/progression.
4. Using Trend Micro and custom defined rules, Endpoint Sensor monitors behavior on endpoints. If a suspicious object is discovered, it is collected and sent to Deep Discovery Analyzer for sandbox analysis

HOW ENDPOINT SENSOR WORKS

Endpoint Sensor Agent

The Agent runs as a low-profile background process, collecting a deep profile of system events and communication. This information is indexed and stored locally to respond to Manager search and analysis activities. The Agent also responds to a variety of real-time requests, including memory and registry snapshots.

Centralized management and control

The centralized Server manages the Agents and is managed through the Trend Micro Control Manager for threat investigation.

Investigation criteria

Multi-level search and investigation can be conducted based on individual, IOC parameters or objects, OpenIOC files, and YARA files. Search parameters can include:

- Communications: IP, Port, Domain, DNS
- Malware or any file by: Sha1 hash, file name, file path, file type
- Registry activity
- Running processes
- User account activity

Behavior monitoring

Using pre-defined rules and custom IOC rules, Endpoint Sensor monitors system behaviors, their relationships, and context to discover attack behavior.

Suspicious object collection

Suspicious objects and attachments can be automatically submitted to a centralized Deep Discovery sandbox for further analysis.

Research and results

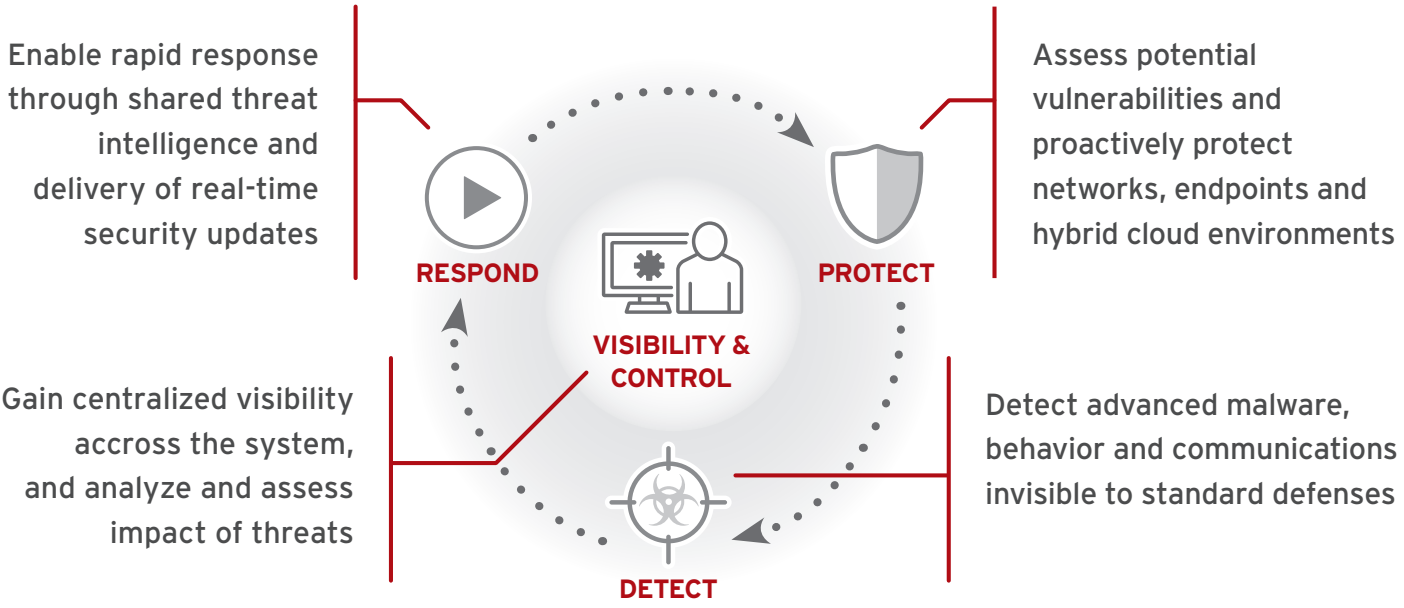
Endpoint Sensor offers a rich multi-level contextual analysis via Interactive dashboards that allow you to view and analyze detailed system activities over time, assess enterprise-wide activity timelines, and export investigation results. Results include:

- Interactive timeline map of system activity
- Step-wise discovery and construction of an attack kill-chain
- Discovery of malicious artifacts, processes, and communications
- Enterprise-wide endpoint search based on specific investigation results

A KEY PART OF TREND MICRO'S CONNECTED THREAT DEFENSE

To adequately protect against the current threat landscape, you'll need a multi-layered protection platform that delivers the full life cycle of threat defense. Trend Micro Connected Threat Defense is a cyber security model that can give organizations a better way to quickly protect, detect, and respond to new threats that are targeting them, while simultaneously improving visibility and control across their network.

- **Protect**: Assess potential vulnerabilities and proactively protect endpoints, servers, and applications.
- **Detect**: Detect advanced malware, behavior, and communications invisible to standard defenses.
- **Respond**: Enable rapid response through shared threat intelligence and delivery of real-time security updates.
- **Visibility and Control**: Gain centralized visibility across the network and systems; analyze and assess the impact of threats.



EXPAND YOUR PROTECTION STRATEGY

Endpoint Sensor is part of an advanced threat strategy that delivers protection where it matters most to your organization—network, endpoint, email, or integrated security. Endpoint Sensor is especially useful to aid in investigation and remediation of targeted attacks identified by Deep Discovery Inspector. Deep Discovery IOC data can be used by Endpoint Sensor to verify endpoint infiltrations and discover the full context, timeline, and extent of the attack.

Deep Discovery Inspector delivers advanced network protection against targeted attacks, monitoring all ports and over 100 protocols to analyze virtually all network traffic. Specialized detection engines and custom sandboxing identify and analyze malware, C&C communications, and evasive attacker activities. Inspector then provides the investigation intelligence to drive a rapid response and shut down attacks.

Control Manager provides centralized management, so you can control and monitor multiple layers of Trend Micro security through a single console. The Endpoint Sensor Manager functionality is embedded within the Control Manager to allow centralized investigations that can leverage the IOC data of most Trend Micro products and enable the investigator to take immediate actions to respond to the attack.

Deep Discovery Analyzer provides advanced sandbox analysis to extend the value of security products such as endpoint protection, web and email gateways, network security, and other Deep Discovery products. Endpoint Sensor can collect and send suspicious objects to Analyzer for analysis. With customized virtual sandboxes that match an organizations standards for operating system, language preferences, and configurations, Deep Discovery Analyzer can detect ransomware, advanced malware, zero-day exploits, C&C, and multi-stage downloads resulting from malicious payloads or URLs on Windows and Mac O/S systems.

Deep Discovery Email Inspector provides advanced malware detection, including sandboxing for email. Email Inspector can be configured to block delivery of advanced malware through email. This malware is often the first stage of a ransomware attack

SPECIFICATIONS

SYSTEM REQUIREMENTS	
SERVER	4 GB minimum, 16 GB recommended. Available disk space: 500 GB minimum, 1 TB recommended **Operating Systems** Windows Server 2008 SP2 (32-bit/64-bit) Windows Server 2008 R2 (64-bit) Microsoft Internet Information Services (IIS) 7 with all of the following role services: • Static Content • Default Document • Directory Browsing • HTTP Errors • HTTP Redirection • ASP.NET • ASP • CGI • ISAPI Extensions • ISAPI Filters • Request Filtering • IIS Management Console • PHP version 5.4.38 **Database** Microsoft SQL Server 2008 Express Microsoft SQL Server 2008 R2 Standard recommended **Web Browsers** Microsoft Internet Explorer 9 or later The latest version of Google Chrome The latest version of Mozilla Firefox
AGENT	**Hardware** RAM: • 512 MB minimum for Windows XP • 1 GB minimum for other operating systems Available Disk Space: • 3 GB minimum for Windows XP, Vista, 7, 8, or 8.1 • 3 GB minimum for Windows Server operating systems **Software** Operating system: • Windows Vista Service Pack 1 (32-bit and 64-bit) • Windows XP Service Pack 3 (32-bit) • Windows 7 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows 10 (32-bit and 64 bit) • Windows Server 2003 (32-bit and 64-bit) • Windows Server 2003 R2 (32-bit and 64-bit) • Windows Server 2008 (32-bit and 64-bit) • Windows Server 2008 R2 (64-bit) • Windows Server 2012 (32-bit and 64-bit) • Windows Server 2012 R2 (64-bit)

Please see your Trend Micro sales representative for full details

TREND MICRO™

Securing Your Journey to the Cloud

©2016 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, Smart Protection Network, and Deep Discovery 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. [DS03_DD_Endpoint_Sensor_160823US]