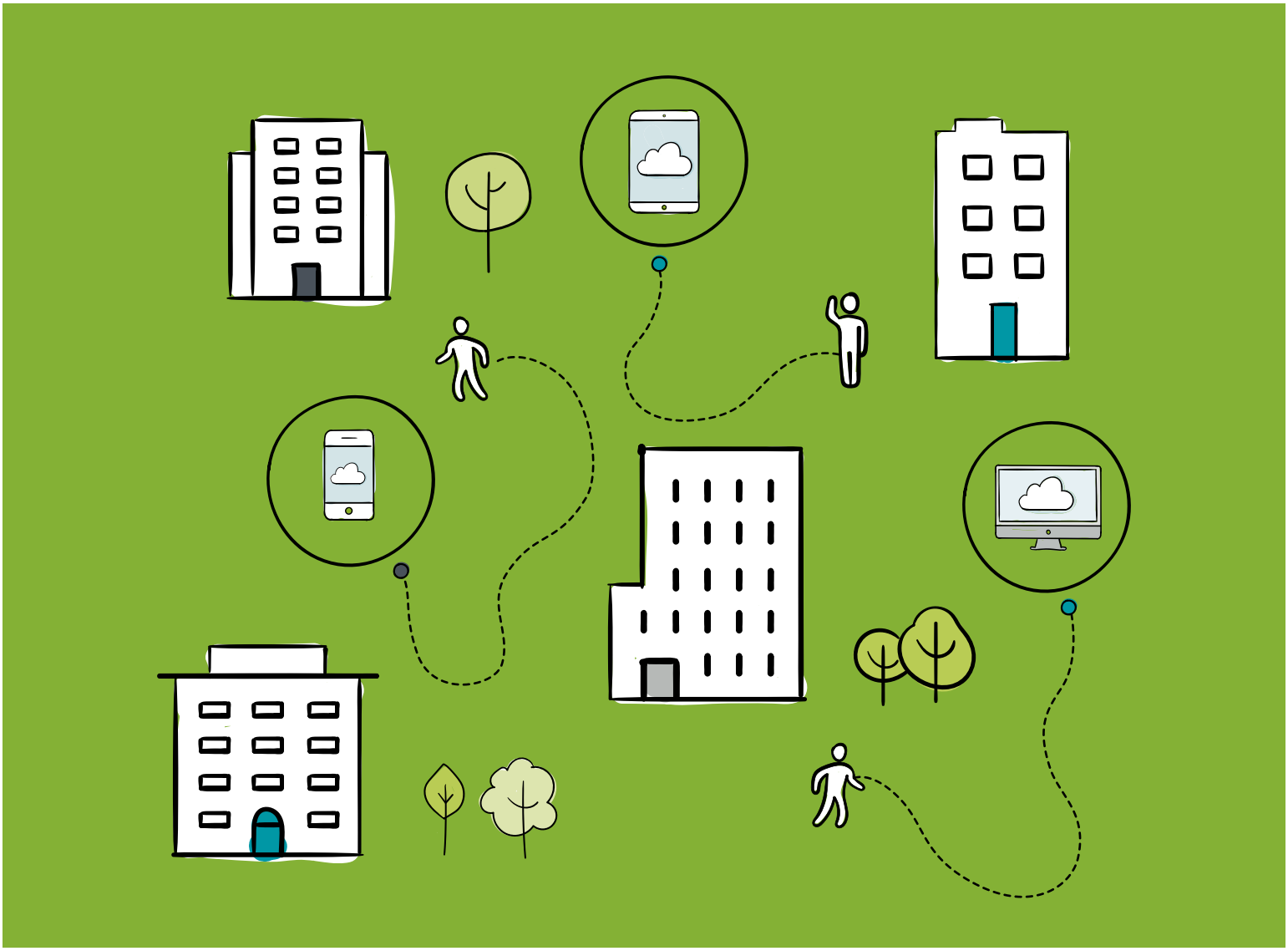
JUNIPER NETWORKS | Engineering Simplicity

E-Guide

Alles, was Sie für den Aufbau eines KI-gestützten Unternehmens benötigen

Ein Leitfaden für Käufer:

So optimieren Sie Ihr kabelgebundenes und kabelloses Netzwerk



März 2020

Inhalt

Einführung **3**

Markttrends bei Campus-Netzwerken **4**
- Die Benutzererfahrung verstehen und definieren 4
- KI für IT 4
- Demokratisierter und dezentraler IT-Betrieb 5
- Der Schritt zu automatisierter Sicherheit 5
- Die Realität der mobilen Revolution 5

Kundenseitige Herausforderungen im Campus-Netzwerk **6**
- Routineaufgaben 6
- Implementierungsphase 6
- Laufender Betrieb (Tagesgeschäft und Monitoring) 6
- Problembehandlung 6

Wichtige Merkmale von Campus-Netzwerken **7**
- Zentralisierte, Cloud-basierte Administration 7
- Modernster Schutz mit Juniper Connected Security 7
- Selbstkonfigurierende Campus-Fabrics 8
- KI-gestützte Tools, Analysefunktionen und Assistenten 8
- Wichtige Merkmale von Campus-Switches 9

Fünf gute Gründe für ein Campus-Netzwerk von Juniper **10**
- 1. KI-gestützte Campus-Netzwerke und mehr 10
- 2. Simplifizierte Betriebsprozesse 10
- 3. Connected Security 11
- 4. Einheitliche Bausteine für mehr Investitionsschutz 11
- 5. Ein übersichtliches Angebot an Campus-Lösungen 12

Warum Juniper Networks **13**

Campus-Netzwerke von Juniper im Überblick **13**
- Multicloud-fähige Campus- und Filialnetzwerke von Juniper 13

Campus-Netzwerke von Juniper im Überblick **14**
- Ethernet-Portfolio der EX-Serie 14

WLAN-Plattform von Mist Systems **15**

Einführung

In KI-gestützten Unternehmen sind Erfahrungen jetzt gleichbedeutend mit Verfügbarkeit. Es geht darum, die Benutzeroberflächen und Daten von Tools zu nutzen und dadurch weniger abhängig von manuellen Eingriffen zu sein, denn in der Zukunft wird es immer mehr um den IT-Betrieb gehen. Und ein sehr wichtiger Teil dieser Zukunft ist das Campus-Netzwerk.

Die Campus-Lösungen von Juniper Networks vereinfachen den Betriebsalltag – von der Konfiguration und Bereitstellung bis hin zur Überwachung und Kontrolle des Netzwerks. Damit sind Sie auf dem richtigen Weg zu einer sicheren, automatisierten Multicloud-Architektur.

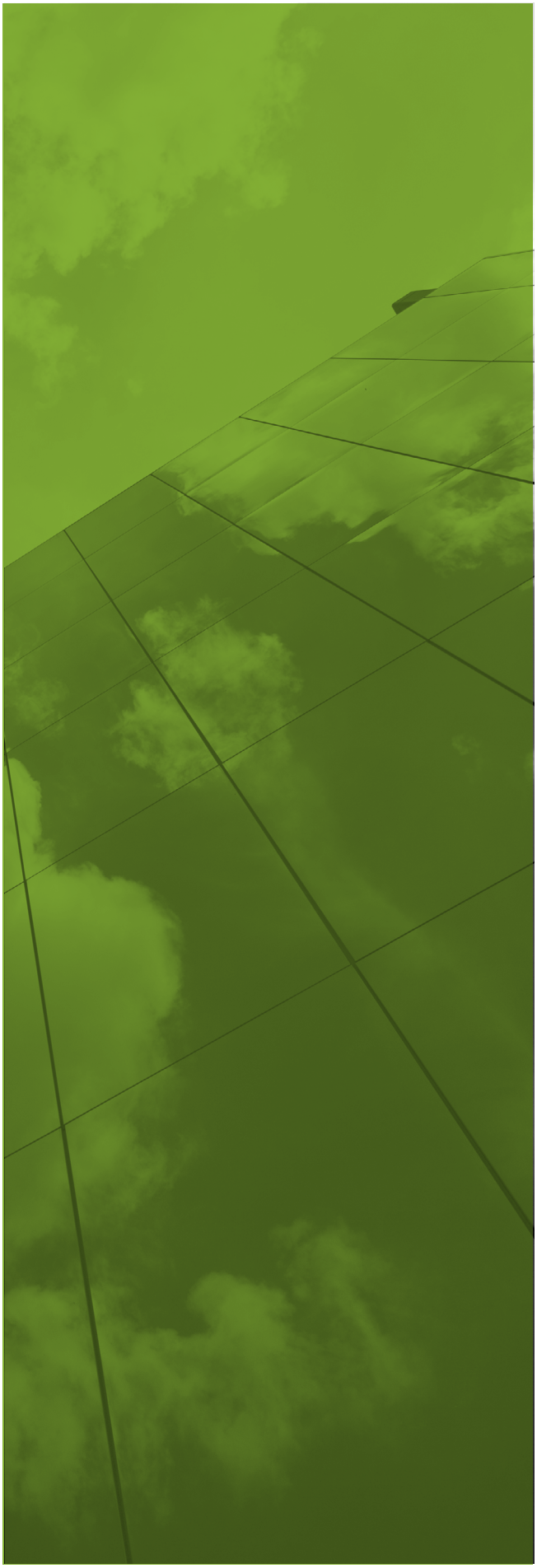
Das Team Juniper Networks und Mist Systems wurde 2019 sowohl im Report „Critical Capabilities for Wired and Wireless LAN Access Infrastructure“ (Wichtige Kriterien für LAN- und WLAN-Infrastrukturen) als auch im Gartner Magic Quadrant „Wired and Wireless LAN Infrastructure 2019“ anerkannt (und dort als „Visionary“ eingestuft). Wir sehen das als Aufforderung an Unternehmen auf der ganzen Welt, Juniper und Mist Systems als Anbieter für sämtliche Belange in Sachen LAN- und WLAN-Zugriff zu erwägen. In allen 6 von 6 Anwendungsfällen waren wir unter den besten drei Bewertungen und wurden außerdem im Magic Quadrant als Visionär eingestuft.

Doch überzeugen Sie sich selbst und lesen Sie die Berichte für Magic Quadrant und Critical Capabilities, um mehr zu erfahren.

Die Umgestaltung und Erweiterung Ihres Netzwerks ist eine gute Gelegenheit, Ihr Unternehmen fit für die Zukunft zu machen.

Gartner Magic Quadrant „Wired and Wireless LAN Access Infrastructure“, Bill Menezes, Christian Canales, Tim Zimmerman, Mike Toussaint, 24. September 2019.

Gartner „Critical Capabilities for Wired and Wireless LAN Access Infrastructure“, Christian Canales, Tim Zimmerman, Bill Menezes, Mike Toussaint, 26. September 2019.



Markttrends bei Campus-Netzwerken

Die Benutzererfahrung verstehen und definieren

Für eine positive Benutzererfahrung zu sorgen, ist ein entscheidender Bestandteil der Produktivität, Effizienz und Zusammenarbeit in Campus-Netzwerken. Der digitale Zugang der Benutzer zu Services in einem Campus-Netzwerk beginnt am Edge-Gerät und unterliegt vielen unsichtbaren und doch entscheidenden Abhängigkeiten. Früher leitete sich die Benutzererfahrung aus einfachen Monitoring-Funktionen und der Verfügbarkeit ab. Diese gelten inzwischen jedoch als Grundvoraussetzung – die Erfahrungsqualität gemäß gestiegener Service-Level-Erwartungen (SLEs) hat neue Maßstäbe gesetzt. Um diese Erwartungen zu erfüllen, müssen Netzwerktechniker von reaktiver zu proaktiver Fehlerbehebung übergehen. Auch der Wechsel von reaktiven zu proaktiven Betriebsabläufen ist in vollem Gange. Diese Veränderung kommt durch KI zustande, die Teams die Einhaltung ihrer Serviceversprechen ermöglicht.

Eine neue Art der KI für IT kann überall im Campus-Netzwerk Ereignisse beobachten, aus ihnen lernen und sie anschließend anhand der Merkmale des jeweiligen Netzwerks zueinander in Beziehung setzen. Dadurch können sinnvolle SLEs festgelegt, eingehalten und in vielen Fällen übertroffen werden. Telemetriedaten aus kabelgebundenen und kabellosen Netzwerken werden pausenlos gestreamt und eingespeist, um bessere Einblicke in die Erfahrung der Endbenutzer zu gewinnen, die Reparaturzeiten (Mean Time To Repair, MTTR) zu verkürzen und Fehlkonfigurationen zu erkennen und zu beheben, bevor die Benutzer überhaupt ein Problem bemerken.

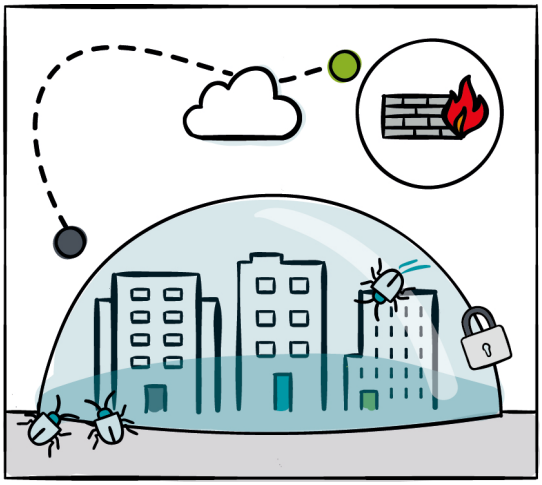
Benutzer von Campus-Netzwerken erwarten unabhängig vom Anwendungs- und Gerätetyp jederzeit sichere, flüssige und zuverlässige Konnektivität. KI-gestützte Unternehmen sichern mit proaktiver Anomalieerkennung, autonomer Mängelbehebung und einer KI-Engine kabelgebundene und kabellose Netzwerke ab und helfen bei der Senkung der IT-Kosten.

KI für IT

Der Weg zu KI für IT beginnt mit dem Campus-Netzwerk. Manuelle, sich wiederholende Tätigkeiten haben oft keinen bleibenden Wert. Sie gelten als indirekte Kosten und nehmen oft proportional zum IT-Aufwand zu. Der IT-Betrieb leidet chronisch unter Beispielen für mühsame Fehlerbehebung, oft in Form von manuellen Arbeitsschritten, die in Betriebsanleitungen und Standardverfahren (Standard Operating Procedures, SOP) beschrieben werden. Solche mühevollen Tätigkeiten führen zu Burnout und sind schlecht für die Moral. Wenn diese Tätigkeiten durch KI und Automatisierung reduziert werden, können sich die Menschen mit interessanteren kundenbezogenen und technischen Problemen beschäftigen, zum Beispiel mit Innovationen und kreativen Problemlösungen.

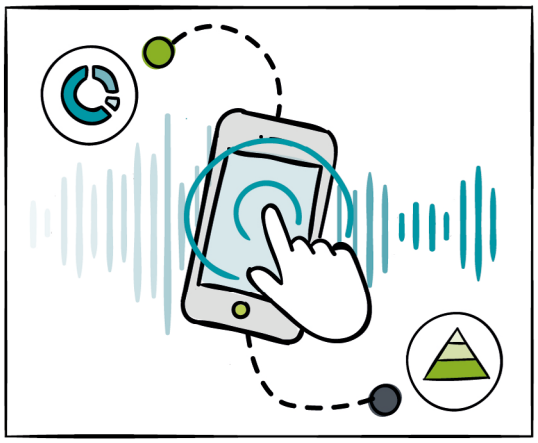
Leistungsstarke IT-Teams nutzen technisch hochentwickelte Plattformen und intelligente Tools zur Skalierung und Vervielfachung ihrer Effektivität. Je weniger Zeit sie zur Aufrechterhaltung des Betriebs benötigen, desto mehr Zeit, Energie und Motivation bleibt ihnen für zukunftsorientierte und strategische Überlegungen.

Demokratisierter und dezentraler IT-Betrieb



Es ist erstaunlich schwer, mit der technologischen Entwicklung Schritt zu halten – nicht nur für Experten, sondern auch für gewöhnliche IT-Teams. Durch die Nutzung von KI-Technologien können sich Teams aus allen Bereichen leichter mit dem Netzwerkstatus vertraut machen, indem sie Fragen in natürlicher Sprache stellen. Derartige Systeme bringen permanent Problemursachen ans Tageslicht und leiten entsprechende Korrekturmaßnahmen ein.

Diese Fähigkeit zur Erkennung und schnellen Behebung von Fehlern beschleunigt die Servicewiederherstellung und stärkt das gegenseitige Vertrauen der Teams. Darüber hinaus können KI-gestützte Plattformen Datenpakete aus von Problemen betroffenen Geräten proaktiv und automatisch erfassen, sodass die Supportmitarbeiter nicht vor Ort tätig werden bzw. anwesend sein müssen.

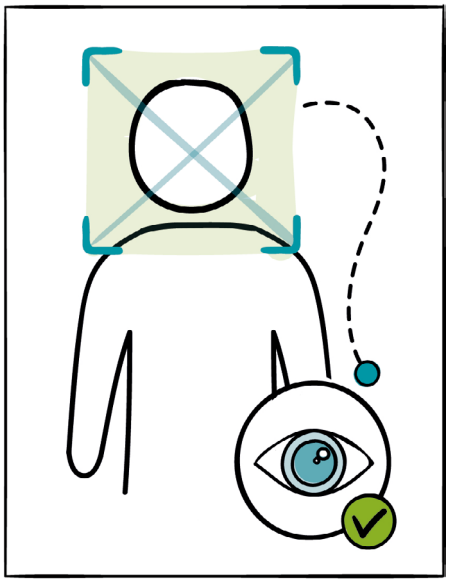


Der Schritt zu automatisierter Sicherheit

Die Absicherung von Campus-Netzwerken und den eingebundenen IT-Ressourcen gewinnt zunehmend an Bedeutung. Netzwerke werden immer umfassender und komplexer und mit dieser stetig wachsenden Angriffsfläche (aufgrund von Cloud-Services, mobilen Lösungen und IoT-Geräten) steigt auch die Anzahl böswilliger Eindringversuche.

Sich einfach hinter einer Firewall an der Netzwerkgrenze zu verstecken, war schon vor Jahren kein umfassendes Sicherheitskonzept. Doch heutzutage kann wirklich kein Unternehmen mehr so tun, als würde es ausreichen, Firewalls einzurichten und Logdateien zu analysieren. Moderne Abwehrstrategien basieren auf ATP-Technologie (Advanced Threat Protection), dem Austausch von Bedrohungsdaten in Echtzeit und KI-basierten Lösungen für eine automatisierte Problembehebung.

Die Realität der mobilen Revolution



Mobile Anwendungen auf WLAN-Basis in Kombination mit standortbasierten Echtzeitdaten treiben die Nutzung mobiler Technologien und die ständige Nachfrage nach höherem WLAN-Durchsatz voran.

Die rasant steigende Anzahl von IoT- und Mobilgeräten macht umfassende Upgrades der WLAN-Campus-Netzwerke erforderlich. Beispielsweise mussten Infrastrukturen in der Vergangenheit von 802.11n auf 802.11ac umgestellt werden und nun steht der Wechsel zum neuesten Standard bevor – 802.11ax (auch Wi-Fi 6 genannt).

Durch das Upgrade einer Netzwerkkomponente werden oft weitere Veränderungen angestoßen, zum Beispiel die Modernisierung von Uplinks (von Gigabit-Ethernet auf Multigigabit-Ethernet) und die Einführung des neuen Standards 802.3bz mit Datenraten von 2,5 bzw. 5 Gbit/s. Auch PoE-Verbindungen (Power over Ethernet) müssen mithalten können, schließlich haben moderne WLAN-Access Points einen deutlich höheren Strombedarf. Kaum haben wir also von 802.3af (15,4 W) auf 802.3at (25,5 W) umgestellt, steht schon 802.3bt (mit mehr als 30 W) vor der Tür.

Kundenseitige Herausforderungen im Campus-Netzwerk

Routineaufgaben

Mit dem Wachstum eines Unternehmens ändern sich die Anforderungen und der Umfang der Routineaufgaben. Gekoppelt mit der steigenden Anzahl an Workloads pro Administrator nimmt der Druck auf die IT enorm zu.

Damit moderne Unternehmen in Sachen Flexibilität nicht hinter dem Wettbewerb zurückbleiben, müssen sich IT-Mitarbeiter mit innovativen Technologien wie dem Internet der Dinge und künstlicher Intelligenz auseinandersetzen, was oft zu folgendem Dilemma führt: Wo finden Teams die Zeit für innovative Projekte, wenn sie ständig mit Routineaufgaben beschäftigt sind?

Im Großen und Ganzen lässt sich der Alltagsbetrieb in drei Kategorien unterteilen:

1) **Implementierungsphase:** Installieren neuer Geräte, Hinzufügen von Anwendungen und Services sowie Einrichten neuer Standorte.
2) **Laufender Betrieb (Tagesgeschäft und Monitoring):** Überwachen des Netzwerkstatus und Konfigurieren des Netzwerks auf der Basis von Richtlinienänderungen und ähnlichen Vorgaben.
3) **Problembehandlung** Wiederherstellung bei ungeplanten Ausfällen, Behebung von Leistungsdefiziten im Netzwerk und Unterstützung bei Sicherheitsverletzungen.

Beispiele für gängige Herausforderungen in der Implementierungsphase:

- Fehlendes Know-how im Unternehmen in Bezug auf die Installation, Fehlerbehebung und Konfiguration neuer Ausrüstung
- Schwierigkeiten bei der Ermittlung neu installierter Geräte und ihrer Einbeziehung in das Administrationsgefüge
- Probleme bei der Anwendung von Sicherheitsstandards auf neue Benutzer/Geräte in allen Infrastrukturen der unternehmensspezifischen Multicloud

Laufender Betrieb (Tagesgeschäft und Monitoring):

- Inkonsistente und fehleranfällige Anwendung von Richtlinien, da diese in zunehmend komplexen Gefügen über mehrere Infrastrukturen hinweg verwaltet werden müssen
- Veraltete und patchbedürftige Betriebssysteme, Anwendungen und Geräte, wobei Netzwerkequipment wie Switches und Router oft den größten Rückstand aufweist
- ACL-Konflikte (Access Control Lists): „ACLs können zur Plage werden ... Man wird sie einfach nicht mehr los.“

Problembehandlung:

- Mühsam und zeitaufwendig
- Isolierte Datenquellen: Die Suche nach einer Ursache erstreckt sich auf Logdateien verschiedenster Quellen.
- Informationsüberlastung: Unmengen bedeutungsloser Meldungen
- Veraltete, fehleranfällige Geräte

Je weniger Routineaufgaben IT-Teams übernehmen müssen, desto mehr Zeit haben Mitarbeiter für Innovationen. Und nur so kann ein Unternehmen flexibel und wettbewerbsfähig bleiben.

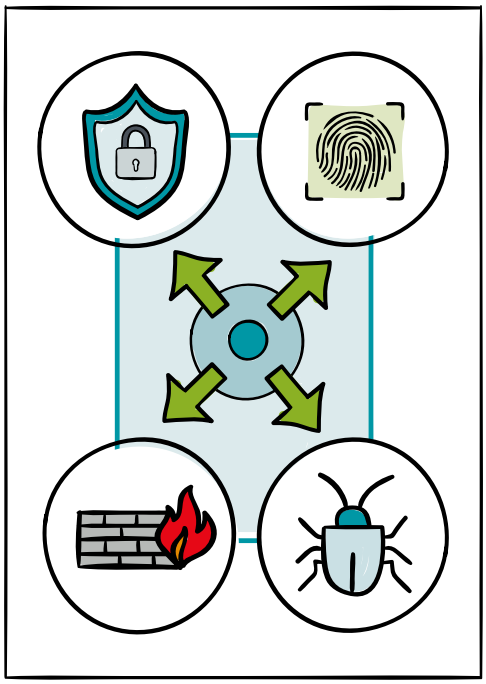
Wichtige Überlegungen zu Campus-Netzwerken

Zentralisierte, Cloud-basierte Administration

In einem zentralisierten Verwaltungsgefüge lassen sich manuelle Routineaufgaben reduzieren oder sogar ganz abschaffen.

Unabhängig davon, ob es sich um Campus-Netzwerke an mehreren Standorten, externe Remote-Netze oder eine Kombination dieser Szenarien handelt – Unternehmen, die eine professionell abgesicherte, Cloud-basierte Managementlösung verwenden, befreien sich vom täglichen Verwaltungsaufwand und der Notwendigkeit interner Spezialisten.

Eine vollständig automatisierte Bereitstellung von Netzwerkgeräten ermöglicht die ortsunabhängige Remote-Einrichtung neuer Standorte über einen Browser.



Modernster Schutz mit Juniper Connected Security

Herkömmliche Sicherheitsmaßnahmen sind der Flut neuer Bedrohungen einfach nicht gewachsen. Um moderne Netzwerke effektiv zu schützen und sicherzustellen, dass Richtlinien netzwerkweit durchgesetzt werden, benötigen Unternehmen umfassende Transparenz und zahlreiche Sicherheitspunkte im gesamten Netzwerk. Wichtig sind auch ATP-Funktionen (Advanced Threat Protection), damit neu erfasste Bedrohungsdaten zuverlässig an alle mit dem Netzwerk verbundenen Systeme und Geräte weitergegeben werden.

Sämtliche Dateien, Daten und auch Bedrohungen werden über das Netzwerk übertragen. Daher ist es sinnvoll, das gesamte Netzwerk in die Sicherheitslösung eines Unternehmens einzubinden.

Ausgereifte, automatisierte Sicherheitslösungen machen es möglich, Daten von mehreren Punkten im Netzwerk zu erfassen und Richtlinien auf Access-Switches und alle anderen Netzwerkgeräte anzuwenden. ACLs und andere Funktionen für die Netzwerkkonfiguration werden damit auf allen Netzwerkebenen automatisch durchgesetzt.

Moderne Netzwerke umfassen eine bunte Mischung aus Produkten und Services verschiedener Anbieter und erstrecken sich häufig über mehrere Infrastrukturen. So entsteht schließlich eine komplexe Multicloud-Umgebung. Dementsprechend werden auch diverse Sicherheitsprodukte genutzt, die meist von mehr als einem Anbieter stammen und im Einklang miteinander funktionieren müssen.

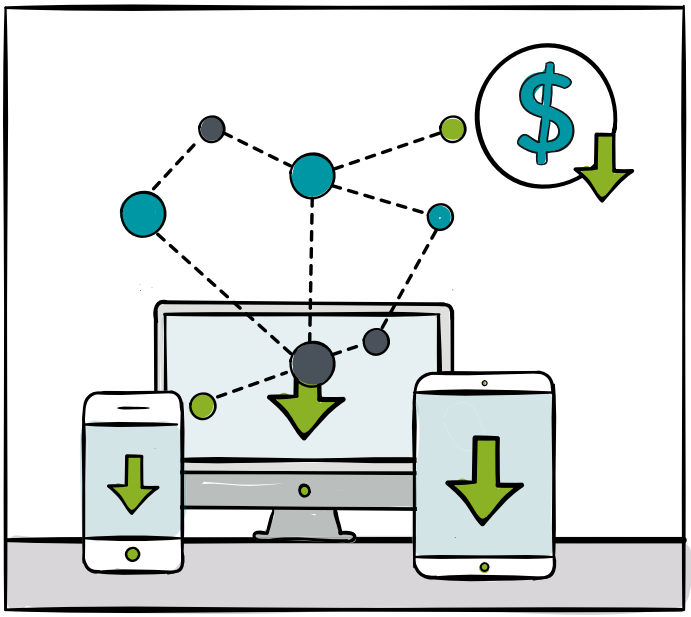
Unternehmen müssen in der Lage sein, Bedrohungen frühzeitig zu erkennen und Richtlinien einheitlich anzuwenden. Dabei darf es keine Rolle spielen, wo sich Workloads oder Daten innerhalb der Infrastruktur befinden.

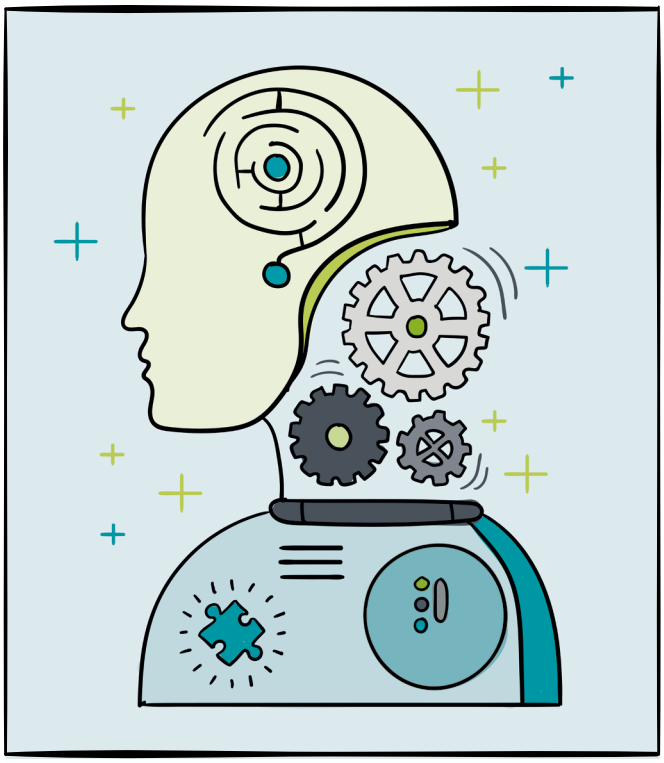
Selbstkonfigurierende Campus-Fabrics

Selbstkonfigurierende Campus-Fabrics machen interne Abläufe effizienter, vereinfachen den IT-Betrieb und helfen, die Anzahl der verwalteten Geräte in der Switching-Infrastruktur zu reduzieren. Damit sinken die Ausgaben für Routineaufgaben – mit potentiell sehr positiven Folgen für Ihre Betriebskosten.

Moderne Fabric-Technologien sind ein guter Weg, um Netzwerkebenen auf ein Minimum zu reduzieren und die Verwendung des durchsatzintensiven Spanning Tree-Protokolls (STP) zu vermeiden. Sie vereinfachen die Bereitstellung durch anwenderfreundliche Plug-and-Play-Lösungen, mindern die Zahl der Ausfälle, die durch Installationsprobleme verursacht werden, und vereinheitlichen die Implementierungsphase.

Netzwerk-Fabrics profitieren von einer offenen, standardbasierten Automatisierungs- und Administrationsarchitektur und ermöglichen den Betrieb über ein zentrales Network Operations Center (NOC). Durch die Verwendung standardisierter Open-Source-Technologien vermeiden Sie nicht nur einen kostenintensiven Austausch der vorhandenen IT-Infrastruktur, sondern können auch eine zentrale Sicherheitsstrategie im gesamten Netzwerk anwenden – vom Campus-Netz bis zur Multicloud-Umgebung.





KI-gestützte Tools, Analysefunktionen und Assistenten

In Campus-Netzwerken werden immer mehr Daten generiert, was unter anderem daran liegt, dass Mitarbeiter in zunehmendem Maß eigene Geräte im Unternehmen verwenden (und zwar nicht nur Smartphones, PCs, Macbooks usw.). Egal ob es sich dabei um persönliche Wearables oder IoT-Geräte für die geschäftliche Nutzung handelt – eins steht fest: Diese wachsende Anzahl an mit dem Netzwerk verbundenen Tools und Anwendungen erhöht die Vielfalt und Komplexität in Ihrer Unternehmensumgebung. Wie sich diese Geräte mit dem Netzwerk verbinden (ob über LAN oder WLAN), spielt letztendlich keine Rolle. Entscheidend ist, dass sie das Netzwerk schwerer berechenbar und komplexer machen.

KI-gestützte Tools und Verfahren können helfen, diese neue Umgebung besser zu verstehen. Auch Drittanbieter-Tools und -Assistenten können eine große Hilfe sein, wenn sie so eingebunden werden, dass sie die Berge von Netzwerkdaten sinnvoll erfassen, strukturieren und verarbeiten. Darauf aufbauend lassen sich Maßnahmen und Entscheidungsprozesse automatisieren und Netzwerkabläufe steuern. Mit KI-Tools und KI-Assistenten ist es relativ einfach, die Nutzererfahrung im Campus-Netzwerk erheblich zu verbessern.

Wichtige Merkmale von Campus-Netzwerken

KI-gestützter Betrieb: Wenn die Benutzererfahrung die Verfügbarkeit als wichtigste Kennzahl ablöst, wird die Rolle des Campus-Netzwerks immer wichtiger. Die Veränderungen in Richtung autonomes Netzwerk machen Daten nutzbar, mit denen KI und Automatisierung schnell und wirksam Anomalien zu Tage fördern und ihre Ursachen herausfinden. Aber mehr noch: Heutzutage möchten wir für das beste Nutzererlebnis, dass komplexe Systeme natürliche Sprache verstehen und keine seltsamen Befehle erwarten, wenn wir einfache Fragen stellen, wie z. B. „Wo sind die unzufriedenen Kunden im Büro“ oder „Wie geht es AP ap-1“.

Power over Ethernet (PoE): PoE-Technologie ist bereits seit mehreren Jahrzehnten im Einsatz und im Laufe der Zeit haben sich verschiedene Versionen herauskristallisiert, die jeweils Leistungsanforderungen zwischen 15 und 100 W (mit dem neuen PoE++-Standard) unterstützen.

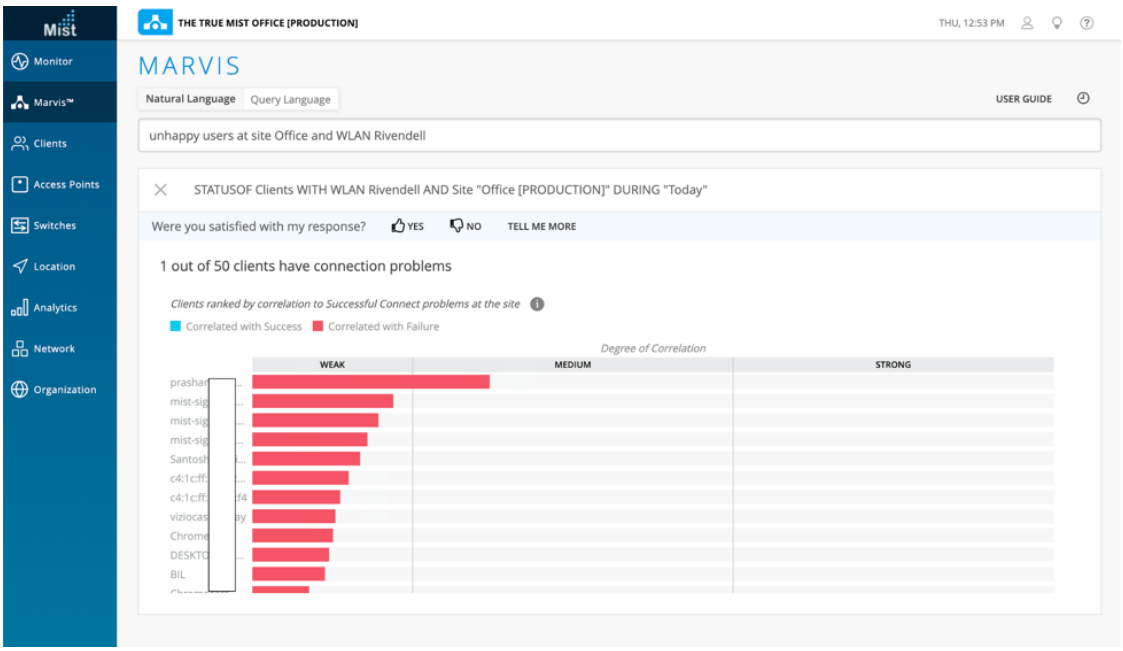
Bei Verwendung von PoE werden oft nur halb so viele Kabel benötigt, was die Verdrahtung eines Campus-Netzwerks deutlich vereinfacht. Die Auswahl der geeigneten Access-Switching-Lösung für Ihr Netzwerk hängt von den Anwendungen und Geräten im Unternehmen, der erforderlichen Anzahl an PoE-Ports, Ihrem Budget und der Leistung pro PoE-Port ab.

Multigigabit-Ethernet: Die Umstellung von einem herkömmlichen 802.11n-WLAN-Netzwerk auf den innovativen WLAN-6-Standard erfordert einen höheren Durchsatz. Eine Geschwindigkeit von 1 GbE reicht nicht mehr aus. Und eine Multigigabit-Ethernet-Umgebung kann diesen höheren Durchsatz bei Access Points unterstützen, ohne dass eine neue Verkabelung erforderlich ist.

Moderne Campus-Switches unterstützen 1GbE- und 2,5GbE-Ports, häufig mit einer Portleistung von 1 GbE, 2,5 GbE, 5 GbE und 10 GbE. Wenn in Ihrem Unternehmen das nächste Netzwerkupgrade ansteht, lohnt sich daher die Investition in Multigigabit-Ethernet-Komponenten.

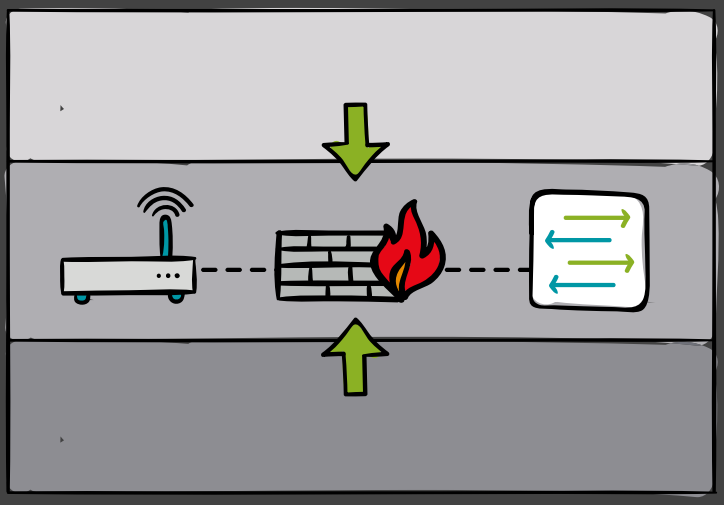
MACsec: Viele Regierungsbehörden schreiben bereits die Nutzung von MACsec-Verschlüsselung zwischen Access-Switches und den Geräten im Campus-Netzwerk vor. Viele andere Industriezweige übernehmen diese zusätzliche Sicherheitsstufe ebenfalls, um sich vor Datendiebstahl durch Hacker zu schützen. Moderne Access-, Aggregation- und Core-Switches bieten MACsec-Verschlüsselung für den Schutz von kupfer- und glasfaserbasierten Leitungen mit Geschwindigkeiten bis zu 10GbE (oder sogar darüber hinaus).

Kompakte, lüfterlose Zugangsgeräte: Innovative integrierte Schalttechnik ermöglicht Unternehmen nun die Verwendung lüfter- und geräuschloser Switches in Campus-Netzwerken. Sie eignen sich für jede Umgebung, die ein niedriges Geräuschniveau erfordert, wie Großraumbüros, Unterrichtsräume oder Hotelzimmer. Dank dem vorwiegend kompakten Design und den flexiblen Montagemöglichkeiten sind lüfter- und geräuschlose Switches vielfältig einsetzbar. Die Nutzung dieser Switches ermöglicht Unternehmen, mehr Geräte in das Netzwerk zu integrieren und jede Einheit mit komplett automatisierbaren und optimal absicherbaren Zugangsports auszustatten.



Fünf gute Gründe
für ein Campus-Netzwerk von Juniper

1 KI-gestützte Campus-Netzwerke und mehr



Die von Mist Systems entwickelte KI-gestützte Plattform ist eine leistungsfähige LAN- und WLAN-Lösung, die KI, maschinelles Lernen und Data Sciences effektiv kombiniert und in einer auf Microservices basierenden Cloud-Architektur bereitstellt. Mit dieser flexiblen Lösung können Sie die Nutzererfahrung Ihrer Kunden optimieren, gewinnen aussagekräftige Einblicke in Ihr Netzwerk und können den Netzwerkbetrieb automatisieren.

Die Plattform von Mist Systems bietet eine Reihe neuer Services, wie die Überwachung der WLAN-Dienste, den virtuellen Netzwerkassistenten Marvis und Bluetooth LE für die Interaktion mit Nutzern und die Lokalisierung von Ressourcen.

Mist Assurance bindet alle kabellosen und kabelgebundenen Lösungen ein und gibt Ihnen einen umfassenden Überblick über die Nutzererfahrung und den Betrieb in allen Netzwerkumgebungen Ihres Unternehmens.

2 Simplifizierte Betriebsprozesse

Die Ausführung derselben Administrations- und Konfigurationsaufgaben auf jedem einzelnen Switch kann sehr aufwendig sein. Juniper vereinfacht das Switch-Management durch die Unterstützung verschiedener Fabric-Architekturen, die den spezifischen Skalierungsanforderungen unterschiedlicher Unternehmen gerecht werden.

Mit Virtual Chassis und standardisierten Technologien wie z. B. MC-LAG und EVPN-VXLAN können mehrere Switches von Juniper zu einem einzigen logischen Gerät zusammengefasst werden. Dadurch reduziert Juniper die Netzwerkkomplexität und die Betriebskosten.

Contrail Service Orchestration (CSO) sorgt für eine zentralisierte, Cloud-basierte Verwaltung des IT-Betriebs für Ihr softwaredefiniertes LAN, WAN und WLAN. Dank der automatisierten Bereitstellung haben Sie Ihr Netzwerk in kürzester Zeit eingerichtet. CSO unterstützt alle Geräte von Juniper, einschließlich Ethernet-Switches der EX-Serie, Next-Generation-Firewalls der SRX-Serie sowie Virtual-Services-Produkte der NFX-Serie. Sogar eine transparente WAN- und LAN-Vereinheitlichung für den kabelgebundenen und kabellosen Betrieb ist möglich.

3 Connected Security

Juniper Connected Security bietet einen zuverlässigen Rundumschutz für Ihr Netzwerk, sodass Sie alle Bereiche und Funktionsebenen Ihrer Multicloud-Infrastruktur sehen, automatisieren und absichern können. Hinzu kommen die tiefgreifende Netzwerksicherheit und zahlreiche Sicherheitspunkte im gesamten Netzwerk.

Dabei kombiniert unsere Lösung Advanced Threat Protection, integriertes Identitätsmanagement, nutzerbasierte Regeln für Next-Generation Firewalls und hochmoderne Analysen mit einer dynamischen, automatisierten Durchsetzung von Sicherheitsrichtlinien. An der Absicherung des Netzwerks sind alle Komponenten beteiligt, auch die Switches der EX-Serie.

Connected Security schützt nicht nur die Netzwerkperipherie, sondern bezieht auch die Netzwerksegmentierung mit ein und nutzt die gesamte Netzwerkinfrastruktur zur Durchsetzung der Sicherheitsrichtlinien.

Eine einfache und geradlinige Funktion von Connected Security ist zum Beispiel MACsec. Dabei handelt es sich um ein Verschlüsselungsverfahren zur Abwehr von Angriffen, bei denen Hacker versuchen, zwischen zwei Netzwerkknoten übertragene Daten abzuhören oder abzufangen. Ob Access-, Core- oder Aggregation-Switches – alle Ethernet-Produkte der EX-Serie unterstützen das MACsec-Protokoll, damit Sie sicher sein können, dass Ihre Daten in jeder Übertragungsphase im Netzwerk gut geschützt sind.

4 Einheitliche Bausteine für mehr Investitionsschutz

Angesichts der steigenden Nachfrage nach Durchsatz und Kapazität sehen sich die meisten Unternehmen gezwungen, ihr Campus-Netzwerk auszubauen. Die Virtual Chassis-Technologie von Juniper ermöglicht eine Erweiterung auf bis zu 10 Switches und die Option, verschiedene Switches der EX-Serie mit 1GbE-, 10GbE-, 40GbE- und 100GbE-Verbindungen beliebig miteinander zu kombinieren, ist die ideale Grundlage für ein reibungsloses Upgrade.

Noch mehr Skalierbarkeit erhalten Sie mit der Fabric-Architektur von EVPN-VXLAN. Mit dieser Technologie können Sie so viele Core-, Aggregations- und Access-Geräte wie nötig hinzufügen, ohne das Netzwerk umzugestalten oder ein kostspieliges Upgrade der Software und Hardware durchzuführen.

5 Ein übersichtliches Angebot an Campus-Lösungen

Ob Access-, Core- oder Aggregation-Switches: Juniper bietet eine übersichtliche und programmierbare Auswahl für jede Art von Campus-Netzwerk. Unsere Access Points der Enterprise-Klasse unterstützen WLAN-, Bluetooth LE- und IoT-Technologien und wir haben Modelle für den Innen- sowie für den Außenbereich im Angebot. Die Multigigabit- und PoE++-Technologien der Access-Switches unterstützen die jeweils aktuellen WLAN-Standards und eignen sich selbst für leistungsintensivste IoT-Geräte. Mit der hohen Verfügbarkeit unserer fest konfigurierten und modularen Core- und Aggregation-Produkte mit 10, 40 oder 100 GbE lassen sich Campus-Netzwerke jeder Größenordnung realisieren. Auch die Funktionsvielfalt unserer WAN-Edge-Geräte ist beträchtlich: Firewalls der nächsten Generation, sicheres Routing, SD-WAN und ein robuster, vielfach bewährter Routing-Stack.

> **„Übertreffen Sie die Erwartungen der Benutzer. Junos und Mist Systems erfüllen garantiert die Service-Level-Erwartungen (SLEs).“**

Warum Juniper Networks?

Juniper Networks bietet sichere, automatisierte Campus-Netzwerke. Unsere Router, Switches und Firewalls nutzen eine Kombination aus handelsüblicher und anwenderspezifischer Hardware und bieten ein breites Leistungs- und Preisspektrum.

All unsere Campus- und Sicherheitslösungen basieren auf dem Junos®-Betriebssystem von Juniper Networks und einem einheitlichen Automatisierungs-Framework mit Programmierschnittstellen und Echtzeit-Telemetriedaten, das die Integration in gängige Verwaltungstools ermöglicht.

Die kombinierte Lösung von Juniper und Mist Systems sorgt durch eine dehnbare und einfache Architektur mit dezentraler Intelligenz in den kabelgebundenen und kabellosen Netzwerken für mehr Leistung, Sicherheit und Zuverlässigkeit und dadurch letztlich für einen besseren Benutzerkomfort.

Campus-Netzwerke von Juniper im Überblick

Multicloud-fähige Campus- und Filialnetzwerke von Juniper

	EINSTEIGERMODELLE	MITTELKLASSE	PREMIUMKLASSE
EDGE	 SRX/NFX-Serie	 SRX-Serie	 MX-Serie
Core/ Aggregation	 EX4600/4650	 EX9250	 EX9200
ACCESS	 EX2300	 EX3400	 EX4300


Juniper Sky Enterprise

Campus-Netzwerke von Juniper im Überblick

Ethernet-Switches der EX-Serie

Access-, Aggregation- und Core-LAN-Switches

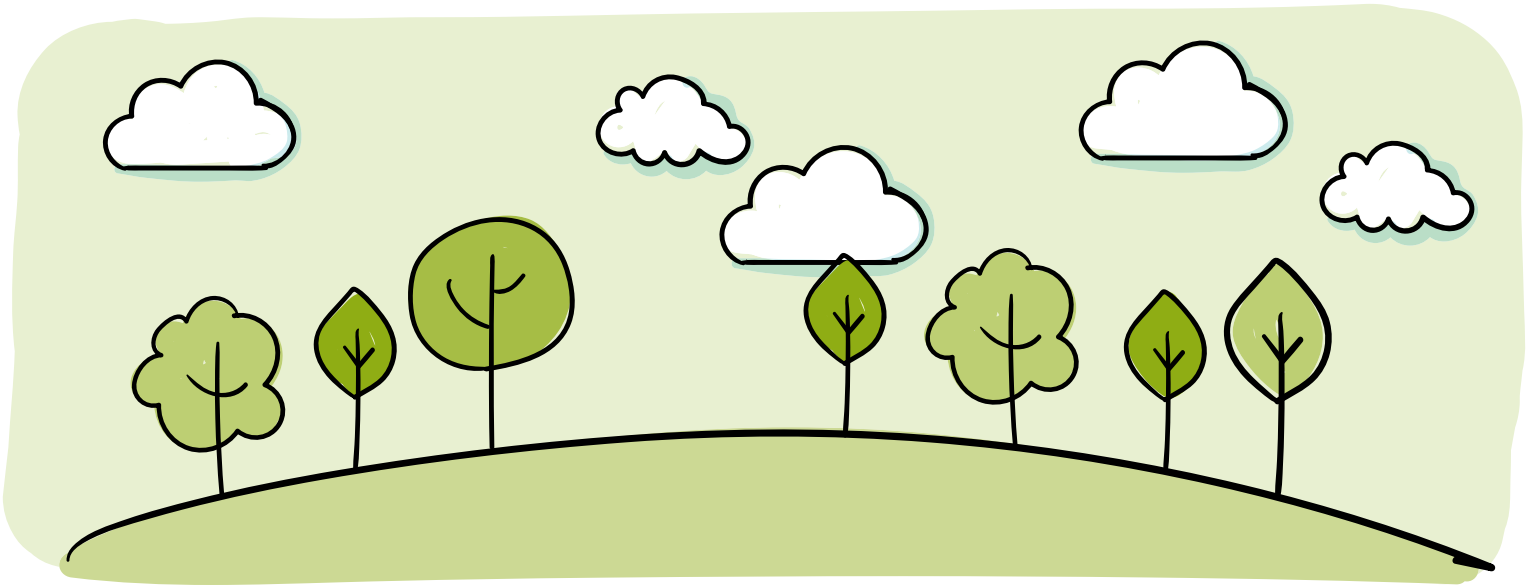




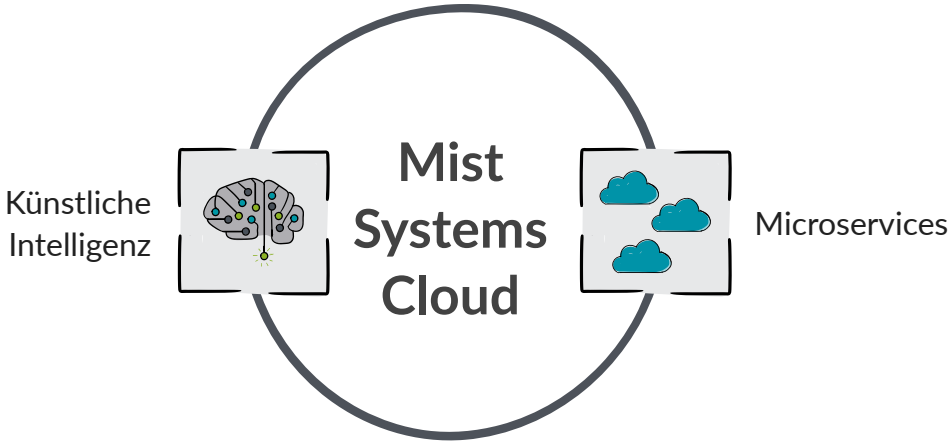


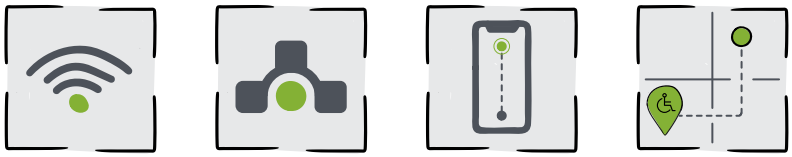


EX2300-C/EX2300	EX2300 Multigigabit	EX3400	EX4300	EX4300 Multigigabit	EX4600	EX4650	EX9200	EX9250
Access-Switches	Multigig-Access	Access-Switches	Access & Aggregation	Multigig-Access & Aggregation	Aggregation	Core & Aggregation	Core & Aggregation	Compact Core & Aggregation
12-24-28 x GE 2-4 x 10GE SFP+		24-48 x GE 4 x 10GE SFP+ 2 x 40GE QSFP+	24-48 x GE 4 x 10GE 4 x 40GE QSFP+		72 x 10 GE SFP+ 12 x 40 GE QSFP+	48 x 10 GbE 8 x 100 GbE	bis zu 320 x 10 GE bis zu 60 x 40GE bis zu 20 x 100GE	bis zu 144 x 10GE bis zu 36 x 40GE bis zu 24 x 100GE
PoE/PoE+	PoE/PoE+	PoE/PoE+	PoE/PoE+	PoE/PoE+/PoE++	k. A.	k. A.	k. A.	k. A.
VC-fähig (Virtual Chassis)					VC und MC-LAG	MC-LAG und EVPN-VXLAN	MC-LAG	

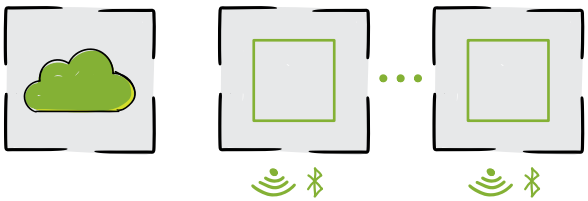


WLAN-Plattform von Mist Systems





Services auf Abonnementbasis



Mist Edge Access Points

AP43: WLAN (802.11ax), Bluetooth® LE und IoT für unschlagbare Leistung

AP61: WLAN und Bluetooth® für den Außenbereich

AP41: WLAN (802.11ac), Bluetooth® LE und IoT für unschlagbare Leistung

AP21: WLAN (802.11ac) und Bluetooth® LE für unschlagbare Leistung

BT11: Bluetooth® LE der Enterprise-Klasse

Melden Sie sich zu einem „Toolkit Thursdays“-Webinar an und erleben Sie eine Live-Demo von Mist Wired Assurance.

Jetzt auf juniper.net/wired-assurance-tuesdays anmelden

Hauptsitz

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

Hauptniederlassung für die Regionen APAC und EMEA

Juniper Networks International B.V.

Boeing Avenue 240
119 PZ Schiphol-Rijk
Amsterdam, Niederlande

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

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

PN 7400100-004-DE

Wichtiger Hinweis:

Dieses Dokument enthält allgemeine Informationen über rechtliche Angelegenheiten.
Diese Informationen sind keine Empfehlungen und sollten nicht als solche aufgefasst werden.

Alle rechtlichen Hinweise in diesem Dokument werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Zusicherungen oder Garantien bereitgestellt. Juniper Networks lehnt alle Zusicherungen oder Garantien in Bezug auf die Angaben in diesem Dokument ab.

Die Angaben in diesem Dokument können nicht die rechtliche Beratung durch Ihren Anwalt oder andere Anbieter professioneller Rechtsdienstleistungen ersetzen. Keinesfalls sollten Sie aufgrund der Angaben in diesem Dokument eine Rechtsberatung hinauszögern, rechtliche Empfehlungen Ihres Anwalts oder anderer professioneller Rechtsdienstleister missachten oder rechtliche Maßnahmen einleiten oder unterbrechen.

Die Angaben in diesem Dokument waren zum Zeitpunkt der Veröffentlichung (März 2020) korrekt.

JUNIPER NETWORKS | Engineering Simplicity