Arista Unveils Attack Surface Assessment Service

12/21/2020

Delivers AI-driven advanced threat hunting and incident response expertise

SANTA CLARA, Calif.--(BUSINESS WIRE)-- Arista Networks (NYSE:ANET) today announced an **Attack Surface Assessment**, an advanced security service delivered through the recent acquisition of **Awake Security**. This new offering identifies cyber security risks from devices, users or third-party systems, especially those that go unmonitored today since they are beyond the visibility of the security team. Designed and delivered by experts who have responded to some of the world's most consequential breaches, this assessment focuses on detecting and evicting the attacker rapidly.

"CIOs are becoming increasingly concerned about security as it has become more complex," stated Golan Ben-Oni, CIO, IDT Corporation. "To make matters worse, sponsored groups can steal intellectual property and attack resources that are now in the wild. Big companies and banks are still getting hacked and technologies like IoT are huge threats. We need to reboot security and make it simple to manage. I believe Arista Networks is simplifying security."

Arista's new assessment service is a fitting example of simplified security. It proactively finds threats to devices and applications known to the IT and security teams, as well as shadow IT and unmanaged infrastructure across client to campus, data center and cloud.

"Sophisticated threats are no longer reliant on traditional malware," said Rahul Kashyap, Vice President and General Manager, Arista's NDR Security Division. "The recent supply chain attacks have exposed gaps in security programs. This new offering reinforces our commitment to help our customers defend against Sunburst and future threats."

Secure Client to Cloud Networking

Fundamental to addressing those gaps is understanding the broad digital attack surface organizations expose, from client to cloud networks. The Attack Surface Assessment provides customers access to the industry-leading NDR platform to proactively discover, detect and respond to threats targeting digital assets within the organization.

Unlike other security technologies that merely identify malicious behavior, the Awake Security Platform goes beyond to separate the known good and identifies any malicious intent lurking in between. With this cognitive knowledge, Arista and Awake experts then perform threat hunting to uncover signs of highly targeted attacks as well as systemic weaknesses that open an organization to risk. The assessment also includes an incident response retainer in case a breach is uncovered.

The industry is dealing with the complexity of attacks that permeate cloud, security and networking assets. Arista's network-based approach delivers detection and response for IT, IoT, shadow IT and infrastructures across client to campus, data center and cloud.

For more details on Awake's approach to detecting supply chains threats like the SolarWinds / Sunburst campaign read our blog at **https://awakesecurity.com/blog/detecting-supply-chain-threats-like-solarwinds-sunburst/**.

For technical insights see **https://awakesecurity.com/blog/a-network-threat-hunting-playbook-for-advanced-attacks/**.

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 CloudEOS are among the registered and unregistered trademarks of Arista Networks, Inc. in jurisdictions around the world. 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 performance, reliability 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/20201221005189/en/**

Media Contact

Amanda Jaramillo

Corporate Communications

Tel: (408) 547-5798

amanda@arista.com

Investor Contact

Curtis McKee

Corporate and Investor Development

Tel: (408) 547-5701

curtism@arista.com

Source: Arista Networks