Trend Micro™

INTERSCAN™ WEB SECURITY VIRTUAL APPLIANCE

Superior protection from web threats and control of internet usage

The web has rapidly become a top threat vector for business. In addition to blocking malicious code, inappropriate websites, and targeted attacks, security managers are also being asked to secure the expanding use of Web 2.0 and cloud-based applications, while reducing overhead and bandwidth costs.

Trend Micro™ InterScan™ Web Security Virtual Appliance is an on-premises secure web gateway that gives you superior protection against dynamic online threats, while providing you with real-time visibility and control of employee internet usage.

Interscan Web Security is also available in the cloud as a service.

KEY BENEFITS

Superior Protection

InterScan Web Security stops threats at the gateway before they ever get to your endpoints. It delivers comprehensive real-time protection against the full scope of web threats, using anti-malware, the strongest advanced threat protection, URL filtering, and web reputation. Interscan Web Security leverages the real-time protection of the Trend Micro™ Smart Protection Network™, ensuring you are protected against new and emerging threats, like ransomware.

Complete Visibility and Control

InterScan Web Security's granular application control for over 1,000 applications and protocols lets you easily enforce acceptable web use policies. It also provides real-time central management and monitoring so you can see web use as it happens, enabling on-the-spot remediation. Interactive and customizable dashboards and reports give you complete visibility of the web usage and data that is most useful to you for assessing your security posture, human resources, and compliance purposes.

Reduced Complexity and Costs

Deployed as a virtual or software appliance, InterScan Web Security Virtual Appliance lets you achieve data center consolidation and standardization. With centralized management of multiple gateways and native failover and redundancy. the solution makes ongoing management simpler – saving you time and resources.

WEB GATEWAY SECURITY

Protection Points

- Internet Gateway

Threat and Data Protection

- Cloud-based applications
- Web 2.0 applications
- Advanced Persistent Threats
- Ransomware
- Zero-day exploit
- Malware
- Data loss
- Viruses and worms
- Bots and command and control (C&C) callback
- Spyware and keyloggers
- Malicious mobile code
- Rootkits
- Phishing attacks
- Content threats

Integrates with:

- LDAP
- Active Directory™
- SNMP

KEY FEATURES

Award-Winning Gateway Antivirus and Antispyware

- Scans inbound and outbound traffic for malware
- Prevents malware from entering your network
- Stops virus and spyware downloads, botnets, malware callback attempts, and tunneling
- Closes the HTTPS security loophole by decrypting and inspecting encrypted content

Advanced Threat Detection

In addition to zero-day exploit scanning and detection of advanced persistent threats and botnets, the optional Trend Micro™ Deep Discovery™ Analyzer applies additional threat intelligence by using sandbox execution analysis to inspect suspicious files offline.

- Detonates files in customer-defined sandbox environment(s) and monitors for risky behavior
- Uses adaptive security updates to block new C&C servers found during analysis
- Identifies attacks using continually updated detection intelligence and correlation rules from Smart Protection Network intelligence and dedicated threat research

Web Reputation with Correlated Threat Data

Trend Micro™ Smart Protection Network™ web reputation technology blocks access to websites with malicious activity.

- Protects against new threats and suspicious activity in real time
- Identifies and blocks botnet and targeted attack C&C communications using global threat intelligence

Powerful and Flexible URL and Active Code Filtering

- Leverages real-time URL categorization and reputation to identity inappropriate or malicious sites
- Offers six different policy actions for web access control, including: monitor, allow, warn, block, block with password override, enforce time quota
- Supports object-level blocking within dynamic web pages such as Web 2.0 mashups
- Stops drive-by downloads and blocks access to spyware and phishing websites

Application Visibility and Control

- Monitors more than 1,000 internet protocols and applications, including instant messaging, peer-to-peer, social networking applications, and streaming media
- Allows users to access cloud-based applications, while enforcing your policies to mitigate risks and conserve resources
- Enables policy creation to control all web activities and user online time

Real-Time Reporting and Centralized Management

Centralizes logging, reporting, configuration management, and policy synchronization across multiple InterScan Web Security servers regardless of their geographic location. Through a single console, administrators can more effectively monitor, manage, and secure their organization’s internet usage.

- Monitors internet activity as it happens for unprecedented visibility
- Changes reporting to a proactive decision-making tool, enabling on-the-spot remediation
- Centralizes the configuration and reporting of multiple instances of the software virtual appliance
- Supports creation of custom reports
- Supports anonymous logging and reporting to protect end-user privacy
- Offloads reporting and logging from individual servers for higher throughput, lower latency, and historical reporting

KEY FEATURES *Continued*

Data Loss Prevention Add-on Module

Extend your existing security to support compliance and prevent data loss. Single-click deployment of DLP capabilities built into InterScan Web Security Virtual Appliance give you visibility and control of data in motion.

- Tracks and documents sensitive data flowing through network egress points
- Identifies risky business processes and improves corporate data usage policies
- Detects and reacts to improper data use based on keywords, regular expressions, and file attributes
- Reduces administration through central management with Trend Micro Control Manager along with other endpoint and email DLP modules
- Simplifies deployment with an add-on module, requiring no additional hardware or software
- Over 200 out-of-the-box DLP templates satisfy major compliance regulations and ensure that Personally Identifiable Information and sensitive data files are protected

Ransomware Protection

InterScan Web Security Virtual Appliance is part of Trend Micro's multi-layered approach to block ransomware at the gateway level before reaching your users. It provides:

- Scanning for zero-day exploits and browser exploits
- Botnet and C&C callback detection to block ransomware botnet and C&C sites
- Integration with Deep Discovery Analyzer for sandbox analysis (optional)
- Real-time web reputation to determine if a URL is a known delivery vehicle for ransomware

MULTIPLE DEPLOYMENT MODES

InterScan Web Security Virtual Appliance is designed to fit your specific needs. It offers multiple network deployment options, including transparent bridge, ICAP, WCCP, forward or reverse proxy.

Complete User Protection

InterScan Web Security is part of Trend Micro User Protection, a multi-layer solution that provides the broadest range of interconnected threat and data protection across endpoints, email and collaboration, web, and mobile devices.

System Requirements

Administrator Web Console Requirements

- Microsoft Internet Explorer 9 or 10
- Mozilla Firefox 39 or later
- Google Chrome 44 or later

Minimum Hardware

- Single 2.0 GHz Intel Core2 Duo 64-bit processor supporting Intel VT or equivalent
- 4 GB RAM
- 50 GB disk space (IWSVA automatically partitions the detected disk space as required)

NOTE: For testing purposes, it is recommended to leave the 50 GB disk allocation at its default. For production environments, provide at least 300 GB for logging and reporting.

Recommended Hardware

- Single 3.3 GHz Intel Quad Core processor supporting Intel Hyper
- Thread Technology or equivalent - 8 GB RAM
- 300 GB disk space or more for log intensive environments IWSVA automatically partitions the detected disk space as per recommended Linux practices

Server Platform Compatibility

- Virtual Appliances

Supports VMware ESX and ESXi v4.0, v4.1, v5.0, v5.1, v5.5 Supports Hyper-V 2.0, 3.0

NOTE: If you use a virtual platform for IWSVA, reserve adequate resources for IWSVA. Otherwise, needed resources may be used by other instances on the same physical machine, and IWSVA may not function as designed

Software Appliances

For the latest Certified by Trend Micro platforms: http://www.trendmicro.com/go/certified

Directory Servers for End-User Authentication

To configure policies based on Lightweight Directory Access Protocol (LDAP) users and groups, the product integrates with the following LDAP directory services:

- Microsoft Active Directory (AD) 2003, 2008, and 2012
- Linux OpenLDAP Directory 2.2.16 or 2.3.39
- Sun Java System Directory Server 5.2 (formerly Sun ONE Directory Server)
- Novell eDirectory 8.8

TREND MICRO™

Securing Your Journey to the Cloud