

[Breaking News](#)
[IT Security News](#)
[Network security](#)
[Mobile & wireless security](#)
[Firewalls](#)
[Authentication & access control](#)
[Security policies](#)
[Data security](#)
[Vulnerabilities & threats](#)
[Web & Internet security](#)
[Hacking & penetration](#)
[Malware and spyware](#)
[Virus and worms](#)
[Virus infection map](#)
[Scanning and removal](#)
[IT Security Directory](#)
[Security events](#)
[Job adverts](#)
[Editorial policy](#)
[Advertise](#)
[Newsletter registration](#)
[Free newsfeed for your site](#)
[Bookmark this page](#)

IT Security links

[Ads by Google](#)
[Network Security](#)
[Computer Security](#)
[It Security](#)

Copyright ©
IT Security Portal

Submit an article
Advertise
Terms & conditions
Bookmark IT Security Portal

CMS and Web design by
www.areza.com

Mykonos security appliance stops IT security attacks before the damage is done

13 August 2010

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.

Mykonos Software have 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.

The Mykonos Security Appliance helps companies prevent their Web applications from being asked to perform tasks they were never intended to perform. The product as 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.

"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 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.

"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."



Need An Alarm System?

[Continue](#)

[Print version](#) | [Email to a friend](#) | [View other articles](#)

Latest IT, computer and network security articles

◆ [Ixia expects networking industry's top trends in 2012 to come from data centre, wireless, security, IPv6 and Carrier Ethernet deployments](#)



Search directory
Register your company



IT, computer and network security books:

