

July 24, 2017

Fortinet Launches Global Threat Intelligence Service

FortiGuard Threat Intelligence Service Arms CISOs with Actionable and Prioritized Threat Intelligence Enabling a Quick and Proactive Response to Targeted Attacks

SUNNYVALE, Calif., July 24, 2017 (GLOBE NEWSWIRE) --

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

"Given the maturity and breadth of our sensor network, Fortinet is uniquely positioned to provide accurate threat intelligence telemetry across a diverse and broad range of sources across the globe. FortiGuard Labs ingests over 50 billion events daily, and now with the FortiGuard Threat Intelligence Service we are able to deliver those same extensive threat insights to our customers and the security community at large."

A photo accompanying this announcement is available at <http://www.globenewswire.com/NewsRoom/AttachmentNg/d45f8f4b-b1c1-45de-9b08-343447d0cc79>

A screenshot of the FortiGuard Threat Intelligence Service interface, showing the title "FortiGuard Threat Intelligence Service" in blue text next to a small icon of a document with a red 'X'.

FortiGuard Threat Intelligence Service IPS Console

News Summary

Fortinet® (NASDAQ:FTNT), the global leader in high-performance cybersecurity solutions, today announced a new threat intelligence service that arms Cybersecurity leaders with cyber situational awareness highlighting the latest threat trends and cyber risks facing their organizations. Fortinet's FortiGuard Threat Intelligence Service (TIS) enables CISOs to stay ahead of the global threat landscape and proactively defend their enterprises against rapidly evolving threats.

- 1 FortiGuard TIS is a cloud-based threat intelligence platform that provides threat metrics and activity trends, enabling CISOs to instantly understand what is happening across the global threat landscape.
- 1 FortiGuard TIS leverages Fortinet's FortiGuard Labs leading threat intelligence research. FortiGuard Labs consists of more than 200 expert researchers analyzing data collected from more than three million sensors around the globe.

Global and Industry Threat Intelligence at a CISO's Fingertips

A recent [Forrester survey](#) of 342 security leaders found that the CISOs' largest cybersecurity challenge is adapting to "the rapidly evolving nature of cyber threats." The report recommends that CISOs gather good threat intelligence that provides insight into attacker methods and indicators of compromise, noting that 78% of CISOs that have adopted a threat intelligence platform haven't experienced a breach. It's clear that CISOs who properly leverage threat intelligence combined with a technology-driven security strategy are better prepared to successfully defend their organizations.

FortiGuard TIS is specifically designed to provide the threat intelligence needed for CISOs to stay on top of the latest threat trends so they can effectively communicate cybersecurity risks to the C-Suite and board while also enabling more efficient management of Security Operations to maximize resources and proactively defend against trending threats.

- 1 Global threat landscape activity is prioritized so that CISOs can instantly understand which type of cyber threat is on the rise. This easy to understand data can be communicated to the wider organization and also enables security leaders to more effectively task their security operations teams.
- 1 Kill Chain reporting provides additional details on the unique and specific threat trends currently impacting their industry and the globe. Security leaders can see the most active applications, intrusion prevention signatures, malware and botnets on an industry-by-industry basis and easily compare these trends within their industry, by company size, by geographic location and with the overall landscape.
- 1 CISOs can drill down further into specific threat details to identify its activity trends, prevalence and ranking. Integration with the FortiGuard Encyclopedia provides enhanced threat descriptions that includes details of the origin, behaviors and remediation steps.
- 1 Individual application vulnerabilities and malware can also feature additional notes created by FortiGuard Labs threat researchers that provide timely insights into campaign-specific or emerging threats. Expanded commentary is often featured in periodic [Fortinet blogs](#), quarterly FortiGuard [Threat Landscape Reports](#), and weekly FortiGuard [Threat](#)

Availability

Fortinet's FortiGuard Threat Intelligence Service is available as an open beta today. Please visit <https://tis.fortiguard.com/signup> to learn more.

Additional Resources

- | Please visit Fortinet's [Threat Intelligence](#) homepage for more details about the Fortinet's FortiGuard Labs threat research and services.
- | Follow Fortinet on [Twitter](#) and [LinkedIn](#), and [Facebook](#).
- | Join the conversation on the [Fortinet blog](#).
 - ° [The Need For Threat Intelligence \(blog\)](#)

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 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 310,000 customers trust Fortinet to protect their businesses. Learn more at <http://www.fortinet.com>, the [Fortinet Blog](#), or [FortiGuard Labs](#).

FTNT-O

Copyright © 2017 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCloud, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiAP, FortiDB, FortiVoice, FortiWeb and FortiCASB. 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, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions, such as statements regarding program, technology and functionality releases and release times. Changes of circumstances, product release delays or product priority or roadmap changes, 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:

Dan Mellinger

Fortinet, Inc.

415-572-0216

dmellinger@fortinet.com

Investor Contact:

Kelly Blough

Fortinet, Inc.

408-235-7700 x 81612

kblough@fortinet.com

Analyst Contact:

Ron Davis

Fortinet, Inc.

415-806-9892

rdavis@fortinet.com

=====

Source: Fortinet, Inc.

News Provided by Acquire Media