Web Filtering and Reporting Suite

The award-winning Trustwave Web Filtering and Reporting Suite (WFR) helps organizations enforce AUPs and comply with regulations easily. Known for its fast performance and multi-tiered administration capabilities, the Trustwave WFR sits outside the flow of network traffic to quickly and accurately filter millions of websites in 100+ categories—without impacting bandwidth or productivity. This best-of-breed, appliance-based solution integrates Internet filtering, detailed forensic and executive reporting, and real-time monitoring of Web traffic and bandwidth use. It delivers reliability, unmatched scalability, and ease-of-use in one affordable solution.

Trustwave WFR Suite

Trustwave Web Filter: Optimized for speed, it filters URLs, IPs, anonymous Web proxies, spyware, botnets, IM, P2P, social media and other sources of emerging threats and is, enhanced by Intelligent Footprint Technology.

Trustwave Security Reporter: Processes and displays Internet filtering logs without impacting filtering and network functions. Built on a dedicated MySQL database, it provides customizable, at-a-glance dashboards and executive reports along with intuitive and extensive forensic, drill-down reporting to prove user intent. It also delivers up-to-the-minute graphical snapshots of Internet traffic and bandwidth use, and is supported by real-time management tools to identify and control user-generated Web threats and bandwidth use.

Key Features

- Internet Content Filtering
- Malware/Threat Blocking
- Proxy-pattern Blocking
- SafeSearch Enforcement
- Application Control
- Multi-tiered/Multi-layered Administration
- Detailed Internet Usage Control
- Directory-based Authentication
- Real-Time Threat Dashboard
- Bandwidth Monitoring and Reporting
- Trend Charting
- Intuitive Graphical Dashboard Reports
- Archiving

Key Benefits

Improves Productivity

- Manages end-user access to the Internet, eliminating time wasted on social networking sites, streaming media, gaming, Instant Messaging (IM) and Peer-to-Peer (P2P) applications
- Enables IT administrators to focus on mission-critical projects instead of filtering or reporting issues
- Allows multi-location/ delegated administration to streamline system and policy management
- Filters all tablets running on Android or iOS operating systems, while on premises.

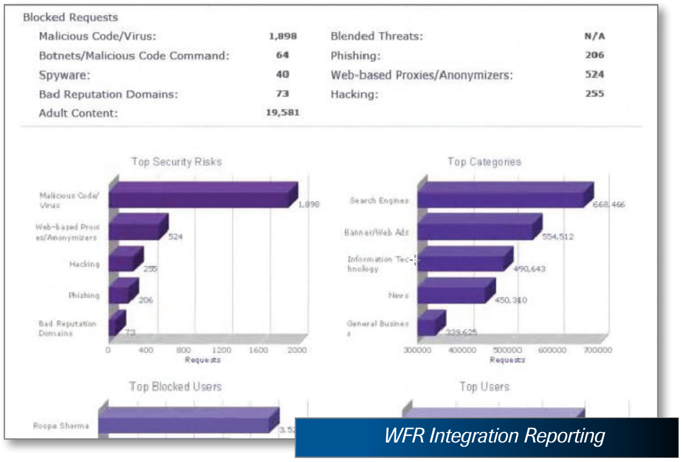
Reduces Liability

- Provides management with tools to enforce an organization's Acceptable Use Policy (AUP)
- Prevents legal liabilities resulting from exposure to inappropriate or offensive Web content
- Secures confidential information from spyware, phishing agents and P2P transfers
- Filters all Web traffic on all TCP ports by URL and/or IP address, file type, HTTP, HTTPS, FTP, newsgroups (NNTP) and TCP
- Scans millions of websites, classifying them into hundreds of categories to meet custom policy needs

Preserves Network Resources

- Monitors bandwidth use in real time
- Controls access to bandwidth-intensive sites and applications by user and groups
- Maintains firewall, proxy or cache for core functions

Trustwave Unified Security solutions provide layered protection from the Web, to applications, to the network, email and finally to the data. These solutions collaborate with Trustwave SIEM to share intelligence to uncover attack patterns that single products, acting alone, miss or cannot protect against.



Blocked Requests

Malicious Code/Virus:	1,898	Blended Threats:	N/A
Botnets/Malicious Code Command:	64	Phishing:	206
Spyware:	40	Web-based Proxies/Anonymizers:	524
Bad Reputation Domains:	73	Hacking:	255
Adult Content:	19,581		

WFR Integration Reporting

Internet Content Filtering

Trustwave Web Filter Database Filters the Internet via URLs and/or IP addresses, file types (e.g. MP3, MPEG, zip), HTTP, HTTPS, FTP, Newsgroups (NNTP) and TCP ports. Includes security categories on spyware, malicious code, and phishing sites.

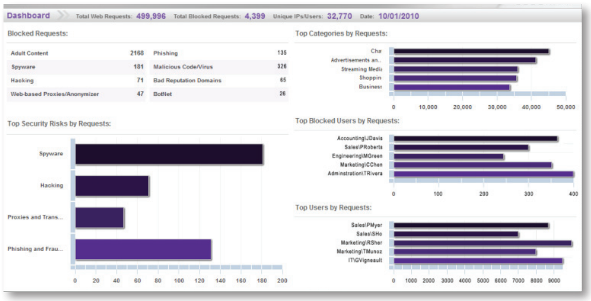
- Internet Threat Blocking: Includes spyware, malicious code, phishing sites and botnets (IRC, command-and-control).
- Proxy-pattern Blocking: Uses unique signature-based/ pattern detection to block anonymous proxies.
- "X-Strikes" Blocking: Locks down a workstation when administrator-defined thresholds for Web access are exceeded.
- Optional Remote User/Laptop Filtering: Extends an organization's Internet usage and security policies to remote users with the Trustwave Mobile Client option. Compatible with MACs and PCs.
- SafeSearch Enforcement: Forces the SafeSearch mode "on" for all searches, including images within search engines and enforces YouTube safety mode.
- Application Control: Uses Trustwave Security's Intelligent Footprint Technology (IFT) to block Instant Messaging and P2P servers by signature or pattern to block more than 125 types of streaming media, gaming, P2P, remote desktop and IM applications. Helps organizations demonstrate compliance, mitigate security risks, prevent data loss, and manage bandwidth more effectively.
- Multi-tiered/Multi-layered Administration: Administrators can define sub-administrator access control to their policy for specific AD/LDAP groups and users. Each sub-administrator can then create a unique filtering profile for their delegated users group(s)/IP range.
- Detailed Internet Usage Control: Provides the administrator the ability to block, warn, and manage Internet usage.
- Calendar-based Time Profiles: Enables profiles to be set by day, day of the week or day of the month. Recurrences can be configured for daily, weekly, monthly and yearly settings.
- Directory-based Authentication: Includes Windows Active Directory, Windows NT, Novell eDirectory, SunOne, open LDAP and transparent MAC authentication.

Real-time Monitoring and Mitigation

- Real-Time Threat Dashboard: Offers graphical "gauge view" of online activity, displaying an organizational snapshot of multiple threat categories and top offenders based on predefined thresholds and policies. Gauges are customizable to monitor different groups and threats.
- Alert Notification: Delivers automatic, predefined notifications via email, SNMP, or as an alarm in the system tray for excessive URL activity or bandwidth usage. Alerts display information regarding the user in violation.
- Real-time Mitigation: Locks out policy violators or users engaging in potentially threatening activity. Activated manually or automatically, the lock-out mechanism can be set to varying levels of restriction, from category lockout to complete quarantine.
- Bandwidth Monitoring and Reporting: Provides real-time bandwidth monitoring of inbound and outbound activity by protocol, port, and user.
- Bandwidth Quotas: Enables administrators to set up bandwidth quotas by protocols or ports. They can mitigate threats proactively based on excessive bandwidth usage.
- Trend Charting: Displays historical trending of Web activity and bandwidth usage based on predefined categories or protocols, enabling optimization of threat gauge settings.

Reporting

- Intuitive Graphical Dashboard Reports: Identifies anomalous Internet activities quickly through easy-to-read graphical reports, including the top-blocked users, top categories, top sites, etc.
- Custom or "Canned" Reports: Uses pre-set templates for quick reference, then drill-down for more details:
- Executive Reports: Provides powerful visibility into all Web-related activity.
- Detailed Forensic Reporting: Provides detailed drill-down reporting using unique criteria that help organizations build compelling forensic reports. User intent is gauged by documenting the full length URLs visited, as well as the search string used within a search engine text box.
- Report Memorization, Scheduling and Distribution: Ensures specific data inquiries can be saved or "memorized" for immediate or future access. Custom reports can be scheduled, executed, and automatically distributed via email at a preferred frequency.
- Archiving: For large installations or networks that generate significant Web traffic, Trustwave offers attached storage solutions to collect historical data for future inquiries.



Dashboard Total Web Requests: 499,996 Total Blocked Requests: 4,399 Unique IPs/Users: 32,770 Date: 10/01/2010

Blocked Requests:

Adult Content	2168	Phishing	135
Spyware	181	Malicious Code/Virus	326
Hacking	71	Bad Reputation Domains	65
Web-based Proxies/Anonymizer	47	BotNet	26

Security Reporter Dashboard

Deployment Options

Trustwave offers various options for installing a single Web Filtering and Reporting (WFR) appliance. The appliance can be deployed in pass-by/SPAN port mode (outside the flow of traffic) or pass-through mode (within the flow of traffic).

Pass-by/SPAN Port Mode

The Trustwave WFR is one of few Web filters that can be deployed outside the flow of network traffic. This type of deployment makes it transparent to the network and uninvolved in the routing of packets from client to the Internet. This allows for automatic redundancy and automatic fail-safe; if the Trustwave WFR should fail and filtering stops, network traffic is unaffected.

Pass-by/Router Mode

This mode allows the WFR to act as an Ethernet router, passing packets from one card to the other. As the packets pass through the WFR, they are scanned and categorized. In this model, only outgoing packets need to be routed, allowing the Web Filter to appear only in the outgoing path of the network traffic which limits the latency. In router mode, the original packets from the client are allowed to pass in all cases (just as if the WFR were an Ethernet router), but if the request is inappropriate, a block page is returned to the client to replace the actual requested Web page.

Pass-through/Firewall Mode

Trustwave WFR offers deployment options that work for each business needs. Although not a common deployment, WFR can be deployed as pass-through to force all outgoing traffic through the Web Filter. WFR will stop any inappropriate requests from progressing beyond the point of the Web Filter, so the caching server only returns Web pages that have been approved by the Trustwave WFR.

About 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.

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave®
Security begins with Trust℠