
 INTUITIVE INFORMATION SECURITY  
 FOR THE ENTERPRISE

SPRING 2002

TREND MICRO

# InterScan™ AppletTrap™

## COMPREHENSIVE MALICIOUS CODE SOLUTION FOR THE ENTERPRISE

### PROBLEM:

Mobile code, including Java, ActiveX, JavaScript, and VBScript, poses a unique security risk to enterprise networks. Besides acting as a transport mechanism for viruses, mobile code in Web content can launch specific attacks designed to steal data or disable systems. Known examples of malicious mobile code can be identified and blocked as they flow through the Internet gateway, but the detection of previously unknown malicious code requires extensive behavior monitoring and analysis.

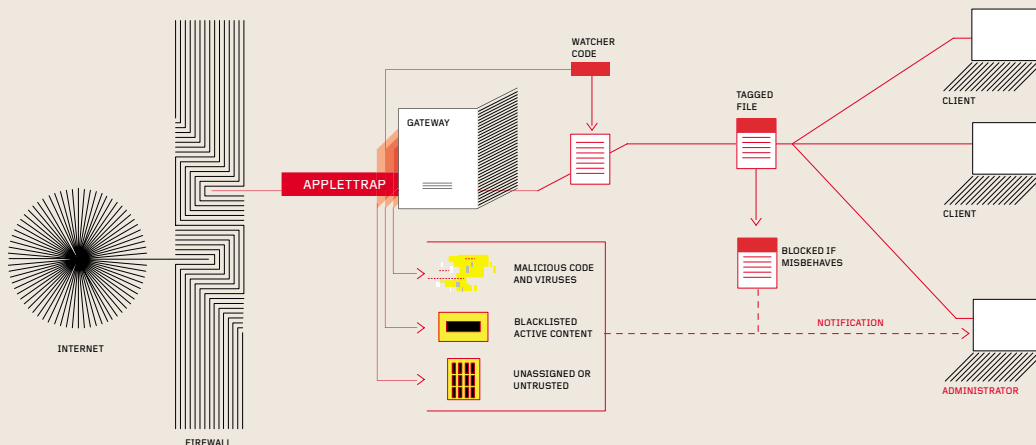
### STRATEGY:

Trend Micro InterScan AppletTrap is a centrally managed, policy-based tool for managing the security of active Web content. It screens out malicious mobile code from Internet traffic with a three-layer defense: analyzing and verifying digital certificates, filtering for known malicious code at the server, and monitoring the behavior of unsigned code at the client browser in real time.

- Server-based solution monitors mobile code on the client in real time
- Requires no client deployment; transparent to end-users
- “Sandbox” behavior monitoring of applets at the client level
- Filters out HTML scripts including JavaScript and VBScript
- Available as a stand-alone proxy or a plug-in to Check Point Firewall-1 (OPSEC certified)

*“Despite growing threats, Fortune 1000 companies are doing very little to protect themselves against malicious Java and ActiveX code. Companies must act now and employ a comprehensive defense that leverages known malicious code detection, real-time monitoring and code signing.”*

—Forrester Research



### APPLETTRAP™ AT WORK

InterScan AppletTrap removes and blocks infected files in real time; in addition it places “watcher code” on suspicious or untrusted applets allowing it to block them if they behave in a manner contrary to accepted policy; the file is immediately prevented from reaching end users and the administrator is notified

# Trend Micro™ AppletTrap™

## MOBILE CODE: AN UNDER-RECOGNIZED THREAT

- Security features exist to prevent Java applets and other mobile code from activating malicious applications on the client. Yet in practice, hostile Java, ActiveX, or script code can poke holes in firewalls, steal passwords, create backdoors, act as a transport mechanism for viruses, and damage data.

## THREE LAYERS OF DEFENSE

- InterScan AppletTrap offers three-layer protection against malicious mobile code without degrading performance, by:
  - Blocking uncertified, unsigned code at the Internet gateway
  - Blocking known malicious code at the Internet gateway
  - Watcher codes are added to applets before they are released to the client to codes monitor the behavior of the applet within a protected sandbox and immediately terminate the applet if it attempts an illegal operation
- Offending applets' signatures are added to the list of blocked code so they will be recognized and halted at the server in the future

## EASE OF USE AND MANAGEMENT

- Central management through AppletTrap's own Web-based management console lets administrators enforce company security policies enterprise-wide
- A comprehensive system log records malicious code detection events, blocked mobile code activities, and HTTP request activities

## NEW FEATURES FOR VERSION 2.5

- Caching function increases performance throughput with greater scanning accuracy
- Central certification management at the Internet gateway creates a more secure e-business environment
- Administrators can allow mobile code from trusted partners to enter the enterprise with full permission, while still subjecting unknown codes to behavior monitoring
- Version 2.5 is highly scalable, supporting environments for over 5,000 users or 500 concurrent users

## THE ADVANTAGES OF TREND MICRO

- **Global Innovation:** Trend Micro has been a pioneer in the antivirus software market since 1989, developing innovative strategies to protect information as new computing standards are adopted around the world
- **Server Market Leadership:** Trend Micro is the global leader in server-based antivirus software, with a market share of more than 60% at the Internet gateway. (IDC bulletin, 2001)
- **Flexible Best-of-Breed Technologies:** Trend Micro antivirus products and services are designed to integrate seamlessly with leading firewalls, intrusion detection systems, and other best-of-breed solutions for the complete enterprise strategy
- **Service and Support:** Trend Micro products and services are backed by TrendLabs, a leading antivirus research and support center that monitors potential security threats worldwide, developing the means to identify, detect, and eliminate new viruses

# TrendLabs

**AWARD-WINNING 24x7 SUPPORT**  
TrendLabs' ISO 9002-certified global headquarters and five regional centers back Trend Micro products with timely, high-quality service. A team of more than 250 engineers operates around the clock to monitor virus activity, develop information on new threats, and deliver prompt, effective solutions.

For more information about Trend Micro service and support, contact TrendLabs at <http://www.trendmicro.com/support>.



## TREND MICRO CONTROL MANAGER™

### Total Centralized Management

Trend Micro Control Manager integrates various layers of virus protection into an enterprise-wide content security strategy. Administrators can view virus activity, configure defenses, set security policies, and update protection throughout the network from a single console at any location.

## SYSTEM REQUIREMENTS

- For Windows™ NT 4.0 with SP6 or Windows 2000 with SP1:
- 200MHz processor; 128MB RAM
- For Sun SPARC Solaris 2.6:
- 64MB of RAM; Solaris patches for Java SDK, standard edition v1.3
- 128MB of swap space
- Cache space—default is 100MB
- Administrator console: Netscape Navigator 4.0 or Microsoft® Internet Explorer 4.0, with Java and Javascript features enabled
- Client console: Netscape Navigator 3.04 or Microsoft Internet Explorer 3.02

## TREND MICRO INCORPORATED

10101 N. De Anza Blvd.  
Cupertino, CA, 95014, USA  
toll free: 1+800-228-5651  
phone: 1+408-257-1500  
fax: 1+408-257-2003

[www.trendmicro.com](http://www.trendmicro.com)