Arista Networks präsentiert die Zukunft von Zero-Trust-Networking

Wichtige Partnerschaft mit Zscaler beschleunigt
die Umsetzung von Zero Trust bei Kunden

Santa Clara (USA), 10.11.2023 – Arista Networks (NYSE: ANET), einer der führenden Anbieter von Cloud-Networking-Lösungen, stellt heute eine umfangreiche Zero-Trust-Networking-Architektur vor. Diese nutzt die vorhandene Netzwerkinfrastruktur, um Sicherheitsbarrieren abzubauen, Arbeitsabläufe zu optimieren und ein integriertes Zero-Trust-Konzept zu realisieren. Der Ansatz basiert auf einer Kombination aus von Arista entwickelten Technologien und strategischen Kooperationen mit wichtigen Partnern und nutzt das Netzwerk, um schwierig zu implementierende Zero-Trust-Kontrollen für Devices, Workloads, Identitäten und Daten auszugleichen.

Ein auf Standards basierender Ansatz für Zero Trust
Unternehmensnetze reichen heute von den klassischen Unternehmensstandorten und Rechenzentren bis hin zu IoT, Remote-Arbeitsplätzen und der Cloud. Die Absicherung dieser verteilten Infrastruktur erfordert einen Mikro-Schutzbereich um jedes sensible digitale Asset. Vor diesem Hintergrund hat die US-Behörde für Cybersecurity und Infrastruktursicherheit (CISA) ein Zero-Trust-Referenzmodell mit verbindlichen Leitlinien für fünf Grundpfeiler entwickelt: Identität, Geräte, Netzwerke, Anwendungen & Workloads sowie Daten.

„Die Zero-Trust-Lösungen von Arista entsprechen genau der Netzwerk-Philosophie des CISA-Modells und sind so konzipiert, dass sie Unternehmen auf ihrem Weg zur Zero-Trust-Umsetzung unterstützen", sagt Rahul Kashyap, Vice President und General Manager für Cybersecurity bei Arista Networks. „Unsere Stärke, dies reibungslos über das Netzwerk zu realisieren, hilft dabei, Hindernisse in anderen Bereichen wie Identität, Devices, Workload und Daten zu überwinden."

Komponenten der Zero-Trust-Architektur von Arista
Die Zero-Trust-Architektur von Arista nutzt die zugrunde liegende Netzwerkinfrastruktur, von Switches bis hin zu WAN-Routern, um wichtige Funktionen bereitzustellen, die sich nahtlos in das bestehende Sicherheitskonzept und die Tools des Unternehmens integrieren lassen.

Die Schlüsselkomponenten dieser integrierten Sicherheitslösung sind:
- Arista CloudVision AGNI vereinfacht das sichere Onboarding und die Fehlerbehebung für Benutzer und Devices sowie die kontinuierliche Zustandsanalyse und die Kontrolle des Netzwerkzugriffs erheblich.

- Arista Macro Segmentation Service (MSS) ermöglicht die Erstellung und Anwendung von Mikroperimetern über Edge Switches, die jedes Asset schützen oder isolieren können, ohne dass Firewalls im gesamten Firmennetz eingesetzt werden müssen. Segmentierungsrichtlinien können einmalig in Arista CloudVision definiert und dynamisch auf der Grundlage von Echtzeitinformationen zu Netzwerk, Anwendung, Gerät oder Benutzeridentität durchgesetzt werden.
- Arista NDR erkennt, profiliert und klassifiziert selbstständig jedes Gerät, jeden Benutzer und jede Anwendung im verteilten Netzwerk. Basierend auf diesem tiefgreifenden Kenntnisstand über die Angriffsfläche erkennt die Plattform Bedrohungen, die von diesen Entitäten ausgehen und liefert den notwendigen Kontext, um schnell eingreifen zu können.
- Arista unterstützt nativ Verschlüsselungsfunktionen wie MACsec und Tunnelsec und ermöglicht es Unternehmen, Daten von und zu Legacy-Anwendungen und Workloads zu verschlüsseln, ohne diese Systeme zu ändern. Stattdessen können sich die Unternehmen darauf verlassen, dass das Netzwerk die Daten vor unbefugtem Zugriff, Abfangen und Manipulationen schützt.

Auf Basis von Arista NetDL und AVA AI Insights
Die Zero-Trust-Architektur von Arista stützt sich auf die Grundlagen des einheitlichen Betriebssystems EOS® und der zentralen Management-Oberfläche CloudVision®. Der EOS Network Data Lake (NetDL™) bietet eine eindeutige Referenzquelle für die Echtheit der Netzwerkdaten und eine gemeinsame Sensor-/Sammelarchitektur, die Forensik und Analytics für die Suche nach Bedrohungen, für die Netzwerk- und Anwendungsüberwachung sowie für Network Detection & Response (NDR) ermöglicht.

Arista Autonomous Virtual Assist (AVA™) nutzt Machine Learning und andere Technologien künstlicher Intelligenz (KI), um die durchgängige Transparenz, die kontinuierliche Erkennung von Bedrohungen, die Segmentierung und die Zugriffskontrolle zu optimieren. In Kombination mit verteilten netzwerkweiten Status- und Telemetriedaten und der Integration von Drittanbietern fördert AVA die Automatisierung und Flexibilität, um den manuellen Aufwand für den Betrieb und die Absicherung von Netzwerken erheblich zu reduzieren.

Ausbau des Client-to-Cloud-Ökosystems mit Zscaler
Die Zero-Trust-Architektur von Arista ist offen und API-orientiert konzipiert. Bei diesem Ansatz liegt der Schwerpunkt auf der Nutzung des vorhandenen Netzwerks, um Schwachstellen und Silos zu beseitigen und gleichzeitig die Arbeitsabläufe in den wichtigsten Sicherheitsbereichen im Netzwerk-Stack zu optimieren. Zu den Partnern im Zero-Trust-Ökosystem von Arista gehören Microsoft, CrowdStrike und der neueste Partner: Zscaler. Arista ist Mitglied der Microsoft Intelligent Security Association (MISA) und unterstützt die Sicherheitstechnologie von Microsoft.

Die neu eingeführte Integration mit der Zscaler Zero Trust Exchange Plattform, einer cloud-nativen Plattform, die Benutzer, Workloads und Devices über jedes Netzwerk und jeden Standort verbindet und absichert, erweitert Arista das NDR um kritische Informationen über Domains und Infrastrukturen der Angreifer.

Darüber hinaus kann Zscaler Internet Access (ZIA) durch diese Integration den Zugriff von Geräten blockieren, die Arista als kompromittiert identifiziert hat und von Domains oder IP-Adressen, die Arista als schädlich eingestuft hat.

„Mit der beschleunigten Einführung der Cloud und der Aufweichung der Sicherheitsbereiche erweist sich das bisherige Schutzkonzept von Unternehmen als unwirksam. Es ist entscheidend, einen Zero-Trust-Ansatz zu verfolgen, um die Sicherheit von Benutzern und Assets zu gewährleisten", sagt Amit Raikar, VP of Business Development and Technology Alliances bei Zscaler. „Die gemeinsamen Kunden von Zscaler und Arista werden in der Lage sein, Risiken zu kontrollieren und Richtlinien für die gesamte Belegschaft einzuführen, was letztendlich die Sicherheit ihrer Unternehmen erhöht."

Weitere Informationen zu dieser Ankündigung finden Sie hier in unserem Zero-Trust-Whitepaper:
https://www.arista.com/assets/data/pdf/Whitepapers/Zero-Trust-Maturity-Model-WP.pdf

Weitere Informationen zu unserer Partnerschaft mit Zscaler finden Sie in dieser Lösungsübersicht:
https://www.arista.com/assets/data/pdf/Arista-NDR-and-Zscaler-Solution-Brief.pdf

Über Arista
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, Automatisierung, Analyse und Sicherheit durch CloudVision® und das fortschrittliche Netzwerkbetriebssystem Arista EOS®.
Weitere Informationen 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