Contacts:
Charles Lim
WatchGuard Technologies
+65 6536 7717
charles.lim@watchguard.com

Raymond Woo
EBA Communications for WatchGuard
+852 2122 9019
raymond.woo@ebacomms.com

WatchGuard Technologies Reinvents Advanced Persistent Threat Management with Launch of WatchGuard APT Blocker

New APT solution provides real-time, advanced-threat visibility for Unified Threat Management and Next-Gen Firewall appliances

Advanced, cloud-based, full-system-emulation sandbox protects in minutes, not hours

Hong Kong, 19 May 2014 – WatchGuard® Technologies, a leader in integrated security platforms, announced its new Advanced Persistent Threat (APT) solution, WatchGuard APT Blocker. Delivering real-time threat visibility and protection in minutes, not hours, APT Blocker identifies and submits suspicious files to a cloud-based, next-generation sandbox, using the industry's most sophisticated full-system-emulation environment for detecting APTs and zero day malware. The WatchGuard solution integrates with the company's visibility tool, WatchGuard Dimension™, providing an instant, single view of advanced threats, along with other top trends, applications and threats covered by WatchGuard's security technologies.

In Hong Kong and other parts of the world, APT Blocker comes pre-installed on all WatchGuard Unified Threat Management (UTM) and Next-Gen Firewall (NGFW) appliances with a free 30-day trial. WatchGuard has extended its proprietary proxy-based architecture to detect suspicious files and send them for full-system emulation and analysis in the cloud. By adding an additional layer to the deep-packet-inspection engine, WatchGuard's highly respected detection capabilities now extend from the universe of known threats (malware for which there is a known pattern) into the unknown.

"Nearly 88 percent of today's malware can morph to avoid detection by signature-based anti-virus solutions*," said Peter McNaull, director of technical marketing , for WatchGuard Technologies. "That means today's anti-virus solutions remain necessary for catching known threats but alone, they're no longer sufficient. APT Blocker's full-system emulation approach to sandboxing provides simple, rapid protection, which doesn't rely on a traditional, signature-based approach to detect and stop advanced malware; in a solution that scales to inspect millions of objects at any given time."

WatchGuard's UTM and NGFW security platforms were purpose-built to simplify the process of adding newly-emerging technologies such as APT management, meaning customers can deploy this sophisticated technology in a couple of clicks. Continuing the strategy of working with best-of-breed technology partners, WatchGuard has teamed with industry veteran and APT heavyweight, Lastline, for cloud-based, full-system-emulation

inspection capabilities. Lastline's founding team has been doing advanced malware research for more than 10 years and their commercial products have significant credibility in protecting businesses against today's unknown APT threats.

"WatchGuard is recognised as a leader in the network security space," said Brian Laing, vicepresident of products for Lastline. "We are thrilled to strike up this partnership to combat advanced cyber threats. With nearly a million red WatchGuard appliances installed worldwide and our unique, cloud-based sandboxing capabilities for detecting advanced malware, companies worldwide now instantly have access to the industry's most sophisticated technologies to stop evasive malware designed to bypass traditional security products."

Historically, APT targets were exclusively governments and large enterprises whose critical infrastructures were stymied by the likes of Stuxnet and Duqu. Today, advanced threats have evolved to target much smaller organisations and corporations to similarly devastating effect.

"Since today's APT targets, including companies in Hong Kong, are not anticipating these threats, they are not sufficiently protected. Often relying almost entirely on anti-virus and digital-signature solutions, these networks are almost completely vulnerable," said Aries Tsui, sales director, Hong Kong, Macau and Taiwan, WatchGuard Technologies.. (Click here to view an infographic on the evolution of APT.)

APT Blocker is now available and comes pre-installed with a free 30-day trial with the launch of version 11.9 of WatchGuard's Fireware security platform, which includes other best-of-breed services such as: AntiVirus, AntiSpam, Application Control and DLP. Fireware also comes standard with WatchGuard Dimension, the company's award-winning, real-time visibility solution.

Major highlights of version 11.9 include:

- Improved **application-traffic management**, allowing users to control and limit application bandwidth, preserving it for business-critical applications;
- Expanded **administrator-audit and change-tracking visibility** for improved HIPAA and PCI compliance, including tying firewall rule changes to individuals;
- **Customisable DLP signatures** that allow companies to build on the extensive pre-defined rule sets of WatchGuard's DLP solution;
- Enhanced **IPv6 support** including link aggregation, VLANS and dynamic routing; and
- New **custom network zone** that allows administrators to quickly segregate wireless guest networks and meet PCI-standard requirements for appliances with integrated wireless.

About WatchGuard Technologies, Inc.

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry standard hardware, Best-of-Breed

security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard products are backed by WatchGuard LiveSecurity® Service, an innovative support program. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuardTech on Facebook, or on the LinkedIn Company page.

About Lastline, Inc.
Lastline, Inc. provides the best-in-class malware protection platform to detect and stop advanced persistent threats, zero-day exploits, and evasive malware. The company was founded in 2011 by world-renowned security researchers and creators of Anubis and Wepawet – malware analysis tools used by thousands of security vendors, enterprises, and government agencies worldwide. The company is headquartered in Redwood City, California, with offices in North America, Europe and Asia Pacific. To learn more, visit www.lastline.com.

###

*Malwise—An Effective and Efficient Classification System for Packed and Polymorphic Malware, Deakin University, Victoria, June 2013