PLATZ FÜR DAS PARTNER-LOGO

TOP 10 Funktionen, die Sie von Ihrem SASE-Anbieter erwarten sollten

Wünschen Sie sich auch, mit einem Klick auf eine SASE-Architektur umstellen und die gesamte Netzwerkinfrastruktur in eine gut funktionierende und sichere Cloud-Umgebung verlagern zu können? Die Realität sieht leider anders aus. Doch das bedeutet nicht, dass der Umstieg kompliziert oder extrem aufwendig sein muss.

Eine reibungslose Umstellung auf eine SASE-Architektur beginnt damit, den richtigen Anbieter zu finden, der Ihnen bei diesem Prozess zur Seite steht. Suchen Sie nach einem Anbieter mit Erfahrung auf diesem Gebiet, der es Ihnen ermöglicht, Ihre vorhandenen Investitionen weiter zu nutzen, und der Ihnen hilft, ohne Störungen des Betriebs und auf sichere Weise auf Cloud-basierte Sicherheit umzusteigen – und zwar in dem Tempo, das für Ihr Unternehmen am besten ist.

1 EINHEITLICHES RICHTLINIENMANAGEMENT

Verwalten Sie die Sicherheit für lokale und Cloud-basierte Umgebungen jederzeit über eine zentrale Benutzeroberfläche über die Cloud.

Der Ansatz für ein einheitliches Richtlinienmanagement (Unified Policy Management, UPM) muss für eine sichere Benutzererfahrung sorgen – mit durchgängigen, standortunabhängigen Richtlinien für Benutzer, Geräte und Anwendungen.

2 SCHNELLER UND EFFEKTIVER SCHUTZ VOR KOMPLEXEN BEDROHUNGEN

Wehren Sie unsichtbare, unbekannte und verschlüsselte Bedrohungen ab.

Entscheiden Sie sich für einen Cloud-basierten Service mit statischen und dynamischen Funktionen zur Malware-Erkennung, die selbst komplexeste und verschleierte Bedrohungen nahezu in Echtzeit identifizieren und blockieren.

3 AUSFALLSICHERHEIT UND SKALIERBARKEIT

Erzielen Sie einfache und effektive Skalierbarkeit in physischen, virtuellen und Cloud-basierten Sicherheitsumgebungen.

Achten Sie auf betriebliche Simplizität und skalierbare Sicherheitsfunktionen, die von den Endbenutzern unbemerkt bleiben und die Benutzererfahrung nicht beeinträchtigen.

4 SINGLE-STACK-ARCHITEKTUR MIT EINHEITLICHEM RICHTLINIEN-FRAMEWORK

Nutzen Sie vorhandene Investitionen als Einstiegspunkt in geschäftskritische Cloud-Sicherheitsdienste.

Erstellen Sie einmalig Richtlinien und wenden Sie diese dann überall mit einheitlichem Richtlinienmanagement an, einschließlich benutzer- und anwendungsbasiertem Zugriff, IPS, Malwareschutz und sicherem Webzugriff über eine einzige Richtlinie.

5 KONSISTENTE SICHERHEIT FÜR MITARBEITENDE AN VERSCHIEDENEN STANDORTEN

Bieten Sie Remote-Mitarbeitenden sicheren Zugriff auf die Anwendungen und Ressourcen, die sie für produktives Arbeiten benötigen.

Konsistente Sicherheitsrichtlinien folgen Benutzern, Geräten und Anwendungen, ohne dass Regelsätze kopiert oder neu erstellt werden müssen.

6 UNTERSTÜTZUNG FÜR HYBRID-UMGEBUNGEN

Ihr SASE-Anbieter sollte in der Lage sein, sowohl lokale als auch Cloud-basierte und Hybrid-Umgebungen zu unterstützen.

Entscheiden Sie sich für einen Anbieter, der Ihnen eine reibungslose, sichere Umstellung auf SASE in einem für ihr Unternehmen optimalen Tempo ermöglicht.

7 ZENTRALE IDENTITÄTSQUELLE

Sie sollten erwarten dürfen, dass das Produkt Ihres SASE-Anbieters jede Identitätslösung auf dem Markt unterstützt.

Sie müssen bei der Wahl einer Identitätslösung freie Hand haben. Schließlich muss diese Lösung Ihre geschäftlichen Anforderungen erfüllen – und nicht die Ihres SASE-Anbieters.

8 DYNAMISCHE BENUTZERSEGMENTIERUNG

Ihre Benutzer müssen jederzeit und überall geschützt sein.

Mit benutzerabhängigen Richtlinien und automatisierter, auf dem Risikostatus basierender Zugriffskontrolle wird der Zugriff durch nicht autorisierte Dritte verhindert. So minimieren Sie die Angriffsfläche am Edge.

9 NACHWEISBAR WIRKSAME SICHERHEIT

Suchen Sie nach einem SASE-Anbieter, der den Erfolg seiner Sicherheitslösung nachweisen kann.

Lassen Sie sich die Effektivität der Schutzmaßnahmen zeigen, einschließlich client- und serverseitiger Abwehr von Exploits, Ransomware, Botnets und DNS-Tunneling. Ihr Anbieter muss die Herausforderungen der modernen Bedrohungslandschaft in Form einer SaaS-Lösung meistern können, damit Angriffe in Ihrer Umgebung abgewehrt werden – lokal und in der Cloud.

10 NAHTLOSER ÜBERGANG ZU CLOUD-BASIERTER SICHERHEIT IN IHREM EIGENEN TEMPO

Lassen Sie sich nicht zum Umstieg auf eine SASE-Architektur zwingen, bevor Sie dazu bereit sind.

Der Übergang zu einer Cloud-basierten Sicherheitsarchitektur sollte reibungslos in einem für Sie optimalen Tempo erfolgen, und zwar über eine Ihnen vertraute Verwaltungsoberfläche mit einheitlichem Richtlinienmanagement und benutzerfreundlichen Bereitstellungsassistenten. Zudem müssen sich die Richtliniendienste leicht und effektiv orchestrieren, bereitstellen und verwalten lassen, unabhängig davon, wo sie sich befinden.

11 BONUSPUNKTE FÜR SECURITY ASSURANCE

Erhalten Sie die Gewissheit, dass Regel- und Richtlinienänderungen effektiv durchgesetzt werden.

Unabhängig davon, ob es sich um eine Regel für eine herkömmliche oder eine als Service bereitgestellte Firewall-Richtlinie handelt, müssen Regeln in der richtigen Reihenfolge platziert werden, um in Kraft zu treten. Ihr SASE-Anbieter muss Ihrem IT-Team helfen, diese Regelsätze korrekt zu interpretieren, damit duplizierte und abgeschattete Regeln automatisch vor dem Commit identifiziert werden.

Die Umstellung auf eine SASE-Architektur verläuft in jedem Unternehmen anders und wie diese neue Infrastruktur konzipiert, umgesetzt und ausgebaut wird, bestimmen Sie selbst. Nur so können Sie Ihre Benutzererfahrung, Services und Daten bedarfsgerecht optimieren. Wofür Sie sich auch entscheiden – Sie benötigen einen SASE-Anbieter an Ihrer Seite, der da ansetzt, wo Sie seine Dienste benötigen, und der Sie auf dem gesamten Weg begleitet.

Hauptsitz und Sitz des Vertriebs

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Telefon: +1-888-JUNIPER (+1-888-586-4737)

oder +1-408-745-2000

Fax: +1-408-745-2100

www.juniper.net/de/de.html

Hauptniederlassung für die Regionen APAC und EMEA

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, Niederlande

Telefon: +31-0-207-125-700

Fax: +31-0-207-125-701

Juniper Networks | Driven by Experience™

3050168-001-DE August 2023