Trend Micro™ Threat Management Services
Frequently Asked Questions

External FAQ:
Trend Micro™ Threat Management Services

Last updated: September 10, 2009

GENERAL QUESTIONS

Q: What is Threat Management Services?

A: For enterprises that need a way to discover and remediate stealthy malware infections such as targeted, data-stealing threats that have evaded detection, Threat Management Services is a network security overwatch service that provides an additional security layer in order to strengthen an organization's existing security infrastructure with threat discovery, containment, and remediation services.

Unlike security solutions that are unaware of active data-stealing malware infiltrations within the network, Trend Micro Threat Management Services helps ensure ultimate protection of corporate assets with increased protection, greater visibility, and less management complexity.

Q: What security issues does this service address?

A: As malware threats become more sophisticated and workplace data leaks grow more prevalent, it is apparent that today's threats are finding new ways to evade detection from the organization's existing security infrastructure.

When a malware infection successfully bypasses detection, the security solution(s) that missed the detection don't sound warning alarms that they missed something. As a result, enterprises find it difficult to gain comprehensive, corporate-wide visibility into malware infections lurking within the network. With Threat Management Services, customers gain visibility into their ongoing security posture along with proactive monitoring, early warning, containment, and remediation services.

Q: What are the unique benefits of Threat Management Services?

A: Threat Management Services provides:

- **Increased Protection** with an additional layer of security that closes the existing corporate security gap with a network security overwatch service. With Threat Management Services, organizations have a faster response to infection containment and remediation along with proactive security planning through the Trend Micro Threat Management Advisors.
- **Greater Visibility** into the organization's security posture with continuous threat discovery reporting and proactive early warning notifications.
- **Less Management Complexity** with Trend Micro's Threat Management Advisors, who offer 20 years of experience in the security industry to help you proactively plan your security.

Q: What are the package options for Threat Management Services?

A: Trend Micro Threat Management Services is the umbrella brand name for the services line, which consists of three services package offerings.

- **Trend Micro Threat Discovery Services:**
  A network security overwatch service that strengthens an organization’s existing security infrastructure by providing 24x7 monitoring and discovery of stealthy threats that have evaded detection.

- **Trend Micro Threat Remediation services:**
  Includes the Threat Discovery Services features as well as adds 24x7 monitoring, proactive early warning notifications, and remediation advisory services. 24x7 remediation is provided by Trend Micro expert Threat Management Advisors working proactively to monitor the threat discovery reports for security breaches. Upon detection of a security event, customers will be notified with an early warning alert and be provided remediation advisory services.

- **Trend Micro Threat Lifecycle Management Services:**
  Encompasses features in the previous packages and extends them to include automated threat remediation and root-cause analysis with Threat Mitigator technology. These services are coupled with security advisory from a dedicated Trend Micro Threat Management Advisor, who offers customized corporate threat security management planning, outbreak drills, infrastructure business impact briefings, and recommendations on best practices.

Q: What are the feature differences between the package offerings?

Feature	**Service**		
	Threat Discovery	**Threat Remediation**	**Threat Lifecycle Management**
Network overwatch threat discovery	✓	✓	✓
Network security assessment reports (manual – daily / weekly)	✓	✓	✓
Proactive threat monitoring & early warning notifications		✓	✓
Threat containment and remediation advisory services		✓	✓
24x7 access to Trend Micro Threat Management Advisors		✓	✓
Automated threat remediation technology			✓
Threat infection root-cause analysis			✓
Bi-annual threat outbreak drills for best practice responses			✓
Customized Threat Security Management Plan			✓
Quarterly Executive Business Review			✓
Annual threat landscape updates briefings			✓

Q: How will Threat Management Services help me measure my overall security effectiveness?

A: Threat Management Services removes the guesswork in measuring an organization’s security effectiveness. With Threat Discovery Reports, customers gain insight into what threats are being missed by the existing security infrastructure, including business risk profile, affected assets, infection sources, and threat statistics. With quarterly business reviews, organizations will gain further insight into their security effectiveness with detailed analysis provided by Threat Management Advisors.

When a malware infection successfully bypasses detection, the security solution(s) that missed the detection don't sound warning alarms that they missed something. As a result, enterprises find it difficult to gain comprehensive, corporate-wide visibility into malware infections lurking within the network. With Threat Management Services, customers gain visibility into their ongoing security posture along with proactive monitoring, early warning, containment, and remediation services.

Q: What are the service level standards for Threat Management Services?

A: Customers who choose Trend Micro Threat Lifecycle Management Services can expect a Threat Management Advisor to contact them within two (2) hours of receiving a notification of a high-profile malware alert to follow up on necessary activities and recommendations. Threat Remediation Services customers can expect a follow-up with one (1) business day.

Q: What type of organization would need Threat Management Services?

A: Threat Management Services is ideal for enterprise organizations with 1,000+ employees who are looking for better oversight, visibility, and management of unknown threat infections. Regardless of your business focus, all industries benefit from TMS helping to ensure ultimate protection of your corporate assets.

Q: What if I don't think I have any unknown threats lurking in my network?

A: Of course, with a top-rated security infrastructure, it is completely natural to wonder if Threat Management Services can provide enterprises greater protection and additional value. Customers who have taken the next steps to introduce a network security overwatch service with Threat Management Services have been greatly impressed with the discovery of unknown threats, the greater visibility gained, and the proactive security planning that is made possible by this additional insight into your network.

The proof of the value can be found in the results. Threat Management Services assessment trials have been performed worldwide on enterprises ranging from 1,000 to 80,000 employees and discovered that:

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

Q: Is it possible to trial Threat Management Services?

A: Absolutely. Interested and qualified customers can conduct a zero-obligation, 2-week trial of Trend Micro Threat Discovery Services. At the completion of the trial assessment period, customers will receive a customized executive summary report. A sample report can be viewed here. If you would like to begin a trial assessment of Threat Discovery Services, please contact your channel partner or a Trend Micro sales representative. You can obtain Trend Micro contact details at www.trendmicro.com.

Q: How do I get pricing information?

A: Please contact a channel partner or sales representative in your region for specific pricing. Trend Micro contact information can be found on our website at www.trendmicro.com.

Q: Can I purchase Threat Management Services through my preferred channel partner?

A: Yes. Threat Management Services can be purchased through your channel partner, provided they have a channel partner contract with Trend Micro. If you would like to find a certified Trend Micro partner, please visit our website at http://channelpartner.trendmicro.com/index.htm.

Threat Discovery Services Package

Q: How does the underlying technology of Threat Discovery Services work?

A: The Threat Discovery Appliance is deployed at the network layer on the core switch, where it is immune to most of the stealth techniques being used by modern malware to evade desktop-based antivirus such as rootkits, disabling antivirus, and host redirection. The appliance therefore provides maximum visibility of outbound traffic from endpoints to the Internet. Capable of analyzing traffic up to the application layer, the Threat Discovery Appliance detects malware as it utilizes the internet for malicious activities such as propagation, downloading additional components and updates, receiving commands, and transferring stolen information. It not only detects malware but also the vectors and mechanisms used by malware to propagate and communicate—including malicious emails, web threats, and exploits.

Traffic received by the Threat Discovery Appliance is analyzed using a combination of Trend Micro's most powerful scanning engines and technologies:

- Trend Micro's file scanning engine determines if a file is known or new malware
- The Trend Micro Web Reputation database identifies malicious URLs
- The Trend Micro Virus Scanning Engine checks the traffic stream for exploits and network worms
- If all these checks fail to detect anything malicious, the Trend Micro Network Content Inspection Engine will correlate the different attributes of the network traffic to identify potentially malicious characteristics and behavior.

The Threat Discovery Appliance works in collaboration with in-the-cloud servers to perform advanced correlation on information from multiple sessions. By integrating with Trend Micro Smart Protection Network™, the most up-to-date threat data is analyzed for superior threat detection.

Threat Remediation Services Package

Q: Who are the Trend Micro Threat Management Advisors?

A: The Threat Remediation Services and Threat Lifecycle Management Services feature additional value provided by the expertise of Trend Micro Threat Management Advisors who will help you manage your threat infections as well as provide proactive security planning. The Threat Management Advisors have a wealth of security expertise based on Trend Micro's 20+ years in the security industry.

Q: How can I access my Trend Micro Threat Management Advisor?

A: As part of the process to set up your new network security overwatch service, you will be provided contact details for the Threat Management Advisors. This team of professionals is staffed around the globe to provide you 24x7 assistance.

Q: How do the threat monitoring and early warning notifications work?

A: Trend Micro Threat Remediation Services offers the added benefits of knowing that Trend Micro is helping to monitor your network for infections. With assistance from the security experts at TrendLabs, we are able to comprehensively monitor the wider threat landscape for emerging threats on a 24-hour basis, providing you with early warning notifications as outbreaks occur.

Q: How will Trend Micro help me with remediation advisory services?

A: Whether you are an existing Trend customer or a new customer strengthening your security with Threat Management Services, you will gain the additional resource support of Threat Management Advisors helping you remediate your network from the infections found through the Threat Discovery Technology. By reviewing the details of the Threat Discovery Services reports that are sent to the Threat Management Advisors, your specialized Advisor can help you contain the outbreak, investigate the root cause (including where it has spread within the network), and assist with remediation.

Threat Lifecycle Management Services Package

Q: I understand that Threat Lifecycle Management Services introduces a technology that does more automated infection remediation. How does it work?

A: With the introduction of revolutionary root-cause analysis based on known malware behavior, the Threat Migitator technology available in the Threat Lifecycle Management Services package helps reduce the complexity of managing malware infection remediation. Threat infection root-cause analysis helps customers understand why the infection happened, ensures that the infection chain is broken, and enables enterprises to make security adjustments based on behaviors leading to infections. The Threat Mitigator's pattern-free cleanup helps ensure faster and more effective remediation with less complexity – providing your organization with a more cost-effective way to respond to infections.

Q: How does Threat Lifecycle Management Services help me with more proactive security planning?

A: The Threat Lifecycle Management Services introduces additional security services provided by Threat Management Advisors, including the creation of an annual threat lifecycle management plan, bi-annual outbreak drills, and recommendations on best practices. The Threat Lifecycle Management Services security services are customized to your specific business environment and include quarterly security infrastructure briefings with your Threat Management Advisor. These quarterly briefings are designed to provide deeper analysis of your threat infections and greater insight into proactive measures that can be taken to close any existing infection entry-points.

Q: What are the outbreak drills?

A: When a malware outbreak takes place, organizations can potentially go into a "fire drill" mode without a clear understanding of who they should notify or how to proceed. Likewise, the process of determining if your customers need to be notified can also be quite extensive and unclear. With the introduction of bi-annual outbreak drills to your security planning, Threat Management Advisors will help your enterprise build a clearly outlined and detailed process to follow when there is an infection. The outbreak process will be customized for your organization, and we will begin the process by drafting a plan with your team. Following the plan creation, we will support you in training your team and corporate sponsors on the process. Following the training, our TMAs will help you conduct "live" outbreak drills twice a year to measure the effectiveness of the drill as well as help analyze any adjustments that may be necessary.