



# **Applicure Whitepaper**

**Network Firewall Protection Is Not Enough**  
**November, 2007**



## Table of Contents

Introduction.....	3
Top Reasons Firewalls Are Not Enough.....	3
Extreme Vulnerabilities .....	3
TD Ameritrade Security Breach .....	3
OWASP’s Top 10 Web Application Security Vulnerabilities 2007.....	4
Web Application Security Consortium Most Common Vulnerabilities Report .....	4
Application Protection Solution .....	5
Protect Your Hosting Customers .....	6
Understanding Application Security .....	6
Who is Applicure? .....	8
Applicure’s Products .....	8
dotDefender .....	8
dotDefender Monitor.....	9
dotDefender’s Role in Application Security .....	9
Applicure and Your Hosting Company .....	11
Generate Additional Revenue for Your Hosting Company .....	11
Application Protection Partner .....	11
Comprehensive Solution.....	11
Simple Operation .....	12
Why Applicure? .....	12
Global Presence .....	12
Invested Company .....	12
Recognition .....	12
Start Protecting Your Customers in Less Than 30 Minutes.....	13
Free 30 Day dotDefender Evaluation .....	13
Free Ongoing dotDefender Monitor License .....	13
Contact Applicure Today .....	13

## **Introduction**

Website owners are vulnerable to unwanted intrusions by malicious hackers and other harmful code. If a website's server and applications are not protected from security vulnerabilities, identities, credit card information, and billions of dollars are at risk. Currently there are thousands of vulnerabilities and attacks appearing globally that must be stopped before damage occurs. Many hosting companies rely on a firewall to protect their customers' servers and websites from security breaches. Unfortunately, firewalls do not provide enough protection.

## **Top Reasons Firewalls Are Not Enough**

The standard security measures for protecting network traffic, network firewalls and Intrusion Prevention and Detection Systems (IDS/IPS), do not offer a solution to application level threats. Network firewalls are designed to secure the internal network perimeter, leaving organizations vulnerable to various application attacks. Intrusion Prevention and Detection Systems (IDS/IPS) do not provide thorough analysis of packet contents. Applications without an added layer of protection increase the risk of harmful attacks and extreme vulnerabilities.

## **Extreme Vulnerabilities**

Web Application Level Attacks - In the past, security breaches occurred at the network level of the corporate systems. Today, hackers are manipulating web applications inside the corporate firewall. This entry enables them to access sensitive corporate and customer data. An experienced hacker can break into most commercial websites with even the smallest hole in a company's website application code. These sophisticated attacks have become increasingly threatening to organizations even as recent as September 2007. For example, TD Ameritrade, a Fortune 1000 company, had millions of customers' personal data stolen by a hacker or rogue employee.

## **TD Ameritrade Security Breach**

Experts suggest that while financial firms may be securing the front doors of their companies with encryption and authentication technologies, hackers are constantly looking for new ways to compromise systems through unguarded, and sometimes not so obvious, side doors. The personal data of approximately 6.3 million TD Ameritrade customers was stolen by a hacker. In this incident, a hacker planted malware on the company's server and it managed to go

unnoticed for weeks. Unfortunately, traditional security measures cannot prevent these multistage, back-door attacks.<sup>1</sup>

The standard security measures for protecting network traffic do not protect against web application level attacks.

## **OWASP's Top 10 Web Application Security Vulnerabilities 2007**

Open Web Application Security Project (OWASP)<sup>2</sup>, an organization that focuses on improving the security of application software, has put together a list of the top 10 web application security vulnerabilities.

1. Cross Site Scripting (XSS)
2. Injection Flaws
3. Malicious File Execution
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to Restrict URL Access

## **Web Application Security Consortium Most Common Vulnerabilities Report**

According to the Web Application Security Consortium (WASC), an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best-practice security standards for the World Wide Web, reported the top five web application vulnerabilities by testing 31,373 sites.<sup>3</sup> (See Figure 1)

---

<sup>1</sup> Excerpted from "Locking the Back Door" by Melanie Rodier (<http://www.wallstreetandtech.com/>) or view article "Financial Firms Continue to Struggle to Plug Security Loopholes" online at <http://www.wallstreetandtech.com/showArticle.jhtml?articleID=202600762>.

<sup>2</sup> Open Web Application Security Project (OWASP): [http://www.owasp.org/index.php/Main\\_Page](http://www.owasp.org/index.php/Main_Page)

<sup>3</sup> Web Application Security Consortium (WASC): <http://www.webappsec.org>

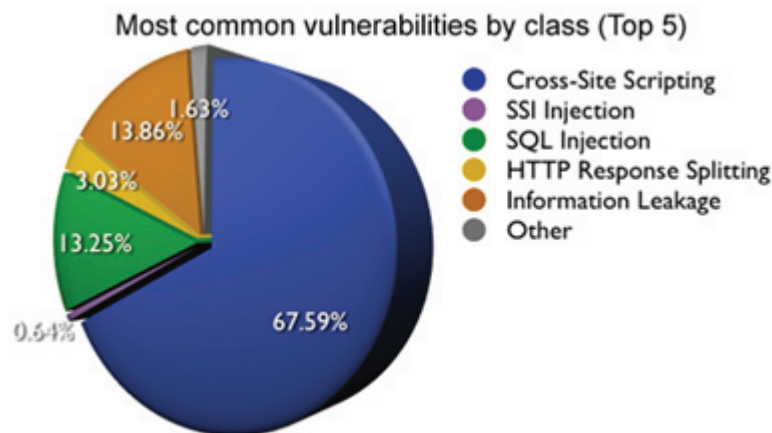


Figure 1

Web applications can be secured and protected from vulnerabilities by implementing application protection. Applicure's dotDefender™, a solution developed exclusively for web application security, protects applications from OWASP's top 10 and WASC's most common vulnerabilities. By implementing Applicure's dotDefender web application solution, organizations such as TD Ameritrade can have the added protection they need to help prevent security breaches.

## Application Protection Solution

In addition to network firewalls, data centers, hosting companies, and organizations with one or multiple services can take advantage of two advanced software products that protect systems at the application level. Applicure Technologies introduces dotDefender and dotDefender Monitor exclusively for the web hosting industry. dotDefender is the first web application firewall (WAF) to offer a viable application security solution for hosting providers. In addition to advanced security protection, companies can generate additional revenues with built-in features regardless of their business model.

With dotDefender, organizations can protect the following platforms:

- Web Client - Active content execution, cross-site scripting errors. dotDefender blocks cross-site scripting attacks on the server level, thus protecting the website's users.
- Web Server - Web server software vulnerabilities. dotDefender stops any request that attempts to abuse web server vulnerabilities.
- Web Application - Attacks against authentication, authorization, site structure, input validation, and application logic. A sophisticated set of rules intercepts application-level attacks.

Hosting customers are aware of the many threats on the Internet, but often do not understand what it takes to protect their websites beyond a network firewall. Instead, customers rely on their hosting provider for their websites' protection. However, many hosting providers do not protect websites at the application level leaving websites vulnerable to security breaches.

According to the annual Computer Security Institute (CSI) Survey 2007, 97% of companies have a network firewall installed and 98% utilize anti-virus software. The survey states that based on 194 Enterprise responses, computer security attacks yielded losses of \$66,930,950 in 2007.<sup>4</sup>

## **Protect Your Hosting Customers**

Hosting customers' websites and server applications can be protected from vulnerabilities by using Applicure's dotDefender software.

- Customized Solution for Dedicated and Shared Server Hosting
- dotDefender is easily customizable through a user-friendly GUI interface.
- Multi-Platform - A simple method for application security starts at the web server level by utilizing advanced server plug-in technology. dotDefender technology provides server plug-in technology for Apache, Microsoft Internet Information Services (IIS), and Microsoft Internet Security and Acceleration (ISA) web servers.

Regardless of hosting environment, understanding why application security should be part of a security plan is crucial to the success of an organization.

## **Understanding Application Security**

Application level attacks are best detected by analyzing the contents of incoming traffic. An application security solution should include the following:

- Encryption - Ability to open and read all requests, including SSL encrypted requests.
- Content - Ability to read the entire request, including headers and content.
- Application - Ability to view the request in the exact form the application will execute it.
- Emerging Threats - Ability to counter emerging threats from hackers.

A web application security solution is needed to protect your organization's external websites, internal applications, and extranet applications. Applicure Technologies' dotDefender software plays a vital role in securing applications for any organization.

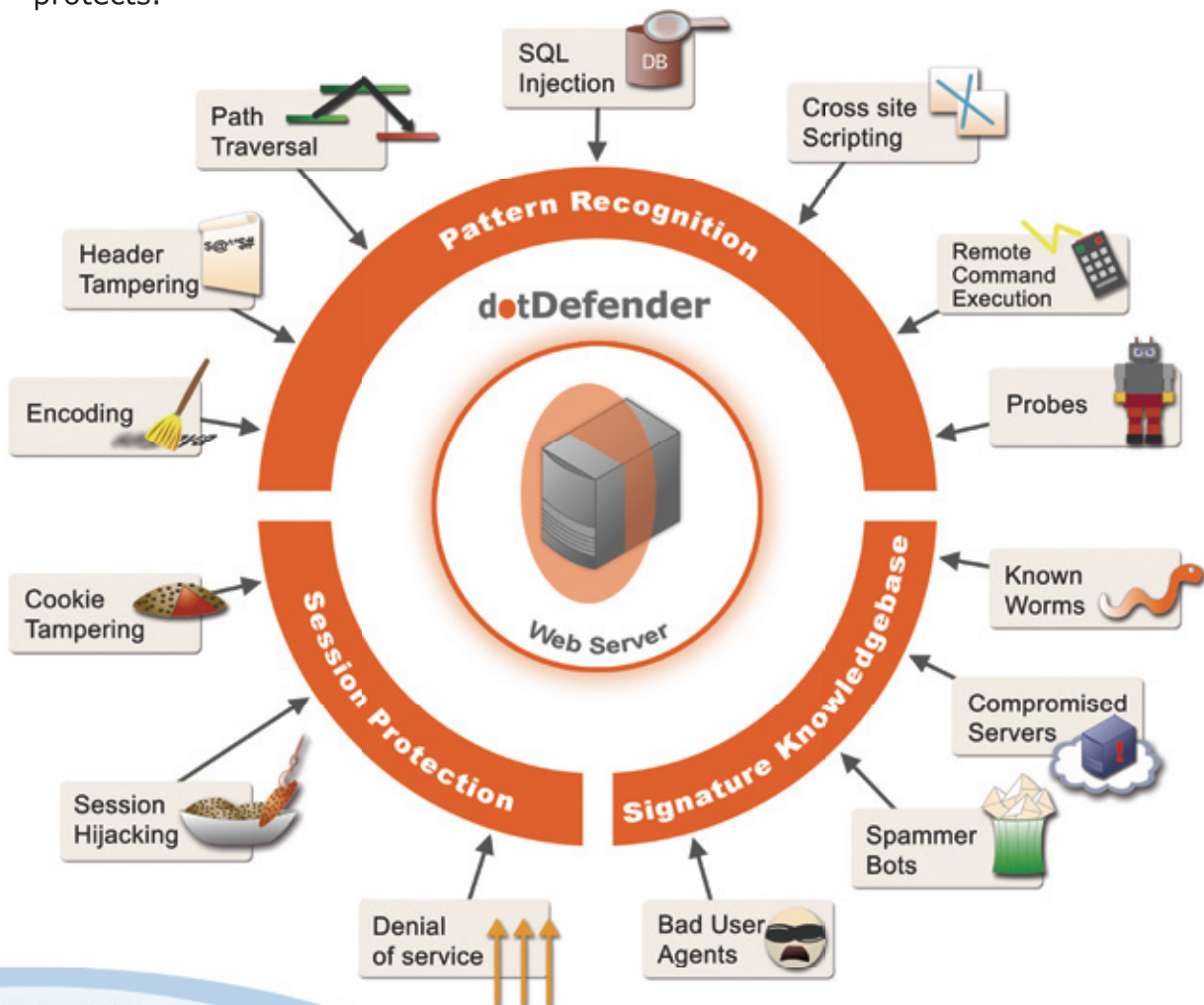
---

<sup>4</sup> Computer Security Institute (CSI): <http://www.gocsi.com/>

Applicure's dotDefender software utilizes three security engines to achieve optimal protection.

- Pattern Recognition – The Pattern Recognition security engine automatically stops attempts from website hackers. The Pattern Recognition security engine includes SQL Injection and Cross Site Scripting; both named the top two security vulnerabilities by OWASP.
- Session Protection – The Session Protection security engine focuses on the user session level. Session Protection prevents impersonation and the sending of large volumes of automatic requests that could potentially crash a server.
- Signature Knowledgebase – The Signature Knowledgebase security engine checks for requests from known malicious sources such as hackers and spammers. The Signature Knowledgebase security engine identifies bad user agents including hacking tools used to locate vulnerabilities in the application. Signature protection prevents hacking tools from gathering information about an application's vulnerable soft spots.

The following illustration shows the vulnerabilities each security engine protects.



## Who is Applicure?

Applicure Technologies, Ltd. develops advanced solutions to protect websites and applications from hackers, security breaches, and unwanted intrusion. Established in 2004, the Israel based software company provides two distinct products for optimizing data integrity and server protection against the following:

- Data Theft
- Site Defacement
- Website content manipulation
- Access control violation
- Denial of Service
- Impersonation

## Applicure's Products

Applicure's security products include dotDefender and dotDefender Monitor. These software products are designed exclusively for application-level security and monitoring.

## dotDefender

dotDefender provides dedicated application security that complements the network protection (firewall, IPS/ IDS). dotDefender is deployed as a server plug-in for Apache, Microsoft IIS, or Microsoft ISA servers. This innovative website security software provides strong protection against SQL Injection, Cross-site scripting, Path Traversal, and many other application attacks.

## With dotDefender you can...

- Protect websites against application attacks.
- Protect intranet applications against application attacks.
- Secure a variety of platforms using the same product.
- Enjoy best practices security right out of the box.
- Customize security settings for each website or web application.
- Receive automatic security updates against new threats.
- Monitor traffic and view reports about attackers and attack attempts.
- Easily integrate application security with monitoring and management systems.

## **dotDefender** MONITOR

dotDefender Monitor is a software tool installed on a web server to identify attacks. It comes packed with best practices security rules that work for any web application. Users do not need advanced security skills to use the monitoring tool. For complex environments, advanced customization features are available.

The monitor provides very detailed attack information including time stamp, originating IP, type of attack, which website or web application was attacked, and the original request. Even better, it presents attack statistics over time in a colorful, easy to understand log viewer.

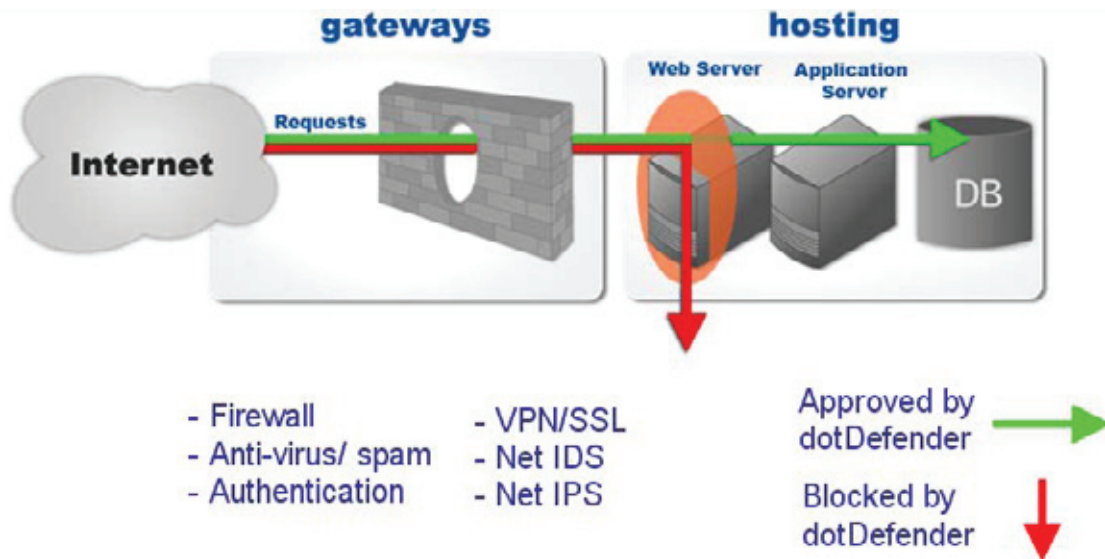
### **With dotDefender Monitor you can...**

- Immediately identify web application attacks.
- Identify sources of insider attacks.
- Receive real-time information about attempts to attack websites.
- Receive real-time information about attempts to attack internal web applications.
- View detailed statistics about attackers and attack attempts.
- Receive automatic updates for detecting new threats.
- Gain insight into your web application security posture.

### **dotDefender's Role in Application Security**

dotDefender web server plug-in analyzes traffic exactly as the application will execute it once it has been assembled and decrypted by the web server. By doing so, dotDefender software examines the complete contents of the request.

Legitimate and malicious requests are sent from the Internet. Traffic passes through the firewall, Secure Socket Layer (SSL), and Intrusion Prevention System (IPS), which leaves applications vulnerable to attacks. Once the application level attacks reach dotDefender on the server, malicious requests are identified and stopped. dotDefender complements the network firewall and stops the attacks at the server level while maintaining server performance and capacity.



dotDefender's advanced security rules define the patterns that indicate hacking. These rules are based on up-to-date hacking techniques. Applicure's dotDefender provides a low false-positive rate and powerful security with low maintenance for optimal security.

## **Applicure and Your Hosting Company**

### **Generate Additional Revenue for Your Hosting Company**

With products and support from Applicure Technologies, your hosting company can generate additional revenue through multiple channels. Your customers will benefit by the application and website security services you offer in addition to your regular hosting products and services.

Generate revenue by providing the following dotDefender benefits:

- Allows you to provide better security for your customers.
- An opportunity to offer another premium security service to your clients.
- An additional connection to your customers.
- Protects your reputation and exposure in case of attack.

### **Application Protection Partner**

Hosting companies can utilize Applicure products as value added services to customers such as application protection. When hosting companies use Applicure products, they receive the following:

- dotDefender and dotDefender Monitor Licenses
- Unlimited Updates & Upgrades
- Sales and Technical Training
- Marketing Materials
- 2<sup>nd</sup> Level Support
- An Assigned Account Manager

### **Comprehensive Solution**

- Multi-platform (Apache, Microsoft IIS, Microsoft ISA)
- Independent of customer applications.
- Can be used on both shared and dedicated servers.
- Scalable.
- Non-intrusive (No effect on traffic or network).
- Powerful Protection with Triple Security Engines
- Cost-Effective

## Simple Operation

- Easy Installation – Install in minutes as software plug-in. No need to modify the network architecture.
- Easy Implementation – dotDefender has predefined security rules and can secure the web environment immediately after installation providing your customers with immediate protection. Simple integration with your organization's current monitoring and management systems.
- Easy Maintenance – dotDefender produces few false positives, provides automatic live updates of security rules and signatures and introduces flexible customization tools for ongoing maintenance.
- Easy Upgrades
- Automatic Security Updates

## Why Applicure?

### Global Presence

Applicure Technologies, based in Israel, has assembled a team of security engineers to develop protection software beyond the firewall level. Applicure security engineers are located in three locations around the world – United States, United Kingdom, and Israel, providing support at multiple levels.

### Invested Company

Applicure Technologies has invested significant resources to build the most secure, advanced application protection software in the industry. Applicure Technologies is publicly traded on the Tel Aviv Stock Exchange.

### Recognition

Applicure Technologies was recognized as a "Top 100 Vendor" by *IT Week Magazine* in 2006.



## **Start Protecting Your Customers in Less Than 30 Minutes**

### **Free 30 Day dotDefender Evaluation**

Data centers, hosting companies, and organizations can try dotDefender by downloading a free 30 day evaluation license at [www.Applicure.com](http://www.Applicure.com).

### **Free Ongoing dotDefender Monitor License**

Download DotDefender Monitor at anytime for a free ongoing license at [www.Applicure.com](http://www.Applicure.com).

## **Contact Applicure Today**

To learn more about Applicure and dotDefender, visit <http://www.applicure.com> or call our Hosting Specialist at (770) 656-0777.

#### 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