Arista forciert Zero-Trust-Sicherheitsstrategie mit Weiterentwicklungen der KI-gesteuerten Awake Security-Plattform

Network Detection und Response in Kombination mit durchgängiger Überwachung verstärken die Datensicherheit in Cloud-, Hybrid- und IoT-Umgebungen

Santa Clara (USA), 03.03,2021 – Awake Security, der Geschäftsbereich für Network Detection & Response (NDR) von Arista Networks (NYSE:ANET), präsentiert heute signifikante Erweiterungen der Plattform: Die Funktionen zur Erkennung komplexer Bedrohungen, zum Schutz nicht-administrierter Angriffsflächen und zur autonomen Durchführung von Threat Hunting und forensischen Analysen wurden ausgebaut. Zu den Erweiterungen gehören zudem neue Funktionen, die die Plattform für Sicherheitsexperten auf allen Ebenen noch intuitiver gestalten. Sechs Monate nach der Übernahme von Awake durch Arista ist die KI-gesteuerte NDR-Plattform ab sofort in die Zero Trust- und DANZ Monitoring Fabric (DMF)-Lösungen von Arista integriert und bietet den Kunden innovative und zugleich sichere Einsatzszenarien.

Die NDR-Plattform von Awake ist eine wichtige Säule von Aristas Vision für Zero-Trust-Sicherheit. Mit einem neuen netzwerkbasierten Multi-Domain-Makro-Segmentierungsservice, situativer Überwachung aller Netzwerkressourcen und Awake-NDR verwandelt Arista die Netzwerksicherheit zu einem integrativen Bestandteil von Unternehmensnetzwerken. Dieser Ansatz bietet eine kontinuierliche Überwachung, um gefährliche Aktionen zu identifizieren, unabhängig davon, ob sie von außerhalb oder innerhalb des Netzwerkbereichs ausgehen, und ermöglicht es, sofortige Gegenmaßnahmen zu ergreifen.

Mit diesen Neuerungen gewinnt die Awake-Plattform dank der vertieften Integration mit Arista-Lösungen entscheidende Funktionalitäten hinzu. Aristas DANZ Monitoring Fabric (DMF) ist eine Netzwerküberwachungslösung der nächsten Generation, die eine durchgängige Beobachtung sowohl des Nord-Süd- als auch des Ost-West-Verkehrs ermöglicht. In Kombination mit der Awake-Plattform profitieren Kunden von einer Scale-out-Architektur, die Netzwerke mit hohem Datendurchsatz effizient schützt und dabei Anwendungen wie Network Detection and Response, Bedrohungsanalyse und umfassende Netzwerkforensik ermöglicht.

„Zero Trust ist entscheidend für die Schutzmaßnahmen eines Unternehmens, und die Integration von Awake in Arista ermöglicht dies, auch wenn sich das Netzwerk und die darin befindlichen Geräte dynamisch ändern", sagt Katie Teitler, Senior Analyst bei TAG Cyber. „Insbesondere im derzeitigen Umfeld von Remote- und mobiler Arbeit ist das Erkennen und Kontrollieren von Geräten, die nicht administriert werden und dem Sicherheitsteam oft unbekannt sind, essemtiell wichtig für die Beurteilung von Cyber-Risiken. Die Produkterweiterungen von Awake Security helfen Unternehmen, auf ihrem Zero-Trust-Pfad weiter zu kommen und ermöglichen ihnen einen sicheren Geschäftsablauf."

Zu den wichtigsten Funktionen, die jetzt mit der Awake-Plattform verfügbar sind, gehören:

Autonome Device Discovery und Risk Tracking: Durch die Überwachung der Infrastruktur des Kunden liefert EntityIQ™, der Security Knowledge Graph von Awake, einen detaillierten Überblick über alles, was mit dem Netzwerk verbunden ist.

Mit den jüngsten Erweiterungen nutzt die Plattform verschlüsselte Traffic-Analysen und andere KI-Techniken, um Geräte zu entdecken, die nicht von der Unternehmens-IT und den Security-Teams kontrolliert zu werden scheinen. Dadurch werden Shadow-IT, IoT und andere Einfallstore, die sonst für das Sicherheitsteam unsichtbar sind, aufgedeckt, markiert und eingeordnet. Firmen werden so in die Lage versetzt, gezielte und proaktive Schritte zu unternehmen, die die Sicherheit erhöhen, das Risiko senken und die Kosten und Effizienz des Digital Asset Managements verbessern.

Autonomes Threat Hunting und Untersuchungen: Ava™, das autonome Sicherheitsanalysetool von Awake, verfügt über erweiterte Funktionen zur Automatisierung forensischer Untersuchungen. Ava führt nun eine Open-Source-Intelligence-Analyse der entdeckten Objekte mithilfe von natürlicher Sprachverarbeitung und Themenmodellierung durch. Von Ava generierte forensische Untersuchungsberichte haben gezeigt, dass Ava häufiger kritische Vorfälle identifiziert als ein erfahrener menschlicher Analytiker, der dieselben Aktivitäten prüft.

Intelligente, rollenzentrierte Benutzerfreundlichkeit: Angesichts der Tatsache, dass die Informationen, die ein Level-1 Threathunter für relevant und wertvoll hält, sich stark von denen eines Level-3 Threathunters unterscheiden, hat Awake rollenzentrierte Benutzeroptimierung und Workflows zu einem grundlegenden Element der Plattform gemacht. Die heutige Markteinführung ermöglicht es Unternehmen, Analytikern genau die richtige Menge an Daten und Funktionen anzuzeigen, die diese für deren Rolle benötigen. Dies ermöglicht es dem Anwender, schnell Risikomanagement-Entscheidungen zu treffen, anstatt sich in der Datenflut zu verzetteln.

„Um Zero Trust zu realisieren, muss Sicherheit in das Netzwerk eingebaut sein, und Arista ist Vorreiter bei der Verwirklichung dieses grundlegenden Sicherheitsansatzes", sagt Rahul Kashyap, VP / GM Arista NDR Security Division. „In kürzester Zeit leistet Awake einen wesentlichen Beitrag zu dieser umfassenden Sicherheitsstrategie und nutzt gleichzeitig die Innovationen von Arista, um Network Detection und Response zu optimieren. Diese Kombination wird auch für die Zukunft eine sehr leistungsstarke Verbindung bilden."

Die Funktionen der Awake-Plattform sind auch über die Managed Network Detection and Response (MNDR)-Lösung von Awake verfügbar. Mit MNDR können Unternehmen den Leistungsgrad und die Effektivität ihrer Sicherheitsprogramme sofort verbessern, indem sie sich auf die Rund-um-die-Uhr-Überwachung durch die hochspezialisierten Threat Hunting- und Incident Response-Analysetools von Awake Labs verlassen.

Um mehr Einblicke in die Neuerungen von Awake zu erhalten und mehr über Aristas breit angelegte Sicherheitsstrategie zu erfahren, können Sie an dieser exklusiven virtuellen Veranstaltung teilnehmen:

„Zero Trust Security Strategies in a Multi-Cloud World" mit führenden Vertretern von Arista und Awake sowie Vordenkern der Sicherheitsbranche am Dienstag, den 9. März 2021: https://events.arista.com/arista-security-innovate-2021

Registrieren Sie sich hier, um mehr über die neuesten Innovationen von Awake in unserem Webinar am 1. April 2021 zu erfahren: https://events.arista.com/2021-4-awake-security-webinar

Lesen Sie mehr über diese Ankündigung auf dem Blog von Rahul Kashyap:
https://awakesecurity.com/blog/never-trust-always-verify/

Über Arista Networks
Arista Networks ist ein Marktführer bei kognitiven Cloud-Netzwerklösungen für große Rechenzentrums- und Campus-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, CloudVision und EOS gehören zu den eingetragenen und nicht eingetragenen Marken von Arista Networks, Inc. in Gerichtsbarkeiten weltweit. Andere Firmen- oder Produktnamen können Marken der jeweiligen Eigentümer sein. Weitere Informationen und Ressourcen 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.

Medienkontakt

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

Investorenkontakt

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