



## Palo Alto Networks eyes one-hour malware turnaround



By [James Hutchinson](#) on Nov 21, 2011 12:30 PM  
Filed under [Security](#)

### [Fires up cloud-charged detection.](#)

Firewall vendor Palo Alto Networks has begun using Amazon Web Services' (AWS) cloud platform to more quickly capture and diagnose malware distributed to its customers, in hopes of distributing signatures to combat an attack within an hour.

The Wildfire service, launched last week, combines Amazon's cloud platform with Palo Alto's internal server farm to scan email attachments and other files that pass through Palo Alto's gateway appliances.

Suspicious files are run in a sandboxed virtual machine on AWS, then cross-checked against 70 criteria for potential of malware, before the vendor tests and distributes a signature to combat the attack.

The service has been made available across most of Amazon's availability zones, allowing companies to choose where their data is sent to for verification.

Palo Alto founder and chief technology officer Nir Zuk said Wildfire and the company's existing malware automation technologies allowed it to produce signatures within 24 hours to prevent further vulnerabilities.

Wildfire provides additional malware samples to Palo Alto Networks, which already receives in excess of 100,000 samples from the more common feeds used by anti-virus and intrusion prevention system vendors.

Since launching in beta phase with "under ten customers", Zuk said the company had identified 700 instances of malware, more than half of which were previously unknown.

Though many of these were widespread attacks, the company planned to use the service to protect against malicious attacks targeted at a specific company or companies.

Australian customers of the vendor include the Australian Tennis Federation, managed security provider Networx Australia and a large financial institution.

### **Automating detection**

The move to a cloud-based service was part of Zuk's attempt to automate as much of the security analysis process as possible.

"It can take a week to create the IPS and anti-virus signatures... a single rack in a data centre can replace about thousands of security researchers," he said.

"How do you take a well-trained hacker who's been doing it for 20 years and replace them with software? It's been done before, just never been successfully as a complete system."

Human analysts would still be required to develop the signatures that fix the targeted vulnerabilities but Zuk said this process would decrease time required to three days, at most.

"I think this is where the world is going to, bringing it down from two months or more to one hour," he said.

Zuk conceded that malware detection was a catch-up game with hackers but said an hour-long turnaround improved security professionals' chances and ease of detecting high profile attacks.

He pointed to [Operation Aurora](#) - a widespread attack on thousands of US companies including Google, exposed six months after it was believed to have first begun - as an example of the slow-moving security process that had effectively crippled large companies during attacks of similar scales.

Recent attacks against RSA and Sony Corporation had also proved slow to detect, coming about as the result of social engineering and targeted attacks.

In order to reach the one-hour target for automatic malware detection, Zuk told *iTnews* that the company "just needs to build the compute".

It had opted against deploying virtual machine sandboxes within the firewalls themselves.

He allayed concerns future malware attempts would simply bypass use of virtual machines for detection.

"It's a cat and mouse chase," he said. "We have techniques to prevent them from being able to detect that they're running in a virtual environment and they have techniques to overcome our techniques."

The massive compute capability offered by Amazon Web Services has previously been used for [malware distribution](#) and hacks, reportedly including the high-profile [Sony breach in April](#).

*James Hutchinson travelled to Thailand as a guest of NetEvents.*