

VIPRE ANTI-MALWARE FEATuRES

VIPRE Anti-Malware Engine
(Note: subscription payable)

Next Generation Anti-Malware

Real-time behavioral analysis technology

Certification

MX-Virtualisation™ (MX-V)

Genscan™ and Cobra™ heuristics

ThreatTrack™

SteadyStream™

BENEFITS

Uses heuristic, behavior and pattern-based technologies, alongside the fastest emulation technique available (MX-V™) which protects users from unidentified or new variants of malware.

New codebase delivering high speed threat scanning using an advanced technology stack with low impact on CPU and memory.

Protection against known and unknown “zero-day” malware threats by using proprietary detection methods which include; traditional signature-based, behavioral analysis, heuristics and most importantly dynamic translation.

VB100 and Checkmark Certified with exceptional detection rates and fast updates.

The fastest most adaptable Dynamic Translation technique for malware analysis which analyses potential threats by observing their behavior in a safe virtual environment.

Dynamic pattern assessment to determine if a source is malware.

Data feeds of the latest harmful URLs identifying malware hosts and phishing sites.

Real-time live threat data integration with continuous and compact updates at least once an hour.

WEB FILTERING FEATuRES

Dynamic Content Analysis™

‘Who, What, When, Where’ Policy Tools

SSI interception

unified Policy Tools and Wizards

‘Quick Block’ and ‘Quick Allow’

Advanced Categorization

‘Soft-blocking’ per content category

Flash filtering

Outbound (web post) monitoring & Customisable uRI blocklists

Internet Watch Foundation

BENEFITS

Screens the content, context and construction of web pages in detail, accurately detecting and blocking all objectionable, inappropriate, hidden or malicious content (including anonymous proxies).

True ‘who, what, when, where’ filtering with flexible user, group, time and location based controls.

Allows all unknown secure traffic to be decrypted and inspected (using Dynamic Content Analysis), so harmful HTTPS/SSL content (including SSL proxies) can be effectively blocked even in transparent proxy mode.

Unified, easy to use policy setting tools with policy and configuration wizards. With unlimited groups and ‘per user’ policies and the ability to combine policies with multi-group membership.

‘Quick Block’ and ‘Quick Allow’ buttons for fast one click fixes

Add-to-category functionality allows in-built categorisation to be adjusted with ease. Enhanced real-time categorisation - delivers higher accuracy, better reporting and fewer over-blocks

Delivering a better user browsing experience without compromising safety, security or control.

Screens actual SWF file code to accurately detect and block undesirable Flash content such as online games and video players.

Monitors and blocks text posted on the web (i.e. inappropriate blog / forum / Social Networking / Twitter posts) using a keyword analysis system.

Current, categorised and customisable URL blocklists control access to a pre-defined list of undesirable websites.

Blocklists are updated daily with IWF datafeeds.

WEB FILTERING FEATuRES

- Whitelist mode**
- Temporary 'Banned user' list**
- Manage MIME, file extension and download size**
- Block advertising and cookies**
- Policy based controls**
- logging, filtering and censoring of Instant Messenger applications**
- Search engine filtering**
- Temporary bypass controls**
- Configurable 'Site Blocked' page**
- 'Softblock' option**
- Stealth mode**
- Flexible request and content**
- Web proxy cache**
- Default 'safe' configuration**

BENEFITS

- Users can only access a customised list of 'allowed' sites.
- Ban selected users until a selected date or time and run reports with lists of 'banned users' and the duration of their bans.
- Filtering policies can be set to manage specific file types, and limit download sizes.
- Advertising and cookies can be automatically blocked.
- Different filtering policies can be created and set for different groups of users, in accordance with organisation policy or the AUP.
- Control and monitor the use of Instant Messaging applications. IM file transfers and attachments can be logged or blocked and selected words or phrases can be censored and set to trigger alerts with responses sent direct to users' messaging clients. Encrypted Instant Messaging is also supported.
- Filter, monitor and report upon search terms used and force "safe search" on popular search engines.
- Block page includes password protected options to bypass the filter on a temporary basis.
- 'Site blocked' page can be customised to include a logo, message text, a reason for blocking, un-block buttons, IP address and username.
- Instead of automatically blocking inappropriate content, users are issued warning messages about content and given options to either continue or cancel.
- Web pages are filtered and logged as normal, but are not blocked, allowing administrators to monitor activity without affecting users (useful when testing a new installation as it allows the filtering rules to be fine-tuned before 'going live').
- Modify web page requests and content 'on the fly' to enable neutralisation of malicious JavaScript and other web threats.
- Reduce bandwidth utilisation by storing and retrieving frequently accessed web pages from local disk storage.
- Guardian can be installed with a default 'safe' configuration which filters out a standard range of illegal and objectionable content. Note: Guardian's default 'safe' configuration matches the requirements of CIPA and BECTA standards.

AuThENTICATION FEATuRES

- Integrates with user Authentication systems**
- Multiple filter groups**
- Transparent proxy mode**
- Password-protected authentication**

BENEFITS

- Control access based on authenticated identity as opposed to assumed identity derived from a computer's IP address. Supports Apple and other mobile devices.
- Different filter policies can be allocated to up to 100 different groups of users. Particular users can also be configured to not be subject to any filtering at all.
- System administration is simplified with support for NTLM authentication in transparent proxy mode; which avoids the need to configure proxy settings for each user computer.
- The use of NTLM with password verification provides seamless single sign-on without the need for users to log into Guardian or enter their ID/ password again.

REPORTING FEATURES

Built-in report templates

Users can create, customise and save their own report templates and utilise an extensive range (300+) of report templates. Report options include site-specific reports (e.g. YouTube top viewed videos) and IM reporting (time spent messaging and chat friends per user).

Drill down to a single user or IP

Reports include the user name and IP address of the user PC so AUP violators can be quickly identified. A drill-down facility allows data to be explored to a greater depth - e.g., from a list of blocked sites that users have attempted to access, drill-down to find out which users have been trying to access any particular site. It is possible to view the entire browsing history (including time spent browsing) of a single user.

Automated reports

User-specific reports can be automatically time-scheduled to run on a daily or weekly basis. Reports can also be automatically saved or distributed to recipient lists via email.

AJAX real-time logs & traffic graphs

View web activity instantaneously, with the option to filter by user name, IP address, web site, category or group.

Export into PDF, HTML, Excel, Crystal Reports® user portal

Reports can be produced in a range of formats for ease of viewing (with pie charts/graphs) and to aid integration with existing systems.

Selected users (or groups of users) can be given access to a separate Guardian interface specifically for viewing reports/logs, controlling temporary bans and downloading SSL VPN clients.

Reports on domains and categories

Report on top domains, categories, page visits and offenders based on user, group and/or IP address.

Group/aggregate reports

Automatic data aggregation from multiple remote systems provides district wide reporting.

Incident alerts

Alert messages can be sent by both email and SMS text message to cell (mobile) phones for issues requiring immediate attention.

OPERATION FEATURES

Optional Bridge Mode (Transparent Inline Proxy) SWG Appliance Only

'Drop in' deployment - allows the appliance to be deployed inline between a switch and a perimeter firewall for ease of installation and configuration.

Rate limiter by URI

The speed or rate at which the proxy server can download information from the Internet can be limited. Bandwidth use can also be limited for specific URLs.

Support for browser autoconfiguration files

Provides WPAD (Windows Proxy Auto-Detection) and PAC file support, for automatic configuration of proxy settings in client browsers.

hardware healthcare alerts

Notifications about system resource issues (eg low disk space, high memory use, high CPU loads, UPS failures).

BENEFITS

EMAIL SECURITY & ANTI-SPAM OPTIONAL MODULE

SMTP Validity Checking

Checks for malformed email (usually either spam or designed to attack mail server/client vulnerabilities).

Grey listing

Mail from unknown senders may be temporarily rejected. Genuine email servers (as opposed to zombies or botnets) usually resend after a short delay - if a second attempt is made, the sender is then automatically added to the list of known senders.

Remote Blackhole list (RBL)

The option to utilise RBL services (maintained databases of IP addresses that are acting as open mail relays for bulk spamming).

hardware healthcare alerts

Notifications about system resource issues (eg low disk space, high memory use, high CPU loads, UPS failures).

EMAIL SECURITY & ANTI-SPAM OPTIONAL MODULE

Sender Domain Spoofing Prevention

Rejects any incoming email that falsely uses an internal domain in the 'from' address.

Disclaimer Footers

Ability to add standardised disclaimers to the footer of outgoing emails. Different disclaimers can be used for different domains.

Attachment Removal

Allows dangerous or unwanted attachments to be discarded based on type (e.g. executable files, documents and multimedia files).

Content Analysis (Mailshell 3.0 Spam Content)

Examines the content of messages in detail, including address fields, subject, headers, SMTP envelope content, email format, design and layout, image layout, hyperlinks, contact information, language and origin.

Reputation Checking

Sender reputations are determined using comprehensive 'real-time' databases of IP addresses, domains and email addresses of known spammers. Bayesian analysis is used to combat attempts to hide sender identity.

Bulk Mail Detection

Identifies if a message or similar messages were sent in bulk by creating 'fingerprints' based on message elements that are tough for spammers to fake or change.

Phishing

Identifies special formatting used to evade spam filters and for phishing attacks and economical bulk mailings (including image-only messages, HTML obfuscation and manipulation using relays). Analysis of the message header includes time stamps and the SMTP envelope.

user-configurable Spam Treatment Controls

Users have the option to add email addresses to their own blacklists or whitelists and set automatic rules for changing subjects, replacing content or sending to a quarantine mailbox. Quarantines can be set up for individual email addresses with daily 'spam trapped' email reports sent to users so they can view and release emails.

Near Real-Time updates

The software is updated every 5 minutes with the latest email fingerprints and detection rules.

UK + INTERNATIONAL

Smoothwall Ltd
1 John Charles
Way Leeds LS12
6QA United

+44 (0)800 5 999 040 UK
+44 (0)870 1 999 500
International
sales@smoothwall.net

Philippines

SAV25 Data Systems
7869 mckinley Street
Makati City
Philippines 1230

+ 632 893-2488
+ 632-984-6055
sales@sav25.com
www.sav25.com