Zero Trust beginnt im Kopf

Wie sieht es in Ihrem Netzwerk aus?

2025 Reimagine GERMANY

Christian Schulmeister

Technical Solutions Architect – CyberSecurity

CISSP

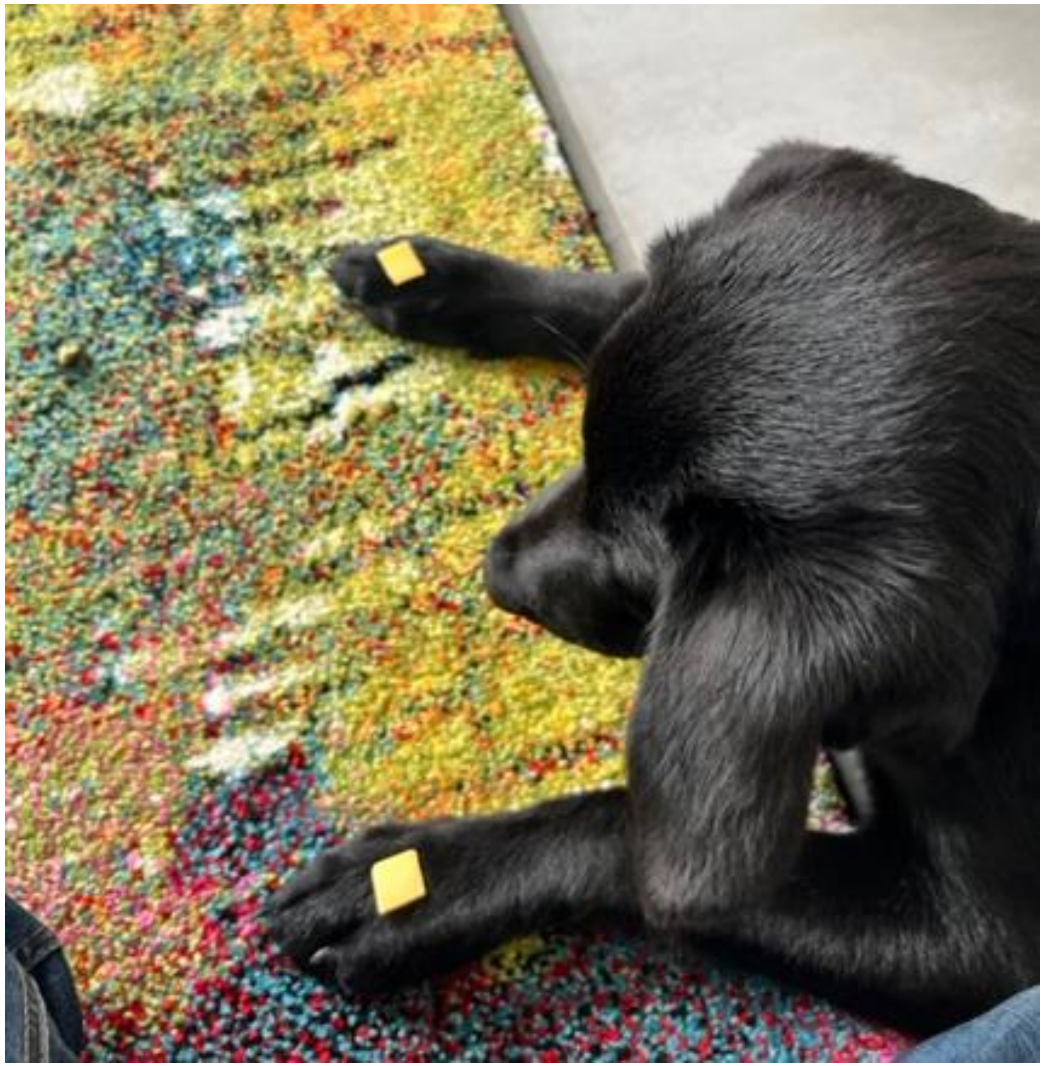
September 2022

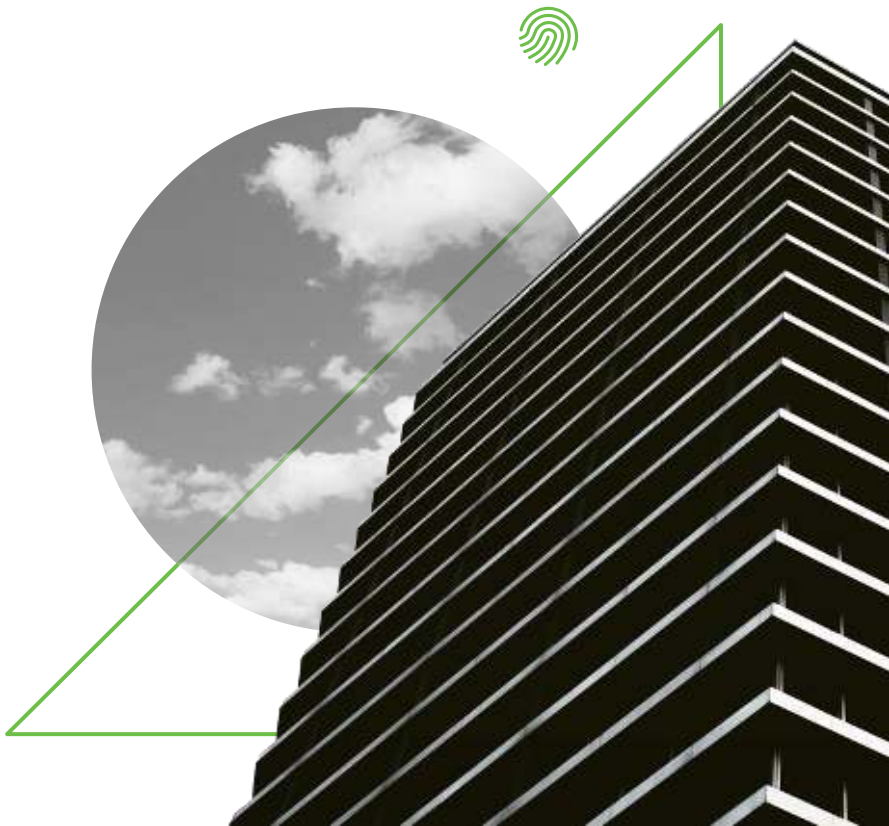
Agenda

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

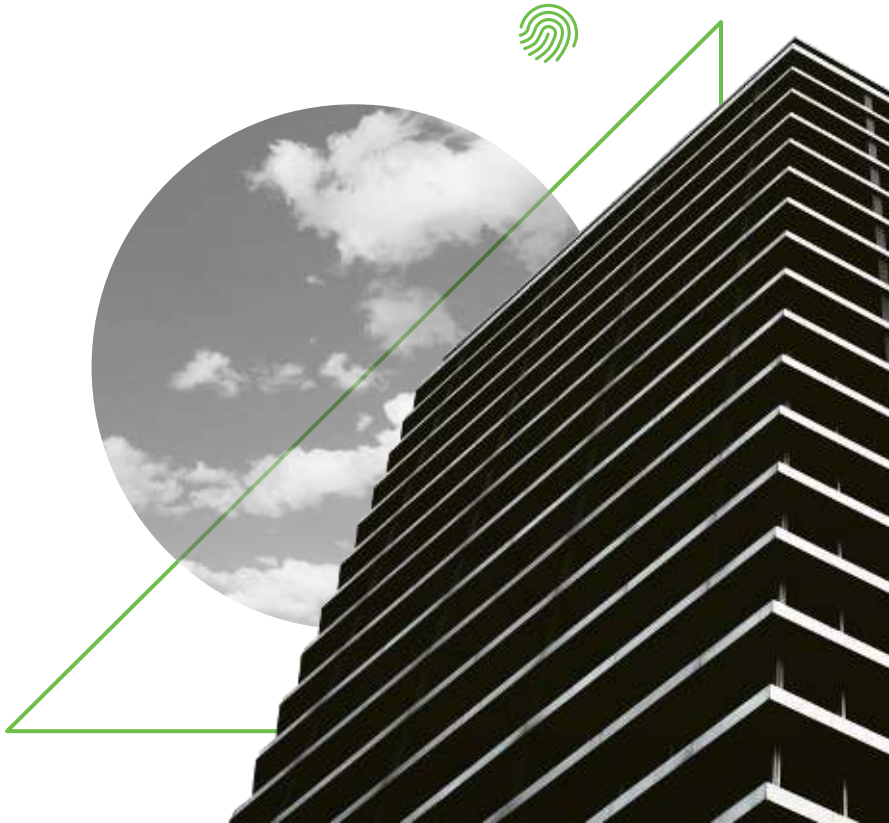
Ich bin Paul

Vertrauen Sie mir?

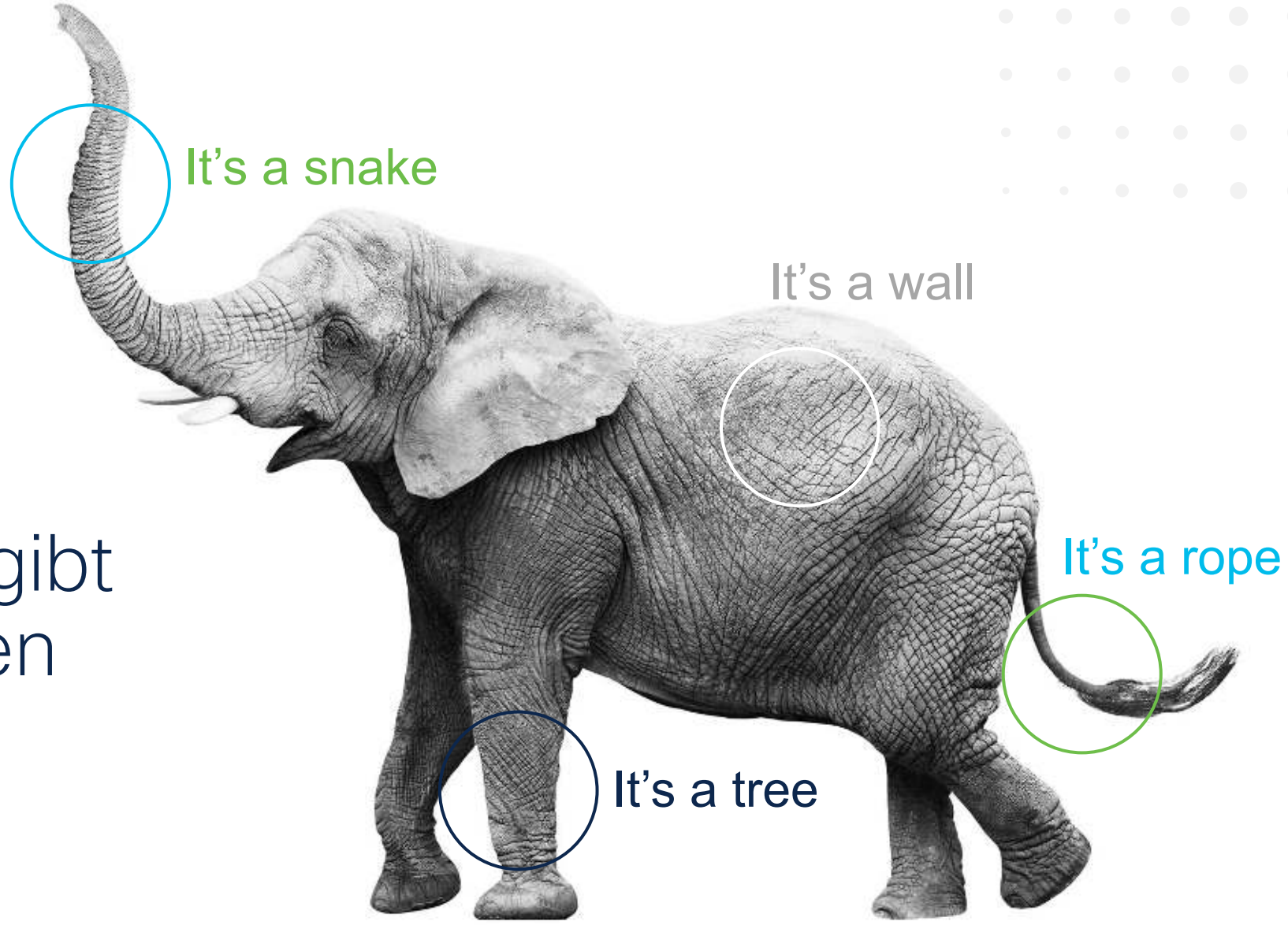




Richtlinien helfen...aber wer kontrolliert sie?

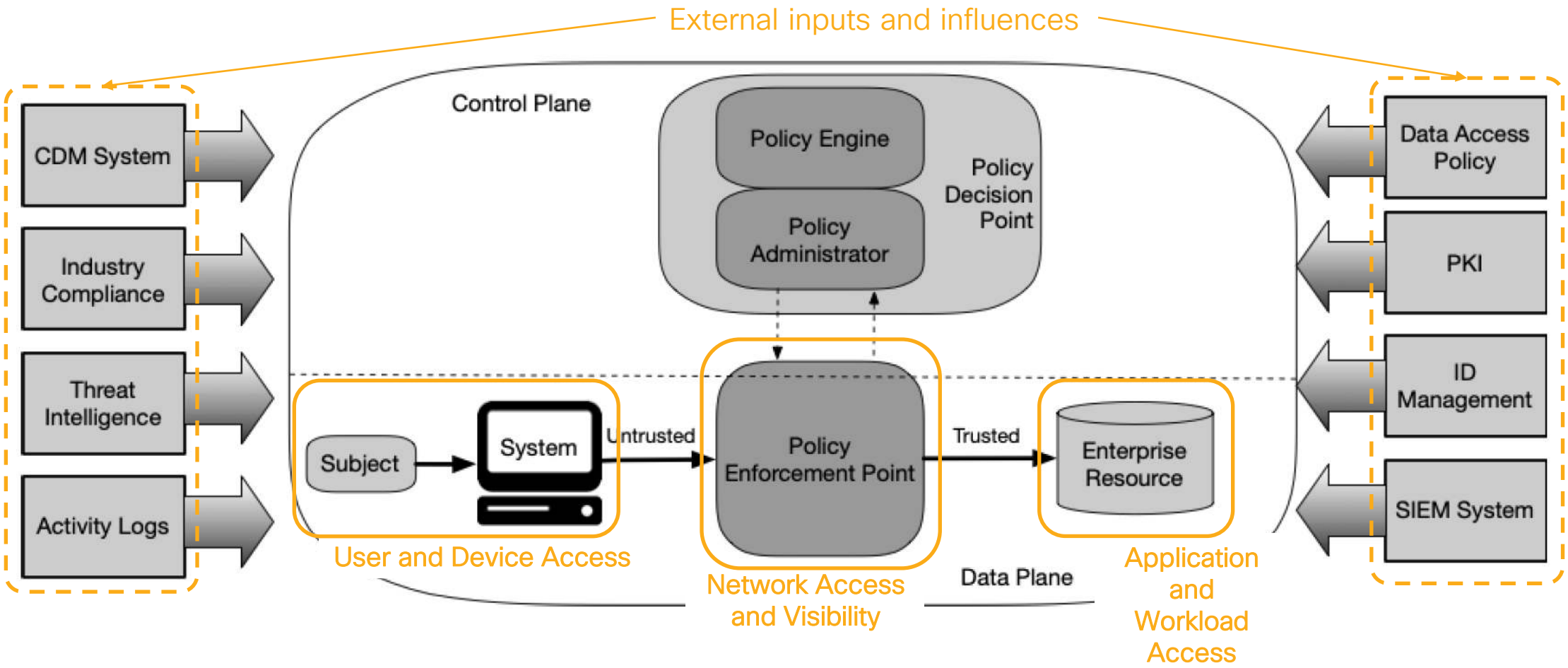


Zero Trust... Es gibt viele Perspektiven



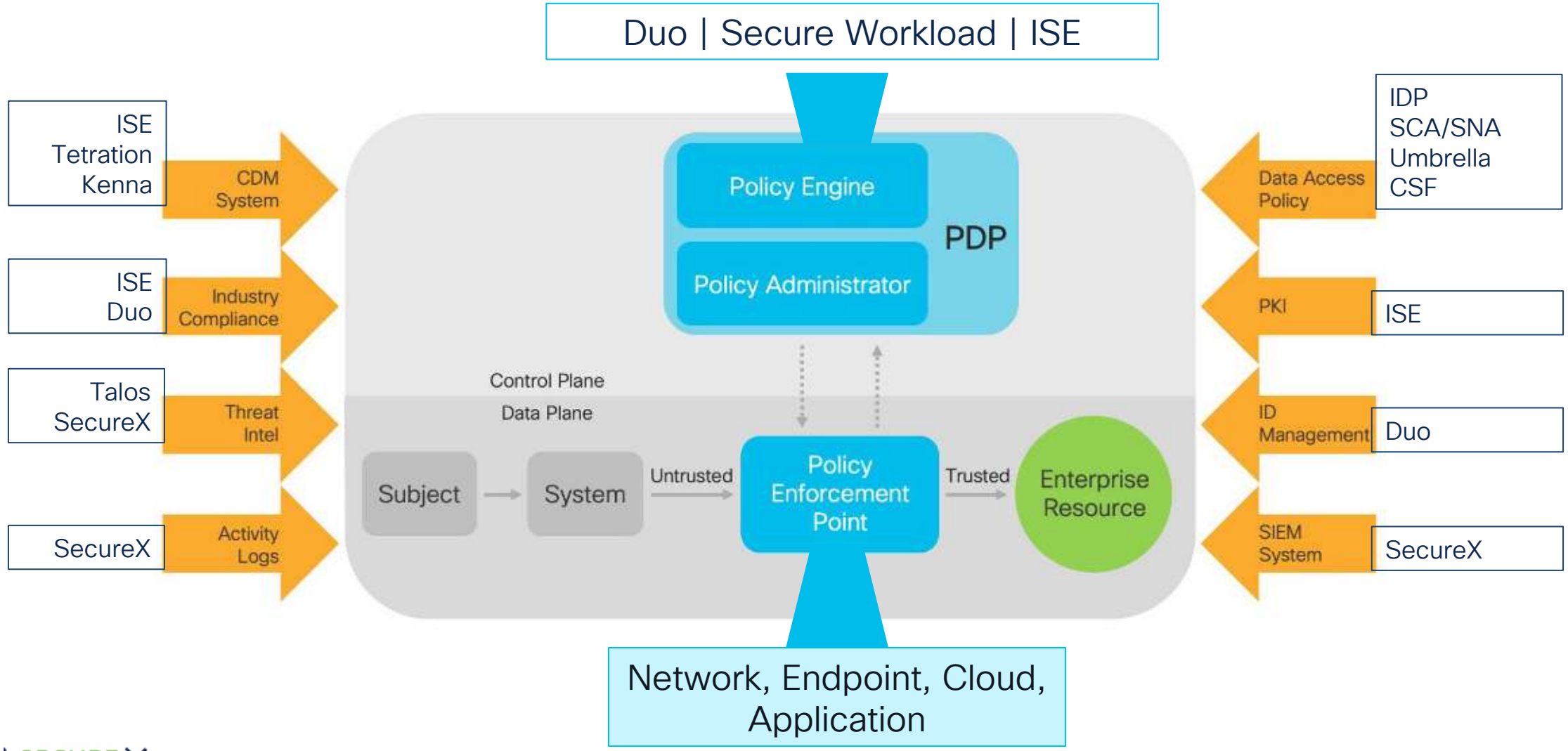
6

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



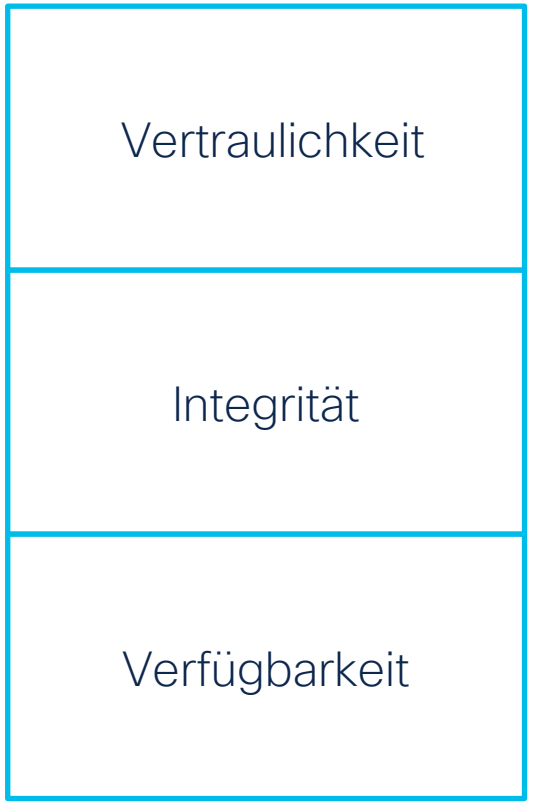
8

NIST 7 Principles of Zero Trust
800-207

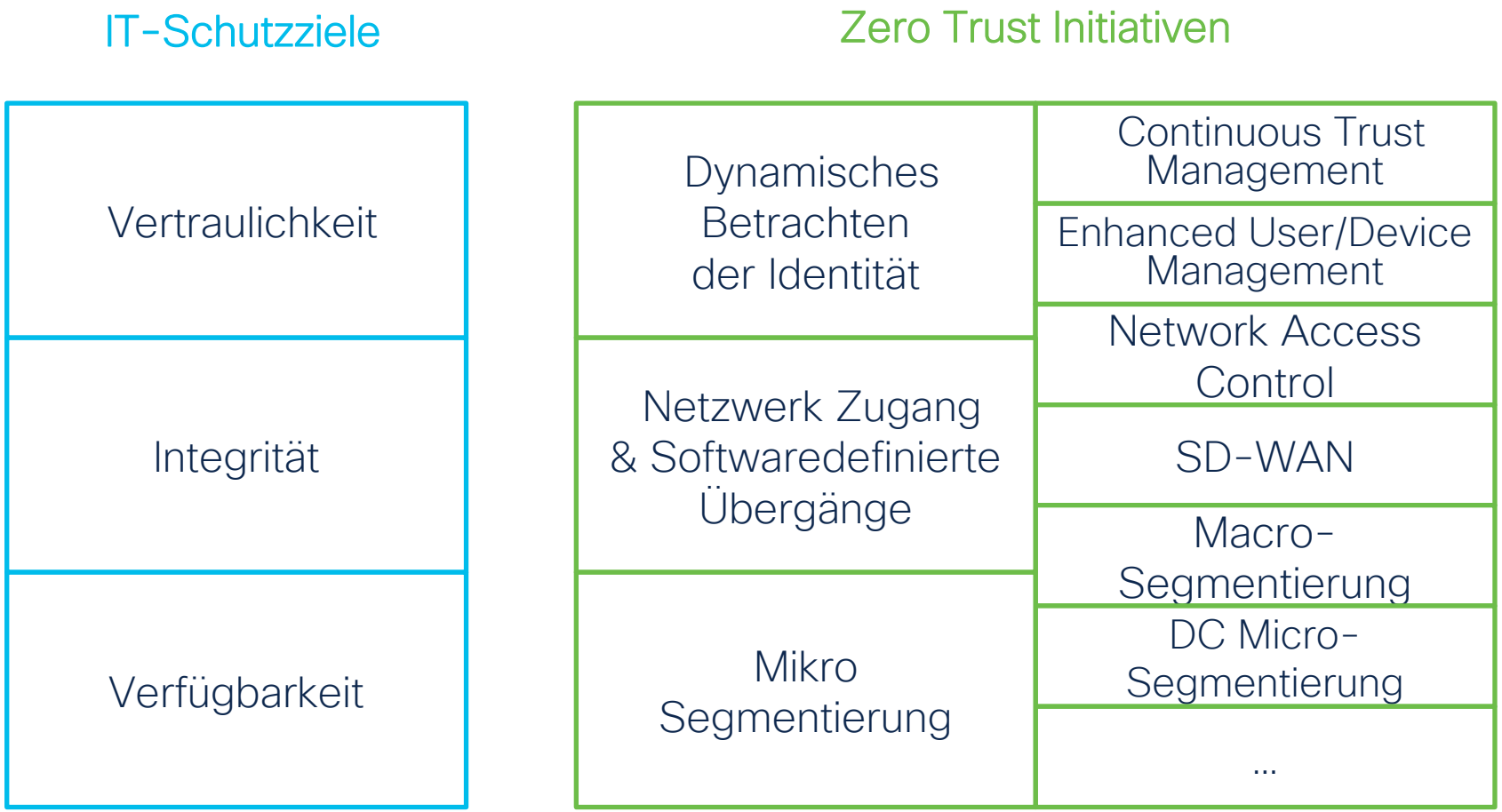
- All data sources and computing services are considered resources
- All communication is secure regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- Access to individual enterprise resources is determined by dynamic policy.
- The enterprise monitors 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

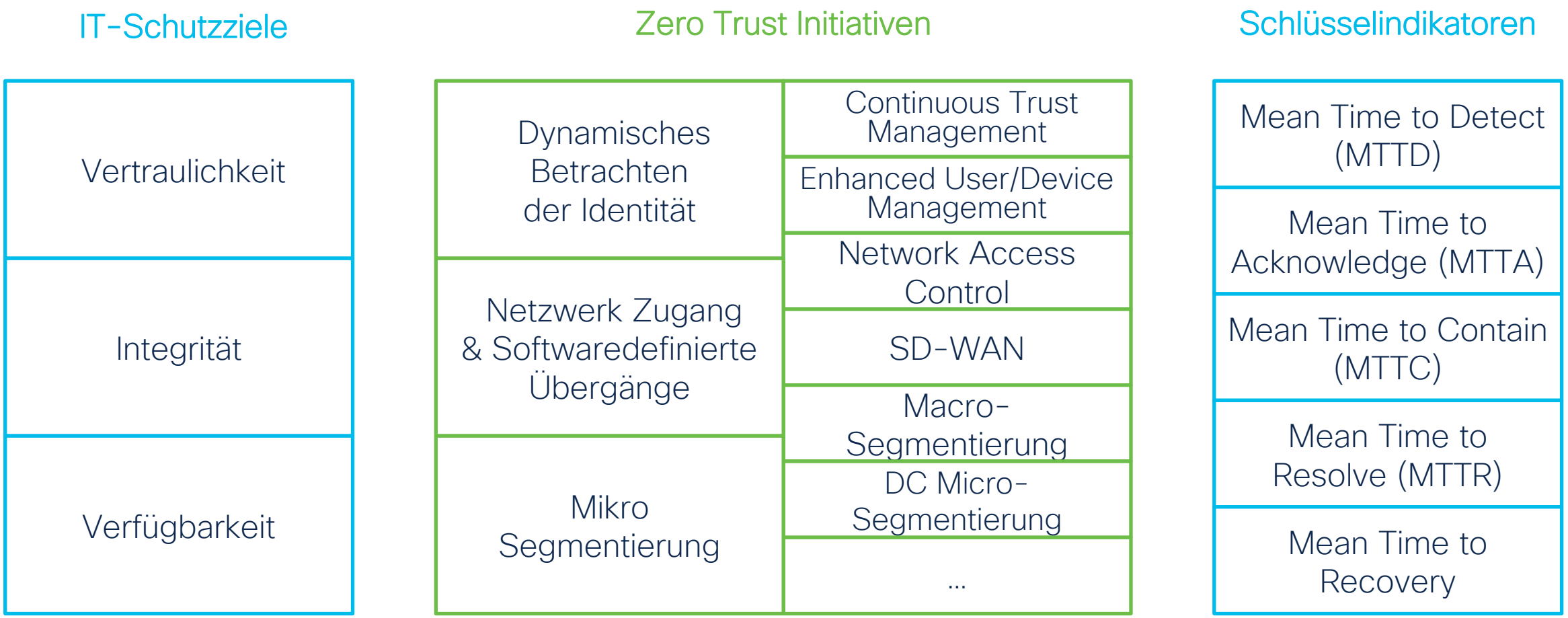
IT-Schutzziele



IT-Sicherheitsziele und Initiativen



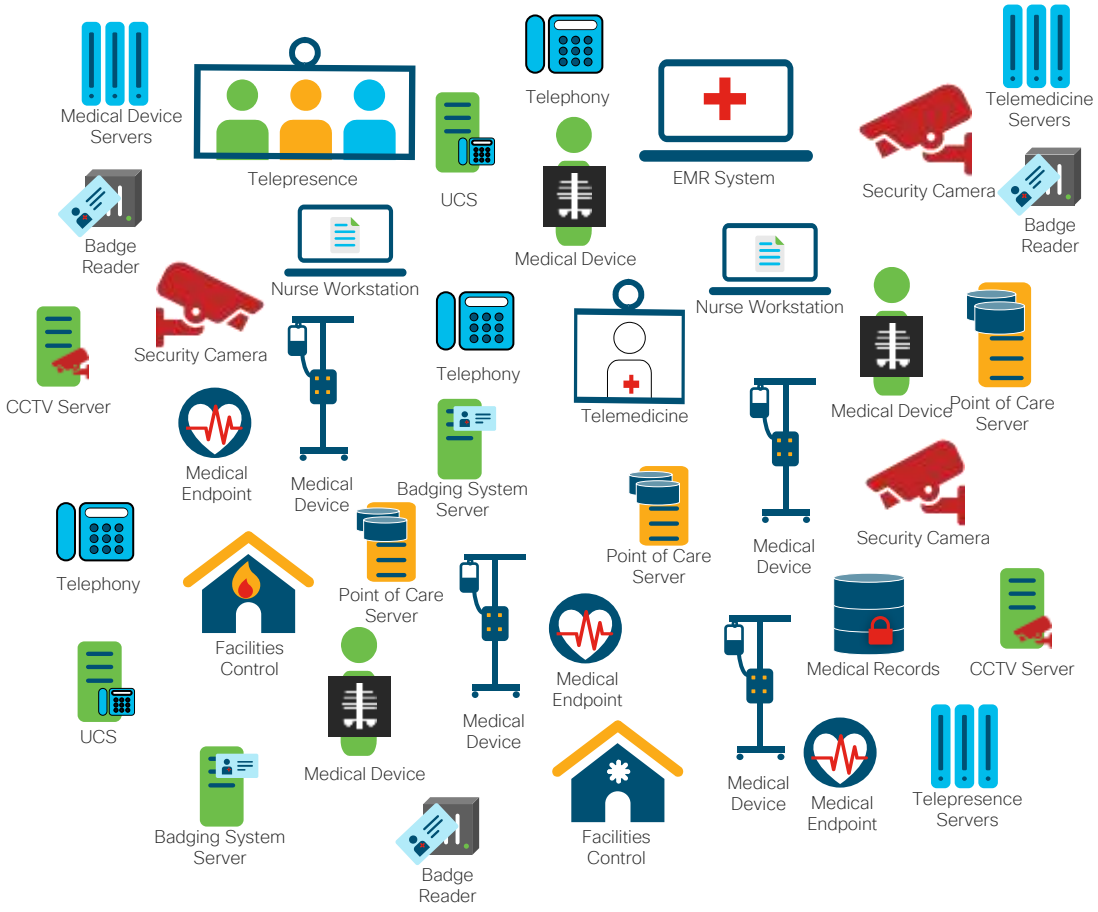
IT-Sicherheitsziele und Initiativen



Cisco Zero Trust Prinzipien

Wo kann ich anfangen?

Wer und was ist im Netz



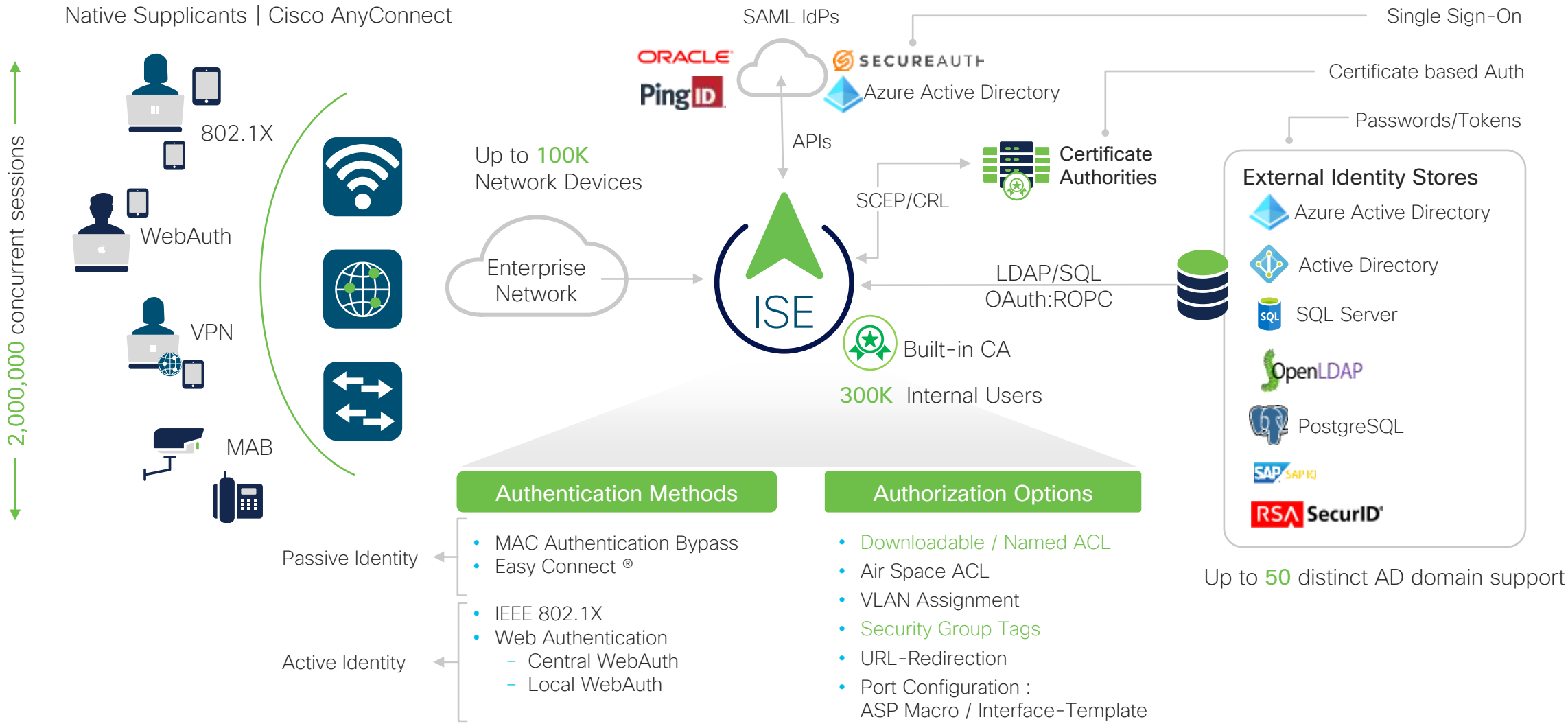
Wo?

On prem
Datacenter/XaaS

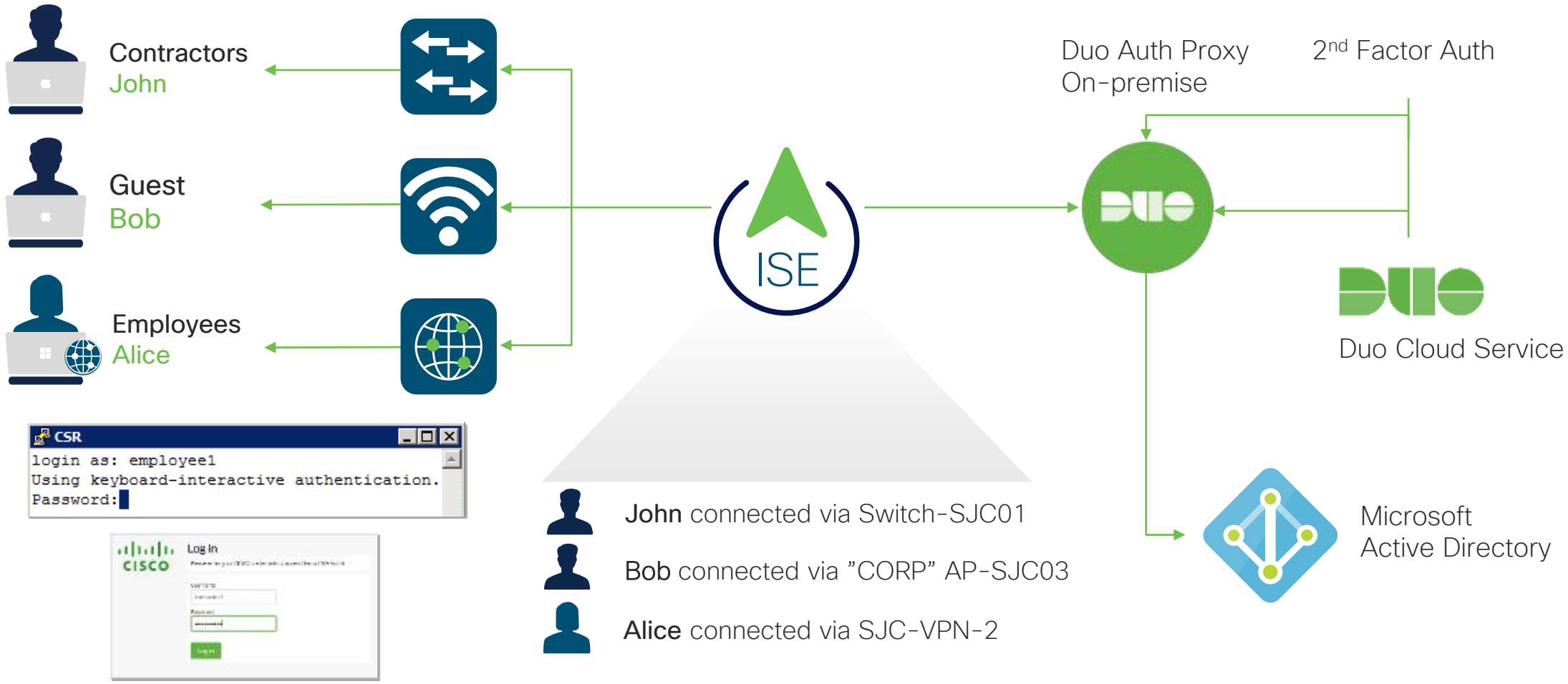
Gäste(w)lan

Büro-/Krankenhaus

Identitäten etablieren und kontrollieren



Ein zweiter Faktor für die Benutzer?



Der Gastzugang

1 million

# of supported Guest accounts

EMAIL PRINT SMS

Guest account notification options

Portal language customization

Social Media Login support

API

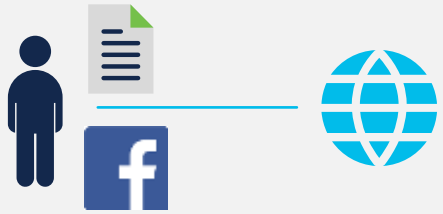
Manage guest accounts via REST

The 3 types of guest access

Hotspot

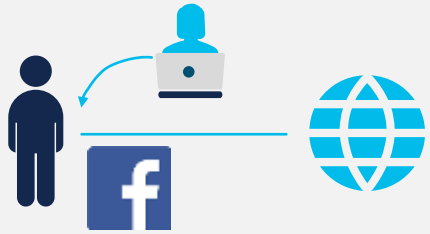
Immediate, un-credentialed Internet access

Self Registered



Self-registration by guests, Sponsors may approve access

Sponsored Guest Access



Authorized sponsors create account and share credentials

Endpoint Profiling

Endpoints send interesting data, that reveal their device type

ISE Data Collection Methods for Device Profiling

Active Probes: Netflow | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

AnyConnect: ACIDex

Feed Service (Online/Offline)

MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

AnyConnect Identity Extensions (ACIDex) | Device Sensor (DS)

Profiling Packages and Integrations

Medical Devices

Hospital

350+ Medical device profiles

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

IOT Building & Automation

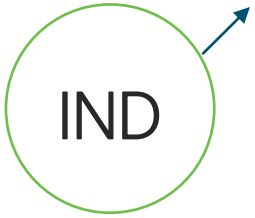
Library

- 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

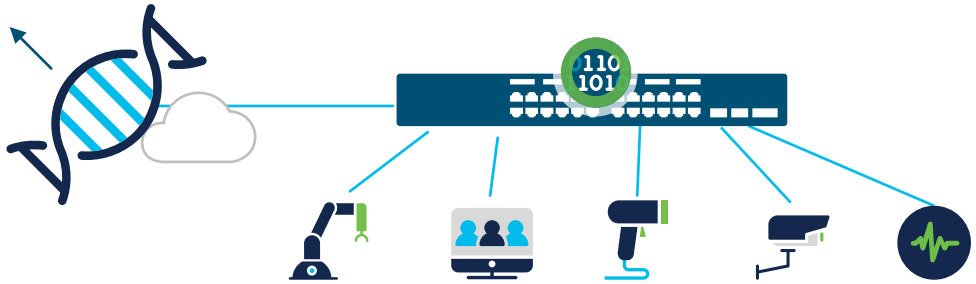
Factory

Industrial Devices

pxGrid



Cisco Industrial Network Director

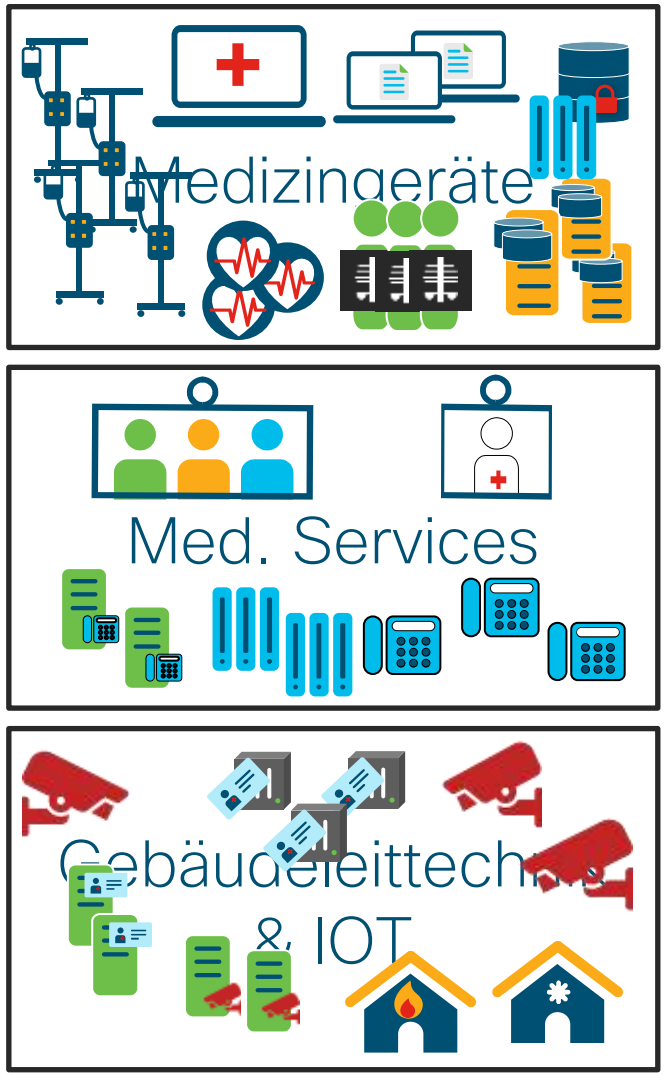


Cisco AI Endpoint Analytics

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

https://community.cisco.com/t5/tag/ise-endpoint-profile/tg-p/board-id/4561-docs-security

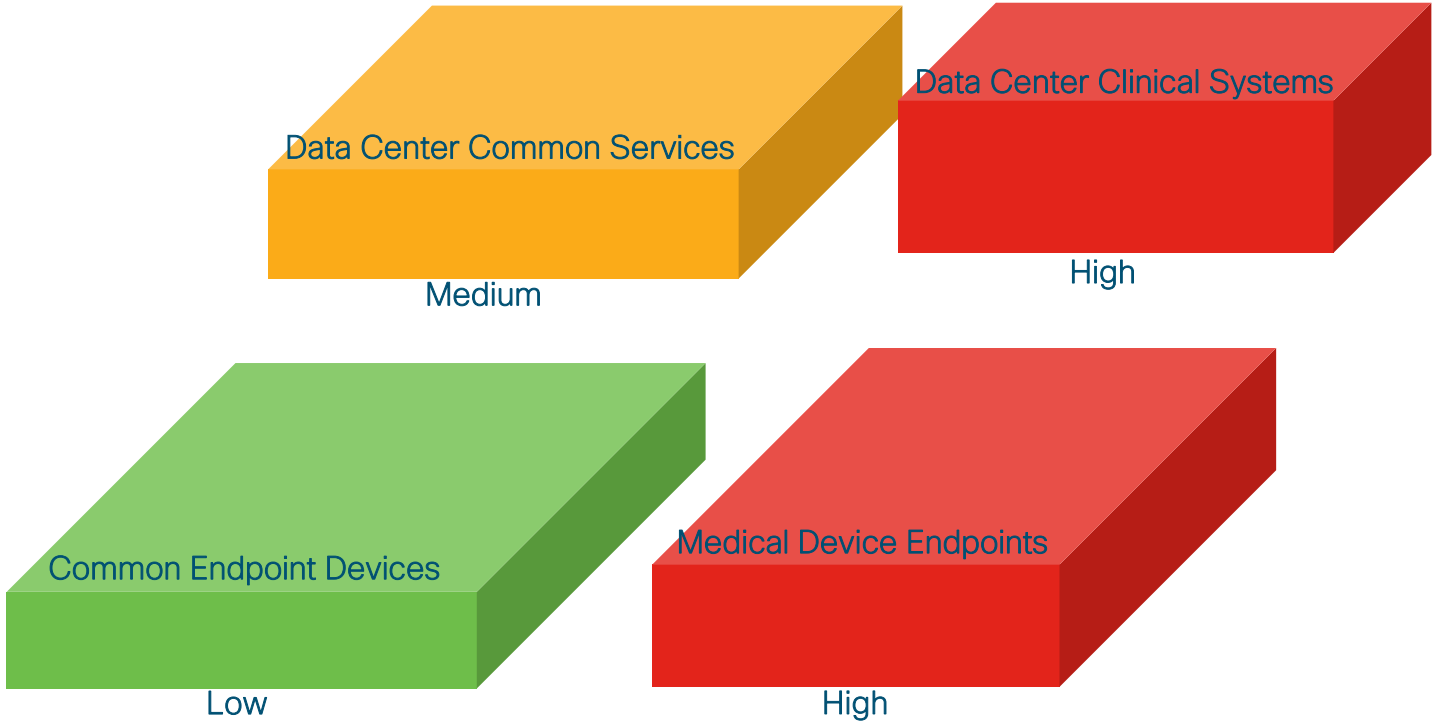
Bewertung



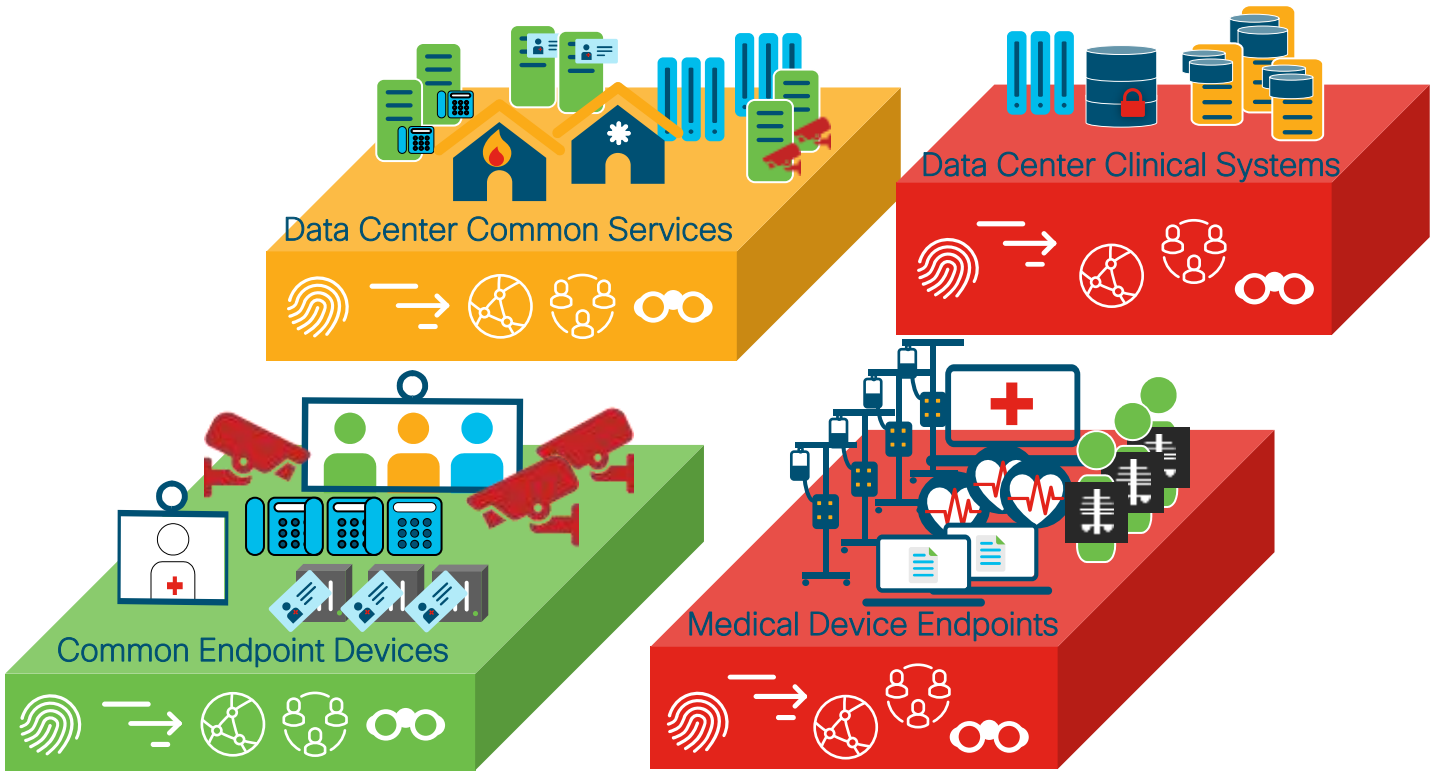
Mapping der Schutzziele / Richtlinien

Vertraulichkeit	Integrität	Verfügbarkeit

Enklaven definieren und Assets zuordn



Richtlinien & Kontrollen

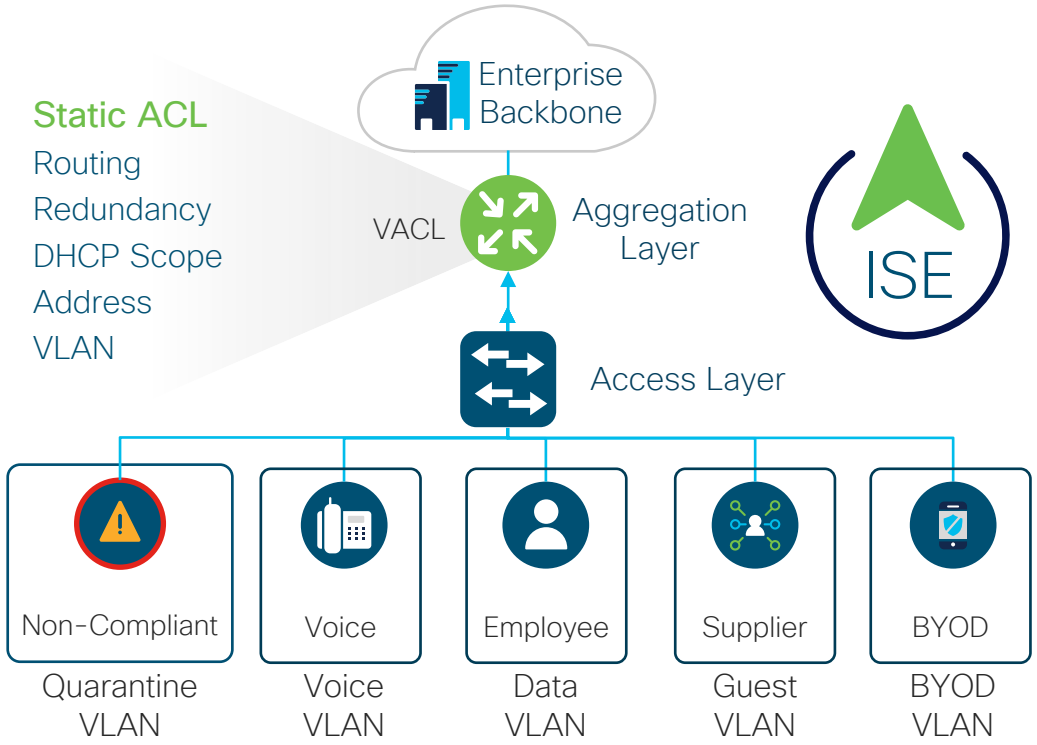


- Identitäts- und Vertrauensbildung
- Durchsetzung von Richtlinien
- Isolation
- Verfügbarkeit
- Sichtbarkeit

Access Netzwerke

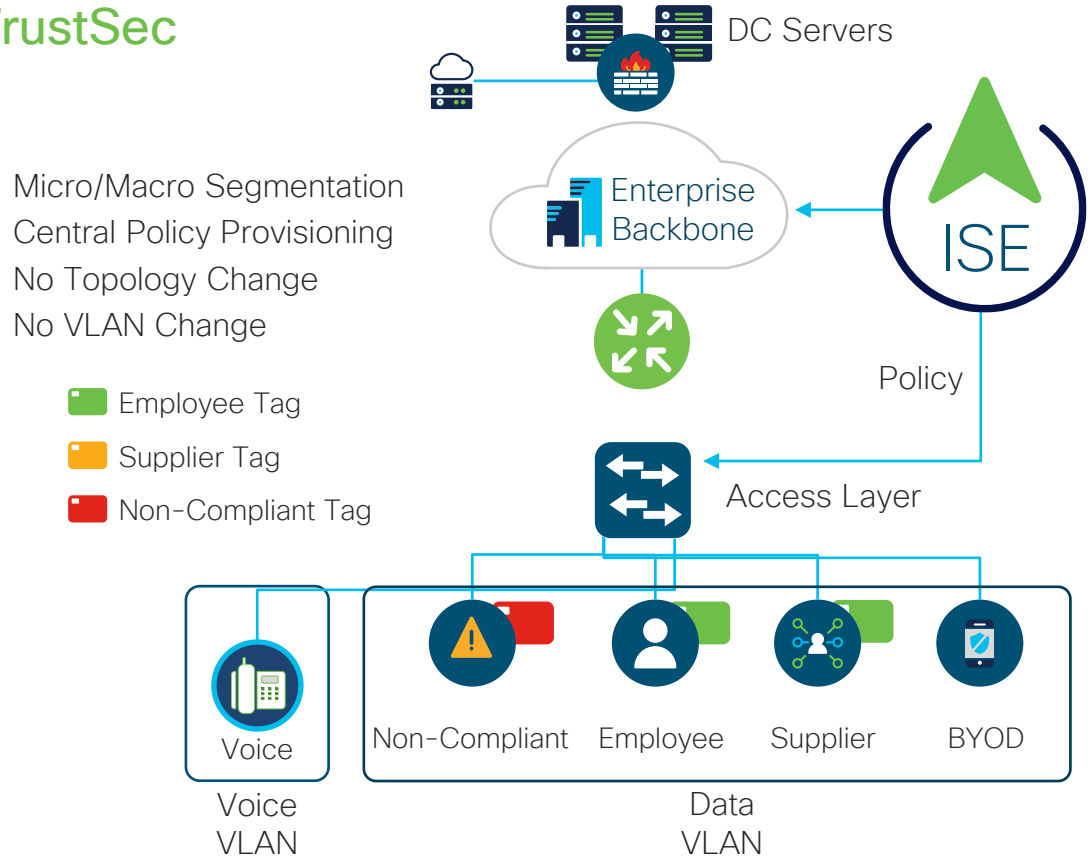
Kontextbasierte Segmentierung

Traditionelle Segmentierung



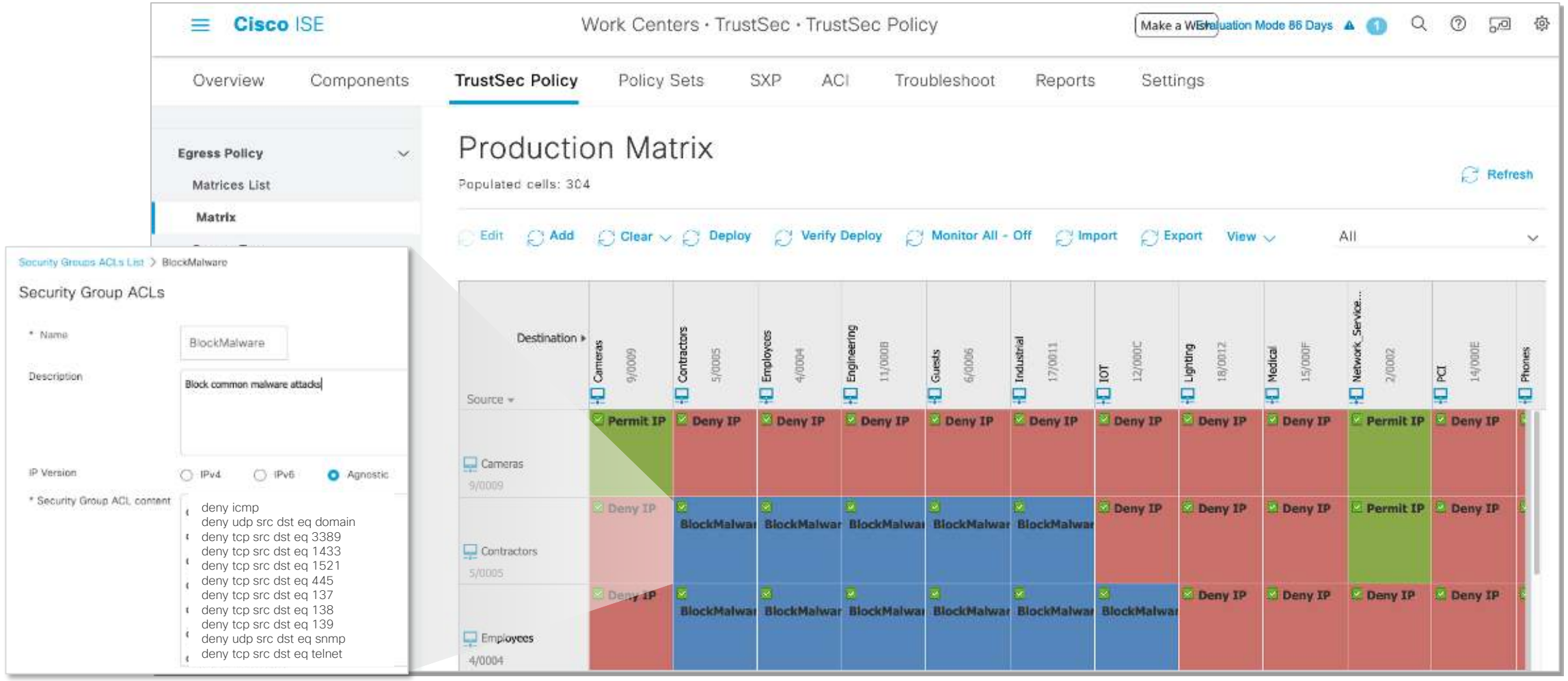
Security Policy based on Topology
High cost and complex maintenance

TrustSec



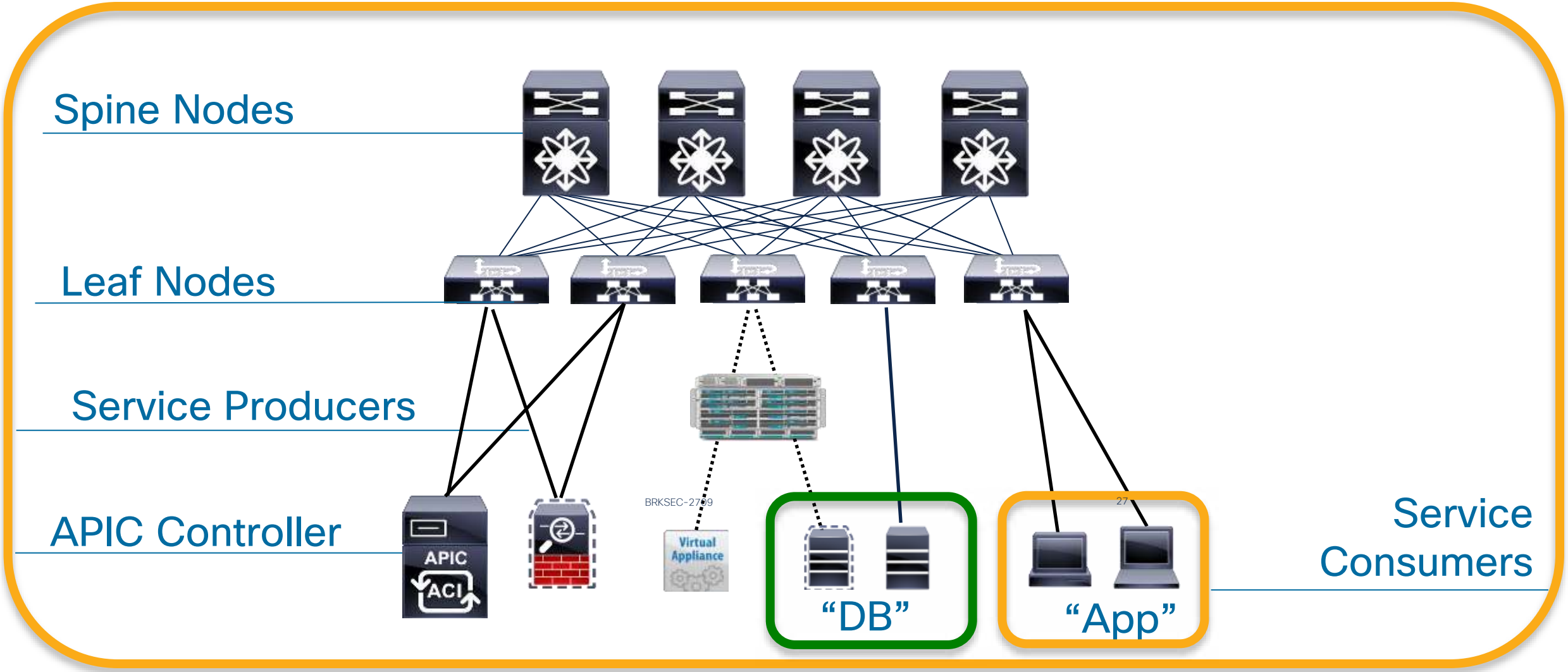
Use existing topology and automate
security policy to reduce OpEx

Ein Blick in eine Policy-Matrix

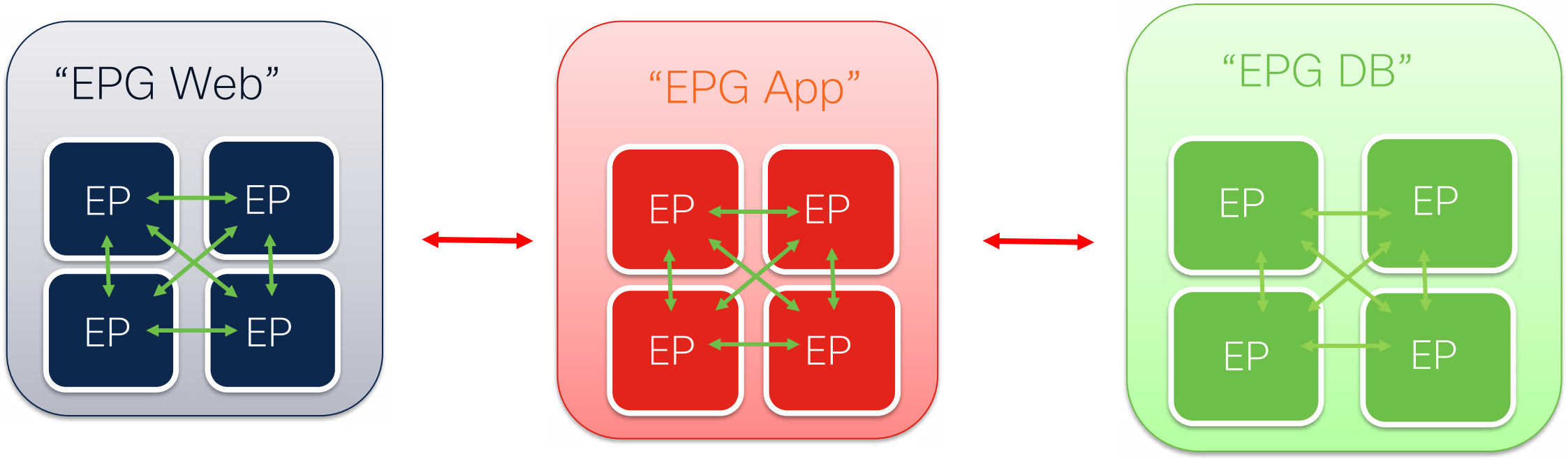


Datacenter&Cloud

ACI Devices Role



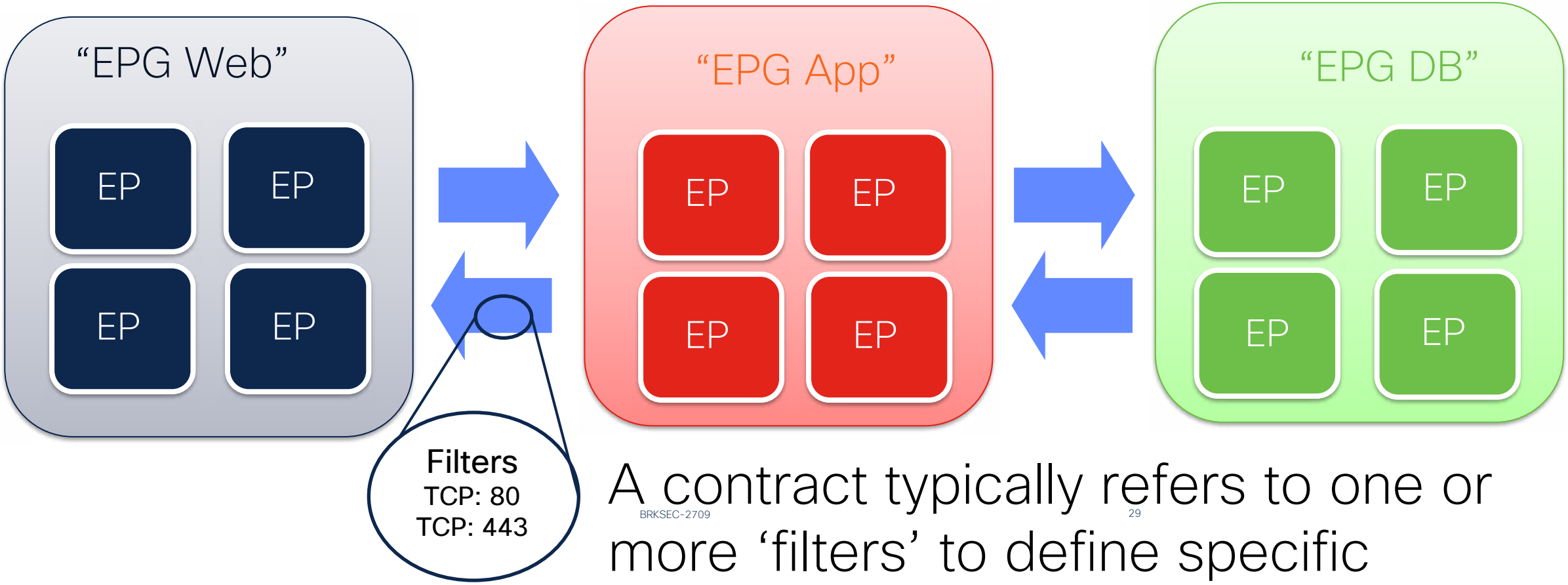
Endpoint Groups Communications



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

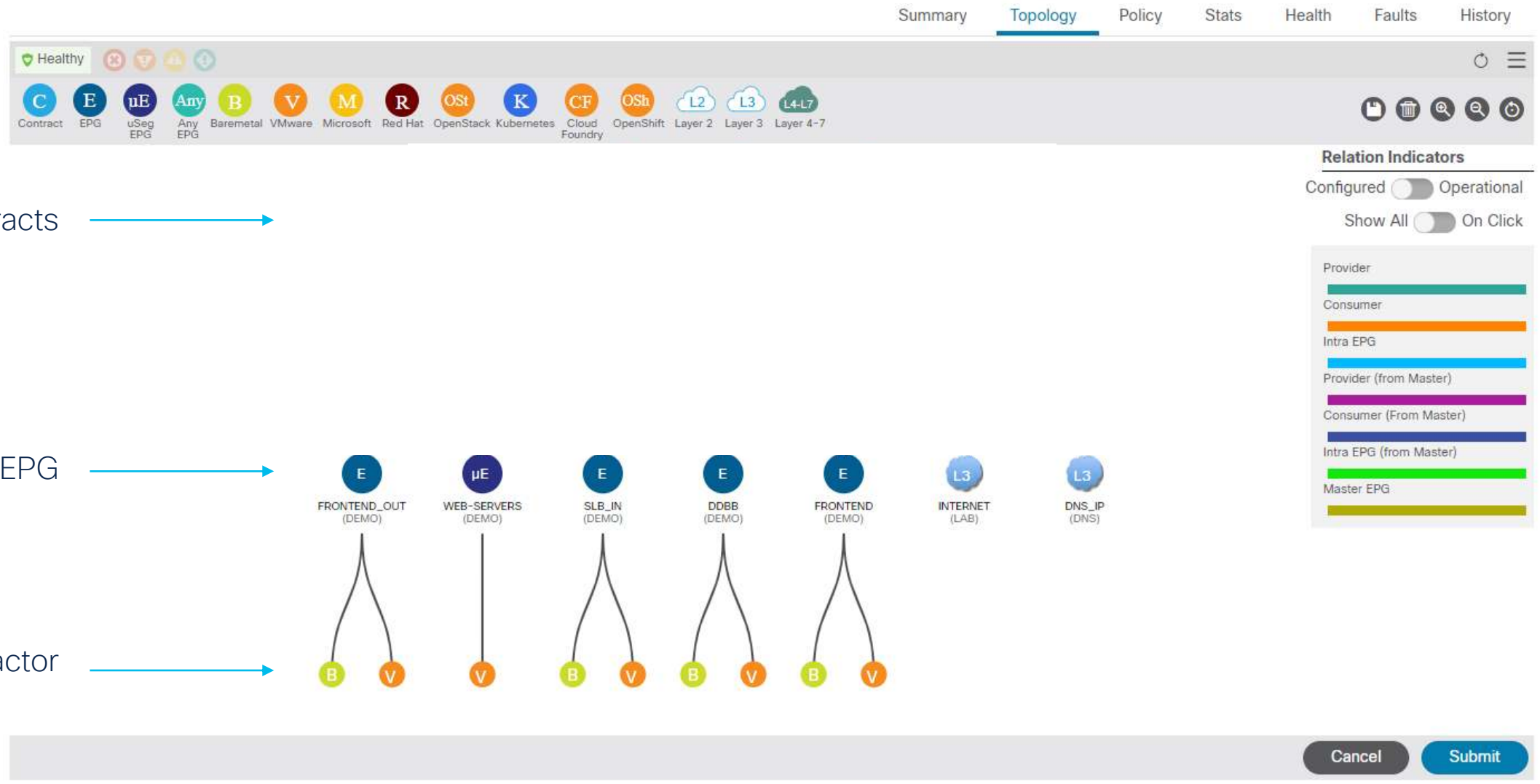
Communication between Endpoint groups is, by default, not permitted.

Contract : Kind of reflexive “Stateless” ACLs

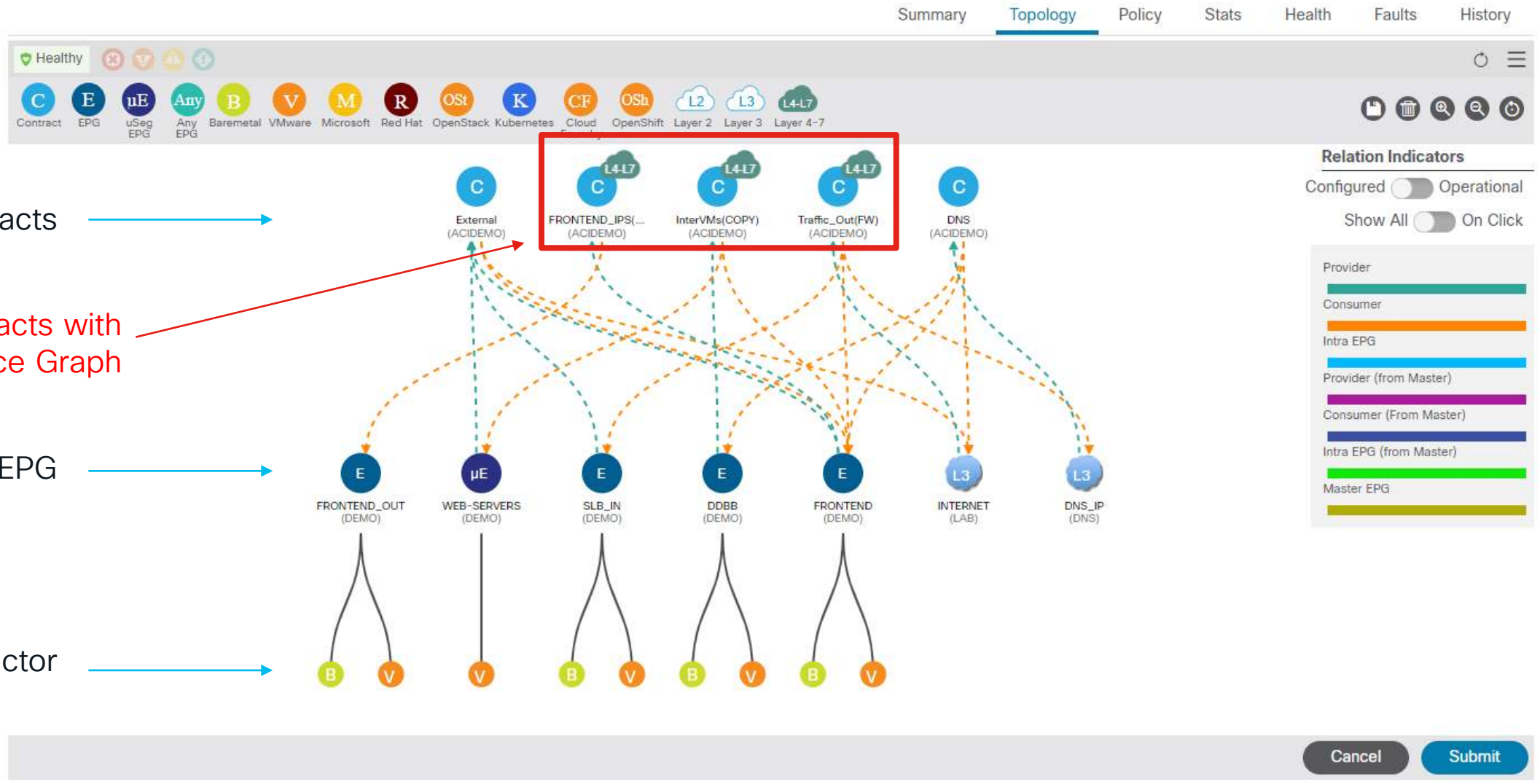


A contract typically refers to one or more ‘filters’ to define specific protocols & ports allowed between EPGs.

Application policy with contract



Application Policy with Contract



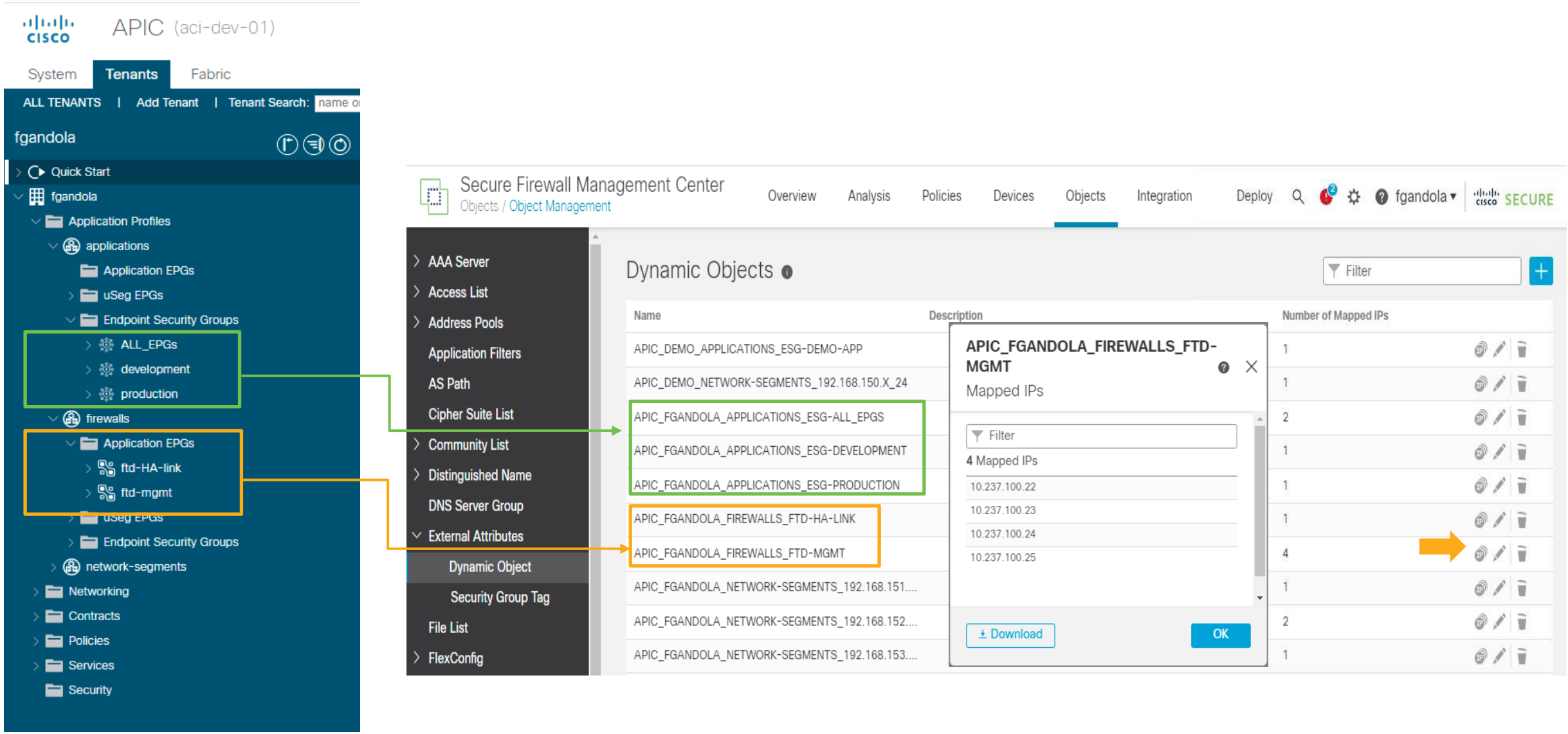
Contracts

Contracts with Service Graph

EPG

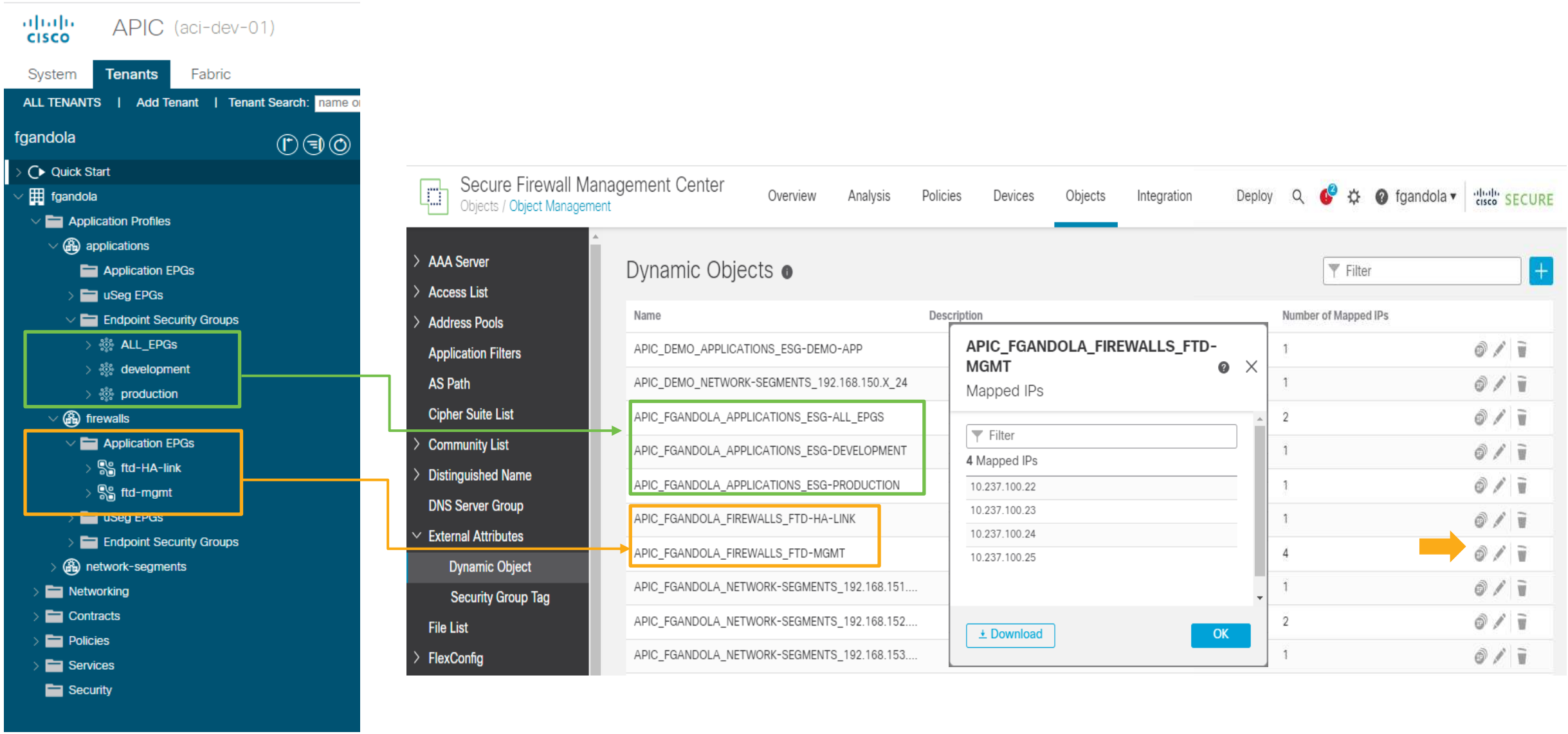
Form Factor

Kontext teilen

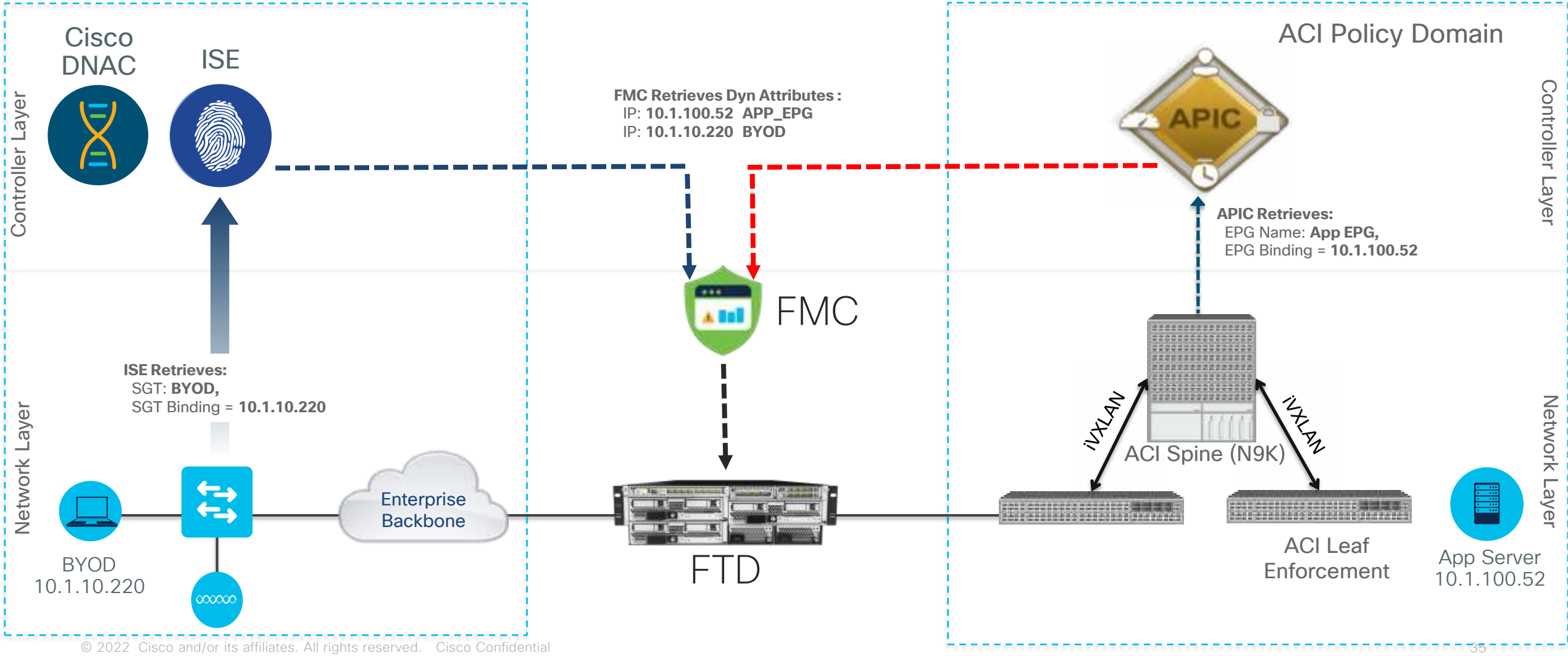


Datacenter/Cloud

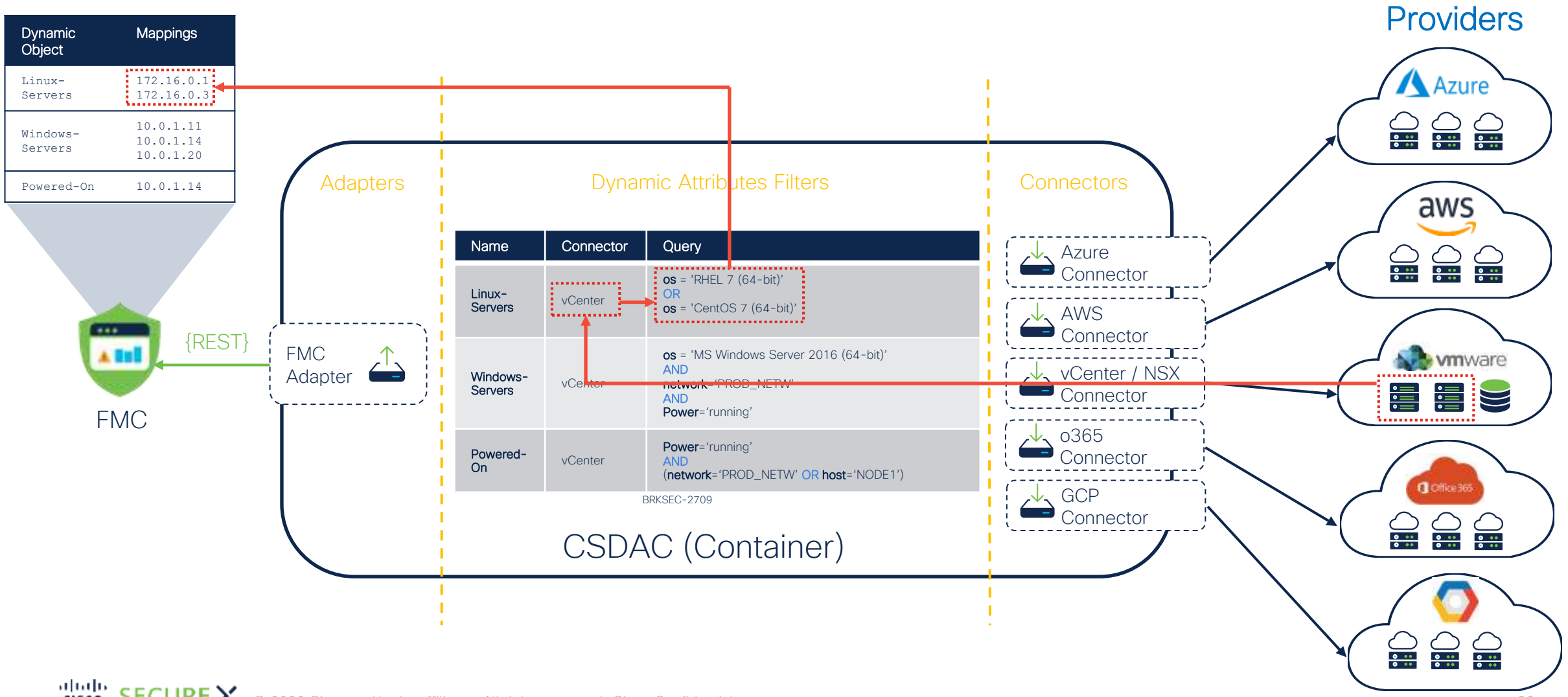
Kontext teilen



SGT/ACI Firepower Integration

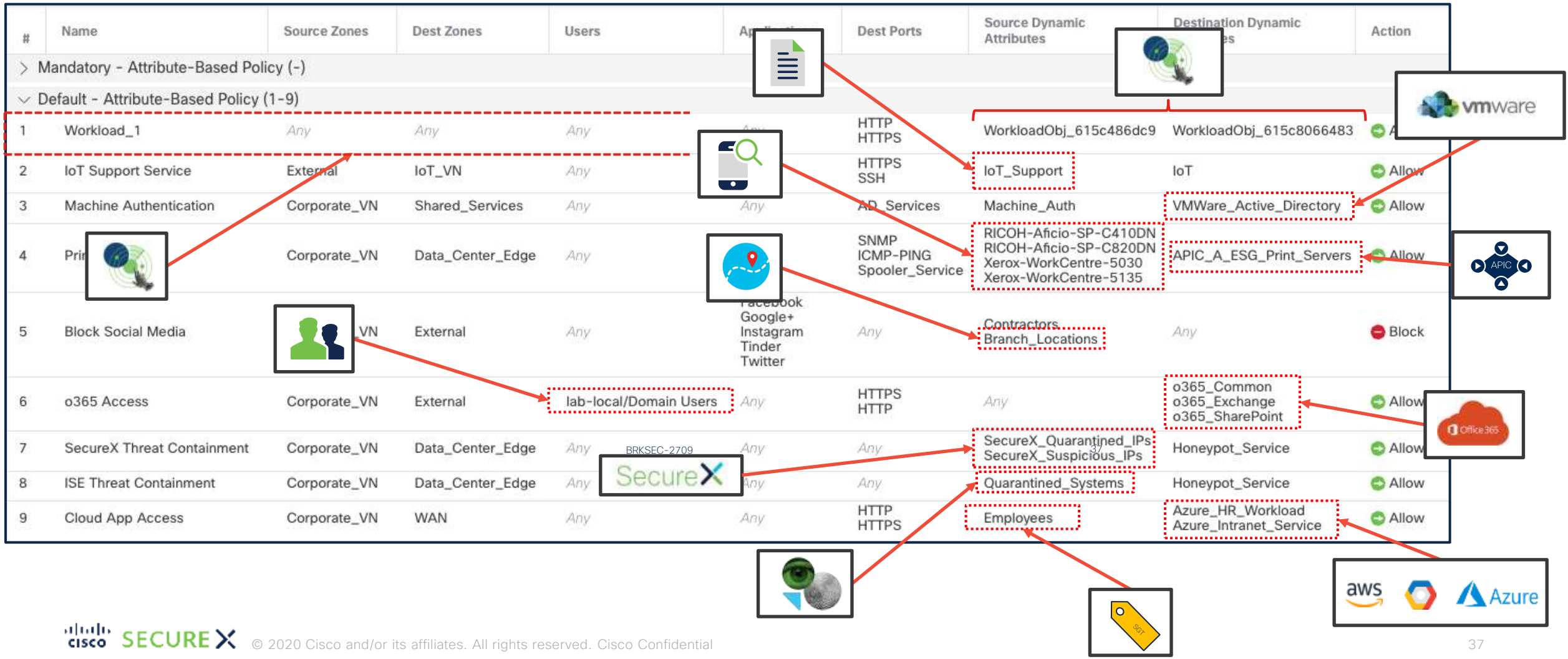


Architecture of the Dynamic Attributes Connector

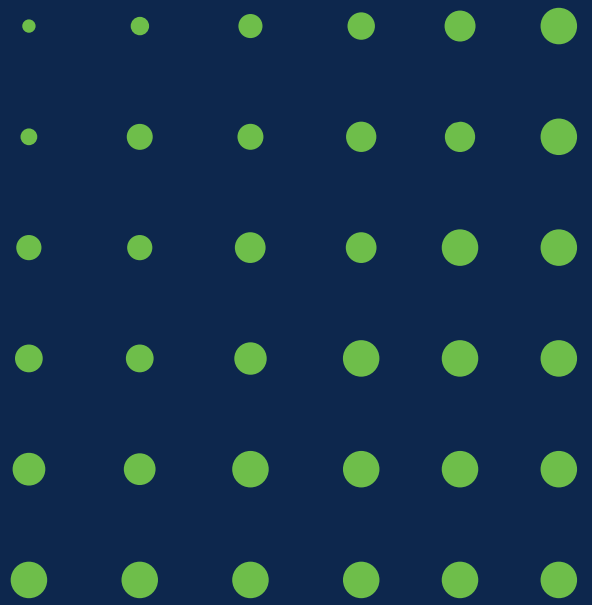


Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	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	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	A
2	IoT Support Service	External	IoT_VN	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Pri	Corporate_VN	Data_Center_Edge	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	VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	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	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow



Fazit



2025 Reimagine GERMANY