Trend Micro™

Threat Management System
Real-time network threat detection, analysis, and automated remediation

Advanced targeted and persistent threats can easily evade standard security, software vulnerabilities are rampant, insider threats are a constant, and now consumerization and mobility are opening the network even further to exploitation. To minimize your exposure and risk of data breach, analysts recommend a proactive strategy using network analysis and visibility tools to continually monitor your network for malicious activity.

Trend Micro Threat Management System is a network analysis and visibility solution that uniquely detects evasive intrusions and automates remediation, giving you the real-time visibility, insight, and control you need to protect your company from advanced targeted attacks. Powered by Trend Micro Smart Protection Network, an array of threat detection and analysis engines, and the latest intelligence of Trend Micro Threat Researchers, Threat Management System provides the most accurate and up-to-date threat deterrence capability.

Trend Micro Dynamic Threat Analysis System is a malware identification and analysis platform that uses sandboxing and other advanced methods to provide further exploration, simulation and full forensic analysis of suspected malware captured by Threat Management Services or submitted directly by a threat researcher.

Trend Micro Risk Management Services put Trend Threat Researchers and Service Specialists on your team to augment your security responsiveness and expertise. At your request, we can deliver a complete portfolio of proactive monitoring, remediation and strategic consulting services designed to further reduce your risk exposure and security management costs.

DETECTS AND PROTECTS AGAINST
- Advanced Persistent Threats
- Targeted network exploits
- Web-based threats (web exploits, cross-site scripting)
- Email-based threats (phishing, spear-phishing)
- Sensitive data loss or transfer
- Bots, Trojans, and Worms
- Key Loggers and Crimeware
- Disruptive applications

KEY BENEFITS
- Network Visibility and Control
  Real-time network-wide protection from advanced attacks
- Automated Threat Remediation
  Stops evasive intrusions without manual intervention and endpoint downtime
- Threat Behavior Analysis
  Forensic analysis provides insight needed to optimize risk posture
- Reduced Cost & Complexity
  Reduce security, cost and complexity

THREAT MANAGEMENT SYSTEM KEY FUNCTIONS

<table>
<thead>
<tr>
<th>Network Visibility and Control</th>
<th>Endpoint Security Automation</th>
<th>System and Device Protection</th>
<th>Regulatory and IT Security Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides the real-time visibility, insight, and control you need to protect your company from advanced attacks.</td>
<td>Provides automated endpoint detection &amp; mitigation of the advanced threats that easily evade endpoint and perimeter security.</td>
<td>Protects the Point of Sale, medical, production, SCADA and legacy systems that cannot directly run antivirus.</td>
<td>Provides important controls, DLP, and reporting capabilities to aid the success of your compliance program.</td>
</tr>
</tbody>
</table>

- Identifies evasive malicious activity with network traffic analysis
- Eradicates any infections that are found using automated malware remediation
- Provides multi-level analysis and reporting of total threat posture
- Keeps you ahead of advanced infections and their proliferation
- Identifies infected post-PC and mobile devices
- Minimizes your risk of a serious multi-phase attack
- Reduces your endpoint security management costs
- Keeps equipment running and your network clean with automated detection
- Prolongs lifetime of legacy systems that can’t be patched or protected
- Meets compliance requirements for these devices and systems
- Automates Incident Management processes and provides auditable logging
- Detects regulated data leaving the network via any means
- Achieves compliance for hard-to-secure systems and devices
Threat Management System

**KEY FEATURES**

**Advanced Threat Deterrence and Detection Capabilities**
- Inspects network traffic through the application layer with comprehensive protocol support
- Powered by an array of threat detection engines, sandboxing technology, Smart Protection Network Intelligence, and continually updated threat detection rule sets
- Detects zero-day threats while minimizing false positives using multi-level correlation
- Detects malware command and control communication with web reputation
- Reveals unencrypted regulated data exfiltrated or transferred using integrated DLP reporting
- Inspects user traffic for unauthorized applications and malicious web/email sources
- Isolates infected endpoints pending mitigation

**Automated Threat Remediation**
- Performs real-time automated mitigation triggered by Threat Discovery Appliance
- Uses advanced forensic techniques to locate and eliminate malware without signatures
- Identifies and rolls back any system changes made by malware
- In case of issues, automatically generates and provides to customer a custom cleanup kit

**Threat Analysis and Reporting**
- Provides end-to-end visibility of threat activity and status
- Offers automated drill down forensic analysis of malware characteristics, behavior, communication, source, and channel of entry
- Delivers customizable event alarms
- Supports multi-level reporting for network managers and security executives

**Risk Management Services Offerings**
- Proactive monitoring and alerting
- Threat analysis and advisory
- Threat remediation assistance
- Risk posture review and analysis
- Strategic security planning

**WHY YOU NEED NETWORK ANALYSIS AND VISIBILITY**

Trend Micro studies on corporate security have found:
- 100% of enterprises across all industries had undetected malware¹
- Over 50% of enterprises have active data-stealing malware
- 57% of IT managers are not confident that their organization knows the state of every endpoint that connects to their network
- Only 29% of companies check to make sure computers are up-to-date and patched before allowing remote employees to access the network

¹ Source: 130 global Threat Discovery Services trials conducted by Trend Micro through August 2009. Companies had an average of 7,484 employees and included representatives from the manufacturing, government, education, financial services, retail, and healthcare industries.