



**WEBGUARD®**

Secure Web-Browsing Management



One quarter of employees waste 30% of their time online at work

(YouGov PLC)



## WEBGUARD®

### Secure Web Browsing Management

WebGuard protects business networks, and the assets they contain, by eliminating malware and viruses before they reach your network.

#### The Business Challenge

Web-browsing presents one of the fastest growing threats to your network, and ultimately your business. More malicious software is downloaded from innocent web-browsing than is received via infected email. Our research suggests that a new piece of malware (malicious software designed with criminal intent) is introduced approximately every six seconds.

This malware is embedded in perfectly legitimate websites (Sony Playstation, Business Week are two examples of sites recently found to be unwittingly hosting such malware) and downloaded without the user being aware of it. And unlike viruses, which are designed to cause immediate and obvious damage, malware can sit in your network undetected, quietly gathering information that can be used for criminal purposes.

#### Secure Web Content Filtering 'in the Cloud'

WebGuard protects business networks from web-based threats by filtering web-browsing, and eliminating malware and viruses before they reach your network. It provides easy management of staff Internet usage by controlling access to websites deemed unsuitable. WebGuard allows you to block or set time limits for staff web surfing or social networking which not only costs your business financially in terms of bandwidth usage, but also lost productivity.



## Features

Zero Onsite Software or Hardware Footprint

Anti-Virus and Malware Detection

Real Time Website Categorisation

Secure Browsing when Roaming Outside the Corporate Network

Comprehensive Service Level Agreements (SLA)

24-Hour Provisioning Service Level Agreement

## Benefits

Delivers low Total Cost of Ownership (TCO)

Delivered as fully managed Software-as-a-Service, WebGuard requires no hardware and no software licensing costs and avoids the need for expensive integration costs associated with on-premise solutions. With no technology to maintain, total cost of ownership is five to 10 times less than the traditional on-site application-hosting model.

Real-time Network Protection

WebGuard keeps viruses, files and unwanted web content outside your network. Drawing on a comprehensive URL database, or by real time content inspection, staff access to high risk websites can be controlled by site categorisation.

Delivered as SaaS (Software-as-a-Service), WebGuard's global filtering network neutralises web-based threats before they infect workstations, protecting your business from diminished network performance and data leakage.

Performance Guaranteed

WebGuard is governed by strict Service Level Agreements (SLA) with 100% service uptime guarantee.

Fast Deployment and Seamless Protection

WebGuard requires no onsite software or hardware installation and through the use of Windows Active Directory can be deployed in minutes to an entire organisation. In addition, authentication of users can be enabled transparently and securely using Windows NTLM.



### Detailed Management Reporting

### Drive Down Costs

Almost every business could reduce their bandwidth usage by gaining transparency around what's being downloaded and whether it's for personal or business use. WebGuard's easy to navigate reports provide the necessary visibility around web usage and highlight where bandwidth savings can be made.

### Improved Productivity

WebGuard promotes increased user and IT staff productivity and a safer work environment by enabling you to set reasonable guidelines and parameters around Internet usage. Delivered as a fully managed service, WebGuard frees up time for IT management to focus on mission-critical projects rather than web security management.

### Set Organisational, Group or Individual Policies to Manage Staff Browsing in Real Time

### Enforce corporate compliance

WebGuard provides protection against content-related legal liabilities and reputation-damaging web content by allowing you to put in place policies to manage and, where appropriate, restrict web browsing. These policies can block and/or report access to certain sites such as gambling, pornography and hate sites, as well as restrict access to sites such as Twitter and Facebook during certain hours.



## Key Security Benefits

### Web Anti-Virus

Staff accessing websites depend on their desktop anti-virus software to protect them from downloaded malware. This puts the onus on individual staff members to ensure their antivirus software is kept up-to-date and that their computer is configured to scan every download. By the time a virus becomes scannable by desktop anti-virus, it's already inside the company network.

WebGuard automatically checks every website and download for virus and security threats against the latest (SLA backed) anti-virus libraries available before they enter your network.

### Trojan

A trojan is a program that installs malicious software while under the guise of doing something else. Trojans are notorious for installing backdoor programs, to allow remote access to the victim's machine by unauthorised parties - usually with malicious intent.

WebGuard can detect and block trojans from being downloaded through its signature heuristic identification engines.

### Prevent Leakage of Sensitive Information

Social networking sites are extremely popular, and can easily be used to publicly share sensitive information. This unnecessary risk can be prevented.

WebGuard can block websites based on category: Social networking and blogging being the most effective. Preventing leakage of sensitive information is a sound investment in information security.

### Drive-by Downloaders / Key Loggers

Drive-by downloaders automatically execute programs from websites by taking advantage of vulnerabilities in browser security. Key loggers are programs that are often downloaded as part of "free software" or automatically by "drive-by downloaders". They compromise the security of your user credentials.

WebGuard manages website access by category and file-type to ensure users are not downloading dangerous and non-approved software onto work computers.

### Phishing

Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay and PayPal are often targeted, along with online banks.

WebGuard protects staff from accessing known phishing sites and draws on global phishing databases, together with one of the most comprehensive phishing databases — compiled by MailGuard.

### Reporting on Security Breaches

Reporting on security breaches can be difficult, especially if it is not known where the breach has originated. This is usually done manually and as a reactive measure once the breach has been resolved.

WebGuard offers enhanced reporting which can rapidly identify how many infections have been blocked. It allows administrators to identify which users are attempting to download or access harmful content, and act accordingly.



## Risk Profile Reporting

Efficiency and high staff productivity are two key benefits of a well maintained network. With WebGuard, highlighting gaps in productivity and efficiency has never been easier.

WebGuard Risk Profiling is based on sophisticated fact-based reporting techniques, which highlight the aspects of the user's browsing behaviors which put the company at risk. It also highlights the aspects which are affecting the productivity of your business.

## Advanced Authentication

The setup and management of multiple usernames and passwords for every staff member requires additional effort by network administrators. Staff forgetting their usernames or needing new passwords wastes the time of both the staff member and the administrator.

Instead, WebGuard uses Microsoft's secure NTLM authentication to seamlessly identify staff without the need for additional credentials. Once the user is logged into their computer, they are automatically identified by WebGuard.

User identification allows policy customisation and reporting on a per-user basis.

Microsoft networks, and Windows desktops are already configured for NTLM.

“ Universities of Sydney, Melbourne and Tasmania were sued by record companies after their computer networks were harnessed by students to illegally copy music

(The Age) ■■

## MailGuard

MailGuard is one of the largest providers of SaaS managed online solutions addressing security, compliance and online management, serving thousands of clients across 18 countries.

For more information on WebGuard or any other MailGuard service, contact:

### **Sales**

+61 3 9694 4444 or 1300 30 44 30  
sales@mailguard.com.au

### **Technical Support**

1300 30 65 10  
support@mailguard.com.au

### **Head Office**

68-72 York Street, South Melbourne  
Victoria, Australia 3205  
1300 30 44 30 or +61 3 9694 4444  
Fax: +61 3 9011 6110

[www.mailguard.com.au](http://www.mailguard.com.au)

### **MailGuard Pty Limited**

Copyright © 2009 MailGuard Pty. Ltd.