Juniper Networks | Engineering Simplicity

Whitepaper

„THE RISE OF ZERO TRUST“

Trennung von Realität und Mythen

INHALT

KURZFASSUNG

Unternehmen stehen unter starkem und wachsendem Druck, nachzuweisen, dass sie angemessene Maßnahmen zum Schutz vor Cyberangriffen ergreifen und unbefugte Zugriffe auf vertrauliche Daten unterbinden. Der derzeit am weitesten verbreitete – und vielleicht auch praktikabelste – Ansatz zur Unternehmenssicherung ist das Zero-Trust-Konzept. Als Vorstandsmitglied, Manager oder Techniker mit Verantwortung für IT oder Sicherheit sollten Sie sich unbedingt darüber im Klaren sein, warum Zero Trust bei der Entwicklung einer tragfähigen Sicherheitsstrategie eine wesentliche Rolle spielt.

In diesem Whitepaper trennen wir die Realität der Zero-Trust-Sicherheitsarchitektur von einigen hartnäckigen Mythen und Missverständnissen und zeigen, wie Juniper Connected Security eine Zero-Trust-Netzwerkarchitektur nicht nur unterstützt und ermöglicht, sondern Ihnen auch hilft, sie schneller und einfacher zu implementieren.

Einleitung: Ein Modell für wirksamere Sicherheit

Das Zero-Trust-Konzept gewinnt zunehmend an Bedeutung und verändert die Art und Weise, wie wir Sicherheit im Allgemeinen und Netzwerkarchitektur im Besonderen angehen. Und das wurde auch Zeit. Die vorherrschende Annahme, dass wir internen Benutzern, Netzwerken und Systemen einfach vertrauen sollten, ist schlicht nicht mehr haltbar, wie eine endlose Reihe von Datenschutzverletzungen beweist.

Während die Vorteile eines Zero-Trust-Ansatzes klar und überzeugend sind, gibt es für Netzwerk- und Sicherheitsexperten, die mit der Implementierung der Architektur beauftragt sind, viele Fragen und Herausforderungen. Muss die gesamte Netzwerkinfrastruktur ersetzt werden? Ist die Mikrosegmentierung ein realistisches Ziel? Schließt die Cloud die Möglichkeit einer Zero-Trust-Architektur aus?

In diesem Whitepaper werden wir die heutige Realität von einigen hartnäckigen Mythen und Vorurteilen über Zero-Trust-Sicherheitsarchitekturen trennen. Gleichzeitig zeigen wir Ihnen, wie Juniper Connected Security nicht nur eine Zero-Trust-Netzwerkarchitektur unterstützt und ermöglicht, sondern Ihnen auch helfen kann, diese schneller und einfacher zu implementieren.

Gesucht: Bessere Möglichkeiten zum Schutz moderner Umgebungen

Damals: Erinnern Sie sich an die Zeit, als alle Endgeräte dem Unternehmen gehörten und intern verwaltet und gesichert wurden? Damals konnte man annehmen, dass jeder Benutzer und jedes Gerät innerhalb des Unternehmensnetzwerks vertrauenswürdig war. Unternehmensanwendungen wurden in einem sicheren Datencenter betrieben und konnten sich gegenseitig vertrauen.

Heute: Der Edge des Netzwerks hat sich verschoben, da viele Workloads in die Cloud verlagert wurden und nicht verwaltete, mobile Geräte eher die Norm als die Ausnahme geworden sind. Der Standort von Anwendungen, Benutzern und ihren Geräten ist nicht mehr statisch. Daten sind nicht mehr auf das Datencenter des Unternehmens beschränkt. Die Lücken in der Sichtbarkeit und im Schutz werden immer größer, da sich die Angriffsfläche vergrößert und Unternehmen gezwungen sind, verschiedene, nicht miteinander verbundene Tools zu verwenden, um wirklich alles zu sehen und zu schützen.

Gleichzeitig werden Cyberkriminelle immer versierter darin, moderne Sicherheitsmaßnahmen zu umgehen. Immer mehr Angreifer erreichen ihre Angriffsziele mittels lateraler Ausbreitung. Sie haben Zugang zu immer ausgefeilteren Toolkits und laienfreundlichen Anleitungen zur Ausnutzung von Schwachstellen. Gleichzeitig wächst die Zahl dieser Schwachstellen: 2018 enthielt die National Vulnerability Database bereits 14.760 bekannte Sicherheitsschwachstellen — mehr als doppelt so viele wie noch 2016.

Fazit: Die Stärkung des Netzwerkrandes reicht zum Schutz von Netzwerken, Nutzern, Anwendungen und Daten längst nicht mehr aus.

Die Anfänge von Zero Trust

Im Jahr 2009 stellte Forrester Research das neue Zero-Trust-Modell für Informationssicherheit vor, das seitdem weithin akzeptiert und übernommen wurde. Durch die Übernahme der Konzepte und architektonischen Komponenten von Zero Trust können Unternehmen sicherer werden und gleichzeitig den Aufwand für die Einhaltung von Vorschriften verringern und letztlich die Kosten senken.

Quelle: „No More Chewy Centers: The Zero Trust Model of Information Security“, Forrester Research, Inc., März 2016

Ein neues Sicherheitsparadigma

Hier kommt Zero Trust ins Spiel, das moderne Sicherheitsparadigma, das mittlerweile vielerorts genutzt wird und einen besseren Schutz vor aktuellen Bedrohungen bietet. Der Grundgedanke von Zero Trust lautet: „Niemals vertrauen, immer überprüfen“ – mit anderen Worten: Gehen Sie davon aus, dass jede Komponente Ihres Netzwerks potenziell so gefährlich ist, als ob sie direkt im Internet wäre, und behandeln Sie Zugriffsanfragen entsprechend.

Beim Zero-Trust-Ansatz gilt inhärentes Vertrauen als kritische Schwachstelle. Die Annahme, dass alles innerhalb des eigenen Unternehmensnetzwerks vertrauenswürdig ist, ermöglicht es Bedrohungsakteuren und böswilligen Insidern, die sich Zugangsdaten verschafft haben und diese missbrauchen, sich mühelos lateral in ihren Zielumgebungen zu bewegen, dort auf Daten zuzugreifen oder diese auszuschleusen.

Die zunehmende Bedeutung von Zero Trust

Unternehmen, die in einer kürzlich durchgeführten Umfrage von Forbes Insights als „Vorreiter in Sachen Cybersicherheit“ identifiziert wurden, betrachten Initiativen wie Zero Trust als „extrem wichtig“ für ihre Sicherheitsstrategien.

Quelle: „Cybersecurity Trailblazers Make Security Intrinsic to Their Business“, Forbes Insights, 2019

Wenn Sie stattdessen Mikroperimeter um kritische Daten, Anwendungen und Dienste herum einrichten, können Sie dafür sorgen, dass nur bekannte, zulässige Ströme und Anwendungen Zugriff auf die zu schützenden Assets haben. Mit einer Zero-Trust-Architektur legen Sie fest, wer einen Mikroperimeter passieren darf, und richten Kontrollen in der Nähe der zu schützenden Objekte ein, um den unbefugten Zugang zu und die Ausschleusung von vertraulichen Daten zu verhindern.

Dieser Ansatz schützt Unternehmen zwar nicht vor jedem denkbaren Angriff, bietet aber folgende Vorteile:

- Das Risiko einer ausgefeilten Bedrohung oder eines Datendiebstahls wird reduziert, indem unbefugte laterale Bewegungen und Zugriffe verhindert werden.
- Die Erkennung von und Reaktion auf Bedrohungen werden beschleunigt.
- Die Transparenz wird gestärkt.
- Die Compliance mit Vorgaben wie HIPAA, PCI-DSS, FISMA und anderen wird unterstützt.

Die Säulen von Zero Trust

Seit der Entwicklung des Zero-Trust-Konzepts haben sich auch Branchenexperten wie die Analysten von Forrester eingebracht. Forrester nennt es das Zero Trust eXtended (ZTX) Ecosystem[1].

In seiner einfachsten Form ist Zero Trust ein konzeptionelles und architektonisches Modell dafür, „wie Sicherheitsteams Netzwerke mit sicheren Mikroperimetern umgestalten, die Datensicherheit mithilfe von Verschleierungstechniken stärken, die mit übermäßigen Benutzerprivilegien und Zugriffsrechten einhergehenden Risiken mindern und die Sicherheitserkennung und -reaktion mit Analysen und Automatisierung drastisch verbessern“.

Das ZTX-Ökosystem verfolgt einen ganzheitlichen Ansatz, der Prozesse und Technologie umfasst. Es beinhaltet Daten, Workloads, Netzwerke, Geräte, Menschen, Transparenz und Analysen sowie Automatisierung und Orchestrierung (siehe Abb. 1).

Immer mehr Unternehmen übernehmen den Zero-Trust-Ansatz. Derzeit arbeiten 60 Prozent der Unternehmen weltweit an Zero-Trust-Strategien, was bedeutet, dass sie den Plan entweder formalisieren oder aktiv an seiner Umsetzung arbeiten.[2] Diese Unternehmen haben bereits erkannt, dass die falschen Vorstellungen, die Zero-Trust-Bemühungen in der Vergangenheit behindert haben, nicht mehr der Realität entsprechen. Sehen wir uns einige dieser Mythen und Missverständnisse genauer an.

Befürworter von Zero Trust

„Zero Trust kann heute eine ausgereifte Lösung anbieten, die keine zusätzliche betriebliche Komplexität oder größere Änderungen der Architektur erfordert. Vielmehr kann es den Betrieb vereinfachen und gleichzeitig die Sicherheit und den Schutz kritischer, wertvoller Vermögenswerte verbessern.“

Quelle: „Zero Trust Cybersecurity Current Trends“, American Council for Technology-Industry Advisory Council (ACT-IAC), April 2019

[1] „The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook“, Forrester Research, Inc., Juli 2019
[2] „The Digital Enterprise Report: How the World's Largest Organizations Are Evolving with Technology“, Okta, 2019

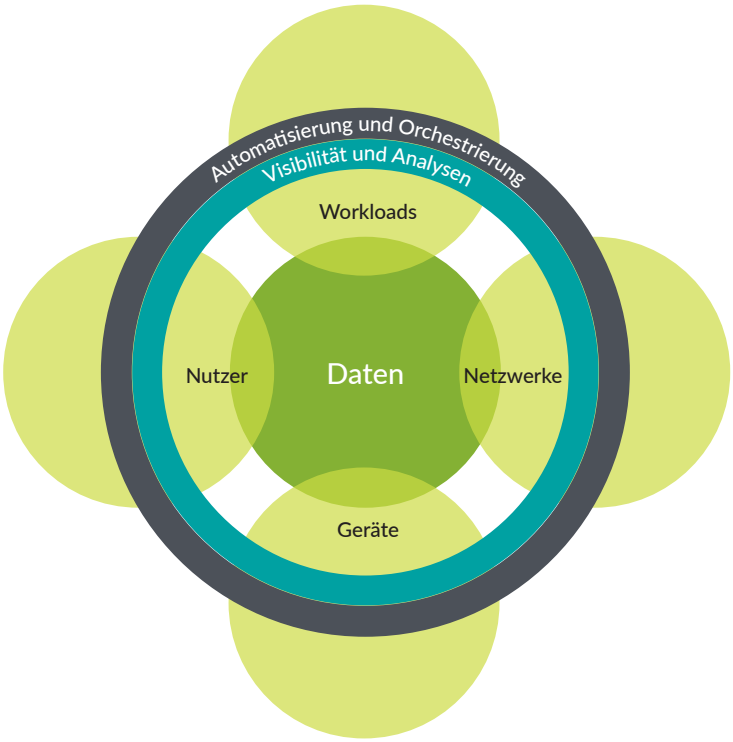

Abbildung 1: Das Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc.

Mythos 1: Zero Trust ist für die meisten Unternehmen zu teuer

Viele Unternehmen gehen fälschlicherweise davon aus, dass die Einführung eines Zero-Trust-Modells nur für sehr große Unternehmen bezahlbar ist. Wenn man bedenkt, dass Unternehmen wie Google und Coca-Cola zu den bekanntesten Nutzern von Zero Trust in der Industrie gehören, ist es verständlich, dass Unternehmen mit weniger großzügigen Budgets dies befürchten.

Die Realität ist jedoch, dass Zero Trust für Unternehmen nahezu jeder Größe geeignet und erschwinglich ist, von kleinen Startups bis hin zu internationalen Großkonzernen. Und zwar aus diesen Gründen:

1. Es ist kein einmaliges Projekt, sondern eine laufende Entwicklung. Während Unternehmen mit beneidenswerten finanziellen Mitteln und zahlreichen Widersachern es vielleicht rechtfertigen können, mit einer Zero-Trust-Architektur bei Null anzufangen, wäre die überwiegende Mehrheit der Unternehmen besser beraten, einen pragmatischeren, schrittweisen Ansatz zu wählen. Bei einem iterativen Ansatz müssen Unternehmen nicht gleich zu Projektbeginn beträchtliche Ressourcen und Budgets einsetzen, sondern können diese Kosten und Anstrengungen über einen längeren Zeitraum verteilen.
2. Die Implementierung von Zero Trust kann die Sicherheitskosten senken, da sie die betriebliche Effizienz verbessert und die Komplexität reduziert. Laut Forrester „reduziert Zero Trust auch die Ausgaben, indem es die Sicherheitsverwaltung zentralisiert“.[3]

Juniper Connected Security kann Ihnen helfen, Schritt für Schritt eine Zero-Trust-Architektur zu implementieren, die bereits vorhandene Sicherheitsvorkehrungen stärkt und Ihnen und Ihren Sicherheitsteams eine bessere Übersicht über Ihre Umgebung und potenzielle Risiken vermittelt, ohne Sie mit einer „Alarmflut“ zu überwältigen. Die fünf Schritte von Juniper auf dem Weg zu einem sichereren Netzwerk können Ihnen beispielsweise dabei helfen, festzustellen, wo sich Ihr Unternehmen auf dem Weg zu mehr Sicherheit befindet und was noch zu tun ist (siehe Abb. 2).

[3] „The Eight Business and Security Benefits of Zero Trust“, Forrester Research, September 2019

Abbildung 2: Die fünf Schritte zu Juniper Connected Security

Mythos 2: Mikrosegmentierung ist zu kompliziert für die Praxis

Mikrosegmentierung ist ein wirksames Instrument zur Sicherung von Netzwerken im Sinne von Zero Trust. Sie zerlegt monolithische Perimeter in eine Reihe von Mikroperimetern, die granulare Sicherheitskontrollen konzentrieren und Angriffe eindämmen (siehe Abb. 3). Warum setzen sich also nicht mehr Sicherheits- und Netzwerkexperten für diesen Ansatz ein?

Anfangs wurde die Mikrosegmentierung als viel zu zeitaufwendig und komplex empfunden, um für bestehende Anwendungen und Umgebungen praktikabel zu sein. Viele meinten, dass die Implementierung und Pflege von Mikroperimetern angesichts der großen Anzahl von Anwendungen, Anwendungsabhängigkeiten, Diensten und Benutzern einfach nicht machbar sei. Für Unternehmen mit mehreren, nicht miteinander kompatiblen Sicherheits- und Netzwerkprodukten, die keine einheitliche Übersicht über das Netzwerk und die Umgebung bieten konnten, traf das möglicherweise auch zu.

Technologien, die Zero Trust nutzen und robuste Unterstützung für die architektonischen Komponenten eines Zero-Trust-Netzwerks bieten, reduzieren jedoch die Kosten und die Komplexität der Erstellung und Pflege von Mikroperimetern. Dies geschieht durch die Integration von Sicherheitsfunktionen in Geräte, die mit zentralen Sicherheitsrichtlinien verwaltet und kontrolliert werden können.

So bietet Juniper Connected Security beispielsweise alle Funktionen, die für die Unterstützung der wichtigsten Komponenten einer Zero-Trust-Architektur erforderlich sind, die Mikroperimeter ermöglicht:

- **Ein Gateway zur Netzwerksegmentierung**: Das Segmentierungs-Gateway ist der Kern des Netzwerks und integriert traditionell eigenständige Sicherheitsdienste und -geräte in einem Gateway. Juniper Connected Security bietet Segmentierungs-Gateway-Funktionen, die eine Firewall der nächsten Generation, UTM-Dienste (Unified Threat Management) und vollständige, standardbasierte IPsec-Verschlüsselung mit Routing und Switching in einer einzigen, leistungsstarken und kostengünstigen Plattform kombinieren.
- **Parallele, sichere Mikroperimeter**: Eine Switching-Zone, die auf eine Hochgeschwindigkeitsschnittstelle abgebildet wird, schafft ein sicheres Segment, das von Forrester als Microcore und Perimeter (MCAP) bezeichnet wird. MCAPs sind mehrere parallele Mikroperimeter, die zu einer einheitlichen „Segmentation Gateway Fabric“ zusammengefasst werden. Juniper Connected Security bietet eine Microcore-Segmentierung des Netzwerks auf der Grundlage definierter Sicherheitsattribute und ermöglicht Einblicke in die Netzwerkaktivitäten auf Anwendungs-, Benutzer- oder Rollenbasis für eine strenge Zugriffskontrolle über jeden MCAP. Juniper geht noch einen Schritt weiter und dehnt die Sicherheit auf jede Ebene des Netzwerks aus, einschließlich Switches, Router und WLAN-Zugangspunkte. Das verhindert, dass sich Bedrohungen über das gesamte Netzwerk – einschließlich der Switches von Juniper und Drittanbietern – ausbreiten.
- **Zentralisierte Verwaltung**: Für eine effiziente, skalierbare und benutzerfreundliche Verwaltung ermöglicht Juniper Connected Security IT-Teams die transparente Verwaltung aller MCAPs von einem einzigen System aus, das als Backplane für das Netzwerk dient. Sicherheitsteams können eine Reihe von ganzheitlichen Richtlinien verwalten, die die Sicherheit jedes MCAP unabhängig vom Standort aufrechterhalten. Dadurch wird die Anzahl der benötigten Richtlinien und Regeln reduziert und gleichzeitig eine feinere Granularität für einzelne Instanzen des Segmentierungs-Gateways unterstützt.

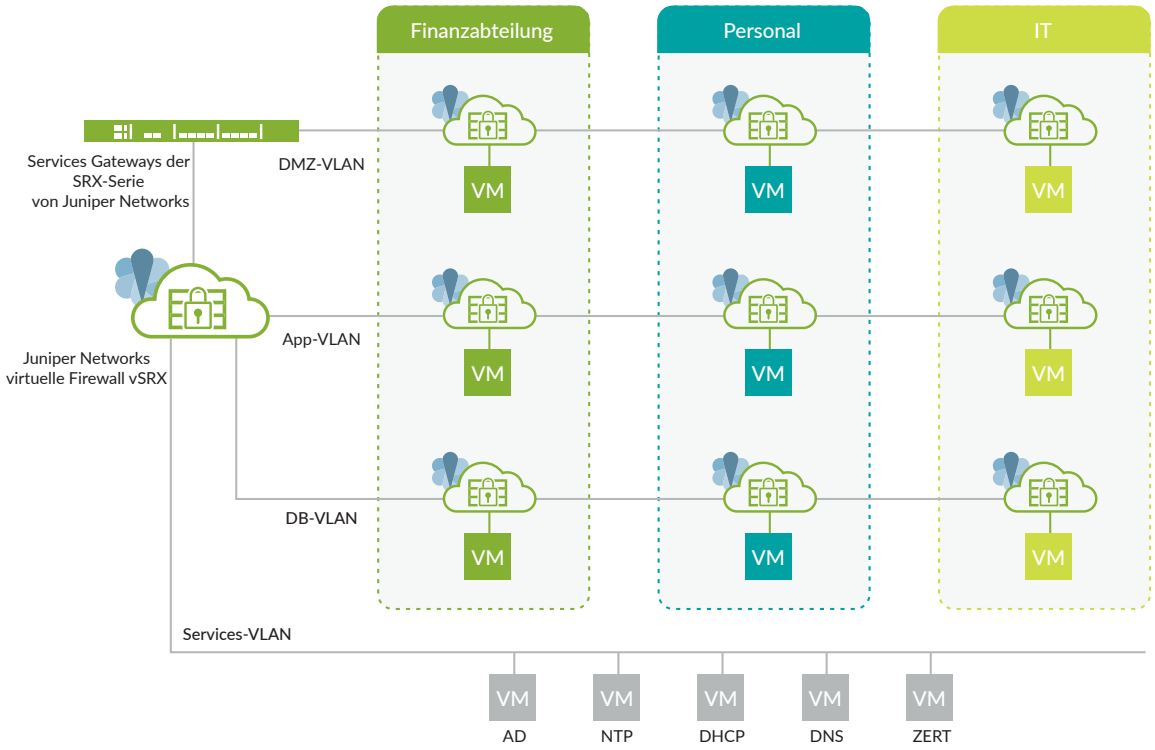

Abbildung 3: Beispiel einer Mikrosegmentierung im Datencenter

Mythos 3: Zero Trust funktioniert nur bei neuen Implementierungen

Eine weitere weit verbreitete Annahme ist, dass Zero Trust nur bei Greenfield-Implementierungen funktioniert. In bestehenden Netzwerken müsste man eigentlich alles ersetzen und mit einer einzigen Plattform neu anfangen.

Das wird zwar mitunter gemacht, ist aber für die meisten Unternehmen viel zu radikal. Glücklicherweise ist es auch gar nicht erforderlich – im Gegenteil, um eine Zero-Trust-Architektur zu erreichen, muss nicht das gesamte Netzwerk ersetzt werden, und schon gar nicht in einem einzigen Kraftakt.

Stattdessen können Unternehmen eine Roadmap für die schrittweise Einführung von Zero Trust erstellen und den Reifegrad damit in ihrem eigenen Tempo erhöhen. Der Schlüssel zur erfolgreichen Umsetzung eines schrittweisen Ansatzes liegt in der Auswahl von Lösungen, die das, was Ihr Unternehmen bereits hat, problemlos unterstützen und integrieren können. So können Sie neue Sicherheitsfunktionen zur Unterstützung von Zero Trust implementieren und gleichzeitig die Sicherheit auf das gesamte Netzwerk ausweiten.

Anstatt zu versuchen, alle Anforderungen aller Unternehmen zu erfüllen, konzentriert sich Juniper auf offene Standards und Produktinteroperabilität. Kein Anbieter kann ein modernes Unternehmensnetzwerk allein absichern. Juniper Connected Security bietet einen konsolidierten Überblick über alle vorhandenen Sicherheitslösungen, sodass alle Sicherheitsinformationen problemlos genutzt, etwaige Probleme zuverlässig erkannt und Bedrohungen abgewehrt werden können, ohne dass die Lösung zu komplex wird.

Mythos 4: Zero Trust ist nur für On-Premises-Umgebungen praktikabel

Da das Hauptargument für Zero Trust darin besteht, dass Unternehmen nicht mehr davon ausgehen können, dass alles in ihren Unternehmensnetzwerken vertrauenswürdig ist, ist es ein weit verbreiteter Mythos, dass Zero Trust nur innerhalb der eigenen Datencenter eines Unternehmens anwendbar ist. Es stimmt zwar, dass Cyberkriminelle die Abwesenheit von Kontrollen innerhalb des Netzwerkperimeters von Unternehmen ausgenutzt haben. Das heißt jedoch nicht, dass sie nur On-Premises-Umgebungen im Visier haben.

Ein weiterer häufig angeführter Grund, die Implementierung von Zero Trust hauptsächlich – oder ausschließlich – auf Unternehmens-Datencenter zu beschränken, ist der Irrglaube, dass der Cloud-Service-Anbieter für die Sicherheit verantwortlich sei. Dies ist einer der gefährlichsten Irrtümer bei der Cloud-Nutzung. Tatsächlich ist das vorherrschende Modell für die Sicherheit in der Cloud das Modell der geteilten Verantwortung, bei dem der Cloud-Service-Anbieter für die Sicherung der Cloud-Infrastruktur und der Kunde für die Sicherung seiner Workloads, Daten und Benutzer verantwortlich ist. Zero Trust ist nicht nur auf die Cloud anwendbar, sondern auch unbedingt erforderlich, um die unternehmenseigenen Assets in Cloud- und Multi-Cloud-Umgebungen zu schützen.

Juniper Connected Security weitet die Sicherheitsrichtlinien und deren Durchsetzung auf die Cloud aus, um neue Service-Bereitstellungsmodelle zu unterstützen und Workloads und Daten vom Endpunkt bis zum Edge und in jeder dazwischenliegenden Cloud zu schützen. So können Unternehmen in Cloud-Umgebungen dasselbe Sicherheitsniveau erreichen wie On-Premises. Mit Juniper können Sie das Zero-Trust-Prinzip auch auf containerisierte Workloads anwenden und die Transparenz und Durchsetzung von Sicherheitsrichtlinien sogar auf die Kommunikation zwischen einzelnen Microservices innerhalb einer Anwendung ausweiten.

Mythos 5: Zero Trust erfordert einen Single-Vendor-Ansatz

Manche Hersteller versuchen, maximal vom Trend hin zu Zero Trust zu profitieren, indem sie potenziellen Kunden einreden, dass das Prinzip nur in homogenen Umgebungen umsetzbar sei und dass sie daher alles bei einem Anbieter kaufen müssten. Angeblich lässt sich nur so sicherstellen, dass alles in einer Zero-Trust-Architektur zusammenpasst.

Die Realität ist, dass kein einziger Anbieter jemals alles anbieten wird, was für ein sicheres Netzwerk innerhalb einer Zero-Trust-Architektur erforderlich ist. Forrester berichtet, dass die Integration von Funktionen aus verschiedenen Sicherheitsbereichen von entscheidender Bedeutung ist: „Benutzerfreundlichkeit und die Steuerung von Ressourcen über verschiedene Datensysteme, Netzwerke und Infrastrukturen hinweg sind für Zero Trust unverzichtbar.“

Aus diesem Grund hat Juniper Connected Security ein globales Partner-Ökosystem aufgebaut, das sich der Bereitstellung und Implementierung von Netzwerken widmet, die auf allen Ebenen der Unternehmen unserer Kunden einen echten Mehrwert bieten. Diese Partnerschaften nutzen erstklassige Lösungen und Branchenkenntnisse, die die eigenen Angebote von Juniper ergänzen und ein breiteres Spektrum an Kundenanforderungen erfüllen.

Einstieg in Zero Trust und Juniper Connected Security

Nachdem wir nun einige der Mythen über Zero-Trust-Architekturen aufgeklärt haben, lassen Sie uns einen Blick darauf werfen, wie Juniper Connected Security Ihr Unternehmen bei der Implementierung von Zero Trust am besten unterstützen kann.

In erster Linie sind wir führend bei sicheren, leistungsstarken Netzwerken. Wir helfen Kunden, die weltweit modernsten Netzwerke aufzubauen. Wir betreiben Netzwerke für die größten Unternehmen der Welt, darunter 97 der Fortune Global 100, die fünf größten sozialen Netzwerke der Welt und mehr als 86 Prozent des Smartphone-Datenverkehrs in den USA.

Dank erheblicher Investitionen in Forschung und Entwicklung gelingen Juniper Networks immer wieder bahnbrechende Innovationen in allen Bereichen der Netzwerktechnologie, von der Siliziumtechnologie über Systeme und Software bis hin zur Sicherheit. Juniper bringt Firewalls der nächsten Generation, Switching, moderne Malware-Abwehr, intelligente Richtlinien und flexible Bereitstellungsmodelle mit Juniper Connected Security zusammen. Damit ist Juniper in der Lage, die Zero-Trust-Anforderungen von Unternehmen auf der ganzen Welt zu erfüllen (siehe Abb. 4).

[4] „The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook“, Forrester Research, Inc., Juli 2019

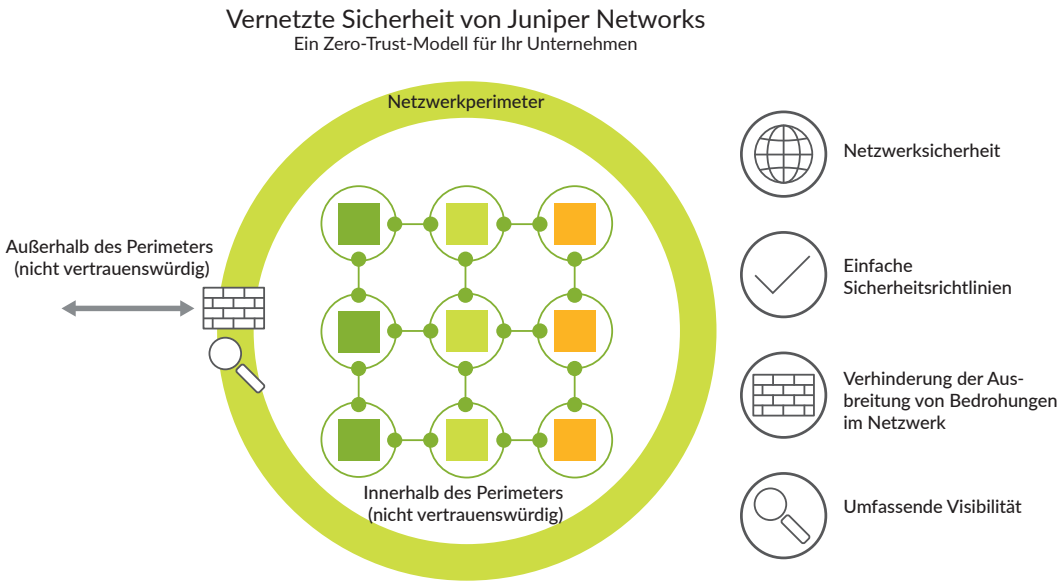

Abbildung 4: Eine Zero-Trust-Architektur mit Juniper Connected Security

Tabelle 1: Juniper Connected Security unterstützt alle Säulen des Zero-Trust-Modells

Säule	Juniper-Funktionen
Daten	• Bietet eine vollständige, standardbasierte IPsec-Verschlüsselung für den sicheren Transport von Geschäftsdaten über Netzwerke • Unterstützt die Einrichtung von Mikroperimetern
Netzwerke	• Ermöglicht es Ihnen, das Netzwerk als ein großes Ganzes zu sehen, zu schützen und zu automatisieren • Erweitert die Sicherheit auf alle Punkte des Netzwerks, auch auf Produkte von Drittanbietern • Unterstützt Mikrosegmentierung mit robusten Segmentierungs-Gateway-Funktionen
Nutzer	• Ermöglicht die Verwaltung und Durchsetzung des Benutzerzugriffs mit einem hohen Maß an granularer Kontrolle • Sichert und schützt Benutzerinteraktionen
Geräte	• Unterstützt auf Benutzerabsichten basierende Richtlinien, damit alle Netzwerkgeräte (Switches, Router, Firewalls und andere Sicherheitsgeräte) die Daten, Ressourcen und, wenn Bedrohungen erkannt werden, Abhilfemaßnahmen innerhalb des Netzwerks gemeinsam nutzen können
Workloads	• Bietet zeitgemäßen Schutz hinter dem Perimeter, in der öffentlichen Cloud und überall dort, wohin moderne Servicebereitstellungsmodelle die Workloads eines Unternehmens verlagern • Ermöglicht granulare Richtlinienkontrolle
Analyse und Visibilität	• Bietet Einblick in den Netzwerkverkehr, einschließlich Benutzer- und Anwendungserkennung • Analysiert Sitzungsinformationen in Echtzeit und sendet Paketaufzeichnungen über einen Span-Port an ein zentrales Repository
Automatisierung und Orchestrierung	• Bietet einheitlichen Schutz durch Automatisierung, maschinelles Lernen und Echtzeit-Bedrohungsdaten • Vereinfacht die Verwaltung mit einer zentralen Plattform für die Erstellung, Anwendung und Weitergabe gemeinsamer Sicherheitsrichtlinien, um die Implementierung neuer Anwendungen und Dienste zu erleichtern

Fazit

Angesichts der aktuellen Bedrohungslage und der Beschaffenheit moderner IT-Umgebungen ist es für Unternehmen und Institutionen aller Größenordnungen an der Zeit, Zero Trust zu einem Grundpfeiler ihrer Informationssicherheitsstrategie zu machen. Wer sich weiterhin nur auf die Stärkung der Sicherheit am Netzwerkrand verlässt, lädt damit zu immer erfolgreicheren und häufigeren Cyberangriffen auf seine Unternehmens- und Cloud-Umgebungen ein.

Mehr über Juniper Connected Security erfahren Sie unter www.juniper.net/de/de/solutions/security/.

Über Juniper Networks

Juniper Networks vereinfacht mit seinen Produkten, Lösungen und Services die Netzwerke, die unsere Welt umspannen. Durch kontinuierliche Innovation überwinden wir die Einschränkungen und die Komplexität, mit der Netzwerkadministratoren in der Cloud-Ära zu kämpfen haben, und unterstützen unsere Kunden und Partner bei der Bewältigung ihrer größten Herausforderungen. Wir bei Juniper Networks sind überzeugt, dass Netzwerke ein Medium für den weltweiten Wissensaustausch und den die Welt verändernden Fortschritt der Menschheit sind. Deshalb haben wir uns das Ziel gesetzt, bahnbrechende Lösungen für automatisierte, skalierbare und sichere Netzwerke zu entwickeln, die mit dem Tempo unserer schnelllebigen Geschäftswelt Schritt halten.

Unternehmens- und Vertriebshauptsitz
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Telefon: +1 888 586 4737
oder +1 408 745 2000
Fax: +1 408 745 2100
www.juniper.net/de/de

Hauptniederlassung für die Regionen APAC und EMEA
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Niederlande
Telefon: +31 0207 125 700
Fax: +31 0207 125 701

JUNIPER NETWORKS | Engineering Simplicity