FURTINET

November 28, 2012

Fortinet(R) Earns 27th Virus Bulletin VB100 Award

FortiOS™ 5 Advanced Threat Detection Technology Delivers Excellent VB100 Comparative Results

SUNNYVALE, CA -- (Marketwire) -- 11/28/12 -- Fortinet® (NASDAQ: FTNT) -- a leader in high-performance network security -- today announced FortiOS 5 has been certified by Virus Bulletin and earned a Reactive and Proactive (RAP) measurement score of 96.6%. The Virus Bulletin RAP score measures a security solution's ability to detect malware collected from previous weeks (Reactive) and new malware (Proactive) that has appeared since a particular solution was submitted to Virus Bulletin. Proactive testing is extremely important to stop advanced threats that use the latest malware variants to avoid detection. Out of 30 participating vendors, Fortinet was the only company to score above 90% in proactive detection.

"Fortinet's scores have been climbing steadily of late and, for this specific test, detection scores were once again excellent across the board, taking a commanding position on the RAP chart; a VB100 certification award was easily earned," said test team director John Hawes at Virus Bulletin. "The design is simple and clear, and the interface proved reliable and responsive throughout testing."

The FortiOS 5 Advantage
FortiOS 5 powers both the FortiGate network security platform and the FortiClient endpoint protection solution, giving enterprises of all sizes innovative technologies to help protect and manage their networks in light of fundamental changes in both the nature of attacks targeting them as well as the way users are accessing the network. The new operating system includes more than 150 new security features that were designed to help protect against today's Advanced Persistent Threats (APTs) and targeted attacks. The enhancements roll up into five elements, which give organizations of any size the ability to easily deploy maximum protection:

- Advanced Malware Detection
- Exploit Discovery and Protection
- Cloud-Based Reputation Systems
- Local Client Reputation
- Multi-Vector Policy Engine

Advanced Malware Detection
The Advanced Malware Detection engine has three elements: The first consists of an advanced antivirus engine with one-to-many signatures to help reduce the size and increase the performance of the signature database. For example, a single signature can now detect multiple virus variants rather than having to create a separate signature for each discovered variant. The second element runs file scans and filters and determines if a file is suspicious in nature. The engine then passes suspect files through an inline sandbox where it applies behavior models against the sample file to help determine if it is a threat. The third part is cloud-based inspection, where the engine sends suspicious files for a more detailed analysis. Confirmed malware is placed into the database by the FortiGuard global threat research team, creating a feedback loop that improves proactive detection.

In the April 17, 2012 Gartner report titled: "A Buyer's Guide to Endpoint Protection Platforms," Peter Firstbrook, research vice president for Gartner, said, "Antivirus/anti-spyware databases are 90% to 99% effective at detecting well-known, widely circulating threats. However, they are only 20% to 50% effective at detecting new or low-volume threats. Security effectiveness is significantly enhanced by non-signature-based techniques. The simulation of unknown code before the code is executed to determine malicious intent without requiring end-user interaction with the unknown code is another deterministic technique."

Exploit Discovery and Protection
Although social engineering has become a favorite ploy of targeted threats, using exploits via vulnerabilities is still an important threat target. The FortiOS 5 Exploit Discovery and Protection engine is able to scan and identify vulnerabilities via a network or agent scan, providing a wide scope of coverage. Intrusion protection systems can then be deployed to protect vulnerable assets until the normal patching cycle remediates the vulnerability.

Cloud-Based Reputation Systems
Cloud-Based Reputation systems, where reputation is discovered in and delivered by the cloud, are an invaluable part of any network or endpoint security platform. Base-level reputation checks against a known bad list of domains and URLs. The next level, also referred to as application control, classifies applications to identify dangerous communication. More advanced reputation systems can check for known botnet controllers or relay servers.

Local Client Reputation
Fortinet's local client reputation is based on the dynamic behavior of a client. It maintains reputation by maintaining numerous parameters such as dangerous application usage, IPS attacks, malware detected and Websites (Malicious URLs and botnets) visited. It then constructs a reputation score for each client, allowing action to be taken against the top offenders.

Multi-Vector Policy Engine
Since the aforementioned security functions need to be deployed within endpoint, network and application platforms, the security engine that applies profiles of the security function and takes action on the results needs to be multi-vectored. Hence, although traditional policy can be applied based on source (IP address), there is also the ability to apply policy based on the user and device identity. This is an important attribute for distributed, virtual and cloud networks.

"Today's Advanced Persistent Threats use zero day exploits, rapidly-changing malware variants and other techniques to avoid detection and penetrate enterprise networks," said Michael Xie, founder, CTO and vice president of engineering for Fortinet. "One dimensional solutions that only employ antivirus or check sum scanning will not work against these types of attacks. Fortinet's software developers and FortiGuard Labs work tirelessly with product managers to continually deliver best-of-breed network and endpoint and security platforms, and their hard work is paying off with this latest VB100 award win."

About FortiGuard Labs
Founded in 2000, Fortinet's FortiGuard Labs consists of a world-class security team that monitors the threat landscape and helps ensure Fortinet customers are continuously informed and protected. Consisting of more than 200 dedicated research analysts, FortiGuard helps protect customers 24 hours a day, 7 days a week and 365 days a year. The team discovers new third party threats and then delivers rapid signature updates and detailed security knowledge designed to provide practically instant protection from new and emerging threats. In a typical week, the FortiGuard team adds or updates approximately 145,000 antivirus signatures, 25 intrusion prevention (IPS) signatures, 400,000 URLs ratings for Web filtering and 28,000,000 antispam signatures. Additionally, FortiGuard has made more than 130 zero day discoveries in the last three years.

Fortinet is able to discover threats quickly via Fortinet's extensive customer network and then push out signature updates to every customer in the world in minutes -- unlike competing security companies that have to rely on third party security companies to provide them with the latest malware signatures.

Follow Fortinet Online: Subscribe to threat landscape reports: http://blog.fortinet.com/feed/; Twitter at: www.twitter.com/fortinet; Facebook at: www.facebook.com/fortinet; YouTube at: http://www.youtube.com/user/SecureNetworks.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2011 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

Fortinet has not independently verified statements or certifications herein attributed to third parties, including Virus Bulletin and Gartner, and Fortinet does not independently endorse such statements. Nothing in the news release constitutes a warranty, guaranty, or contractually binding commitment. This news release may contain forward-looking statements that involve uncertainties and assumptions. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements and does not intend to update these forward-looking statements.

FTNT-O

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contact:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media