TREND MICRO

Securing Your Web World

Trend Micro™

Threat Management Solution

Discovering, Mitigating, and Managing Threats Inside Your Network

Trend Micro's Threat Management Solution provides organizations with a better, more effective way to discover, mitigate, and manage internal threats at the network level. This solution helps you respond to malware quickly and efficiently, minimizing data loss and significantly reducing damage containment costs while improving your overall security posture.

LIMITATIONS OF TODAY'S SECURITY SOLUTIONS

As threats become more sophisticated and workplace data leaks grow more prevalent, conventional technologies like firewalls, IDS systems, and VPNs prevent outside threats but fail to protect against "inside threats" from employees who accidentally infect the network. In addition, security solutions such as Network Access Controls (NAC) focus on initial posture assessment and authentication of the employee's endpoint but fail to monitor users afterwards, opening the door to possible data breaches or infections.

In addition, greater numbers of telecommuting and traveling employees and the blurring between home and work offices have increased mobile device use, making it difficult to control how and where users connect. Inadequate remote office security, lack of personnel, and lax policy enforcement also impact security.

Unprotected channels, such as Web mail or wireless networks, and easily exploited technologies, such as P2P file sharing, streaming media, and instant messaging, allow malware to enter the network while draining valuable network bandwidth. In addition, most antivirus applications fail to adequately address zero-day malware.

Once inside, malware can leak data to cybercriminals, posing problems both for the consumers who lose confidential data and for businesses whose reputations are damaged when data is lost. Damage clean-up costs and lost productivity are additional reasons that organizations seek a better solution to protect against internal threats.

Today's security environment is ready for a new approach—one that introduces more visibility into the location and cause of infections to deliver the information needed for better protection.

THE SOLUTION

Trend Micro delivers the industry's most comprehensive solution to discover, mitigate, and manage threats in your internal network. Designed from the ground-up to identify and respond to next-generation threats, the Threat Management Solution helps companies minimize data loss from malware activity, reduce damage containment costs, and improve the overall security posture.

TREND MICRO THREAT MANAGEMENT SOLUTION

- Discover how, where, and why infections entered your network
- Stop threats before they spread further
- Prevent future threats with in-the-cloud threat intelligence and management

The Threat Management Solution detects the following threats:

- Worms
- Bots
- Trojans
- Crimeware
- Spyware/adware
- Network exploits
- Web-based threats (Web exploits, cross-site scripting)
- Email-based threats (phishing, spear-phishing)
- Disruptive applications

THE THREAT MANAGEMENT SOLUTION CONSISTS OF TWO PRODUCT SUITES

The Trend Micro Threat Discovery Suite monitors the network to uncover stealthy and zero-day internal threats that traditional security products fail to detect. The solution identifies a wide range of unauthorized applications and services that disrupt the network and pose security risks. Collaborating with in-the-cloud technology powered by Trend Micro's Smart Protection Network, the Threat Discovery Suite utilizes cutting-edge analysis of malware behavior and advanced threat correlation logic to provide accurate, timely, actionable threat reports and recommendations to improve knowledge of your network.

The Trend Micro Threat Mitigation Suite acts on information from the Threat Discovery Suite to contain and remediate threats and enforce policies. Using advanced, pattern-free clean-up technology, the Threat Mitigation Suite automatically removes threats from infected endpoints. Using root-cause analysis, the Mitigation Suite provides IT administrators with the event chain needed to diagnose why endpoint infections occurred.

THREAT DISCOVERY SUITE – FEATURES

Detects malicious activities at the network layer such as:

- Malware that attempts to propagate or infect other users
- Hidden malware that communicates to external parties to leak information or receive commands
- Web or email content-based attacks such as Web exploits, cross-site scripting, and phishing

Discovers disruptive network applications and services:

- Detects unproductive network usage such as instant messaging, P2P file sharing, and streaming media
- Identifies unauthorized services that pose security risks such as abused SMTP open-relay and rogue DNS service

Analysis leverages Network Content Inspection Technology:

- Inspects network traffic up to the application layer with comprehensive protocol support
- Correlates suspicious events for positive threat identification
- Analyzes file content, powered by Trend Micro's advanced Virus Scan Engine

Integrates with Trend Micro Threat Management Services:

- Utilizes the computing power of in-the-cloud servers to run an advanced correlation engine for improved threat detection, root-cause identification, forensics, and threat analytics
- Leverages Trend Micro's Smart Protection Network to ensure access to the most up-to-date threat data to perform analyses
- Accesses Trend Micro's security intelligence for in-depth, timely information on the current and emerging threat landscape

Threat analysis and reporting capabilities:

- Generates a holistic view of corporate-wide security posture
- Manages reports and incident information through a centralized portal
- Delivers a daily administrative report for incident response, a weekly/monthly executive summary for reviewing overall security posture and an incident review and comparison report
- Provides interactive drilldown reporting for navigate incident information
- Displays granular view with comprehensive threat intelligence
- Recommends security policy improvements and actionable remediation and response

THREAT DISCOVERY KEY COMPONENTS

- Threat Discovery Appliance
- Threat Management Services

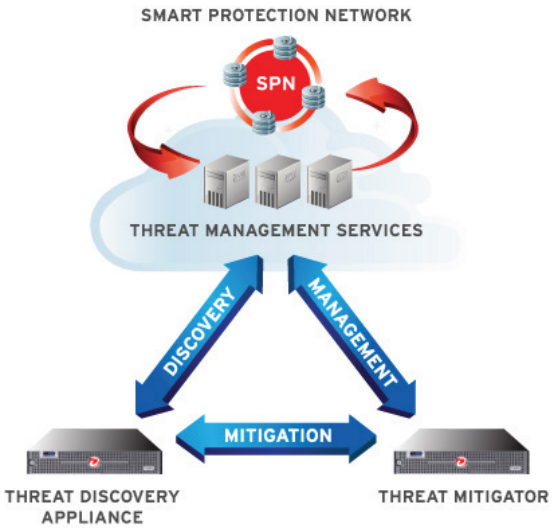
Monitor
Continuously monitor for malware infections, information stealing, and disruptive applications such as P2P and instant messaging.

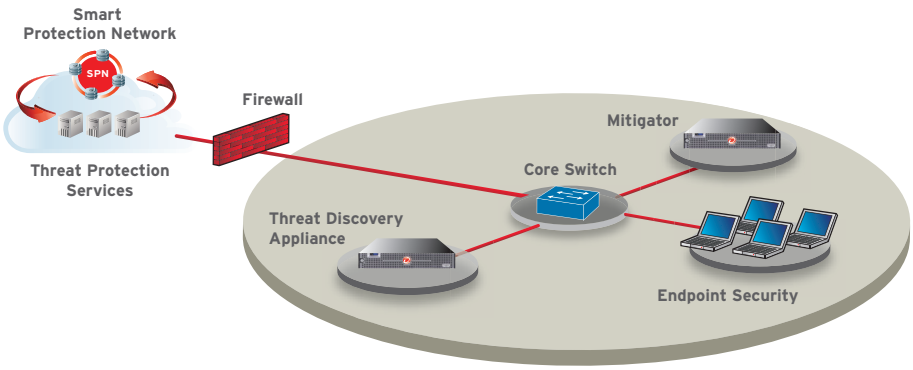
Collaborate
Leverage the advanced threat intelligence of Trend Micro's Smart Protection Network for behavioral analysis, correlation, and forensics.

Mitigate
Network-wide Threat Mitigation features root-cause analysis, damage clean-up, and recovery.

Enforce
Enforce policies and control access to endpoints to ensure compliance with corporate security policies.

Manage
Review proactive and customized threat reports, incident analysis review, and remediation.





THREAT MITIGATION SUITE – FEATURES

Automated damage clean-up:

- Requires no user intervention with fully automated, real-time threat response and flexible clean-up options to set the desired level of incident response
- Cleans up simultaneous, damaging incidents across multiple hosts
- Quarantines infected hosts prior to clean-up to effectively prevent malware from spreading

Pattern-free clean-up of new and known malware:

- Utilizes advanced forensic techniques to locate and eliminate malware and its components from the infected endpoint without requiring any pattern or signature updates
- Performs comprehensive clean-up of endpoints containing more than one malware infection using an intelligent trace logic
- Avoids false alarms with safety checks to ensure only malicious files are removed
- Adds safety mechanisms through clean-up, rollback, and restore functionality

Root-cause analysis of security incidents:

- Determines the chain of events that led to the endpoint infection
- Pinpoints the channel and method malware used to infiltrate the system (i.e. via USB, malicious link, etc.)
- Identifies system changes malware made on the endpoint

Endpoint posture assessment and policy enforcement:

- Verifies that endpoints have the latest OS security patches to ensure baseline security
- Automatically checks for installed antivirus software and provides the latest signatures with support for different vendors
- Quarantines and prevents non-compliant endpoints from gaining network access

Flexible deployment:

- Uses port spanning on a network switch to mirror network packets for content inspection—ensuring network services are not disrupted
- Offers out-of-band or inline deployment for mitigation and policy enforcement

For more information, visit www.trendmicro.com.

THREAT MITIGATION – KEY COMPONENTS

- Threat Mitigator
- Network VirusWall Enforcer
- Threat Management Agent

KEY BENEFITS

- **Faster response** to data loss due to early detection of new and known malware
- **Cost savings** in damage clean-up and containment, and reduced downtime, due to automated pattern-free clean-up of new security threats
- **Proactive security infrastructure** planning due to increased knowledge of network weak points and root cause of threats
- **Bandwidth and resource savings** due to detection of disruptive applications and services in the network
- **Easier management** of threat and incident information through centralized management portal
- **Minimal interruption to existing services** due to flexible out-of-band deployment

HARDWARE SPECIFICATIONS	THREAT DISCOVERY APPLIANCE
Performance	
Max. Throughput	1 Gbps
Max. Concurrent Connections	10,000
Connectivity	
Monitoring Interfaces	2 x Gigabit Ethernet 10/100/1000 Copper
Management Interfaces	1 x Gigabit Ethernet 10/100/1000 Copper
Serial Console Interface	1 x RS232
Mode of Operation	
SPAN Port Monitoring	Yes
High Availability	
Redundant Power	Yes
Device Failure Detection	Yes
Processors	2 x Quad Core Xeon Processor
Hardware status monitoring	Yes
Physical/Operational	
Form Factor	2U rack mountable
Height	3.4" (8.64cm)
Width	17.5" (44.43cm)
Depth	29.31" (74.4cm)
Weight	50.71 lbs (23 Kg)
Operation Temperature	10º C to 35º C (50º F to 95º F)
Management	
Web-based central management console	Yes
TrendMicro Control Manager	Optional, recommended for multiple deployments
Live update enable	Yes
SSH secure management console	Yes
Serial management console	Yes
Live update enable	Yes
SSH secure management console	Yes
Serial management console	Yes

SYSTEMS REQUIREMENTS – VIRTUAL APPLIANCES

Virtual Appliance/Software Support VMware ESX 3.5 server

Minimum Hardware Requirements

CPU	Two 1.5 GHz or higher Intel or AMD x86 processors
Memory	At least 2GB of physical memory
Hard drive	10 GB Free Space
Networking	"2 or 3 Ethernet interfaces (2 data ports or additional one management port) P.S.: 1 Ethernet interface for mitigation only"

Recommended Hardware Requirements

CPU	Two Dual-core 3 GHz or higher Intel or AMD x86 processors
Memory	At least 4 GB of physical memory (RAM)
Hard drive	10 GB Free Space
Networking	"2 or 3 Ethernet interfaces (2 data ports or additional one management port) P.S.: 1 Ethernet interface for mitigation only"