Trustwave®

Trustwave WebMarshal

SECURE WEB GATEWAY

Benefits

Unrivalled in Security

- Secures your web gateway against all internet threats
- Safeguards against data leakage
- Improves productivity and enforces acceptable use policies
- Provides dependable legal liability protection
- Meets or exceeds compliance obligations
- Protects your reputation

Ease of Implementation

- Easy administration
- Simple, easy deployment
- Flexible and scalable

WebMarshal is a Secure Web Gateway, to manage an organization's internet use. Web sites and apps expose unprecedented risk with new threats and vulnerabilities. WebMarshal is the answer to managing and securing internet use for any size organization.

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 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.

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.

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 publicly embarrassing position as a result of inappropriate or careless Internet use.

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 reports.

Web Threat Security

- **TRACEnet:** employs reputation-based blacklists and heuristic filters to identify new threats in real-time, and it specifically targets sites linked to malware, phishing, and spam.
- **Anti-Malware Protection:** real-time anti-virus and anti-spyware scanning identifies malicious content at the gateway before it is downloaded or accessed.
- **File Type Security:** control restricted file types such as executables 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.
- **Anonymous Proxy Blocking:** Stops access to security bypass sites which can potentially allow a user to circumvent web security and create an insider threat to your organization.
- **HTTPS Scanning:** Validation of SSL certificates and full content inspection of SSL secured traffic, preventing exposure to malware from supposedly secure websites.
- **URL Classification:** Use the Trustwave Web Filter Database to set security policies for specific categories of web content such as denying access to known hacker sites or sites with poor reputation.

Web Access Control

- **Trustwave Web Filter Database:** controls access by site content using this classified listing of millions of URLs in 100+ categories.
- **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:** provides policy-based management of file downloads. Files can be controlled by size, file type, user permissions and domain.
- **Application and IM Control:** allows comprehensive application control to manage access to streaming media, P2P and instant messaging applications, as well as WebSocket 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), Website 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 options for popular search engines such as Google and Yahoo!.
- **IP Address/Workstation Policies:** 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:** 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.
- **Header Matching and Rewriting:** allows blocking and control of applications that pass data in the transmission headers of HTTP requests and responses.
- **Reporting:** comprehensive reports identify the most visited websites, 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. Browsing details can be passed to a Syslog server for enterprise threat correlation (SIEM).

Data Leakage Prevention

- **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 Microsoft Word documents.
- **Webmail/Blogs/New Media:** 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.

Trustwave®

www.trustwave.com

WM_0523