Arista liefert Multi-Domain-Segmentierung für Zero-Trust-Unternehmensnetzwerke

Vereinfachte Netzwerksegmentierung mit dynamischer Partnerintegration

Santa Clara (USA), 03.02.2021 – Arista Networks (NYSE:ANET) hat heute ein neues Zero-Trust-Sicherheits-Framework für moderne digitale Unternehmen vorgestellt. Der „Arista Multi-Domain Macro-Segmentation Service“ ist eine Suite von Funktionen zur Integration von Sicherheitsrichtlinien in das Netzwerk, die einen offenen und konsistenten Ansatz zur Netzwerksegmentierung über alle Netzwerkdomänen hinweg bieten. Die neueste Funktionalität von Arista MSS® (Macro-Segmentation Service), die durch Arista EOS® (Extensible Operating System) und CloudVision® ermöglicht wird, umfasst den neuen Gruppensegmentierungsansatz MSS-Group, der die Zugriffskontrolle für Benutzer und IoT-Geräte in den modernen Arbeitsumgebungen von Unternehmen vereinfachen wird.

„Sicherheit und Vernetzung wachsen zusammen. Aristas Zero-Trust-Strategie stützt sich stark auf Analysen und KI, um schädliche Inhalte zu identifizieren, und ist gut positioniert, um den vielleicht größten Wandel im Netzwerkbereich zu vollziehen", sagt Zeus Kerravala, Gründer und Principal Analyst bei ZK Research.

Zero Trust Security in einer Cloud- und IoT-Welt
Traditionelle Netzwerksicherheitsarchitekturen schützten die Nutzer nur an den Netzwerkgrenzen. Dieser Ansatz ist bei verteilten Benutzern und einer Vielzahl von IoT-Endpunkten in heutigen Unternehmen nicht mehr ausreichend. Eine Zero-Trust-Architektur, die davon ausgeht, dass kein Benutzer oder Gerät freien Zugriff auf das Netzwerk hat, ist erforderlich, um moderne Netzwerke zu sichern. Zero-Trust vertraut niemals ohne Überprüfung, beschränkt den Zugriff auf nur notwendige Verbindungen und überwacht dann kontinuierlich das Verkehrsverhalten. In diesem neuen Ansatz muss das implizite Vertrauen, das mit dem Standort des Netzwerks verbunden ist, durch eine kontinuierliche, proaktive Netzwerküberwachung mit verhaltensgestützter Situationsanalyse ersetzt werden, um die Übersicht über Netzwerkgeräte und eine schnelle Reaktion auf Vorfälle zu gewährleisten. Der Zero-Trust-Sicherheitsansatz von Arista ist darauf ausgelegt, diese Entwicklung zu unterstützen, indem er netzwerkbasierte Multi-Domain-Segmentierung, situationsbezogene Überwachung und Transparenz für alle Netzwerkressourcen sowie KI-gesteuerte Netzwerkerkennung und -reaktion kombiniert.

IoT-fähige Gruppensegmentierung
Eine sichere Gruppensegmentierung muss auf Basis funktionaler Rollen, wie Kameras oder DVRs, über Unternehmensbereiche hinweg und unabhängig von traditionellen Netzwerkadressierungskonstrukten definiert werden. Darüber hinaus muss jede Netzwerklösung auf einem offenen Framework aufbauen, das den Einsatz sowohl in Greenfield- als auch in Brownfield-Implementierungen ermöglicht.

Arista stellt mit MSS-Group einen neuen Netzwerksegmentierungsdienst zur Steuerung zugelassener Netzwerkkommunikation zwischen Gruppen vor. MSS-Group ist auf EOS-basierten Switches verfügbar und ermöglicht – im Gegensatz zu traditionellen Ansätzen, die auf Schnittstellen, Subnetzen oder physischen Ports beruhen – die Durchsetzung von Sicherheitsrichtlinien auf der Basis logischer Gruppen.

Der Dienst beruht auf einem effizienten Mechanismus zur wirkungsvollen Umsetzung von Vorgaben zur Sicherheit auf der Datenseite und vermeidet die Einschränkungen von herstellerspezifischen Lösungen, die proprietäre Hardware-Tags verwenden und durch ineffiziente Hardware-Ressourcen-Mappings begrenzt sind. Die MSS-Group-Lösung nutzt mit CloudVision die gleiche Management-Plane-Plattform für Multi-Domain-Automatisierung, Telemetrie und Analyse zur Verwaltung und Transparenz von Sicherheitsrichtlinien. Darüber hinaus ist die MSS-Group-Lösung am leistungsfähigsten, wenn CloudVision über vorhandene APIs mit einem dynamischen Identitätsanbieter integriert wird.

Arista hat in Zusammenarbeit mit Forescout eine solche Lösung entwickelt, die das Design und die Verwaltung von Richtlinien vereinfacht. Unternehmen können mit Forescout eyeSegment automatisch Echtzeit-Kontext anwenden, um jedes angeschlossene Gerät mit der entsprechenden Sicherheitssegmentierungsgruppe zu verknüpfen, auf einfache Weise gruppenbasierte Richtlinien zu entwerfen und zu überwachen und die entsprechenden Segmentierungsrichtlinien an CloudVision zu übermitteln. CloudVision übernimmt dann die dynamische Orchestrierung der erforderlichen Richtlinie zur Weiterleitung an die Arista-Switches.

Arista Multi-Domain Segmentierung
Arista Multi-Domain Segmentierung verknüpft das Netzwerk sicher über den Campus, das Rechenzentrum und die Cloud. Die Lösung vermeidet die proprietären Silo-Architekturen der bisherigen Anbieter.

Mit dem Fokus auf Multi-Domain- und Netzwerksicherheitskonvergenz optimiert Arista zudem MSS für Enterprise-Edge-Firewall- und Anwendungsfälle im Bereich der Rechenzentrumsvirtualisierung, und bietet damit umfassende Segmentierungslösungen für unternehmensweite Einsatzszenarien.

MSS Firewall ermöglicht das Einfügen von Sicherheitsdiensten und eine flexible Platzierung von Firewall-Richtlinien über DMZ-Edge-, Rechenzentrums- und Campus-Netzwerke hinweg. MSS Firewall nutzt Netzwerkstrukturen, die auf offenen Standards basieren, und leitet den Datenverkehr dynamisch zum Kontrollpunkt der Firewall-Policy, um die Durchsetzung der Sicherheitsrichtlinien auf breitere Datenverkehrsmuster auszuweiten. MSS Firewall nutzt dieselbe CloudVision-Orchestrierung und lässt sich mit Palo Alto Networks und anderen führenden Firewall-Lösungen aus dem Sicherheitspartner-Ökosystem von Arista integrieren.

MSS Host ist eine auf Rechenzentren fokussierte Lösung, bei der die Sicherheitsrichtlinien vom virtualisierten Host auf das physische Netzwerk ausgedehnt werden. Durch eine API-Integration zwischen CloudVision und der VMware NSX-Plattform erweitert MSS Host die NSX-Mikrosegmentierungsrichtlinien auf Bare-Metal-Workloads.

Arista ermöglicht dies durch eine breite Palette von Integrationen mit Partnern aus dem Sicherheits-Ökosystem wie Aruba, Forescout, Palo Alto Networks, VMware und Zscaler (siehe Herstellersupport). Zusätzlich zu den fortschrittlichen MSS-basierten dynamischen Segmentierungsdiensten unterstützt Arista weiterhin umfangreiche Netzwerksegmentierungsmodelle wie VXLAN/EVPN, VRFs, VLANs und Access Control Listen.

Verfügbarkeit
Die MSS-Firewall- und MSS-Host-Funktionalität wird als Teil von Arista CloudVision ausgeliefert. Die MSS-Group-Funktionalität wird in Q1 2021 für Testläufe verfügbar sein.

Registrieren Sie sich hier, um mehr über Aristas Multi-Domain-Segmentierungslösung in unserem Webinar am 18. März 2021 zu erfahren.

Lesen Sie mehr über diese Ankündigung im Blog von Jayshree Ullal hier.

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.

Diese Pressemitteilung enthält zukunftsgerichtete Aussagen, einschließlich, aber nicht beschränkt auf, Aussagen über die Vorteile und Best Practices, die bei der Entwicklung und Implementierung von Aristas EOS- und CloudVision-Software verwendet werden, sowie über die Ermöglichung von Kosteneinsparungen, Sicherheitsfunktionen, gesteigerte Leistung und Effizienz. Alle Aussagen, mit Ausnahme von Aussagen über historische Fakten, sind Aussagen, die als zukunftsgerichtete Aussagen angesehen werden können. Zukunftsgerichtete Aussagen unterliegen Risiken und Unsicherheiten, die dazu führen könnten, dass die tatsächliche Leistung oder die Ergebnisse wesentlich von denen abweichen, die in den zukunftsgerichteten Aussagen zum Ausdruck gebracht werden, einschließlich: unserer begrenzten Historie und Erfahrung mit der Entwicklung und Markteinführung neuer Produkte; Probleme mit der Produkt-, Support- oder Servicequalität; sich schnell entwickelnde Veränderungen in der Technologie, den Kundenanforderungen und den Industriestandards sowie andere Risiken, die in unseren Unterlagen bei der SEC angegeben sind, die auf der Website von Arista unter www.arista.com und der Website der SEC unter www.sec.gov. verfügbar sind. Arista lehnt jede Verpflichtung ab, zukunftsgerichtete Aussagen öffentlich zu aktualisieren oder zu überarbeiten, um Ereignisse oder Umstände widerzuspiegeln, die nach dem Datum, an dem sie gemacht wurden, eintreten.

Kontakt für Medien
Amanda Jaramillo
Corporate Communications
Tel: 001(408) 547-5798
amanda@arista.com

Kontakt für Investoren
Charles Yager
Product and Investor Advocacy
Tel: 001(408) 547-5892
cyager@arista.com