Trend Micro™

DEEP DISCOVERY 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, nor can they single-handedly investigate the details and extent of the attack across the entire enterprise.

Deep Discovery™ Endpoint Sensor is a context-aware endpoint security monitor 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 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 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 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

Rapid response
Reduces the time to assess and respond to targeted attacks

NSS LABS RECOMMENDED
Trend Micro™ Deep Discovery
MOST EFFECTIVE
Recommended Breach Detection System
2015 Breach Detection Tests

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.

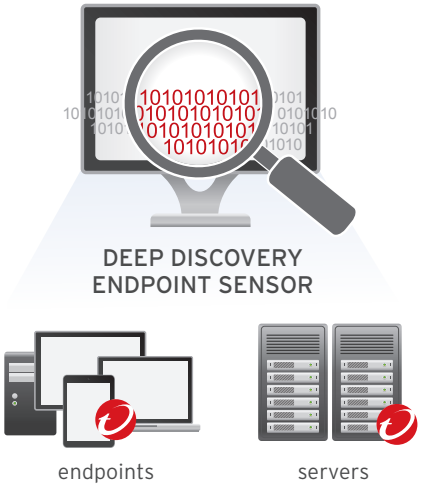
Rich search parameters
Endpoints can be queried for specific communications, specific malware, registry activity, account activity, running processes, and more. Search parameters can be individual parameters, OpenIOC files, or YARA files.

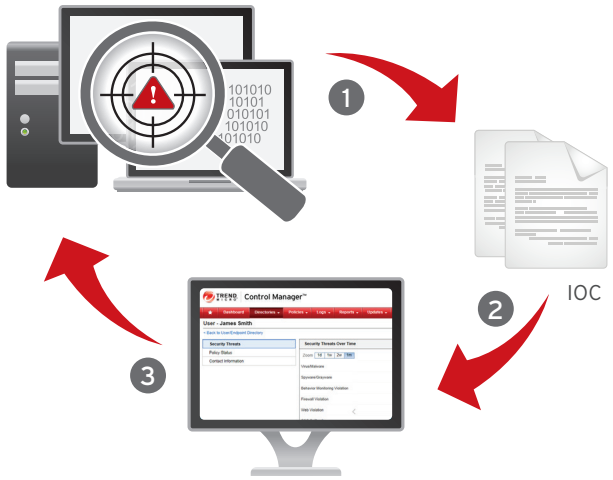
Centralized search and analysis
Searches can be executed directly from the Endpoint Sensor Manager or within Trend Micro™ Control Manager™—so you can immediately respond to attacks based on real-time IOC and activity data from other products.

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.

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.





Control Manager console

Investigate and respond with network and endpoint threat detection

1. Deep Discovery identifies malware or malicious activity
2. Deep Discovery Indicators of Compromise (IOC) intelligence used as search criteria
3. Endpoint Sensor multi-level investigations can:
   - Confirm and investigate infiltration alerts
   - Scan endpoints for similar IOCs
   - Map attack timeline/progression
   - Plan containment and remediation

HOW DEEP DISCOVERY 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.

Endpoint Sensor Server and Manager
The Server manages the Agents and supports a web-based console—the Endpoint Sensor Manager—for threat investigation. The full functionality of the Manager console can also be utilized within the Trend Micro Control Manager to facilitate broader investigation activities.

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

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:

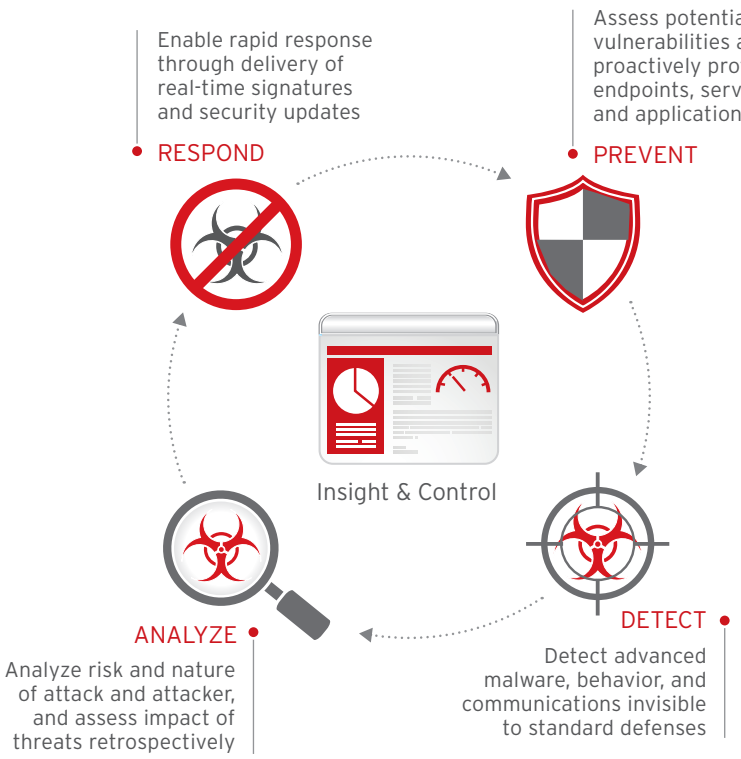
- Interactive timeline map of system activity
- Step-wise discovery and construction of attack kill-chain
- Discovery of malicious artifacts, processes, and communications
- Enterprise-wide endpoint search based on specific investigation results

PART OF A CONNECTED THREAT DEFENSE

To adequately protect against the current threat landscape, you'll need a multi-layered endpoint protection platform that delivers a full lifecycle of threat defense. As the diagram below shows, this consists of four stages: Prevent, Detect, Analyze, and Respond. Trend Micro Endpoint Sensor is a key part of the Analyze quadrant: After threats have been prevented or detected, the analysis phase of the threat protection lifecycle occurs. Endpoint Sensor assesses the risks and the full nature of the attacks, and determines retrospectively the impact of these threats. This includes endpoint forensic investigation and threat correlation.

Trend Micro™ Smart Protection Suites along with Trend Micro Custom Defense deliver connected threat defense with a multi-layer security solution that covers the entire threat defense lifecycle.

Trend Micro will fortify your defenses to the highest levels with the broadest range of threat prevention, detection, analysis, and response capabilities



EXPAND YOUR PROTECTION STRATEGY

Deep Discovery Endpoint Sensor is part of the Deep Discovery platform, delivering advanced threat 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.

Trend Micro 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.

Trend Micro 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.

CUSTOM DEFENSE

The Deep Discovery platform is at the heart of the Trend Micro Custom Defense, weaving your security infrastructure into a comprehensive defense tailored to protect your organization against targeted attacks.

Deep Discovery's custom detection, intelligence, and controls enable you to:

- Detect and analyze your attackers
- Rapidly respond before sensitive data is lost

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 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