



Threat Management Services



Next-generation malware keeps finding new ways to evade detection. In fact, after conducting over 100 Threat Management Services assessment trials in enterprises worldwide, Trend Micro found that **100% of enterprises had undetected malware**. These targeted, coordinated attacks are dangerous precisely because they are specifically designed to go undetected while systematically stealing sensitive data.

WHY ARE CORPORATE NETWORKS STILL VULNERABLE TO MALWARE ATTACKS?

Evasive Emerging Threats

- Cybercriminals now use the abundance of personal and corporate information found in social networking sites, corporate websites, and web searches to slip by security mechanisms and unleash new targeted attacks, enabling explosive growth in the sheer number and variety of malware threats.

Security Infrastructure Vulnerabilities

- As increasing numbers of mobile users go on and off networks with easily infected, vulnerable devices, they compromise corporate networks when connected from inside or via VPN.
- Inadequate remote office security, lack of onsite IT personnel, and lax policy enforcement create numerous malware entry points.

Unsecured Technologies

- Unmanaged and unpatched resources—including legacy systems, contractors, and guest laptops—and mass storage drives like USB devices are common gateways for malware infections.
- Increased usage of easily exploited technologies such as P2P, file sharing, streaming media, and instant messaging expose networks to malware.

Once inside your network, malware can steal sensitive data and leak information to cybercriminals, harming your customers and damaging your company's reputation. Even worse, enterprises often have no early warning system to catch a pending or active data breach, and no comprehensive strategy to contain threats or recover from an outbreak.

Today's enterprise needs an advanced approach to protect systems from the next generation of sophisticated security attacks—one that goes beyond traditional security solutions to provide greater network visibility, proactive alerts, and effective tools to disarm malware, clean up networks, and stop infections before they happen again.

➔ Trend Micro Threat Management Services

THE SOLUTION

Trend Micro™ Threat Management Services is a network security overwatch service that provides an additional security layer, strengthening an organization's existing security infrastructure with threat discovery, containment, and remediation services.

By helping companies find and respond to sophisticated information-stealing malware faster and more efficiently, Threat Management Services minimizes data loss, reduces damage containment and cleanup costs, and improves security posture overall. Other security solutions frequently miss active data-stealing malware infiltrations within the network, but Threat Management Services has been built by industry-leading experts to find and wipe out hidden malware, helping ensure the ultimate protection of corporate data.

Powered by the Trend Micro™ Smart Protection Network™, Threat Management Services includes three packages that provide a critical, network security overwatch layer for complete threat lifecycle management:

THREAT DISCOVERY SERVICES

- Assess and monitor networks 24x7 for stealthy malware infections
- Generate daily incident reports for faster threat response
- Access real-time threat dashboard showing threat metrics, business risk meters, and affected assets and departments
- Receive weekly executive summary reports detailing overall security posture and trends

THREAT REMEDIATION SERVICES

Supplements Threat Discovery Services with:

- Expert, proactive oversight from Threat Management Advisors, including early warning notifications of malware outbreaks both inside and outside your company
- Security advisory services provided by Threat Management Advisors to help diagnose outbreaks, determine containment measures, and provide remediation strategies

THREAT LIFECYCLE MANAGEMENT SERVICES

Supplements Threat Discovery Services and Threat Remediation Services with:

- Automated threat remediation, pattern-free cleanup technology for day-zero malware, and root-cause analysis with Threat Mitigator technology
- Proactive security planning services from a dedicated Trend Micro Threat Management Advisor, including customized corporate threat security management planning, outbreak fire drills, security infrastructure business impact briefings, and security best practices recommendations

KEY BENEFITS

- **Increases protection** by closing gaps in your corporate security with patent-pending, multiprotocol technology to detect malware across 120 protocols
- **Provides greater visibility** into your security posture with continuous threat discovery, early warning notifications, root-cause-analysis, and reporting
- **Reduces management complexity** with Trend Micro's Threat Management Advisors offering proactive security planning recommendations based on over 20 years of experience in the security industry

THE NEED FOR A NETWORK SECURITY OVERWATCH LAYER

After conducting over 100 enterprise network assessments worldwide with Threat Management Services, Trend Micro found:

- 100% of companies had active malware
- 56% of companies had an information-stealing malware
- 72% of companies had one or more IRC bots
- 80% of companies had a malware web download
- 42% of companies had a network worm

Source: Figures calculated from 130 global Threat Discovery Services trials 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.



Comprehensive THREAT LIFECYCLE MANAGEMENT

Complete end-to-end threat infection management

- **Assess:** Discover threats to gain insight into your current security posture
- **Monitor:** Continuously monitor for active, data-stealing malware infections and receive early warning outbreak notifications
- **Diagnose:** Correlate suspicious events and activities on the network to determine steps for effective containment
- **Contain:** Respond to threats and isolate infected systems quickly
- **Remediate:** Conduct network-wide threat remediation with pattern-free clean-up, root-cause analysis, and assistance with the expertise of Trend Micro Threat Management Advisors
- **Learn:** Rely on proactive security advisory services from trusted Trend Micro Threat Management Advisors to prevent security threats

Trend Micro Threat Management Services

As you can see in the chart below, the service packages within Threat Management Services build on each other to progressively reinforce your network security by offering a complete threat lifecycle management experience.

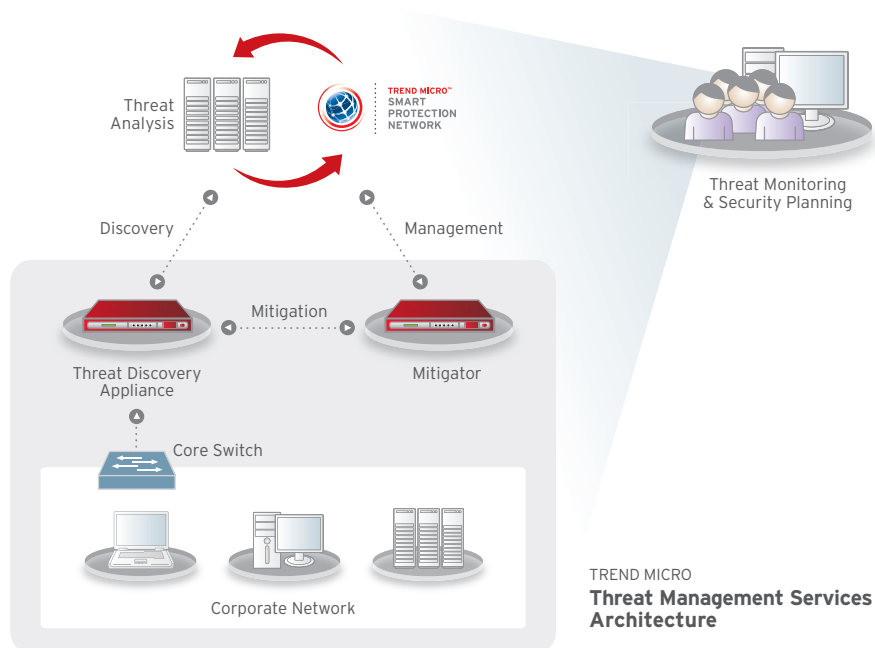
Feature Summary	Benefits	Discovery	Remediation	Lifecycle Management
Network overwatch threat discovery	<ul style="list-style-type: none"> Offers network-wide view of active malware infections Works across 120 different protocols and with Layer 2 to Layer 7 protocol scanning Detects hidden malware attempting to leak data to external parties 	✓	✓	✓
Threat discovery reports	<ul style="list-style-type: none"> Enhances visibility with weekly/monthly executive summary reports Allows real-time access to business risk meters, threat statistics, and infection trends through a threat management portal Improves effective incident response with daily reports 	✓	✓	✓
Advanced cloud correlation with Smart Protection Network	<ul style="list-style-type: none"> Uncovers multi-channel, day-zero threats and conducts threat analysis Performs detailed correlation of large volumes of data to provide actionable threat discovery Helps ensure that analysis includes the most up-to-date threat data 	✓	✓	✓
Out-of-band threat discovery deployment	<ul style="list-style-type: none"> Layers into existing security infrastructure with flexible, out-of-band network placement without affecting network performance 	✓	✓	✓
Proactive threat monitoring and early warning notifications	<ul style="list-style-type: none"> Increases response time for fast management of malware infections Provides constant network monitoring by a trusted partner 		✓	✓
Threat containment and remediation advisory services	<ul style="list-style-type: none"> Assists resource-constrained security staff with infection diagnosis, containment, and cleanup services from expert Threat Management Advisors 		✓	✓
24x7 access to Trend Micro Threat Management Advisors	<ul style="list-style-type: none"> Helps ensure peace of mind with 24x7 access to Trend Micro security professionals 		✓	✓
Threat infection root-cause analysis	<ul style="list-style-type: none"> Pinpoints malware infection channels Breaks the infection chain Enables your company to make behavioral security adjustments 			✓
Automated pattern-free remediation	<ul style="list-style-type: none"> Speeds response time with advanced forensic techniques that locate and eliminate day-zero malware without requiring any pattern or signature updates Uses intelligent trace logic to clean up endpoints containing more than one malware infection 			✓
Annual threat landscape update briefings	<ul style="list-style-type: none"> Provides the latest technical information on threat landscape changes Details new trends in threats and technology Facilitates ongoing security planning 			✓
Bi-annual threat outbreak drills	<ul style="list-style-type: none"> Tests outbreak handling processes and procedures Increases business preparedness and response time Facilitates development of organizational best practices 			✓

➔ Trend Micro Threat Management Services

COMPLETE ENTERPRISE SECURITY SOLUTIONS

Threat Management Services is part of Trend Micro Enterprise Security, a tightly integrated offering of content security products, services, and solutions optimized to deliver immediate protection—all with the goal of reducing the time, risk, and costs associated with acquiring, deploying, and managing content security.

HOW THREAT MANAGEMENT SERVICES WORKS



Threat Management Services uses the Trend Micro Threat Discovery Appliance to discover malware that has evaded detection. The appliance is deployed out of band at the network layer on the core switch, where it can monitor the stealth techniques being used by modern malware.

Capable of analyzing traffic up to the application layer across 120 different protocols, the Threat Discovery Appliance not only detects malware but also the mechanisms used by malware to propagate, including:

- Malware downloading additional components and updates
- Malware receiving and executing commands
- Malware transferring stolen information

A powerful combination of Trend Micro's scanning engines and technologies

When traffic is received by the Threat Discovery Appliance, a multi-step process occurs:

- Trend Micro file scanning engine determines if a file is known or new malware
- Trend Micro Web Reputation technology identifies malicious URLs
- Trend Micro Virus Scanning Engine checks the traffic stream for exploits and network worms
- Trend Micro Network Content Inspection Engine correlates network traffic attributes to identify potentially malicious characteristics and behavior
- The appliance works with in-the-cloud servers and the Trend Micro Smart Protection Network to perform advanced correlation on information from multiple sessions

Trend Micro Threat Management Services

Removing the infection—and determining the cause

Once a threat is uncovered, the Threat Discovery Appliance sends a message to the Threat Mitigator, which will initiate a revolutionary pattern-free cleanup. The Threat Mitigator first removes the files and malware processes associated with the infection, then identifies the chain of events that led to the infection with a detailed root-cause analysis; for example, the report may point to a malicious website download or an infected USB stick.

Gain greater visibility through reporting

Comprehensive reports provide valuable insight into your security posture, including:

- Malicious activity detected
- IP address of the hosts infected
- Frequency of incidents and the departments or network domains affected

Expert advisors help you take the next steps toward improved security

If the Threat Mitigator is unable to clean the infection, it automatically sends all of the necessary forensic file data from the infected machines to the Trend Micro Threat Management Advisors. This team of seasoned security experts can then initiate an early warning communication in conjunction with diagnosis and remediation advisory services—helping you save valuable time.

As part of the infection learning phase, Trend Micro Threat Management Advisors provide proactive security planning services, including:

- Customized corporate threat security management planning
- Outbreak fire drills
- Security infrastructure business impact briefings
- Security best practices recommendations

Throughout this process of discovering and remediating network infections, you gain a crucial advantage—greater insight into your security posture.

To learn more about Trend Micro Threat Management Services, contact your Trend Micro representative or obtain our contact details online at <http://us.trendmicro.com/us/about-us/contact/index.html>

