Arista integriert Threat Detection & Response in Cognitive Campus

AI-Lösung „AVA“ schließt die Lücke zwischen Netzwerk und Sicherheit

Santa Clara (USA), 28.02.2022 – Arista Networks (NYSE:ANET), spezialisiert auf datengesteuerte Netzwerke, fügt seinen Switches der 720XP-Serie für den Campus-Einsatz eingebettete Sicherheits- und Paketanalysefunktionen hinzu. Durch die Integration von NDR-Funktionen (Network Detection & Response) in die auf Arista EOS basierenden Switches erhalten Unternehmen eine viel größere Transparenz und können Bedrohungen im gesamten kognitiv ausgerichteten Campus abwehren. Die abgesicherte Infrastruktur optimiert bestehende Arbeitsprozesse und fördert gleichzeitig die automatische Risikominderung, ohne dass zusätzliche externe Netzwerksicherheitsprodukte integriert werden müssen.

„Als renommierter Anbieter von Netzwerkinfrastruktur verfügt Arista über eine starke Marktposition, um Sicherheitsfunktionen in den Kern des Netzwerks zu integrieren. Die Einbeziehung von Elementen künstlicher Intelligenz wie Deep Learning, Belief Propagation und Natural Language Processing in Daten, die direkt am Switch erfasst werden, kann die Sicherstellung der Netzwerksicherheit für Kunden erheblich vereinfachen“, sagt Dr. Edward Amoroso, Chief Executive Officer, TAG Cyber und Research Professor, New York University. „Als früher selbst aktiver Sicherheitsexperte finde ich die Möglichkeit, den operativen Aufwand für die Nachrüstung von Sicherheitslösungen zu vermeiden, sehr reizvoll.“

Präzises NDR mit Arista AVA
Basierend auf AVA™ (Autonomous Virtual Assist), besteht diese KI-gesteuerte Funktion aus zwei Schlüsselkomponenten: AVA Sensoren und AVA Nucleus. AVA-Sensoren unterstützen eine Vielzahl von Formfaktoren, von Standalone-Appliances über virtuelle bis hin zu Cloud-Workloads und jetzt auch Power-over-Ethernet (PoE)-Switches auf dem Campus. Diese Sensoren erfassen und übertragen die Deep-Packet-Daten an den AVA Nucleus, der sowohl als On-Premise- als auch als SaaS-Lösung angeboten wird. Mit einem einfachen Software-Upgrade für die Switches und minimalen Auswirkungen auf die Switch-Performance oder Ausfallsicherheit bietet die Arista NDR-Plattform:

- Bessere Sichtbarkeit: Identifizierung von Schadenspotenzialen, Erstellung von Profilen und Tracking aller Benutzer, Apps und Geräte – unabhängig davon, ob es sich um gemanagte Desktops und Workstations oder nicht gemanagte Zulieferer, Lieferketten, Cloud- und IoT-Workloads handelt.

- Elemente werden auf der Grundlage von Verhaltensanalysen zueinander in Beziehung gesetzt, um eine objektorientierte Ansicht zu erstellen und den Arbeitsablauf eines Sicherheitsexperten bei der Bedrohungsanalyse zu vereinfachen.

- Situationsanalyse in Echtzeit: Die gesamte Bedrohungslandschaft und das Ausmaß eines Angriffs verstehen, damit Sicherheitsanalytiker intelligente und risikoabhängige Entscheidungen treffen können.

• KI-gesteuerte Bedrohungserkennung: Automatisierte Erkennung von und Reaktion auf Bedrohungen im Netzwerk mit einer Plattform, die zugrundeliegende Angriffstaktiken, -techniken und -verfahren identifiziert und nicht nur auf bekannte Indikatoren für eine Kompromittierung reagieren kann.

• Managed NDR: Nutzung der Leistungsfähigkeit der Arista NDR-Plattform in Verbindung mit den kompetenten Experten von Awake Labs, die über jahrzehntelange Erfahrung verfügen, um den 24x7-Sicherheitsbetrieb, die Gefahrenabwehr und das Incident Response-Programm des Kunden zu verbessern.

„Netzwerksicherheit ist für die meisten Unternehmen eine ständige Herausforderung, da Hardware-Installationen und Konfigurationsänderungen auf der Ebene der Netzwerkinfrastruktur erforderlich sind. Obwohl die Unternehmen wissen, dass das Netzwerk eigentlich einen einzigartigen Überblick bietet, sind die Sicherheitsteams gezwungen, einen Kompromiss zwischen der Informationsfülle des Netzwerks und den laufenden operativen Kosten zu finden“, sagt Rahul Kashyap, Vice President und General Manager of Cybersecurity und CISO bei Arista Networks. „Durch die Integration von NDR-Funktionen in die Switching-Infrastruktur selbst schafft Arista ein integriertes, sicheres Netzwerk, das das Unternehmensrisiko reduziert, indem es sowohl die Zeit bis zur Erkennung einer Bedrohung als auch die Zeit bis zur Schadensbehebung verkürzt.“

Bisherige NetFlow-basierte Lösungen haben nur eine begrenzte Detailtiefe (Port-, IP-Adresse und allgemeine Protokolldaten) und verfügen nicht über den nötigen Kontext, um auch die neuesten Gerätetypen oder Risiken zu identifizieren. Im Gegensatz dazu analysieren die AVA-Sensoren das gesamte Paket, einschließlich der Daten der Applikationsebenen, und bilden so die Grundlage für eine automatisierte oder auch manuelle Bedrohungssuche.

Innovationen wie diese haben dazu geführt, dass Arista NDR im KuppingerCole „Network Detection & Response Leadership Compass 2021 Report“ als Leader eingestuft wurde. Die Plattform erhielt außerdem den „AI Breakthrough Award“ für die beste KI-basierte Lösung für CyberSecurity.

AVA-Verfügbarkeit
Die neuen Funktionen werden voraussichtlich im zweiten Quartal 2022 allgemein verfügbar sein, erste Tests laufen im März 2022 an.

Lesen Sie mehr über diese Ankündigung im Blog von President und CEO Jayshree Ullal hier: https://blogs.arista.com/blog/network-security-to-secure-networks

Über Arista Networks
Arista Networks ist ein branchenführender Anbieter von datengesteuerten Client-to-Cloud-Netzwerken für große Rechenzentrums-, Campus- und Routing-Umgebungen. Die mehrfach ausgezeichneten Plattformen von Arista bieten Verfügbarkeit, Agilität, Automatisierungsanalysen und Sicherheit durch CloudVision® und das fortschrittliche Netzwerkbetriebssystem Arista EOS®.
Weitere Informationen finden Sie unter: www.arista.com

ARISTA, EOS, CloudVision, NetDL und AVA gehören zu den eingetragenen und nicht eingetragenen Marken von Arista Networks, Inc. in allen Ländern der Welt. Andere Firmennamen oder Produktnamen können Marken ihrer jeweiligen Eigentümer sein. Weitere Informationen und Materialien finden Sie unter www.arista.com.

Diese Pressemitteilung enthält zukunftsgerichtete Aussagen, einschließlich, aber nicht beschränkt auf, Aussagen zu Kosteneinsparungen, Leistung, Funktionen und Sicherheit. Alle Aussagen, die sich nicht auf historische Fakten beziehen, sind Aussagen, die als zukunftsgerichtete Aussagen betrachtet werden können. Zukunftsgerichtete Aussagen unterliegen Risiken und Ungewissheiten, die dazu führen können, dass die tatsächliche Leistung oder die Ergebnisse wesentlich von den in den zukunftsgerichteten Aussagen zum Ausdruck gebrachten abweichen, einschließlich des raschen Technologie- und Marktwandels, der Kundenanforderungen und der Industriestandards sowie anderer Risiken, die in unseren bei der SEC eingereichten Unterlagen aufgeführt sind, die auf der Website von Arista unter www.arista.com und auf der Website der SEC unter www.sec.gov verfügbar sind. Arista lehnt jede Verpflichtung ab, zukunftsgerichtete Aussagen öffentlich zu aktualisieren oder zu revidieren, um Ereignisse oder Umstände widerzuspiegeln, die nach dem Datum, an dem sie gemacht wurden, eintreten.

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

Investorenkontakt
Liz Stine
Investor Relations
Tel: (408) 547-5885
liz@arista.com