TREND MICRO™ **Threat Management Services**

Security Threat Assessment

The Security Threat Assessment is a valuable and insightful opportunity for you to evaluate the effectiveness of your current security infrastructure. Want to know if malware has infiltrated your systems? If sensitive data is being lost? The true measure of your endpoint, web, and messaging security? In just two weeks, Trend Micro can reveal the answers in a customized executive report.

The Security Threat Assessment reveals your true security posture by detecting both active and potential threats that are evading your existing security measures. Our Security Threat Assessment uses non-invasive technology and the Trend Micro™ Smart Protection Network to provide an informative risk report that reveals the following information:

- Active malware infiltrations
- Infection points
- Threat exposure levels
- Sensitive data loss
- Potential compliance violations

TODAY'S INTERNET SECURITY ENVIRONMENT

In the last few years, conventional security solutions have struggled to protect against increasingly targeted malware attacks. Today's threats are multi-dimensional, coordinated attacks that are particularly dangerous because they are specifically designed to go undetected while they systematically steal sensitive data that can result in:

- Loss of confidential customer data
- Loss of intellectual property
- Regulatory violations
- Downtime, reduced productivity, and loss of revenue
- Damage to your company reputation and diminished customer loyalty
- Exposure to fines and litigation

Once cybercriminals infiltrate your network, your company's sensitive data can be quickly dispersed to organized criminal networks around the world.

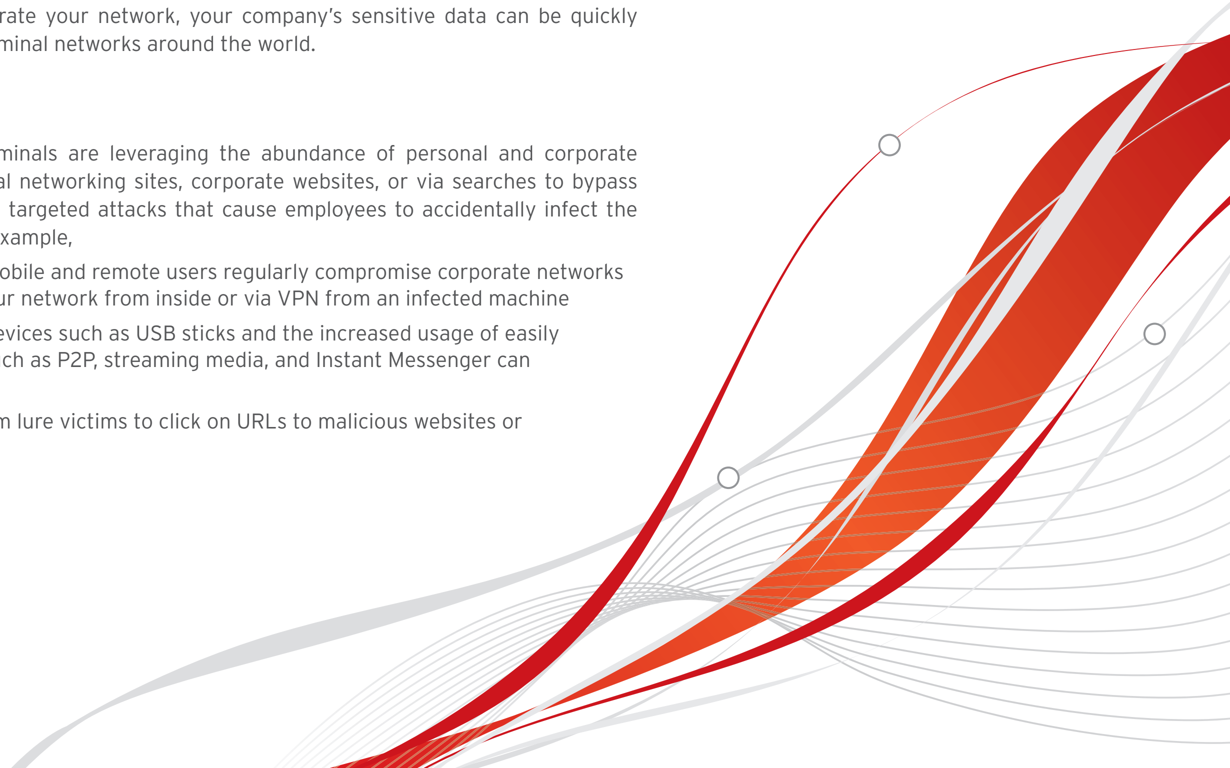
TARGETED ATTACKS

More and more, cybercriminals are leveraging the abundance of personal and corporate information found in social networking sites, corporate websites, or via searches to bypass security mechanisms with targeted attacks that cause employees to accidentally infect the network from within. For example,

- Increasing numbers of mobile and remote users regularly compromise corporate networks when they connect to your network from inside or via VPN from an infected machine
- Portable mass storage devices such as USB sticks and the increased usage of easily exploited technologies such as P2P, streaming media, and Instant Messenger can give threats entry
- Targeted emails and spam lure victims to click on URLs to malicious websites or malware attachments

THREAT MANAGEMENT SERVICES

The Security Threat Assessment is enabled by the Trend Micro Threat Discovery Appliance, a key component of Trend Micro Threat Management Services. Threat Management Services is a network security overwatch service that provides an additional security layer that strengthens an organization's existing security infrastructure against data-stealing malware threats that have evaded detection. It monitors the corporate network for threatening malware activity and delivers discovery, containment, and remediation services that provide a last line of defense for your valuable data and resources.



PUT YOUR SECURITY SYSTEM TO THE TEST

Over 100 Security Threat Assessments on enterprises worldwide have shown:

- 100% of companies had active malware
- 56% of companies had information-stealing malware
- 72% of companies had one or more IRC bots
- 80% of companies had malware web downloads
- 42% of companies had one or more network worms

Source: Figures calculated from 130 global Security Threat Assessments through August 2009. Companies had an average of 7,484 employees and included representatives from the manufacturing, government, education, financial services, retail, and healthcare sectors.

Want to know how your current security infrastructure is performing? Find out with the Security Threat Assessment.

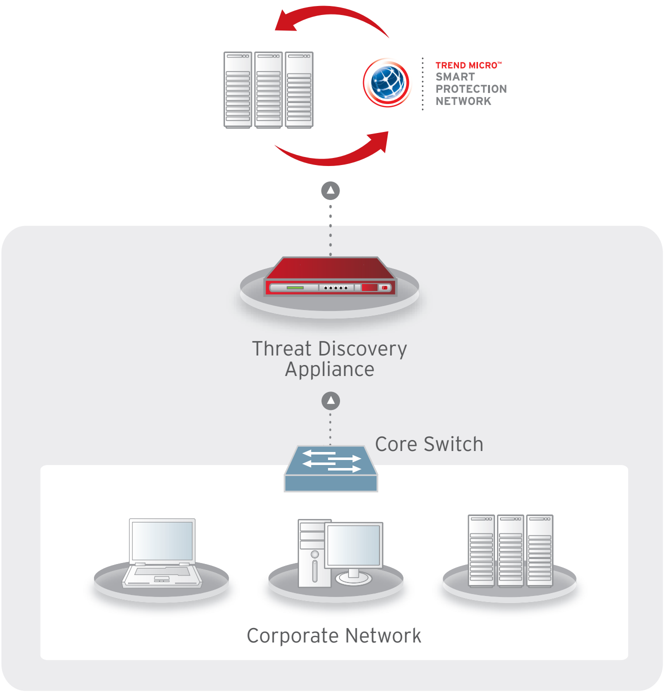
INSTALLATION

The Security Threat Assessment utilizes the non-invasive, listen-only technology of the Threat Discovery Appliance. In just one hour, one of our engineers will install the TDA on your network. The appliance is deployed out of band at the core switch as a smart network sniffer, where it can monitor the stealth techniques being used by modern malware. The TDA is passive, meaning that it:

- Does not interfere with network operations
- Does not write anything
- Only listens to mirrored traffic

OPERATION

Capable of analyzing traffic up to the application layer across 120 different protocols known to be used by malware, the TDA detects malware as it utilizes the internet for malicious activities such as propagation, downloading 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.



CASE STUDIES

Even in the presence of the most current industry standard security technology, 100% of participants to date have discovered unknown threats in their network.

Insurance company discovers its own lack of coverage

- 16,000 employees

A major insurer in Canada had utmost confidence in their updated security and reporting solution. Trend Micro tested only 400 of their endpoints and discovered:

- 13 instances of generic malware
- 1,247 malicious URL visits
- 53 malware downloads
- 584 malicious emails

Their security needed to be re-engineered

- 25,000 employees

This prestigious Australian engineering firm knew that its network was infected—but our competitor's reporting feature couldn't identify the origin or the extent of the infection. We assessed 1,000 endpoints and pinpointed numerous infections down to the IP addresses, including:

- 12 network worms
- 5 IRC bots
- 1,206 malicious URL visits
- 32 malware downloads

Traffic received by the TDA is analyzed using a combination of Trend Micro's most powerful scanning engines and Smart Protection Network 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 TDA works in collaboration with in-the-cloud servers to perform advanced correlation on information from multiple sessions. By integrating with the Trend Micro Smart Protection Network, the most up-to-date threat data is analyzed for superior threat detection.

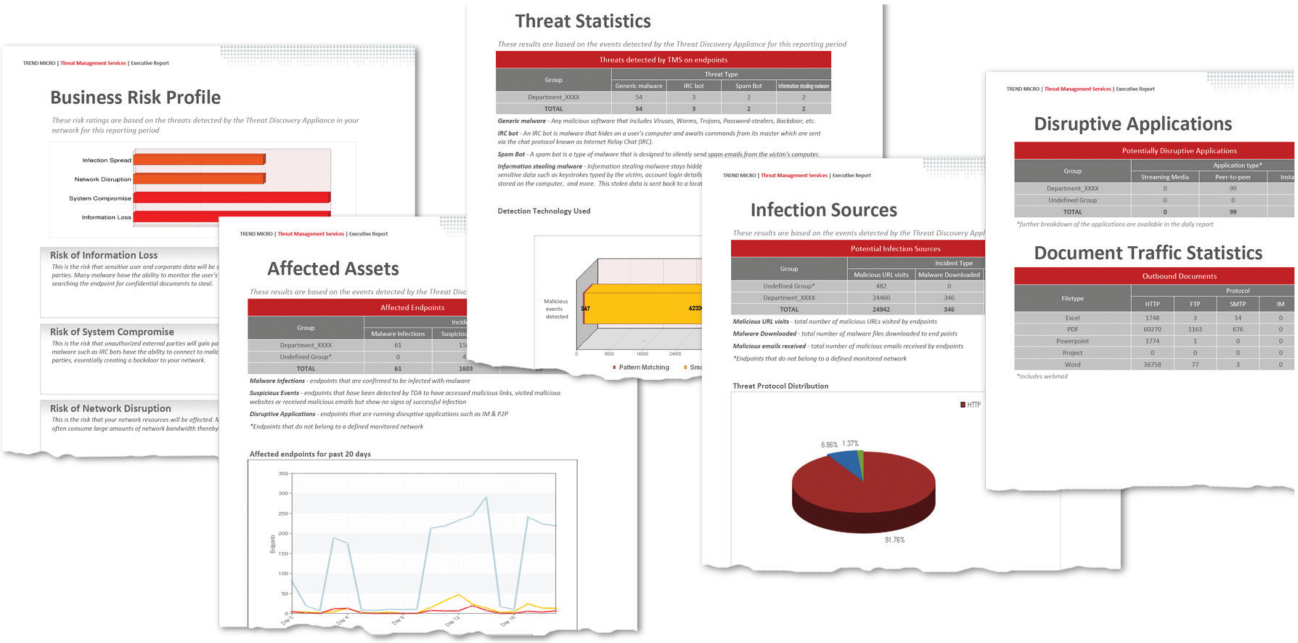
> “70% of SMEs enter 2009 with networks at risk of a security breach, and 57% of IT managers are not confident that their organization knows the state of every endpoint that connects to their network.”
>
> **Market Wire**
> December 2008

REPORTING

At the end of the two weeks, you'll receive a comprehensive security assessment report that details:

- **Business Risk Meters:** risks associated with detected threats
- **Affected Assets:** groups and endpoints affected by threats
- **Threat Statistics:** malware types found in the network
- **Infection Sources:** where the malware is coming from
- **Disruptive Applications:** which applications are causing the most problems
- **Trends:** trends of threats/events within your company

Download a sample report ››



TREND MICRO | Threat Management Services | Executive Report

Business Risk Profile

These risk ratings are based on the threats detected by the Threat Discovery Appliance in your network for this reporting period

Risk of Information Loss

This is the risk that sensitive user and corporate data will be s… parties. Many malware have the ability to monitor the user's … searching the endpoint for confidential documents to steal.

Risk of System Compromise

This is the risk that unauthorized external parties will gain pa… malware such as IRC bots have the ability to connect to malic… parties, essentially creating a backdoor to your network.

Risk of Network Disruption

This is the risk that your network resources will be affected. N… often consume large amounts of network bandwidth thereby

TREND MICRO | Threat Management Services | Executive Report

Affected Assets

These results are based on the events detected by the Threat Disc…

Affected Endpoints

Group	Malware Infections
Department_XXXX	61
Undefined Group*	0
TOTAL	**61**

Malware Infections *- endpoints that are confirmed to be infected with malware*

Suspicious Events *- endpoints that have been detected by TDA to have accessed malicious links, visited malicious websites or received malicious emails but show no signs of successful infection*

Disruptive Applications *- endpoints that are running disruptive applications such as IM & P2P*

**Endpoints that do not belong to a defined monitored network*

Affected endpoints for past 20 days

Threat Statistics

These results are based on the events detected by the Threat Discovery Appliance for this reporting period

Threats detected by TMS on endpoints

Group	Threat Type			
	Generic malware	IRC bot	Spam Bot	Information stealing malware
Department_XXXX	54	3	2	2
TOTAL	**54**	**3**	**2**	**2**

Generic malware *- Any malicious software that includes Viruses, Worms, Trojans, Password-stealers, Backdoor, etc.*

IRC bot *- An IRC bot is malware that hides on a user's computer and awaits commands from its master which are sent via the chat protocol known as Internet Relay Chat (IRC).*

Spam Bot *- A spam bot is a type of malware that is designed to silently send spam emails from the victim's computer.*

Information stealing malware *- Information stealing malware stays hidde… sensitive data such as keystrokes typed by the victim, account login details… stored on the computer, and more. This stolen data is sent back to a locat…*

Detection Technology Used

TREND MICRO | Threat Management Services | Executive Report

Infection Sources

These results are based on the events detected by the Threat Discovery Appl…

Potential Infection Sources

Group	Incident Type	
	Malicious URL visits	Malware Downloaded
Undefined Group*	482	0
Department_XXXX	24460	346
TOTAL	**24942**	**346**

Malicious URL visits *- total number of malicious URLs visited by endpoints*

Malware Downloaded *- total number of malware files downloaded to end points*

Malicious emails received *- total number of malicious emails received by endpoints*

**Endpoints that do not belong to a defined monitored network*

Threat Protocol Distribution

TREND MICRO | Threat Management Services | Executive Report

Disruptive Applications

Potentially Disruptive Applications

Group	Application type*	
	Streaming Media	Peer-to-peer
Department_XXXX	0	99
Undefined Group	0	0
TOTAL	**0**	**99**

**further breakdown of the applications are available in the daily report*

Document Traffic Statistics

Outbound Documents

Filetype	Protocol			
	HTTP	FTP	SMTP	IM
Excel	1748	3	14	0
PDF	60270	1163	676	0
Powerpoint	1774	1	0	0
Project	0	0	0	0
Word	36758	77	3	0

**includes webmail*

This revealing report will allow you to:

- **Examine** potential vectors of infection
- **Identify** malware, information stealers, affected assets, infection sources, and disruptive applications
- **Uncover** sensitive data loss and regulatory compliance violations
- **Pinpoint** specific problem areas by IP address
- **Evaluate** the effectiveness of your web, messaging, and endpoint security
- **Increase** visibility into your security so that you can better understand how the threats occurred, where they entered your network, and how to fill your security gaps

THE SECURITY THREAT ASSESSMENT DETECTS THE FOLLOWING THREATS:

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

WHO QUALIFIES?

No matter where you are in the threat cycle, you'll find this non-intrusive assessment insightful—even shocking.

If you meet these criteria, you can get started right away:

- You must have a minimum of 1,000 endpoints visible to the core switch
- You must be willing to meet with a Trend Micro Security Specialist to review your network security results at the completion of the assessment

Secure
Jack believes his enterprise security system is watertight. But is he really safe?

Infected
Sam knows the network is infected, but how bad is the damage?

Recovering
Scott is in recovery mode, but are all the endpoints fully cleaned-up?

GETTING STARTED COULDN'T BE EASIER

Trend Micro makes it easy for you to take advantage of this valuable opportunity:

1. Complete and return our **evaluation agreement**
2. Complete and return our **scoping document** detailing your network information
3. **Grant us permission to connect** to the mirror or SPAN port of your core switch
4. **Schedule about one hour** for our Sales Engineer to install the Threat Discovery Appliance and allow it to gather information for two weeks

At the end of the two weeks, you'll get the opportunity to review your executive threat report with a Trend Micro Security Specialist, who will also provide recommendations on how you can improve your security posture. Armed with detailed threat intelligence, you can make more informed decisions that will enable your enterprise to deploy the best security infrastructure possible.

To learn more about Trend Micro Threat Management Services and to get started with your Security Threat Assessment, contact your Trend Micro representative or obtain our contact details online at **http://us.trendmicro.com/us/about-us/contact/index.html**.

[DS02_TMS_Assessment091007US]