Trustwave
Smart security on demand

SECURE WEB GATEWAY FOR GOVERNMENT

FLEXIBLE, EASY-TO-MANAGE PROTECTION

Trustwave Secure Web Gateway offers government agencies the most accurate protection from next generation threats and the most flexible deployment options in the industry, providing the same high level coverage to remote, mobile and on-premise users. It provides true, zero-day protection with the ability to instantly analyze the "intent" of the code and enables safe, productive access to Web 2.0 while ensuring compliance, minimizing data loss and eliminating malware risks. Centralized policy control and a single interface make the solution easy to manage—whether deployed as a traditional appliance, virtual appliance, hybrid cloud or any combination of the three.

OVERVIEW

For government agencies who wish to safely take advantage of the Web and its social media tools, the Trustwave Secure Web Gateway (SWG) protects against dynamic, cross-component and Web 2.0 malware threats using patented real-time code analysis, analyzing the whole composition of a Webpage. Trustwave SWG is the only Web security provider in the industry to deliver this technology in a single solution. With Trustwave SWG, government agencies have safe access to Web 2.0 applications, reduce data breach risks, and manage productivity. Trustwave SWG is the most versatile, cost effective, secure Web gateway in the market today, with flexible deployment options to best suit your agency's needs.

Key features:

- Multi-Layered Anti-Malware Engine
- Web 2.0 Productivity Controls
- Advanced Application and Operation Controls
- Robust Deployment Options
- Flexible Policy Tools
- Detailed, Customizable Reporting
- Granular User Authentication and Identification
- Data Loss Prevention
- Built-in Web Filtering and Antivirus
- Inspection and Validation of SSL-Encrypted Traffic

KEY BENEFITS

Intelligent malware prevention

The Trustwave SWG multi-layered anti-malware engines are comprised of intelligent technologies that detect and block next generation malware that evades other solutions. This helps maintain productivity, reduces costly desktop re-imaging and cleanup, and safeguards data from data-stealing malware.

Safe and productive Web 2.0 use

Granular Social Media Control, coupled with the multi-layered anti-malware engine, allows users to access Web 2.0 and social media without worrying about malware infection, data leaks and productivity loss.

Security for all users, regardless of location or connection

Available as a traditional appliance, virtual appliance, or hybrid deployment option (both on-premise and cloud based), the Trustwave SWG extends full security and policy control to remote and mobile users.

Single solution for security, policy control and reporting

Regardless of the combination of deployment options used, government agencies can manage their security and reporting solution easily through a single, central interface.

Data Loss Prevention (DLP)

SWG scans inbound and outbound communication and identifies data-stealing malware, including keystroke loggers, phishing attacks, Trojans and root kits.

Furthermore, it creates policies, enforces rules (e.g., FISMA), and makes it easy to prevent users from posting or uploading sensitive data to social media sites.

SWG enables integration with other DLP solutions to extend the DLP capabilities. The combination of the SWG appliance and the DLP solutions provides government agencies with a state-of-the-art solution that prevents the loss or theft of confidential information over the Web.

Regulatory and AUP Compliance

Simple, yet robust SWG reporting facilitates tracking and analysis of potential policy breaches or regulatory violations (such as FISMA compliance). Because the Trustwave SWG prevents data loss, it enforces compliance with regulations that require data security and integrity. Furthermore, SWG flexible mechanism of enforcement of security-related policies and rules enables the support of various government regulations.

Affordable solution with low TCO

SWG cost saving features include convenient, flexible deployment options, ease-of-maintenance, scalability, adaptable malware detection and remediation, a future-proof design and single, centralized management. These features offer high value at an exceptionally low TCO.

Robust, flexible and easy-to-use reporting

Trustwave SWG includes complete out-of-the-box reporting. For additional reporting capabilities, the Trustwave Security Reporter can be integrated with the Trustwave SWG to provide powerful, easy-to-use reports (templates or custom-built), real-time dashboards and more. In addition, a complete set of packaged FISMA reports is offered; the reporting service automates scheduling and report distribution and includes a repository to archive reports, meeting the requirement of FISMA regulations.

Extended integration options

Trustwave SWG introduces the ICAP RESPMOD (Response Modification) and ICAP REQMOD (Request Modification), which enable SWG to communicate with all types of ICAP servers or client devices. ICAP, the Internet Content Adaption Protocol, is a lightweight protocol for executing a “remote procedure call” on HTTP messages. The common use case of extending the system’s functionality is by using ICAP to connect to DLP systems or anti-virus systems. The system can also be extended by utilizing the syslog built-in capabilities to export logs’ data to Trustwave Security Information and Event Management system.

WHAT WE CAN DO FOR YOU

Trustwave Unified Security Solutions for Government 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. By integrating products and correlating events, Trustwave can offer a ‘self sealing’ network, covering common use cases, like Bring Your Own Device (BYOD).

SC MAGAZINE AWARDS 2013 WINNER

> “The SWG offers a unique and very effective range of security measures against web threats. It is easy to deploy and configure, with the latest code adding a number of useful new features, including greatly improved reporting.”
>
> *Dave Mitchell, SC Magazine*

ADVANCED THREAT PROTECTION

Real-time Code Analysis
With Trustwave SWG Real-Time Code Analysis technology, government users are able to detect and block advanced, dynamic malware with precision and accuracy. As inbound and outbound Web communication occurs, it is dynamically analyzed and viewed by multiple malware engines to determine intent. These engines run in parallel, providing the industry’s fastest and most accurate performance, minimizing latency and virtually eliminating inaccuracies experienced by other security solutions.

- Detection and blocking of advanced, dynamic malware from cross-component attacks
- Highly accurate detection rate of malicious code on HTTP and HTTPS Webpages
- Fast detection and remediation for productive Web (and Web 2.0) use
- Comprehensive Webpage analysis of both single and multiple component attacks

Zero-hour defense
Instead of blocking malicious content that matches a pattern, signature, or algorithm, Trustwave Vulnerability Anti-dote blocks malicious content that attempts to exploit known vulnerabilities (by detecting weaknesses before a patch is applied)—eliminating exposure to the threat. It is the only technology that provides true zero-hour defense against unpublished vulnerabilities.

Data Loss Prevention

Through granular social media controls, government enterprises can freely open up access to social media sites, knowing posts, comments or uploads are controlled and monitored. Additionally, the Trustwave SWG is the best solution for protecting against even the most complex threats designed to steal data, further securing sensitive information. This combination of granular controls and advanced protection prevents data loss to maintain acceptable use, simplify compliance of data-related mandates, and secure sensitive information. For those who already have a robust DLP solution, the Trustwave SWG is a full ICAP proxy, enabling direct communication with the DLP solution of choice.

PRODUCTIVITY

Application control
With the Trustwave SWG, costs normally associated with excessive bandwidth consumption and malware-related desktop remediation are vastly reduced. Trustwave Granular Social Media Control enables government agencies to grant full access to those who need it and block posts, comments, or uploads for those who do not need access to sites like Facebook or LinkedIn.

Global policy control
Trustwave SWG extends the same level of on-premise security and policy control to mobile workers and remote offices. It ensures consistent real-time protection from dynamic Web threats to users, regardless of their location.

Trustwave Web Filter list
Trustwave Web Filtering capabilities provide government users with an industry-leading filtering technology with more than 100 categories for granular Acceptable Web Usage Policy enforcement.

Content acceleration/caching
Content acceleration with built-in caching capabilities offers users fast Webpage load time while they remain protected from malicious content, leading to a safe and productive workforce.

MANAGEMENT

Centralized Management

Trustwave Secure Web Gateway has a centralized policy manager with a comprehensive single interface. The changes in configuration are done on one location and automatically distributed to the scanners. The distribution options and intervals can be easily configured, and the distribution process can easily be monitored.

Reporting

The Trustwave Security Reporter is a fast, high-performance security reporting solution that provides complete visibility into a government agency's Web traffic. It enables government agencies to analyze Web traffic trends for remediation, execute proactive notifications, and review security analytics. It provides the largest data processing range available today.

Industry and regulatory compliance

Government agencies require solutions that demonstrate proof of regulatory compliance for FISMA. The Trustwave Security Reporter provides an easy-to-use interface, consolidated threat monitoring, and historic reporting with an extensive archiving capacity of up to 12 TB for proof of compliance.

Flexible deployment options

The scanning server component of the Trustwave SWG is available on a number of platforms including traditional appliance, virtual appliance, cloud based virtual appliance and virtual appliance platform service.

These platform options can be mixed in a Hybrid Deployment with two important benefits. First, full security can be extended to remote/mobile workers. Second, flexibility in the deployment architecture allows a close fit with an agency's network infrastructure, geographic coverage, cost and resource requirements.

Trustwave®

Smart security on demand

For more information: https://www.trustwave.com.