t 1 300 780 730
f 9417 5355
e info@advantagetechnology.com.au
w advantagetechnology.com.au

Suite 1, Level 2, 58-62 Rupert Street,
Collingwood VIC 3066

Advantage IT Solutions & Supplies Pty Ltd
trading as Advantage Technology Solutions
ABN: 68 647 558 443

Canalys: Advanced security meets Big Data

What is the opportunity in advanced threat analytics for vendors and channel partners?

- **Traditional signature based solutions are no longer sufficient to protect from new threats**
- **Partners will gain differentiation and potentially high margins from services and consulting practices**
- **Use of analytics tools in advanced security will become mainstream by the end of 2013**

Advanced threat analytics is fast becoming an important area of focus for many IT security vendors. The shift is being stimulated by many businesses demanding higher feature set that include intelligence for advanced threats; these threats are increasingly targeted and leverage a combination of simultaneous attack mechanisms. Some threats are also left undetected for long periods of time, until an attack is executed. Businesses have a greater need to invest in security analytical tools that provide granular information about suspicious events – events that would otherwise be ignored by security products using signature and coding techniques to detect threats.

There have been many successful publicized attacks in recent years. One of the most famous was Stuxnet, a sophisticated threat aimed at the Natanz uranium enrichment facility in Iran that temporarily crippled thousands of centrifuges. The consequences of advanced threats can be devastating and these threats not only target large enterprises and organizations but, increasingly, small to medium-size businesses as well. Combating advanced threats now requires a combination of threat behavioral intelligence and remediation capabilities coupled with Big Data tools (see Canalys report, "Defining Big Data", published 27 Sep 2012). Traditional anti-malware solutions are fast becoming redundant against the new wave of threats.

Vendors invest in advanced capabilities to remain competitive

Many vendors have already added advanced feature sets to their portfolios by innovating internally, partnering with other specialized vendors or by acquiring new technology:

- **McAfee** acquired Nitro Security and released its Big Data for security solution by combining security information and event management (SIEM) with its ePolicy Orchestrator. The solution offers

t 1 300 780 730
f 9417 5355
e info@advantagetechnology.com.au
w advantagetechnology.com.au

Suite 1, Level 2, 58-62 Rupert Street,
Collingwood VIC 3066

Advantage IT Solutions & Supplies Pty Ltd
trading as Advantage Technology Solutions
ABN: 68 647 558 443

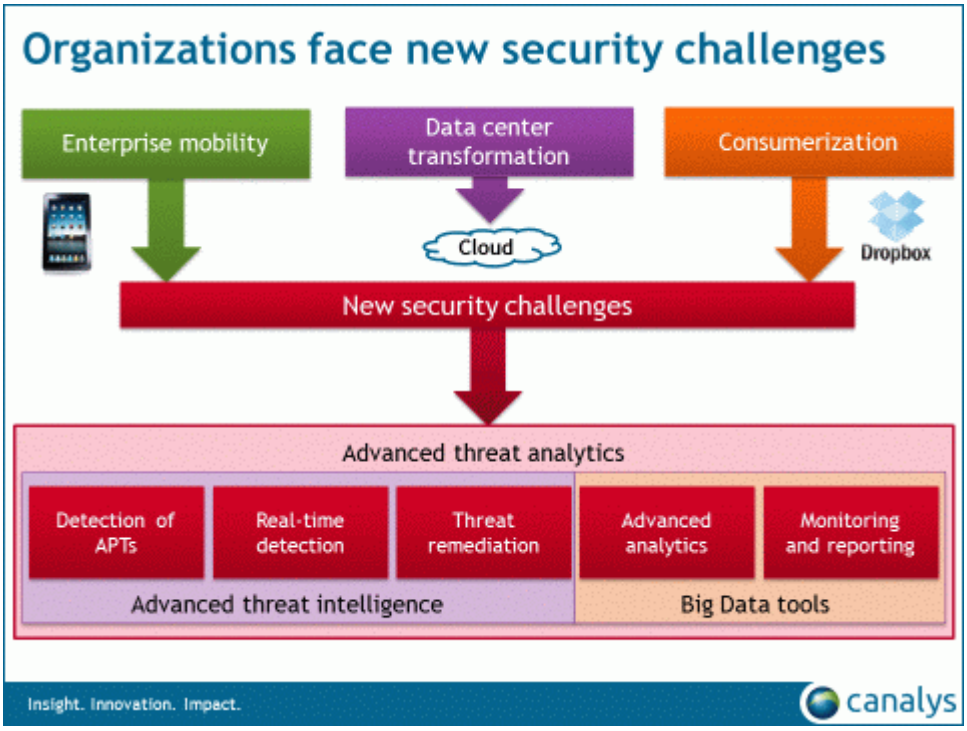
advanced threat intelligence, leveraging McAfee's Global Threat Intelligence (GTI), coupled with security task prioritization and remediation.

- **Trend Micro** launched its Custom Defense solution designed to detect and analyze advanced persistent threats (APTs) using Trend Micro's global threat intelligence Smart Protection Network. The solution then remediates attacks by responding with calculated actions depending on the type of threat.
- **Websense** announced CyberSecurity Intelligence (CSI), a security service which combines an online sandbox environment and access to Websense Security Labs for detecting threats. The solution is available as a standalone on-demand service or an online service that incorporates live support.
- **Panda Security** recently announced the beta launch of its Panda Cloud Office Protection Advanced 6.50. The solution is an update to its core offering including new features to detect zero-day vulnerabilities and other advanced malware. The technology leverages Panda's Collective Technology capabilities to analyze behavior and block advanced malware.
- **FireEye** is a specialized vendor focused on advanced threat detection. It offers a virtualized environment which correlates suspicious behavior patterns. It has created many partnerships over the last year. It partnered with Imperva on a solution that combines external threat technology with internal data protection capabilities. It also partnered with RSA to launch RSA NetWitness advanced threat network monitoring platform, combining analytics and advanced threat detection. FireEye has also invested in a service-provider program that will expand its market presence further.
- **TaaSERA** is a niche vendor specializing in advanced malware detection. Its TAAS NetAnalyzer offers real-time malware behavior detection and analysis tool that correlates behavioral data against life-cycle behavior information.
- **Cisco** acquired Cognitive Networks to gain advanced threat capabilities, which can be integrated into its existing cloud-based global threat intelligence to provide real-time threat data to its wider security product set (see Canalys Chain, "Q4 2012 security trends", last updated 1 February 2013).
- **IBM** recently launched IBM Security Intelligence with Big Data, which combines IBM's security capabilities with custom analytics and data forensics.

t 1 300 780 730
f 9417 5355
e info@advantagetechnology.com.au
w advantagetechnology.com.au

Suite 1, Level 2, 58-62 Rupert Street,
Collingwood VIC 3066

Advantage IT Solutions & Supplies Pty Ltd
trading as Advantage Technology Solutions
ABN: 68 647 558 443



Other vendors have followed a similar pattern or will likely make announcements in this area in 2013. Advanced threat analytics will become the new standard of security solutions and vendors will develop their capabilities in a natural evolution of the anti-malware market. IT managers will launch refresh projects in order to maintain control and visibility over their infrastructure and safeguard against unknown threats, which could bypass some of their legacy security systems. Many vendors are likely to launch new solutions in this area and ramp up marketing campaigns in hope to gain mindshare. Launching a comprehensive solution by developing capabilities internally will be difficult for many security-focused vendors. Establishing partnerships with other specialist vendors will be a good initiative until they are able to provide a higher level of expertise in data analytics. Canalys expects implementing intelligence-based security programs will become part of prevailing Big Data strategies. Businesses will begin to establish shared-data architecture comprised of event feeds from multiple products of different types across the infrastructure. Organizations will move away from point products and instead opt for multi-function solutions for simplicity in data collection. This will be coupled with analytical-based tools to create real-time monitoring and reporting systems, which IT staff will need to be trained to manage.

t 1 300 780 730
f 9417 5355
e info@advantagetechnology.com.au
w advantagetechnology.com.au

Suite 1, Level 2, 58-62 Rupert Street,
Collingwood VIC 3066

Advantage IT Solutions & Supplies Pty Ltd
trading as Advantage Technology Solutions
ABN: 68 647 558 443

Advanced threat analytics will present new channel opportunities. Partners who embrace this change by skilling up and offering new solutions will immediately gain a strong differentiator. Those that go further and develop innovative services around threat detection and analytics will stand to gain higher margins in addition to those associated with solution selling. Partners will also find consulting opportunities around security policies, as well as incident response. Security centric resellers will need to invest in hiring specialist staff or in certifying existing staff to gain expertise on data analytics. This will be crucial in order to convey information to customers effectively on the implementation processes, as many IT managers will be unfamiliar with these advanced solutions. They will also need to provide advice on best practice and deliver a high level of technical support. For some vendors that sell security as well as analytics solutions, such as RSA and IBM, it would be possible to engage with both sets of partners to sell these solutions.

The shift to advanced threat analytics, however, could leave some traditional security vendors and resellers behind. To stay competitive, they will have to start considering the long-term need for incorporating analytics into their portfolio. Vendors will need to create more education on the need for such solutions and build offerings, which are not just suited to large enterprises. Channel partners should draw out successful implementation case studies that businesses will find useful in decision-making processes. The year 2013 will signal a shift in traditional security solutions and Canalys expects Big Data tools will play a growing role in advanced threat predictive capabilities, which will lead to more acquisitions between security vendors and data analytics vendors.