



NT OBJECTIVES, INC.

DATA SHEET: NTO DEFEND

OVERVIEW

Today's organizations don't have the luxury of time when it comes to fixing web application vulnerabilities. In the time it takes for the security team to notify the development team that a code fix is needed, a site can be defaced, taken down, or have customer data stolen.

While investment in web application firewalls (WAF's) grew from 72 percent to 80 percent in the past year.¹ Only 5-50% of enterprises ever put their WAF's into 'active blocking mode'.² This is because it is difficult to create custom rules that will train the WAFs to actively block. Without proper training, they can only block certain attacks and can sometimes block good traffic. Some solutions are generating custom rules, but one-size fits all rules, need to be weak so that good traffic is not blocked.

Malicious hackers are targeting vulnerable web applications and the applications are vulnerable, but fixing defects in the code takes time and all too often, the source code or the skilled developers simply aren't available.

With NTODefend, enterprise security teams now have the ability to easily customize and train their ISPs/WAFs to be optimally effective, while eliminating the difficulties, costs and risks associated with traditional manual methods in creating custom rules to discover web application vulnerabilities. Additionally, NTODefend allows security teams to test the site to make sure that good traffic is not being blocked.

LEVERAGE IPS INVESTMENT

Only NTODefend effectively enables an IPS solution to behave like a WAF which supports PCI Compliance and leverages existing investment/limits number of solutions in play which reduces complexities and costs.

BENEFITS

Quick & Automated

NTODefend enables security professionals to patch vulnerabilities immediately - in a matter of minutes instead of the days or weeks it can take to build a custom rule for a WAF or IPF or the time it takes to deliver a source code patch. This gives developers time to identify the root cause of the problem and fix it in the code.

Easy

Users simply take the results of their NTOSpider scan, import them into NTODefend and generate custom rules that protect the web application from attacks on these vulnerabilities.

Accurate

Custom rules can leverage NTOSpider's knowledge of the application to create strong, safe rules. NTODefend takes the NTOSpider results and generates strong customized rules that target the application's specific vulnerabilities which increases the WAF's accuracy and ability to protect WAF/IPS. These filters are able to pinpoint vulnerabilities without blocking desirable traffic.

Confirmable

As a safeguard, NTODefend's performs a good/bad data QuickScan to test only the areas that are vulnerable and test for false positives.

Flexible

NTODefend allows users to optimally configure a WAF or to leverage their investment in their IPS device to block web application vulnerabilities.

PCI Compliance

PCI Compliance 6.6 requires a WAF, dynamic analysis tools, source code reviews or static analysis tools.

Integrations

NTODefend includes more integrations with WAF and IPS than any other solution available.



NT OBJECTIVES, INC.

DATA SHEET: NTO DEFEND

HOW IT WORKS

Automated Custom Rule Generation for WAF/IPS

Users of NTOSpider can leverage the results of application scans to quickly and easily generate custom rules to patch vulnerabilities on their WAF/IPS.

Vulnerability Report Selection

After a simple import from NTOSpider, the user is able to review the vulnerability report and quickly select which vulnerabilities to patch and automatically generate the highly targeted filters for their WAF/IPS solution

Integration with WAF/IPS Appliances

NTO integrates with market leading WAFs including, Sourcefire SNORT, Citrix F5, DenyAll, Imperva, ModSecurity, Nitro SNORT. NTO automatically generates rules for each WAF/IPS that are highly targeted to the specific vulnerabilities which reduces the risk of false-positives.

Re-scan Ability to Confirm Effectiveness

The NTO solution enables security teams to conduct a quick re-scan applications to confirm the trained WAF/IPS effectiveness. Now, teams can quickly confirm that target vulnerabilities are patched and that good traffic can continue to flow through as expected eliminating the risk of false positives & false negatives and dramatically reducing or eliminating QA time.

About NTO

NT OBJECTIVES, Inc brings together an innovative collection of experts in information security to provide a comprehensive suite of technologies and services to solve today's toughest application security challenges. NTO solutions are well-known as the most comprehensive and accurate Web Application security solutions available. For more information visit www.ntobjectives.com.

1. Are CIO's too Cocky About Security, CIO, George Hulme, September 28, 2011

2. Whither the WAF? The 451 Group, Wendy Nather,, September 9, 2011

"WAFs are a highly recommended element of a security defense strategy, but it is also clear that even the best WAFs will miss attacks and thus are not adequate as the single element for protecting web applications. What is interesting is that the use of training tools combined with a tool like NTODefend can dramatically increase their effectiveness and make them a far more useful part of an enterprise's application security strategy"

Larry Suto, Application Security Consultant
'Analyzing the Effectiveness of Web Application Firewalls'

SPECIFICATIONS

Windows with .NET 2.0 or greater

Available for the following WAF and IPS solutions:

WAF

- Imperva
- ModSecurity
- Denyall

Coming soon

- Citrix NetScaler
- F5 ASM
- Barracuda

IPS

- Sourcefire
- NitroSecurity