Arista Advances Zero Trust Security Strategy with Enhancements to AI-driven Awake Security Platform

3/3/2021

Network detection and response combined with pervasive observability strengthens cybersecurity across cloud, hybrid and IoT environments

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **Awake Security**, the network detection and response (NDR) security division of **Arista Networks** (NYSE:ANET), today unveiled platform enhancements that strengthen its ability to detect advanced threats, protect the unmanaged attack surface and autonomously perform threat hunting and forensic investigations. Enhancements also include new features that make the platform even more intuitive for security analysts at all levels. Within six months of Arista's acquisition of Awake, the AI-driven network detection and response (NDR) platform is now integrated into Arista's zero trust and DANZ Monitoring Fabric (DMF) solutions, delivering innovative and secure capabilities to customers.

Awake's NDR platform is a key pillar of **Arista's vision for zero trust security**. With a new network-based **multi-domain macro-segmentation service**, situational awareness for all network resources and Awake's NDR, Arista is transforming network security from an afterthought to networks that are inherently secure. This approach provides continuous monitoring to identify malicious intent whether originating from outside or inside the network perimeter along with the ability to then rapidly take remedial action.

With this launch, the Awake platform gains critical capabilities through its deepening integration with Arista solutions. **Arista's DANZ Monitoring Fabric (DMF)** is a next-generation network visibility solution that provides pervasive observability for both north-south and east-west traffic. When combined with the Awake platform, customers benefit from a scale-out architecture that efficiently protects high-throughput networks by enabling use cases such as network detection and response (NDR), threat hunting and full packet network forensics.

"Zero trust is critical to an organization's defenses and the integration of Awake into Arista enables this posture even when the network and entities on it are continuously changing," said Katie Teitler, Senior Analyst at TAG Cyber. "In particular, in this age of remote and mobile work, discovering and controlling devices unmanaged and often

unknown to the security team is incredibly important to the cyber risk equation. Awake Security's product enhancements help organizations move further in their zero trust journey and empower them to operate more securely."

Key capabilities now available with the Awake platform include:

Autonomous Unmanaged Device Discovery and Risk Tracking: By monitoring the customer's infrastructure, Awake's security knowledge graph, EntityIQ™ has deep visibility to everything plugged into the network. With the most recent enhancements, the platform uses encrypted traffic analysis and other AI-techniques to automatically discover devices that do not appear to be managed by corporate IT and security teams. This surfaces, labels and profiles shadow-IT, IoT and other aspects of the attack surface otherwise invisible to the security team. Organizations are thus enabled to take purposeful and proactive steps that enhance security, lower risk and improve the cost and efficiency of digital asset management.

Autonomous Threat Hunting and Investigations: Ava™, Awake's autonomous security analyst, sees enhanced capabilities to automate forensic investigations. Ava now performs open source intelligence analysis of discovered artifacts using natural language processing and topic modeling. Ava-generated forensic investigation reports have shown that Ava frequently finds more incident-related activity than a senior human investigator analyzing the same activity.

Intelligent Role-Centric User Experience: Recognizing that the information a Level 1 analyst finds useful and valuable is very different than a Level 3 threat hunter, Awake has made role-centric usability and workflows a foundational element of the platform. Today's launch enables organizations to surface just the right amount of data and capabilities based on the role of the analyst using the platform. This allows the analyst to quickly make risk management decisions rather than getting bogged down with data overload.

"To enable zero trust, security needs to be baked into the network, and Arista has led the charge in making this foundational approach to security a reality," said Rahul Kashyap, VP / GM Arista NDR Security Division. "In very short order, Awake is contributing to this comprehensive vision for security while tapping Arista's innovations to advance network detection and response. This will continue to be a very powerful combination."

The capabilities of the Awake platform are also available through Awake's Managed Network Detection and Response (MNDR) solution. With Awake's MNDR, organizations can instantly improve their security programs' maturity and effectiveness by relying on round-the-clock and round-the-world monitoring by the highly skilled threat hunting and incident response analysts at Awake Labs.

To get more insight into Awake's latest innovations and to hear about Arista's broader security strategy, join an

exclusive virtual event, **Zero Trust Security Strategies in a Multi-Cloud World** featuring Arista and Awake executives and security industry thought leaders on Tuesday, March 9th, 2021.

Register **here** to learn more about Awake's most recent innovations at our webinar on April 1st, 2021.

Read more about this announcement on Rahul Kashyap's **blog**.

About Arista Networks

Arista Networks is an industry leader in cognitive cloud networking solutions for large data center and campus environments. Arista's award-winning platforms deliver availability, agility, automation analytics, and security through CloudVision® and Arista EOS®, an advanced network operating system. For more information, visit **www.arista.com**.

ARISTA, CloudVision and EOS are among the registered and unregistered trademarks of Arista Networks, Inc. in jurisdictions worldwide. Other company names or product names may be trademarks of their respective owners. Additional information and resources can be found at **www.arista.com**. This press release contains forward-looking statements including, but not limited to, statements regarding cost savings, performance, capabilities, and security. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Forward-looking statements are subject to risks and uncertainties that could cause actual performance or results to differ materially from those expressed in the forward-looking statements, including rapid technological and market change, customer requirements and industry standards, as well as other risks stated in our filings with the SEC available on Arista's website at **www.arista.com** and the SEC's website at **www.sec.gov**. Arista disclaims any obligation to publicly update or revise any forward-looking statement to reflect events that occur or circumstances that exist after the date on which they were made.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20210303005286/en/**

Media Contact

Amanda Jaramillo
Corporate Communications
Tel: (408) 547-5798
amanda@arista.com

Investor Contact

Charles Yager
Product and Investor Development
Tel: (408) 547-5892
cyager@arista.com

Source: Arista Networks