

Network VirusWall



Trend Micro™ Sales Training Module

Press <Page Down> to Advance to Next Slide

Welcome to Trend Micro's **Network VirusWall** Sales Training Module!

Trend Micro's sales training modules are designed with the sales professional in mind and will help you do the following:

1. Understand Trend Micro's award-winning security solutions
2. Position these solutions in your selling efforts
3. Better Sell these solutions to your customers

Following this course, you should be better prepared to address the virus and Internet content security threats facing your customers and provide your customers with the information and technology they need to respond to these threats.


This training module has been designed to be taken instructor-led or as a self-paced “independent study” training module. If you are taking this course independent study, there’s a few things you should know....

Prerequisite: The Trend Micro Foundation Course

Length: Approximately 45 minutes, depending on your reading speed

Format: Adobe Acrobat PDF format

Testing: 15 question certification exam available online, details to follow

In addition, “Notes from the Instructor” have been provided throughout the course in the form of standard PDF notes. To view these notes, just place your mouse over or select the  symbol that appears throughout this training module. *Try it on this page!*

As one of Trend Micro's official certification modules, this course can move you closer to receiving your status as a Trend Micro Certified Salesperson (TMCS) or as a Trend Micro Certified Sales Specialist (TMCS Specialist).

TMCS Requirements

Trend Micro Foundation Course
Any Four Certification Modules

TMCS Specialist Requirements

Trend Micro Foundation Course
Any Eight Certification Modules

Why get certified with Trend Micro?

- Credibility as a specialist in the security space
- Confidence in working with your customers
- Information on the latest-and-greatest coming out of Trend Micro
- Sales Opportunities and Promotions specific to TM Certified Salespeople





1.

Understanding the Technology

- The Problem
- The Trend Micro Solution
 - Elevator Pitch
 - Product Overview

2.

Positioning the Product

- Leverage Points
- Understanding the EPS
- Market Opportunity
- Target Customers
- Competitive Positioning

3.

Selling the Solution

- Summary of Key Selling Points
- Handling Objections
- Product Licensing Model



1.

Understanding the Technology

- The Problem
- The Trend Micro Solution
 - Elevator Pitch
 - Product Overview

2.

Positioning the Product

- Leverage Points
- Understanding the EPS
- Market Opportunity
- Target Customers
- Competitive Positioning

3.

Selling the Solution

- Summary of Key Selling Points
- Handling Objections
- Product Licensing Model

Network Viruses and Worms: Rampant and Virtually Unstoppable

Network viruses (e.g., Internet worms like *Sasser*) are viruses that propagate from machine to machine at the network layer. Over the last couple of years, these viruses have become rampant and virtually unstoppable due to an increasing number of software vulnerabilities. ?



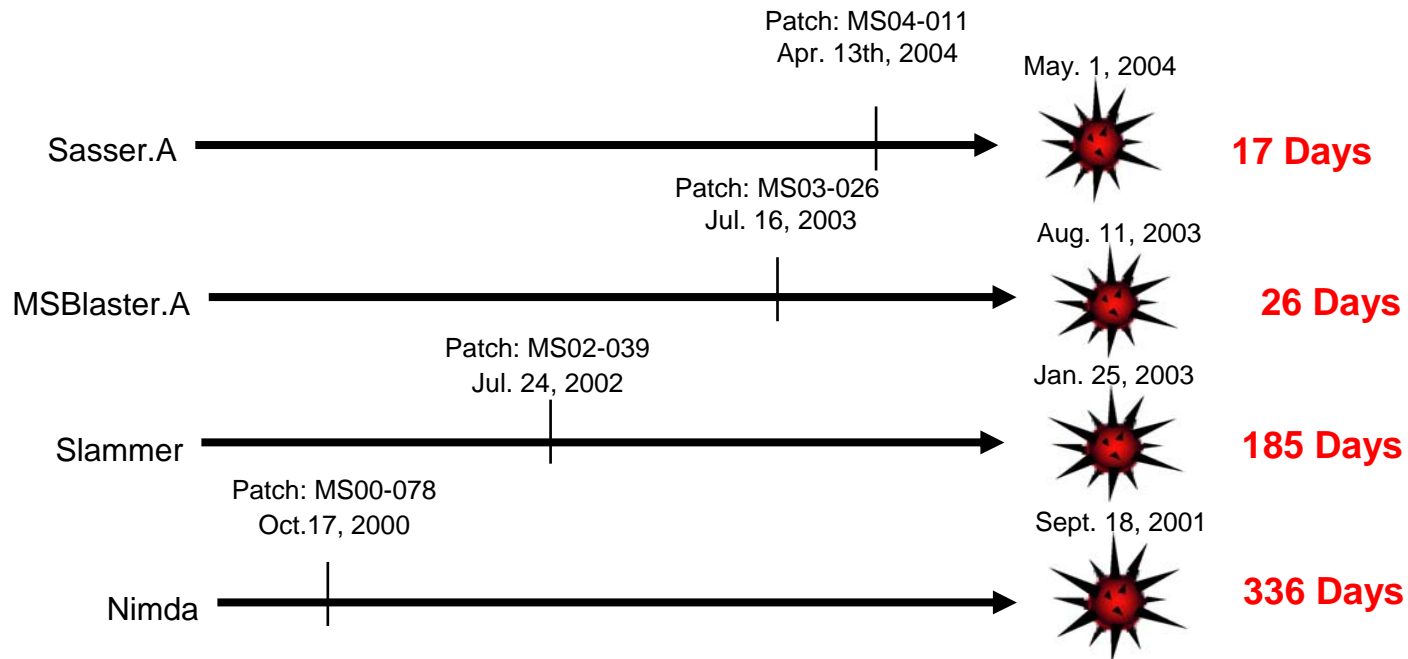
Traditional Methods of Detection, Prevention and Cleanup Aren't Working

Current security solutions such as antivirus, firewall, vulnerability assessment, and intrusion detection and prevention systems are unable to stop these network viruses and as a result the estimated worldwide damages from worms such as SQL Slammer, MSBlaster.A, and Nachi skyrocketed to \$2.15B in 2003*.





The Patching Approach Has Also Proven Futile...



The time window from patch availability to outbreak is becoming shorter and shorter...

Unprotected and Unmanaged Devices Accessing the Network Exacerbates the Problem

The network virus problem is exacerbated by a growing number of unprotected and unmanaged devices accessing the network from multiple entry points.

THE PROBLEM

Specific Issues and their Impact

Sales Training Module for Network VirusWall

Issue

Business Impact

Security gaps from not confirming that every system has been properly installed and configured with current antivirus



Employee Productivity Reduced
Business Operations Disrupted
IT Costs Increased

System-wide outbreak from not containing the spread of a new attack before a pattern file exists



Increased IT Expenses
IT Productivity Reduced
Employee Productivity Reduced
Business Operations Disrupted

Eradicating new viruses using manual/slow processes



IT Costs Increased
IT Productivity Reduced
Business Opportunities Endangered or Lost

System-wide re-infection after the initial clean process



IT Costs Increased
IT Productivity Reduced
Employee Productivity Reduced
Business Operations Disrupted
Business Opportunities Endangered or Lost



Network VirusWall is **an outbreak prevention appliance that helps organizations stop network viruses** (e.g., Internet worms), block high threat vulnerabilities during outbreaks, and quarantine and clean up infection sources including unprotected devices as they enter the network.

Unlike security solutions that only monitor threats or provide threat information, Network VirusWall helps organizations take precise outbreak security actions and proactively detect, prevent, contain, and eliminate outbreaks.





- **Network Virus/Network Worm Outbreak Prevention***

- Helps prevent network viruses and worms with threat-specific prevention policies from TrendLabs that can be deployed in the network LAN segment to block the spread of the virus through file transfers, instant messaging, etc. 
- Isolates and contains the spread of infections by not allowing infections in or out of the affected LAN segment, thereby keeping the rest of the network up and running 

- **Monitoring the Network and Providing Early Warning**



- Provides early warning of outbreaks in the network segment(s) using heuristics ?
- Monitoring methods include the following:
 - analyzing traffic flow delta
 - number of connections initiated to and from a single client
 - sudden increases in traffic through specific ports or protocols (TCP, UDP, ICMP, and IGMP) ?

• Security Policy Enforcement

- Enables organizations to enforce antivirus security policies and minimize network infections and re-infections by doing the following:
 - Detecting antivirus client products, scan engines and pattern files as users access the network and blocking network access if the antivirus protection is not in compliance
 - Enabling users to update their antivirus scan engine and pattern files or download an antivirus product per the company's security policies



- **Network Scanning and Detection**

- Scans and detects network viruses and worms using network signatures from TrendLabs. Infected packets are dropped. (Traditional antivirus products scan for viruses only at the application layer and not the network layer.)





• **Automated Damage Cleanup***

- Sources of infection on the network are targeted and isolated until cleanup
- Automated agentless, remote cleanup of infected host machines with damage cleanup templates from TrendLabs
- Damage cleanup includes the fixing of unwanted registry entries, memory resident code, garbage and viral file drops as well as system files such as system.ini after it has been infected or altered by the virus



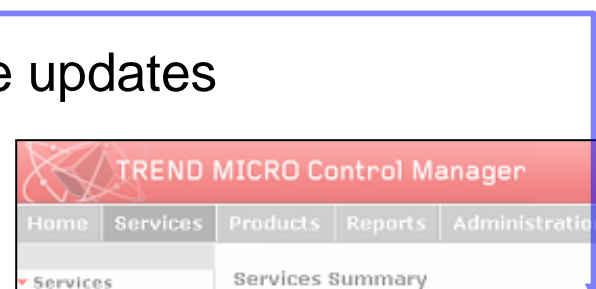
- **Vulnerability Isolation using Trend Micro Vulnerability Assessment***

- Allows the administrator to selectively isolate vulnerable/unpatched machines
- Minimizes network traffic congestion by not allowing unpatched machines to infect machines in other network segments





- TrendLabs Message Board
 - view status of any new service updates
 - Vulnerability Pattern
 - Outbreak Prevention Policy
 - Virus Pattern
 - Network Signatures
 - Scan Engine
 - Damage Cleanup Template



TREND MICRO Control Manager Signed in as: guest | Sign Out

Home Services Products Reports Administration

Services Summary

Date / Time	Notification
May 25, 2003 15:15 GMT	Posted Outbreak Prevention Policy for Worm_Lovegate.F
May 25, 2003 14:40 GMT	Posted Virus Pattern file 544
May 23, 2003 07:45 GMT	Posted Scan Engine v6.510
May 22, 2003 14:23 GMT	Posted Damage Cleanup Pattern 108

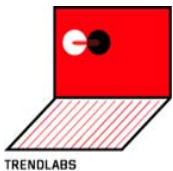
Outbreak Prevention Service **Activated**

Outbreak Prevention Policy: Worm_Lovegate.F
Last prevention task performed: Work_Klez
Last policy download: May 25, 2003 15:30
Scheduled policy download: On (Next download: May 26, 2003 15:30) [Download Now...](#)
Automatic policy deployment: On

Damage Cleanup Service **Activated**

Damage cleanup pattern: 108
Damage cleanup engine: 3.5
Scheduled pattern download: On (Next download: May 26, 2003 18:30) [Download Now...](#)
Current damage cleanup: Taipei-Marketing cleanup (started: May 25, 2003 16:30)

TrendLabs



May 25, 2003 15:15 GMT
Posted Outbreak Prevention Policy for Worm_Lovegate.F





1.

Understanding the Technology

- The Problem
- The Trend Micro Solution
 - *Elevator Pitch*
 - *Product Overview*

2.

Positioning the Product

- Leverage Points
- Understanding EPS
- Market Opportunity
- Target Customers
- Competitive Positioning

3.

Selling the Solution

- Summary of Key Selling Points
- Handling Objections
- Product Licensing Model





- **Trend Micro's Corporate Size, Stability and Reputation**
 - Enterprise-ready security solutions for over 14 years
- **Trend Micro's Enterprise Protection Strategy**
 - A comprehensive end-to-end, layered approach to assessing vulnerabilities, preventing outbreaks, responding to viruses and restoring systems to health
- **Trend Micro's Technology Leadership**
 - #1 market share in the server/Internet gateway category
 - First-to-market with server and gateway protection products



- Network VirusWall extends Cisco NAC's security enforcement promise with a broader scope and threat-specific policies
- Long term: Trend Micro security services integration into Cisco infrastructure

Problems Solved	Cisco NAC	Network VirusWall
Vulnerability Isolation		<input checked="" type="checkbox"/>
Network Virus Outbreak Prevention		<input checked="" type="checkbox"/>
Network Virus Detection		<input checked="" type="checkbox"/>
Infection Locator/Automated Cleanup		<input checked="" type="checkbox"/>
Security Policy Enforcement	<input checked="" type="checkbox"/> <i>partial</i>	<input checked="" type="checkbox"/>
Centralized Outbreak Management		<input checked="" type="checkbox"/>
Ease of Deployment (no forklift upgrade)		<input checked="" type="checkbox"/>

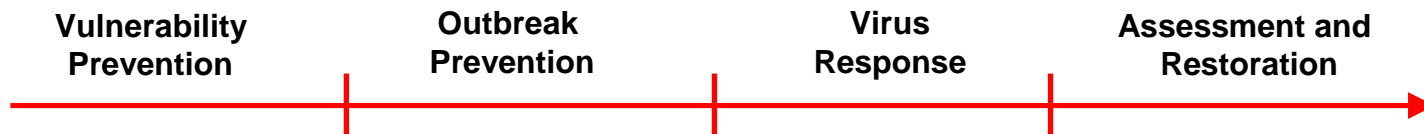
Legend: Only Partially Addresses Need



NVW Extends Cisco NAC:

1. Agentless
2. Network-vendor agnostic
3. Cleanup of infected machines
4. Unpatched machine isolation is threat-specific

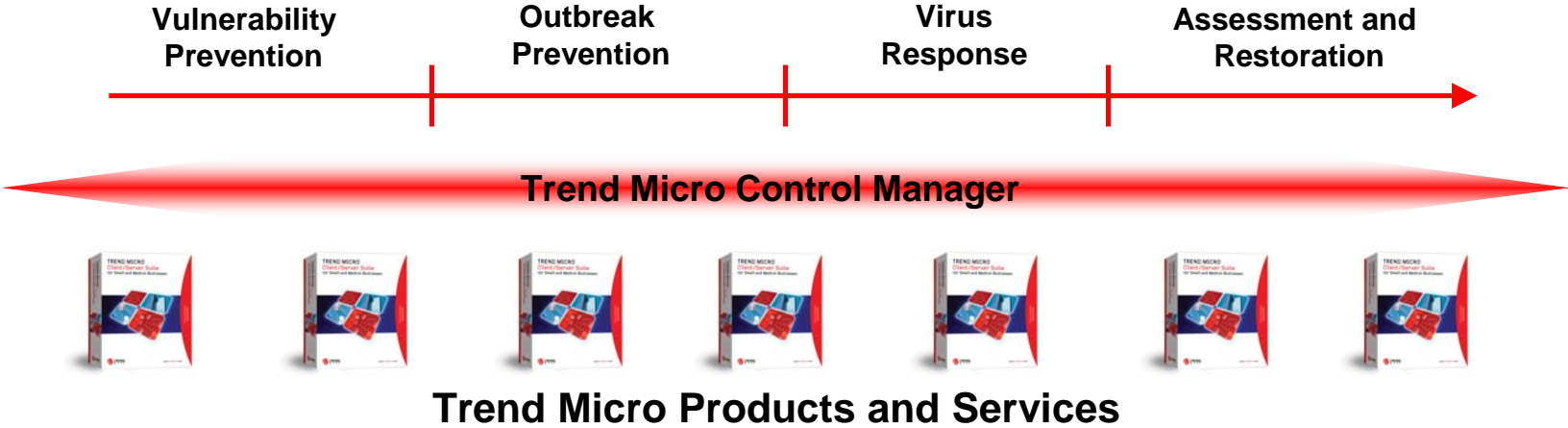
Network VirusWall is a key component of the Enterprise Protection Strategy (EPS), which is an end-to-end, layered defense strategy against viruses and other threats to your customer's IT environment for the entire lifecycle of those threats.



Trend Micro's award-winning Enterprise Protection Strategy spans everything from pre-empting attacks by detecting vulnerabilities in the Microsoft Operating System all the way to cleaning up virus remnants after an outbreak has been contained.

Centralized Management is a Key Element of the Enterprise Protection Strategy

Trend Micro Control Manager™ is a centralized outbreak management console designed to simplify enterprise-wide coordination of outbreak security actions and management of Trend Micro products and services



*Network VirusWall customers can order Trend Micro Control Manager Standard at no charge

- ① **Vulnerability Assessment** – helps pre-empt attacks by detecting major threats associated with vulnerabilities in Microsoft Operating Systems and ranking them by severity and likelihood to invite a virus attack
- ① **Outbreak Prevention Services (OPS)** – delivers outbreak prevention policies to help IT managers prevent and/or contain outbreaks during that critical period before the patch, pattern file, or network signature is available for a new virus
- ① **Virus Response Services** – provides customized virus information from TrendLabs 24x7 regarding potential threats, suspicious activity and strategies for outbreak protection.
- ① **Damage Cleanup Services (DCS)** – assesses damage and can automatically clean up worms, virus remnants, Trojans and memory registries to help prevent re-infection.

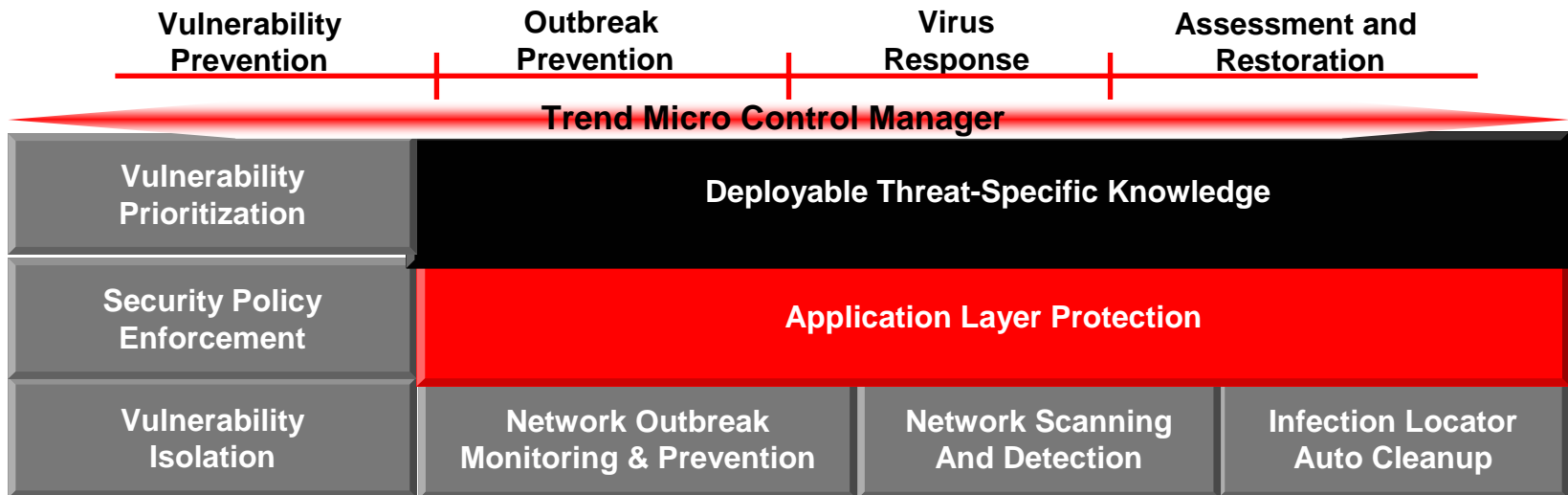
Thanks to the Enterprise Protection Strategy, Network VirusWall can protect your customer's network during all phases of the outbreak management cycle...

Vulnerability Prevention = NVW + Vulnerability Assessment

Outbreak Prevention = NVW which includes Outbreak Prevention Services!

*Virus Response = NVW**

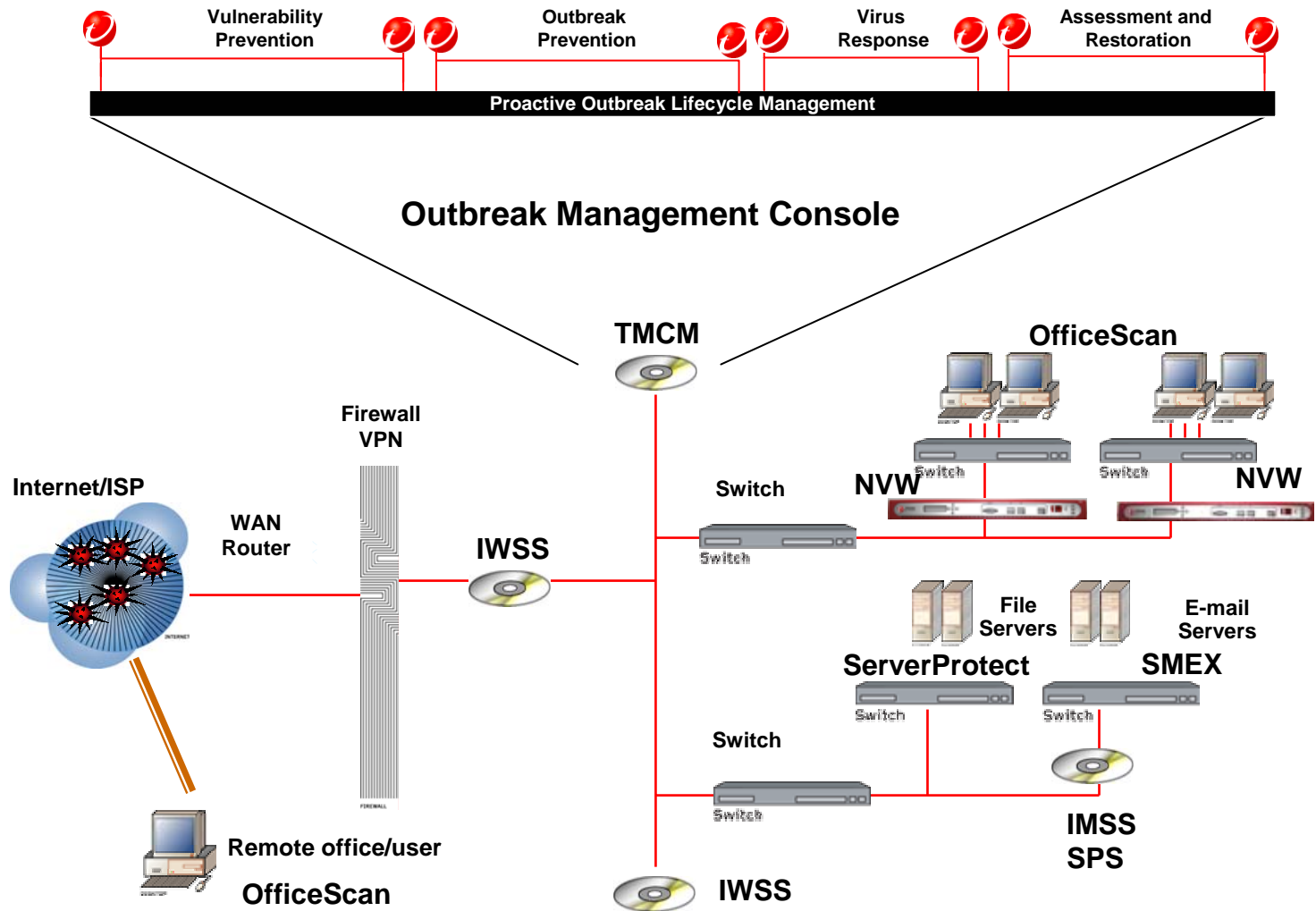
Assessment and Restoration = NVW which includes Damage Cleanup Services!



*Add Virus Response Services for enhanced response capabilities!

WHERE DOES NETWORK VIRUSWALL FIT INTO THE CUSTOMER'S IT ENVIRONMENT?

Sales Training Module for Network VirusWall





Target Customer Type

- Existing Trend Micro Customers
- Customers Currently Running Symantec Mail Security for Lotus Notes
- Information-oriented organizations dependent on computers for daily activities
- Distributed businesses with direct connections to remote workers and/or small remote offices
- Victims of MSBlaster, SQL_Slammer, Nachi, Nimda, Code Red, Welchia or other Network worms
- Early Adopters who are open to deployment in select segments

Customer Size

- Medium- and Enterprise-Sized Organizations
- 500+ seats

Key Influencers

- Network and Security infrastructure management
- Security Operations professionals (including gateway anti-virus)



Antivirus

- Antivirus does file scanning only; cannot stop network viruses spread at network layer

Firewall

- Not the only network entry point
- Most viruses bypass firewalls
- Cannot do much once virus is inside the network
- Blocking at firewall could be disruptive
- F/W vendors have limited threat expertise

Vulnerability Assessment

- Cannot isolate/block vulnerabilities to prevent/contain virus – only provides assessment

Security Management

- Correlates threat events; but, so what? – no enforcement or outbreak management

Host-based IDS/IDP*

- Managing agents at hosts is complex; could become expensive

COMPETITIVE POSITIONING

Sales Training Module for Network VirusWall



Key Capabilities	VA	IDS/ IDP	Security Mgmt.	Traditional Antivirus	Network VirusWall
Vulnerability Isolation*					<input checked="" type="checkbox"/>
Network Outbreak Monitoring					<input checked="" type="checkbox"/>
Network Virus Outbreak Prevention					<input checked="" type="checkbox"/>
Network Virus Detection		<input checked="" type="checkbox"/> <i>partial</i>			<input checked="" type="checkbox"/>
Infection Locator/ Automated Cleanup					<input checked="" type="checkbox"/>
Security Policy Enforcement					<input checked="" type="checkbox"/>
Centralized Outbreak Management**			<input checked="" type="checkbox"/> <i>partial</i>	<input checked="" type="checkbox"/> <i>partial</i>	<input checked="" type="checkbox"/>

*Requires Trend Micro Vulnerability Assessment (TMVA)

**Trend Micro Control Manager (TMCN) 3.0 included

Legend: Partially Addresses Need

VA - Vulnerability Assessment
IDS - Intrusion Detection System
IDP – Intrusion Detection/Prevention





- **Only Monitoring – No prevention or isolation**
 - IDS only provides threat information
 - Companies rarely use IDP/IPS prevention mechanisms due to false positive issues
- **Ineffective once virus is inside network – No containment**
 - Virus-related traffic generating from clients/servers could bring down the network
- **Limited threat/virus expertise or 24 x 7 “outbreak” support**
 - Many IDS/IDP vendors depend on AV companies, such as Trend Micro, for samples and expertise

“Intrusion detection systems do not provide protection – only faster notification that your security has failed” – Mark Nicolett, Gartner, December 2003

COMPETITIVE POSITIONING

Comparison with IDS/IDP

Sales Training Module for Network VirusWall

Problems Solved/Addressed	IDS	IDP	NVW
Vulnerability Isolation*			<input checked="" type="checkbox"/>
Network Outbreak Monitoring	Primarily designed to detect hack attacks and not viruses; many false positives		<input checked="" type="checkbox"/>
Network Virus Outbreak Prevention			<input checked="" type="checkbox"/>
Network Virus Detection	Limited threat expertise; many vendors do not even get virus samples		<input checked="" type="checkbox"/>
Infection Locator/Automated Cleanup			<input checked="" type="checkbox"/>
Security Policy Enforcement			<input checked="" type="checkbox"/>
Centralized Outbreak Management**			<input checked="" type="checkbox"/>
Denial of Service/Anti-hack Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

*Requires Trend Micro Vulnerability Assessment (TMVA)

**Trend Micro Control Manager (TMCM) 3.0 included

IDS - Intrusion Detection System

IDP – Intrusion Detection/Prevention

NVW – Network VirusWall



TREND MICRO

Network VirusWall

vs. Network Associates IntruShield

- No isolation/containment
- No security enforcement
- No vulnerability isolation
- No virus/remnant cleanup
- False positives
- Currently not managed by ePolicy Orchestrator

TREND MICRO

Network VirusWall

vs. McAfee System Protection

- Complex to manage all of these host agents
- No enforcement
- Host IDP could interfere with some applications

TREND MICRO

Network VirusWall

vs.

**Symantec Vulnerability Assessment
Plus Symantec IDP**

- No isolation and containment
- No security enforcement
- No vulnerability isolation
- No remnant cleanup

TREND MICRO

Network VirusWall

vs. **Symantec Security Suite**

- Collection of individual point products; no meaningful integration

TREND MICRO

Network VirusWall

vs. **SESA**

(Symantec's Event Correction/Management Framework)

- In development TWO years with no significant results
- Management/Integration frameworks not successful in other industries

Sygate

- Security enforcement only (which is currently not agentless)

Tipping Point

- Intrusion Detection/Prevention only

Fortinet

- Firewall and Intrusion Detection/Prevention only

ForeScout

- No security enforcement; virus elimination and cleanup

Why Trend Micro will win...

- First mover advantage, threat-specific expertise and vendor viability
- Delivering a truly comprehensive solution
- Backed by 24X7, award-winning global antivirus service and support infrastructure



POSITION AS...

- This is revolutionary! No one else is solving these problems.
- Outbreak Prevention Appliance—enabling organizations to detect, prevent, and eliminate outbreaks.
- Great vehicle for deploying Trend Micro knowledge and expertise.
- Moving security where it is most effective—off the hosts and into the network.

DO NOT POSITION AS...

- IDS/IDP* or Vulnerability Assessment. It's more than that.
- Replacement of antivirus (antivirus products complement Network VirusWall)
- Antivirus – This is not just antivirus!
 - Includes network packet scanning (heuristics), vulnerability isolation, security policy enforcement, and outbreak prevention policies.

TERMINOLOGIES TO USE...

- Network viruses/worms
- Network LAN segments, Network sub-segments, Network access points
- Network layer



1.

Understanding the Technology

- The Problem
- The Trend Micro Solution
 - *Elevator Pitch*
 - *Product Overview*

2.

Positioning the Product

- Leverage Points
- Where does Network VirusWall fit into the EPS?
- Market Opportunity
- Target Customers
- Competitive Positioning

3.

Selling the Solution

- Summary of Key Selling Points
- Handling Objections
- Product Licensing Model

SUMMARY OF KEY SELLING POINTS

Sales Training Module for Network VirusWall

Don't forget EPS!

- Addresses viruses at the network layer for a whole new level of protection
- Monitors *and* helps prevent, contain and eliminate viruses at the network level
- Trend Micro's threat-specific expertise is used to facilitate outbreak management and accelerate recovery



Network viruses continue to wreak havoc on organizations, even those that invest heavily in information security. An array of point products working in isolation makes solving the network virus problem even more difficult. Organizations looking to reduce the number and impact of outbreaks should consider deploying an integrated, network-based security solution. Key components might range from vulnerability management to intrusion prevention to antivirus.

— Chris Christiansen

Program VP for Security Products, IDC



! OBJECT

Objection: Do I need to buy and deploy Network VirusWall across my entire network all at once?

Answer: No. You can adopt a phased approach based on your security risk profile, problem areas/hot spots, network infrastructure and budgetary constraints. (Some other security solutions, like IDP, require complete coverage all at once with a substantial initial investment.)

! OBJECT

Objection: Does Network VirusWall address file-based viruses?

Answer: No. Trend Micro's antivirus and content security products address file-based viruses while Network VirusWall addresses network viruses and worms.

! OBJECT

Objection: Why can't I simply use firewall or IDP to block viruses?

Answer: They are not threat-specific and consequently, respond poorly and/or result in false positives. In fact, most organizations never use these "preventative" features in IDP or their firewall during outbreaks.

! OBJECT

Objection: Can Network VirusWall handle the throughput or will I see a degradation in performance?

Answer: The 100 MBps (180 MBps full-duplex) solution can handle throughput on network LAN segments for most organizations. Higher throughput solutions (GBps) are scheduled for release later this year.



● Product Licensing Model

- Per Seat Pricing
- Annual maintenance cost at 30% of then current SRP

Software Product <i>Number of Seats</i>	Network VirusWall <i>(Includes TCMC-E)</i> <i>Per Seat Price</i>	TCMC Enterprise Suite <i>(incl. OPS & DCS)</i> <i>Per Seat Price</i>	Network VirusWall Upgrade for TCMC-E <i>Per Seat Price</i>	Vulnerability Assessment <i>Per Seat Price</i>
5-25 seats	\$52.64	\$11.10	\$39.48	\$65.00
26-50 seats	\$46.32	\$9.77	\$34.74	\$57.20
51-100 seats	\$40.53	\$8.55	\$30.40	\$50.05
101-250 seats	\$36.08	\$7.61	\$27.06	\$44.56
251-500 seats	\$30.00	\$6.33	\$22.50	\$37.05
501-1000 seats	\$24.21	\$5.11	\$18.16	\$29.90



Note: all pricing SRP
Valid as of June '04

- **Product Licensing Model**
 - Per Unit Pricing
 - Maintenance cost at 20% of then current SRP

Hardware Product <i>Number of Units</i>	Network VirusWall 1200 Appliance <i>Per Unit Price</i>
1-5 units	\$5,995.00
6-10 units	\$4,495.00
11-25 units	\$3,495.00
26-50 units	\$2,495.00
51-100 units	\$1,995.00
>100 units	\$1,595.00

Note: all pricing SRP
Valid as of June '04





Pricing Model is not a one-size-fits-all but flexible to meet organizations' needs and network configuration.


S/W Stack
(user license)

Number of Seats	Network VirusWall User License
500 seats	\$30.00
1,000 seats	\$24.21
2,500 seats	\$20.75
5,000 seats	\$17.37
10,000 seats	\$13.69
25,000 seats	\$10.29
50,000 seats	\$ 7.90

+ H/W

Number of Units	Network VirusWall Hardware
1-5 units	\$5,995
6-10 units	\$4,495
11-25 units	\$3,495
26-50 units	\$2,495
51-100 units	\$1,995
> 100 units	\$1,595



- **Network VirusWall 1200 Appliance** (physical SN) 
- **Network VirusWall software**
 - includes TMCM-Enterprise (code & RK, OPS RK, and DCS RK)
 - Note: No NVW code. Also, the RK resembles a TMCM-E RK.
- **Network VirusWall software upgrade to current TMCM-Enterprise customers**
 - includes TMCM-Enterprise (code & RK)
- **TMCM-Standard** (code & RK)
- **TMCM-Enterprise**
 - includes TMCM-Enterprise (code & RK)
 - includes OPS (RK only to activate within TMCM-E)
 - includes agent-less DCS (RK to activate TMCM-E side; code and SN for DCS server)
- **Vulnerability Assessment** (RK only)
 - Note: requires TMCM-S or TMCM-E to operate



- Online Testing for **Network VirusWall** can be found at the following URL:
<http://certification.trendmicro.de>
- 15 Questions
- 80% is passing score
- Immediate results!





THANK YOU!

And good selling...