National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Trend Micro InterScan™ VirusWall™ 3.52 for NT and Trend Micro InterScan™ VirusWall™ 3.6 for Solaris, HP-UX, and Linux

Report Number: CCEVS-VR-03-0039
Dated: 16 May 2003
Version: 1.2

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Franklin Haskell
The MITRE Corporation
Bedford, Massachusetts

Kathy Cunningham
National Security Agency
Ft. George G. Meade, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of Trend Micro InterScan™ VirusWall™ 3.6 for Solaris, HP-UX, Linux and Trend Micro InterScan™ VirusWall™ 3.52 for NT was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 16 May 2003. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Trend Micro InterScan™ VirusWall™ product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

1.1 Evaluation Details

Evaluation Completion:	16 May 2003
Evaluated Products:	Trend Micro InterScan™ VirusWall™ 3.6 for Solaris, HP-UX, and Linux Trend Micro InterScan™ VirusWall™ 3.52 for NT
Developer:	Trend Micro Incorporated 10101 N. De Anza Blvd., 2nd Floor Cupertino, CA., 95014
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Validation Team:	Franklin Haskell The MITRE Corporation 202 Burlington Road Bedford, MA 01730-1420 Kathy Cunningham National Security Agency (NSA) 9800 Savage Rd Ft. Meade, MD 20755-6740
Evaluation Class:	EAL 4
Completion Date:	16 May 2003

1.2 Interpretations

The Evaluation Team determined that the following CCIMB Interpretations were applicable to this evaluation:

1. Use of 'as a minimum' in C&P elements (038)
2. Meaning of "clearly stated" in APE/ASE_OBJ.1 (043)
3. Use of Documentation Without C & P Elements (051)
4. No Component to call out security function management (065)
5. Aspects of Objectives in TOE and Environment (084)
6. SOF Claims Additional to Overall Claim (085)

The Evaluation Team determined that the following NIAP interpretations were applicable to this evaluation:

1. Empty Selection or Assignments (407)
2. Association of Information Flow Attributes W/Subjects and Information (417)
3. Evaluation of the TOE Summary specification: Part 1 Vs Part 3 (418)
4. Identification of Standards (427)

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

T.ACCESS_DATA: An unauthorized user may gain access to the TOE and alter and/or delete data contained in the TOE.

T.OVRLOAD: Overload of the TOE caused by excessive network traffic that exceeds the amount permissible by the TOE may allow malicious code to enter the network undetected.

T.UNAUTH: An unauthorized user may gain access to the TOE and alter the TOE configuration, causing malicious code to enter the network undetected.

2 Identification

ST:	Trend Micro InterScan™ VirusWall™ 3.6 for Solaris, HP-UX, Linux and Trend Micro InterScan™ VirusWall™ 3.52 for NT Security Target, Version 1.0, 28 April 2003
TOE:	Trend Micro InterScan™ VirusWall™ 3.6 for Solaris, HP-UX, Linux and Trend Micro InterScan™ VirusWall™ 3.52 for NT
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.
PP:	The TOE does not claim conformance to a PP.
CEM:	Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 1.0, August 1999.

The TOE is comprised of two product versions, 3.52 for the NT platform and 3.6 for the UNIX platform. The two versions are similar with the exception of the audit function.

2.1 IT Security Environment

The TOE security environment consists of the threats to the security of the TOE, organizational security policies, and usage assumptions as they relate to InterScan™ VirusWall™. InterScan™ VirusWall™ provides for a level of protection that is appropriate for IT environments that require detection of virus infected files before they enter or leave the network system but is not designed to resist direct or hostile attacks. It is suitable for use in both commercial and government environments.

2.1.1 Physical Boundaries

The TOE is the InterScan™ VirusWall™ software product. There is no difference between the TOE and the InterScan™ VirusWall™ product. The TOE runs on an operating system and relies on the operating system and the hardware in the IT environment for it to operate. The operating system and hardware are addressed by the IT Environment descriptions. The operating system and hardware are included by assumption and are not part of the TOE.

2.1.2 Logical Boundaries

The TOE includes management interfaces provided to the administrator to primarily define the information flow policy and to review the logs, and the interfaces to utilize services provided by operating system.

The logical boundaries of the TOE can be described in the terms of the security functionalities that the TOE provides to the system that utilizes this product for the detection of viruses and malicious code.

Audit: The InterScan™ VirusWall™ provides an auditing mechanism that collects data with respect to the security risks associated with the information that is entering or leaving the network. For SMTP traffic, the designated personnel that receives notification of security violations can additionally include an administrator specified recipient, while for HTTP and FTP traffic the designated personnel is fixed to only include the client and the administrator.

User Data Protection: The virus-detection, monitoring and managing capabilities of the TOE services ensures that the information received by the network is free of any potential risks.

Security Management: The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to provide the most efficient method of implementing the risk detection to ensure the steady flow of information through the network.

TSF Protection: The FTP, SMTP, and HTTP traffic are subjected to the information process flow policy before flowing through the TOE.

3 Security Policy

The Security Target identified the following Security Policies for the evaluated product:

P.ADMIN The TOE shall provide the tools to manage and monitor the TOE services and its related data.

P.TRAFFIC All network traffic that is related to email, web and ftp shall be able to be monitored for malicious code.

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

A.MANAGE: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL: The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

A.LOCATE: The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

A.PROTECT: The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.3 System Assumptions

The following system assumptions are identified in the Security Target:

A.CONFIG: The TOE is configured to ensure all SMTP, HTTP and FTP traffic flows through the TOE.

A.HARDWRE: The TOE will be installed on a hardware system that meets or exceeds the following constraints:

InterScan™ VirusWall™ 3.52:

- Windows 2000 server or Windows NT version 4.0 build 1381 with Service Pack 3.0,
- PC with a Pentium 200 or faster processor,
- 64 MB of memory; 128 MB recommended,
- 25 MB free disk space for program files; 100 to 500 MB is recommended for optimal performance on high-traffic systems,
- A 800x600 monitor; 1024x768 or higher resolution is recommended,

InterScan™ VirusWall™ 3.6:

Solaris Version

- Solaris 2.6 or above on Sun SPARC platform,
- 256 MB main memory (DRAM),
- Swap space should be 2 to 3 times the main memory,
- 20 MB disk space
- 9 GB or more disk space for operation

Linux Version

- OS: Linux kernel 2.2.x ONLY, glibc 2.1.x ONLY
- IBM/AT compatible PC with Intel Pentium® processor 133 MHz or faster
- 28 MB or more of memory
- Swap space should be 2 to 3 times the main memory
- 20 MB disk space
- At least 9 GB disk space for operation (processing emails)
- Package name: libstdc++-compat

HP-UX Version

- HP-UX 10.20 or later
- 128 MB RAM
- swap space should be 2 to 3 times the main memory
- 20 MB disk space for InterScan™
- At least 9 GB disk space for operation(processing emails)

The following devices can be attached to either product version:

- Keyboard,
- Mouse,
- Floppy Disk Drive,
- CD-ROM Drive
- Tape Drive,
- Fixed Disk Drives,
- Printer, and
- Network Adapter

A.IDENT: The operating environment will provide a method of administrative identification and authentication.

A.SYSPRCT: The operating environment will provide protection to the TOE and its related data.

A.SYSTIME: The operating environment will provide reliable system time.

5 Architectural Information

The TOE is comprised of two product versions, 3.52 for the NT platform and 3.6 for the UNIX platform. The two versions are similar with the exception of the audit function.

InterScan™ VirusWall™ is a suite of anti-virus programs that work at the Internet gateway to detect and optionally pass, delete, quarantine or clean virus-infected files before they enter or leave the corporate network system. The TOE is installed on computers using Windows 2000 or Windows NT for version 3.52 and UNIX variants for version 3.6.

The TOE is comprised of the following services:

- E-mail InterScan™ VirusWall™ - monitors and scans all inbound and outbound email messages (SMTP traffic).
- Web InterScan™ VirusWall™ - monitors all inbound HTTP traffic, checking for viruses and malicious Java and ActiveX applets, and providing enterprise-wide Java and Authenticode standards.
- FTP InterScan™ VirusWall™ - ensures that all inbound file transfers made via FTP are virus-free (FTP traffic).

These services are configurable to a great degree.

6 Documentation

Purchasers of InterScan™ VirusWall™ will receive the following documentation:

- Trend Micro InterScan™ VirusWall™ 3.5 Administrator's Guide For NT version, dated 2002/08/07
- Trend Micro InterScan™ VirusWall™ 3.6 Administrator Guide For Solaris, HP-UX, and Linux, dated 2002/08/07
- Quick Start Guide For Solaris, HP-UX, and Linux, dated 2003/04/24

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The vendor shipped a TOE configuration to the CCTL for installation and testing. The evaluation team installed the TOE and ran a subset of the vendor test procedures on the TOE in the evaluated configuration. The vendor provided a complete set of test results for analysis.

Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues.

SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

The evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected.

The Evaluation Team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The Evaluation Team chose to run a subset all of the tests that the developer performed. The subset was chosen to ensure adequate coverage for all security functional requirements. This ensured that the Evaluation Team adequately addressed both security functions. The Evaluation Team used the developer's test configurations to perform the tests.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of vulnerability test tools, open-source vulnerability documentation, and a set of test procedures proposed by the penetration test team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

8 Evaluated Configuration

The following hardware is used to create the test configurations:

- 1 Sun V100 system for InterScan™ VirusWall™ 3.6 Unix version
- RAM: 256 MB
- Hard Disk space: 20MB and 9 GB for operation
- 1 Laptop system used to connect to Sun system utilizing Hyper Terminal
- 2 Desktop system for InterScan™ VirusWall™ 3.52 NT version
- Pentium 200 or faster
- RAM: 64 MB minimum; 128MB recommended
- Hard Disk space: 100 - 500 MB

- 1 6-port hub
- Network cables

The following software is required, to be installed on the machines used for the test:

- Sun Ultra 10 systems Operating System
- Solaris 2.6 or above
- InterScan™ VirusWall™ 3.6 Unix version
- Microsoft Windows Operating System
- Windows 2000/Win NT 4.0 build 1381 SP3
- Microsoft Exchange (only on one desktop to support SMTP)
- Microsoft IIS
- InterScan™ VirusWall™ 3.52 NT version

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.1 and the Common Evaluation Methodology (CEM) Version 1.0 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> "The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST."

The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for Trend Micro InterScan™ VirusWall™ 3.52 for NT and Trend Micro InterScan™ VirusWall™ 3.6 for Solaris, HP-UX, and Linux Part II" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

"The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured according to the following guidance documentation:

- Trend Micro InterScan™ VirusWall™ 3.5 Administrator's Guide For NT version, dated 2002/08/07
- Trend Micro InterScan™ VirusWall™ 3.6 Administrator Guide For Solaris, HP-UX, and Linux, dated 2002/08/07
- Quick Start Guide For Solaris, HP-UX, and Linux, dated 2003/04/24

The InterScan™ VirusWall™ TOE (see product identification below) satisfies Trend Micro InterScan™ VirusWall™ Security Target, Version 1.0, 28 April 2003."

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The security goals for the product, described in Section 3 above, are modest. As pointed out in Section 4, the TOE is designed solely to detect and respond to incoming data. It relies upon the environment and underlying operating system to protect itself from attack.

While aspects of the function were tested no claims were made for the security of the pattern download facility.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as Trend Micro InterScan™ VirusWall™ Security Target, Version 1.0, 28 April 2003.

The document identifies the security functional requirements necessary to implement Information Flow Protection and TOE Self Protection security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4.

13 Glossary

The following definitions are used throughout this document:

FTP – File Transfer Protocol

Hardware: the physical equipment used to process programs.

HTTP – Hypertext Transfer Protocol

SMTP – Simple Mail Transfer Protocol

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, Parts 1, 2, and 3.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.
- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.
- Trend Micro InterScan™ VirusWall™ Security Target, Version 1.0, 28 April 2003.
- ETR Part 1 (Non-Proprietary), Version 1.0, 30 April 2003.