January 9, 2018

Fortinet Demonstrates Integrated Security and Threat Protection for the Connected Car of the Future at CES 2018

Fortinet Collaborates with Renesas on Cutting-Edge Cybersecurity Solution to Secure Connected Car Domains, Including Powertrain, Telematics and Infotainment Systems

LAS VEGAS, Jan. 09, 2018 (GLOBE NEWSWIRE) -- **CES 2018**

Michael Xie, founder, president and chief technology officer at Fortinet
"Connected vehicles are the next major technology innovation disrupting the automotive industry. With 3D mapping, sensor processing, smart device integration, cloud-based services, advanced LAN/CAN networks, and autonomous driving defining the connected car of the future, the cyber risks are enormous. And with IoT devices connecting to the car network to access content and applications, the attack surface is even larger. Integrated security is paramount for the safety and consumer confidence in the connected car. Fortinet is extending its global leadership in network security to the automotive industry as manufacturers begin to develop vehicles that require automated security with real-time threat intelligence and strategic segmentation to protect the car's complex architecture. We are excited to collaborate with Renesas and demonstrate secure network solutions that meet the unique requirements of the evolving automotive operating environment at CES."

News Summary
Fortinet (NASDAQ:FTNT), a global leader in broad, integrated and automated cybersecurity, today announced it is exhibiting advanced cybersecurity capabilities for the connected car of the future at CES 2018 in the Renesas Advanced and Autonomous Test Track and Future Ready Solutions Showcase, January 9 - 12 in Las Vegas, Nevada.

- Developed in collaboration with Renesas Electronics, the cybersecurity prototype will demonstrate how the Fortinet FortiOS security operating system integrates with Renesas' R-Car H3 system-on-chip (SoC) to secure vehicle network domains, cloud-based services and applications.

- Fortinet and Renesas have created mock cyber breaches on a prototype connected car at CES, including intrusion prevention system (IPS) attacks and a DDoS (distributed denial of service) attacks to showcase the effectiveness of automated, integrated security to protect drivers from intruders taking control of their vehicle or applications.

Automated Security is Foundational for Technology and Safety Systems of the Connected Car
By 2025, it is projected that there will be 300 million connected cars up from 37 million in 2016, with annual revenues for connected car equipment and associated services to surpass $250 billion.[i] Key factors driving the global connected car market are increasing demand for self-driving features, implementation of data-driven decision-making, and connectivity solutions within the vehicle, such as access to smartphone features, music on-demand, Internet connectivity and infotainment in vehicles.

A connected car is equipped with Internet access and a wireless local area network (LAN), allowing drivers to share Internet connectivity with other devices both inside and outside the vehicle. To provide suitable cyber protection and ensure consumer confidence, automobile manufacturers need to design and deploy technology with a security-first mindset. Security systems need to span across communications standards, devices, and networks. They also need to extend visibility, interaction and control beyond a single vehicle to include the larger transportation ecosystem, including road and traffic control systems.

Connected cars require several different security solutions working as a single system and therefore need to include strategic segmentation of key function domains, such as powertrain, telematics and infotainment to ensure that threats are automatically contained and mitigated. Another key requirement is a real-time threat update system, like Fortinet's FortiGuard Labs, where the latest vulnerability and threat information can be fed to the vehicle to provide effective and automated protection. This also includes connecting back to a cloud network to share and correlate events to receive timely security patches and updates.

Fortinet and Renesas Demonstrate Security for Connected Car Networks
Fortinet and Renesas have collaborated on a prototype security solution that addresses the major cybersecurity risks in today's connected car network architecture. Recent cyber breaches demonstrate the urgent need for integrated security for these increasingly sophisticated vehicle networks, including the 2015 Jeep Cherokee hack where a hacker group wirelessly broke into the vehicle and electronically controlled vital functions, as well as the more recent Tesla Model S hack of its CAN

bus, interfering with the car's brakes, door locks, and dashboard computer from 12 miles away.

At CES, Fortinet and Renesas will show how the Fortinet Security Fabric technology running on the R-Car H3 SoC provides security policy management and automated protection of the powertrain and communication domains in the vehicle, including the LTE module, vehicle-to-vehicle communications module, the wireless access point, the engine control module and more. Supported by the on-chip security functions of the Renesas R-Car H3, Fortinet secures the communications between the domains and sets policies to limit access between certain domains to mitigate and control potential cyber threats. Specific demonstrations of mock IPS and DDoS cyber attacks will show how FortiOS automatically secures the data transmitted from a public cloud service to the in-car entertainment system.

To learn more about the Fortinet/Renesas demo and the Renesas Advanced and Autonomous Test Track and Future Ready Solutions Showcase, please visit http://renesasatces.com.

Supporting Quote
"Automotive engineers from throughout the supply chain look to Renesas for comprehensive solutions that accelerate development cycles and shorten the road to market. Renesas has partnered with Fortinet to help design cutting-edge cybersecurity solutions that aim to provide the level of integrated protection required of tomorrow's connected vehicle. We look to Fortinet as a trusted advisor who can extend its leading knowledge of network security to fit the unique demands and infrastructure requirements of automotive network security systems of the future."

- Amrit Vivekanand, Vice President, Automotive Systems Business Division, at Renesas

Additional Resources

- Follow Fortinet on Twitter, LinkedIn, Facebook and YouTube.

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

FTNT-O

[i] ON World Connected Car Markets Report, April 2017

Media Contact
Darlene Gannon
Fortinet, Inc.
408-235-7700
pr@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.