Trustwave®

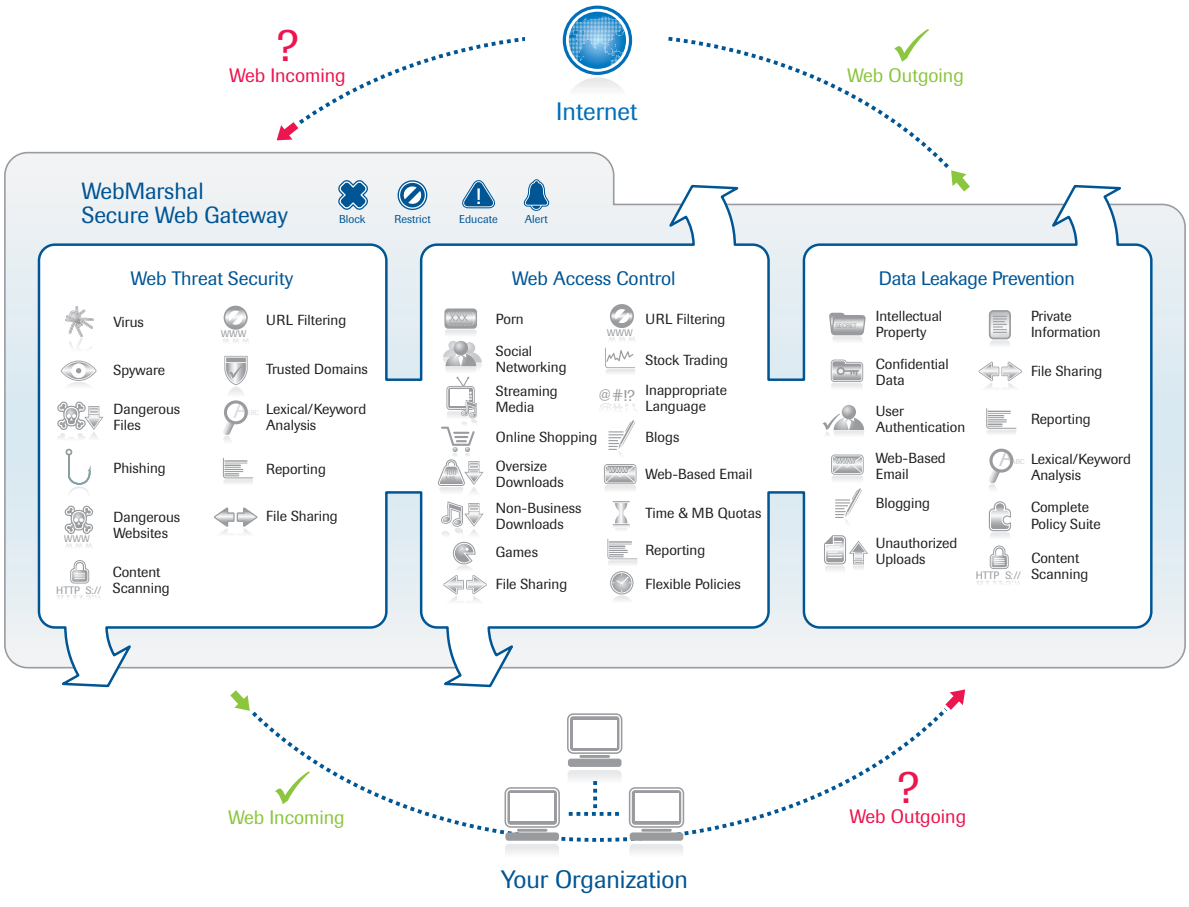
WebMarshal™

Secure Web Gateway

WebMarshal is a Secure Web Gateway – a comprehensive solution which addresses the many requirements and issues that arise in managing Internet use. In a Web 2.0 world, organizations and employees are increasingly reliant on Internet access for business, education and work/life balance. Yet in terms of security and data protection Web 2.0 has created an unprecedented risk environment with new threats and vulnerabilities. WebMarshal is the answer to managing and securing Internet use for any size organization.

Key Features

- Inspects incoming and outgoing Web traffic in real time.
- Manages access to websites by category and content analysis.
- Blocks Internet security threats such as viruses, malware, blended attacks and social engineering scams.
- Controls bandwidth consumption and applications including streaming media, instant messaging and social networking.
- Provides data leakage prevention (DLP) by controlling what users upload to the Web including text and files.
- Supports flexible and intuitive policy enforcement with advanced Directory integration for user authentication and time/bandwidth quotas for personal Internet use.
- Enables detailed yet easy to understand Internet activity reporting.



Overview

As a Secure Web Gateway, WebMarshal is deployed between your network and the Internet where it inspects all incoming and outgoing Web traffic. WebMarshal protects you and your users against the full spectrum of Internet threats, including malware, viruses, blended attacks and attempted fraud. It ensures that Internet use is appropriate and complies with your acceptable Web use policies. WebMarshal also monitors and controls the flow of information in and out of your organization, protecting confidential information and intellectual property.

WebMarshal provides the solutions to a wide range of Web security issues in one seamless, easy to use, highly scalable, dependable and cost effective solution.

Key Benefits

Secures Your Web Gateway Against All Internet Threats

Blocks viruses, malware, blended threats, anonymous proxies and other harmful Web content, protecting your users and your IT resources from malicious Web sites.

Safeguards Against Data Leakage

By controlling the information users can upload, WebMarshal ensures that unauthorized staff cannot intentionally or accidentally transmit confidential or sensitive data.

Improves Productivity and Enforces Acceptable Use Policies

WebMarshal allows you to control where users go on the Web, when, what they can do and for how long. This ensures that users spend less time on personal Internet use and are prevented from accessing inappropriate content.

Manages Bandwidth Use, Improves Performance and Saves Costs

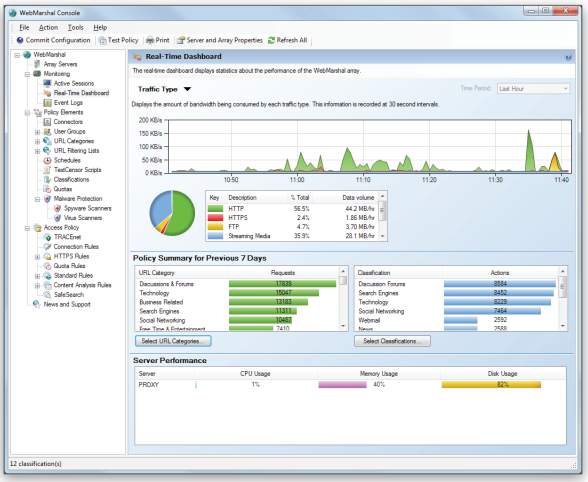
Uncontrolled Internet use can be a drain on bandwidth, network performance and can lead to significantly increased costs. WebMarshal allows you to manage access to high bandwidth sites and applications such as YouTube and even assign individual bandwidth quotas to help manage personal Internet use. Proxy caching saves bandwidth and delivers popular content faster.

Offers Speedy and Measurable Return on Investment

WebMarshal reporting demonstrates a rapid return on investment (ROI) and enables stakeholders to understand the key business benefits it offers. It also saves bandwidth, improves user productivity and protects against costly malware infections, all contributing to even greater ROI.

Provides Dependable Legal Liability Protection

Inappropriate or offensive Web content is blocked, preventing users from exposure to pornography or obscene material. WebMarshal demonstrates that you have undertaken all reasonable measures to protect staff and students, fairly enforce policies and provide a safe working or learning environment.



Trustwave webmarshal's real-time dashboard presents a range of information and useful statistics in a clear, easy-to-use interface. Recent web traffic by protocol is shown here including http, https, ftp, streaming media and instant messaging.

"It is hard to put a value on threat prevention, but [WebMarshal] has done exactly what we wanted. It is great software for content scanning of proxy traffic, one of the hidden threats that can cause damage if undetected. We undertook some very basic benchmarks and identified key features and benefits in the various solutions and are very happy with Trustwave".

Ludwig Brograd, Network Manager, Ernst & Young Ab

Meets or Exceeds Compliance Obligations

Enables organizations to place restrictions on who can transmit confidential information over the Web and prevent access to banned Web content. This allows you to demonstrate regulatory compliance with relevant authorities or governing agencies.

Protects Your Reputation

Upholds standards and ensures that confidential information is not leaked to the Web. WebMarshal prevents users from placing your organization in a publically embarrassing position as a result of inappropriate or careless Internet use.

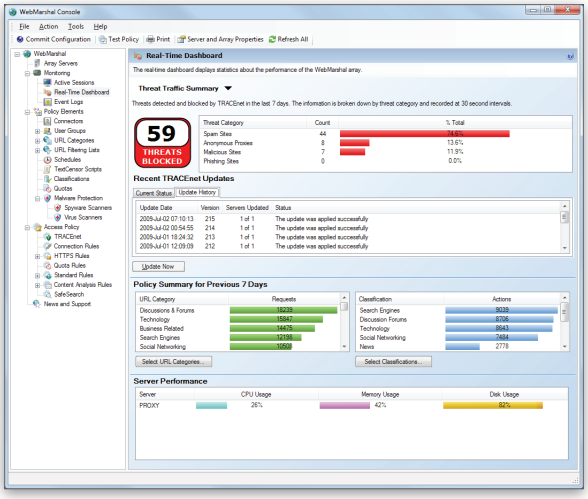
Delivers Low Total Cost of Ownership

Easy deployment on a cost effective, future-proof platform with minimal administrative overhead consolidation of key web security functions into a single management interface and centralized reporting makes WebMarshal an exceptional option for organizations looking for a good value all round Secure Web Gateway.

Web Threat Security

No single technology on its own can completely secure you against all Web threats. For this reason, WebMarshal employs a multi-faceted approach to threat protection which ensures it can address the full spectrum of Internet threats.

- TRACEnet – a continuously updated threat protection system designed to address a constantly evolving Web threat landscape. TRACEnet employs a range of technologies including reputation-based blacklists and heuristic filters to identify new threats in real time. TRACEnet specifically targets:
- Malicious Sites – containing malware, browser exploits, Cross Site Scripting or part of a blended attack.
- Phishing Sites – established by scammers to impersonate legitimate sites and attempt to defraud unsuspecting users.
- Spam Sites – associated with spam campaigns or botnet-related infection sites designed to convert your computer into a spambot.
- Anonymous Proxies – security bypass sites which canpotentially allow a user to circumvent Web security and create an insider threat to your organization.
- Anti-Malware Protection (Optional) – real-time anti-virus and anti-spyware scanning using your preferred choice from four name-brand anti-virus vendors to identify malicious content at the gateway before it is downloaded or accessed.
- MIME File Type Security – control restricted file types (e.g. EXE) by their structure and content, ensuring that intentionally mislabeled files are correctly identified and cannot circumvent security. WebMarshal also unpacks and scans archive files.
- Real-time Lexical Analysis – thorough lexical analysis of inbound and outbound traffic ensures content analysis is not limited to URL classification.
- Domain-specific Security – enforce enhanced security procedures for unfamiliar Web sites or relax policies for trusted domains such as Microsoft.com.
- HTTPS Scanning – full content inspection of SSL secured traffic, preventing exposure to malware from supposedly secure Web sites. Can also deny access to sites using self-signed or expired certificates.
- URL Filter List (Optional) – set security policies for specific categories of Web content such as denying access to known hacker sites or sites with poor reputation.



Trustwave Webmarshal provides a variety of reports and real-time performance counters that allow you to understand how users are utilizing internet access. Here the real-time dashboard displays threat information detected by TRACEnet.

Web Access Reporting

WebMarshal provides a rich, intuitive and flexible platform for enforcingc of Acceptable Use Policy and overall management of Web usage. It not only controls where users go on the Web but what they can do when they get there.

- Trustwave Web Filter Database (Optional) – ontains millions of URLs in 100+ categories to simplify management and administration of Web access and reporting.
- Real-time Lexical Analysis – allows WebMarshal to dynamically filter, classify and block websites based on their content at the time they are accessed.
- File Controls – policy-based management of file downloads. Files can be controlled by size, file type, user permissions and domain.
- Application and IM Control – comprehensive application controls allow you to manage access to streaming media, P2P and instant messaging applications..
- Personal Use / Quotas – flexible policy-based enforcement options are provided to suit your workplace culture, including bandwidth and time quotas (with optional extensions and personal reports for users to track their quota usage), Web site category access by time of day (e.g. lunch time access to Facebook or Twitter), educational reminders/warnings and “click-to-confirm” access options.
- SafeSearch – enforce SafeSearch options for popular search engines such as Google and Yahoo!.
- Workstations – policy options linked to specific workstations allow you to offer access by computer or IP address as well as by user or group.
- Proxy Caching – WebMarshal provides full, standalone proxy caching functionality which helps improve browsing performance, reduces bandwidth consumption and helps saves costs by delivering frequently accessed Web content from a local cache.
- Reporting – comprehensive reports identify the most visited Web sites, top Web users, itemized bandwidth costs and blocked content. Understandable executive summaries, system monitoring, and auditing of user behavior for human resources are all provided in easy to access, Web-based reports.

Data Leakage Prevention

Despite the wealth of intellectual property and confidential data currently in digital formats, data leakage prevention is often overlooked, especially when it comes to securing the Web Gateway. WebMarshal closes this door and allows you to control who has the ability to upload sensitive or confidential information to the to the Internet, even making sites like Facebook ‘read-only’.

- Keywords – WebMarshal analyzes and blocks text containing specific keywords or phrases from being uploaded to the Web, either in Webmail messages, blog postings, short message updates, like Twitter, or even contained within popular files such as Word documents.
- Webmail/Blogs / Web 2.0 – limit or block access to Webmail accounts, blog sites and other new media sites which facilitate user-enabled content and restrict what information or material users can transmit via the Web, not only protecting your data, but potentially also your reputation.
- File Restrictions – control the types of files that users are permitted to upload to the Web. File types can be blocked altogether or can be limited to authorized users or approved domains as required.

- Directory-based Management – integrate with corporate directories, including Active Directory and Novell Directory Services, for simplifies policy management and reporting.
- HTTPS Inspection – inspect content inside HTTPS traffic. WebMarshal can be configured to inspect suspicious HTTPS traffic to ensure integrity and protect data.

Advantages Anyone Can Appreciate

WebMarshal is ideally suited to meet the needs of businesses, agencies and institutions of any size. Offering flexibility, powerful features and reliable proxy-based design, WebMarshal also boasts a highly scalable enterprise architecture which can easily support geographically distributed, multi-server environments, providing them with centralized management and consolidated reporting of Internet usage.

Simple, Easy Deployment

WebMarshal can be installed and running within half an hour. With an intelligent installation wizard and automatic configuration of clear default policies, WebMarshal affords out-of-the box protection against offensive and malicious content. It can be deployed as a standalone proxy server (with caching), a Microsoft ISA Server plug-in or on multiple servers in a load-balanced array.

Flexible and Scalable

WebMarshal gives you the flexibility to grow as your requirements change or expand. With support for virtualized environments and it's highly scalable array-node architecture, WebMarshal provides a predictable and cost effective path for securing and managing the increase in Internet usage that most organizations are experiencing.

Set and Forget Administration

WebMarshal has been designed with minimal administration in mind, so you can concentrate on more productive tasks. Close Active Directory and Novell Directory Services integration ensures that WebMarshal is automatically up-to-date with new user accounts.

System Requirements

HARDWARE	**Minimum**	**Recommended***
Processor	Pentium 4 or equivalent	Pentium Core 2 Duo 3.0 GHz or higher
Disk Space	20GB (NTFS) or higher 30GB additional disk space for proxy caching	80GB (NTFS) or higher
Memory	2GB RAM or higher	3GB RAM or higher
SOFTWARE		
Operating System	Windows Server 2008 (32/64 bit)/Windows 7/ Windows Vista SP1 Business or Ultimate (32/64 bit)/ Windows XP Professional SP2 or later/Windows 2003 Server SP1 or later	
Database	SQL Server 2008/SQL Server 2008 Express/SQL Server 2005/SQL Server 2005 Express	
ISA Server (Optional)	ISA 2006 (Standard and Enterprise editons)/ISA 2004 SP2 or later (Standard and Enterprise editions)	

These requirements are recommended for up to 500 concurrent Internet users.

Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations — ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers — manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information: https://www.trustwave.com.

Corporate Headquarters
70 West Madison St.
Suite 1050
Chicago, IL 60602 USA

P: 312.873.7500
F: 312.443.8028

EMEA Headquarters
Westminster Tower
3 Albert Embankment
London SE1 7SP UK

P: +44 (0) 845 456 9611
F: +44 (0) 845 456 9612

LAC Headquarters
Rua Cincinato Braga,
340 nº 71 Edificio Delta Plaza
Bairro Bela Vista - São Paulo - SP
CEP: 01333-010 - BRASIL

P: +55 (11) 4064-6101

APAC Headquarters
Level 7/Suite 3
100 Walker Street
North Sydney NSW 2060 Australia

P: +61 2 9089 8870
F: +61 2 9089 8989