



Zero Trust beginnt im

 Kopf

Wie sieht es in Ihrem Netzwerk aus?

2025 Reimagine
GERMANY

Christian Schulmeister

Technical Solutions Architect - CyberSecurity

CISSP

September 2022

Agenda

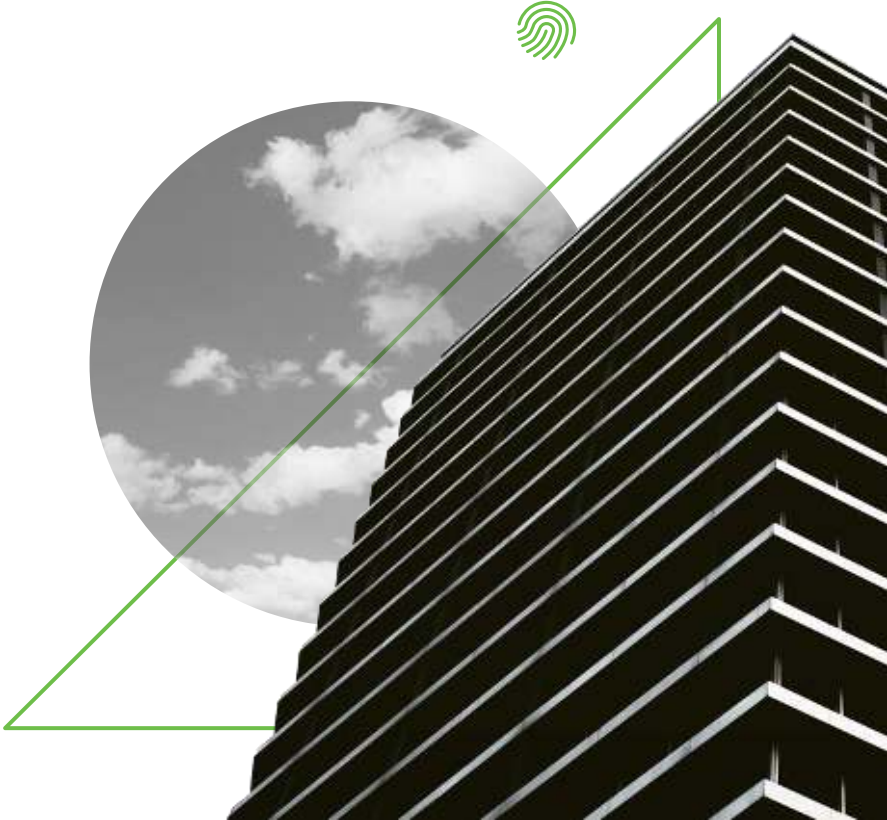


- ▶ Intro
- ▶ Wo kann ich anfangen?
- ▶ Access Netzwerke
- ▶ Rechenzentrum & XaaS

Ich bin Paul

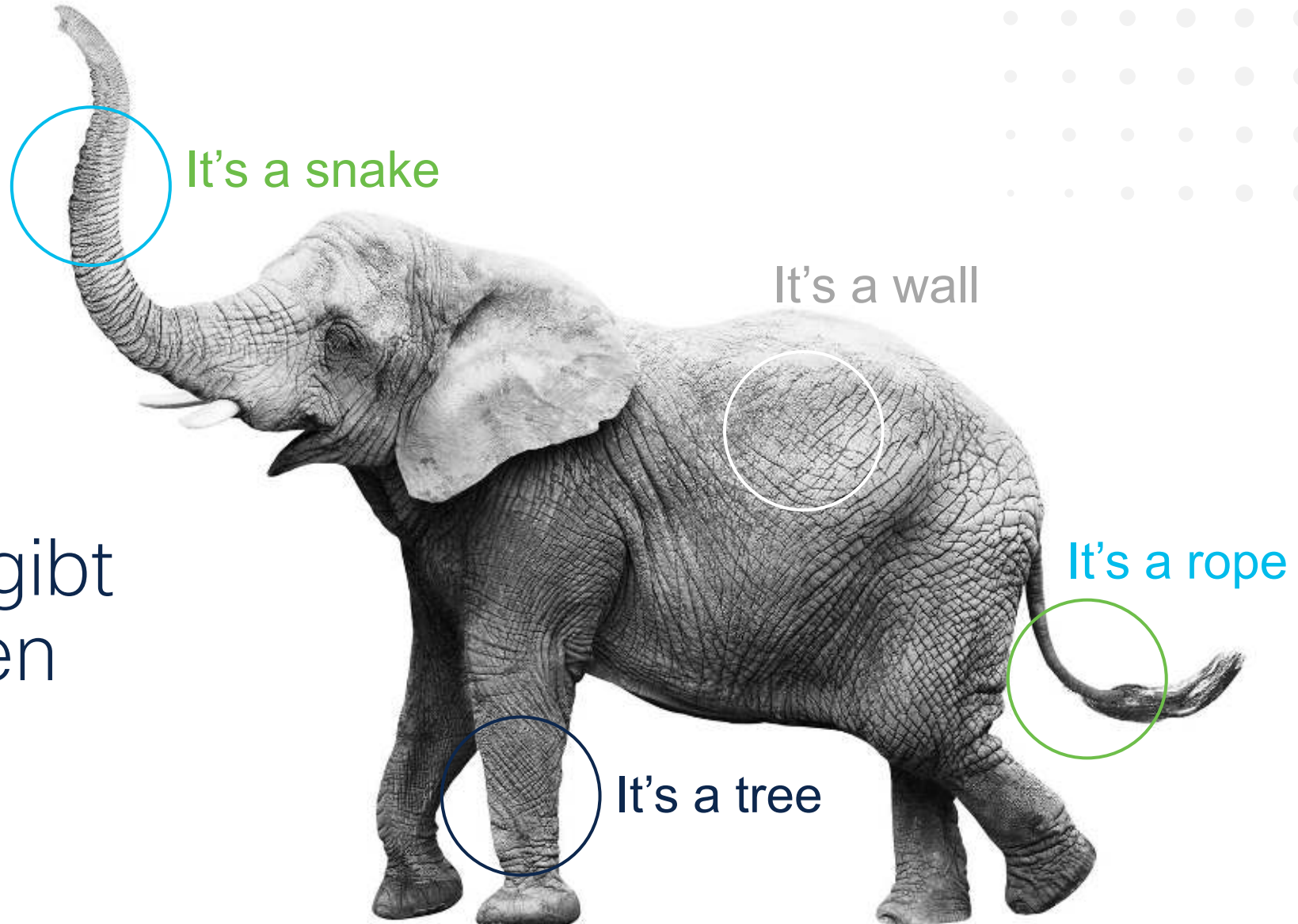


Vertrauen Sie mir?



Richtlinien helfen...aber wer kontrolliert sie?





It's a snake

It's a wall

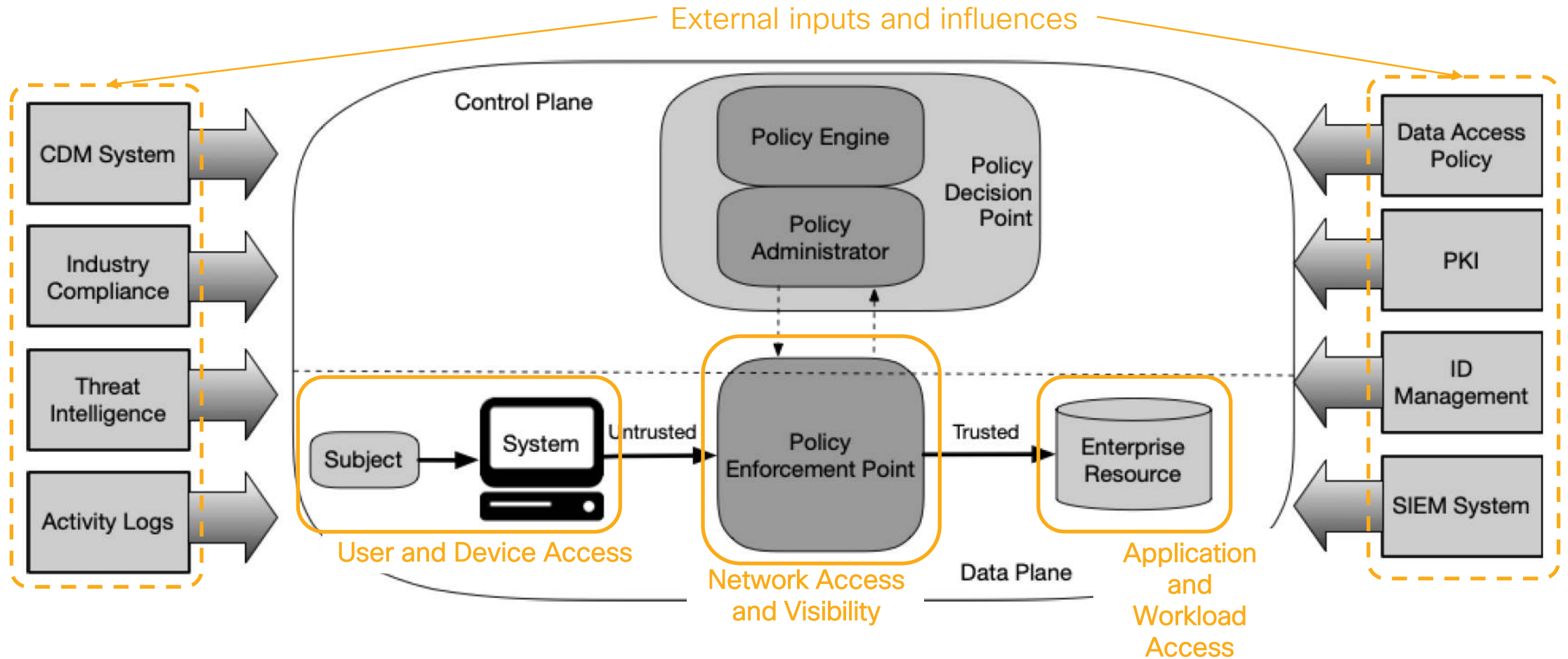
It's a rope

It's a tree

Zero Trust... Es gibt viele Perspektiven

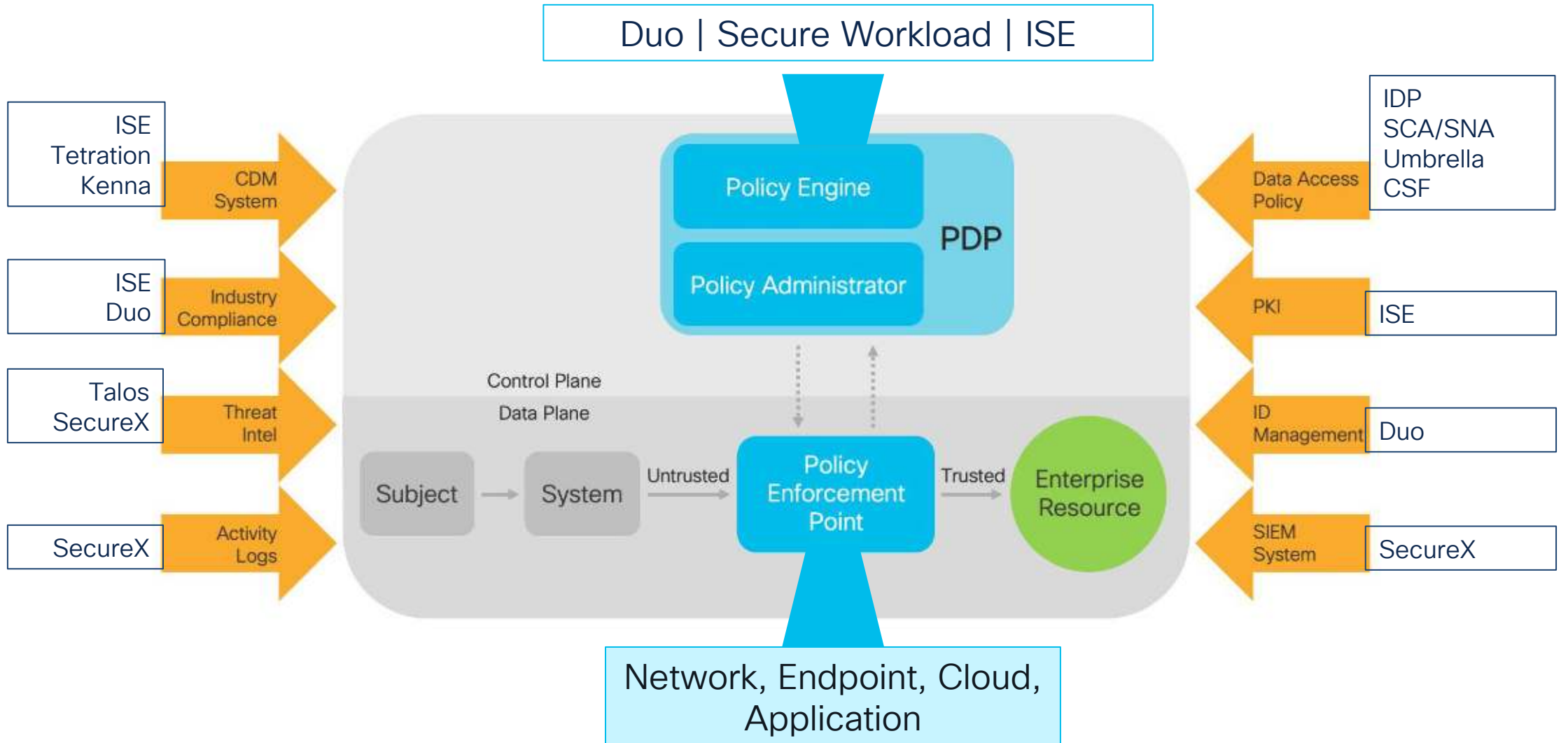
NIST Zero Trust Architecture logical components

800-207 (Aug 11, 2020)



<https://csrc.nist.gov/publications/detail/sp/800-207/final>

NIST 800-207: Aligning Cisco Zero Trust



NIST 7 Principles of Zero Trust

800-207

- All **data sources** and computing **services** are considered **resources**
- All **communication** is **secure regardless** of network **location**
- **Access** to individual enterprise resources **is granted** on a **per-session basis**
- **Access** to individual enterprise resources **is determined by dynamic policy**.
- The **enterprise monitors and measures** the **integrity** and **security posture** of all owned and associated assets
- All resource **authentication and authorization** are **dynamic** and **strictly enforced** before access is allowed
- The enterprise **collects as much information as possible** about **the current state of assets**, network infrastructure and communications and uses it to **improve its security posture**

IT-Sicherheitsziele und Initiativen

IT-Schutzziele



IT-Sicherheitsziele und Initiativen

IT-Schutzziele

Vertraulichkeit
Integrität
Verfügbarkeit

Zero Trust Initiativen

Dynamisches Betrachten der Identität	Continuous Trust Management
	Enhanced User/Device Management
Netzwerk Zugang & Softwaredefinierte Übergänge	Network Access Control
	SD-WAN
	Macro-Segmentierung
Mikro Segmentierung	DC Micro-Segmentierung
	...
	...

IT-Sicherheitsziele und Initiativen

IT-Schutzziele

Vertraulichkeit
Integrität
Verfügbarkeit

Zero Trust Initiativen

Dynamisches Betrachten der Identität	Continuous Trust Management
	Enhanced User/Device Management
Netzwerk Zugang & Softwaredefinierte Übergänge	Network Access Control
	SD-WAN
	Macro-Segmentierung
Mikro Segmentierung	DC Micro-Segmentierung
	...
	...

Schlüsselindikatoren

Mean Time to Detect (MTTD)
Mean Time to Acknowledge (MTTA)
Mean Time to Contain (MTTC)
Mean Time to Resolve (MTTR)
Mean Time to Recovery

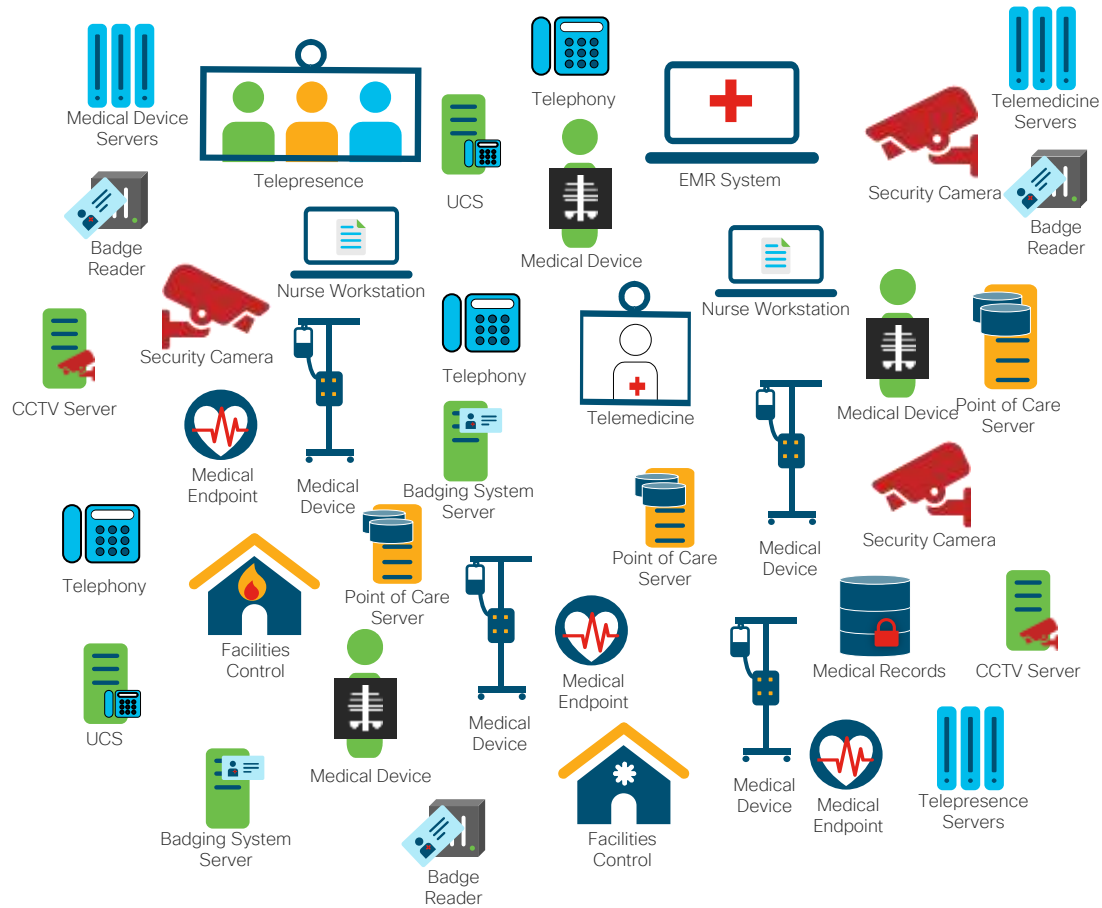
Cisco Zero Trust Prinzipien



Wo kann ich
anfangen?

Wer und was ist im Netz

Wo?

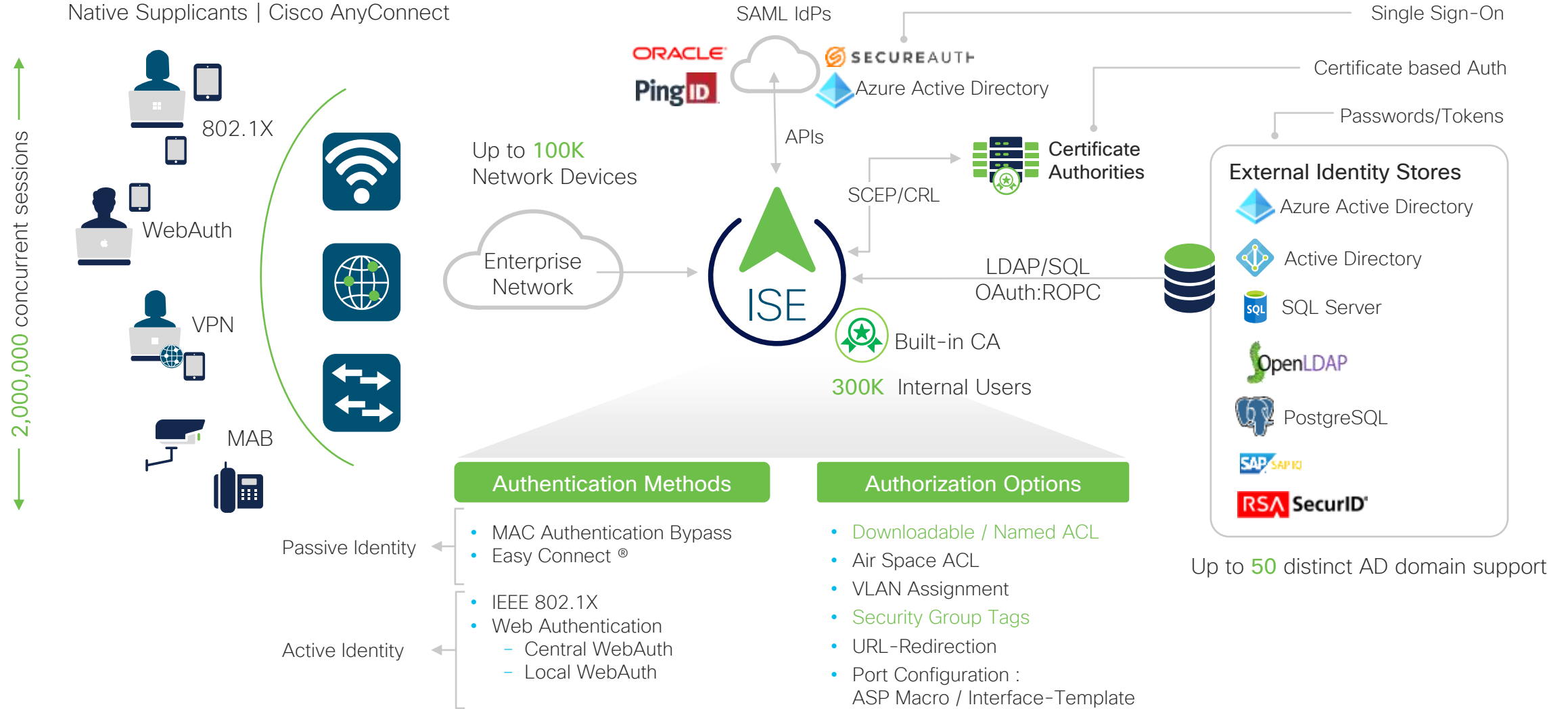


On prem
Datacenter/XaaS

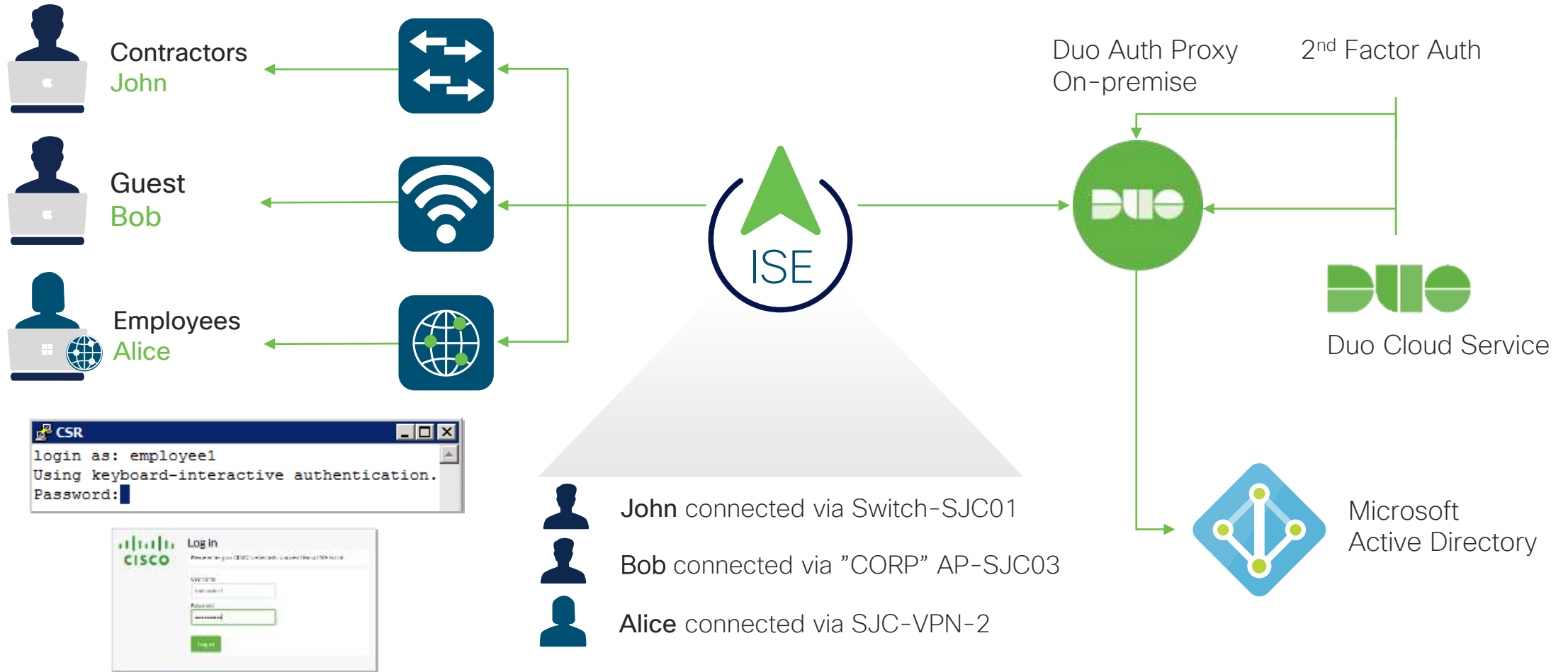
Gäste(w)lan

Büro-/Krankenhaus

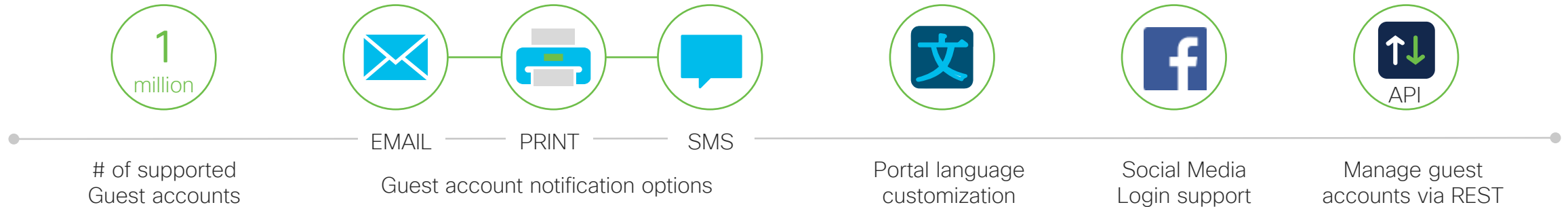
Identitäten etablieren und kontrollieren



Ein zweiter Faktor für die Benutzer?

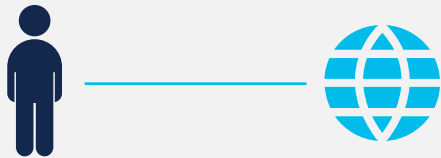


Der Gastzugang



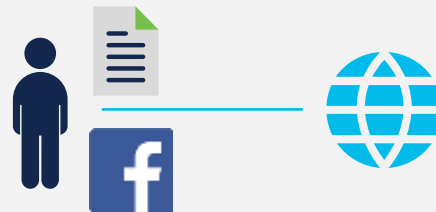
The 3 types of guest access

Hotspot



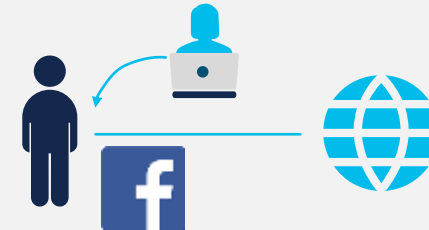
Immediate, un-credentialed Internet access

Self Registered



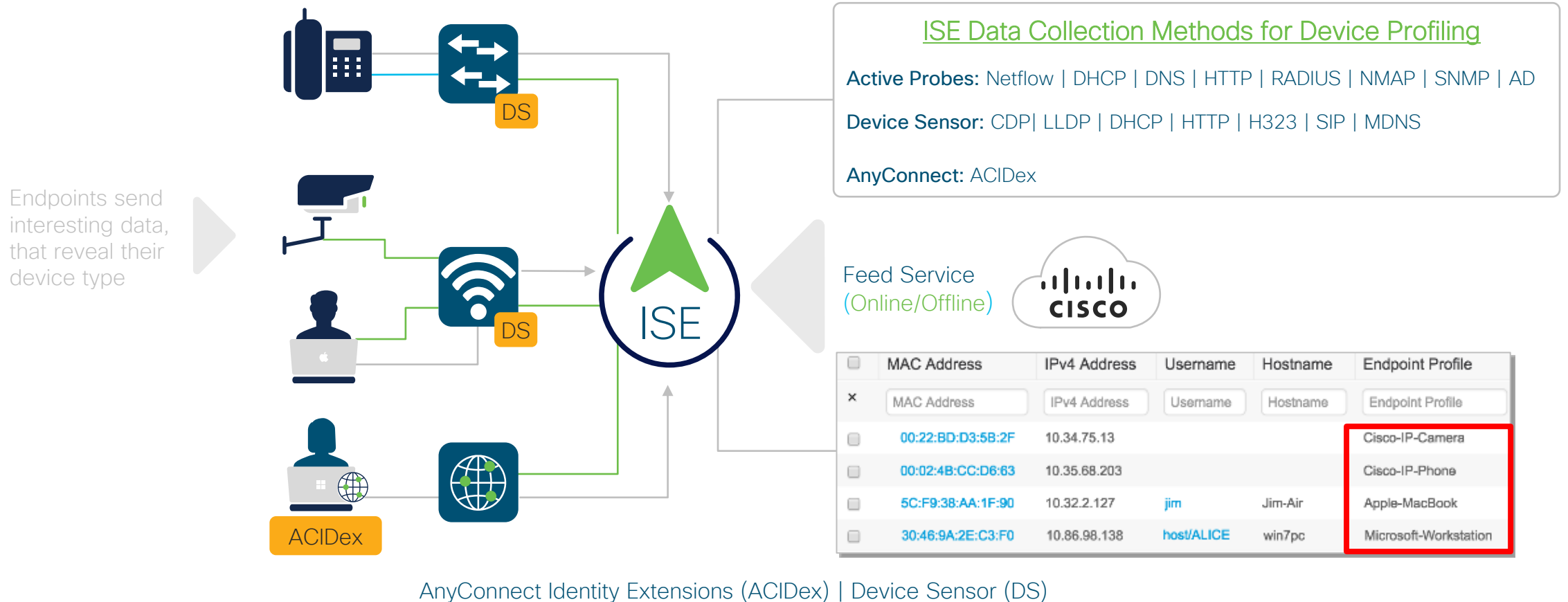
Self-registration by guests, Sponsors may approve access

Sponsored Guest Access



Authorized sponsors create account and share credentials

Endpoint Profiling



Profiling Packages and Integrations

Medical Devices



Hospital



350+ Medical device profiles

Pharma-Smart-Device
Phillips-Analytical-X-Ray-Device
Phillips-CareServant-Device
Phillips-Healthcare-PCCI-Device
Phillips-Medical-Systems-Device
Phillips-Oral-Healthcare-Device
Phillips-Patient-Monitoring-Device
Phillips-Personal-Health-Device
Phillips-Respironics-Device
Phonak-Communications-Device

IOT Building & Automation

Library



Siemens-Device
Siemens-Automation-Drives-Device
Siemens-Building-Device
Siemens-Building-Technologies-Device
Siemens-Convergence-Device
Siemens-Digital-Factory-Device
Siemens-Energy-Automation-Device
Siemens-Energy-Management-Device
Siemens-Home-Office-Device
Siemens-Industrial-Automation-Device



pxGrid



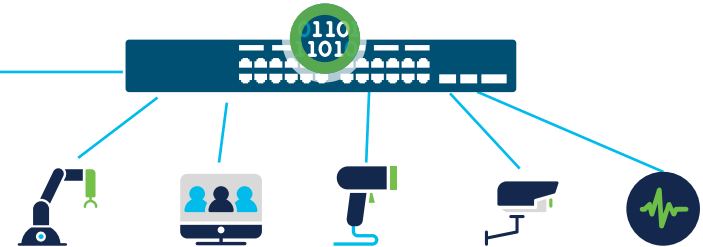
Cisco Industrial Network Director



Factory



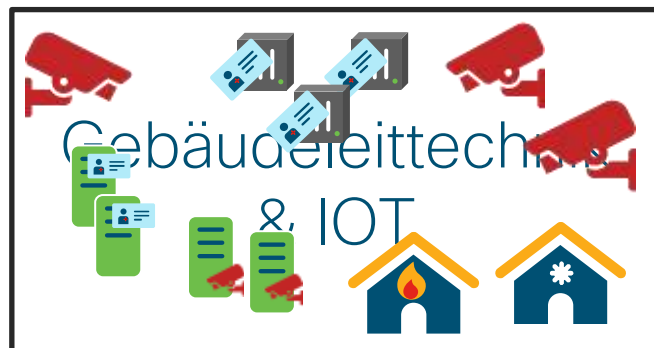
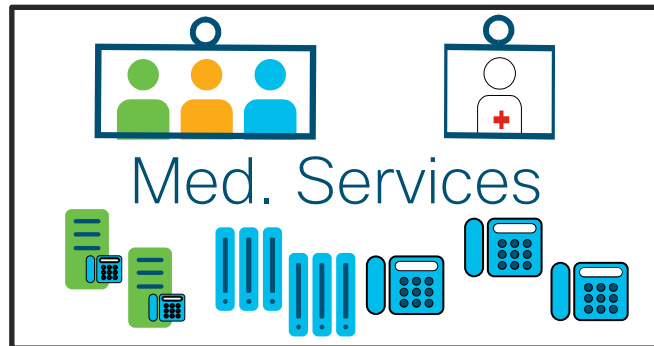
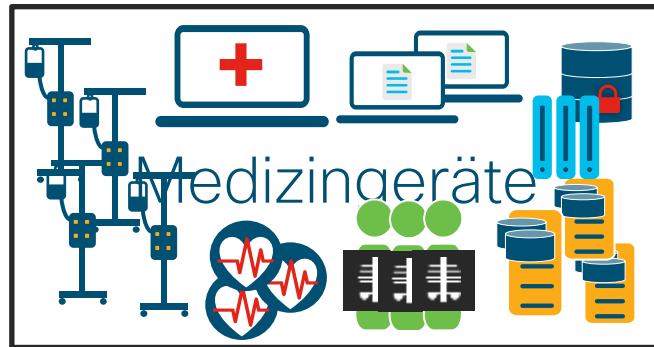
Industrial Devices



Cisco AI Endpoint Analytics

Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization

Bewertung



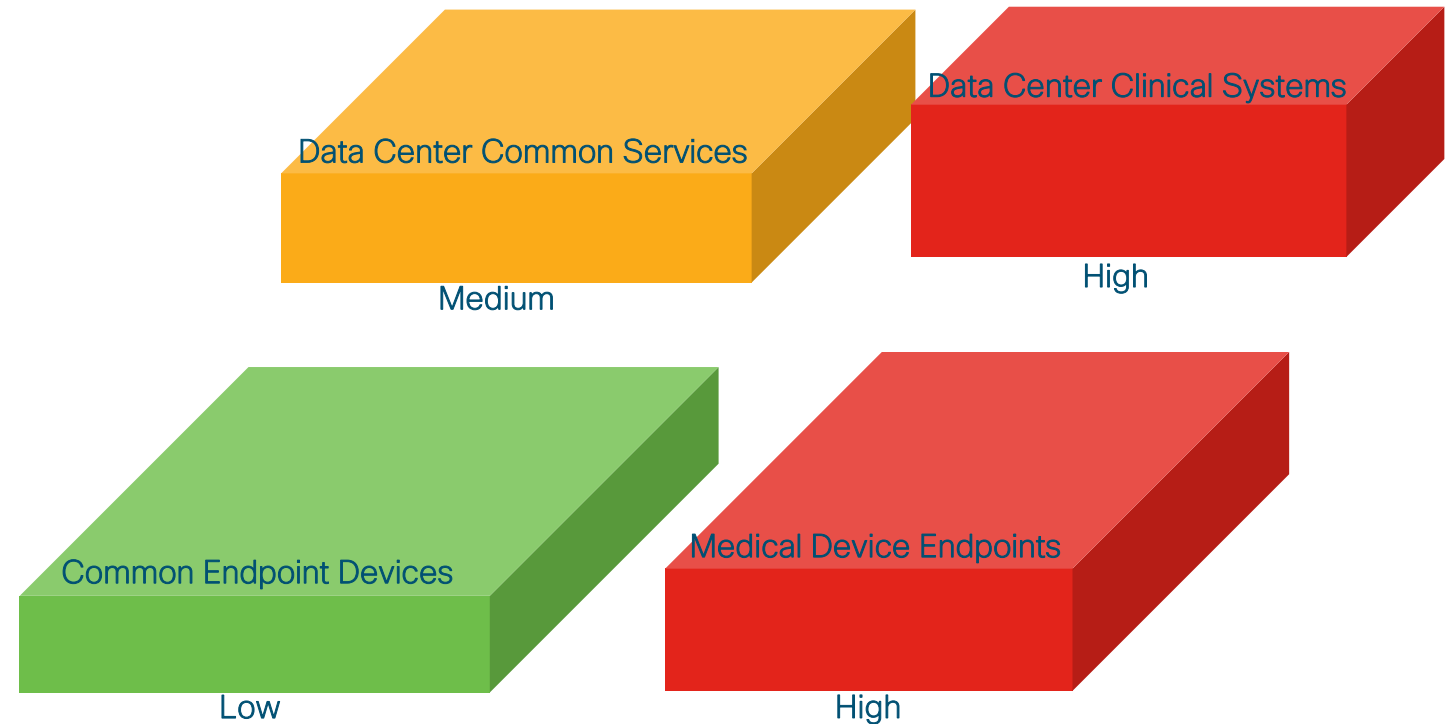
Mapping der Schutzziele / Richtlinien

Vertraulichkeit

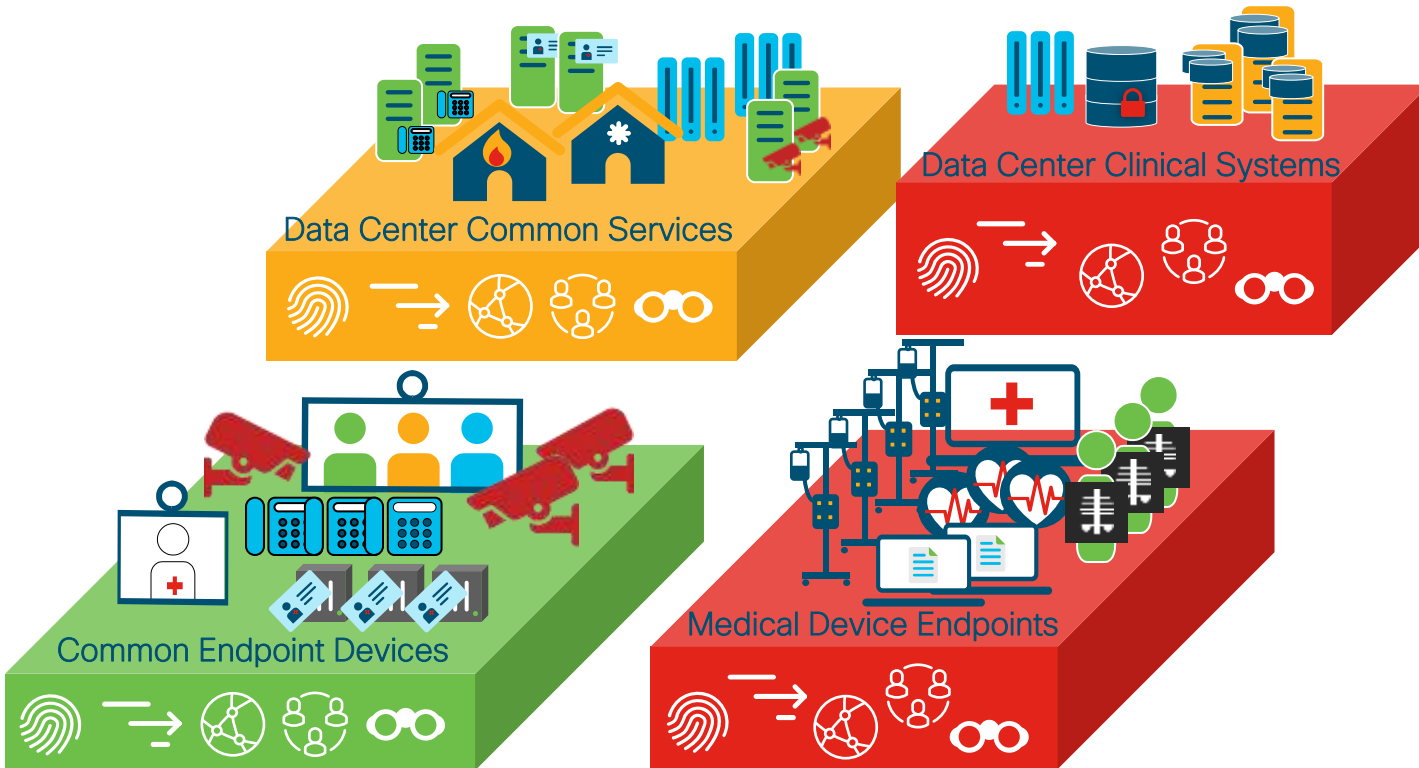
Integrität

Verfügbarkeit

Enklaven definieren und Assets zuordnen



Richtlinien & Kontrollen



Identitäts- und Vertrauensbildung



Durchsetzung von Richtlinien



Isolation



Verfügbarkeit

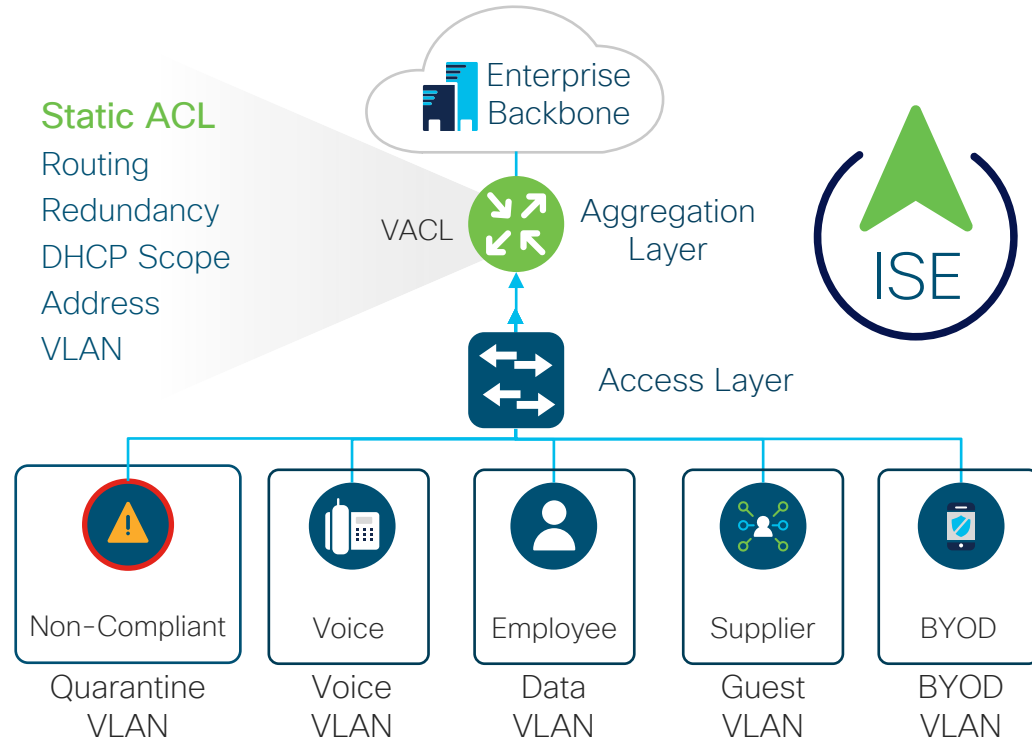


Sichtbarkeit

Access Netzwerke

Kontextbasierte Segmentierung

Traditionelle Segmentierung

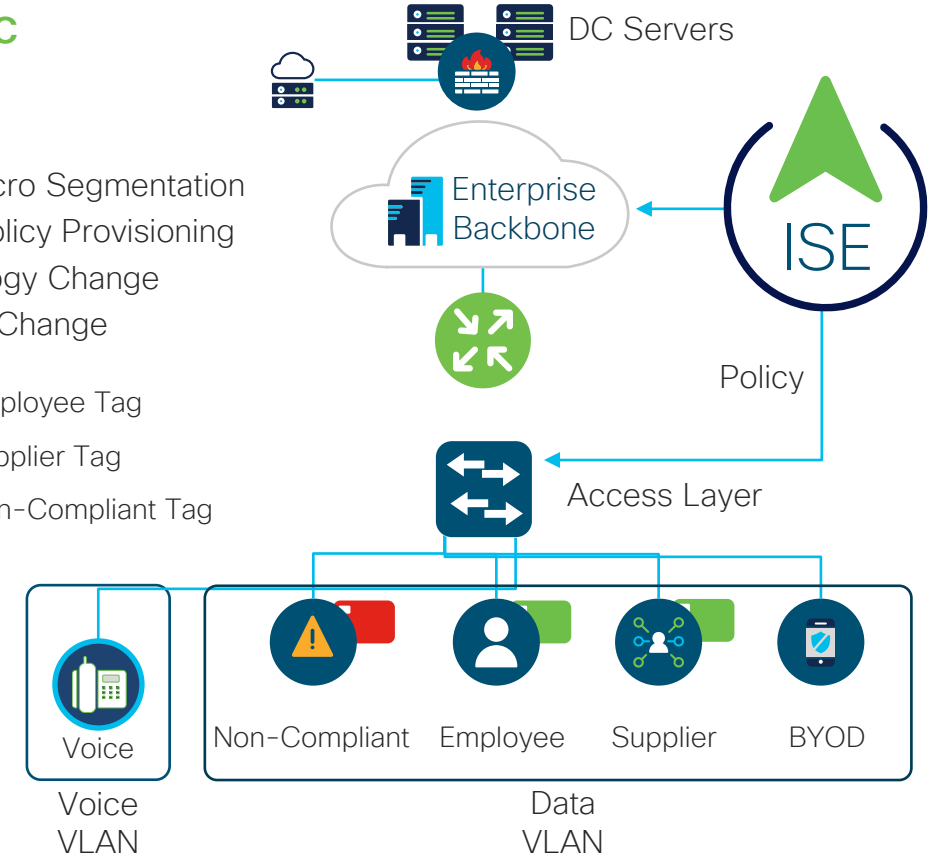


Security Policy based on Topology
 High cost and complex maintenance

TrustSec

Micro/Macro Segmentation
 Central Policy Provisioning
 No Topology Change
 No VLAN Change

- Employee Tag
- Supplier Tag
- Non-Compliant Tag



Use existing topology and automate security policy to reduce OpEx

Ein Blick in eine Policy-Matrix

The screenshot displays the Cisco ISE TrustSec Policy configuration interface. The main view is the 'Production Matrix' for the 'TrustSec Policy' under the 'Egress Policy' section. The matrix shows the relationship between various source and destination groups. A pop-up window on the left provides details for the 'BlockMalware' Security Group ACL.

Security Group ACLs

Name: BlockMalware

Description: Block common malware attacks

IP Version: IPv4 IPv6 Agnostic

Security Group ACL content:

```
deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
```

Production Matrix

Populated cells: 304

Source	Cameras 9/0009	Contractors 5/0005	Employees 4/0004	Engineering 11/000B	Guests 6/0006	Industrial 17/0011	IOT 12/000C	Lighting 16/0012	Medical 15/000F	Network_Service... 2/0002	PCI 14/000E	Phones
Cameras 9/0009	Permit IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	Deny IP
Contractors 5/0005	Deny IP	BlockMalware	BlockMalware	BlockMalware	BlockMalware	BlockMalware	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	Deny IP
Employees 4/0004	Deny IP	BlockMalware	BlockMalware	BlockMalware	BlockMalware	BlockMalware	BlockMalware	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP

Datacenter&Cloud

ACI Devices Role

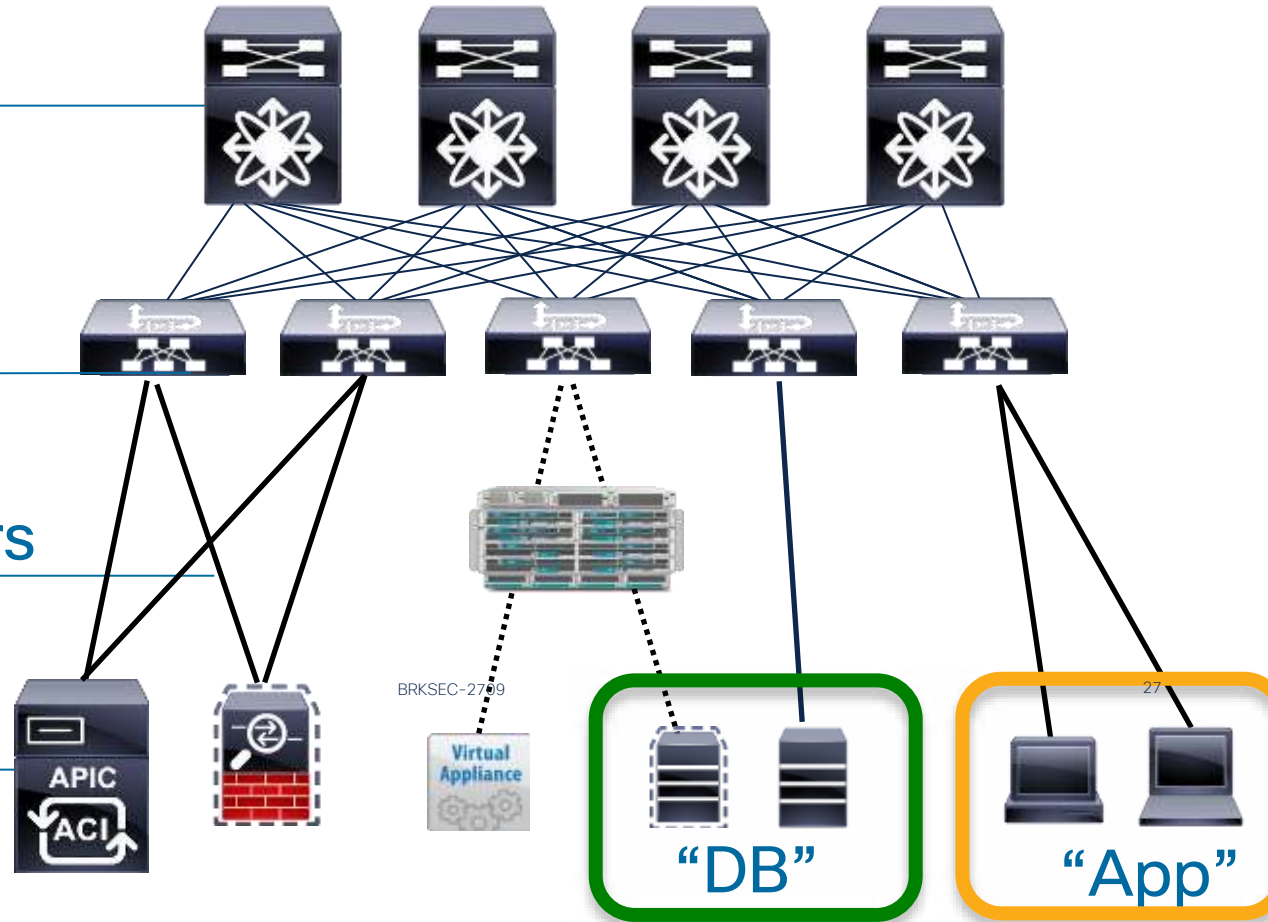
Spine Nodes

Leaf Nodes

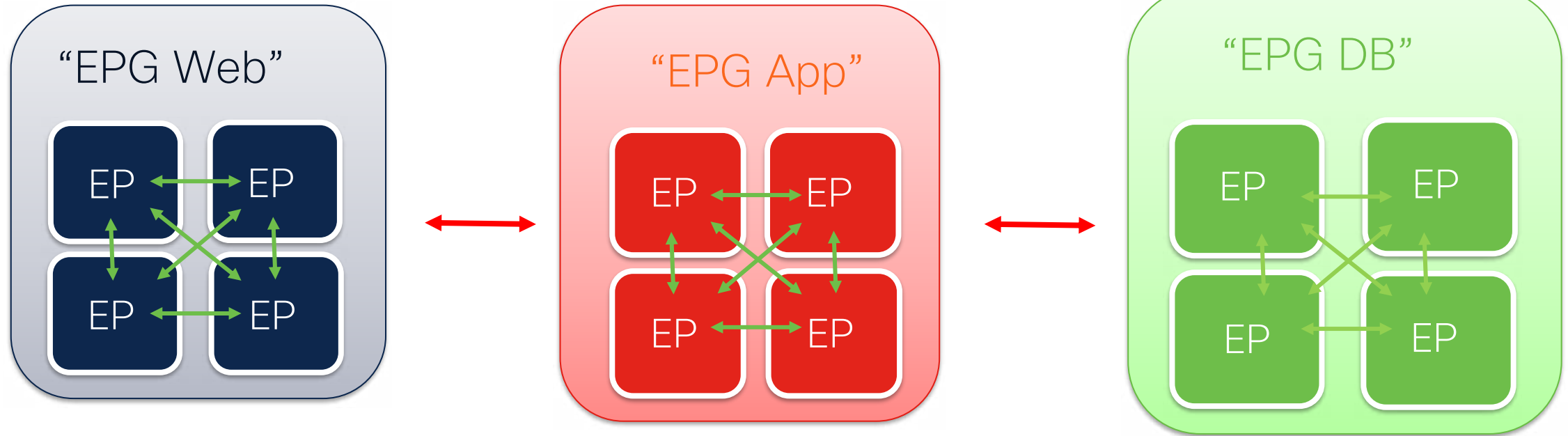
Service Producers

APIC Controller

Service Consumers



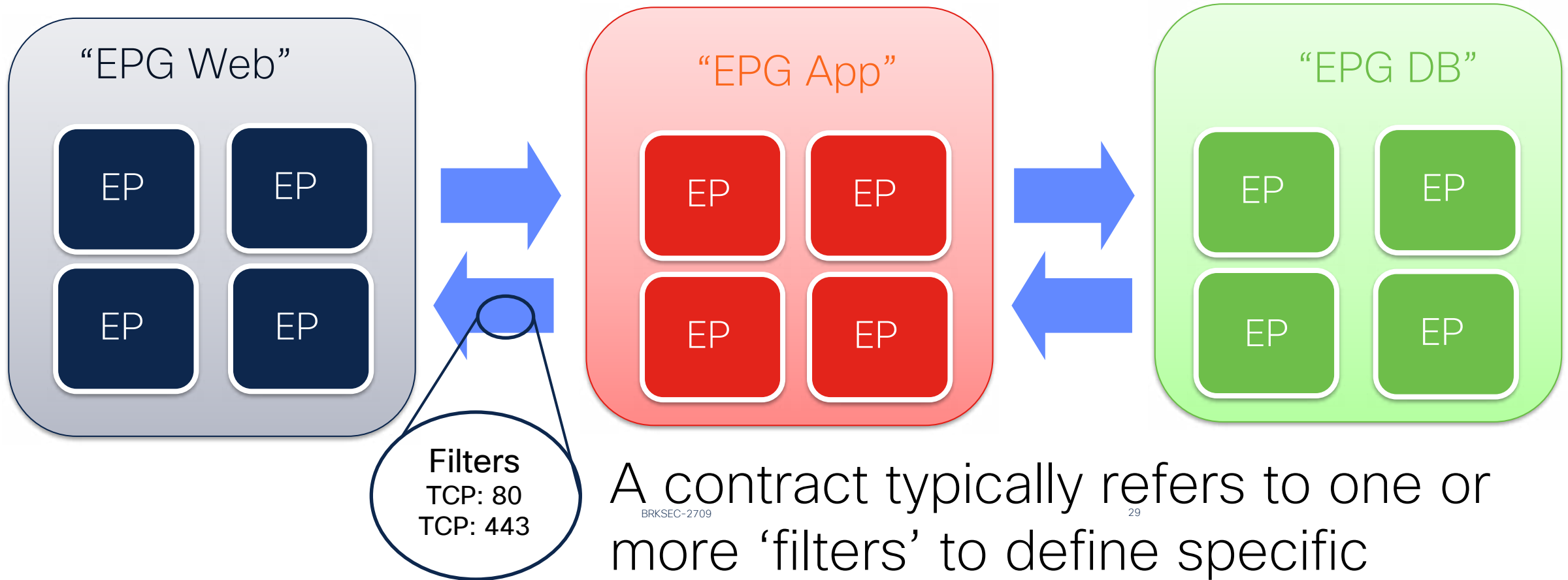
Endpoint Groups Communications



Devices within an Endpoint group can communicate, provided that they have IP²⁸ reachability (provided by the Bridge Domain/VRF).

Communication between Endpoint groups is, by default, not permitted.

Contract : Kind of reflexive “Stateless” ACLs



A contract typically refers to one or more ‘filters’ to define specific protocols & ports allowed between EPGs.

Application policy with contract

Summary **Topology** Policy Stats Health Faults History

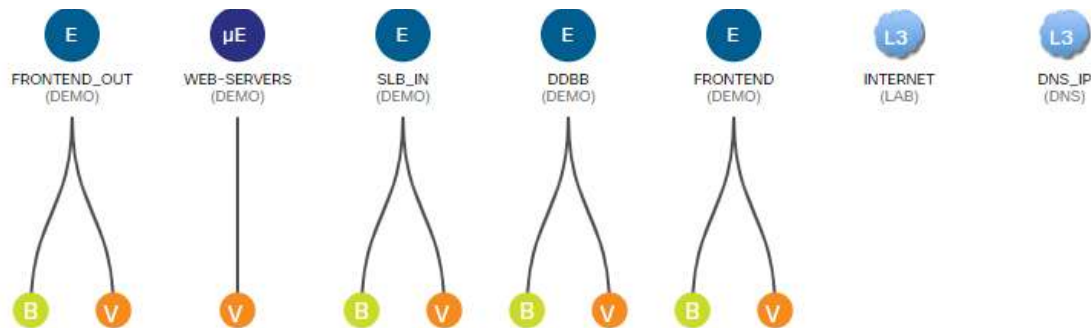
Healthy

Contract EGPE uSeg EPG Any EPG Baremetal VMware Microsoft Red Hat OpenStack Kubernetes Cloud Foundry OpenShift Layer 2 Layer 3 Layer 4-7

Contracts →

EPG →

Form Factor →



Relation Indicators

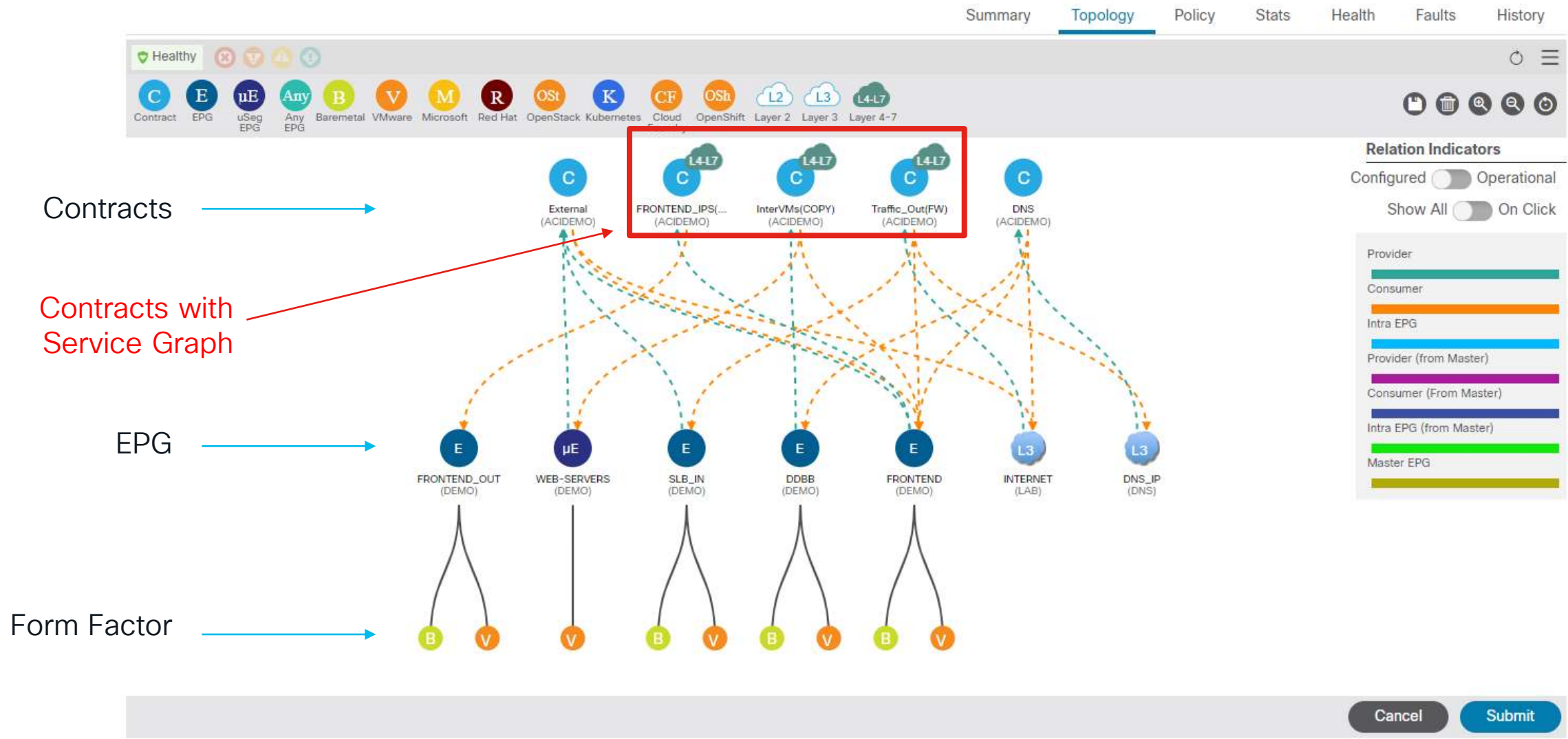
Configured Operational

Show All On Click

- Provider
- Consumer
- Intra EPG
- Provider (from Master)
- Consumer (From Master)
- Intra EPG (from Master)
- Master EPG

Cancel Submit

Application Policy with Contract



Kontext teilen

APIC (aci-dev-01)

System **Tenants** Fabric

ALL TENANTS | Add Tenant | Tenant Search: name o

fgandola

- Quick Start
- fgandola
 - Application Profiles
 - applications
 - Application EPGs
 - uSeg EPGs
 - Endpoint Security Groups
 - ALL_EPGs
 - development
 - production
 - firewalls
 - Application EPGs
 - ftd-HA-link
 - ftd-mgmt
 - uSeg EPGs
 - Endpoint Security Groups
 - network-segments
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

Secure Firewall Management Center

Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

Dynamic Objects

Name	Description	Number of Mapped IPs
APIC_DEMO_APPLICATIONS_ESG-DEMO-APP		1
APIC_DEMO_NETWORK-SEGMENTS_192.168.150.X_24		1
APIC_FGANDOLA_APPLICATIONS_ESG-ALL_EPGS		2
APIC_FGANDOLA_APPLICATIONS_ESG-DEVELOPMENT		1
APIC_FGANDOLA_APPLICATIONS_ESG-PRODUCTION		1
APIC_FGANDOLA_FIREWALLS_FTD-HA-LINK		1
APIC_FGANDOLA_FIREWALLS_FTD-MGMT		4
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.151....		1
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.152....		2
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.153....		1

APIC_FGANDOLA_FIREWALLS_FTD-MGMT

Mapped IPs

4 Mapped IPs

- 10.237.100.22
- 10.237.100.23
- 10.237.100.24
- 10.237.100.25

Download OK

Datacenter/Cloud

Kontext teilen

System **Tenants** Fabric

ALL TENANTS | Add Tenant | Tenant Search: name o

fgandola

- Quick Start
- fgandola
 - Application Profiles
 - applications
 - Application EPGs
 - uSeg EPGs
 - Endpoint Security Groups
 - ALL_EPGs
 - development
 - production
 - firewalls
 - Application EPGs
 - ftd-HA-link
 - ftd-mgmt
 - uSeg EPGs
 - Endpoint Security Groups
 - network-segments
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

Secure Firewall Management Center

Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

Dynamic Objects

Name	Description	Number of Mapped IPs
APIC_DEMO_APPLICATIONS_ESG-DEMO-APP		1
APIC_DEMO_NETWORK-SEGMENTS_192.168.150.X_24		1
APIC_FGANDOLA_APPLICATIONS_ESG-ALL_EPGS		2
APIC_FGANDOLA_APPLICATIONS_ESG-DEVELOPMENT		1
APIC_FGANDOLA_APPLICATIONS_ESG-PRODUCTION		1
APIC_FGANDOLA_FIREWALLS_FTD-HA-LINK		1
APIC_FGANDOLA_FIREWALLS_FTD-MGMT		4
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.151....		1
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.152....		2
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.153....		1

APIC_FGANDOLA_FIREWALLS_FTD-MGMT

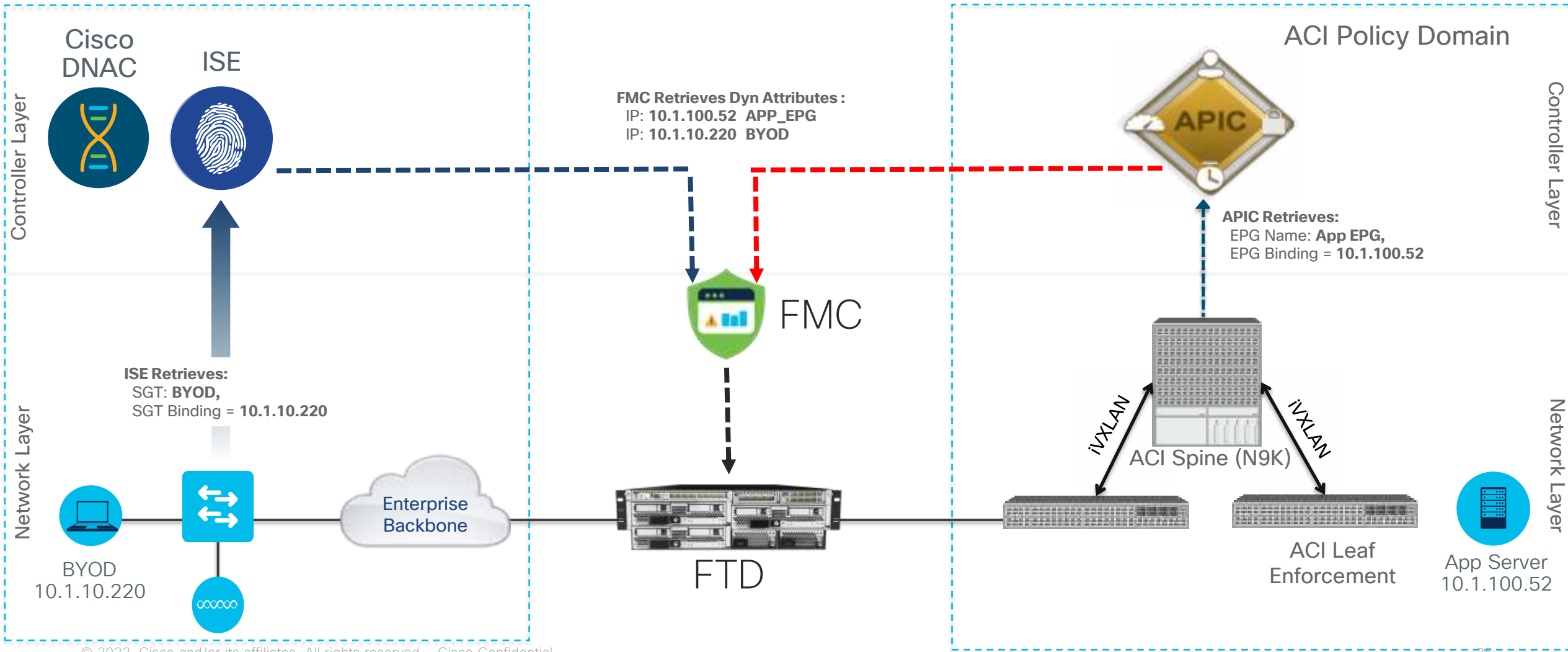
Mapped IPs

4 Mapped IPs

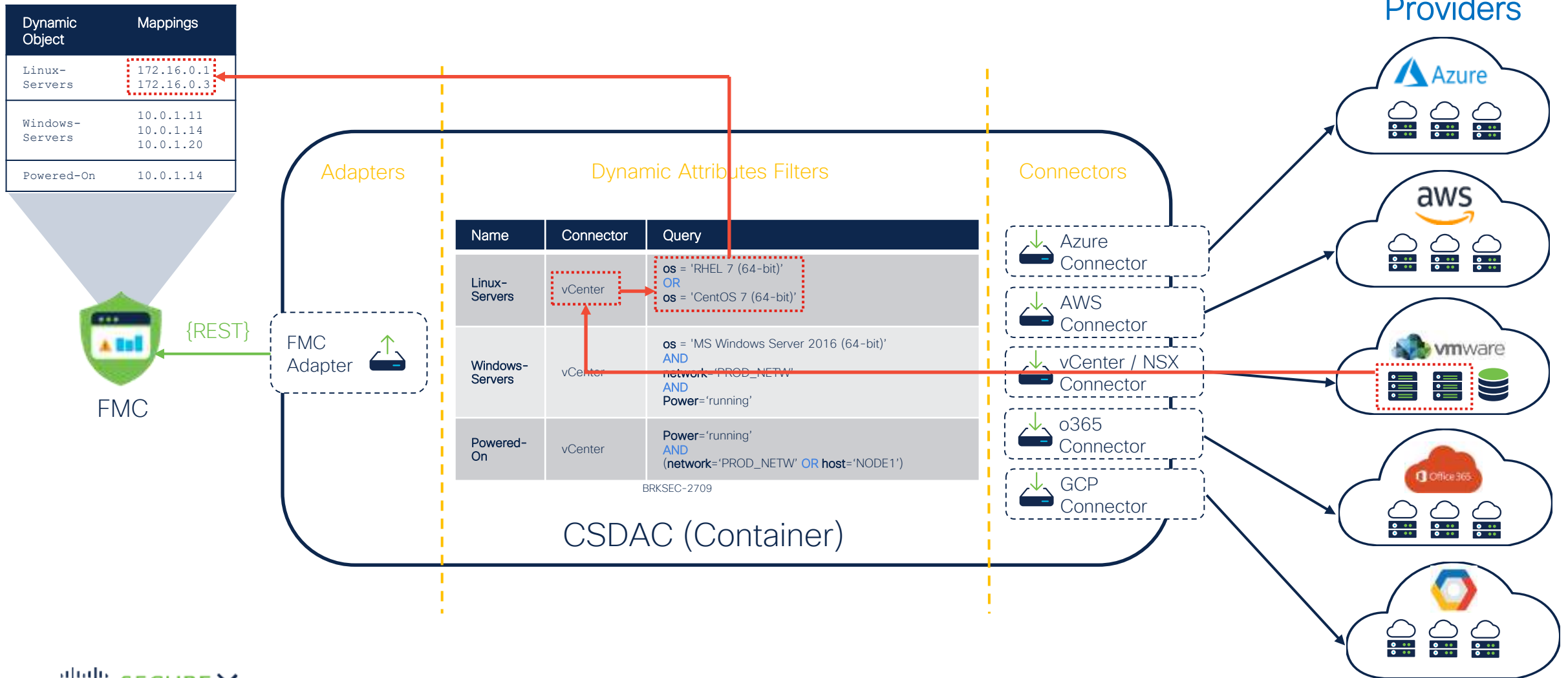
- 10.237.100.22
- 10.237.100.23
- 10.237.100.24
- 10.237.100.25

Download OK

SGT/ACI Firepower Integration



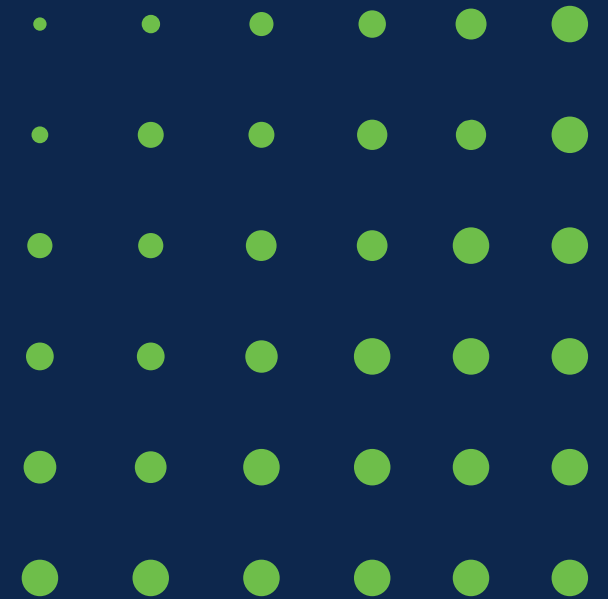
Architecture of the Dynamic Attributes Connector



Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	App. Prot.	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
Mandatory - Attribute-Based Policy (-)									
Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Print	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Any	Facebook Google+ Instagram Tinder Twitter	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	BRKSEC-2709	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	SecureX	Any	Any	Quarantined_Systems	Honeypot_Service
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

Fazit



2025 Reimagine
 **GERMANY**