



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-premise 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, and both the cloud-offering and on-premise solution can be seamlessly deployed together with common management and policies. This hybrid deployment is ideal for organizations that have multiple worksites geographically spread out or those with a highly mobile workforce.

## 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 Trend Micro's global Smart Protection Network™, ensuring you are protected, even against new emerging threats.

### 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
- 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 Deep Discovery Advisor 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 Command and Control 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 Command and Control (C&C) communications using global threat intelligence

### Powerful and Flexible URL and Active Code Filtering

- Leverages real-time URL categorization and reputation to identify 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 1000 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

### 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 100 out-of-the-box DLP templates satisfy major compliance regulations and ensure that Personally Identifiable Information and sensitive data files are protected

## 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.

## DEPLOYMENT OPTIONS

**Software Appliance:** bare metal installation with tuned, security-hardened OS

- Certified by Trend Micro: Through extensive testing and validation, Trend Micro certifies platforms for compatibility with Trend Micro software appliance solutions. See certified by Trend Micro server platforms at: <http://www.trendmicro.com/go/certified>

**Virtual Appliance:** virtualized deployments via hypervisor technologies

- Microsoft® Hyper-V™ Virtual Appliance
- VMware Ready Virtual Appliance: Rigorously tested and validated by VMware, achieving VMware Ready validation. Supports VMware ESX or ESXi v3.5+ and vSphere



- **Complete User Protection**
- InterScan Web Security is part of Trend Micro Complete 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.

## MINIMUM SYSTEM REQUIREMENTS

Server Platform Compatibility	<p><b>Virtual Appliances:</b> VMware ESX/ESXi v3.5 and higher; Microsoft Hyper-V Windows 2008 SP1 or Windows 2008 R2 Windows Server 2012 Hyper-V</p> <p><b>Software Appliances:</b> For the latest Certified by Trend Micro platforms, please go to <a href="http://www.trendmicro.com/go/certified">www.trendmicro.com/go/certified</a></p>
CPU	<p><b>Minimum:</b> Single 2.0 GHz Intel™ Core2Duo™ 64-bit processor supporting Intel VT™ or equivalent</p> <p><b>Recommended:</b></p> <ul style="list-style-type: none"> <li>• For up to 4000 users: Dual 2.8 GHz Intel Core2Duo 64-bit processor or equivalent</li> <li>• For up to 9500 users: Dual 3.16 GHz Intel QuadCore™ 64-bit processor or equivalent</li> </ul>
Memory	<p><b>Minimum:</b> 4GB RAM</p> <p><b>Recommended:</b></p> <ul style="list-style-type: none"> <li>• For up to 4000 users: 6GB RAM</li> <li>• For up to 9500 users: 24GB RAM</li> <li>• For up to 15,000 users: 32GB RAM</li> </ul>
Disk Space	<p><b>Minimum:</b> 20GB of disk space</p> <p><b>Recommended:</b> 300GB of disk space (Automatically partitions the detected disk space as required)</p>



©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, InterScan and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS02\_IWS\_VA\_140329US]

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