



Learn more about how IBM Tivoli Endpoint Manager can help enterprises address their patch and endpoint security needs

[SC Magazine](#) > [Reviews](#) > Mykonos Software Mykonos Security Appliance

Mykonos Software Mykonos Security Appliance

Peter Stephenson 3/1/2011

[PRINT](#) | [EMAIL](#) | [REPRINT](#) | [PERMISSIONS](#) | [TEXT: A | A | A](#) | [Like](#) | [Confirm](#)

Product Information



Vendor: [Mykonos Software](#)
 Product: [Mykonos Security Appliance](#)
<http://www.mykonossoftware.com>
 Price: Starts at \$25,000

Product Rating

- Features
- Ease of Use
- Performance
- Documentation
- Support
- Value for Money
- Overall Rating
- For:
- Against:
- Verdict:

Related Group Test

[Security Innovators Throwdown](#)

Eight sales pitches went head to head in our Security Innovators Throwdown competition to find the most innovative security products and services from young companies.

1st place

If you were a cyber detective trying to catch attackers what would you do? First, you would need to detect the fact that an attack actually was happening. Then, you probably would want to identify the attacker and take some action to prevent them from returning without your knowledge. You certainly would want to understand the skill level of the attacker so you could implement appropriate countermeasures to prevent their return. If it was a script kiddie, you might want to take some affirmative action to scare them away. If it was a skilled intruder, you would surely want to take defensive measures as well. Or you might just deploy the Mykonos Security Appliance and let it do the job for you.

We spent about an hour on the phone with one of the company's founders and came away with the strong impression that the level of thinking and analysis in this start-up is absolutely amazing. As a digital investigator for many years, I know exactly how to go about tracing an attack, and know it is very difficult to do and not always successful. There are reasons for this, and Mykonos seems to have captured them all and provided solutions to them.

One of the most interesting aspects to this product is its methodology. It mimics very closely the steps an analyst would take. First, it addresses pre-attack activity. Pre-attack is important because the probes and scans done by an adversary may give important information about the adversary's location, skill level and identity. During this phase, the attacker is led into a code-level honeypot and is presented with appropriate responses of increasing complexity and difficulty. Mykonos calls this process "hoops and hurdles."

For example, if the adversary does a simple SQL injection attack and then gets to a password file, a fake password file is returned. Then the adversary will attempt to crack the passwords and, if successful, is allowed to log into the honeypot using the bogus credentials. Meanwhile, the tool is profiling the attacker and responding appropriately - "appropriately" meaning based on policies you set up.

SC Magazine Video

[Find more videos at SC Video](#)

Also, from the first indication that the attacker is attempting or is going to attempt a compromise, the appliance tags the attacker using multiple methods, including hidden, encrypted cookies, among other methods. That way, no matter where the attacker comes from, they are identifiable. These tags are persistent and redundant so that simply removing one does not get rid of the tag.

Another very interesting aspect is the recognition that what is good for Mykonos - profiling the attacker - is also good for the attacker - profiling Mykonos. Since the earliest days of anti-virus (AV) software, when virus writers reverse-engineered McAfee's .dat files to learn the bit patterns the software used to identify a particular virus, the idea of the attacker profiling the target's defenses and then developing countermeasures has been popular. Mykonos makes every individual appliance somewhat different and adds the capability for the user to add to that. The result is that no two Mykonos appliances look exactly alike to the attacker. That prevents attackers from creating a profile of the Mykonos honeypot and attempting to circumvent it.

Administration is very straightforward. The web-based admin console lets you drill down into events and get detailed information about them. The console even sports a nifty geolocation capability that helps pinpoint the source of an attack attempt.

Finally, the appliance does not require configuration of a rules engine. Setup is very simple and the product is up and running almost out of the box. However, if you want to create new custom processors, Mykonos, resellers or your own team can do that. It is the custom processors that provide detection and countermeasures. However, the appliance comes with a full library of processors for typical attack types. Overall, there is no question that the Mykonos Security Appliance is information security innovation at its finest. It is no wonder that this young start-up - beta launched in 2010 - is our Throwdown winner this year and we predict very big things for them in the future. Starting at \$25,000 for the base model, the appliance may be the smartest buy of the year for any organization with an online presence.

Ads by Google

[Download Open Source ETL](http://www.Talend.com/Open_Source_ETL)

Leading Open Source Extraction Tool Suite. Get Free Download Now!

www.Talend.com/Open_Source_ETL

SPONSORED LINKS

What makes an APT advanced?

[This Damballa paper, "How Advanced Malware Morphs to Remain Stealthy and Persistent"](#) examines how criminals defeat IT defenses with stealthy malware and how you can protect against data theft.

Secure your third party programs

The new Secunia CSI 5.0 has arrived. Scan your PCs and Macs for vulnerabilities. Patch your 3rd party application with Microsoft WSUS & SCCM. Get a Free trial now!

- Most Popular
- Most Emailed
- Most Recent

- [Malicious apps discovered in Android Market](#)
- [Anonymous claims new Monsanto-related hack](#)
- [Four charged with hacking Subway, other retailers](#)
- [Blue Coat acquired by equity firm for \\$1.3 billion](#)
- [Vandals hack checkout terminals at California supermarkets](#)
- [Lockheed Martin hit, but not breached, with Adobe zero-day](#)
- [Three "critical" patches to be in Microsoft security update](#)
- [Thirteen patches from Microsoft, including Duqu fix](#)
- [Cyber crime aftermath: Beyond the indictment](#)
- [Yahoo wins \\$610M spam judgment](#)

www.twitter.com/SCMagazine

SC Magazine



netsecu @SCMagazine: Industry group creates guidelines for issuing SSL certs <http://t.co/x6Xww9v3>
49 minutes ago · reply · retweet · favorite



afabmedia @alfranken Online privacy and security is critical to US growth. For a lot more on data security, follow [@SCMagazine](#). Happy to talk anytime
27 minutes ago · reply · retweet · favorite



Join the conversation