dotDefender™

for

Web Application Protection

White Paper

Contents

The Challenge **4**

The Problem of Securing the Web **4**

dotDefender™ — A New Approach **4**

Broad Attack Coverage **5**
- Web Application Attacks 5
- Session Attacks 5
- Known Attack Sources 6

dotDefender Technology **6**

dotDefender Architecture **6**
- Pattern Recognition 6
- Session Protection 7
- Signatures Knowledge-base 7
- dotDefender Features 7

Working with dotDefender **8**
- Basic Security Settings 8
- Attack Categories 8
- Protection Rules 9
- Logs 9

Performance **11**

Platforms Supported **12**

Limitations of other Solutions **13**

About Applicure Technologies LTD. **14**

Document Revision: January 2007

© 2007 Applicure Technologies. All rights reserved

Terms and Acronyms

The following terms and acronyms are used in this document:

Term / Acronym	Description
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SMB/E	Small-to-Medium Business/Enterprise
ISAPI	Internet Server Application Program Interface
ISA	Internet Security and Acceleration Server
Apache Server	Apache server is an open source web server software produced by Apache Software Foundation (http://www.apache.org/). It is the most commonly used Web server on the Internet; it is available on platforms such as Windows, Unix/Linux, and Mac OS X.
IIS Server	IIS (Internet Information Services) is a Web server produced by Microsoft(http://www.microsoft.com). For more information: http://www.microsoft.com/iis.
ISA Server	Microsoft Internet Security and Acceleration Server is an integrated edge security gateway that helps protect the IT environment from Internet-based threats while providing users with fast and secure remote access to applications and data. For more information, visit the Microsoft Internet Security and Acceleration (ISA) Server TechCenter at http://www.microsoft.com/isaserver.

© 2007 Applicure Technologies. All rights reserved

The Challenge

The Problem of Securing the Web

In recent years, web applications have become business criticial across all sectors. Companies operate E-commerce sites, online services such as banking, so that applications have become a crucial medium for business to interact with customers.

However, the very success and open nature of the Web has made it a more susceptible to increasingly sophisticated attacks threatening to disrupt Web functionality, or use it as an 'open door' to gain access to sensitive data. Most disheartening, the standard security measures in place for protecting network traffic (network firewalls and Intrusion Detection System/ Intrusion Prevention Systems (IDS/IPSs) offer no solution to this problem.

Network firewalls are designed to secure the internal network perimeter except for ports 80 and 443 (industry standard HTTP access to the Internet), leaving the corporate web assets exposed to various application attacks. IDS/IPSs do not provide Layer 7 analysis of packet contents—such attacks that are embedded within HTTP simply pass through undetected. Thus, despite employing security measures, many organizations are still vulnerable to the growing wave of application attacks perpetrated by hackers and criminal frauds.

A web application security solution is needed to protect all organizational assets:

- External websites
- Internal applications (e.g. CRM or ERP)
- Extranet applications

dotDefender™[1] — A New Approach

The growing need for application security calls for the development of a new approach that provides effective protection functionality and, at the same time, is cost-effective and simple to deploy and maintain. AppliCure Technologies LTD. meets the challenge: dotDefender™ is a 100% software-based solution that is deployed on the Web server itself.

dotDefender has been designed to achieve the following goals:

- **Effective, powerful Web security**

dotDefender is deployed as a Web server plug-in, to provide security inherent in the application. dotDefender leverages the Web server's inherent HTTP parsing, interpreting and decrypting capabilities. dotDefender provides powerful coverage against a range of attacks, including application attacks, session attacks, and known attack sources.

- **Plug-and-play deployment and maintenance**

dotDefender is a purely software-based solution. This software can be installed within minutes on the web server, with no need to modify the network architecture. No

[1] **Note: dotDefender™** is a trademark of AppliCure Technologies LTD.

© 2007 Applicure Technologies. All rights reserved

additional resources and laborious configuration procedures are required. As dotDefender is installed with predefined best-practices security rules, the software can secure the Web environment immediately after installation. Since rule-based security generates few false positivies, ongoing maintenance is negligible. An automatic live update ensures continuous protection against emerging threats and 0-day attacks.

- **Cost-effective protection**

The combination of powerful security at a competitive price and effortless maintenance, make for excellent ROI.

Broad Attack Coverage

dotDefender provides comprehensive protection capabilities that enhance organizational security posture. dotDefender complements the network firewall and other network security products by intercepting seemingly legitimate users attempting to use the web application to commit fraud, or gain access to valuable and confidential information.

dotDefender provides web environment security according to the categories described:

Web Application Attacks

dotDefender detects and blocks attacks that display within the HTTP request logic.

- **SQL Injection**—dotDefender intercepts and blocks attempts to inject SQL statements, queries or commands, causing corruption or manipulation of corporate data
- **Cross-site Scripting**—dotDefender intercepts and blocks attempts to inject malicious scripts that cause user account hijacking, information theft, or malicious code execution
- **Encoding**—dotDefender detects attempts to disguise an attack, using character encoding
- **Path Traversal—**dotDefender blocks attempts to navigate through the host's internal file system, in order to traverse between directories on a corporate file system
- **Header Tampering**—dotDefender identifies and blocks requests containing corrupted header data
- **CRLF Injection**—dotDefender blocks attempts to inject CR/LF into parts of HTTP response headers, embedding malicious HTML tags, or completely rewriting the body of HTTP requests
- **Remote Command Execution**—dotDefender detects attempts to execute OS commands or programs installed on that web server
- **Windows Directories and Files**—dotDefender detects attempts to attack a publicly available directory or file on a Web servers
- **Probes**—dotDefender detects attempts to breach the server, taking advantage of common practices and educated guesses

Session Attacks

dotDefender blocks and intercepts security attacks at the user session level.

- **Session Hijacking**—overtaking (hijacking) a legitimate user to perform unauthorized operations
- **Denial of Service**—dotDefender detects and blocks attempts that threaten to overwhelm server functionality and cause the server to crash
- **Cookie Tampering**—attempts to tamper with session cookies, an attack

© 2007 Applicure Technologies. All rights reserved

aiming to modify user information stored in cookies

Known Attack Sources

dotDefender identifies known attack sources and blocks requests originating from them.

- **Bad User-Agents Signatures**—dotDefender blocks suspicious connection attempts made by application scanners which map the application and find points of failure
- **Compromised Servers**—dotDefender intercepts and blocks requests originating from servers that are recognized as compromised and are used for automated attacks
- **Anti-Proxy Protection**—dotDefender blocks attempts to fraudulently abuse a web server to become a public proxy server that will be used to anonymize web servers
- **Known Worm Signatures**—dotDefender blocks requests bearing signatures of known worms that exploit application vulnerability
- **Known Spammer Crawlers**—dotDefender intercepts targeted attempts by spammer bots to access e-mail addresses, IP addresses, Page Links and other confidential proprietary data

dotDefender Technology

dotDefender Architecture

Designed with innovative architecture, dotDefender provides powerful application-level protection, as well as enhanced user session protection. Where desired, specific settings customization is easily accomplished via dotDefender's intuitive administration GUI.

dotDefender is deployed as a web server security plug-in which inspects incoming requests as they are processed by the server. This allows dotDefender to deliver excellent performance, and support all types of encryption.

dotDefender's HTTP security engine checks all incoming requests for signs of malicious use by comparing against attack patterns, session attacks, and signatures. The dynamic security engine scans each part of the request and the cookies sent by the user for malicious code. dotDefender also takes into consideration encoding and byte range that are used by hackers to camouflage harmful code. The flexibility that allows dotDefender to look into each part of the request ensures that emerging types of attack can be effectively countered, through dynamic updates to security rules.

dotDefender uses a rule-based security model that is simple to configure, and can apply web site protection immediately, without requiring a long learning period. Additionally, rule-based security makes for efficient maintenance because it generates few false positives. dotDefender also incorporates positive security elements to support any deployment scenario.

dotDefender's website protection rules and signatures are regularly updated by Applicure Technologies. Application security rules are submitted for confirmation by the administrator to ensure that they apply to customized deployments. Signatures of known attack sources are automatically updated.

Pattern Recognition

dotDefender checks incoming traffic for patterns that indicate attack attempts. The

© 2007 Applicure Technologies. All rights reserved

dotDefender engine can identify attack patterns in any part of the request for granular and accurate HTTP security. A whitelist mechanism is also provided for customization.

Session Protection

dotDefender uses digital signatures, encoding validation, byte range enforcement and other techniques to protect against attempts to tamper with cookies for session hijacking and other modes of attack. dotDefender also intercepts denial of service attacks at the application level that cannot be detected by network security solutions.

Signatures Knowledge-base

Applicure Technologies collects and confirms a listing of known attack sources, that dotDefender downloads automatically for cutting edge, continuous web server security. dotDefender also identifies user agents associated with penetration attempts.

dotDefender Features

- **Powerful website security**

dotDefender protects Web applications from malicious application-level attacks.

- **Rapid installation and integration**

Installed as a web server plug-in, dotDefender™ provides tight security quickly and efficiently. dotDefender does not impact network traffic or architecture. Users simply install the plug-in on the their web server and enjoy unbreachable application security.

- **Out-of-the-box web application protection**

dotDefender™ is supplied with a best-practices set of rules that provide out-of-the –box application protection.

- **Performance**

dotDefender™ utilizes negligible web server resources and handles encryption transparently to prevent network performance degradation.

- **Automatic live update**

Automatic live update of rules and signatures ensures continuous, up-to-date protection available to stop the latest attacks.

- **Simple to customize and maintain**

dotDefender is easy to customize through a user-friendly GUI interface. Once installed , dotDefender provides a high level of continuous security, with the least maintenance effort.

- **Cost-effective**

dotDefender™ delivers excellent ROI from installation to maintenance, liberating clients to focus on their business goals.

© 2007 Applicure Technologies. All rights reserved

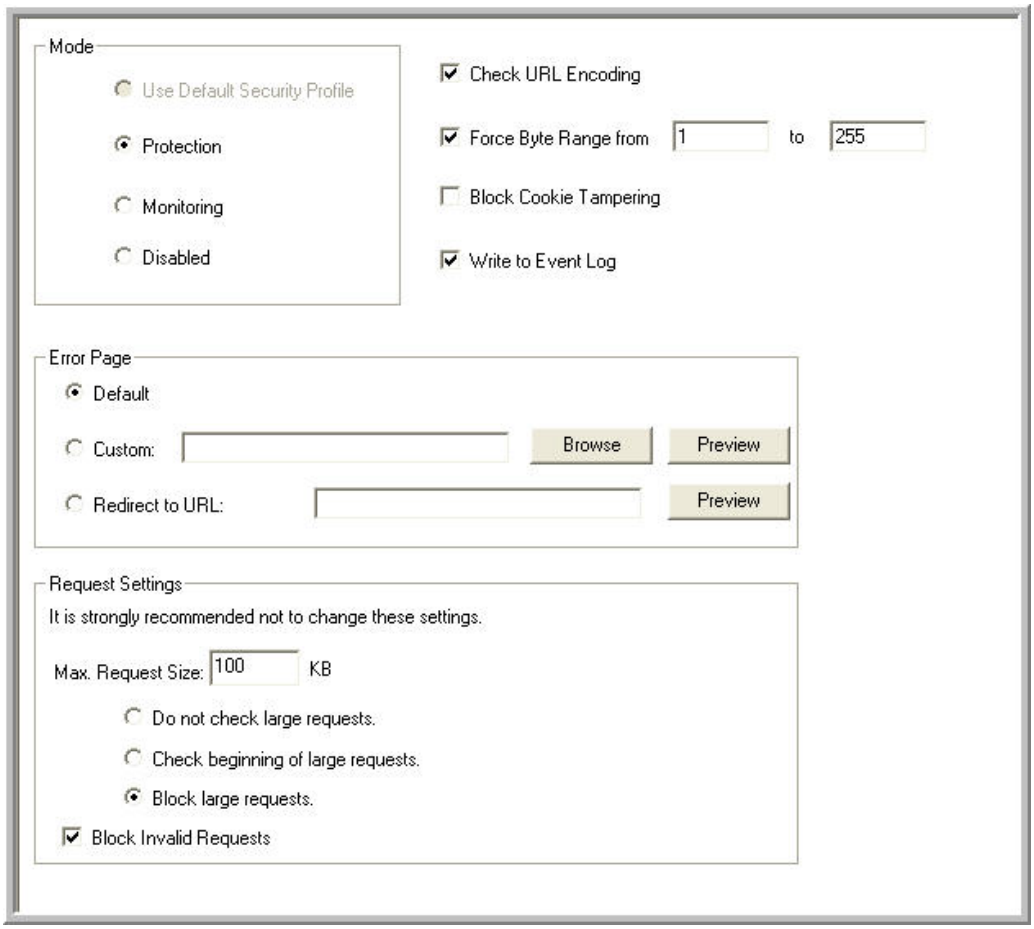
Working with dotDefender

Basic Security Settings

dotDefender is easy to configure for the specific needs of any environment. Its primary configuration capabilities are as follows:

- **Site mode** determines protection settings for each website or application on the server — default security, customized protection, monitoring only, or disabled.
- **Error page** determines which page to send as a response to a security breach, and logging options.
- **More settings** control a variety of security features for each website or application.

Shown below is dotDefender's **Default Security Profile** window.



Attack Categories

dotDefender protects against a broad range of application attack categories. Each category includes rules that stop a specific type to attack. Each attack is briefly described, including potential damage and links for more information.

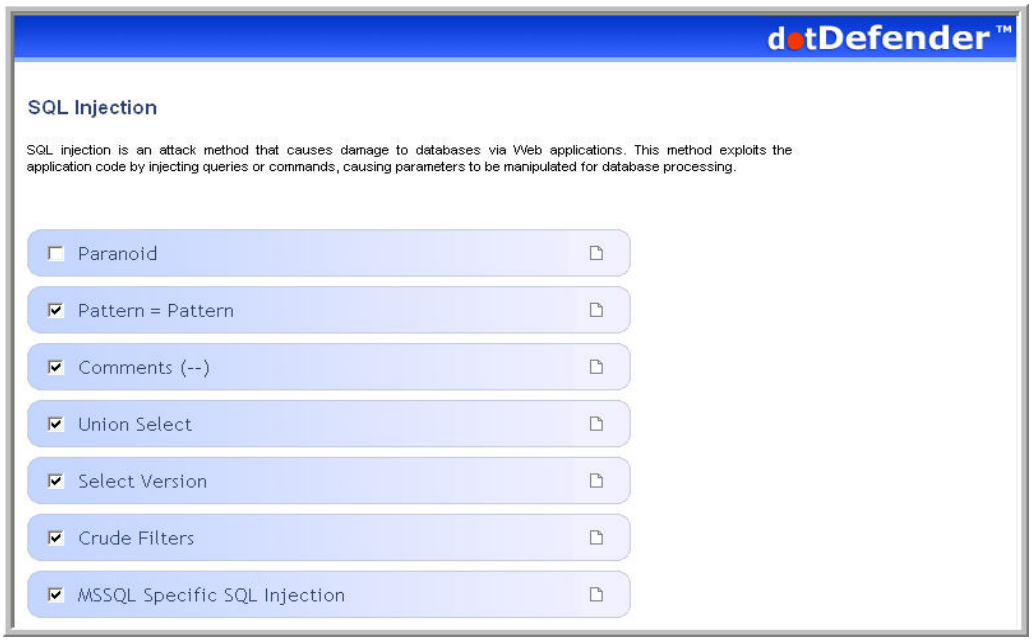
Shown below is dotDefender's **SQL Injection** window.

© 2007 Applicure Technologies. All rights reserved

Protection Rules

For each attack category, dotDefender provides a set of protection rules. Applicure provides a set of Best Practices rules. Users may also remove or add protection rules.

The dotDefender **SQL Best Practices** window is shown below.

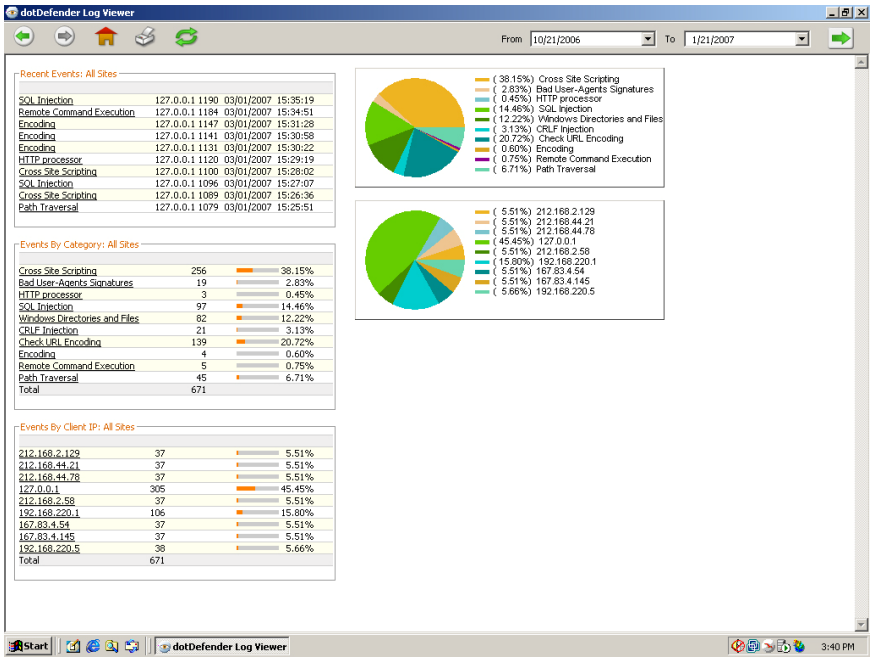


Logs

Every attack attempt is logged by dotDefender and made available for viewing via the dotDefender **Log Viewer**. A detailed account for each attempt includes the IP address, date and time, malicious content, the action taken, the attack category and protection rule.

© 2007 Applicure Technologies. All rights reserved

An example of dotDefender's **Log Viewer** window is shown below.



© 2007 Applicure Technologies. All rights reserved

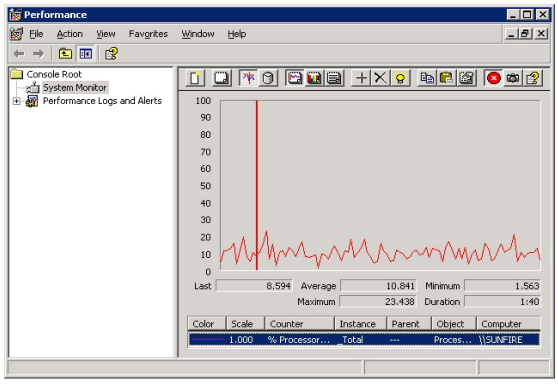
Performance

A test was conducted where 100 requests per second were sent to the server, in order to measure the effect of dotDefender on server performance, when numerous requests arrive in a short period of time. The results are provided below.

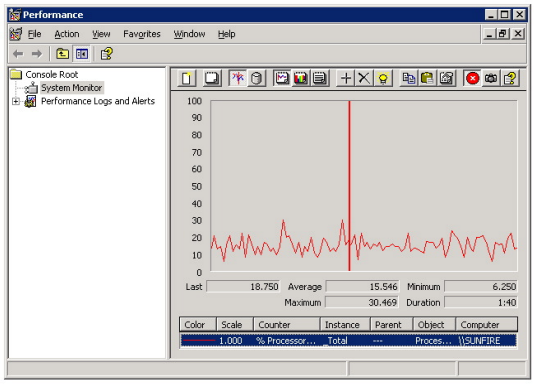
	Server only	dotDefender™ working
Average server bandwidth (Kb/ sec)	865.04	864.04
Average server bandwidth	57.67	57.60
Total work time	122587ms	122546ms
Total pages made	12139	12121
Total average pages per second	99.13	99.01
Average CPU usage	10.841%	15.546%

The CPU usage is shown below.

Server only



dotDefender™ working



© 2007 Applicure Technologies. All rights reserved

Platforms Supported

dotDefender currently supports the following platforms:

dotDefender for Apache Server Versions Supported: >1.3.21 > 2.0.42 > 2.2.X Perl interpreter installed	**Operating Systems & Hardware**
✓	Linux (packages: rpm, Debian, Generic)
✓	Solaris 8/9/10-SPARC Solaris 10-X86
✓	Free BSD–X86
✓	MacOS 10–PPC Intel

dotDefender for IIS Server IIS 5.0/5.1/6.0	**Operating Systems**
✓	Windows 2000
✓	Windows 2003
✓	Windows XP

dotDefender for ISA 2006 Server	**Operating Systems**
✓	Windows 2003

© 2007 Applicure Technologies. All rights reserved

Limitations of other Solutions

Web application firewalls protect web applications from attacks. Firewalls tend to be network-based appliances that are positioned in front of the Web environment, analyzing incoming HTTP requests and blocking requests that are deemed hostile. While they are able to provide a measure of protection against most attacks, their remote location and hardware-based orientation create limitations.

- **Performance issues**

Conventional Web application firewalls are network solutions that provide application-level protection. Thus, in order to intercept and analyze potentially damaging traffic, they must independently perform their own packet inspection that add to response time. Similarly, they must independently decrypt coded traffic in order to analyze it prior to forwarding it to the Web server, causing further performance degradation.

- **Deployment issues**

Because conventional Web application firewalls are network appliances, deploying them impacts the network architecture. Network add-ons and expansion directly impacts network performance and latency. Moreover, these devices can only be deployed in suitable architectures, and cannot provide a solution for every environment.

- **Cost of Ownership**

As hardware-based solutions, conventional Web application firewalls are costly to produce, resulting in high purchasing cost. This leads enterprise customers to question additional large investments, and put Web security expenditure well beyond the reach of SMBs/SMEs. In addition, devices use learning-based security that studies the regular traffic of an application, and stops all exceptions. This method adds the following limitations:

- False positivies: learning-based security generates a high level of false positives, a limitation that requires daily maintenance by security knowledgeable staff.
- Changes to the application: for every change in the application, the learning process needs to be repeated, resulting in long deployment time for updates and changes

© 2007 Applicure Technologies. All rights reserved

About Applicure Technologies LTD.

Applicure Technologies Co. develops software-based products for web security and database compliance. At Applicure Technologies we believe that security and IT controls have to be efficient and cost-effective so that our customers are free to focus on their business goals. Our products employ cutting-edge technology, simple product roll-out and easy maintenance? all at an affordable price.

The company was established in 2004 and has quickly gained reputation among market analysts and specialists. IT Week recognized Applicure's achievements and named it one of the Top 100 Vendors in 2006.

To learn more about Applicure and dotDefender, visit http://www.applicure.com

Applicure Technologies US
Main Office: (516) 661-1900
Atlanta Regional Office: (770) 656-0777

Applicure Technologies UK
Main Office: 0207-936-9755

Applicure Technologies Israel
+972-9-957-9096

© 2007 Applicure Technologies. All rights reserved