

Vom Troubleshooting zur  
Prävention:

Wie autonome Netzwerke den  
Betrieb unterstützen

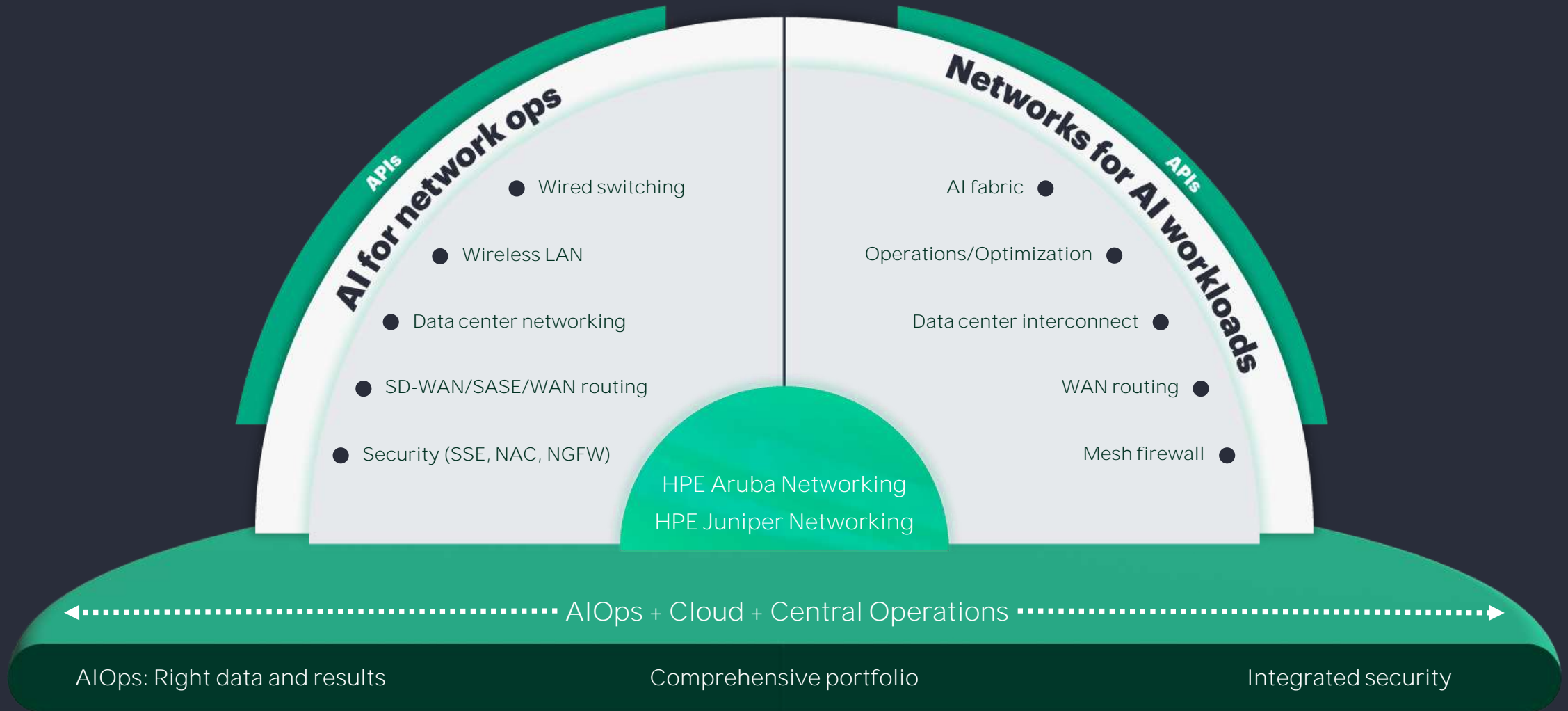
---

Benedikt Sondermann, Senior Systems Engineer  
HPE Networking

[benedikt.sondermann@hpe.com](mailto:benedikt.sondermann@hpe.com)



# 1 Minute Kurzvorstellung von HPE Networking: Das sichere, KI-native Netzwerk



APs

Switches

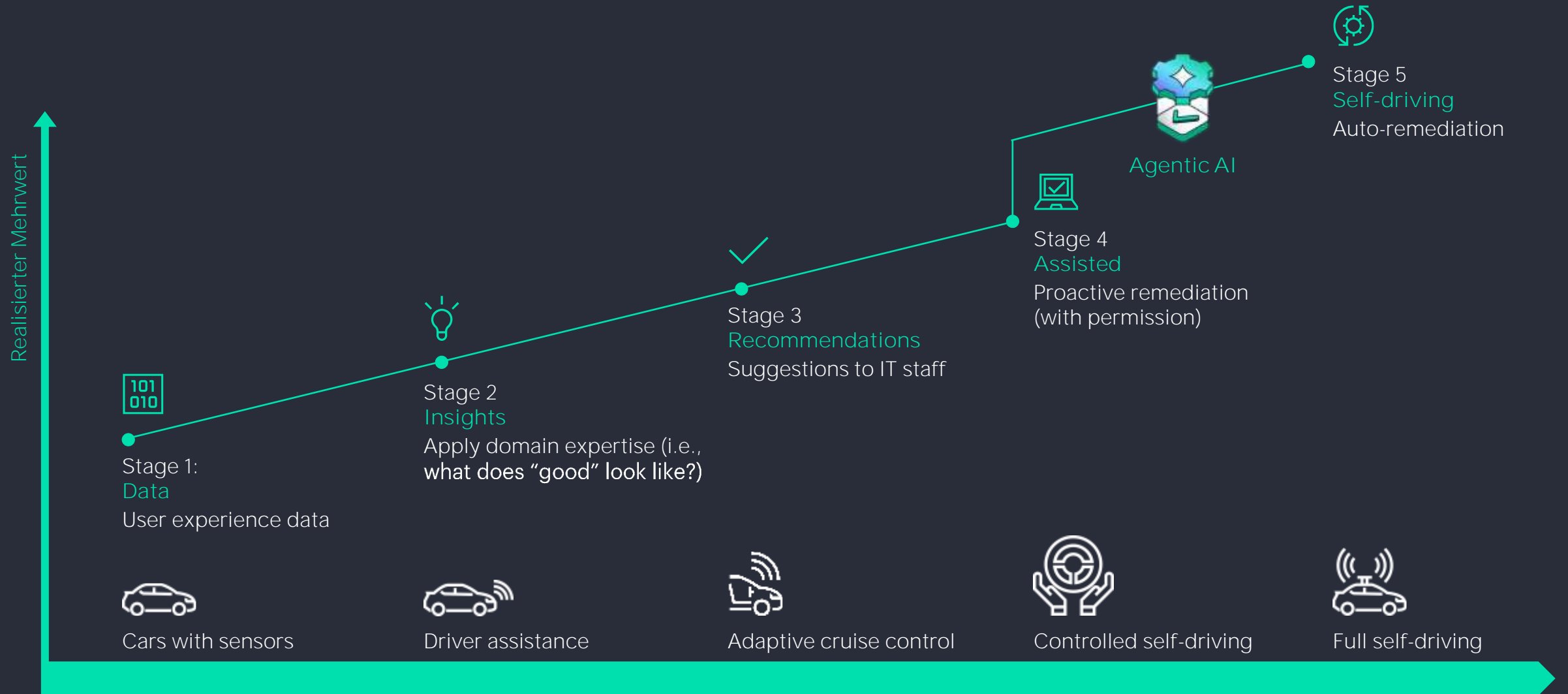
Routers

Firewalls

# Autonome Netzwerke?

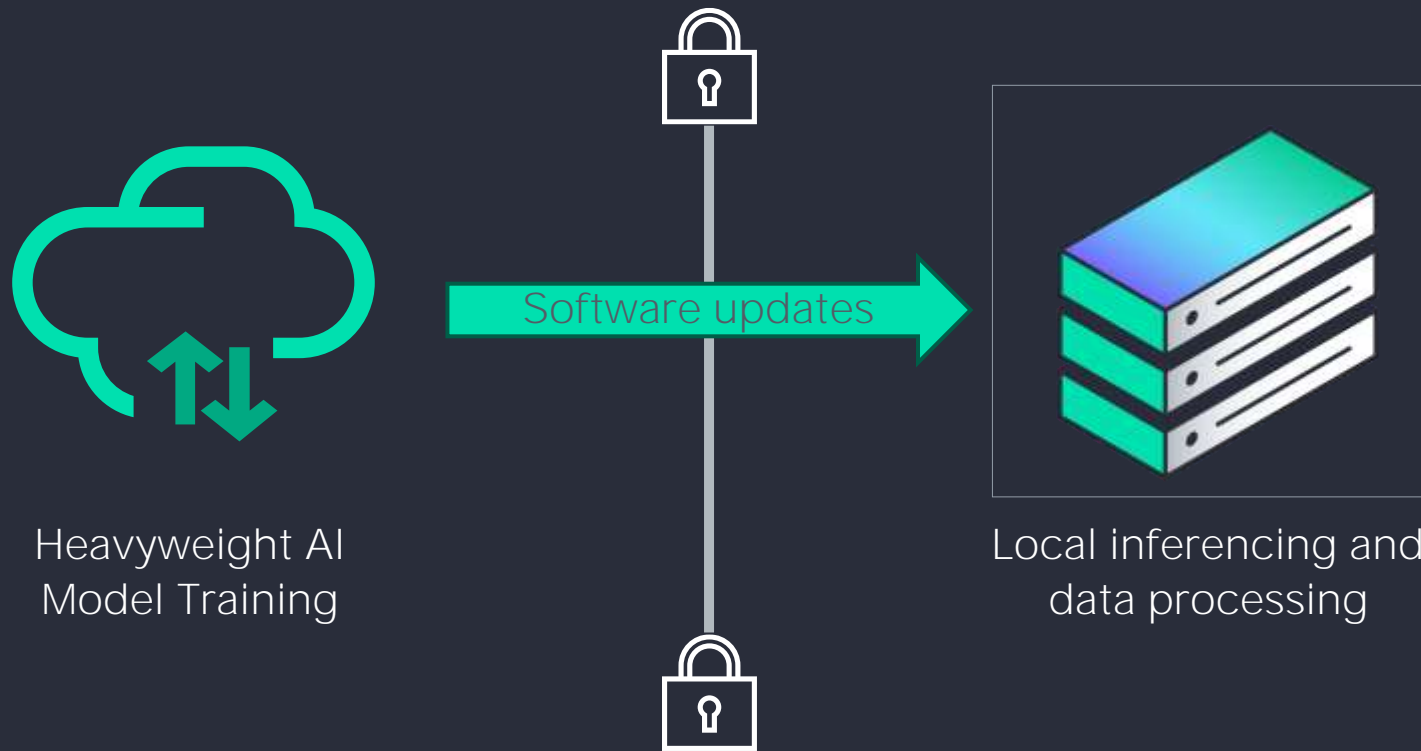


# Wo sind Sie auf der Reise zum autonomen Netzwerk?



# 100% Air-Gapped HPE Aruba Networking Central on Premises

KI mit lokalem Inferencing, ohne jegliche Cloud/Internet-Anbindung



**AI Search:** Delivers fast, NLP-powered access to product and documentation information using a lightweight, HPE-trained on-premises LLM

**Network Insights:** Large number of insights available on premises

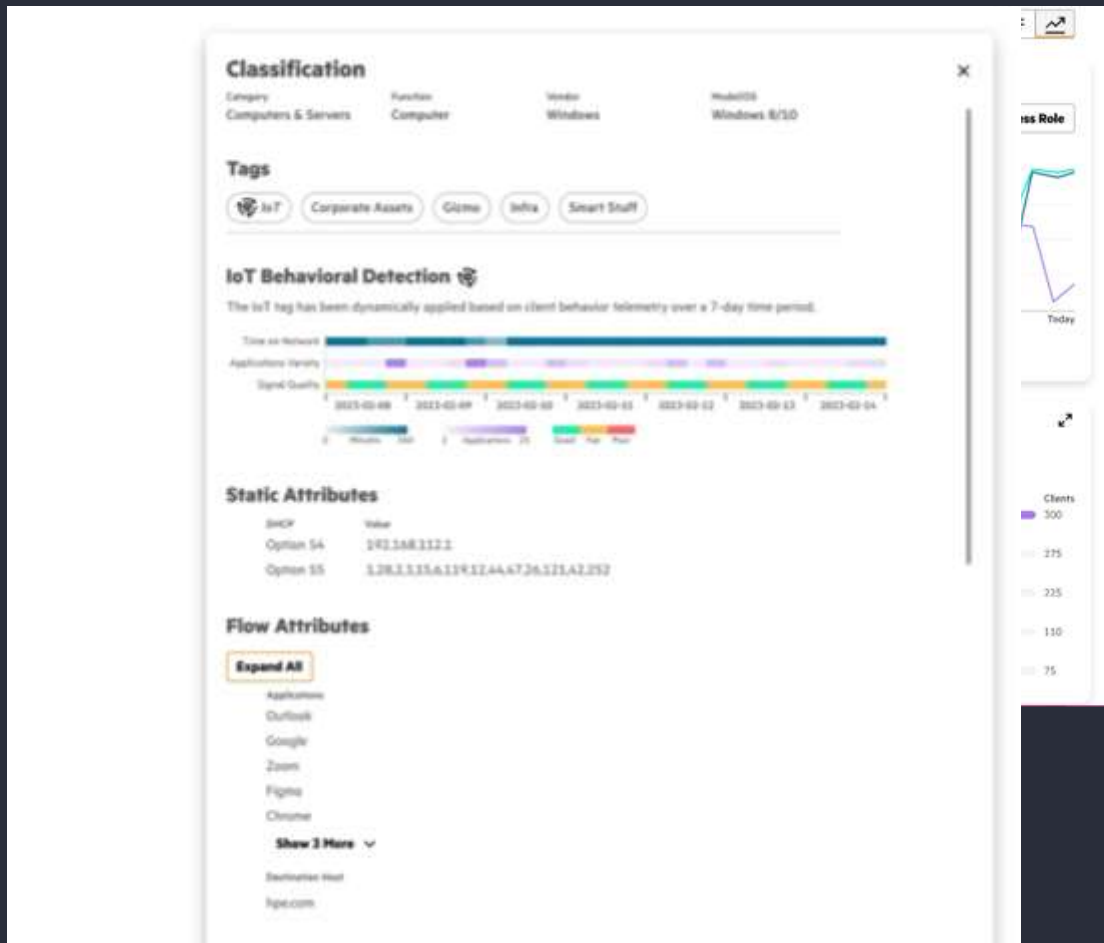
**AI Alerts:** Real-time anomaly detection, reducing alert fatigue

**Client Insights:** Know exactly what's on your network and how it's performing without any additional agents/collectors

Your network and client data never leaves your premises

# KI-basiertes Profiling der Endgeräte

Enhance endpoint visibility for Zero Trust networking



- Only solution with AI-native IoT profiling and behavior analysis for segmentation accuracy
- Traffic flow visibility for high classification efficacy and enhanced protection
- Advanced filtering and custom group tagging aid in policy creation and enforcement



# AI Search

Accurately identifying user intent with LLM

The screenshot shows the HPE Aruba Central interface with a search bar containing the query "windows clients with poor health in site RSVCP". The search results are displayed under the "Clients (2)" tab. Two client entries are shown, both with a status of "Failed - Dot1X Supplicant Timeout". The first entry has MAC address 0024-9b0a-2c3f and IP address 10.3.11.107. The second entry has MAC address 0024-9b0a-8414 and IP address 10.3.11.108. Both clients are identified as Microsoft Windows devices.

Name	MAC address	IP Address	WLAN	VLAN	Role	Last seen	Category	Function	Vendor	Model/OS	Site
0024-9b0a-2c3f Failed - Dot1X Supplicant Timeout	0024-9b0a-2c3f	10.3.11.107	REJECT_AUTH	(1)	REJECT_AUTH	October 22...	Computing...	Operating System	Microsoft	Windows	RSVCP
0024-9b0a-8414 Failed - Dot1X Supplicant Timeout	0024-9b0a-8414	10.3.11.108	REJECT_AUTH	(1)	REJECT_AUTH	October 22...	Computing...	Operating System	Microsoft	Windows	RSVCP

The screenshot shows the HPE Aruba Central interface with a search bar containing the query "AP running software version 10.7.1.0\_91459". The search results are displayed under the "Devices (2)" tab. Two access point entries are shown, both with a status of "ONLINE". The first entry is an RSVC-AC3-AP16 with MAC address a0d3e0c0d1fbf and IP address 10.3.15.116. The second entry is an RSVCP-AC3-AP15 with MAC address 9c8cd8c90e9f5 and IP address 10.3.15.30. Both access points are identified as AP-555 models and are running firmware version 10.7.1.0\_91459.

Name	Type	MAC address	IP Address	Model	Serial Number	Uptime	Firmware Version
RSVC-AC3-AP16 ONLINE	Access Point Standalone	a0d3e0c0d1fbf	10.3.15.116	AP-555	VNKYK9Y06F	32w	10.7.1.0_91459
RSVCP-AC3-AP15 ONLINE	Access Point Standalone	9c8cd8c90e9f5	10.3.15.30	AP-515	DNH5KDS7X8	32w 5d	10.7.1.0_91459

- One-click access to Topology, Alerts, Applications, Clients, and more.
- Search for Clients and Devices by IP, MAC address, Model, OS, and other criteria.
- Easily detect failed clients, malfunctioning devices, and applications experiencing issues, along with corresponding reason codes.
- Search the HPE Aruba Networking Knowledge Base and verify solutions using the Validated Solutions Guide.

# Alerts: KI-unterstütztes Troubleshooting

**Alerts**

Severity: Critical (195) Major (11) Minor (53) Info (00) Active (19) Deferred (00) Cleared (182)

19 items

Name	Priority	Status	First Occurred	Last Occurred	Occurrences	Category
<b>WPA Passphrase is Incorrect</b> Minor - The WPA passphrase provided by the client does not match the configured value.	Medium	Active	09/28/2024, 1:45:00 AM	10/21/2024, 5:35:00 PM	6711	Authentication
<b>DHCP Discover Timeout</b> Minor - The DHCP server did not respond to the client's discovery request.	Medium	Active	10/19/2024, 5:05:00 AM	10/21/2024, 5:30:00 PM	488	DHCP
<b>Loop Detected</b> Critical - A loop was detected between switches.						
<b>Switch Interface Tx Rate</b> Critical - Switch BO-MIAI-EGSW03's transmit rate for interface 1/1/16 was above 90% for 30 minutes						

190+ alert types

**Summary**

Client did not receive a response to its DHCP Discovery broadcast packet.

First Occurred: October 19, 2024 5:05 AM  
Last Occurred: October 21, 2024 5:30 PM  
Occurrences: 688  
Priority: Medium

**Impact**

Clients: 2% (1/68)  
Switches: No impact  
Access Points: 13% (1/8)  
Gateways: No impact

**Troubleshooting**

- VLAN Configuration Check
- Traceroute
- Other IP Allocations Successful in Same VLAN
- Ping Check

Automated troubleshooting steps

5-minutes to generate

**Actions**

**Root Cause**  
Potential connectivity issue with the DHCP server not responding to discover messages

**Actions**

- Ensure correct routing paths to DHCP server
- Check firewall rules blocking DHCP traffic
- Verify VLAN config on AP and upstream switch
- Check switch port configs for correct VLAN tagging
- Check for DHCP server logs

**Root Cause**  
Potential configuration issue with the DHCP server not responding to discover messages

**Actions**

- Check DHCP server config for correct IP scope
- Ensure DHCP server is set to respond to discover mgs
- Verify no firewall rules blocking DHCP traffic
- Check VLAN config on AP and upstream switch
- Check for DHCP server logs

Root cause recommended action

**STEP 1 OF 3 Create Alert**

Configure parameters for this alert.

Scope: Global  
Scope Type: Global

Enable this alert

**Triggering**  
Define what triggers the alert

KPI Category: AP CPU Utilization  
Access Point: [Dropdown]  
Primary KPI: AP CPU Utilization

**Identification**  
Configure parameters to identify this alert

Name: AP CPU Utilization-Custom  
Summary: AP (hostname) average CPU utilization was above (threshold) for (duration) minutes  
Labels: [Dropdown]

**Thresholds**  
Define how primary KPI maps to alert severity levels

Severity: Critical  
 Enable Threshold

Severity: Major  
 Enable Threshold

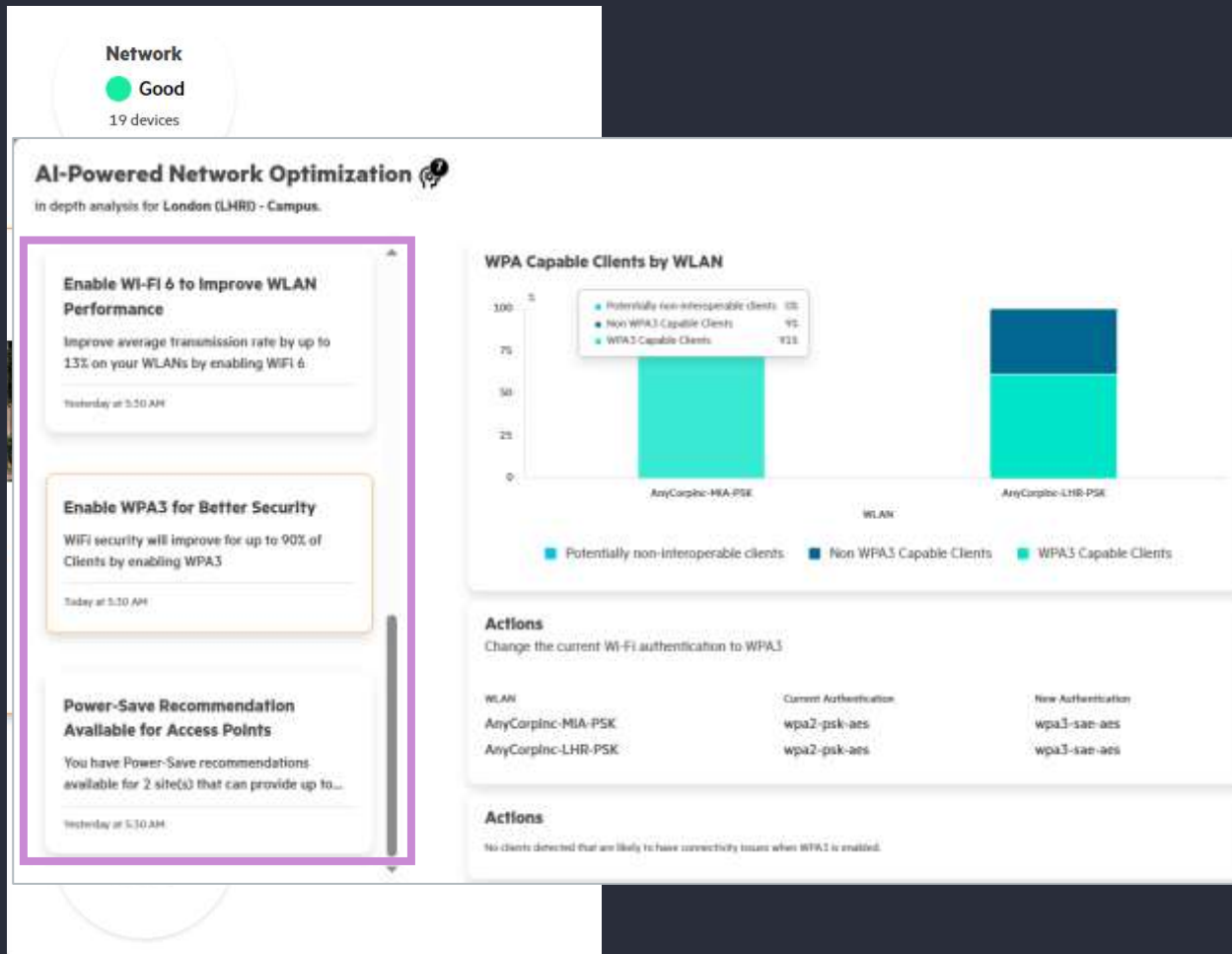
Threshold: 90  
Min: 1, Max: 255

Severity: Minor  
 Enable Threshold

**Duration**  
Elevation Period: 5 Minutes  
Min: 5, Max: 120 minutes

Custom alerts on any KPI

# Proaktive Empfehlungen zur Optimierung des Netzwerks



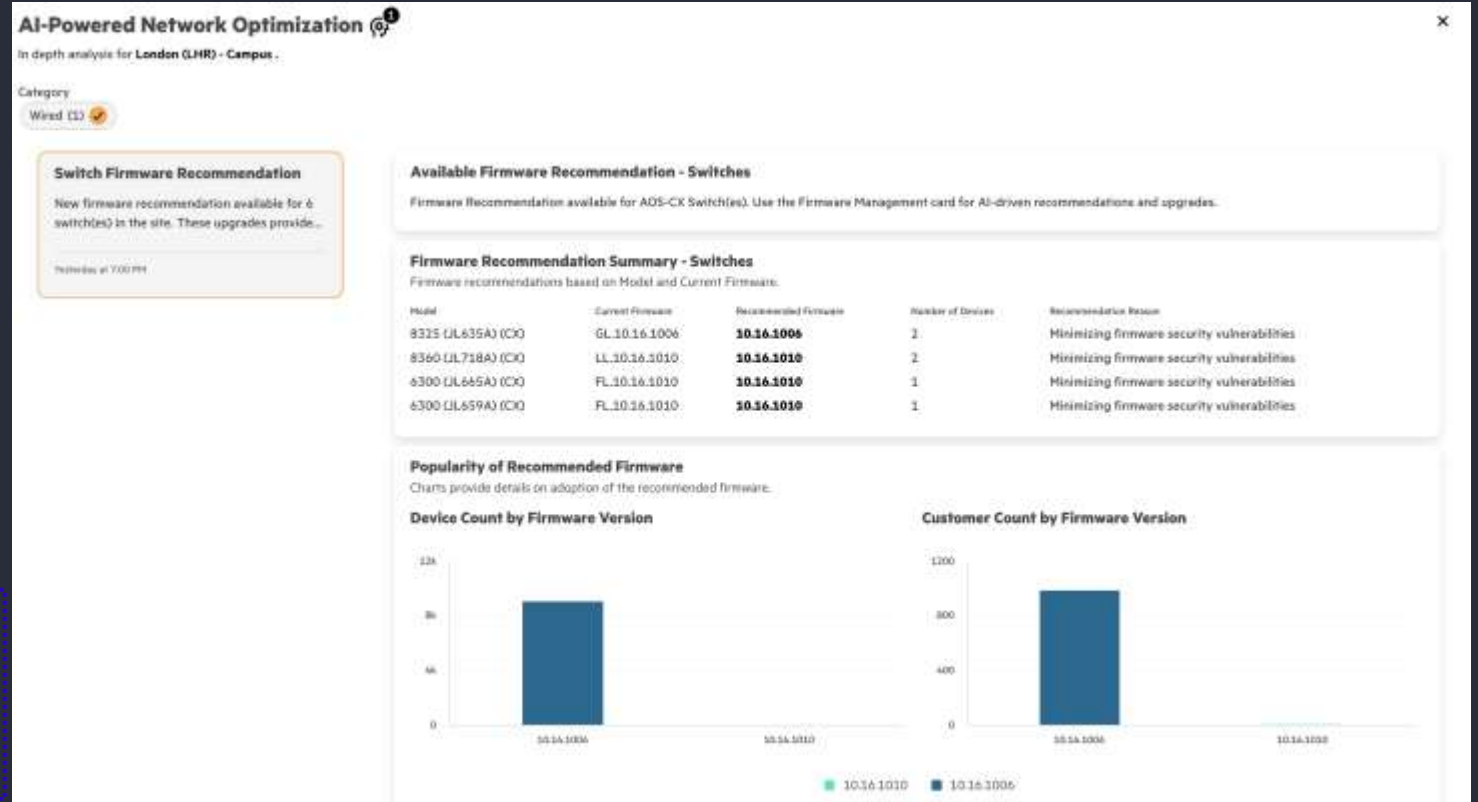
- Custom, actionable recommendations at a global/per-site basis
- AI/ML models trained and re-trained on data from anonymized peer groups with similar environments
- Examples:
  - Firmware recommendations
  - 802.11ax recommendations for Wi-Fi performance
  - AP power save recommendations to support sustainability efforts
  - WPA3 insights for improved security posture and more

# Firmware Recommender



Joey, Network admin

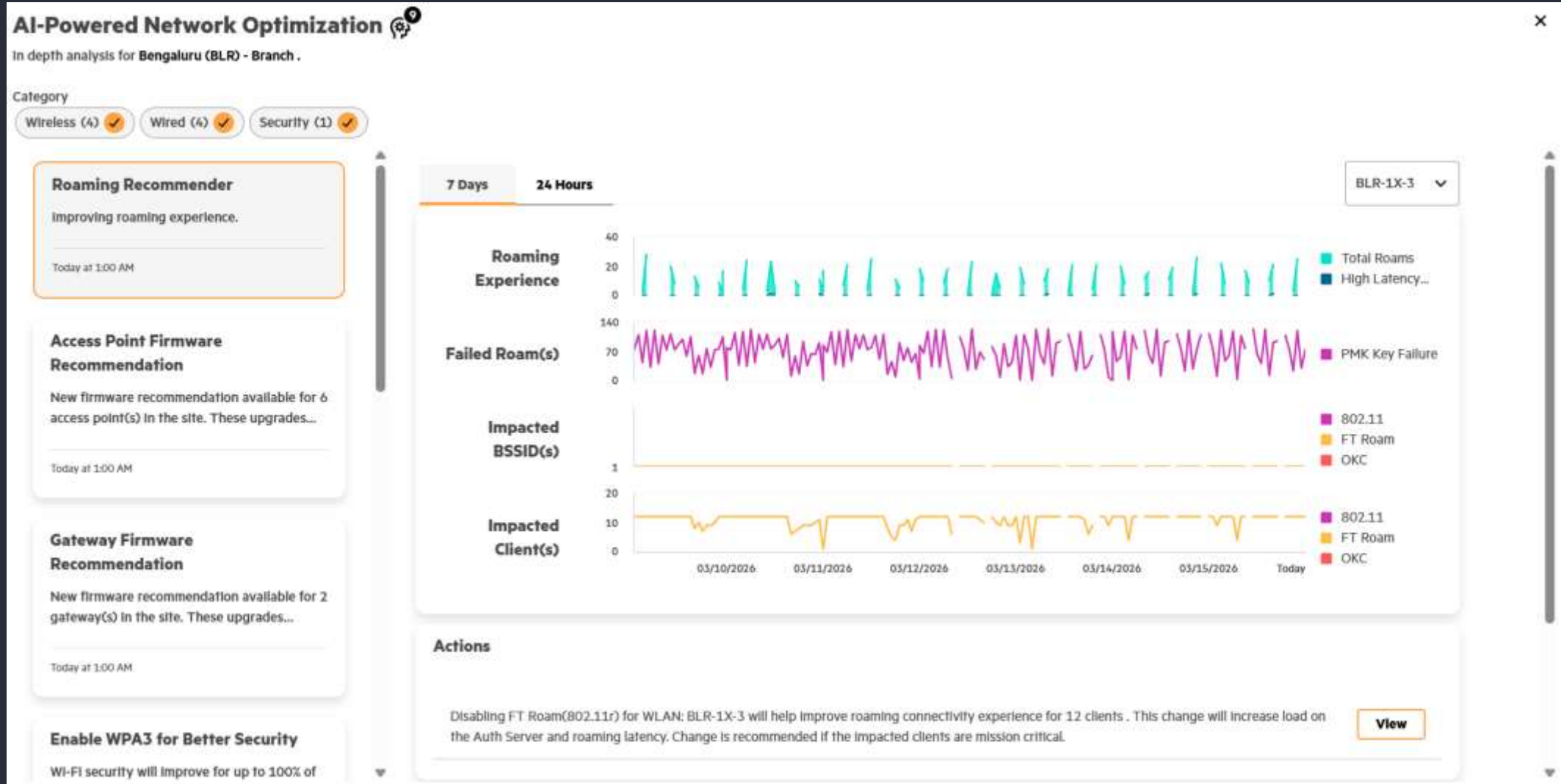
Manages a complex network and is cautious with upgrades. Relies on professional services for firmware assessment and recommendations



## Rely on HPE Aruba Networking's domain expertise

AI-native firmware recommender uses ML models to recommend the **best and most secure version of firmware** for your network devices based on an extensive set of factors (compatibility, bugs, age, vulnerabilities, number of customers etc.)

# Roaming Recommender



# Floor Plan Manager: Day-0 AP-Planung

**STEP 2 OF 3**  
**Planning**  
Manually place access points for simulating its position to extend Wi-Fi coverage on the floor plan.

Placement Method  
 Manual  
 Automatic Optimization

Access Point Name Prefix  
Floor-3

Note: Name format will be Prefix-APModel-Location

Select a Model  
Default (AP-633)

Select Bands to Cover  
 2.4 GHz  
 5 GHz  
 6 GHz

Signal Coverage  
Good ( -60 dBm)

Client Density  
Medium

Plan Access Point Deployment

Challenge – Where should APs be placed?

**STEP 2 OF 3**  
**Planning Summary**

**Placement Attributes**  
Here is the list of attributes used to place the access points on the floorplan.

Placement Method	Optimized Area
Automatic Optimization	Entire floor plan
Access Point Name Prefix	Floor-3
Floor-3	2.4 GHz
	5 GHz
	6 GHz
Model	Unknown

**Planned Access Points**  
List of planned access points used to simulate Wi-Fi coverage. Adding an access point in the browser with the same name to automatically explore the planned access points.

AP #15	AP #16
1 Access Point	2 Access Point
AP #11	
20 Access Points	

Plan

Solution – Predictive AP placement guidance

- Challenge:  
New deployments lack visibility into optimal AP placement.  
Manual planning is time-intensive and error-prone.
- Solution:  
Automated AP placement guidance based on RF heuristics and client density inputs  
Planned vs. deployed views for validation.  
Optimizes coverage and capacity before rollout.
- Results:  
Faster Day-0 design with fewer manual adjustments.  
Reduced site survey overhead.  
Higher confidence in coverage and performance at launch.

# Coverage-Hole-Erkennung



Coverage Hole

## Feature Description

AI-powered detection of uplink/downlink coverage holes using client SNR telemetry

Floorplan-based visualization of impacted APs and client density

Action cards with root cause analysis and remediation steps (e.g., increase transmit power, add APs)

## Customer Benefits

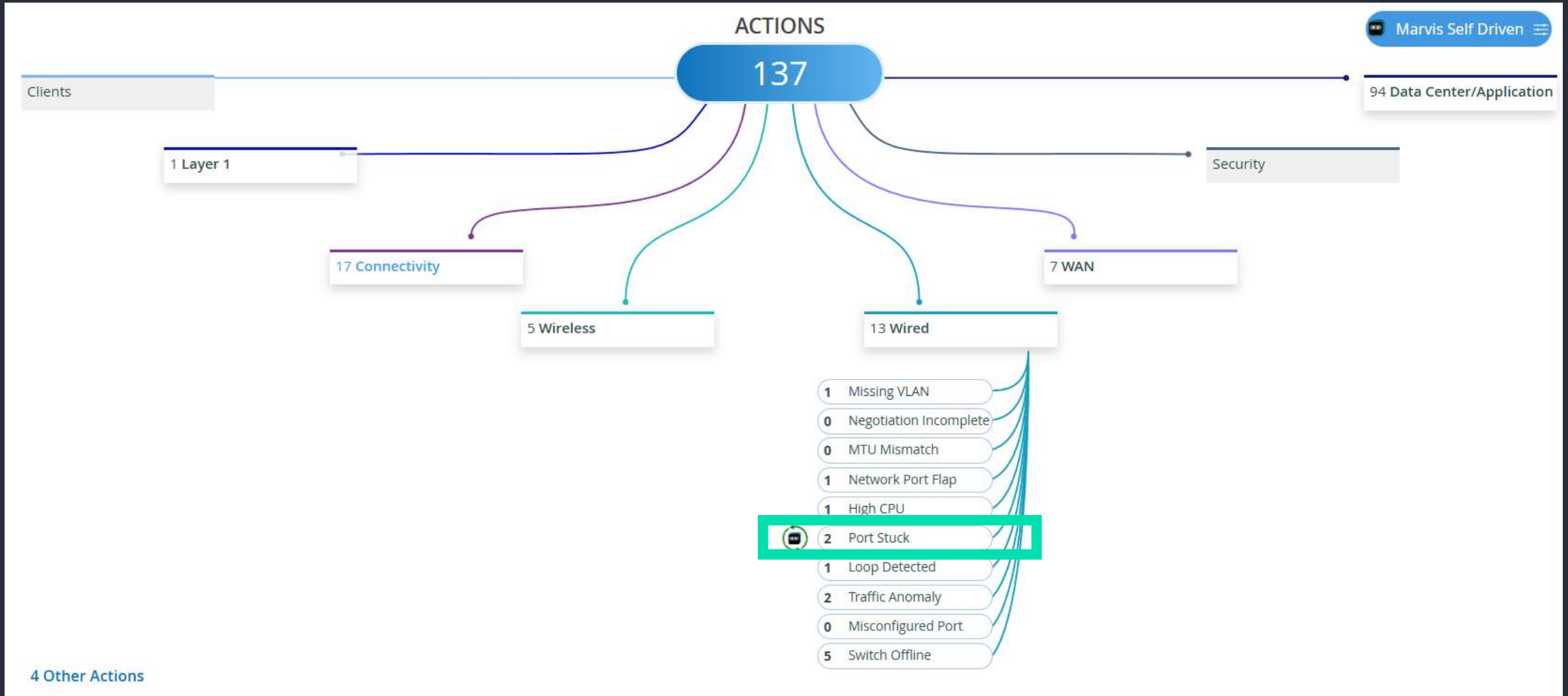
Improved RF coverage and client experience by resolving low-SNR zones

Reduced support tickets and faster resolution through automated recommendations

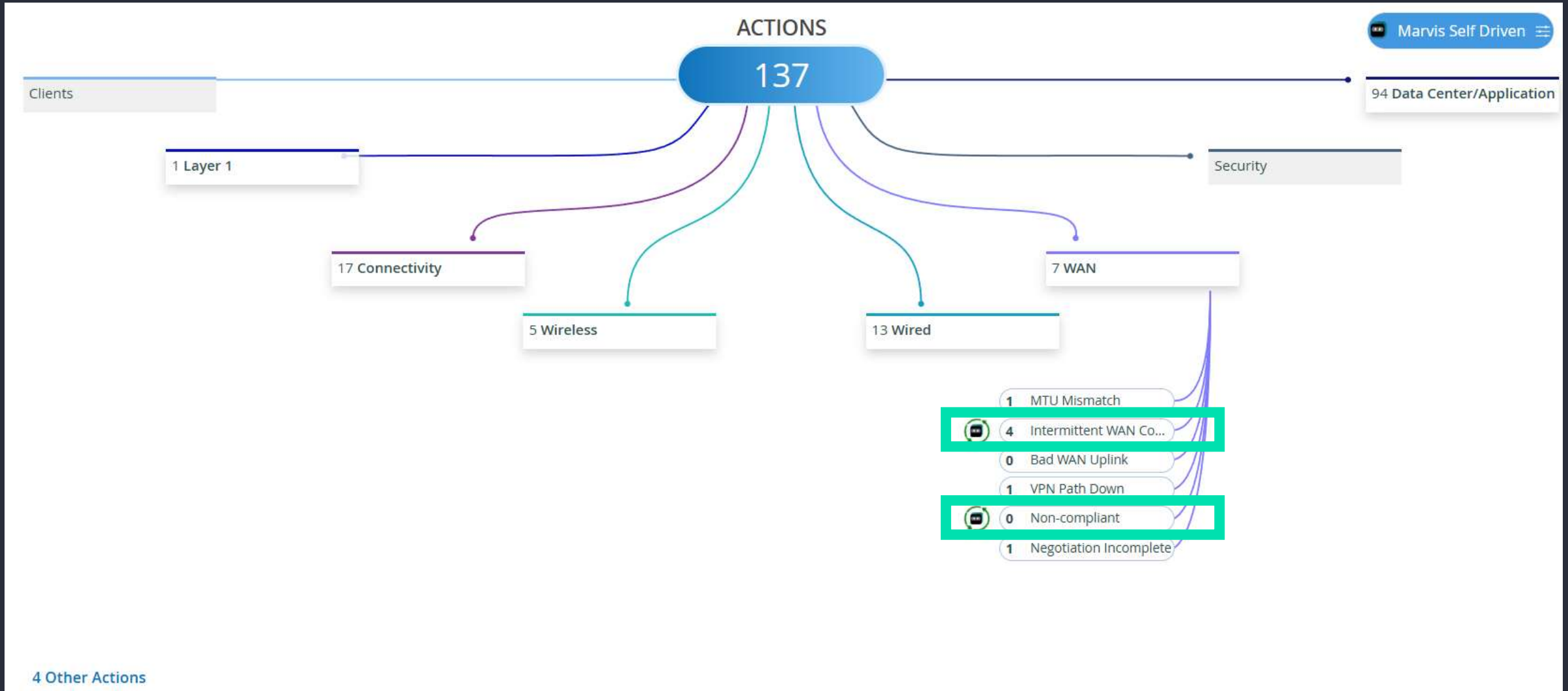
Enhanced visibility into spatial network health across 2.4GHz, 5GHz, and 6GHz bands

Lassen wir Netzwerk-Probleme  
doch einfach von selbst lösen!

# Beispiel für Self-Driven Remediation (Wired)



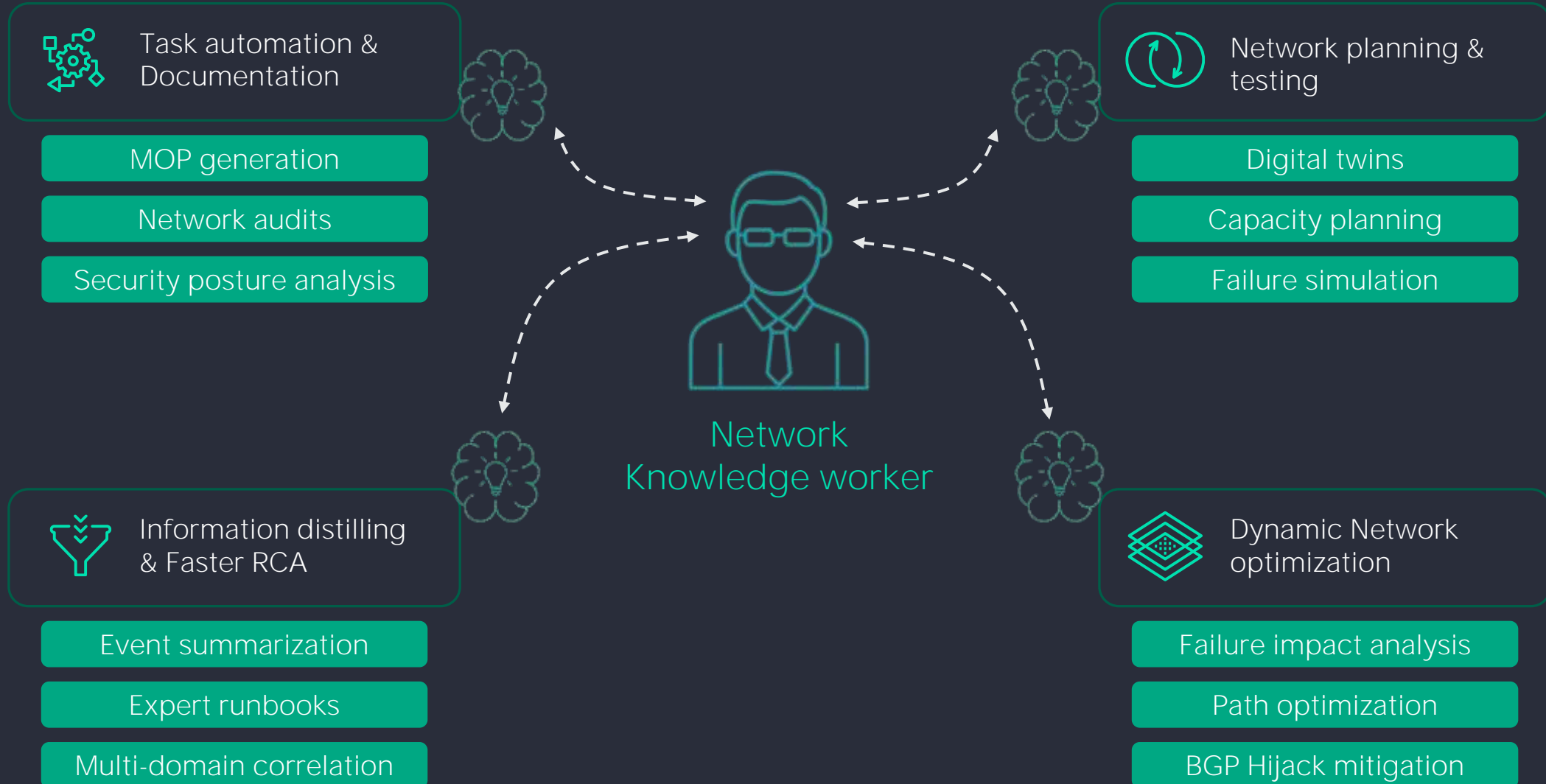
# Beispiele für Self-Driven Remediation (WAN)



# Agentic AI



# Wie AI-Agenten im Netzwerk-Bereich unterstützen können



# Bausteine von Agentic AI

## Anpassung des Systems an seine Umgebung



# Agentic Mesh in HPE Aruba Networking Central (1/2)

Hi, Benedikt

[Agentic-Mesh Actions] Roaming authentication failures impacting 12 clients at one branch site

### Agentic-Mesh Actions

Roaming authentication failures impacting 12 clients at one branch site

New Agentic-Mesh Action features added every release

Updated every min by the Autonomous Agentic-Mesh (03/16/2026,

### Autonomously Identified 1 Issue

- 1. Initial Observation:** Analysis revealed 1624 failed authentication attempts during roaming events on access point BO-BLR-AP01, compared to only 108 successful roams, indicating a 93.8% failure rate.
- 2. Scope Assessment:** The Issue was isolated to WLAN BLR-1X-3 at Bengaluru (BLR) - Branch site, affecting 12 out of 24 total clients. The limited scope (1 out of 96 access points, 1 out of 22 sites) suggested a configuration-specific issue rather than a widespread Infrastructure problem.
- 3. Security Configuration Review:** WLAN BLR-1X-3 uses WPA2-AES security mode, which is compatible with 802.11r Fast Transition. This ruled out basic security misconfiguration as the cause.
- 4. Roaming Protocol Analysis:** The high authentication failure rate specifically during roaming events pointed to an issue with the roaming mechanism itself. Investigation focused on the 802.11r Fast Transition feature, which is designed to accelerate roaming but requires client device support.
- 5. Client Compatibility Assessment:** With 12 clients experiencing failures while others roamed successfully, the pattern indicated client device incompatibility with the 802.11r protocol. Different device types and firmware versions have varying levels of 802.11r support.
- 6. Root Cause Confirmation:** The combination of high failure rates during roaming, successful initial connections, and partial client impact confirmed that 802.11r Fast Transition incompatibility was preventing affected clients from completing the fast roaming authentication process.
- 7. Remediation Strategy:** Disabling 802.11r on WLAN BLR-1X-3 will force all clients to use standard full authentication during roaming, which is universally supported. This trades slightly increased roaming latency for restored connectivity for the 12 impacted clients.

# Agentic Mesh in HPE Aruba Networking Central (2/2)

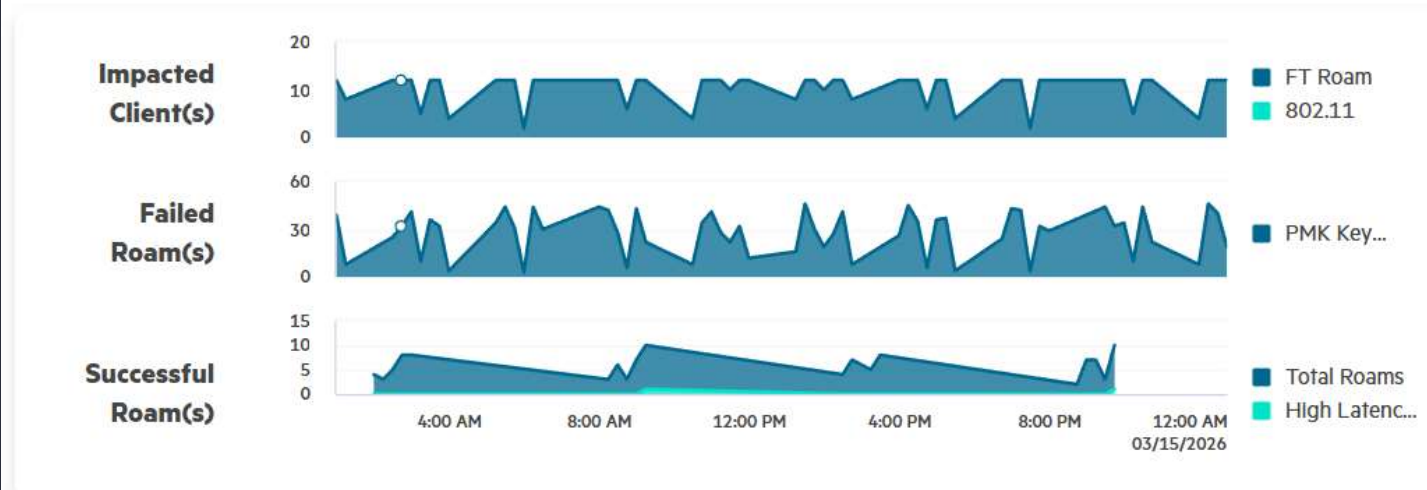
**Site-level Impact:** 12 clients at **Bengaluru (BLR) - Branch** site are experiencing roaming authentication failures with a 93.8% failure rate. Access point **BO-BLR-AP01** recorded 1624 failed authentication attempts during roaming events on WLAN **BLR-1X-3**.

**Root Cause**

802.11r Fast Transition roaming protocol incompatibility with specific client devices. The enabled FT feature on WLAN **BLR-1X-3** is preventing 12 clients from successfully authenticating during handoffs between access points.

**Remediation**

Disable 802.11r Fast Transition on WLAN **BLR-1X-3** to restore roaming functionality. Alternatively, create a separate WLAN without 802.11r for incompatible devices while maintaining the current WLAN for compatible clients.



Search  Filter  View

3 items

FT (802.11r) Compatibility	Vendor	Year	Model	Impacted Clients	Total Clients
FT (802.11r) Capable	Zebra...	2015	Zebra-Mobile-...	0	12
FT (802.11r) Capable	Intel Corporate	2016	Windows...	0	12
FT (802.11r) Compatible	HUAWEI...	2024	Unclassified...	0	5

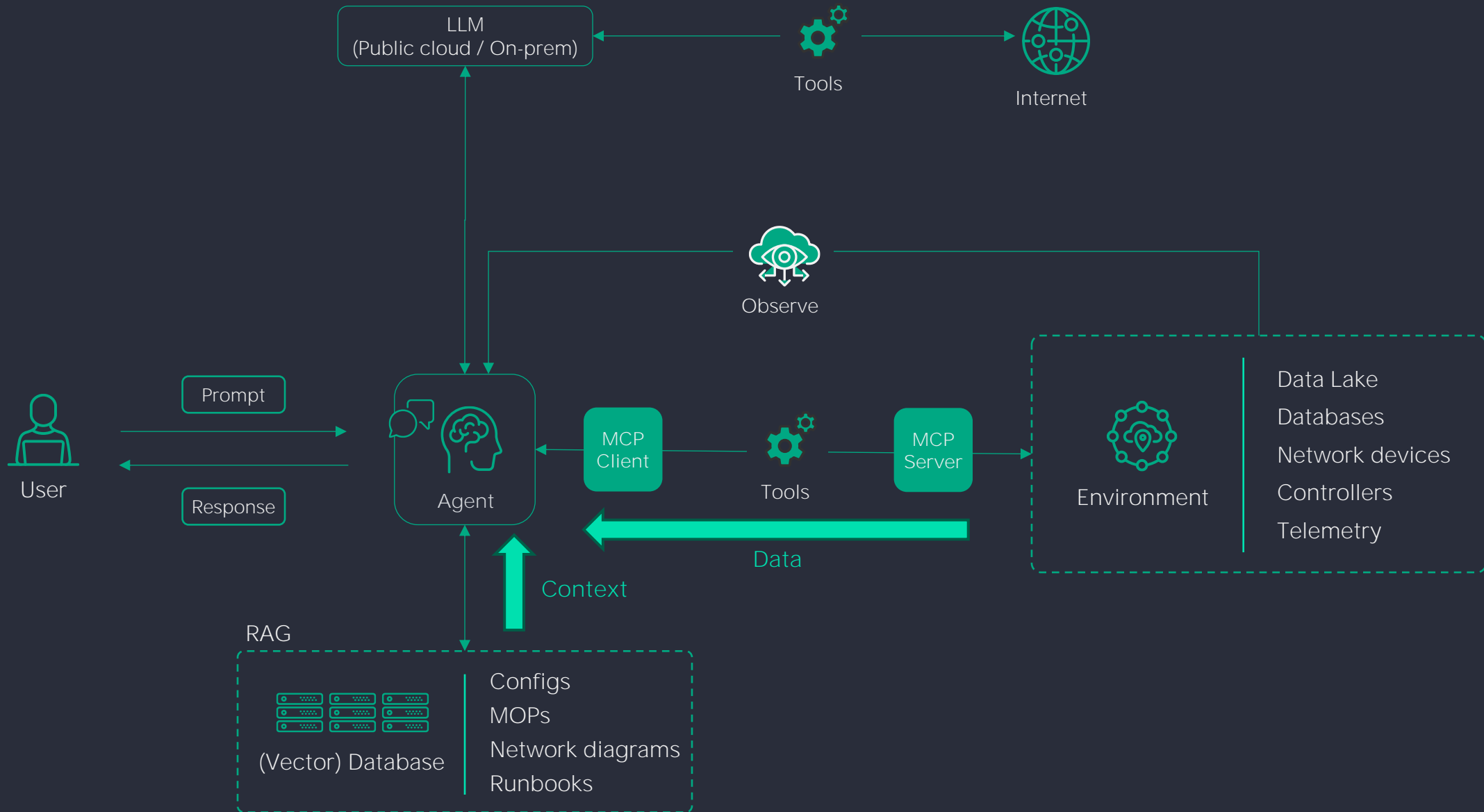
Is this helpful?

Enter a prompt here

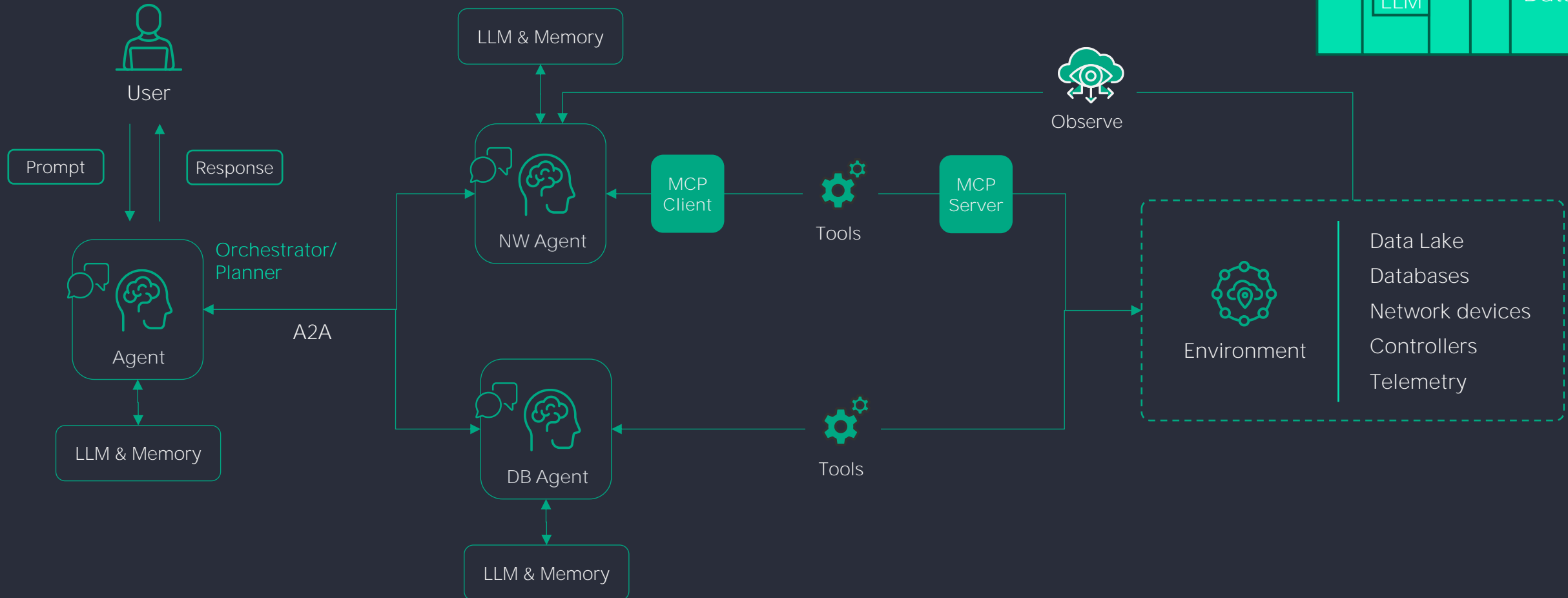


MCP-Server zur Anbindung an eigene  
KI-Agenten für umfassende Aufgaben

# Architektur Single-Agent-AI



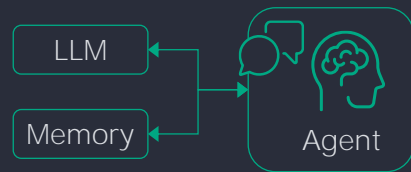
# Architektur Multi-Agent-AI



# Zusammenfassung von Agentic-AI-Architekturen

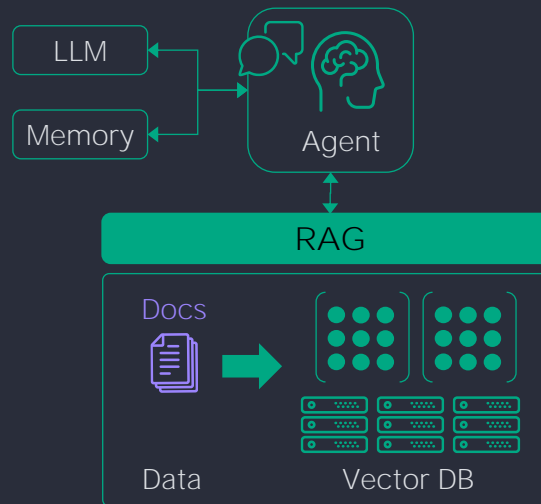
## Inference only

(no RAG, LLM fine-tuning or multi-agent)



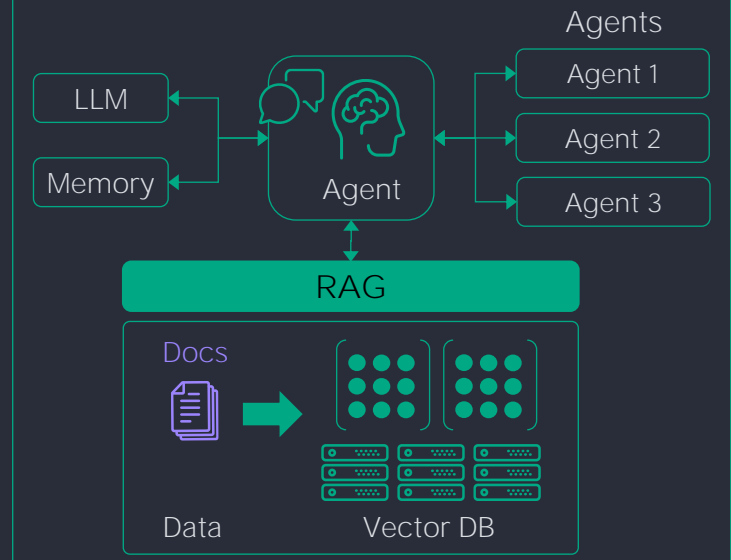
## Inference + RAG

(no LLM fine-tuning or multi-agent)



## Inference + RAG + Multi-agent

(no LLM fine-tuning)



# Klingt spannend? Na dann: nichts wie los!

Ihre Netzwerkkumgebung (Router, Switches, Firewalls) von HPE Juniper Networking können Sie bereits heute mittels MCP-Server an Ihre eigenen AI Agents anbinden.

MCP Server Code auf Github (Open Source):

<https://github.com/Juniper/junos-mcp-server>



# Wichtige Aspekte für die Implementierung von Agentic AI

## Model selection

**Choose wisely:** LLM vs SLM (*Bigger is not always better!*)

**Find your sweet spot:** Experiment with different models / different amounts of parameters

**Consider:** Context window, Training data, Agentic capabilities, Open-source vs Open-weights vs Closed

## Agents

**Be pedantic:** Use Pydantic classes for data validation, parsing, and serialization

**Design your execution patterns:** Sequential vs Parallel, Orchestrator & Planner agents, Observer & Critic agents

**Manage context windows:** Provide only the required tools

## Agent-to-agent

**Frameworks:** Choose your favorite, connect them through A2A

**Design your callbacks:** How and when agents handoff, How they use short-term and persistent memory

**Keep them in check:** Prevent scope creep across agents (define the boundaries)

# Measuring Agents in Production

Research paper: <https://arxiv.org/abs/2512.04123> (Dec 2025)

95% of agent deployments fail. > What separates successful deployments from failures?

What are the applications, users, and requirements of agents?

73%

of successful deployments deploy agents primarily to increase efficiency and decrease time spent on manual tasks.

What models, architectures, and techniques are used to build deployed agents?

70%

of successful deployments use off-the-shelf models without weight tuning

How are agents evaluated for deployment?

74%

of successful deployments rely primarily on human-in-the-loop evaluation

What are the top challenges in building deployed agents?

85%

of successful deployments don't see latency as a challenge (minutes is acceptable)  
**Reliability** remains an unsolved challenge.



# Agentic AI: Von der Planung bis zur Produktivschaltung

## Model Architecture & Design

Small vs Large  
Language Models

Commercial vs  
Open-source LLMs

Context engineering &  
Runbooks

LLM Benchmarking:  
Performance, cost, latency

LLM routing & optimization

## Infrastructure & Deployment

Deployment models:  
On-prem vs Cloud

MCP engineering  
(client, server & host)

CI/CD pipelines

Third-party integrations

User experience:  
UI, APIs, SDKs

## Data & Knowledge integration

Embedding model  
& Vector DB selection

Building & fine-tuning RAG

Multi-modal  
input processing

Data lake integrations

Data quality &  
pre-processing

## Agent architecture

Agent framework selection

Agent discovery

Agent hierarchy &  
Multi-agent interactions

Agent guardrails &  
safety policies

Agent benchmarking

Security, Compliance, Data Privacy, Human-In-The-Loop, Observability & Monitoring, Scale & Performance

# Fragen und Diskussion

