



April 17, 2018

Fortinet Receives Recommended Rating in NSS Labs Latest Advanced Endpoint Protection Test Report

Fortinet's FortiClient Offers a Powerful and Cost-Effective Solution for Safeguarding Endpoint Devices

SUNNYVALE, Calif., April 17, 2018 (GLOBE NEWSWIRE) --

John Maddison, senior vice president of products and solutions, Fortinet

"As organizations aggressively adopt a digital business model, endpoint devices and applications play an increasingly important role in business and networking strategies. Because these devices move freely between networked and cloud environments through a variety of access points, endpoint security is more critical than ever. Endpoint security solutions need to coordinate closely with the network and other security components to share telemetry, correlate intelligence and automate fast responses to increasingly sophisticated threats. Fortinet is pleased to have received another Recommended rating by NSS Labs for our advanced endpoint protection among many other Security Fabric components."

News Summary

Fortinet® (NASDAQ:FTNT), a global leader in broad, integrated and automated cybersecurity solutions, today announced its results from NSS Labs' annual Advanced Endpoint Protection (AEP) Group Test. In this year's test, which included a record 20 vendors, FortiClient demonstrated a 100% block rate on exploits, document and script-based malware, as well as web and offline threats, with zero false positives. FortiClient has received NSS Labs' coveted 'Recommended' rating since this test's inception in 2017, this year with an overall security effectiveness rating of 97.3%.

- | FortiClient delivers an impressive combination of Security Effectiveness and TCO per Agent as reflected in the NSS Labs Security Value Map (SVM) for AEP solutions. NSS Labs defines AEP agents as endpoint security technologies that combine the protective capabilities of anti-threat products with the detection, investigation, and prevention capabilities of endpoint security products.
- | NSS Labs' AEP report provides the industry's most comprehensive test results for effectiveness and TCO for security agents protecting today's increasingly intelligent and hyperconnected endpoint devices.
- | Several Fortinet Fabric-Ready technology alliance partners are also among the "Recommended" vendors in this report, including [Carbon Black](#) and [SentinelOne](#). These solutions are among those certified compatible with FortiClient Fabric Agent to provide integration and intelligence sharing with the Security Fabric. The broad Fortinet Fabric-Ready Partner Program ecosystem of complementary technologies enables customers to maximize their existing technology investments and get even more value from their security deployments.
- | This latest result adds to the long list of Fortinet solutions that have received a Recommended rating from NSS Labs in the last 12 months. Fortinet remains the most independently certified security vendor in the industry and is the only provider with NSS Recommended ratings for network, web application, and endpoint security, as well as for breach detection and breach prevention.

Securing Hyperconnected Endpoints with FortiClient

The transformation of today's networks continues to expand the potential attack surface while eroding traditional network perimeters. At the same time, a growing number of endpoint devices of mixed ownership have access to enterprise data and connect to critical organization resources. Adversaries using new tactics are targeting end user computers and leverage compromised endpoints to achieve their goals. According to the Verizon Data Breach Report, over half of the breaches included malware.

To combat advanced threats, enterprises need an integrated endpoint and network security strategy that provides consistent visibility, protection, and automated response across their distributed network ecosystems. According to NSS Labs research, 93.6% of US enterprises consider endpoint security products to be an essential part of their overall security strategy. While AEP solutions are primarily deployed by large and very large enterprises (81.5%), a growing number of small and medium-sized enterprises are also beginning to look at AEP solutions as a critical way to shore up their expanding network strategy.

As a robust advanced endpoint protection solution, FortiClient effectively detects and blocks threats such as malware, ransomware, exploits and malicious scripts. FortiClient also natively integrates with FortiSandbox and FortiGate to further identify and respond to unknown, advanced and targeted threats.

In addition, the FortiClient Fabric Agent is certified compatible with 3rd party Fabric-Ready partner solutions in order to

share real time endpoint visibility, compliance and control with the Security Fabric. Beyond exploit protection, machine learning and other advanced detection techniques, FortiClient goes a step further in helping organizations maintain a security baseline and reduce their attack surface with integrated vulnerability management.

Fortinet's FortiClient Next-Generation Endpoint Security solution is designed to work as a robust stand-alone endpoint security agent, as well as an essential component of the Fortinet Security Fabric. It integrates with FortiGate, FortiSandbox, and FortiAnalyzer, along with a number of Fabric-Ready partner solutions, for real time endpoint visibility, compliance and control. Its integration with FortiSandbox also enables it to detect unknown, advanced and targeted threats. FortiClient also provides effective vulnerability scanning and flexible patching options to help users and organizations maintain security hygiene and reduce their attack surface.

AEP Test Report Highlights for FortiClient

- | 100% block rate on exploits
- | 100% block rate on document and script-based malware
- | 100% block rate for web, 99.4% for email, and 100% for offline threats
- | 97.2% detection rate for evasions
- | 97.3% overall security effectiveness rating
- | Zero false positives

Fortinet Delivers a Security Fabric built around NSS Labs Recommended Solutions

Fortinet solutions consistently demonstrated superior security effectiveness, advanced features and superior performance when put to the test. Fortinet's commitment to testing and validation has resulted in nine Fortinet solutions earning NSS Recommended ratings across eight different group tests in the last year:

- | [Data Center Intrusion Prevention Systems](#): FortiGate 7060E
- | [Data Center Intrusion Prevention Systems](#): FortiGate 3000
- | [Data Center Security Gateway](#): FortiGate 7060E
- | [Data Center Security Gateway](#): FortiGate 3000
- | [Breach Prevention Systems](#): FortiSandbox Cloud, FortiGate 600D, FortiMail Virtual Appliance, and FortiClient
- | [Next-Generation Intrusion Prevention System](#): FortiGate 600D
- | [Breach Detection Systems](#): FortiSandbox 2000E and FortiClient
- | [Next-Generation Firewall](#): FortiGate 3200D
- | [Next-Generation Firewall](#): FortiGate 600D
- | [Web Application Firewall](#): FortiWeb 3000E
- | [Advanced Endpoint Protection](#): FortiClient

Supporting Quote

"NSS Labs is focused on empowering enterprises to make informed decisions based on independent real-world testing results. We applaud Fortinet's years of consistent commitment to third party testing. Fortinet's Recommended rating in our 2018 AEP Group Test makes them a great option for any business looking to strengthen their endpoint security strategy."
- *Vikram Phatak, chief executive officer of NSS Labs*

Additional Resources

- | Please visit Fortinet's [FortiClient home page](#) to learn more about the advanced endpoint security solution.
- | Download the NSS Advanced Endpoint Protection Test Report and Security Value Map [here](#).
- | Follow Fortinet on [Twitter](#), [LinkedIn](#), and [Facebook](#).

About Fortinet

Fortinet (NASDAQ:FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 340,000 customers trust Fortinet to protect their businesses. Learn more at <http://www.fortinet.com>, the [Fortinet Blog](#), or [FortiGuard Labs](#).

FTNT-O

Copyright © 2018 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and common law trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiCare, FortiManager, FortiAnalyzer, FortiOS, FortiASIC,

FortiMail, FortiClient, FortiSIEM, FortiSandbox, FortiWiFi, FortiAP, FortiSwitch, FortiWeb, FortiADC, FortiWAN, and FortiCloud. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, contract, binding specification or other binding commitment by Fortinet or any indication of intent related to a binding commitment, and performance and other specification information herein may be unique to certain environments. This news release may contain forward-looking statements that involve uncertainties and assumptions, such as statements regarding technology releases among others. Changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. 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 expressly disclaims any obligation to update these forward-looking statements.

Media Contact

Darlene Gannon
Fortinet, Inc.
408-235-7700
pr@fortinet.com

Investor Contact

Peter Salkowski
Fortinet, Inc.
408-331-4595
psalkowski@fortinet.com

Analyst Contact

Ron Davis
Fortinet, Inc.
415-806-9892
rdavis@fortinet.com

Source: Fortinet, Inc.

News Provided by Acquire Media