The Smartest Way to Secure Websites and Web Applications Against Hackers, Fraud and Theft.

The innovative Mykonos Web Security is the first deception-based Web Intrusion Prevention System that detects, tracks, profiles and prevents hackers in real-time.

The First Web Intrusion Deception System

Web Application Firewalls are the only layer seven solution available to secure your Web properties from attackers. But traditional signature-based Web application firewalls are flawed because they rely on a library of signatures to detect attacks and are always susceptible to unknown, or zero day, Web attacks.

Mykonos Software offers a new technology and uses deception to address this problem. Mykonos Web Security is the first Web Intrusion Deception System that prevents Web attackers in real-time.

Unlike legacy signature-based approaches, the Mykonos Web Security uses deceptive techniques and inserts detection points, or tar traps, into the code of outbound Web application traffic to proactively identify attackers before they do damage – with no false positives.

Mykonos vs WAF

Features	Mykonos	Signature-Based WAF
Meets PCI Compliance 6.6	Yes	Yes
Detection Technology	Code-level tar traps and Signatures	Signatures only
Tracking Technique	Client-level	IP address
Deceptive Responses	Yes	No

No False Positives

Mykonos Software's Web Intrusion Deception System does not generate false positives because it utilizes deceptive tar traps to detect attackers with absolute certainty. Mykonos Web Security inserts detection points into the code and creates a random and variable minefield all over the web application. These detection points allow you to detect attackers during the reconnaissance phase of the attack, before they have successfully established an attack vector. Attackers are detected when they manipulate the tar traps inserted into the code. And because attackers are manipulating code that has nothing to do with your Website or Web application, you can be absolutely certain that it is a malicious action– with no chance of a false positive.

IT security professionals know that false positives diminish the effectiveness of any security program. By using this certainty-based approach, Mykonos Web Security solves this problem for Web attacks. Furthermore, this product works out-of-the-box and improves your web application security. There are no rules to write, no signatures to update, no learning modes to monitor and no log-files to review. Just attackers to prevent.

Block Attackers Not IPs

Mykonos Web Security captures the IP address as one data point for tracking the attacker, but realizes that making decisions on attackers identified only by an IP address is fundamentally flawed because many legitimate users could be accessing your site from the same IP address. For this reason, Mykonos Web Security tracks the attackers in, significantly, more granular ways.

For attackers who are using a browser to hack your website, Mykonos Web Security tracks them by injecting a persistent token into their client. The token persists even if the attacker clears cache and cookies and has the capacity to persist in all browsers including those with various privacy control features. As a result of this persistent token, Mykonos Web Security can prevent a single attacker from attacking your site while allowing all legitimate users normal access.

For attackers who are using software and scripts to hack your website, Mykonos Web Security tracks them using a fingerprinting technique to identify the machine delivering the script.

Prevent and Deceive

The importance of detection with no false positives and client level tracking are vital for launching a countermeasure to prevent an attacker. Only with certainty-based detection can you safely prevent an attacker and know that you are not blocking legitimate users. Mykonos Software's Smart Profiling technology profiles the attacker to determine the best response to prevent the attack. Responses can be as simple as a warning or as deceptive as making the site simulate that it is broken for the attacker only. Every detected attacker gets a profile and every profile gets a name. The Smart Profile ultimately creates a threat level for each attacker in order to prevent attackers in real-time, at the client level, with no false positives.

Smart Profiling provides IT security professionals with more valuable knowledge about attackers and the threat they pose than they have ever seen before. With automated countermeasures, Mykonos Web Security works around the clock detecting and preventing attackers. It's not creating log-files for you to review to find an attacker. It just tells you how many attackers it detected and what countermeasure response was applied. It's a security device that works as part of your security team even when you sleep.

mykonos
a Juniper Networks company

Technical Specifications

Intelligence Technology

- Abuse detection
- Abuse tracking
- Abuse profiling
- Abuse response
- Real-time incident management

Abuse Detection Processors

A library of HTTP processors that implement specific abuse detection points in application code. Detection points identify abusive users who are trying to establish attack vectors such as cross-site request forgery. Some examples of processors include:

Authentication Abuse Detection – Detects abuses against application authentication, including:

- Requests for directory configurations, passwords, and protected resources
- Login attempts with invalid credentials
- Attempts to crack authentication

Cookie Abuse Detection – Detects attempts to manipulate the application by changing cookie values

Error Code Detection – Detects suspicious application errors that indicate abuse, including illegal and unexpected response codes.

Suspicious File Request Detection – Detects when an attacker is attempting to request files with known suspicious extensions, prefixes, and tokens.

Header Enforcement – Enables the policing of HTTP headers from the application to ensure critical infrastructure information is not exposed. Response and request headers can be stripped, mixed, or filtered.

Input Parameter Manipulation Detection – Detects attempts to abuse form inputs and establish vectors for injection and cross-site scripting attacks.

Link Traversal Detection – Detects attempts to spider the application for links to hidden and confidential resources.

[New] Directory Traversal Protection – Prevents attackers finding hidden directories.

Illegal Request Method Detection – Detects attempts to abuse non-standard HTTP methods such as TRACE.

Query Parameter Manipulation Detection – Detects attempts to manipulate application behavior through query parameter abuse.

Malicious Spider Detection – Detects attempts to spider and index protected directories and resources.

Cross Site Request Forgery – Detects and prevents cross site request forgery attacks.

Custom Authentication – Allows companies to protect a page or portion of a site if a vulnerability is found.

[New] Third-Party Vulnerability Protection – Detects known attacks.

[New] IP List Export – For Layer 3 firewall integration.

Abuse Recording

Full HTTP Capture – Captures and displays all HTTP traffic for security incidents.

Abusive Behavior Analysis

Abuse Profiles – Maintains a profile of known application abusers and all of their malicious activity against the application.

Tracking and Re-identification – Enables application administrators to re-identify abusive users and apply persistent responses, over time and across sessions.

Abuse Response

Abuse Responses – Enables administrators to respond to application abuse with session-specific warnings, blocks, and additional checks. One-click automation of responses during configuration.

The responses include:

- Warn user: send a custom message
- Block connection and return arbitrary HTTP error
- CAPTCHA
- Connection throttling
- Logout and forced re-authentication
- Simulated broken application (Strip inputs)

Policy Expressions – Simple expression syntax for writing automated, application-wide responses.

Deployment

- Reverse Proxy with Load Balancing
- [New] Available as software ISO, VMWare or AMI image
- [New] Support for alternate ports (other than 80 and 443)

Updates

Automatically downloaded and available within the management console.

Platform Security

Hardened kernel, locked-down ports, encrypted back-ups.

Management

[New] Simplified configuration with set-up wizards.

Web-based Configuration – Browser-based interface for all deployment options.

Monitoring Console – Web-based monitoring and analysis interface.

- Drill into application sessions, security incidents, and abuse profiles
- Manage and monitor manual and automated responses
- [New] Deep search and filtering capabilities
- [New] Real time and historical system monitoring
- Multiple administrators
- [New] Multiple applications/domains
- [New] Remote syslog

SSL Inspection

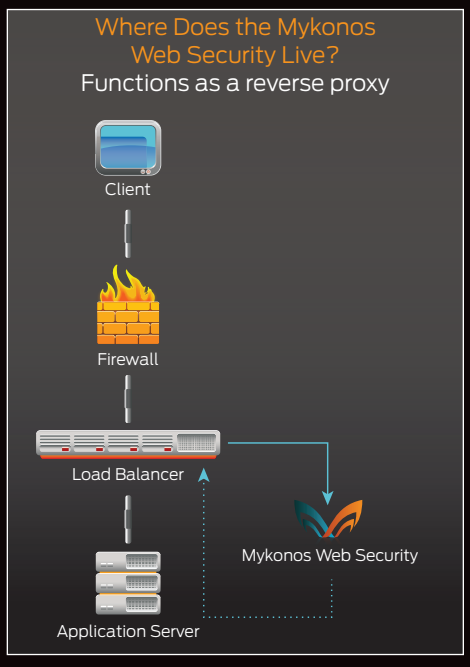
Passive decryption or termination.

Alerts, Reporting, Logging

- Email Alerts – Sends alert emails when specific incidents or incident patterns occur
- Command line interface for custom reporting
- Reporting Management System with user interface
- SNMP system logging
- Auditing – Tracks changes to the system made by the administrators in the configuration interface, security monitor, TUI and report generation
- [New] Security incidents via syslog

Performance

- [New] Higher throughput using master/slave clustering
- Low latency
- [New] Link aggregation



About Mykonos Software

Mykonos, a Juniper Networks company, is the smartest way to protect Websites and Web applications against hackers, fraud and theft. Its Web Intrusion Deception system detects, tracks, profiles and prevents attackers in real-time—with no false positives.

Headquarters
370 Brannan Street
San Francisco
CA 94107
USA

Rochester, NY Office
4 Commercial Street
Suite 101
Rochester, NY 14614
USA

Website: www.mykonossoftware.com
Phone: 650.329.9000
Toll free: 877.88WINGS
Email: sales@mykonossoftware.com

mykonos
a Juniper Networks company