Trend Micro™

DEEP DISCOVERY

Targeted attack detection, in-depth analysis, and rapid response

Advanced Persistent Threats (APTs) and targeted attacks have clearly proven their ability to evade conventional security defenses, to remain undetected for extended periods, and to exfiltrate corporate data and intellectual property. Analysts and experts recognize these issues, and recommend that enterprises redefine security due diligence to embrace specialized threat detection technology and a proactive process of real-time threat management.

Trend Micro™ Deep Discovery 3.5 provides you with the network-wide visibility, insight, and control you need 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 you to assess, remediate, and defend against targeted attacks in your organization.

Deep Discovery is at the core of the Trend Micro Custom Defense—a complete solution that enables you to detect, analyze, adapt, and respond to targeted attacks. Specialized inspection engines and custom sandbox simulation identify zero-day malware, malicious communications, and attacker activities that are invisible to standard security defenses. Deep analysis, containment, and remediation are powered by relevant threat intelligence and visibility into network-wide security events, while security update exports enable protection against further attack.

The Deep Discovery solution is comprised of two components. The Deep Discovery Inspector provides network traffic inspection, advanced threat detection, and real-time analysis and reporting. The optional Deep Discovery Advisor provides open, scalable custom sandbox analysis, visibility to network-wide security events, and security update exports—all in a unified intelligence platform.

DETECTS AND PROTECTS AGAINST

- APTs and targeted attacks
- Zero-day malware and document exploits
- Attacker network activity
- Web threats (exploits, drive-by-downloads)
- Email threats (phishing, spear phishing)
- Data exfiltration
- Bots, trojans, worms, keyloggers
- Disruptive applications

KEY BENEFITS

APT & Targeted Attack Detection

Reduces the risk of damage and data loss from APTs

Network-Wide Visibility

Reveals and tracks your true security posture

In-Depth Contextual Analysis & Insight

Fully characterizes threat and risk factors

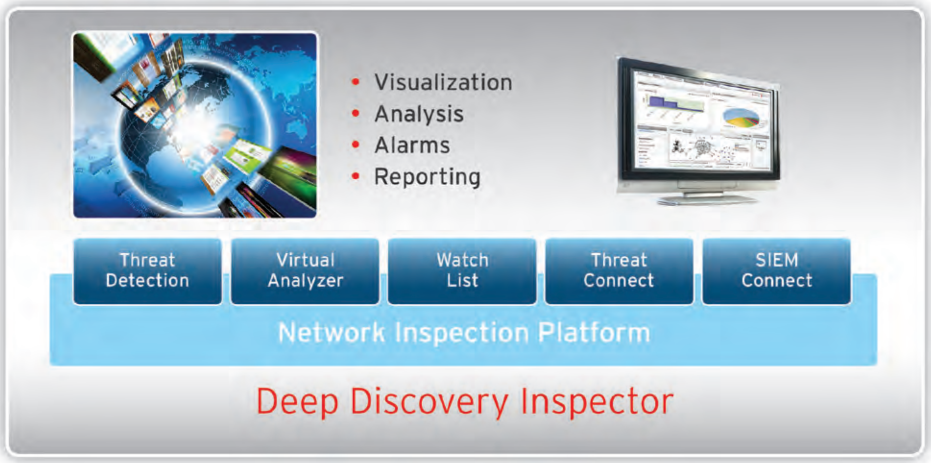
Rapid Containment & Response

Speeds up recovery with actionable intelligence, and security update exports

Cornerstone of a Custom Defense

Combats the threats that matter to you using custom sandbox simulation, intelligence, and updates

Deep Discovery Inspector



Deep Discovery Inspector provides network traffic inspection, advanced threat detection and real-time analysis and reporting—all purpose-built for detecting APT and targeted attacks. It uses a 3-level detection scheme to perform initial detection, then custom sandbox simulation and correlation, and finally, a cross-correlation to discover "low and slow" and other evasive attacker activities discernable only over an extended period.

Specialized detection and correlation engines provide the most accurate and up-to-date protection aided by global threat intelligence from Trend Micro™ Smart Protection Network™, and dedicated threat researchers. The results are high detection rates, low false positives, and in-depth incident reporting information designed to speed up the containment of an attack.

KEY FEATURES

Advanced Threat Detection

Deep Discovery Inspector focuses on *identifying malicious content, communications, and behavior indicative of advanced malware or attacker activity* across every stage of the attack sequence using a non-intrusive, listen-only inspection of all types of network traffic.

- **Dedicated Threat Engines** and multi-level correlation rules deliver the best detection and minimize false positives
- **Virtual Analyzer** ensures accurate detection and reduces false positives by providing full forensic analysis using customer-specific images that exactly match the target environments
- **Smart Protection Network** intelligence and dedicated threat researchers provide continually updated detection intelligence and correlation rules to identify attacks

Threat Tracking, Analysis, and Action

The Deep Discovery Inspector console provides real-time threat visibility and deep analysis in an intuitive format that allows security professionals to focus on the real risks, perform forensic analysis, and rapidly remediate issues.

Real-Time Threat Console

Places threat visibility and deep analysis at your fingertips

- Quick access widgets provide critical information at a glance
- In-depth analysis of attack characteristics, behavior, and communication
- GeoTrack identifies the origins of malicious communication

Watch List

Delivers risk-focused monitoring of high severity threats and high value assets

- Focused tracking of suspicious activity and events on designated hosts
- Hosts to be tracked determined via threat detection or customer selection
- Detailed event timeline tracks all attack activities involving target hosts

Threat Connect

Provides the threat intelligence you need to understand and remediate an attack

- Direct access to Trend Micro intelligence portal for a specific attack or malware
- Detailed threat characteristics; containment and remediation recommendations
- Direction to available antivirus/other signature updates for this threat

SIEM Management

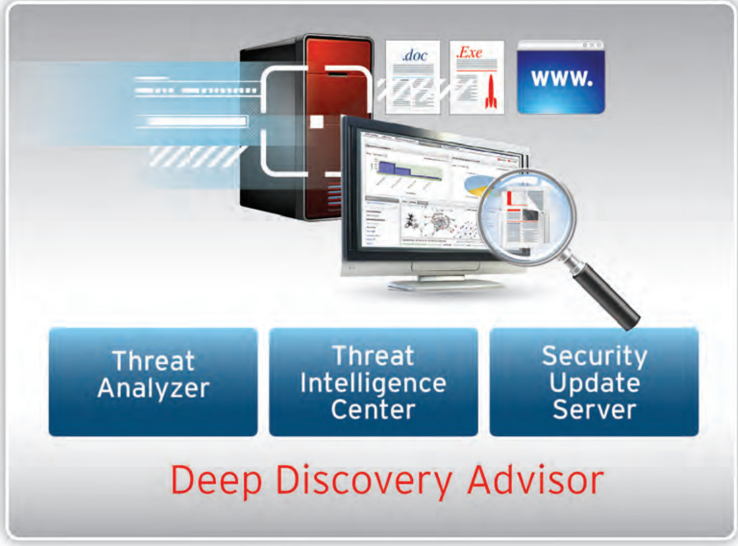
Integration with leading SIEM platforms delivers improved enterprise-wide threat management from a single SIEM console

- Network detections, confirmed incidents, and contextual data are reported to SIEM
- Deep network visibility enhances correlation and multi-dimensional attack profiling of SIEM
- Enterprise-wide threat management provided by SIEM as the central console

Flexible, High-Capacity Deployment

Deep Discovery Inspector features a high-performance architecture designed to meet the demanding and diverse capacity requirements of customers of all sizes. The product is available on a full range of hardware, software, and virtual appliances supporting multi-gigabit corporate backbones down to remote office locations.

Deep Discovery Advisor



Deep Discovery Advisor provides open, scalable custom sandbox analysis, visibility to network-wide security events, and security update exports—all in a unified intelligence platform.

KEY FEATURES

Threat Analyzer

The Threat Analyzer is an optional component designed to offer in-depth simulation and analysis of potentially malicious sample files, including executables and common office documents. It can augment and centralize the simulation of Deep Discovery Inspector, as well as provide advanced detection and analysis security for professionals or any security product or service via an open web services interface.

- In-depth threat simulation, and analysis uses sandbox simulation and other advanced detection engines to classify and deeply analyze submitted files
- Custom sandbox execution environments allow the customer to create and analyze multiple fully custom target images that precisely match their host environments
- Scalable architecture supports incremental capacity that ranges up to 50,000 samples/day
- Open, automated, and manual submission supports input from security analysts, as well as automated submission and results loopback by Trend Micro products and third-party or custom products
- Integration with Deep Discovery Inspector and other Trend Micro products provides expanded detection and analysis options to customers

Threat Intelligence Center

The Threat Intelligence Center is a complete analysis environment for event data from the threat analyzer, as well as security events and logs collected from Deep Discovery Inspector, other Trend Micro products, and third-party solutions. Using these sources and integrated Threat Connect intelligence, Threat Intelligence Center provides in-depth insights to drive risk-based incident assessment, containment and remediation.

- In-depth analysis of incidents, and events using automated analysis, visualization, and advanced search and investigation tools
- Risk-focused monitoring and investigation
- Network-wide security event collection of events/logs from most Trend Micro and third-party products ensures a full risk assessment and effective containment and remediation measures
- Threat Connect intelligence is automatically integrated into analysis results, providing detailed threat characteristics and context-relevant intelligence for containment and remediation
- Deep Discovery Inspector centralized reporting consolidates detection results from multiple Deep Discovery Inspector units into a single dashboard and customizable reports
- SIEM connect with leading platforms delivers improved enterprise-wide threat management from a single SIEM console

Security Update Server

The Security Update Server provides the means to export useful security blocking information learned from Threat Analyzer simulation. This information includes newly identified malicious IP/URL addresses and file hash codes that can be useful to a variety of security products. Deep Discovery Inspector and certain other Trend Micro products automatically receive this information. The information can also be manually exported via CSF files.

How Deep Discovery Works

Deep Discovery is purpose-built for detecting APT and targeted attacks—identifying malicious content, communications, and behavior that may indicate advanced malware or attacker activity across every stage of the attack sequence.

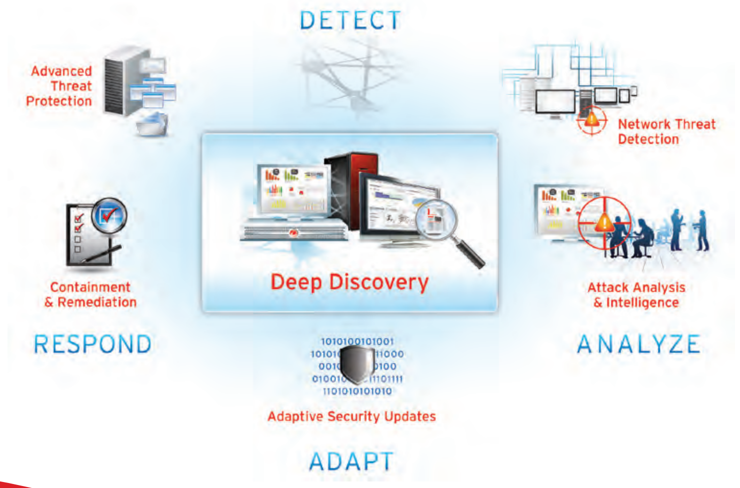
Deep Discovery performs initial detection, custom simulation and correlation, then a final cross-correlation to reduce false positives and discover evasive activities. The detection engines and correlation rules are powered by global threat intelligence from Trend Micro Smart Protection Network and dedicated Threat Researchers. The result is a high detection rate, low false positives, and in-depth incident intelligence to speed the containment of an attack.

	ATTACK DETECTION	DETECTION METHODS
Malicious Content	• Emails containing embedded document exploits • Drive-by-downloads • Zero-day and known malware	• Decode and decompress embedded files • Sandbox simulation of suspicious files • Browser exploit kit detection • Malware scan (Signature and Heuristic)
Suspect Communication	• Command-and-control communication for all malware: bots, downloaders, data stealing, worms, and blended threats • Backdoor activity by attacker	• Destination analysis (URL, IP, domain, email, IRC channel, etc.) via dynamic blacklisting, white listing • Smart Protection Network™ Web reputation • Communication fingerprinting rules
Attack Behavior	• Malware activity: propagation, downloading , spamming, etc. • Attacker activity: scan, brute force, service exploitation • Data exfiltration	• Rule-based heuristic analysis • Identification and analysis of usage of 100's of protocols and applications including HTTP-based apps

The Custom Defense Against Your Attackers

Deep Discovery advanced threat detection is at the core of an effective custom defense against the attacks targeted at your organization. But, Trend Micro™ has also integrated the advanced malware detection of Deep Discovery Advisor with selected Trend Micro products to improve your protection against the all-important initial stage of an attack. In addition, to provide the truly adaptive protection of a custom defense, the in-depth results of Deep Discovery Advisor analysis are used to update Trend Micro products to immediately strengthen your defense against further attack.

- Network-level attack detection and custom analysis
- Protection solutions with custom malware detection
- Custom security updates for adaptive protection
- Actionable intelligence based on full contextual analysis speeds response


DETECT
Advanced Threat Protection
Network Threat Detection
Deep Discovery
Containment & Remediation
Attack Analysis & Intelligence
RESPOND
ANALYZE
Adaptive Security Updates
ADAPT

EXPAND YOUR APT SECURITY STRATEGY

RISK MANAGEMENT SERVICES

Trend Micro service specialists augment your security responsiveness and expertise with installation, monitoring and consulting services to further reduce your risk exposure and security management costs.

TREND MICRO™ THREAT MITIGATOR

A network-resident system provides automated real-time remediation of malware infections identified by the Deep Discovery Inspector

SPECIFICATIONS

Deep Discovery Inspector

- Model 1000: 1 Gbps Hardware and Virtual Appliances
- Model 500: 500 Mbps Hardware and Virtual Appliances
- Model 250: 250 Mbps Virtual Appliance
- Model 100: 100 Mbps Virtual Appliance

Deep Discovery Advisor Suite Hardware Appliance

- Can be clustered up to 5 units

Deep Discovery Advisor Threat Intelligence Center

- Virtual Appliance