



## Extreme Networks Introduces New IoT Security and Automated Threat Mitigation for the Digital Enterprise

May 15, 2019

### ExtremeAI Security Delivers Advanced Behavioral Analysis, Automated Remediation, and Containment to Defend Against Network-Based Cyber Attacks

SAN JOSE, Calif., May 15, 2019 /PRNewswire/ -- Today's cyber threats, once inside, move laterally across networks to reach their targets, compromising everything in their path. The volume, speed and sophistication of these often-undetected attacks requires a new approach to enterprise network security. Accenture's 2018 [State of Cyber Resilience Report](#) found that 83 percent of respondents believe they need advanced technologies to secure their future, but just 2 in 5 had invested in AI and machine learning technologies. To meet this challenge, [Extreme Networks](#), Inc. (Nasdaq: EXTR) today announced its ExtremeAI™ Security application, a new class of network security that leverages artificial intelligence and machine learning to identify and remediate advanced threats against IoT devices.



The convergence of multi-cloud, mobility, and the massive influx of IoT devices in the enterprise expands the attack surface, making it an imperative to deploy advanced security technologies deep inside the network and not just at the perimeter. This explosion of endpoints and network traffic creates complexity and makes it difficult for network administrators and security teams to gain visibility into the chaos through traditional solutions. With IoT devices ranging from million-dollar smart MRI machines to five-dollar sensors, device-level security alone can't be trusted to secure endpoints. As a result, enterprise security teams are working overtime to keep up, but are often shorthanded due to a lack of trained cybersecurity personnel.

ExtremeAI Security delivers deep visibility and detection of malicious traffic, and real-time monitoring of IoT devices for behavioral anomalies, illuminating enterprise networks so attackers have nowhere to hide. Through fully-automated remediation of suspicious devices and traffic, ExtremeAI Security ensures threats are contained without manual intervention, preventing them from moving across the network. Extreme's powerful traffic analytics and visibility capabilities are embedded in this new security solution, combining the best of enterprise networking with innovations in machine learning to identify and remediate threats.

Key features of ExtremeAI Security include:

- **Behavioral monitoring and baselining:** Massively scalable behavioral anomaly detection leverages machine learning to understand typical behavior of IoT devices and automatically trigger alerts when endpoints act in unusual or unexpected ways.
- **Unsupervised learning:** A zero-touch, zero-configuration approach makes ExtremeAI Security easy to implement. The advanced machine learning algorithm automatically responds when triggered and mitigates threats. This major innovation is based on advancements in the field of Natural Language Processing.
- **Insights and granular analytics:** By leveraging its ExtremeAnalytics™ application – the company's flagship, end-to-end, analytics application — users can get deep visibility into the lateral movement of malicious traffic and any impact on crucial network services. Through the analytics platform, they can view threats by severity, category, high-risk endpoints and geography.
- **Multi-vendor interoperability and integration:** ExtremeAI Security works with all leading threat intelligence feeds, and close integration with Extreme Workflow Composer enables automatic threat mitigation and remediation. The automated ticketing feature integrates with variety of popular IT tools like Slack, Jira, and ServiceNow, and the solution as a whole interoperates with many popular security tools, including existing network taps. This extra layer of security is necessary in today's changing enterprise IT environment.

ExtremeAI Security will be generally available in October 2019.

#### Executive Perspectives

##### **Abby Strong, Vice President of Product Marketing, Extreme Networks**

"Security is top of mind for all of our customers. They have seen the devastating impact of data breaches across industries and understand that they need to change the way they view security infrastructure. The ability to stop cyberattacks from moving across networks is an absolute necessity to prevent the types of data breaches that can dramatically harm a business. Extreme's advancements in both security and machine learning will bring added peace of mind and a much-needed extra layer of security for our customers."

**Fritz Buetikofer, Senior IT Manager, University of Bern**

"In the past, we looked at tools that promise to provide visibility into data traffic and pinpoint anomalies. In most cases, it was very time consuming to customize the bells and whistles of these tools so that they were effective and didn't show too many 'false positives' – leaving our IT team to chase after non-issues and potentially exposing our organization to real security risks. In beta tests with ExtremeAI Security, it was immediately clear that Extreme is delivering an outstanding integration of analytics and anomaly detection – as well as device profiling – through the deep integration of its software and hardware capabilities. Even in this very early stage, its easy-to-use dashboard provides us with very precise information about incidents in every 'marked' component of our network infrastructure."

**Volker Kull, CTO, BELL Computer-Netzwerke GmbH**

"The irony of cybersecurity today is that many organizations continue to rely on traditional, perimeter-based defenses, despite ever more sophisticated attacks. This is a deceptive security that we must counteract with intelligent technologies. Extreme Networks is at the forefront of a new era of security, offering comprehensive network visibility, traffic analysis and artificial intelligence. We are proud to partner with Extreme to help customers modernize and improve their security environment, so they can confidently address today's IT challenges."

**Rohit Mehra, Vice President, Network Infrastructure, IDC**

"Traditional perimeter defenses alone are no longer enough to stop today's sophisticated cyberattacks. Enterprises must base their defenses off the idea that they have already been breached and focus their efforts on protecting critical applications and data, while preventing intruders from moving across the network. Extreme's new capabilities that leverage advanced machine learning will help enhance its automation toolset across its network visibility, analytics and management solutions, enabling enterprises to address their security challenges."

**Additional Resources**

- Connect with Extreme via [Twitter](#), [Facebook](#), [LinkedIn](#) and [YouTube](#)
- Extreme Elements: The Building Blocks of the Autonomous Enterprise [Solution Brief](#)
- Extreme Elements [Solution Page](#)
- Six Things You Need to Know about IoT Security in 2019 [Blog Post](#)
- The Future of Networking: The Autonomous Network [Blog Post](#)
- ExtremeAI Security [Product Page](#)
- ExtremeAI Security [Solution Brief](#)
- ExtremeAnalytics [Product Page](#)
- Extreme Workflow Composer [Product Page](#)
- Digital Transformation Requires an Autonomous Network [White Paper](#)

**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-introduces-new-iot-security-and-automated-threat-mitigation-for-the-digital-enterprise-300848484.html>

SOURCE Extreme Networks, Inc.

Christi Nicolacopoulos, 603-952-5005, [pr@extremenetworks.com](mailto:pr@extremenetworks.com)