Extreme Networks Makes Securing Edge Devices Easy with Defender for IoT

February 4, 2019

New Technology Works on Any Network to Protect Wired and Wireless Devices from Cyber-Attacks

SAN JOSE, Calif., Feb. 4, 2019 /PRNewswire/ -- Use of IoT devices is proliferating in every industry, and with this growth comes risk – reports of IoT attacks increased 600 percent from 2016 to 2017. To protect enterprise networks, Extreme Networks, Inc. (Nasdaq: EXTR) today announced the general availability of Extreme Networks' Defender for IoT, a simple security solution to help organizations secure unsecured IoT devices. Defender for IoT can be deployed on any network and is so easy to use even non-technical staff at schools, hospitals, retailers and hospitality venues can use it to isolate and protect both wired and wireless IoT devices from cyberattacks.

IoT devices present two major security flaws for businesses today. Most lack embedded security—they were built to run on private networks where the assumption was it was tightly controlled, and device-level security wasn't required. Manufacturers never considered that the private enterprise network could be connected to the public internet, and therefore the devices may run out-of-date operating systems, have hardcoded passwords and/or lack anti-virus and firewall capabilities. And they are typically deployed in a flat or unsegmented network so that if breached, the attacker can gain access to sensitive areas of the network.

Extreme Networks' Defender for IoT, part of its Smart OmniEdge™ solution, solves these challenges by delivering the following:

- **IoT security without the complexity**: Defender for IoT is simple to deploy and easy to maintain. Users simply plug the Defender Adapter into an Ethernet port, and run the associated application. The Defender application *learns* the typical traffic patterns of network devices, and dynamically generates a security policy that locks down what a device communicates with and how it can communicate, automating edge network security for the enterprise. Once initial device profiles have been dynamically generated, non-technical staff can easily place the adapter between the device and the network and apply the appropriate security profile using a simple drop-down menu.
- **Segmentation and isolation of IoT devices:** With layer 2-7 visibility, Defender for IoT allows users to easily segment groups of IoT devices into multiple, isolated secure zones, reducing the network attack surface. Users can also centrally monitor and track device usage, location and roaming. This helps customers mitigate the risk of an attacker gaining access to more sensitive areas of the network.
- **Deployable on any network infrastructure:** Defender for IoT works with any vendor's IP network, providing in-line protection of IoT devices and segmentation through IPSec tunnels– without network changes. Additionally, Defender for IoT integrates with Extreme Fabric Connect™, giving customers the ability to leverage network automation capabilities and dynamic auto-attach functionality to streamline edge security efforts.

The optional ExtremeMobility™ AP3912 Wall Jack offers the same integrated defense as the Defender Adapter for both wired and wireless devices, but with the ability to support multiple devices in a single room. Defender for IoT is well suited for deployment in schools and universities, hospitals, hospitality venues, manufacturing, transportation, retail, and other industries that rely on connected devices to improve business efficiencies and customer experience.

Executive Perspectives

Mike Oligschlaeger, Vice President Business Management, Ascension
"At Ascension, we pride ourselves on our modern approach to healthcare, and are always looking for ways to improve patient outcomes and experience. But the latest greatest, connected medical technology is a risk to us if we can't ensure its security. Working closely with Extreme, we developed Defender for IoT to protect our patients and staff from the devastating consequences of an IoT breach, which in some cases can even be life threatening. This gives our entire organization peace of mind when it comes to our connected healthcare initiatives."

Christopher Frenz, Assistant Vice President of Information Security and Infrastructure, Interfaith Medical Center
"The continued proliferation of malware and other cyber threats requires a change in how organizations approach security. It is no longer sufficient to have a security strategy that relies solely on reactively blocking known bad behavior as the best reactive security can do is provide protection today against yesterday's threats. Instead, organizations need to establish a strategy that focuses on allowing only known good behavior. Taking a zero-trust approach to network security is a critical part of such a strategy and zero trust strategies need to encompass IoT devices as well."

David Raftery, Chief Revenue Officer, Integration Partners
"Customers across industries struggle with IoT security. One of the most challenging aspects is the creation of security policies for a diverse range of

devices. This can be both time consuming and fraught with error. Extreme's Defender for IoT solution automates this task with its ability to learn a device's typical behavior and then build a security policy that restricts its communication to only what is authorized. With the ability to then segment IoT devices into secure tunnels, Extreme provides our customers multi-layered IoT security over whatever network they have deployed today. It's a unique and a compelling solution."

Mike Leibovitz, Senior Director of Product Management and Strategy, Extreme Networks
"Businesses are extracting so much value from the IoT revolution that it's easy to see why deployments are happening fast, and security should not be viewed as an impediment to that. With Defender for IoT, our goal is not only comprehensive security, but delivering it in a way that is simple and accessible to everyday employees to ensure business productivity is not affected by security protocol. When plugged into our Smart OmniEdge visibility and analytics applications, users can easily control IoT device communication, ensure devices can only communicate with the appropriate resources, and then leverage analytics to prove and measure the outcome. We are the *only* vendor that can provide this level of granular visibility and control for wired and wireless IoT devices at the point of ingress."

Eric Miller, Senior Director of Information Technology, Ascension
"Security is typically a costly endeavor in healthcare organizations due to complexity which has only increased due to explosive growth in connected devices. With Defender for IoT, we can track, segment and secure every critical connected device on our network through a very intuitive user interface, versus the cost and complexity of legacy solutions. This saves our IT team tremendous time and money, giving us the ability to focus on higher-value technology initiatives."

Extreme at HIMSS and Mobile World Congress
To see Extreme's 802.11ax technology in action, visit Extreme in the IHP Pavilion at HIMSS 2019, February 11-15 in Orlando, or in Fira Gran Via, booth 1A26 at Mobile World Congress, February 25-28 in Barcelona.

Additional Resources

- Connect with Extreme via Twitter, Facebook, YouTube and LinkedIn
- Extreme Smart OmniEdge Solution Page
- Extreme Defender for IoT Product Page
- Extreme Fabric Connect Solution Brief
- ExtremeMobility Product Page

About Extreme Networks
Extreme Networks, Inc. (EXTR) delivers software-driven solutions from the enterprise edge to the cloud that are agile, adaptive, and secure to enable digital transformation. Our 100% in-sourced services and support are number one in the industry. Even with 30,000 customers globally, including half of the Fortune 50 and some of the world's leading names in business, hospitality, retail, transportation and logistics, education, government, healthcare and manufacturing, we remain nimble and responsive to ensure customer and partner success. We call this Customer-Driven Networking™. Founded in 1996, Extreme is headquartered in San Jose, California. For more information, visit Extreme's website or call 1-888-257-3000.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and other countries. Other trademarks shown herein are the property of their respective owners.

View original content to download multimedia:http://www.prnewswire.com/news-releases/extreme-networks-makes-securing-edge-devices-easy-with-defender-for-iot-300788512.html

SOURCE Extreme Networks, Inc.

Christi Nicolacopoulos, 603-952-5005, PR@extremenetworks.com