

FOR IMMEDIATE RELEASE



Mykonos Software Releases New Version of Mykonos Security Appliance Aimed at Preventing Web Application Abuse

Stop IT Security Attacks Before the Damage is Done by Detecting Malicious Abuse of Web Application Code.

Burlingame, CA – July 13, 2010 – Mykonos Software, developers of Web application security technology, today announced a new release of their flagship product, the Mykonos Security Appliance, aimed at preventing Web application abuse.

Targeted at organizations with significant web properties such as e-commerce sites, SaaS providers, and consumer on-line services, the Mykonos Security Appliance prevents malicious automation abuse, data theft and fraudulent transactions from occurring through vulnerabilities in Web applications.

“Every day we hear about security incidents even though firewalls and network layer security are widespread,” said David Koretz, President and CEO of Mykonos Software. “The reason incidents are so prevalent is because the primary security threat for businesses now comes through a browser. Every company with a Web application has opened a door for many threats to enter.”

The Mykonos Security Appliance helps companies prevent their Web applications from being asked to perform tasks they were never intended to perform. The product has three key features. First, it helps organizations gain real-time detection of Web application introspection before the damage is done. Second, it allows companies to respond to introspections with policy-based countermeasures that are designed to discourage abuse. Third, it identifies attackers (not IP addresses, but the actual attacker) and builds a profile of their behavior so that their methods can be analyzed and future counter-measures can be tailored.

How Mykonos Security Appliance Works

The Mykonos Security Appliance works by inserting variable and random detection points into the code as it is delivered to the browser. If an attacker abuses these code-level traps and honey-pots they identify themselves, with no chance of a false positive. The Mykonos Security Appliance identifies the person, not an IP address, and gives the attacker a name, so that future intrusion attempts can be highlighted as repeat visits and thwarted appropriately.

Early detection of an attack is important because it saves IT security department’s significant time and money because the cheapest attack is the one that is never completed and requires no response.

“We are looking at security differently,” said Al Huizenga, Director of Product Management at Mykonos Software. “If an attacker can abuse a Web application in hundreds of different ways, we want them to have to worry about thousands of different defenses. Before, they only needed to find

one vulnerability to begin an attack. Now, if they make one mistake, and exploit the wrong vulnerability, they identify themselves and we can stop the attack before it begins.”

Links

- Appliance image and dashboard screenshots: <http://www.mykonossoftware.com/news.php>
- Mykonos application security blog: <https://blog.mykonossoftware.com/>

About Mykonos Software

Mykonos Software is solving the problem of Web application security, differently. The Mykonos Security Appliance sits in front of Web applications to detect and prevent costly abuse in real time. The Mykonos Framework allows developers to create Web applications with complete security coverage at the code-level. More information is available at www.MykonosSoftware.com. For sales information call toll free 1-877-88-WINGS, or email sales@mykonossoftware.com.

Talk to Us

Rich Mullikin
Rocket Science PR, for Mykonos
E-mail: rich@rocketscience.com
Tel: +1 415 464 8110 x216
Mobile: +1 925 354 7444

Al Huizenga
Director of Product Management
Mykonos Software
E-mail: ahuizenga@mykonossoftware.com
Tel: + 1 585.586.2000 x1110
Mobile: +1 585 339 8660