Trend Micro™

INTERSCAN™ WEB SECURITY

Superior protection from Internet threats and control over unsafe web usage

Traditional secure web gateway solutions that rely on periodic updates to cyber threats cannot keep pace with today's rapidly evolving web threats. In addition to blocking malicious code, inappropriate websites, and targeted attacks, security managers also need to secure the expanding use of Web 2.0 and cloud-based applications while reducing overhead and bandwidth costs.

Trend Micro™ InterScan™ Web Security dynamically protects against cyber threats at the Internet gateway. With the growing use of cloud-based consumer applications in the workplace, application visibility is essential to understand network risks. By integrating application control, zero-day exploit scanning, anti-malware scanning, Advanced Persistent Threat (APT) detection, real-time web reputation, URL filtering, and anti-botnet detection, InterScan Web Security delivers superior protection from advanced threats. Plus, the optional **Deep Discovery Advisor** integration conducts sandbox executional analysis on suspicious files to give you visibility and protection against web-borne advanced targeted threats, such as watering-hole attacks.

You can prevent sensitive data from leaving your organization with integrated data loss prevention (DLP) for InterScan Web Security. With customizable templates, the optional Data Loss Prevention Module filters information to help you with regulatory compliance and data privacy. With integrated DLP at the Web gateway, you can:

- Scan outbound traffic for content that includes sensitive data
- Create policies using predefined templates to better meet regulatory privacy requirements by filtering personally identifiable information
- Generate DLP policy violation reports tied to specific users
- Provide auditing functions to measure DLP policy effectiveness

WEB GATEWAY SECURITY

Protection Points

- Internet Gateway

Threat 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 BENEFITS

Superior Protection

- Relieves the burden on endpoint security and stops more threats at the gateway by integrating zero-day exploit scanning, malware scanning, and Advanced Persistent Threat detection with web reputation, URL filtering, and Java Applet and ActiveX code security
- Enforces safe and proper web use by monitoring Internet traffic against malicious content
- Blocks new threats as they emerge
- Provides instant updates for immediate protection

Visibility and Control

- Real-time centralized management for multiple instances and locations
- Monitors web use as it happens, enabling on-the-spot remediation
- Manages and reports on more than 1000 Internet protocols and applications
- Enables granular policy creation to control all web activities including time spent on the Internet

Reduced Complexity and Costs

- Increases utilization rates of existing servers, reducing sprawl and energy costs
- Deploys as a virtual or software appliance for data center consolidation and standardization
- Centralizes management of distributed web gateways across the WAN
- Improves security levels with quick deployment of new features
- Speeds recovery from outages with native failover and redundancy
- Simplifies OS and security updates, version control, and testing

KEY FEATURES

Application Visibility and Control

- Monitors and reports on 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 acceptable user policies to mitigate risks and conserve resources
- Enables granular policy creation to control all web activities and user time spent on the internet

Award-winning Gateway Antivirus and Antispyware

- Scans inbound and outbound traffic for malware
- Prevents malware from entering your network, relieving the burden on endpoint security
- Stops virus and spyware downloads, botnets, malware callback attempts, and malware tunneling
- Closes the HTTPS security loophole by decrypting and inspecting encrypted content
- Allows enterprises to electively decrypt HTTPS traffic to balance content security with user privacy needs

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 target attack Command and Control (C&C) communications using global and local 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 related websites

Advanced Threat Detection

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
- Correlates full forensic analysis with Trend Micro threat intelligence to provide information on the attack and attacker
- 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

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 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

Data Loss Prevention (DLP) Templates for Compliance Regulations

To help you protect critical data, over 100 out-of-the-box DLP templates satisfy major compliance regulations and ensure that Personally Identifiable Information and sensitive data files are protected.

Regulatory Compliance

- PCI/DSS—International standard for data security for credit cards
- IBAN—International Bank Account Number
- US HIPAA—Sets standards for any healthcare organization in the US
- US Gramm-Leach-Bliley Act (GLBA)—Sets privacy regulations for banking, insurance, and investment companies
- US SB-1386—Refers to state data breach laws
- UK NHS Number—Used to identify UK patients and locate health Records

Personally Identifiable Information

- Banking and Financial Information
- Cardholder Information

Other

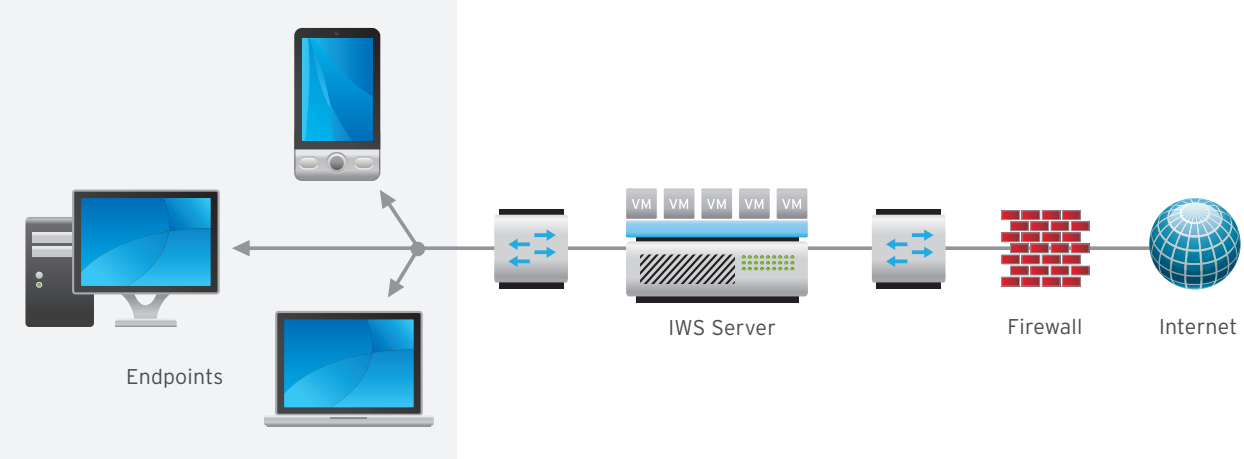
- Source Code Identifiers
- Executables
- Over 170 different file types including MS Office , database , multi-media and compressed files
- And more

MULTIPLE DEPLOYMENT MODES

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

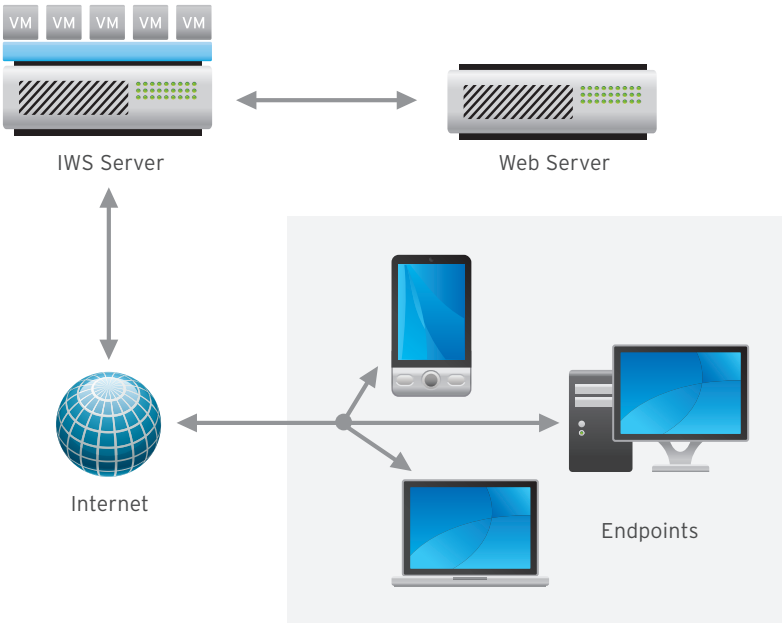
Transparent Bridge Mode

In Transparent Bridge Mode, IWS acts as a bridge between two network segments and transparently scans all traffic, in addition to HTTP(s) and FTP traffic. Transparent Bridge Mode is the simplest way to deploy the solution into an existing network topology and does not require modifications to clients, routers, or switches. IWS acts as a "bump in the wire" while providing all of its content security functionality.



Reverse Proxy

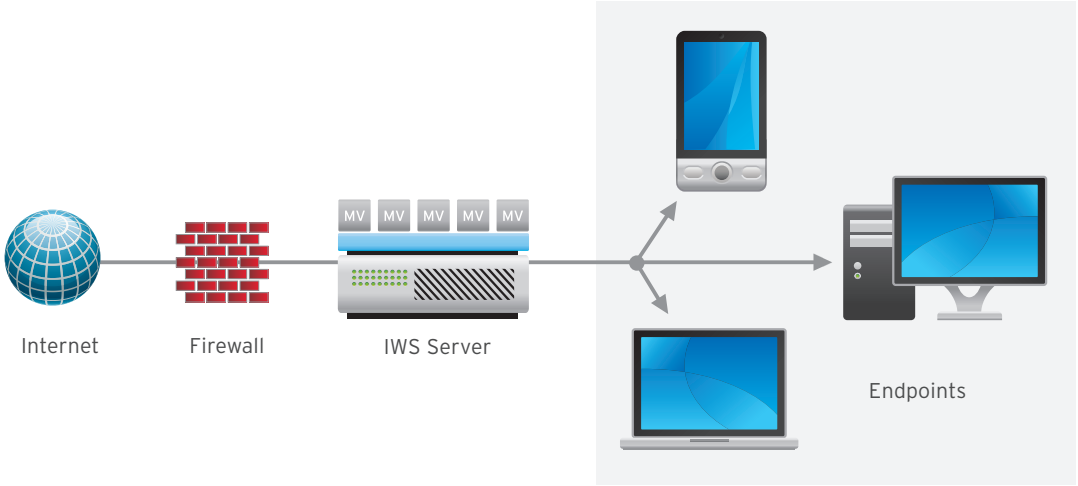
IWS can be installed as a reverse proxy to protect a web server from malware uploads. In Reverse Proxy Mode, the solution is installed in front of the web server that it protects. This mode is useful when the web server accepts file uploads from clients. xSPs can use the solution as an HTTP proxy to protect and oversee uploaded traffic for customers with interactive websites.



MULTIPLE DEPLOYMENT MODES (CONT.)

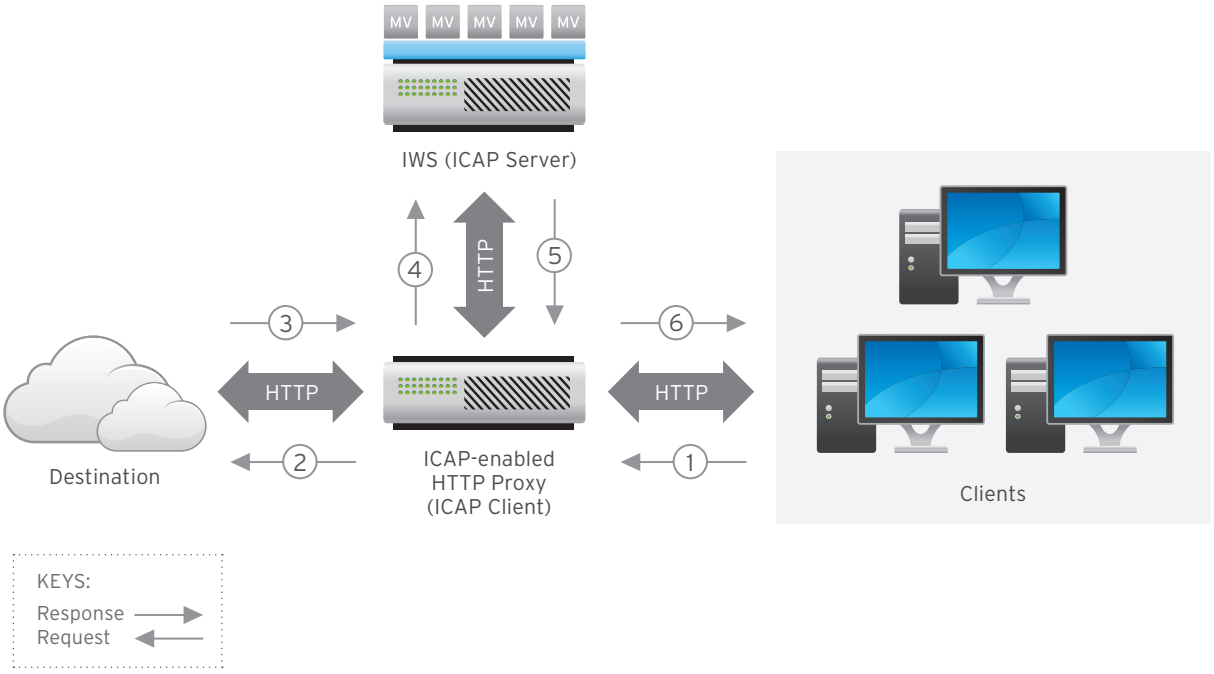
Forward Proxy

IWS can be deployed as a dedicated proxy for network clients. Both explicit and transparent proxy deployments are possible depending on the existing proxy infrastructure. ICAP and WCCP are also supported for networks that need to selectively route Internet traffic from an existing proxy or other network device.



Internet Content Adaption Protocol (ICAP)

IWS supports integration with third-party cache, proxy, and storage servers through the ICAP v1.0 interface, such as Blue Coat Proxy, EMC Isilon Scale-Out Network-Attached Storage, NetApp NetCache, and Cisco Content Engines. In ICAP deployment, IWS accepts ICAP connections from an ICAP v1.0 compliant server, secures all the content returned to the server and then to the end users.



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 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

MINIMUM SYSTEM REQUIREMENTS

Server Platform Compatibility

Virtual Appliances:

- VMware ESX/ESXi v3.5 and higher; Microsoft Hyper-V Windows 2008 SP1 or Windows 2008 R2
- Windows Server 2012 Hyper-V

Software Appliances:

- For the latest Certified by Trend Micro platforms, please go to www.trendmicro.com/go/certified

CPU

Minimum:

- Single 2.0 GHz Intel™ Core2Duo™ 64-bit processor supporting Intel VT™ or equivalent

Recommended:

- For up to 4000 users: Dual 2.8 GHz Intel Core2Duo 64-bit processor or equivalent
- For up to 9500 users: Dual 3.16 GHz Intel QuadCore™ 64-bit processor or equivalent

Memory

Minimum:

- 4GB RAM

Recommended:

- For up to 4000 users: 6GB RAM
- For up to 9500 users: 24GB RAM
- For up to 15,000 users: 32GB RAM

Disk Space

Minimum:

- 20GB RAM

Recommended:

- 300GB of disk space (Automatically partitions the detected disk space as required)

TREND MICRO™

Securing Your Journey to the Cloud