



Mykonos Software Eliminates XSRF Attacks in Next-Generation WAF

Enhanced Technology Prevents "One-Click Attacks" to Overcome 20-Year Security Problem

BURLINGAME, Calif.– February 9, 2011 – [Mykonos Software](#), the creator of the first next-generation Web application firewall that secures Websites and Web applications against hackers, fraud and theft, today announced major updates to its Mykonos Security Appliance. The product, which will be unveiled at [RSA](#) booth #2151, now includes a new security processor that can eliminate Cross Site Request Forgery (XSRF) attacks, one of the [Open Web Application Security Project \(OWASP\) Top 10 attacks](#).

“The Department of Homeland Security has rated XSRF as more of a severe threat than most buffer overflows - because there is no limit to its potential impact. Mykonos Software is proud to have created an innovative solution to solve this problem that dates back to the early 1990s,” said David Koretz, president and CEO of Mykonos. “We continue to focus on solving the challenging real-world security problems that put our customers at risk. This is another major milestone for Mykonos.”

Released today, the enhanced Mykonos Security Appliance also features enhanced hacker tagging, new anti-automation threat protection, new reporting and management capabilities, and more flexible deployment options. The easy-to-use solution detects, tags, tracks and stops hackers in real-time has been upgraded to include several new security capabilities and anti-hacking techniques along with significant improvements in speed, latency, redundancy and reporting.

Key highlights of the new release include:

- **XSRF Protection**—the introduction of a new security processor intended to eliminate XSRF or “one-click attacks” as an attack vector.
- **Enhanced Tagging and Re-Identification**—a major update to the proprietary methods of tagging and re-identification of the hacker to improve persistence. Mykonos Security Appliance uniquely tags the hacker with a “security token” which enables re-identification of the hacker and allows companies to safely prevent an attack.
- **Breaks Automated Attacks**—an enhanced counter-measure that detects bots or other machines running automated scripts. Mykonos’ CAPTCHA processor prevents bots running automated attacks against sites by breaking the script with a CAPTCHA challenge response.
- **Comprehensive Reporting**—the new Reporting Management System now enables administrators to share valuable hacker data with internal stakeholders while the security monitor console and GUI has been enhanced to improve the customer experience.
- **Increased IT Flexibility**—key infrastructure improvements enable the product to work seamlessly within enterprise IT environments. These include SSL configuration to secure internal communication and third-party authentication for access to the product and the

ability for devices to connect to multiple V-LANS. For power users, a command line interface is also included.

The Mykonos Security Appliance is the innovator in a brand new product category of proactive defense solutions. Unlike traditional security solutions like Web application firewalls that simply log the threat to a log file to be discovered days later, the Mykonos Security Appliance traps the attacker in real-time, tags their computer, then profiles them to understand the threat level and then deploys real-time counter-measures to protect the Website.

To access product photos and screenshots of the Mykonos Security Appliance, please visit <http://www.mykonossoftware.com/news.php#media>.

Mykonos Software was named by Gartner as a 'Cool Vendor' in Application Security in 2010 and won the SC Magazine award for "Most Innovative Security Company" at the SCWorld Congress.

About Mykonos Software

Mykonos is the smartest way to secure Websites and Web applications against hackers, fraud and theft. Its next generation Web application firewall detects, tags, tracks and stops hackers in real-time. Unlike legacy signature-based approaches, Mykonos is the first technology that inserts thousands of detection points to proactively identify attackers before they do damage – without any false positives. Mykonos goes beyond the IP address to track the individual attacker, profile their behavior and deploy counter measures. With the Mykonos Security Appliance, administrators are liberated from writing rules, analyzing massive log files or monitoring another console. Mykonos neutralizes threats as they occur, preventing the loss of data and saving companies millions of dollars from fraud or lost revenue.

More information is available at www.MykonosSoftware.com.

For sales information call toll-free 1-877-88-WINGS, or email sales@mykonossoftware.com.

###

Media Contact:

Edward Roberts
Director of Marketing
Mykonos Software
E-mail: eroberts@mykonossoftware.com
Tel: + 1 650.529.9000 x1218

Media Contact:

Jill Reed and Angela Lestar
Schwartz Communications
E-mail: mykonos@schwartzcomm.com
Tel: + 1 415.817.2500