January 31, 2017

Fortinet Extends Security Fabric Protection into the Internet of Things

Fortinet Announces Security Fabric Capabilities to Arm Enterprises with Visibility and Control to Defend Against Rising Threats from IoT

SUNNYVALE, Calif., Jan. 31, 2017 (GLOBE NEWSWIRE) --

Phil Quade, chief information security officer at Fortinet
"Malicious cyber actors have been increasingly targeting the billions of IoT devices online today, essentially turning the Internet of Things into an Internet of Threats. It's critical that today's enterprises implement security solutions that can identify, understand, and protect their infrastructures from the massive attack surfaces created by IoT. The Fortinet Security Fabric arms enterprises with proven security capabilities today, while providing a foundation for the visibility and automation required to maintain an effective IoT cybersecurity posture in the future."

News Summary
Fortinet® (NASDAQ:FTNT), the global leader in high-performance cybersecurity solutions, today announced the extension of the Fortinet Security Fabric to defend enterprises against the exponentially increasing cyber threats posed by the Internet of Things (IoT). Fortinet's Security Fabric delivers the visibility, integration, control and infrastructure scale required to successfully defend the complex attack surfaces created by the ongoing proliferation of IoT devices.

A Security Fabric is Necessary to Defend Against IoT's Massive Volume and Scale
Recent IoT-based attacks have revealed the sheer volume and ease by which billions of devices can be weaponized and used to disrupt the digital economies of entire countries and millions of users. These issues are compounded by the lack of basic security features and management capabilities in many IoT devices.

This is a major challenge for enterprises today whose data needs to remain secure as it traverses many types of devices and environments, from tablets to cloud applications. Current point products and platform security solutions lack the visibility and wider network integration necessary to see, let alone secure, the IoT attack surface.

The Fortinet Security Fabric Expands to Meet Today's IoT Security Requirements
To successfully defend the massive scope of IoT and the cloud, organizations need to implement a Security Fabric that scales the entire infrastructure for comprehensive visibility, segmentation, and end-to-end protection. Enterprises need to consider three strategic network security capabilities to harden their infrastructure against IoT threats:

1. **Learn -** Complete network visibility is critical to securely authenticate and classify IoT devices, build risk profiles, and then assign IoT device groups based on identified trustworthiness. At the core of the Fortinet Security Fabric, FortiOS provides total IT awareness and visibility into every security element and enterprise networking component. This enables IT to identify and manage their IoT devices and traffic at critical points within the infrastructure.

2. **Segment -**Enterprises need to be able to segment IoT devices and communications into policy-driven groups and grant baseline privileges suitable for the specific IoT risk profile. Fortinet's Internal Segmentation Firewall enables enterprises to internally segment their networks and devices, allowing IT to apply layered security policies based on the specific device type and network access requirements.

3. **Protect -** Fortinet's Security Fabric provides the required capability to correlate IoT security incidents and threat intelligence to deliver a synchronized response to IoT threats. It also ensures that compromised IoT devices can be quarantined and remediated at multiple points within the network to contain threats and ensure that malicious traffic never reaches critical IT systems or enterprise data.

Fortinet's Security Fabric is trusted by some of the largest enterprises and government organizations in the world to secure their critical IoT devices, spanning industrial applications and public utilities.

Security Fabric Automation is the Key to A Secure Future for IoT
Fortinet has laid the foundation for its continued innovation with its Security Fabric vision to deliver Intent-Based Network Security. With Intent-Based Network Security, enterprises can automate the execution of their IoT strategy and operations by translating business needs into synchronized network security actions without human intervention. Fortinet is actively driving the development of IoT security innovation and already holds dozens of issued and pending IoT security patents.

Additional Resources

- Please visit www.fortinet.com for more details about Fortinet's IoT Security strategies and solutions.
- Follow Fortinet on Twitter and LinkedIn, and Facebook.
- Join the conversation on the Fortinet blog.
    - Defining and Securing IoT (Blog)
    - Extending the Security Fabric: FortiOS 5.6 and Intent-Based Network Security (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 290,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

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 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:

Sandra Wheatley

Fortinet, Inc.

408-391-9408

swheatley@fortinet.com

Analyst Contact:

Ron Davis

Fortinet, Inc.

415-806-9892

rdavis@fortinet.com

Source: Fortinet, Inc.