



December 12, 2016

FireEye is First Security Company to Detect All Threats Faced in ICSA Labs Advanced Threat Defense Testing

FireEye Network Security (NX) Achieves Certification, Demonstrating Protection Against New Internet Threats in Tests by Leading Independent Laboratory

MILPITAS, CA -- (Marketwired) -- 12/12/16 -- FireEye, Inc. (NASDAQ: FEYE), the intelligence-led security company, today announced that FireEye Network Security (NX) achieved Advanced Threat Defense (ATD) certification in the latest round of independent testing from ICSA Labs, a leading third-party testing and certification body and an independent division of Verizon.

FireEye NX Series detected 100 percent of the threats it encountered during the test cycle. According to ICSA Labs, this is the first time that a security vendor's solution detected all threats it faced. ICSA Labs testing reported only one false positive, spotlighting how the accuracy of FireEye detection reduces the time and effort wasted on non-malicious alerts.

ICSA Labs tests ATD products using real, prodigious sources of new and little-known malware and delivering them to vendor ATD solutions via the same means that they would be delivered to unsuspecting enterprises.

FireEye NX underwent 36 consecutive days of testing during the third quarter of 2016, demonstrating excellent threat detection effectiveness against over 360 new and little-known threats. ICSA Labs tested the detection capabilities of FireEye NX with a mix of 738 test runs using recently harvested threats that were not detected by traditional security products. ICSA Labs also launched innocuous applications and activities to test FireEye ATD capabilities in terms of false positives.

FireEye NX protects against known and unknown advanced attacks with the signature-less Multi-Vector Virtual Execution™ (MVX™) engine, conventional intrusion prevention system and intelligence-driven detection.

"NX has helped establish FireEye as a leader in enabling inline protection to secure against known and unknown threats, and this ICSA Labs certification spotlights the benefits we offer organizations today," said Jason Martin, FireEye executive vice president of global engineering and security products. "With high-fidelity detection and low false positives, FireEye stands apart in its ability to simplify customer workload and orchestrate and automate the security process. As advanced cyber attacks grow in scale and severity worldwide, superior technology is an organization's best defense, and this certification by a trusted independent laboratory is evidence of FireEye's commitment to the continued innovation of NX and our other security products."

"ICSA Labs reports that it has seen a spike in ransomware beginning with its testing in the second quarter of 2016, and this trend underscores the importance of FireEye's inline prevention capabilities," said Martin. "FireEye understands that organizations cannot rely solely on detection when dealing with the one-shot/one-kill nature of ransomware. Our superior inline prevention technology helps organizations address attackers that aren't always interested in dwell time but are instead looking to commoditize their penetration of a network as rapidly as possible to maximize their financial gain."

"Enterprises today must be able to not only identify and protect against known threats but also to protect against new and unknown malicious threats," said Jack Walsh, new initiatives and mobility programs manager at ICSA Labs. "This certification validates FireEye's ongoing commitment to protect enterprise customers by delivering security technology that meets stringent Internet security standards."

A foundational component of the next generation SOC is always-available, real-time protection that provides a resilient defense. FireEye research has shown that inline deployments reduce alert volume up to 76 percent. However, organizations have historically struggled to deploy inline security and balance it with business continuity, in part due to false positives that result in the blocking of legitimate traffic.

FireEye balances the efficacy and accuracy of detection with the need for real-time protection to help provide a more effective and efficient defense. Environments that rely on traditional security and out-of-band sandboxes may face a greater cyber security burden while being more exposed to fast-spreading cyber threats like ransomware.

With a focus on high availability and automatic failover NX updates, FireEye creates a transparent end-user experience to

prevent business disruption, allowing organizations to more confidently balance inline security with business continuity.

To learn more about updates to FireEye Network Security, which are available now for selected models, visit:
<https://www.fireeye.com/products/nx-network-security-products.html>.

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 825 of the Forbes Global 2000.

About ICSA Labs

ICSA Labs, an independent division of Verizon, offers third-party testing and certification of security and health IT products, as well as network-connected devices, to measure product compliance, reliability and performance for many of the world's top security vendors. ICSA Labs is an ISO/IEC 17025:2005 accredited and ISO 9001:2008 registered organization. Visit <http://www.icsalabs.com> and <http://www.icsalabs.com/blogs> for more information.

© 2016 FireEye, Inc. All rights reserved. FireEye, Multi-Vector Virtual Execution, MVX and Mandiant are registered trademarks or trademarks of FireEye, Inc. in the United States and other countries. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.

Source: FireEye

News Provided by Acquire Media