October 25, 2017

Fortinet Expands Security Fabric Visibility and Protection into the Industrial Internet of Things

Fortinet Demonstrates IoT Security Momentum and Industry-Leading Patent Innovation

SUNNYVALE, Calif., Oct. 25, 2017 (GLOBE NEWSWIRE) --

John Maddison, senior vice president of products & solutions at Fortinet
"IoT-based attacks have revealed the sheer volume and ease by which billions of devices can be weaponized and used to disrupt global digital economies, critical infrastructure and the data of millions of users. To successfully defend the massive scope of IoT, organizations need an architecture that scales the entire infrastructure for complete visibility, segmentation and end-to-end protection. The Fortinet Security Fabric arms enterprises with a comprehensive solution that spans the entire IoT attack surface, delivering the performance and threat intelligence required to learn, segment, and ultimately protect the varied attack surfaces created by IoT."

News Summary
Fortinet® (NASDAQ:FTNT), the global leader in high-performance cybersecurity solutions, today announced its new FortiGuard Industrial Security Service, extending the Fortinet Security Fabric visibility, control and protection into the Industrial Internet of Things (IIoT).

- FortiGuard Industrial Security Service (ISS) builds on the award-winning threat intelligence services of FortiGuard Labs by providing application control and defensive signatures specific to critical infrastructure and industrial sector organizations, including utility, oil and gas, transportation, and manufacturing.
- Customers around the globe are selecting the breadth of IoT solutions in Fortinet's Security Fabric to secure their complex networks and endpoint devices, from manufacturing, natural resources, and aviation to government organizations.
- Fortinet demonstrates its continued commitment to innovation in IoT with its expanded portfolio of patents on IoT security.

Securing the Industrial Internet of Things with FortiGuard Threat Intelligence
Enterprise and consumer demand has created an explosion in the number of IoT devices connecting to global networks. McKinsey estimates that 20 to 30 billion IoT devices could be connected globally by 2020, up from 10 billion to 15 billion devices in 2015. However, as devices proliferate, the security risks also increase.

Traditionally, commercial and industrial networks and their IoT devices have operated in isolation, but the mainstreaming of things like smart cities and connected homes have begun to merge these devices within local, national and global infrastructures. This is requiring organizations to rethink how they secure increasingly converged IT, OT and IoT networks and devices. Integrating distinct security tools into a unified Security Fabric enables organizations to collect and correlate threat intelligence in real time, identify abnormal behavior and automatically orchestrate a response anywhere across this complex IoT attack surface.
FortiGuard ISS protects the most widely-used Industrial Control System (ICS) and Supervisory Control And Data Acquisition (SCADA) devices and applications. The new service provides vulnerability protection, deep visibility and granular control over ICS and SCADA systems and is backed by real-time threat intelligence updates - enabling organizations to restrict access and minimize the attack surface of their critical IIoT infrastructures. FortiGuard ISS complements Fortinet's industrial-strength security appliances, which are designed to run in harsh environments.

Global Enterprises Securely Leveraging the Benefits of IoT with Fortinet
Organizations of all sizes and across industries are adopting the Fortinet Security Fabric to solve their IoT security challenges:

- **Gibsons Energy** - An an oil and gas company involved in the midstream operations between extraction and retail, Gibsons has a highly distributed IT infrastructure and needed a better way to secure its move to the cloud and manage the IoT devices deployed in the field. "We have several thousand devices in the field and previously we had to manually monitor these devices. Now we have a plan to connect them to the cloud and provide important operation analytics," said Richard Hannah, VP of information services at Gibson Energy. "Working with Fortinet, our operations teams can now monitor these devices in real-time, saving thousands of hours of maintenance and man time while ensuring the security of our infrastructure."

- **City of Mumbai** -The Government of Maharashtra selected Fortinet to provide wireless internet access for the Mumbai WiFi project to cover all major areas in the city with public WiFi hotspots for its citizens and also to be used for smart parking and smart transportation. "The Mumbai WiFi project plays a crucial role in empowering our citizens digitally. Our goal was to cover all major areas in the city with public WiFi in order to make important government services available online," said Vijay Kumar Gautam, Principal Secretary Information Technology, Government of Maharashtra. "Because of the hyper-connected nature of our public infrastructure today, an ambitious project like this requires technology that can scale and be flexible to enable more users, devices, and applications over time."

An Integrated Solution for IoT Security
Fortinet is uniquely positioned to address the IoT security challenge with its broad and integrated solutions that secure IoT at all points across the attack surface. Enterprises need three strategic network security capabilities of learn, segment and protect to harden their infrastructure against IoT threats. Fortinet's breadth of IoT security solutions include : FortiOS, FortiGate, FortiSIEM, Secure Access, FortiGuard Threat Intelligence, and Advanced Threat Protection. Additonally, Fortinet's robust Fabric Ready Partner ecosystem enables advanced integration and complete protection through technical partnerships with additional IoT and endpoint security vendors like ForeScout, Nozomi Networks and SentinelOne.

Industry-Leading IoT Security Innovation
Fortinet has a long history of delivering security innovation and holds the most robust portfolio of IoT security patents in the industry, outpacing the nearest security vendor portfolios by several times. Patents like these are foundational to Fortinet's continued leadership and ability to deliver cutting-edge IoT security solutions to its customers.

- System for Managing and/or Securing the Internet of Things
- IoT Intrusion Detection at the Physical Level
- Fingerprinting IPv6 Clients in Stateless Auto-Configuration of IoT
- Heuristics-based Techniques to Identify IoT Attacks in WiFi

Fortinet's continued momentum and innovation has earned it recent accolades such as being named in Fortune's inaugural Future 50 list of companies best positioned for breakout growth.

Additional Resources

- Please visit the FortiGuard Industrial Security Service homepage for more details.
  - You can find more information about Fortinet's IoT security solutions here.
  - You can find more information about Fortinet's ICS and SCADA security solutions here.
- Follow Fortinet on Twitter, LinkedIn, and Facebook.
- Join the conversation on the Fortinet 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 320,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

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:	**Investor Contact:**	**Analyst Contact:**
Dan Mellinger	Kelly Blough	Ron Davis
Fortinet, Inc.	Fortinet, Inc.	Fortinet, Inc.
415-572-0216	408-235-7700 x 81612	415-806-9892
dmellinger@fortinet.com	kblough@fortinet.com	rdavis@fortinet.com

Source: Fortinet, Inc.