

# **Was ist schon sicher... und was hat KI damit zu tun?**

Oliver Loke

2026-06-24

# Agenda

|                      |                                                                             |
|----------------------|-----------------------------------------------------------------------------|
| <b>10:15 – 11:15</b> | HPE Networking: Was ist schon sicher .. Und was hat KI damit zu tun?        |
| <b>11:15 – 12:00</b> | Exclusive Networks: Fortinet SASE in der Praxis                             |
| <b>12:00 – 13:00</b> | Mittagspause                                                                |
| <b>13:00 – 13:30</b> | Arctic Wolf: Trend, Neuerungen und Ausblick                                 |
| <b>13:30 – 14:30</b> | Theben x Arctic Wolf x Borgware: Warum unsere Kunden auf Arctic Wolf setzen |
| <b>14:30 – 14:45</b> | Kaffeepause                                                                 |
| <b>14:45 – 15:45</b> | HPE & Borgware: Was HPE Morpheus VM Essentials wirklich kann                |
| <b>15:45 – 16:00</b> | Q&A, Verlosung und Verabschiedung                                           |
| <b>16:00 – 17:00</b> | Führung durch die MOTORWORLD                                                |
| <b>Ab 17:30</b>      | Abendessen                                                                  |



# Ebenen der Security im Netzwerk

## Physische Ebene

... die erste Verteidigungslinie der Netzwerksicherheit.

**Zutrittskontrollen**

**Überwachungssysteme (CCTV)**

**Hardware-Abschließbarkeit**

**Portsperrren**

**Umweltkontrollen**

## Technische Ebene

... zielt darauf ab, unbefugten Zugriff zu verhindern und die Integrität sowie Verfügbarkeit der Systeme zu sichern.

**Zugriffskontrolle (Network Access Control – NAC)**

**Firewalls und Next-Generation-Firewalls (NGFW)**

**Intrusion Detection und Prevention Systems (IDS/IPS)**

**Segmentierung und VLANs**

**Verschlüsselung und Authentifizierung**

## Administrative Ebene

..Ein ganzheitlicher Ansatz schützt Daten, Infrastruktur und Identitäten vor Cyberangriffen und gewährleistet die Einhaltung regulatorischer Vorgaben

**Identity and Access Management (IAM) & Zero Trust**

**Next-Generation Firewalls (NGFW) & Intrusion Prevention Systems (IPS)**

**Autom.Schwachstellen-Scanner**

**Netzwerksegmentierung & Mikrosegmentierung**

**Regelmäßige Backups**

# Der Hauptstandort



Router

Firewall  
SIEM  
IDS/IPS



**DMZ**

Firewall

Back-Up/Restore

NAC (+AD + Zertifikate)

Segmentierung/ Micro-Segmentierung

Viren-Scanner

Interne Komponenten Sicherheit

Physikalische Zugriffsabsicherung

**Campus**



Firewall



NAC (+AD + Zertifikate)

Segmentierung/ Micro-Segmentierung

Viren-Scanner

Interne Komponenten Sicherheit

Physikalische Zugangskontrollen

Ev. Videoüberwachung



**Rechenzentrum**



# **Wie hilft HPE-Networking grundsätzlich?**

# Hewlett Packard Enterprise

## Die Edge-to-Cloud Firma

**One HPE:**  
**Zusammen**  
**einfach**  
**noch**  
**besser**



Erweiterbar | Offen | durch Partner getrieben

# HPE Networking führt das „Campus & Branch Feld“ an



**HPE Networking**

Gartner, Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure, Mike Leibovitz, Christian Canales, Nauman Raja, Tim Zimmerman, 25 June 2025.  
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.  
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.  
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Juniper Networks.

***Damit gilt:  
Im Netzwerk einfach starten  
und zukunftssicher wachsen mit***

# **HPE Networking**

**HPE** **aruba**  
networking

+

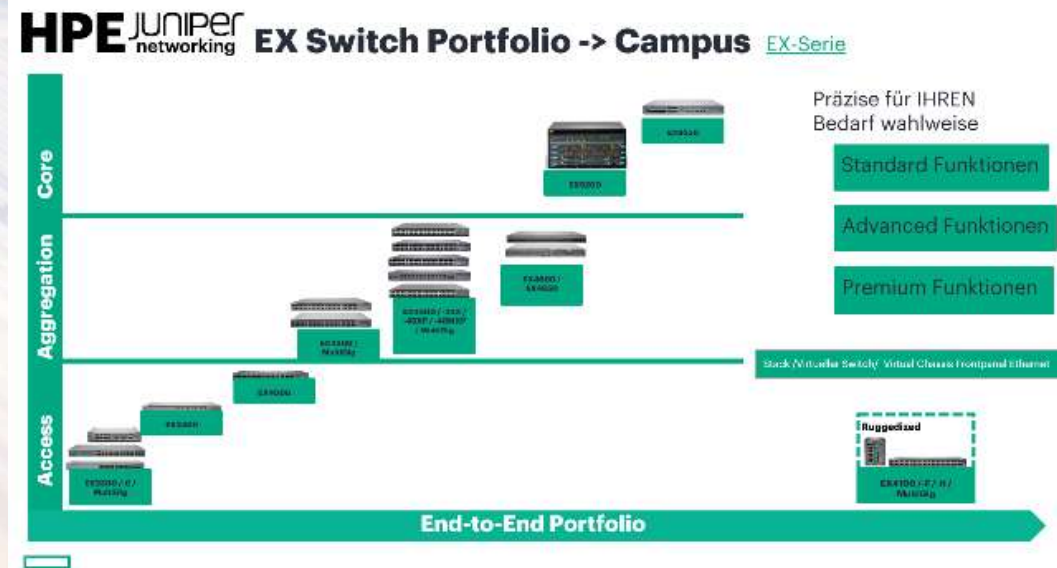
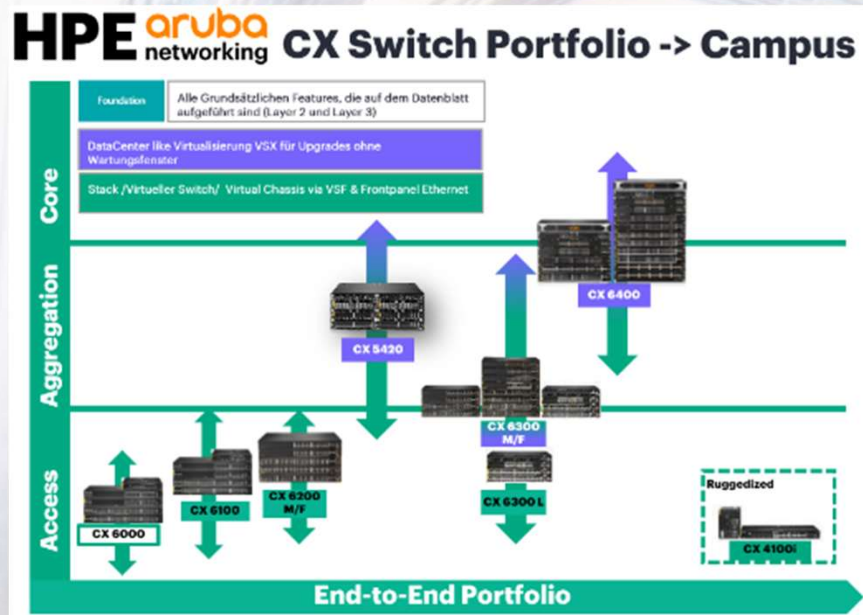
**HPE** **juniper**  
networking





# **LAN / WLAN für alle Belange**

10/10/2016



# Campus WLAN

**HPE aruba networking WLAN Portfolio**

Management: **Central**

Alle APs sind Wi-Fi Alliance CERTIFIED

| Indoor                                                            |                            |                                   | Outdoor & Hazardous Locations                                                                |                 |
|-------------------------------------------------------------------|----------------------------|-----------------------------------|----------------------------------------------------------------------------------------------|-----------------|
| <b>Campus</b><br>720 Serie<br>730 Serie<br>740 Serie<br>750 Serie | <b>Hospitality</b><br>723H | <b>Remote Access opt.</b><br>605R | 760 Serie<br><br>670 Serie & 670 EX Serie*                                                   | <b>Wi-Fi 7</b>  |
| 610 Serie<br>630 Serie<br>650 Serie                               | 605H                       |                                   | 670 Serie & 670 EX Serie*                                                                    | <b>Wi-Fi 6E</b> |
| 500 Serie<br>510 Serie<br>530 Serie<br>550 Serie                  | 500H Serie                 | 503R                              | 516 Serie*<br>560 Serie*<br>570 Serie*<br>580EX Serie*<br>570EX Serie*<br>580 & 580EX Serie* | <b>Wi-Fi 6</b>  |

\*AT&T Speed Certified against temperature, productivity, and speed.

**HPE juniper networking Wireless Portfolio**

Management: **Mist**

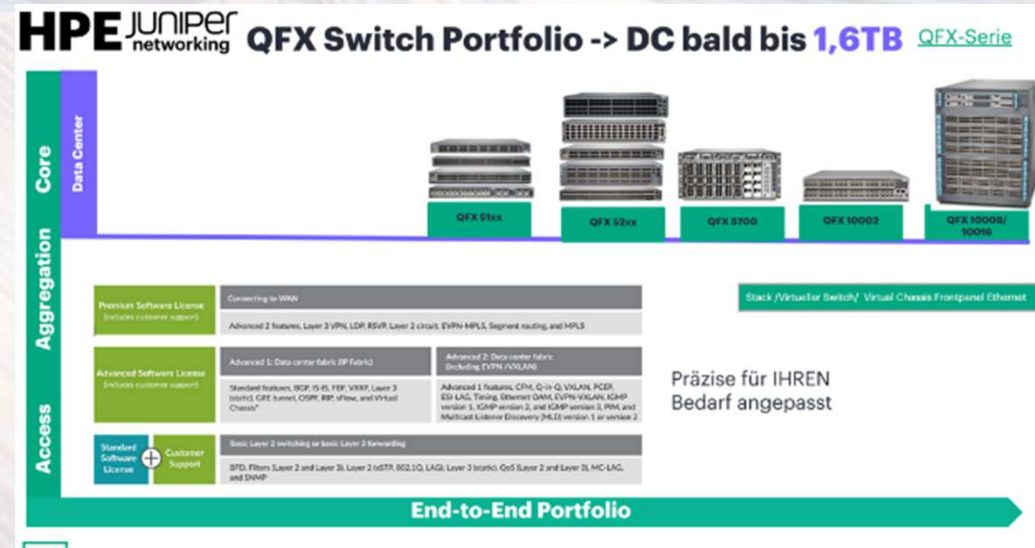
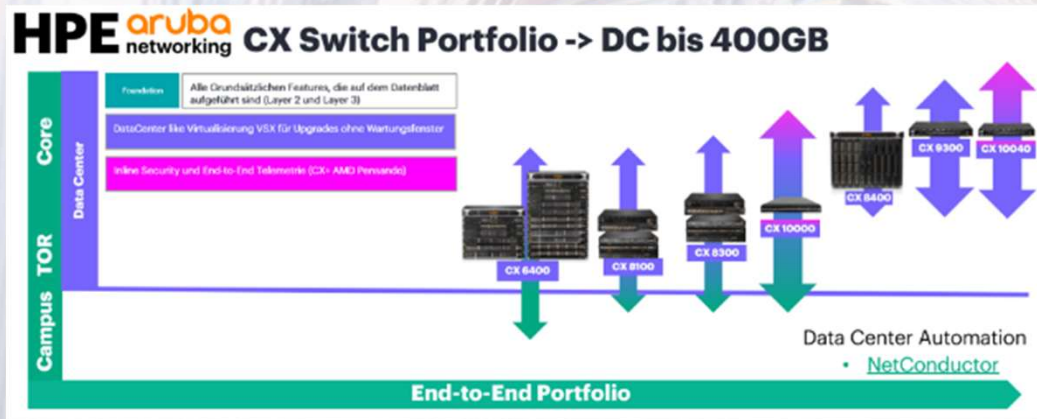
Wi-Fi 6 / 6E    Wi-Fi 7

| Indoor                                                      | Outdoor        |
|-------------------------------------------------------------|----------------|
| <b>Wi-Fi 7</b><br>AP-36<br>AP-37<br>AP-47<br>723H           | AP-66          |
| <b>Wi-Fi 6E</b><br>AP-24                                    | AP-64          |
| <b>Wi-Fi 6</b><br>AP-32<br>AP-33<br>AP-34<br>AP-43<br>AP-44 | AP-12<br>AP-63 |

**Services**

- Wireless Assurance (Wi-Fi)
- Marvis AI
- Asset Visibility (Indoor Location)

# Rechenzentrum





# **Wie hilft HPE Networking im Speziellen?**



# **Sicherheit durch KI (im Mgmt)**

# KI-basiertes Netzwerk Management

Ein gemeinsames Konzept

**HPE** **aruba** networking **Central**

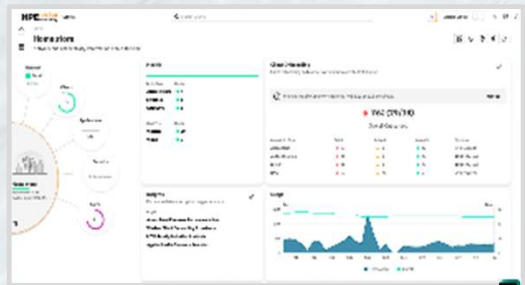
**HPE** **JUNIPER** networking **Mist**

## AGENTEN BASIERTE KI

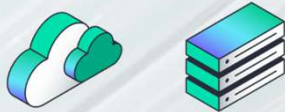
Autonome Funktionen werden im Rekordtempo hinzugefügt

## MICROSERVICES

Gemeinsamer Code und gemeinsame technische Ressourcen, die für beide Lösungen genutzt werden



Marvis



**Self-Driving  
Netzwerk**

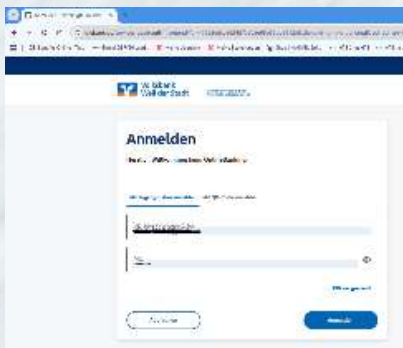


Marvis



# KI-basiert im Netzwerk Management mehr sehen

## Auffällige Zugriffe



## Auffällige Up-/Downloads



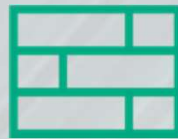
## Kommunikation mit ungewollten Lokationen (Ländern)





# **Sicherheit im ersten Kontakt (WAN Router)**

# Nur einige Beispiele für Security in den WAN-Routern



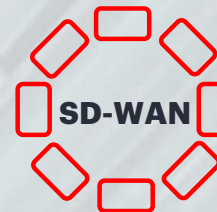
**Stateful Firewall  
& Next-Generation-  
Funktionen**



**Intrusion Detection und  
Prevention (IDP)**



**Security Intelligence  
(SecIntel)**



**SD-WAN  
& Zero-Trust-Netzwerke**



**Content- und Web-  
Filtering**



**Integrierte  
Verschlüsselung**



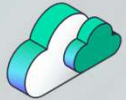
**Port-  
Sicherheit**

# HPE JUNIPER networking WAN Router Portfolio

ACX Router

MX Router

PTX Router



Management: Paragon Automation (Routing Director)

WAN Automation

Edge Routing Assurance

Routing Director

Paragon Active Assurance

Paragon Planner

Paragon Insights

Paragon Pathfinder



**PTX Router**

Hohe Datenmengen  
(Juniper ASIC)



**MX Router**

Geringe Latenz  
(Juniper ASIC)



**ACX Router**

Ausgewogen  
(Broadcom ASIC)





# **Sicherheit zwischen den Bereichen (Firewalls)**

# Führend in den letzten Jahren

Unabhängig validierte Sicherheitswirksamkeit

**HPE** JUNIPER  
networking

## NetSecOPEN

2022

**99.8%**

Wirksamkeit gegen Exploits

## Cyber Ratings

2023 Next-Gen Firewall - **AAA Rating**

**99.9%**

Gegen client- und serverseitige  
Exploits

## Cyber Ratings

2024 Cloud Network Firewall

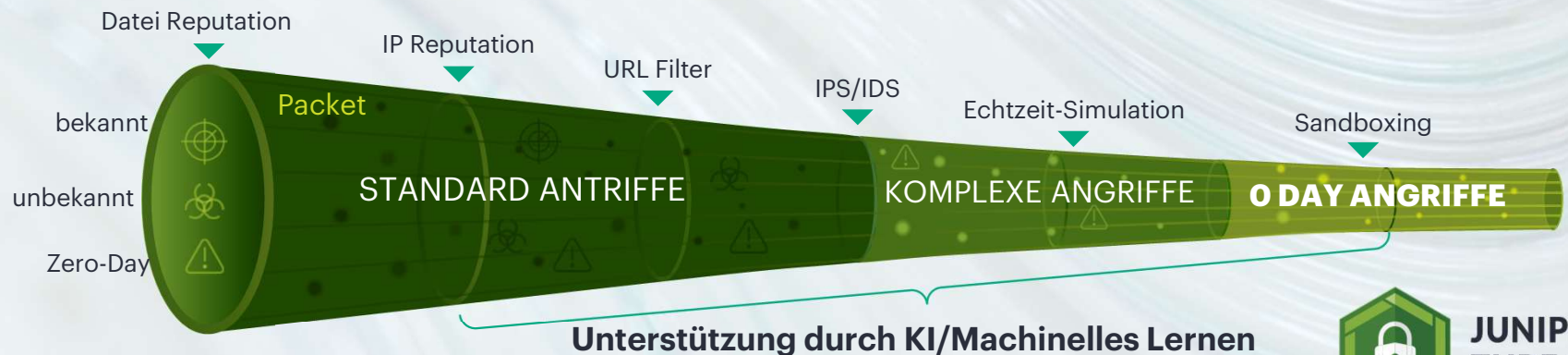
**99.7%**

Exploit Blockrate

**0**

Falsch-positive  
Ergebnisse

## SECURITY SOFTWARE SERVICES



**JUNIPER  
THREAT LABS**

# HPE Juniper Networking – SRX-Serie

**HPE** JUNIPER  
networking

## Branch



SRX300



SRX320



SRX340



SRX345



SRX380

## Campus & Scale-Out RZ/Cloud/SP



SRX1500



SRX4100



SRX4200



SRX4600



SRX1600



SRX2300 (SRX4120)



SRX4300



SRX4700

## Scale-Up RZ/Cloud/SP



SRX5600



SRX5400



SRX5800

## Verwaltung



SD Cloud



Security Director



Mist Cloud

## Cloud Firewalls



vSRX



cSRX



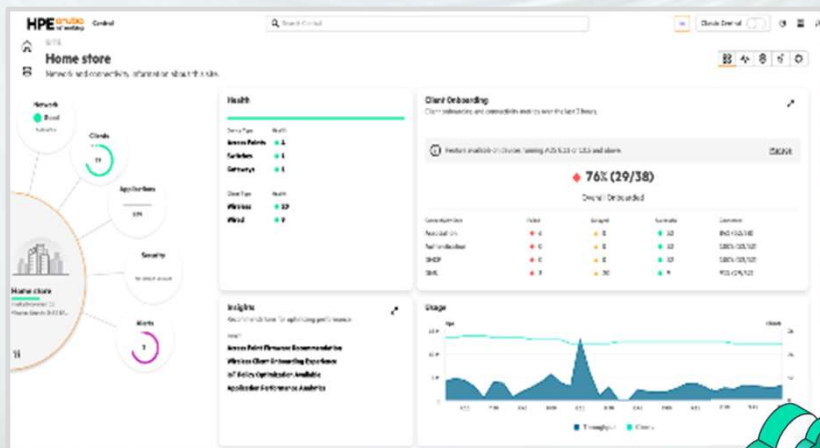
Secure Edge



# **Sicherheit durch NAC (Netzwerk Zugangs Kontrolle)**

# NAC geht via Cloud Management

**HPE** **aruba** networking **Central**



**HPE** **JUNIPER** networking **Mist**



# ... oder doch lieber NAC+ on Prem?

## CLEARPASS Policy MGR



Gäste  
(inkl.)

### Extensions



#### Onboard

- IOT/ BYOD onboarding



#### OnGuard

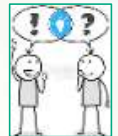
- PC Device Manager



Profiling  
(inkl.)



On Connect  
(inkl.)



Exchange  
(inkl.)

**Cloud basierte  
Erweiterung für  
KI gestütztes Profiling  
auch in 3rd Party  
Netzwerken verfügbar  
(bei Central Management  
inklusive)**



Clearpass  
Device Insight

# HPE aruba networking Clearpass als Sicherheits-Schaltzentrale\*

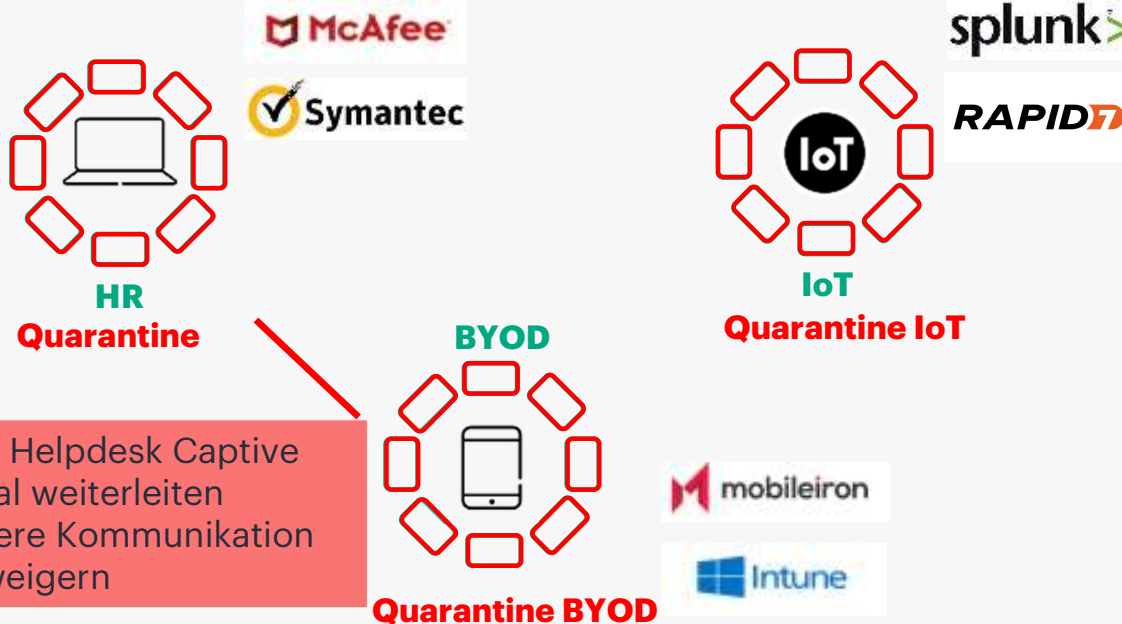


\*Funktionalitätsumfang ist je Hersteller unterschiedlich und zu prüfen

# HPE aruba networking Zero Trust (LAN/WLAN) Security mit Clearpass

Integration mit 3rd Party

## Netzwerk



- Rollen werden abhängig zu sicherheitsrelevanten Events von 3<sup>rd</sup> Party Komponenten automatisch angepasst
- Firewalls können damit einen Angriff stoppen – nicht nur abwehren!!

Interaktion und Umsetzung von allen Ebenen der Sicherheitstechnologie auf die aktive Netzwerkhardware



# **Verteilte Sicherheit Services [RZ] (Distributed Services Switch)**

# Hohe Komplexität und Kosten veralteter Netzwerk- und Sicherheitsarchitekturen überwinden

## Eine völlig neue Switch Kategorie Distributed Services Switch

**CX 10040**  
100/400G



**CX 10000**,  
10/25G  
Available since  
2022



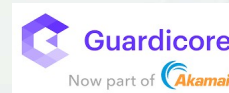
Integrierte DPUs



**L2/3, Distributed Firewall, VPN, Telemetry,  
skalierbares NAT**

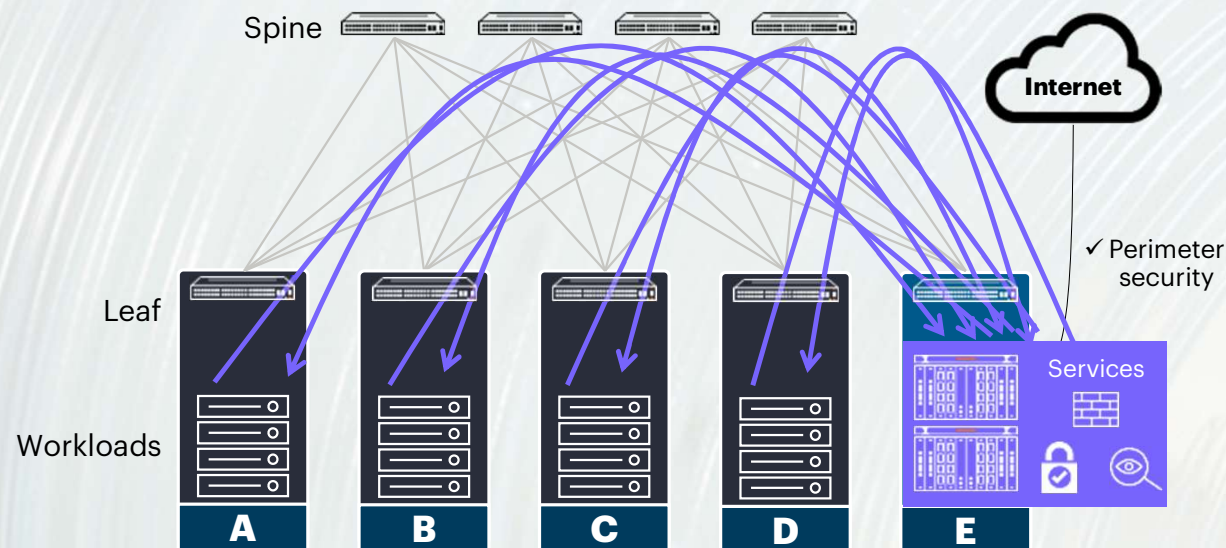
Der branchenweit am häufigsten eingesetzte  
Smart Switch  
– seit 2022

- Hochleistungsfähige L2/3-Switching mit **DPU-Beschleunigung**
- **1,6 T Stateful Firewall mit NAT**, Verschlüsselung und hochauflösender Telemetry in großem Maßstab
- Einheitliche Netzwerk- und Sicherheitsrichtlinien und Automatisierung
- **10-fache Leistung und Skalierbarkeit** im Vergleich zu herkömmlichen Legacy-Switches und Sicherheitsanwendungen/-agenten
- **Offenes Partner-Ökosystem:**



So läuft es heute meist:

## EVPN VXLAN: Zentralisierte Services Architektur



Zentralisierte Services Architektur

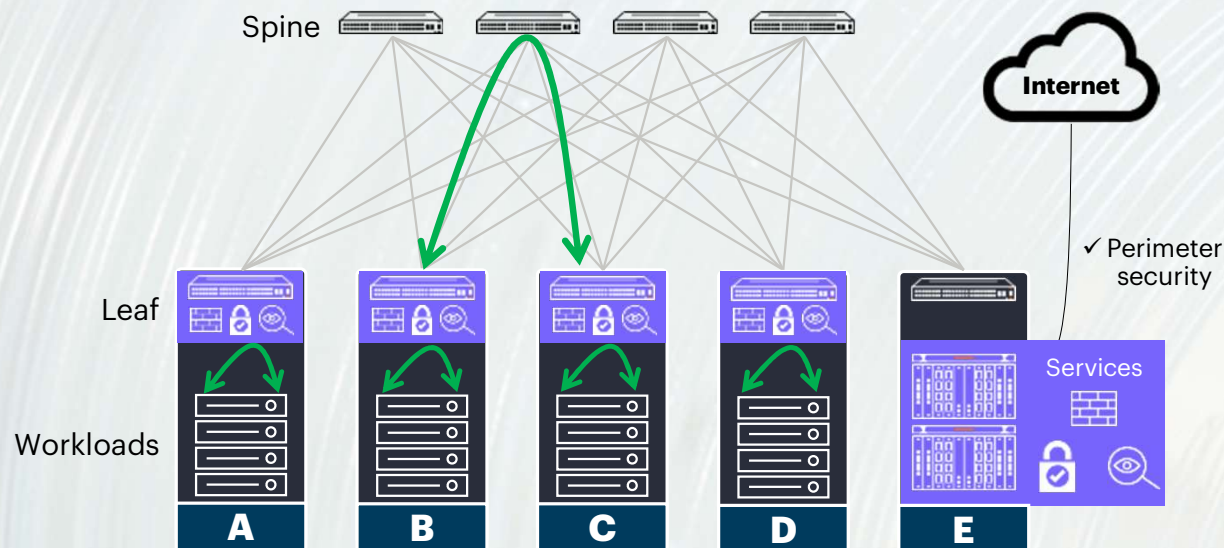
### Herausforderungen:

- Der Verkehr muss zum L4-7-Services Leaf/Rack weitergeleitet werden
- Skalierung von Last/Geschwindigkeit des O-W-Datenverkehrs nicht möglich
- Hohe und kostenintensive Komplexität (Appliance-Wildwuchs, Lizenzen)

So kann es gehen



# Verteilte Services Architektur

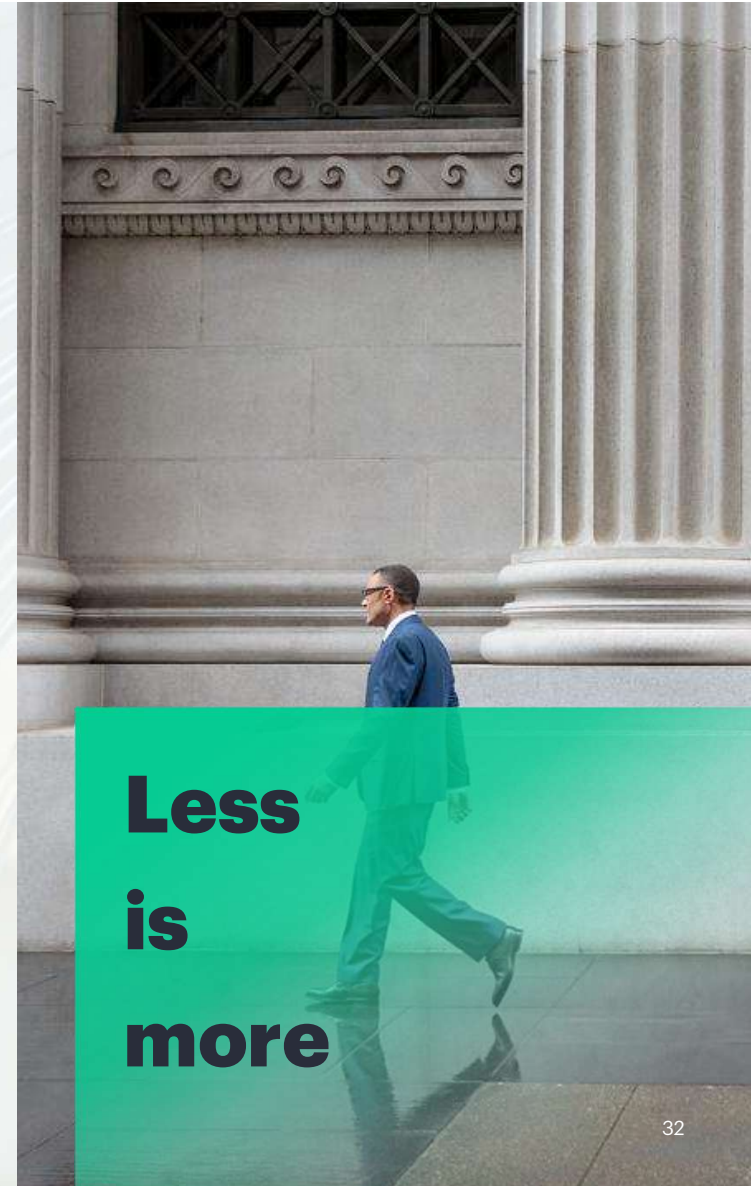
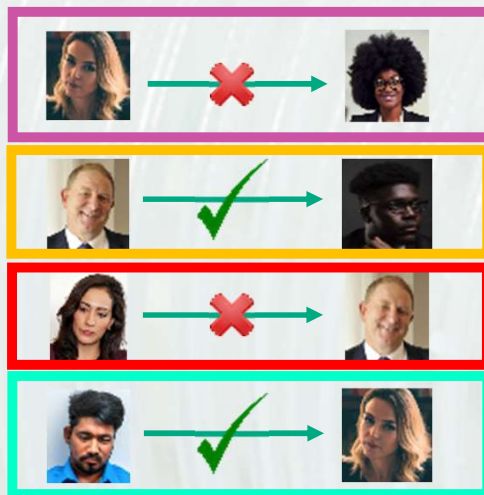
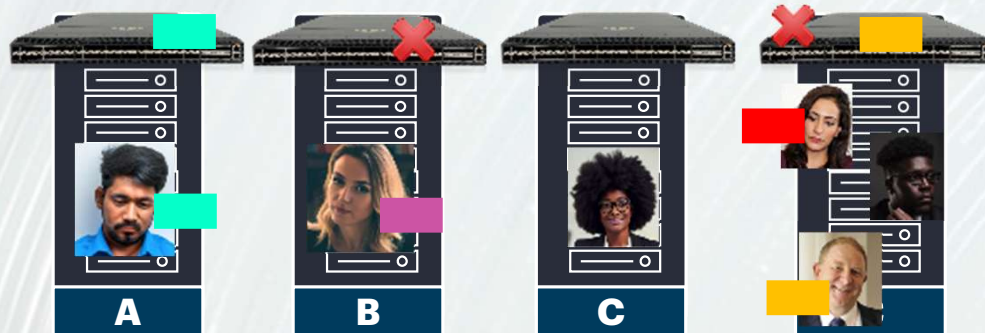


Verteilte Services Architektur

## Vorteile

- Bessere Sicherheitslage – Firewall auf jedem Leaf-Port
- Niedrigere Betriebskosten, keine Legacy-Appliances/Software-Agenten
- Echtzeit-Telemetrie
- Automatisierte Netzwerk- und Sicherheitsrichtlinien inkl. der Bereitstellung
- Verbesserte App-Latenz/-Leistung

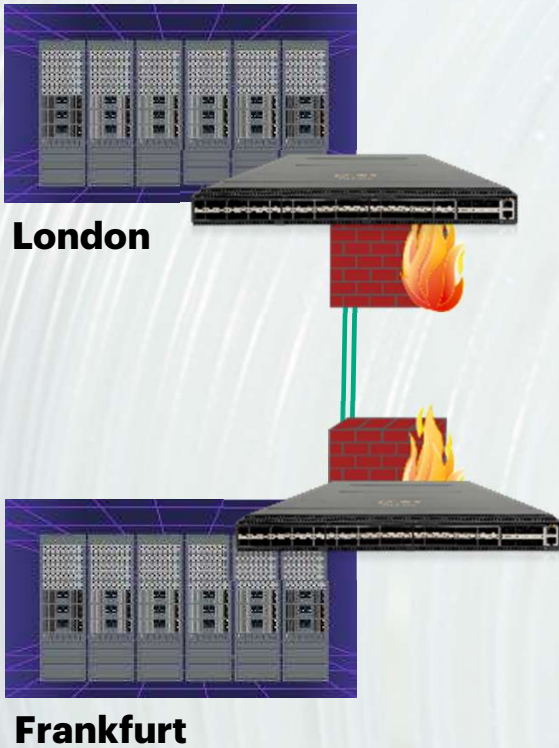
# Segmentierung im RZ



**Less  
is  
more**

**HPE** **aruba**  
networking

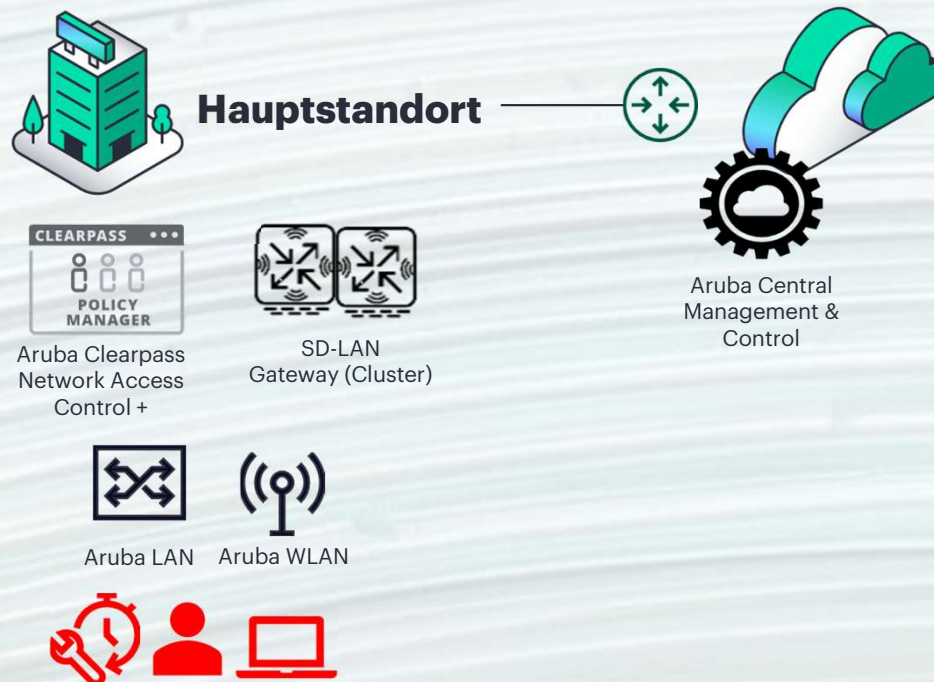
## Verschlüsselung zwischen Standorten



**Less  
is  
more**



# **Sicherheit durch Automatisierung (Dynamische Segmentierung)**



# Der Hauptstandort



Router

Firewall  
SIEM  
IDS/IPS



DMZ

Firewall

Campus



Firewall



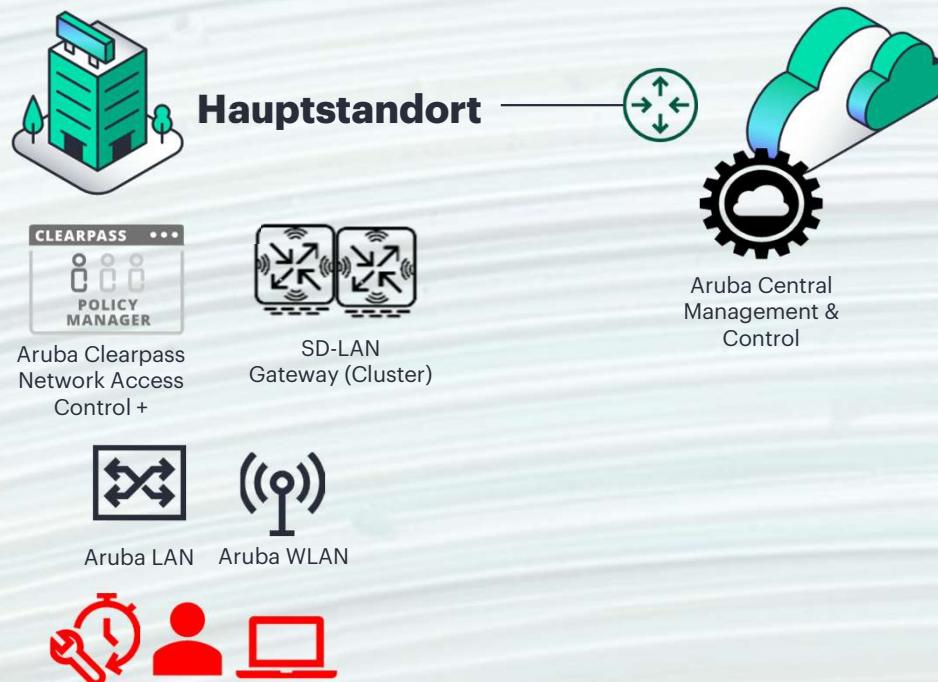
Rechenzentrum

# Das Remote Bild

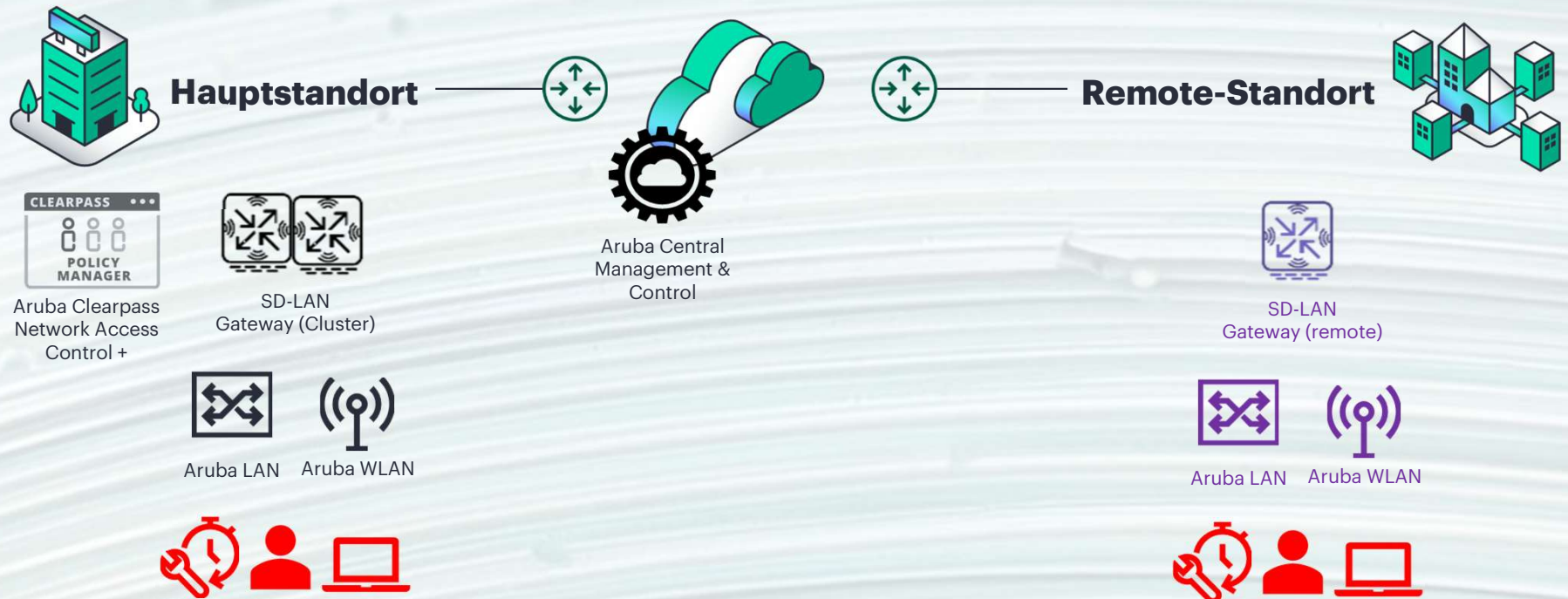




# **Sicherheit durch Automatisierung auch am Remote Standort (SD-LAN)**



# HPE aruba networking SD LAN Lösung



**Dynamische Segmentierung**

**Software Defined Branch**



# **Interaktive Sicherheit zwischen Remote + Hauptstandort (SD-WAN + SSE = SASE)**

... davon gleich mehr im nächsten Vortrag

Aber wann nutze ich was?

# HPE Networking

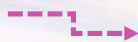
**HPE** aruba  
networking

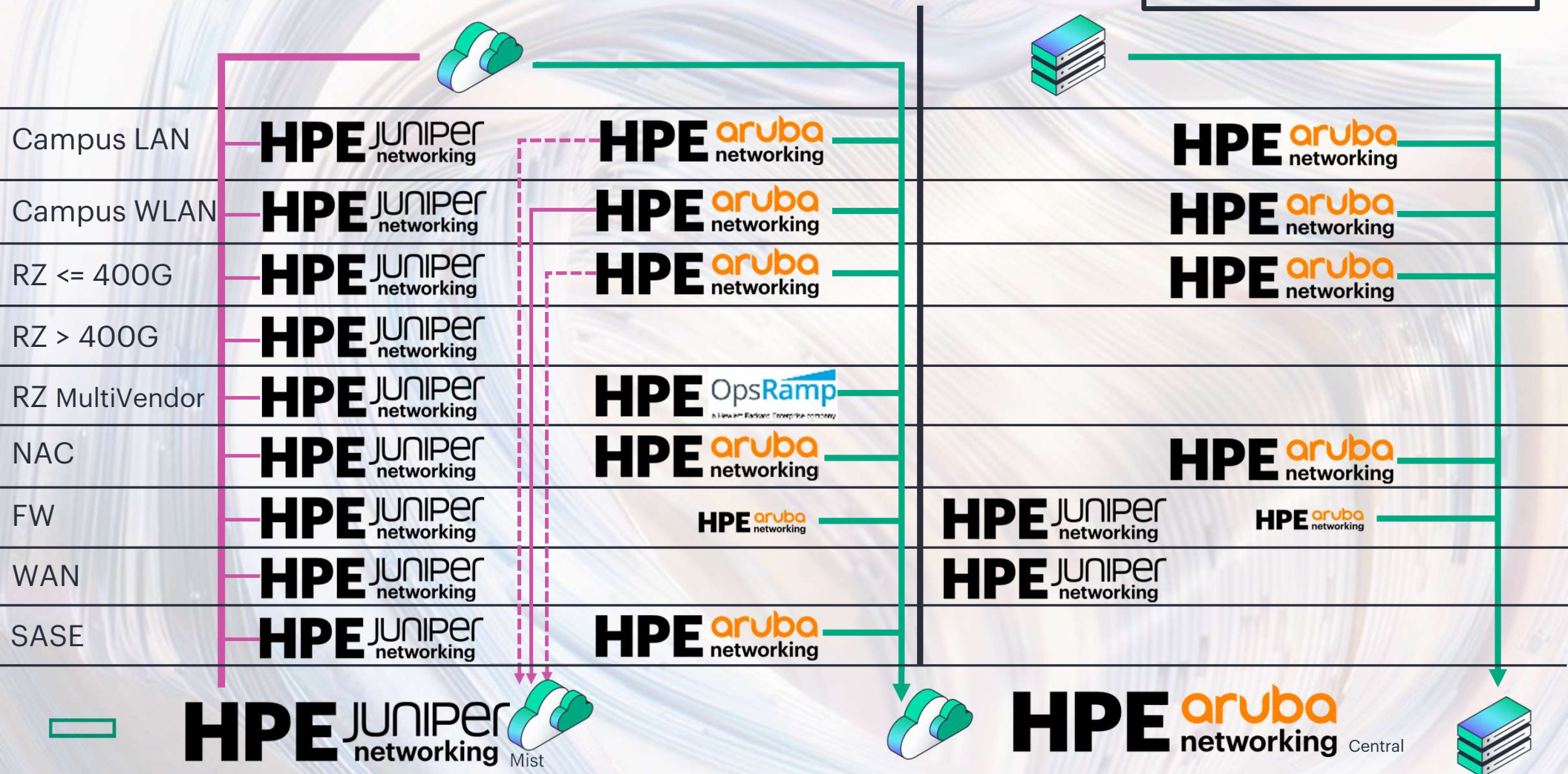
Und/Oder

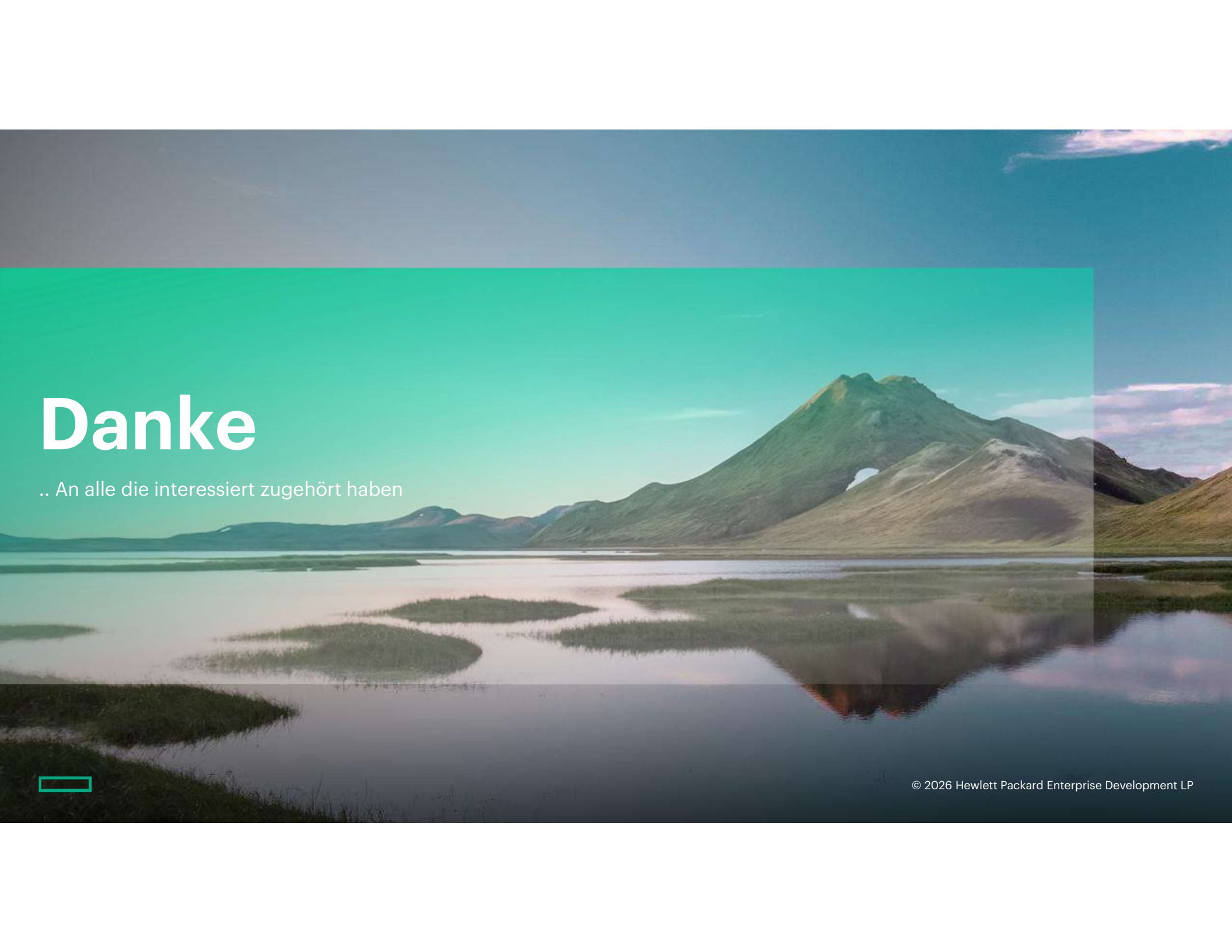
**HPE** JUNIPER  
networking



# Der Entscheidungs-Flow

Geplant:   
Keine Timeline committed





# Danke

.. An alle die interessiert zugehört haben

