FORTINET

December 12, 2017

Fortinet Protects Operational Technology Deployed in the Harshest Environments

Broad Security Fabric Architecture Provides Integrated Security Across Environmentally Controlled and Non-Environmentally Controlled Enterprise Facilities

SUNNYVALE, Calif., Dec. 12, 2017 (GLOBE NEWSWIRE) --

John Maddison, senior vice president of products and solutions at Fortinet
"Securing critical infrastructure against cyber attacks is an increasingly urgent priority as the adoption of smart cities and connected utility services drives the convergence of IT, OT and IoT networks. To successfully defend the scope of these converged networks, organizations need an architecture that scales the entire infrastructure for complete visibility, segmentation and integrated protection. Fortinet's latest OT solutions arm critical infrastructure organizations with a broad security solution that spans their traditional IT environments and also provides the advanced capabilities needed to defend critical OT infrastructure."

News Summary
Fortinet® (NASDAQ:FTNT), the global leader in broad, integrated and automated cybersecurity solutions, today announced the availability of its Operational Technology (OT) Security solution for critical infrastructure and industrial organizations. The new solution integrates ruggedized firewall, switching, and wireless access point appliances with FortiGuard industrial threat intelligence to provide integrated cybersecurity protections for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems deployed in the field and non-environmentally controlled facilities across an organization's OT infrastructure.

- The Fortinet Security Fabric enables critical infrastructure and industrial organizations to deliver advanced segmentation, access control, and malware protection needed to unify their security architecture and defend their OT networks regardless of the operating environment.
- Fortinet's ruggedized security products enable industrial organizations to protect their OT infrastructure and devices, even those deployed in harsh environments that would render other security devices inoperable.
- Fortinet's industrial-grade appliances leverage its recently announced FortiGuard Industrial Security Services, which delivers application control and defensive signatures specific to critical infrastructure and industrial sector organizations, including utility, oil and gas, transportation, and manufacturing.

The Convergence of OT and IT Demands Unified, Automated Security
Critical infrastructure is being increasingly targeted by cyber criminals, with a reported 51% of organizations experiencing a SCADA/ICS security breach within the past 12 months. The consequences of a successful attack can lead to the disruption, and even destruction of physical assets and essential services like water, electricity, and fuel.

As the utility, oil and gas, transportation, and manufacturing sectors increasingly adopt connected control systems and Industrial IoT devices, the attack surface is rapidly growing. The connected nature of these devices and systems poses serious challenges as they begin to utilize traditionally IT owned network infrastructure, wireless access points, and mobile networks. The specialized nature of OT infrastructure technologies means that most security and threat intelligence solutions don't have visibility into, let alone the ability to defend against attacks on critical infrastructures.

According to a 2014 Forrester report, "There are fundamental differences between traditional information technology (IT) and operational technology (OT)…S&R (security and risk) pros from IT and OT must respect and accept each other's differences and learn to work together."[1]

Fortinet's Operational Technology Security solution solves the unique security challenges specific to critical infrastructure and industrial organizations, while unifying the management and administration of both OT and traditional IT infrastructures through the Fortinet Security Fabric.

Security Fabric Protection Tailored for OT Infrastructure
Fortinet's rugged and outdoor products are industrially-hardened appliances that deliver enterprise-class connectivity and security for critical control systems facing malicious attacks, as well as extreme weather and other demanding physical environments.

- FortiGate Rugged Series are all-in-one firewalls that deliver specialized threat protection for securing critical industrial

and control networks against malicious attacks.
- FortiSwitch Rugged Series deliver all the performance and security of Fortinet's trusted FortiSwitch line, but with added reinforcement that makes them ideal for deployments in harsh outdoor environments. Management by the FortiGate simplifies operation and extends security policies down to the switch ports.
- FortiAP Outdoor Series delivers secure, identity-driven WiFi access points with management provided by the integrated wireless controller functionality within the FortiGate. Combined with FortiSwitch, this provides for a truly unified access layer with common security policies.
- Fortinet's rugged and outdoor series devices are offered in various form factors with features like superior mean time between failure, electromagnetic interference protection, vibration tolerance, ingress protection waterproofing, wide thermal operating ranges, fanless cooling and power over ethernet.

These devices are controlled by Fortinet's FortiOS security operating system and are backed by FortiGuard Industrial Security Service to protect the most widely-used ICS and SCADA devices and applications. FortiGuard Industrial Security Service delivers OT-specific, real-time threat intelligence for vulnerability protection, deep visibility and granular control over proprietary ICS and SCADA protocols.

The Fortinet Fabric-Ready Partner Program also enables organizations to seamlessly integrate complementary, third-party OT security solutions with the Fortinet Security Fabric. These deep technical integrations are pre-validated to ensure consistent interoperability, ease of deployment, reduced complexity, and increased automation.

Supporting Quotes

"The energy industry is becoming increasingly digital and thus securely connecting vast numbers of renewable energy sources to critical grid control centers is a significant and growing challenge. We are excited to be working with Fortinet to develop security solutions for mission-critical utility communication infrastructures. The cooperation with Fortinet has resulted in the development of deep packet inspection capabilities needed to address our utility-specific requirements. This development has been crucial for us to reach the next level in security and visibility for our OT networks."

- **Dr. Jürgen Tusch, Head of Telecommunications, Innogy SE**

"Nozomi Networks is a leader in delivering innovative cybersecurity and operational visibility solutions for OT systems. Working with Fortinet through its Fabric-Ready program enables Nozomi to integrate our OT network monitoring and behavioral analytics to deliver real-time visibility and threat detection, while seamlessly enabling automated enforcement through Fortinet's FortiGate Rugged series firewalls. We are proud to partner with Fortinet to deliver a broad detection and remediation solution for the OT space."

- **Chet Namboodri, VP, Alliances & Business Development, Nozomi Networks**

Additional Resources

- Please visit the Fortinet Critical Infrastructure Security homepage for more details about Fortinet's security solutions for Operational Technology infrastructures.
- Follow Fortinet on Twitter and LinkedIn, and Facebook.
- Join the conversation on the Fortinet blog.
  - What is the Appropriate Level of Cybersecurity for OT Systems? Cyber Insurers Want to Know.

[1] Forrester Brief: S&R Pros Can No Longer Ignore Threats To Critical Infrastructure, Rick Holland, Stephanie Balaouras, Katherine Williamson, July 2014

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 330,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

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:	**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.

News Provided by Acquire Media