Hewlett Packard
Enterprise

Sicherheit im eigenen Netzwerk

Wie kann es mit Hilfe von KI gelingen?

Dr. Łukasz Budzisz, Senior Presales Engineer
CWNE #572, ACX-NS, ACEX #98 (ACMX, ACCX, ACDX)

April 2025

Sicherheit

KOMPLEXITÄT REDUZIEREN

Komplexität erhöht die Fragilität der Infrastruktur. Sie wird anfälliger für Angriffe

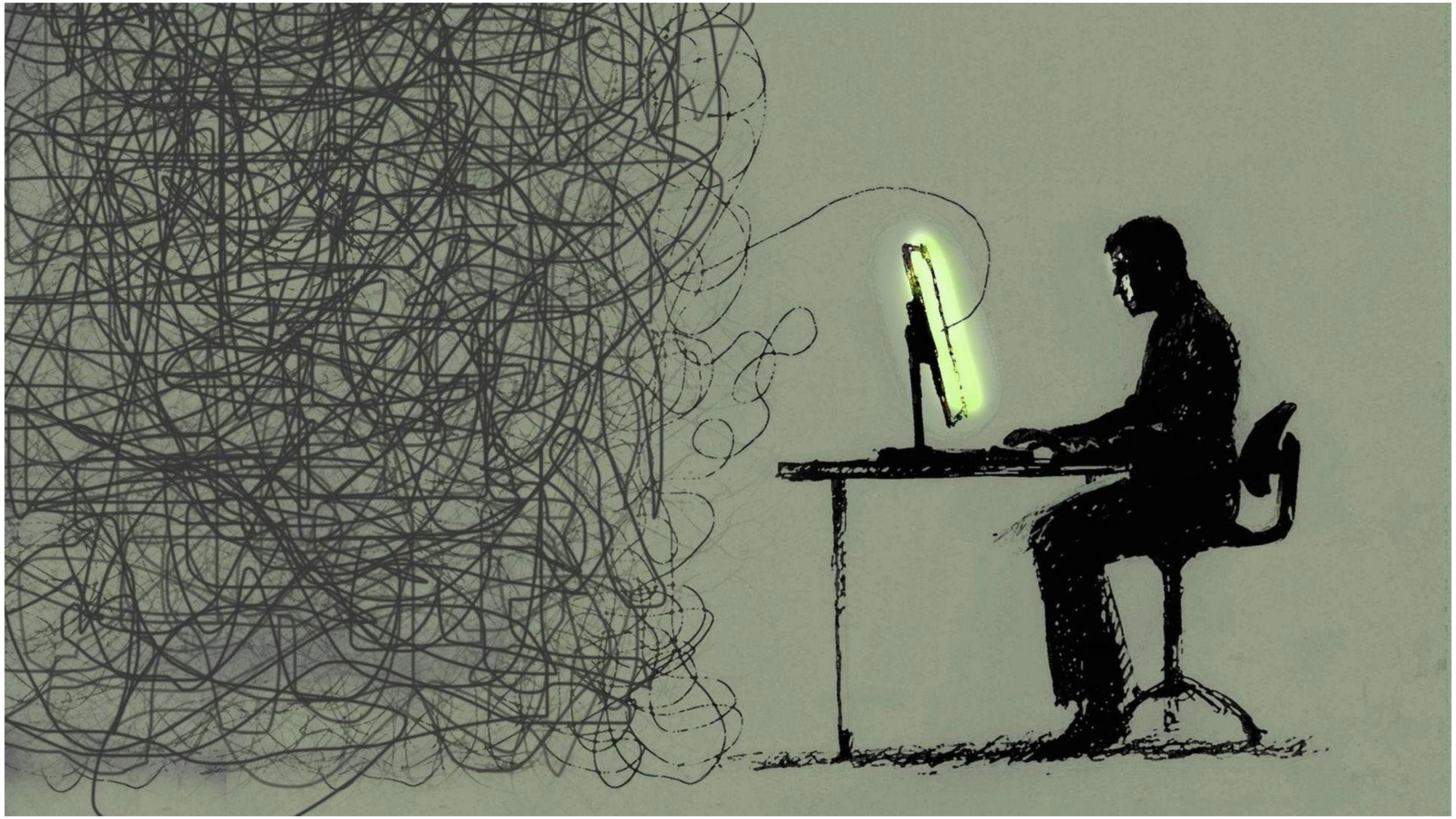
Stand der Technik Security

NIS2, KRITIS & Co fordern Security nach dem **‚Stand der Technik‘** aufzubauen

XLAs statt SLAs

Verfügbarkeit ist eine Säule der Sicherheit. Wenn Applikationen nicht nutzbar sind, verlieren wir Geld.

KOMPLEXITÄT REDUZIEREN



Bundesamt
für Sicherheit in der
Informationstechnik

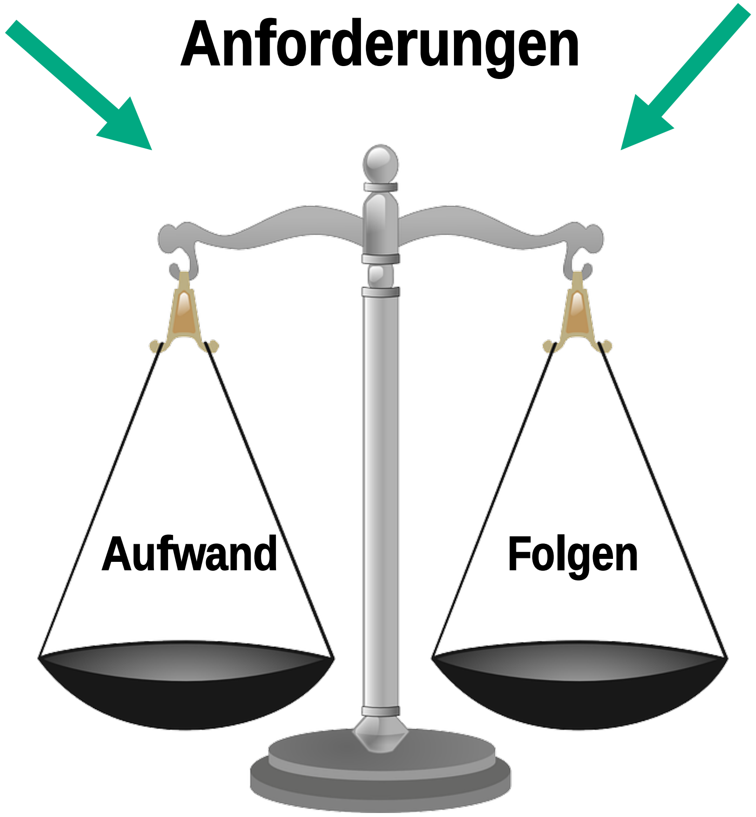
IT-Grundschutz

Frage: Wer hat das BSI Grundschutzkompedium gelesen?
(es sind über 850 Seiten…)

BSI-Grundschutz Kompendium

10 Bausteine

ISMS	Sicherheitsmanagement
ORP	Organisation & Personal
CON	Konzeption & Vorgehensweise
OPS	Betrieb
DER	Detektion und Reaktion
APP	Anwendungen
NET	Netze und Kommunikation
IND	Industrielle IT
INF	Infrastruktur
SYS	IT-Systeme


Anforderungen
Aufwand
Folgen

BSI-Grundschutz Kompendium

Anforderung	Grundschutz Baustein	Lösung
Absicherung des Bootvorgangs	SYS.1.1 Allgemeiner Server	Silicon Root of Trust
Authentisierung an Servern		Compute Ops Management
Systemüberwachung und Monitoring von Servern		HPE GreenLake Cloud

BSI-Grundschutz Kompendium

Anforderung

Netzsegmentierung der VDI-Komponenten

Absicherung eines SANs durch Segmentierung

Client-Server-Segmentierung

Grundschutz Baustein

SYS / NET
(Micro-)Segmentierung

Lösung

CX 10000 Switch
800Gbps Stateful
L4-Firewall (EW traffic)
Data Center Switch

48 x 1GbE/10GbE/25GbE - 6 x 40GbE/100GbE

BSI-Grundschutz Kompendium

Anforderung

Planung des IT-Betriebs unter besonderen Notsituationen

Grundschutz Baustein

OPS
Disaster Recovery

Lösung

Zerto
a Hewlett Packard Enterprise company

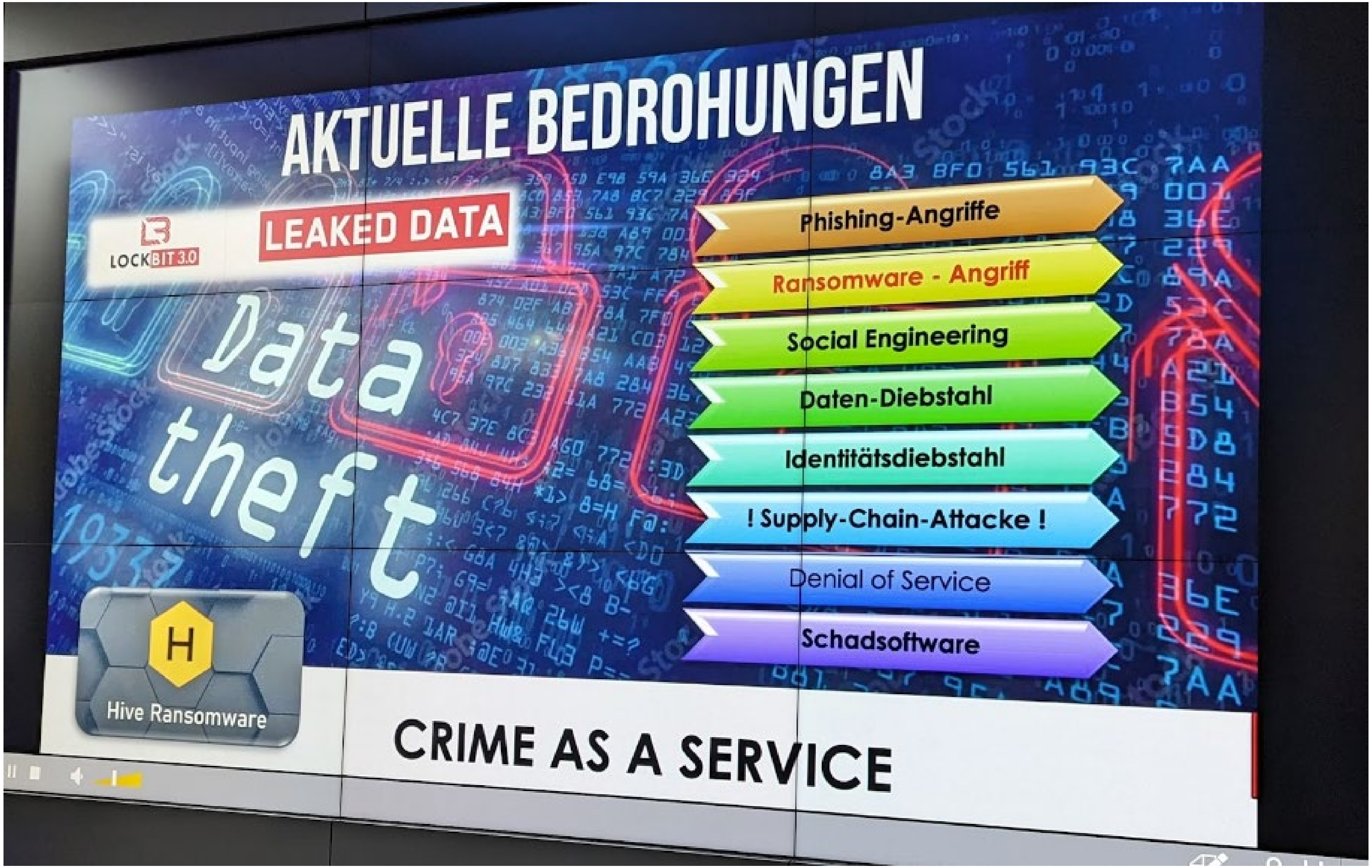
Ransomware Resilience

Disaster Recovery

Continuous Data Protection
Any App, Any Data & Any Cloud

Aber jetzt kommen wir zur Infrastruktur…

Wie die Welt heute aussieht... (von Daniel Lorch)



LOCKBIT 3.0
LEAKED DATA
Data theft
Hive Ransomware

AKTUELLE BEDROHUNGEN

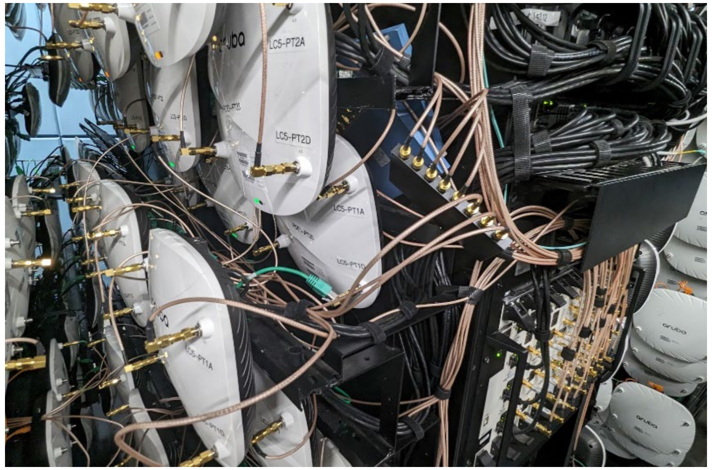
- Phishing-Angriffe
- Ransomware - Angriff
- Social Engineering
- Daten-Diebstahl
- Identitätsdiebstahl
- ! Supply-Chain-Attacke !
- Denial of Service
- Schadsoftware

CRIME AS A SERVICE

Kunden
Herausforderungen

Wie gut ist das WLAN?

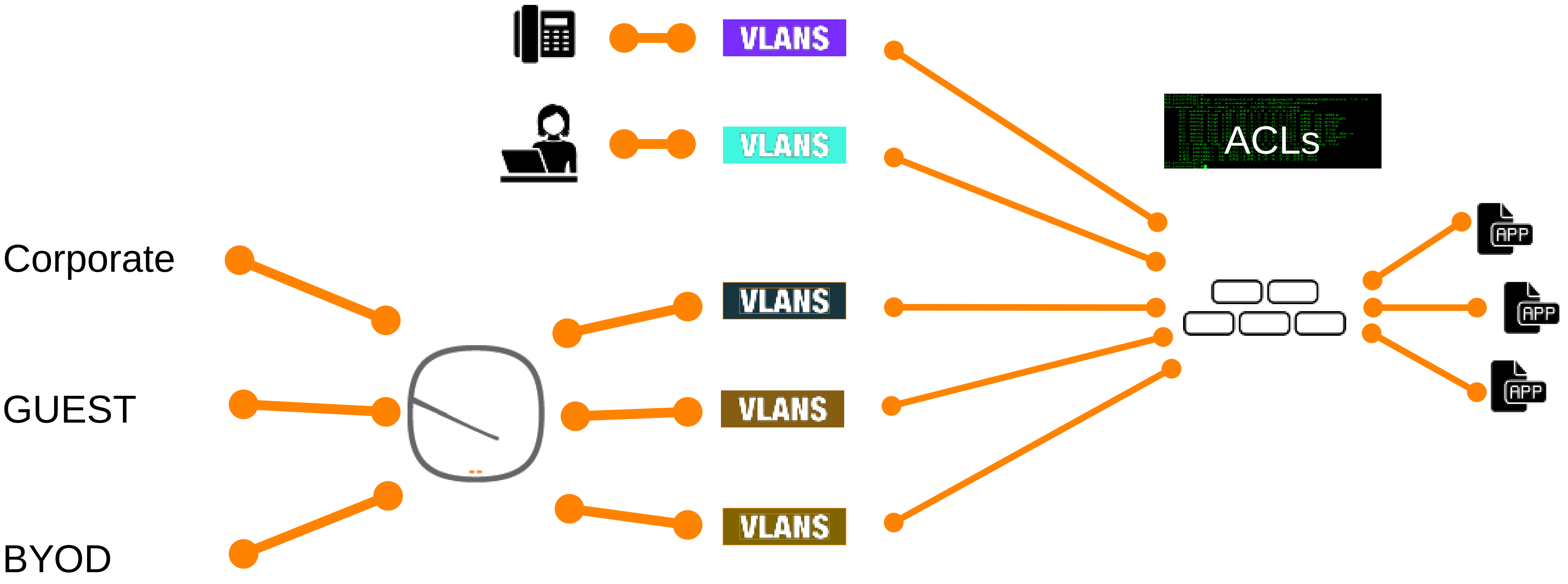
Komplexe Administration



Sicherheits – Bedenken

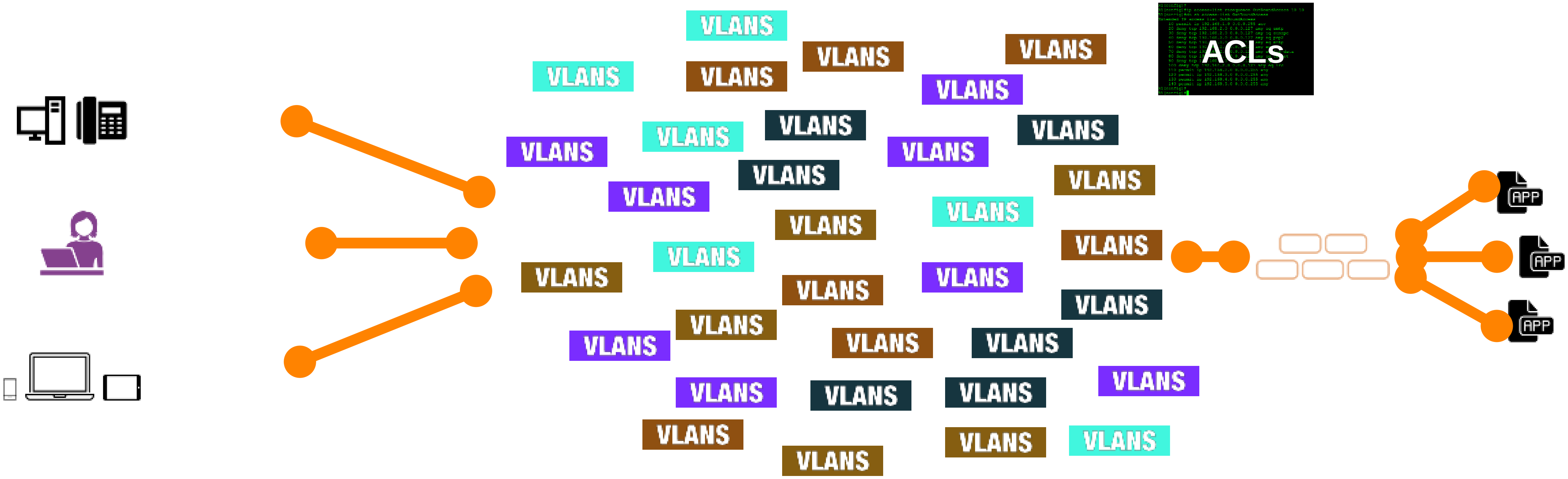
1. Frage:
Wissen Sie zu 100%, was in Ihrem Netzwerk ist?

Wie alles begann...


VLANS
VLANS
ACLs
Corporate
VLANS
APP
APP
GUEST
VLANS
APP
BYOD
VLANS

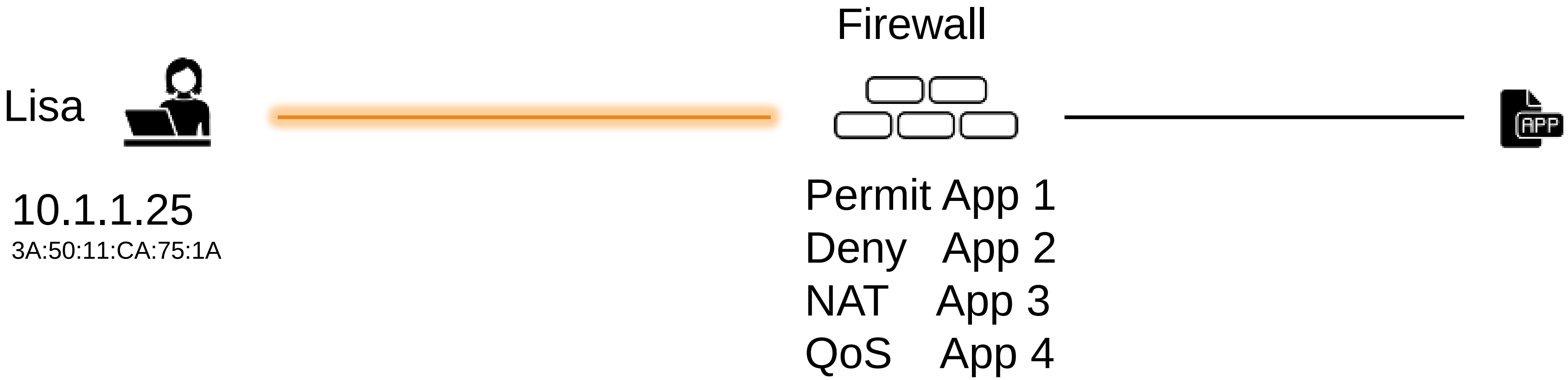
Skalierung und Segmentierung bringt

KOMPLEXITÄT


VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
VLANS
ACLs
APP
APP
APP

2. Frage:
Was darf jede IP-Adresse im Netzwerk tun?

Über VLANs zum Anwender



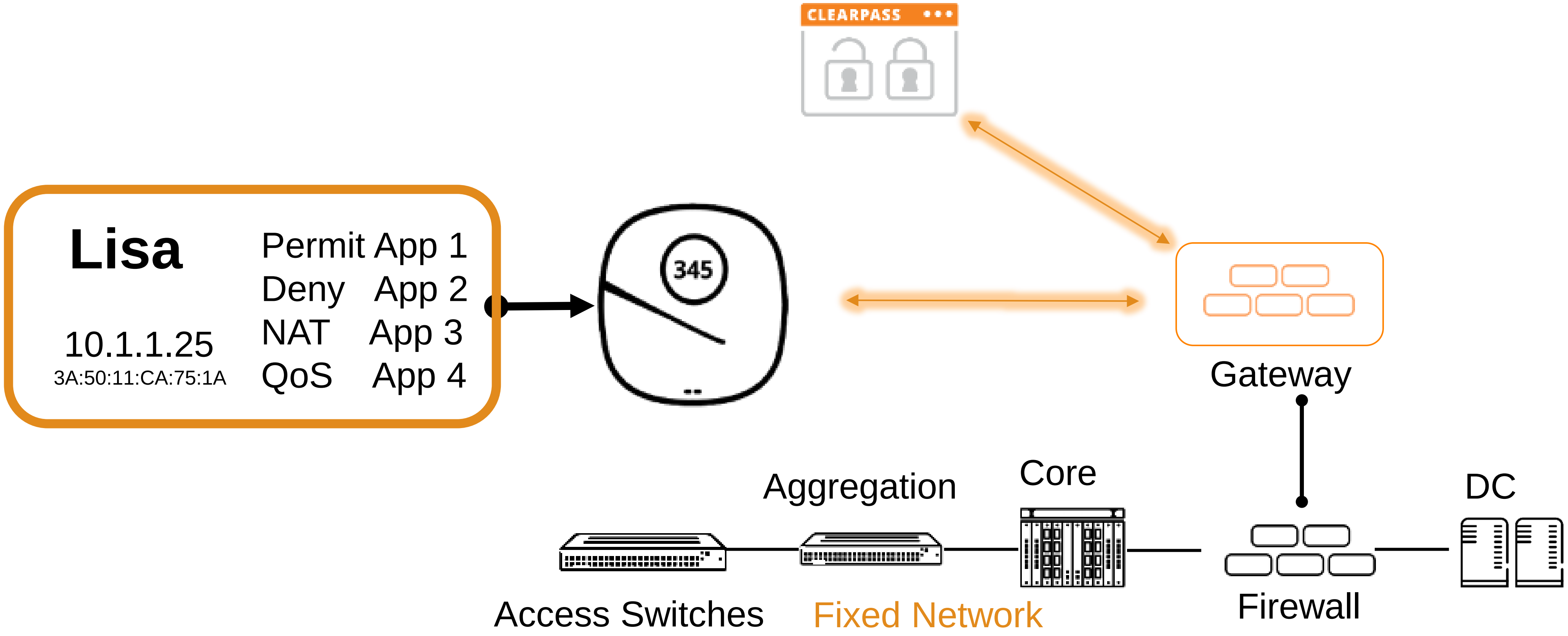
Firewall

Lisa

10.1.1.25
3A:50:11:CA:75:1A

Permit	App 1
Deny	App 2
NAT	App 3
QoS	App 4

Erste personalisierte Firewall



Lisa

10.1.1.25
3A:50:11:CA:75:1A

Permit	App 1
Deny	App 2
NAT	App 3
QoS	App 4

Gateway

Aggregation

Core

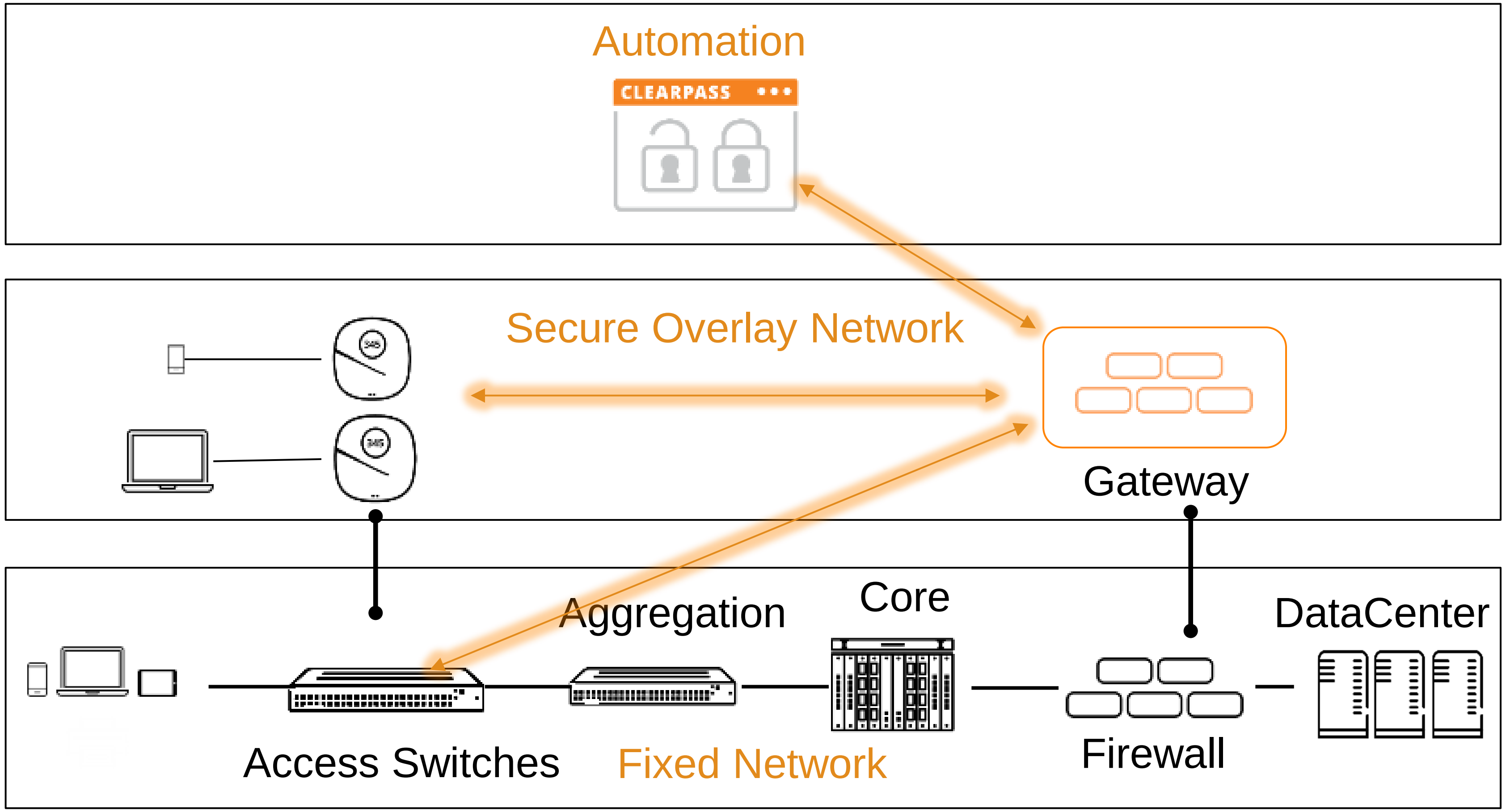
DC

Access Switches

Fixed Network

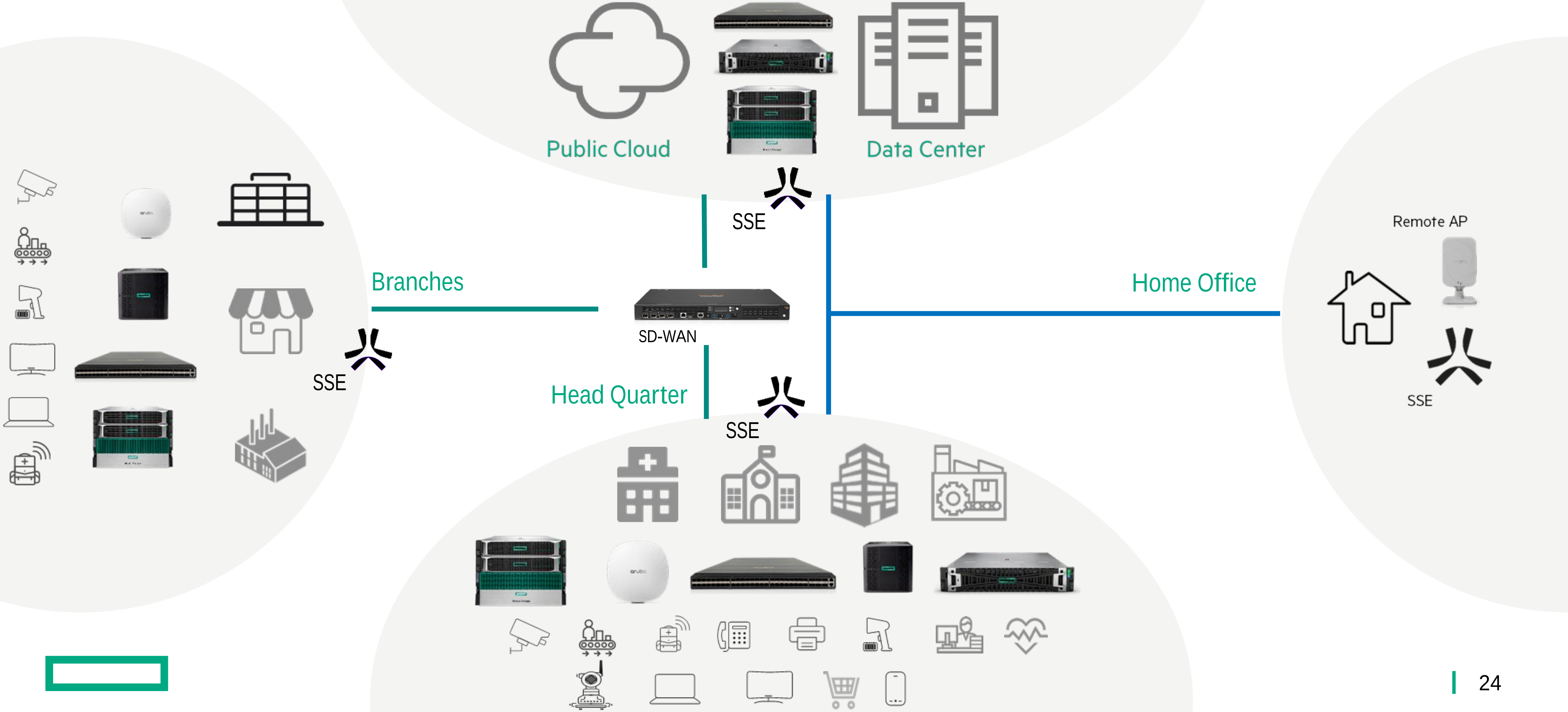
Firewall

Evolution der Architektur im Access


Automation
CLEARPASS
Secure Overlay Network
Gateway
Aggregation
Core
DataCenter
Access Switches
Fixed Network
Firewall

3. Frage:
Wie kann ich ein Regelwerk durch Policies im Netzwerk durchsetzen?

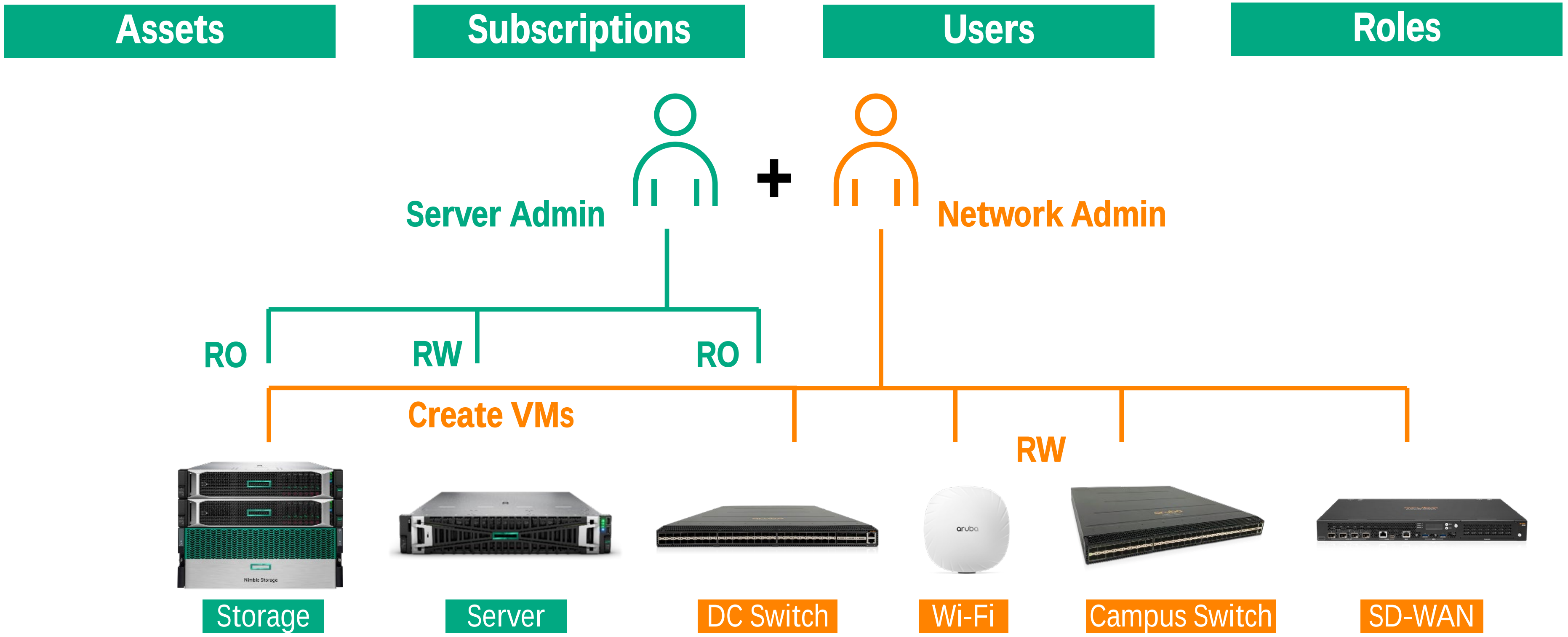
IT Infrastruktur ist komplex


Public Cloud
Data Center
SSE
Branches
SD-WAN
SSE
Head Quarter
SSE
Remote AP
Home Office
SSE

Komplexität reduzieren

HPE GreenLake

Sicherheitsmechanismen an einem Ort



Assets | **Subscriptions** | **Users** | **Roles**

Server Admin + Network Admin

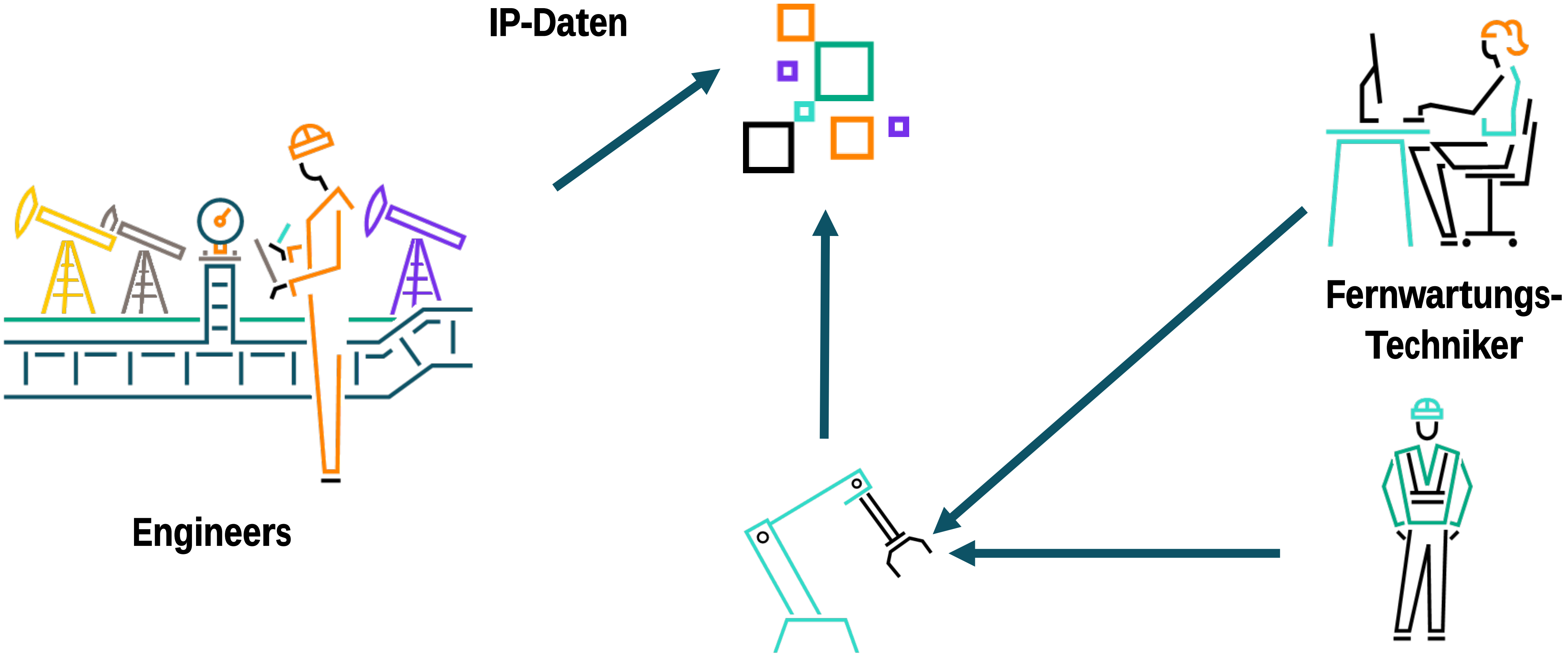
RO
RW
RO
Create VMs
RW

Storage
Server
DC Switch
Wi-Fi
Campus Switch
SD-WAN

Sicherheitsziel:

Intellectual Property (IP) Daten müssen geschützt werden

IP-Daten müssen geschützt werden



IP-Daten

Engineers

Fernwartungs-Techniker

Techniker

Ind. Device

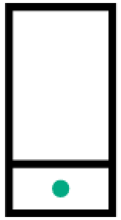
Visibilität & Authentifizierung

CLEARPASS
POLICY MANAGER

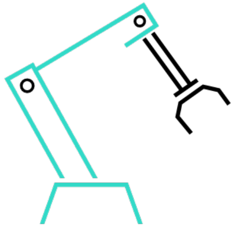
Central

Rolle
Engineer

Rolle
Techniker



Rolle
VoIP



Rolle
Robot

Zuweisung von Rechten

Rolle Engineer

HTTPS → IP-Daten ✓
Internet * → Je nach Policy ✓
Alles Andere ✗

Rolle Techniker

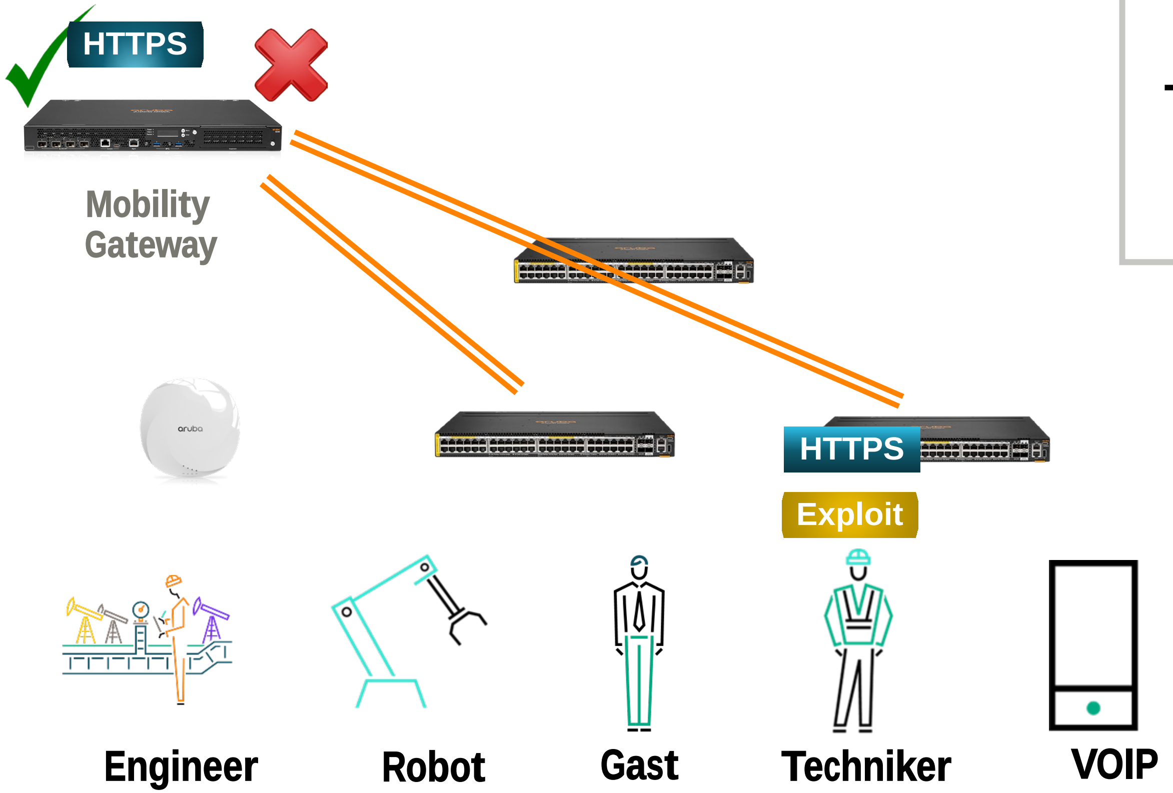
HTTPS, SSH → Rolle Robot ✓
Internet * → Je nach Policy ✓
Alles Andere ✗

Rolle Robot

HTTPS → Ind. Server ✓
SFTP → Firmware Upgrade ✓
Alles Andere ✗

Mikrosegmentierung

Dynamic Segmentation


HTTPS
✓
✗
Mobility Gateway
HTTPS
Exploit
Engineer
Robot
Gast
Techniker
VOIP

Role
Techniker

HTTPS, SSH → Rolle Robot ✓
Internet → Nach Policy ✓
All Traffic → All Destinations ✗

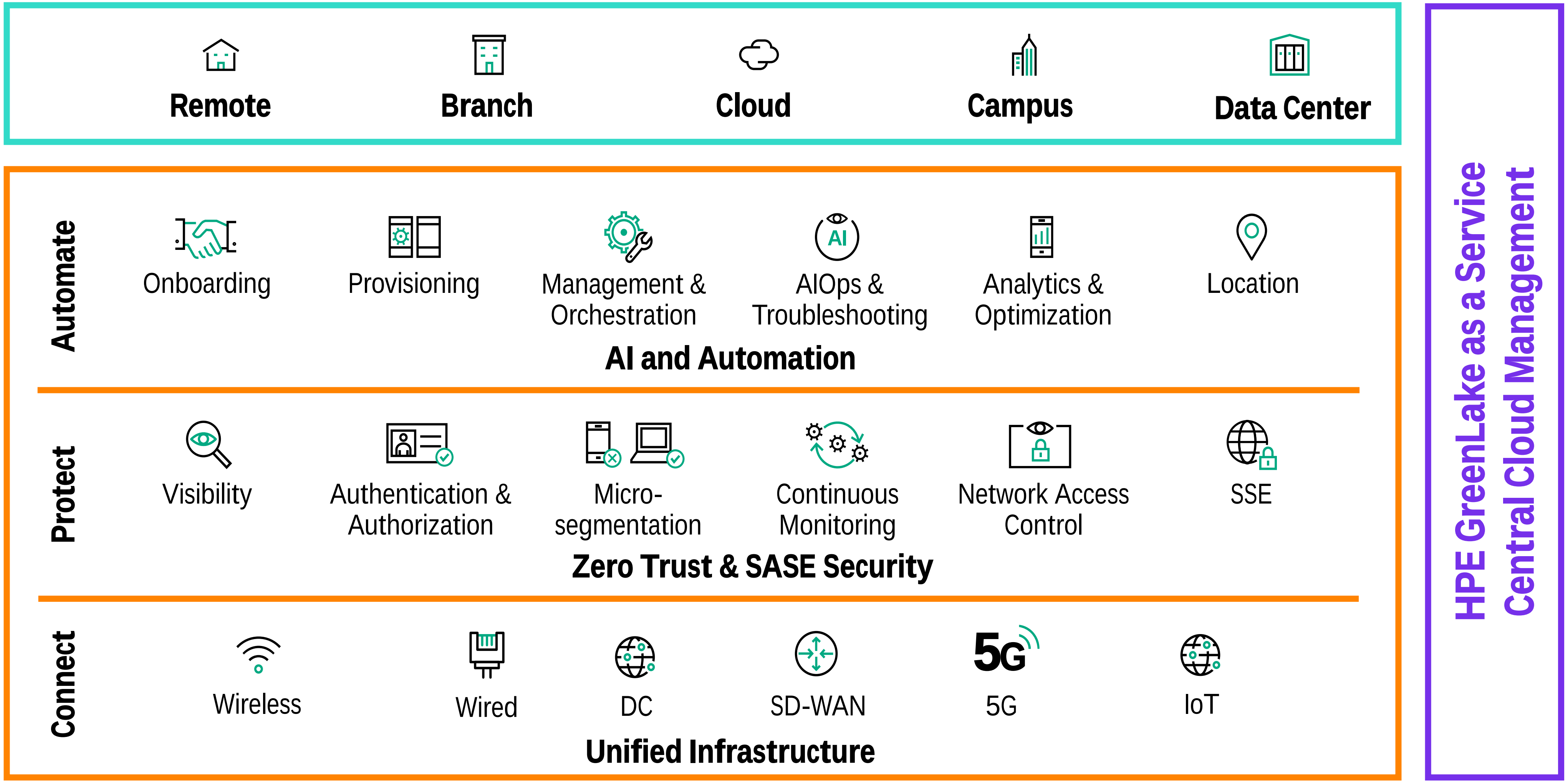
1. Wissen Sie zu 100%, was in Ihrem Netzwerk ist?

2. Was darf jede IP-Adresse im Netzwerk tun?

3. Wie kann ich ein Regelwerk durch Policies im Netzwerk durchsetzen?

Was brauche ich noch?

EDGE SERVICES PLATTFORM ARCHITEKTUR



Remote | **Branch** | **Cloud** | **Campus** | **Data Center**

Automate

- Onboarding
- Provisioning
- Management & Orchestration
- AIOps & Troubleshooting
- Analytics & Optimization
- Location

AI and Automation

Protect

- Visibility
- Authentication & Authorization
- Micro-segmentation
- Continuous Monitoring
- Network Access Control
- SSE

Zero Trust & SASE Security

Connect

- Wireless
- Wired
- DC
- SD-WAN
- 5G
- IoT

Unified Infrastructure

HPE GreenLake as a Service
Central Cloud Management

Und wo ist die KI?

Umfangreiche, relevante und vielfältige Daten: Das Fundament der KI

Branchenführender Data Lake

~4.7
Million
Komponenten[1]

~1.6
Milliarden
Endgeräte[1]

30+
Industrie
verticals

250K
Kunden in
AMS, EMEA, APJC

Wie hilft ein Data Lake?

UNCOVER INSIGHTS AND TRENDS

RECEIVE OPTIMIZATION TIPS

POWER & CONSTANTLY TRAIN AI/ML MODELS

---

[1] HPE Aruba Networks Intros GenAI Trained On Networking Giant's Own 'Massive' Data Lake

EDGE SERVICES PLATTFORM ARCHITEKTUR

Remote **Branch** **Cloud** **Campus** **Data Center**

Automate

- Onboarding
- Provisioning
- Management & Orchestration
- AIOps & Troubleshooting
- Analytics & Optimization
- Location

AI and Automation

Protect

- Visibility
- Authentication & Authorization
- Micro-segmentation
- Continuous Monitoring
- Network Access Control
- SSE

Zero Trust & SASE Security

Connect

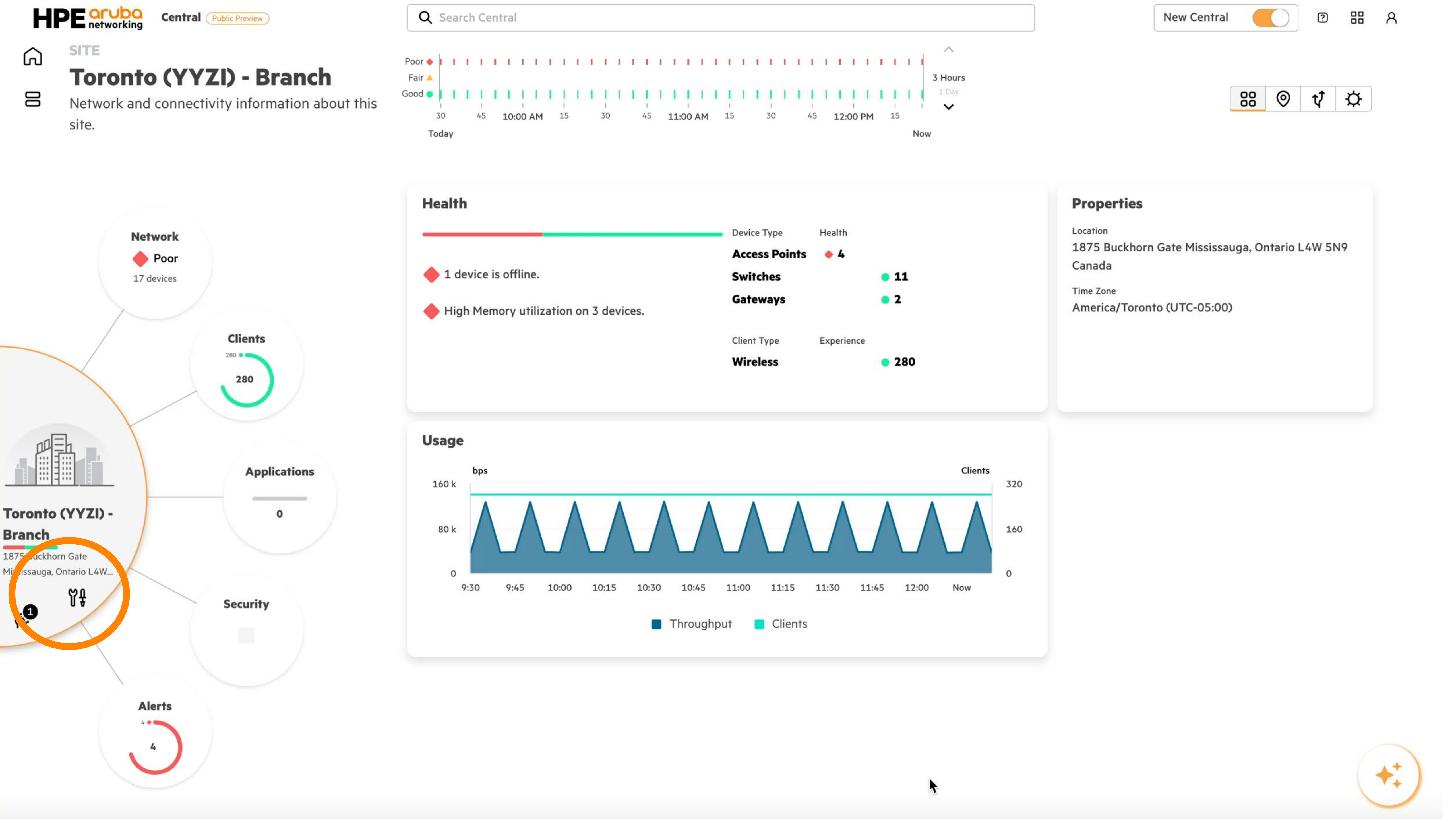
- Wireless
- Wired
- DC
- SD-WAN
- 5G
- IoT

Unified Infrastructure

HPE GreenLake as a Service
Central Cloud Management

KI im Einsatz

Demo


HPE aruba networking
Central
Public Preview
Search Central
New Central
Poor
Fair
Good
30
45
10:00 AM
15
30
45
11:00 AM
15
30
45
12:00 PM
15
Today
Now
3 Hours
1 Day
Network
Poor
17 devices
Clients
280
280
Applications
0
Security
Alerts
4
4
1

SITE

Toronto (YYZI) - Branch

Network and connectivity information about this site.

Toronto (YYZI) - Branch

1875 Buckhorn Gate Mississauga, Ontario L4W...

Health

1 device is offline.

High Memory utilization on 3 devices.

Device Type	Health
Access Points	4
Switches	11
Gateways	2

Client Type	Experience
Wireless	280

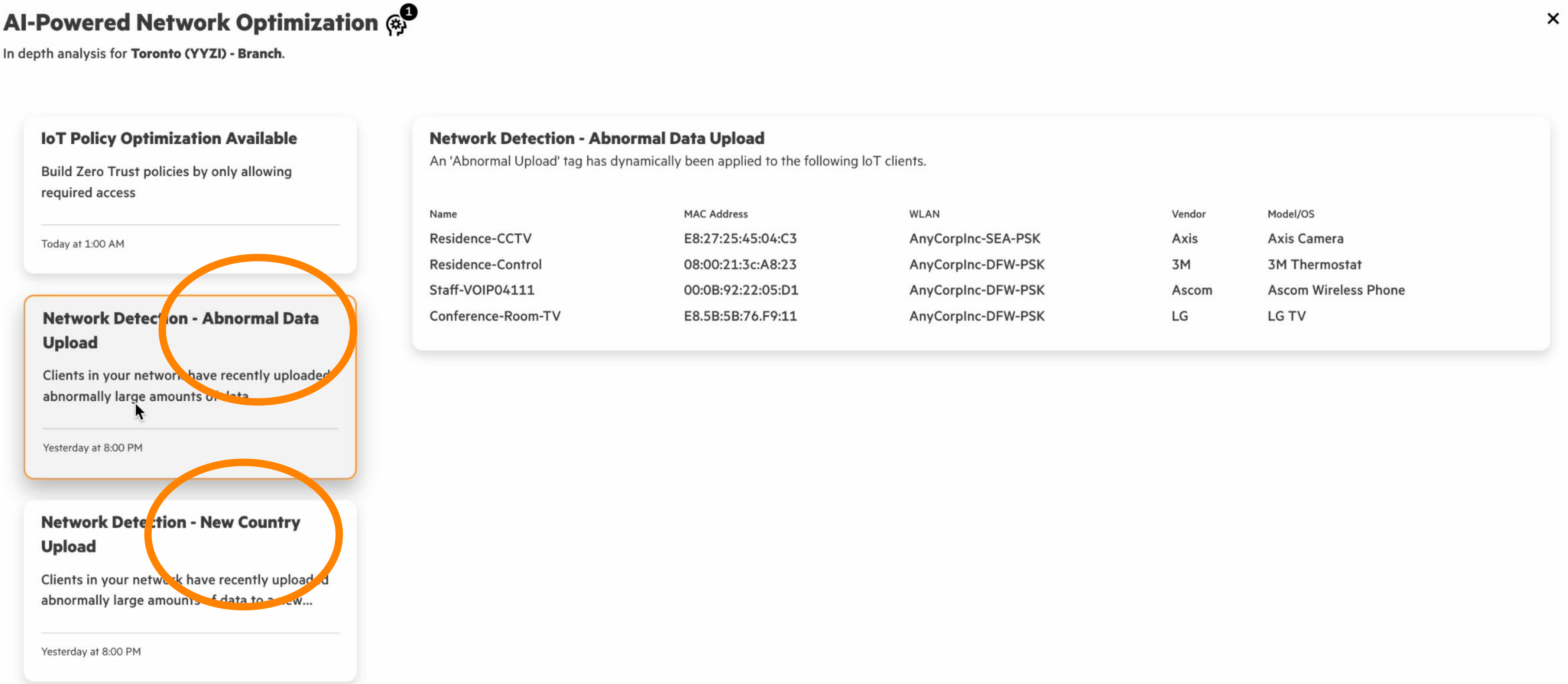
Properties

Location
1875 Buckhorn Gate Mississauga, Ontario L4W 5N9 Canada

Time Zone
America/Toronto (UTC-05:00)

Usage

bps
Clients
160 k
80 k
0
320
160
0
9:30
9:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
11:45
12:00
Now
Throughput
Clients



AI-Powered Network Optimization

In depth analysis for **Toronto (YYZI) - Branch**.

IoT Policy Optimization Available

Build Zero Trust policies by only allowing required access

Today at 1:00 AM

Network Detection - Abnormal Data Upload

Clients in your network have recently uploaded abnormally large amounts of data.

Yesterday at 8:00 PM

Network Detection - New Country Upload

Clients in your network have recently uploaded abnormally large amounts of data to a new...

Yesterday at 8:00 PM

Network Detection - Abnormal Data Upload

An 'Abnormal Upload' tag has dynamically been applied to the following IoT clients.

Name	MAC Address	WLAN	Vendor	Model/OS
Residence-CCTV	E8:27:25:45:04:C3	AnyCorpInc-SEA-PSK	Axis	Axis Camera
Residence-Control	08:00:21:3c:A8:23	AnyCorpInc-DFW-PSK	3M	3M Thermostat
Staff-VOIP04111	00:0B:92:22:05:D1	AnyCorpInc-DFW-PSK	Ascom	Ascom Wireless Phone
Conference-Room-TV	E8.5B:5B:76.F9:11	AnyCorpInc-DFW-PSK	LG	LG TV

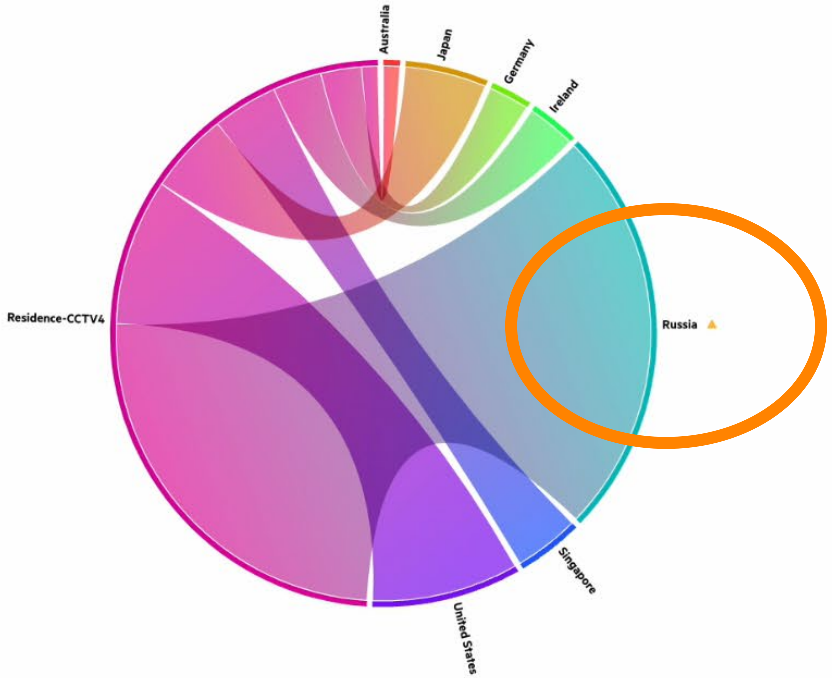
Network Detection - New Country Upload

×

An 'New Country Upload' tag has dynamically been applied to **'Residence-CCTV4'**. This client uploaded **11.09 GB to Russia** on **February 23, 2025 12:30 PM**, compared with an average of **0 MB** uploaded daily during the past **30** days.

Behavior Mapping

Visualizes historical traffic and highlights anomalies.



Country Uploads

Records per-country activity once the baseline threshold is exceeded.

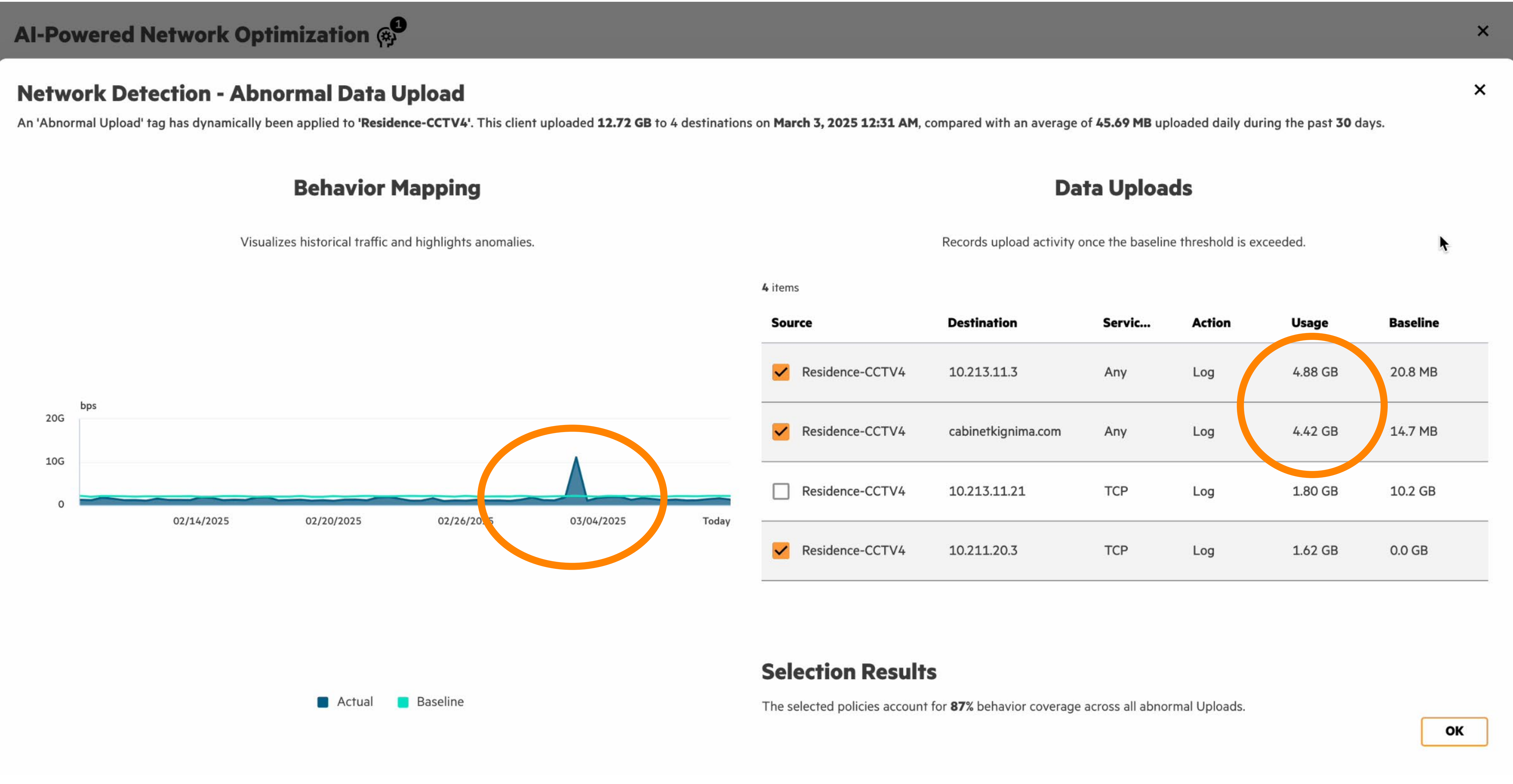
1 item

Source	Destination	Service /...	Action	Usage	Baseline
☑ Residence-CCTV4	russia	Any	-	11.09 GB	0 MB

Selection Results

The selected policies account for **100%** behavior coverage across all new country uploads.

OK


AI-Powered Network Optimization
1
✕
✕
bps
20G
10G
0
02/14/2025
02/20/2025
02/26/2025
03/04/2025
Today
OK

Network Detection - Abnormal Data Upload

An 'Abnormal Upload' tag has dynamically been applied to **'Residence-CCTV4'**. This client uploaded **12.72 GB** to 4 destinations on **March 3, 2025 12:31 AM**, compared with an average of **45.69 MB** uploaded daily during the past **30** days.

Behavior Mapping

Visualizes historical traffic and highlights anomalies.

■ Actual ■ Baseline

Data Uploads

Records upload activity once the baseline threshold is exceeded.

4 items

	Source	Destination	Servic...	Action	Usage	Baseline
☑	Residence-CCTV4	10.213.11.3	Any	Log	4.88 GB	20.8 MB
☑	Residence-CCTV4	cabinetkignima.com	Any	Log	4.42 GB	14.7 MB
☐	Residence-CCTV4	10.213.11.21	TCP	Log	1.80 GB	10.2 GB
☑	Residence-CCTV4	10.211.20.3	TCP	Log	1.62 GB	0.0 GB

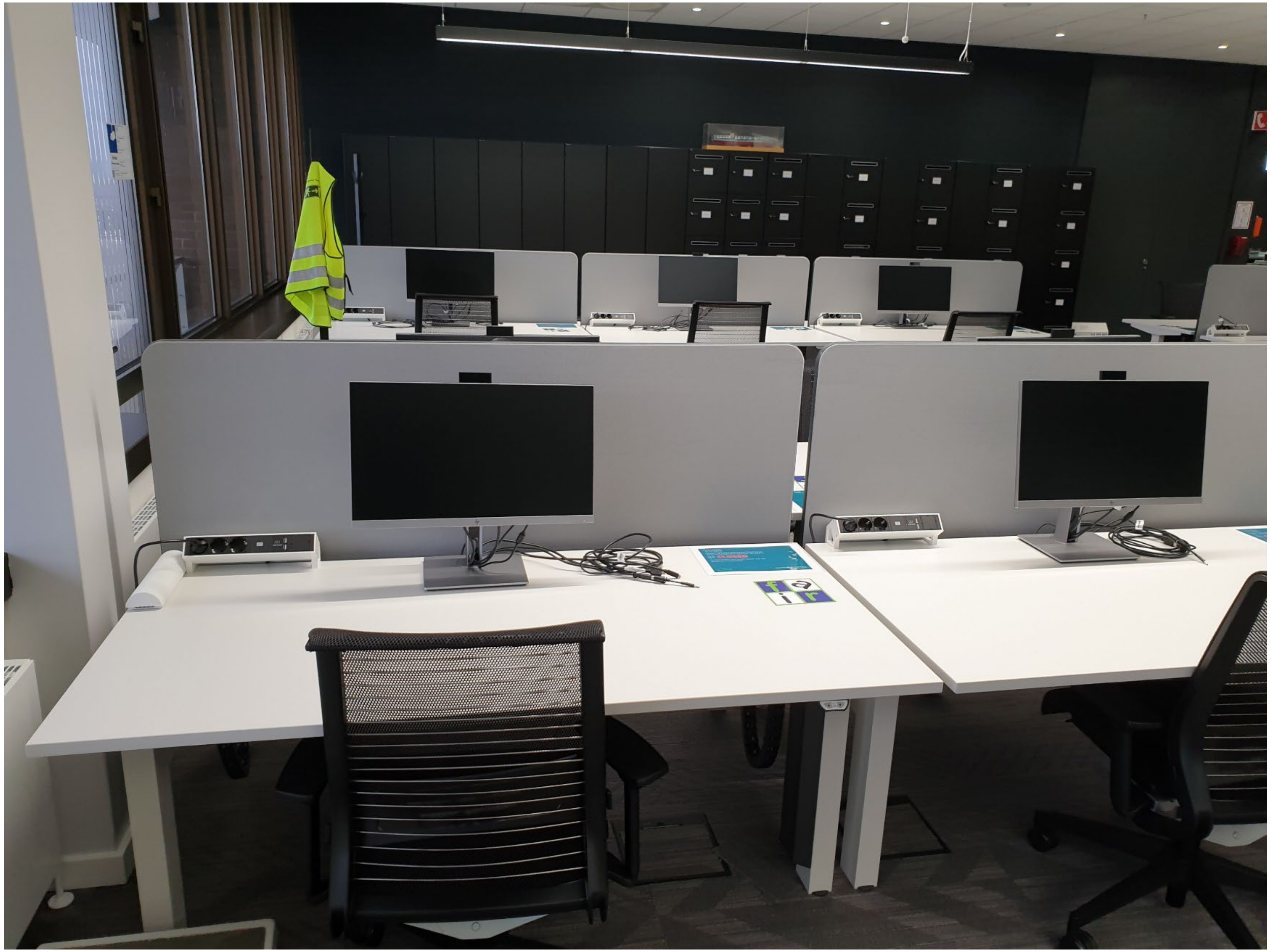
Selection Results

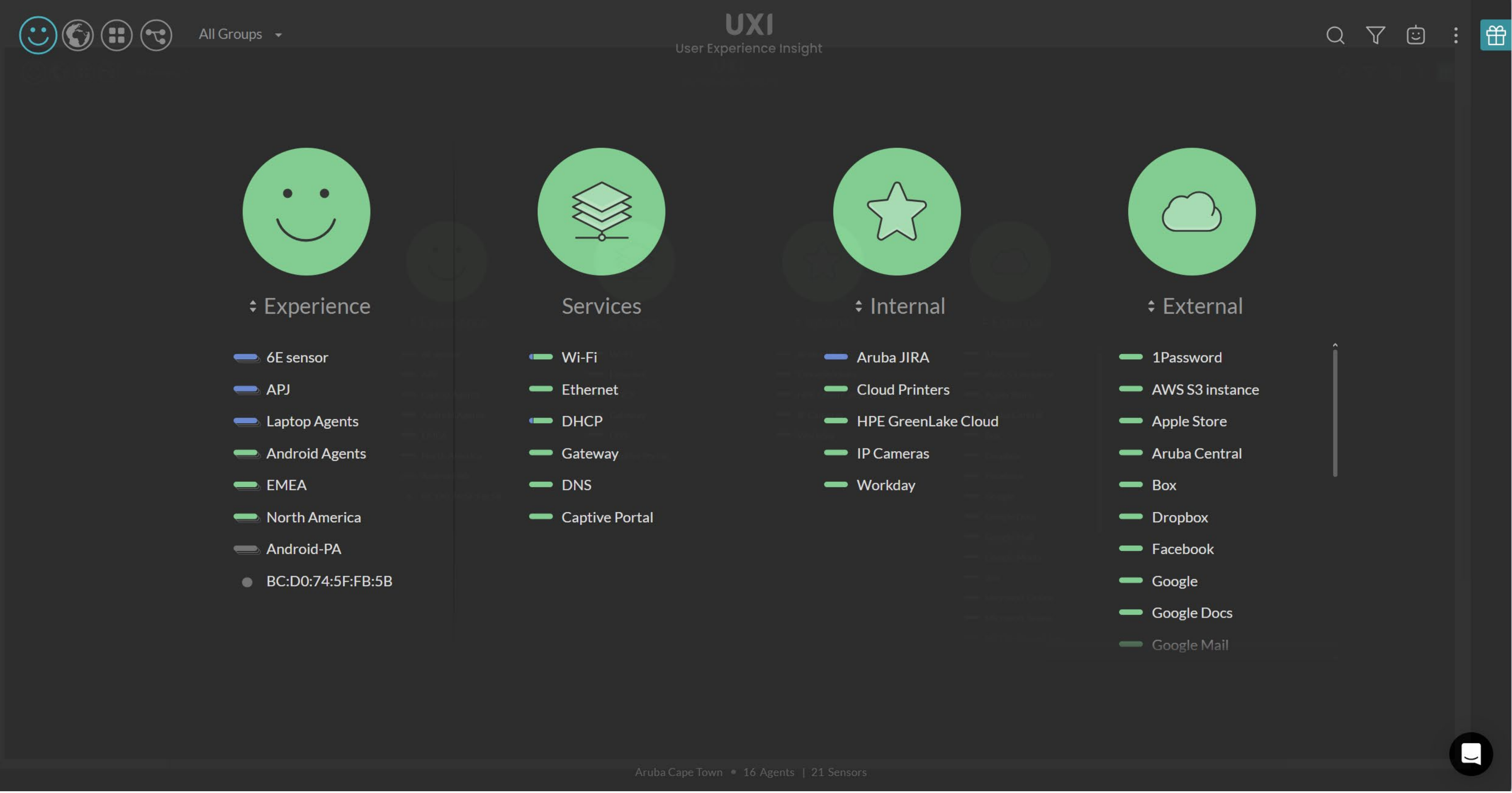
The selected policies account for **87%** behavior coverage across all abnormal Uploads.

XLAs statt SLAs

Service Assurance: User eXperience Insight (UXI)

Finde den Sensor...!





UXI
User Experience Insight

All Groups

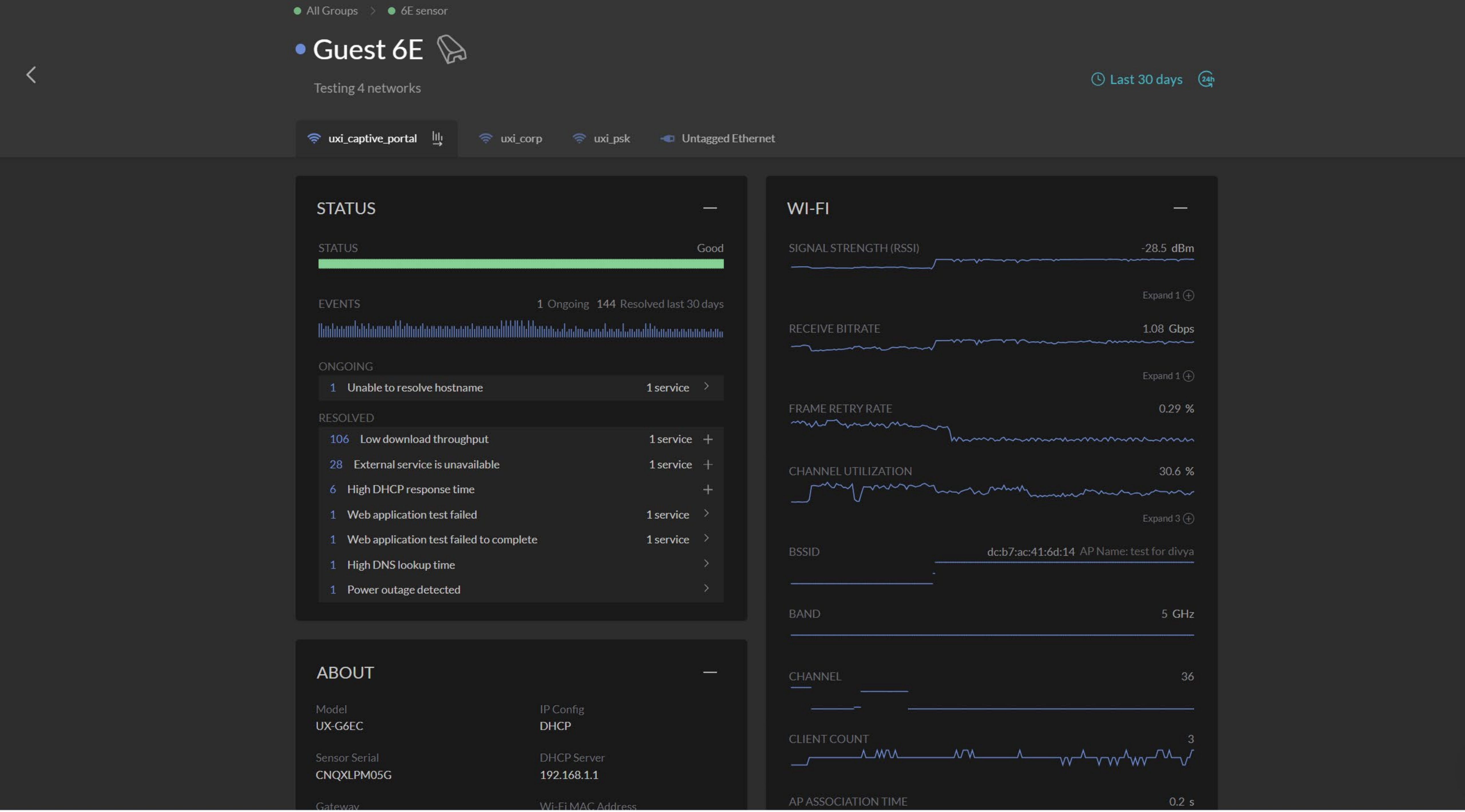
Experience
- 6E sensor
- APJ
- Laptop Agents
- Android Agents
- EMEA
- North America
- Android-PA
- BC:D0:74:5F:FB:5B

Services
- Wi-Fi
- Ethernet
- DHCP
- Gateway
- DNS
- Captive Portal

Internal
- Aruba JIRA
- Cloud Printers
- HPE GreenLake Cloud
- IP Cameras
- Workday

External
- 1Password
- AWS S3 instance
- Apple Store
- Aruba Central
- Box
- Dropbox
- Facebook
- Google
- Google Docs
- Google Mail

Aruba Cape Town • 16 Agents | 21 Sensors



All Groups > 6E sensor

Guest 6E

Testing 4 networks

Last 30 days

STATUS

STATUS Good

EVENTS 1 Ongoing 144 Resolved last 30 days

ONGOING

1	Unable to resolve hostname	1 service

RESOLVED

106	Low download throughput	1 service
28	External service is unavailable	1 service
6	High DHCP response time	
1	Web application test failed	1 service
1	Web application test failed to complete	1 service
1	High DNS lookup time	
1	Power outage detected	

ABOUT

Model
UX-G6EC

IP Config
DHCP

Sensor Serial
CNQXLPM05G

DHCP Server
192.168.1.1

Gateway

Wi-Fi MAC Address

WI-FI

SIGNAL STRENGTH (RSSI) -28.5 dBm

RECEIVE BITRATE 1.08 Gbps

FRAME RETRY RATE 0.29 %

CHANNEL UTILIZATION 30.6 %

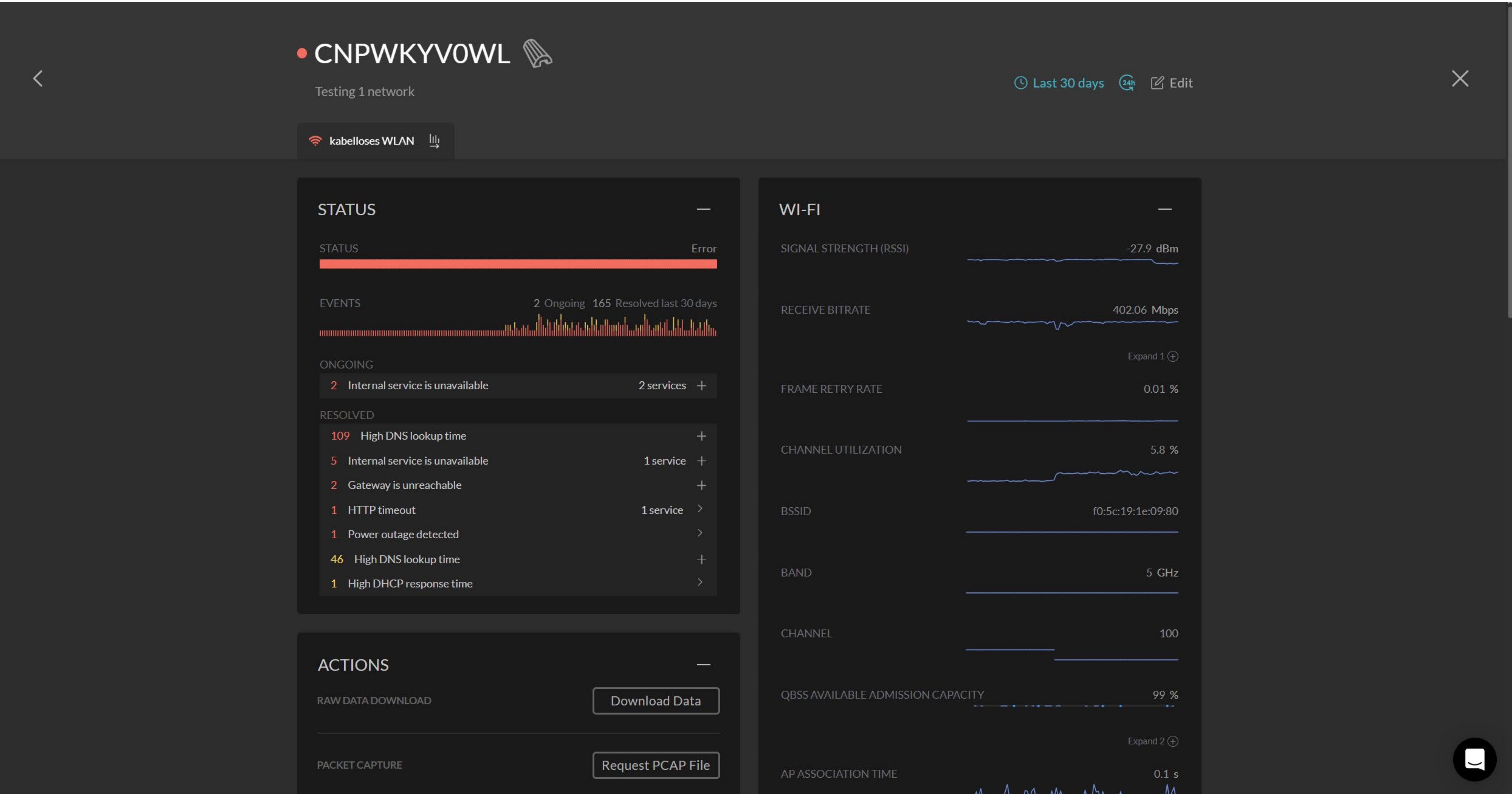
BSSID dc:b7:ac:41:6d:14 AP Name: test for divya

BAND 5 GHz

CHANNEL 36

CLIENT COUNT 3

AP ASSOCIATION TIME 0.2 s



CNPWKYV0WL

Testing 1 network

Last 30 days Edit

kabelloses WLAN

STATUS

STATUS Error

EVENTS 2 Ongoing 165 Resolved last 30 days

ONGOING

2	Internal service is unavailable	2 services	+

RESOLVED

109	High DNS lookup time		+
5	Internal service is unavailable	1 service	+
2	Gateway is unreachable		+
1	HTTP timeout	1 service	>
1	Power outage detected		>
46	High DNS lookup time		+
1	High DHCP response time		>

ACTIONS

RAW DATA DOWNLOAD Download Data

PACKET CAPTURE Request PCAP File

WI-FI

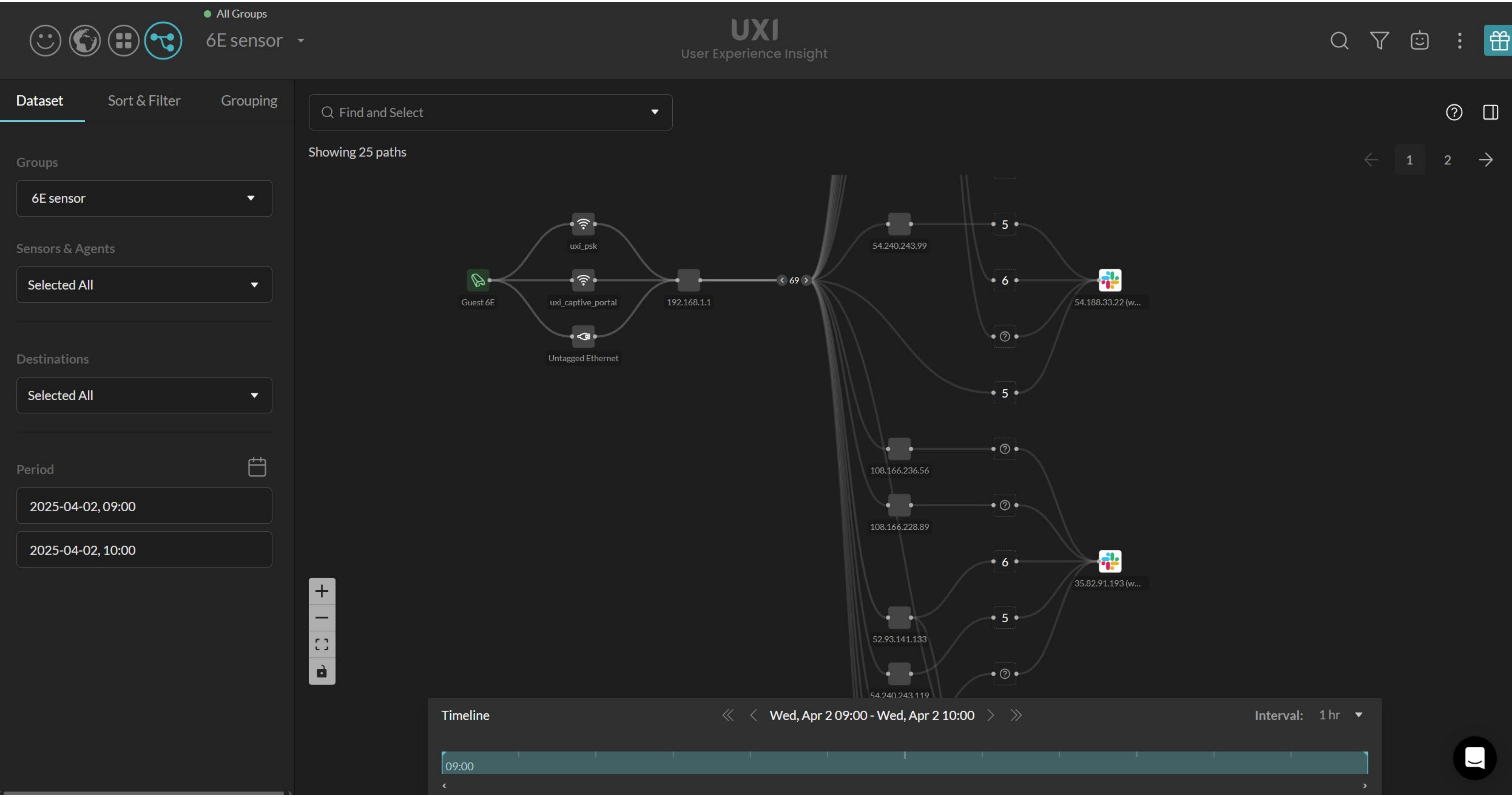
SIGNAL STRENGTH (RSSI)	-27.9 dBm
RECEIVE BITRATE	402.06 Mbps

Expand 1 ⊕

FRAME RETRY RATE	0.01 %
CHANNEL UTILIZATION	5.8 %
BSSID	f0:5c:19:1e:09:80
BAND	5 GHz
CHANNEL	100
QBSS AVAILABLE ADMISSION CAPACITY	99 %

Expand 2 ⊕

AP ASSOCIATION TIME	0.1 s



All Groups

6E sensor

UXI

User Experience Insight

Dataset | Sort & Filter | Grouping

Groups: 6E sensor

Sensors & Agents: Selected All

Destinations: Selected All

Period

2025-04-02, 09:00

2025-04-02, 10:00

Find and Select

Showing 25 paths

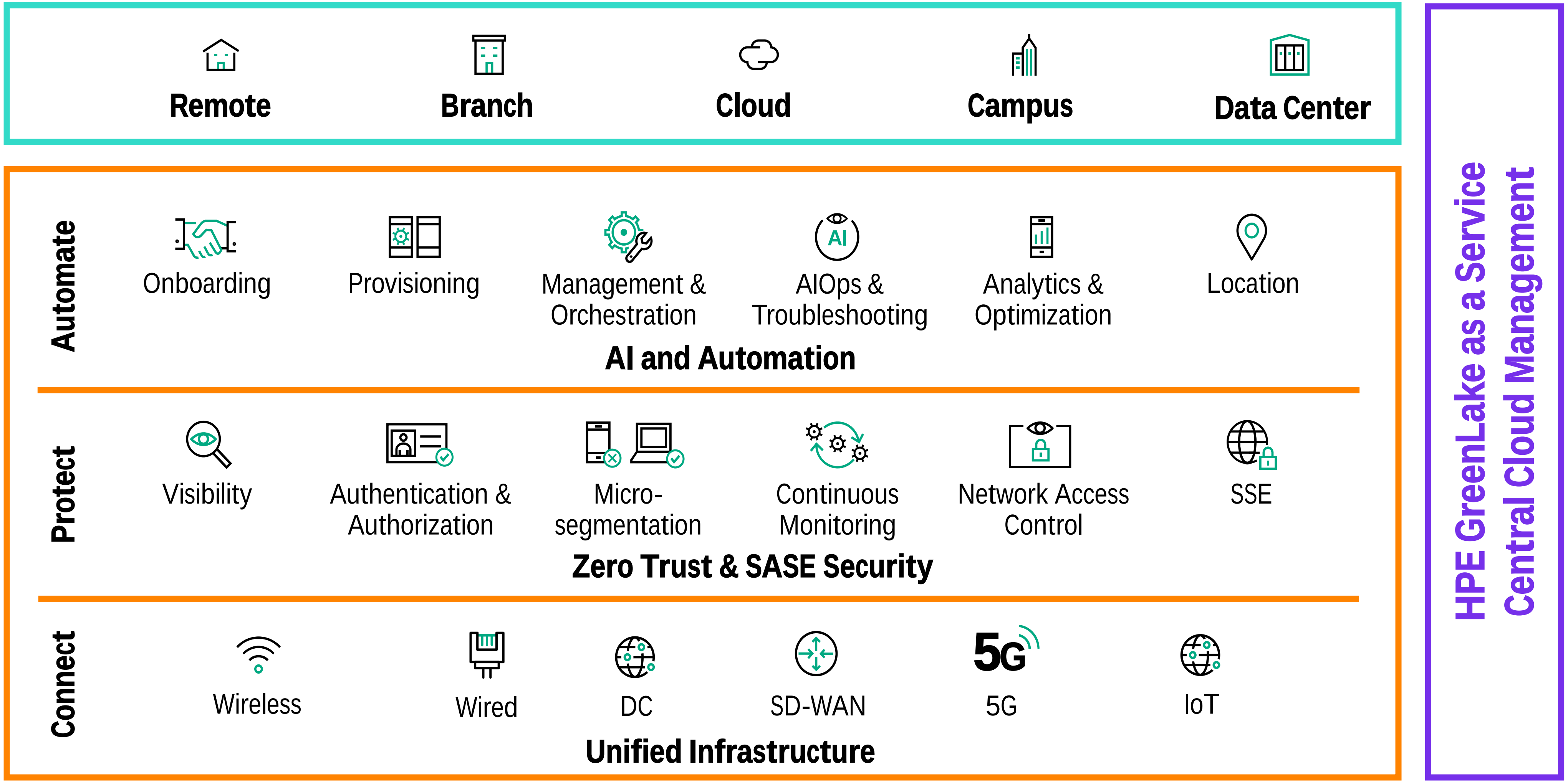
Timeline

Wed, Apr 2 09:00 - Wed, Apr 2 10:00

Interval: 1 hr

1
2
Guest 6E
uxi_psk
uxi_captive_portal
Untagged Ethernet
192.168.1.1
69
54.240.243.99
108.166.236.56
108.166.228.89
52.93.141.133
54.240.243.119
5
6
?
5
?
?
6
5
?
54.188.33.22 (w...
35.82.91.193 (w...
09:00

EDGE SERVICES PLATTFORM ARCHITEKTUR



Remote | **Branch** | **Cloud** | **Campus** | **Data Center**

Automate

- Onboarding
- Provisioning
- Management & Orchestration
- AIOps & Troubleshooting
- Analytics & Optimization
- Location

AI and Automation

Protect

- Visibility
- Authentication & Authorization
- Micro-segmentation
- Continuous Monitoring
- Network Access Control
- SSE

Zero Trust & SASE Security

Connect

- Wireless
- Wired
- DC
- SD-WAN
- 5G
- IoT

Unified Infrastructure

HPE GreenLake as a Service
Central Cloud Management

Zusammenfassung

ü **HPE Green Lake, eine Plattform, um die gesamte IT-Infrastruktur im Griff zu haben**

ü **BSI-konforme ‚Stand der Technik‘ IT-Infrastruktur mit HPE bauen**

ü **Sicherheit erhöhen und Kosten senken im Data Center**

ü **HPE Aruba Central, mehr Sicherheit im Netzwerk**

ü **360° Applikationsvisibilität**

Vielen Dank!

lukasz@hpe.com