Arista launcht neueste Version von Multi-Domain-Segmentierung für Zero Trust Networking

Lösung zur Mikrosegmentierung entschärft Bedrohungen bei der Übertragung von Datenpaketen zwischen Servern innerhalb eines Rechenzentrums

Santa Clara (USA), 02.05.2024 – Arista Networks (NYSE: ANET), führender Anbieter von Cloud-Networking-Lösungen, veröffentlicht ein umfangreiches Update seines Arista MSS® (Multi-Domain Segmentation Service) Produktportfolios. Damit löst das Unternehmen die Herausforderung, ein wirklich unternehmensweites Zero-Trust-Netzwerk zu schaffen. Ohne Software-Agents für Endgeräte und proprietäre Netzwerkprotokolle ermöglicht Arista MSS effektive Mikroperimeter, die laterale Aktivitäten in Campus- und Rechenzentrumsnetzen einschränken und so den Angriffsradius von Bedrohungen wie Ransomware reduzieren.

Unternehmensweites Zero Trust braucht eine wirksame Mikrosegmentierung

Die verteilte IT-Infrastruktur von heute mit der Möglichkeit, von überall aus zu arbeiten, die explosionsartige Zunahme von IoT-Geräten sowie Multi-Cloud-Anwendungen haben den klassischen Sicherheitsrahmen auf den Kopf gestellt und zu einer dynamischen und unkalkulierbaren Angriffsfläche geführt. Um ihre Sicherheitslage zu verbessern, haben Unternehmen mit Zero-Trust-Maßnahmen begonnen, die eine granulare Kontrolle sowohl der ein- und ausgehenden (north-south) als auch der rechenzentrumsinternen Datenflüsse (east-west) erfordern.

Firewalls sind schlichtweg nicht für den Schutz vor lateralen Datenströmen konzipiert, würden eine Vielzahl zusätzlicher Sicherheits-Appliances erfordern, die Kosten in die Höhe treiben und zu einer riesigen Zunahme komplexer Regelsätze führen – die dennoch keinen Schutz vor lateralen Datenbewegungen bieten.

Um diese Aufgabe zu bewältigen, empfiehlt das „Zero Trust Maturity Model" der Cybersecurity and Infrastructure Security Agency (CISA) die Einführung von Mikrosegmentierung für eine hochgradig verteilte, granulare Kontrolle mittels Mikroperimetern.

Zwar gibt es auf dem Markt viele Mikrosegmentierungslösungen, sowohl netzwerk- als auch endgerätbasiert, doch haben sie mit der operativen Komplexität, mit Interoperabilitäts- und Portabilitätsproblemen sowie hohen Kosten zu kämpfen, was ihre breite Akzeptanz in Unternehmen einschränkt. Als Folge davon geraten die Bemühungen um Zero Trust oft ins Stocken.

Standardbasierte Netzwerk-Mikrosegmentierung

Arista MSS bietet eine auf Standards basierende Mikrosegmentierung unter Verwendung der bestehenden Netzwerkinfrastruktur und überwindet damit die Probleme der bestehenden Lösungen. MSS ist netzwerkagnostisch und endgerätunabhängig.

Es vermeidet proprietäre Protokolle und lässt sich daher nahtlos in eine Umgebung verschiedener Netzwerkanbieter integrieren. Die Lösung erfordert auch keine Software für die Endgeräte und vermeidet die für agentenbasierte Mikrosegmentierungslösungen typischen Einschränkungen der Portabilität und der Komplikationen im praktischen Betrieb.

„Wir sind sehr beeindruckt von dem Potenzial der MSS-Mikroperimeter-Segmentierungstechnologie von Arista", so Evan Gillette, Security Engineering, Paychex Inc. „Wir halten diese Technologie für äußerst vielversprechend und glauben, dass sie das Potenzial hat, unsere Sicherheits- und Segmentierungsstrategie von einem traditionellen Perimeter-Ansatz zu einer stärker verteilten, netzwerkzentrierten Architektur zu verändern. Wir freuen uns auf die Zusammenarbeit mit Arista, um die Möglichkeiten diese innovative Technologie und ihrer Anwendungen in unsere Infrastruktur einzugliedern."

Arista MSS kombiniert drei Funktionen, die es Unternehmen ermöglichen, Mikroperimeter um jeden digitalen Asset zu bauen, den sie schützen sollen, sei es auf dem Campus oder im Rechenzentrum.

Arista MSS ermöglicht:

- Stateless Wire-Speed Enforcement im Netzwerk: Arista EOS®-basierte Switches bieten ein einfaches Modell für eine granulare, identitätsbasierte Mikroperimeter-Überwachung. Dieses Enforcement-Modell ist unabhängig vom Typ des Endgeräts und identisch in Campus- und Rechenzentrumsumgebungen, was den Betrieb im Tagesgeschäft vereinfacht. Arista MSS ermöglicht somit eine laterale Segmentierung, die heute oft fehlt und entlastet gleichzeitig die Firewalls, die explizit für diesen Zweck implementiert werden müssten.

- Umleitung zu Stateful Firewalls: Arista MSS kann nahtlos in Firewalls und Cloud-Proxys von Partnern wie Palo Alto Networks und Zscaler integriert werden, um Stateful Network Enforcement zu ermöglichen, insbesondere für externen und interzonalen Traffic. MSS stellt somit sicher, dass der gewünschte Datenverkehr an diese kritischen Sicherheitskontrollen weitergeleitet wird, so dass sie sich auf L4-L7 Stateful Enforcement konzentrieren können und unnötiges Hairpinning von anderem Datenverkehr vermieden wird.

- CloudVision für Mikroperimeter-Management: Arista CloudVision® powered by NetDL™ bietet tiefe Echtzeiteinblicke in Pakete, Datenströme und Endgeräte-identitäten. Dies ermöglicht eine wirksame laterale Segmentierung des internen Rechenzentrumstraffics. Darüber hinaus erleichtern die MSS-Dashboards innerhalb von CloudVision den Arbeitsaufwand des Administrators für die Steuerung der Mikroperimeter. MSS erweitert Aristas Ask AVA™ (Autonomous Virtual Assist) Service um eine chat-ähnliche Schnittstelle für Anwender, mit der sie in den Dashboard-Daten navigieren sowie Policy-Verstöße abfragen und filtern können.

„Als Bank ist es unser Ziel, umfassende Finanzprodukte und -lösungen anzubieten, wobei die Daten und die Sicherheit unserer Kunden für uns oberste Priorität haben. Sicherheit ist auch eines unserer wichtigsten architektonischen Prinzipien bei der Gestaltung unserer Rechenzentrumsnetze", so Komang Artha Yasa, Technology Division Head bei OCBC. „Arista MSS vervollständigt unsere Zero-Trust-Struktur, indem es effizient mit den Firewalls zusammenarbeitet, um unsere kritischen Zahlungssysteme zu mikrosegmentieren. Der Service von Arista ist für uns einfach zu implementieren, da er ohne softwarebasierte Agenten auskommt und uns dennoch Interoperabilität in unserer gesamten Rechenzentrumsumgebung bietet."

Zero Trust-Ökosystem

Arista MSS lässt sich nahtlos in die umfassende Arista Zero Trust Networking-Lösung integrieren, einschließlich Arista CloudVision, CV AGNITM und Arista NDR. Es lässt sich auch mit branchenführenden Firewalls wie Palo Alto Networks, IT-Service-Management (ITSM) wie ServiceNow und Virtualisierungsplattformen wie VMware integrieren.

„Arista MSS ist eine willkommene Ergänzung unserer Zero-Trust-Strategie", sagt Dougal Mair, Associate Director, Networks and Security an der University of Waikato. „Die Möglichkeit, ein offenes, aber sicheres Netzwerk für viele Benutzer (z. B. Studenten, Dozenten, Gäste), IT-Geräte (z. B. Laptops, Drucker) und IoT-Tools (einschließlich Sensoren und Smart Lighting) in einer großen Umgebung bereitzustellen, war eine enorme Herausforderung für die Universität. Arista MSS verhindert jegliche unbefugte Peer-to-Peer- und laterale Bewegung in unserem dynamischen Netzwerk."

Verfügbarkeit

Arista MSS befindet sich derzeit in der Testphase und wird im 3. Quartal 2024 allgemein verfügbar sein.

Besuchen Sie uns gern am Stand #6453 in der North Hall auf der RSA Conference.

Erfahren Sie mehr über Multi-Domain-Segmentierungsservices in Aristas Webinar am 9. Mai: https://events.arista.com/zero-trust-microperimiters

Weitere Informationen zu dieser Ankündigung finden Sie im Blog von Jayshree Ullal hier: https://blogs.arista.com/blog/the-era-of-microperimeters

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

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