



**Security im Fokus:
Vom User bis zur Applikation - transparent und sicher!**

Oliver Knon

Senior Consultant, CCIE #42421

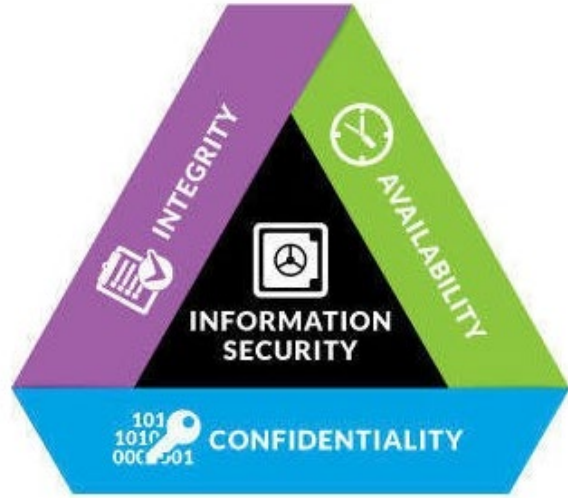
Enterprise Networking

19 Jahre bei SWS AG

Innovation, Technologie und Wertschöpfung



Schutzziele der IT Security



Confidentiality = Vertraulichkeit
Integrity = Integrität
Availability = Verfügbarkeit

IT Security und Regulatorik

- die EU Netz- und in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden haben...
- Das AktG schreibt in seinen §§ 91, 93 AktInformationssicherheitsrichtlinie aus 2016 (EU NIS-RL, mit einem Vorschlag der EU-Kommission für eine NIS-RL 2 vom 16. Dezember 2020)
- die EU Datenschutz-Grundverordnung aus 2016 (wirksam geworden in 2018, DSGVO, umfasst die Verarbeitung von personenbezogenen Daten und deren Datensicherheit
- das deutsche IT-Sicherheitsgesetz aus 2015 (ITSiG) inkl. der den Anwendungsbereich konkretisierenden BSI-Kritisverordnung (BSI-KritisV aus 2016 und 2017)
- das IT-Sicherheitsgesetz 2.0 (ITSiG 2.0, Inkrafttreten am 28.05.2021)
- das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) aus 2019
- das Zweite Datenschutzanpassungs- und Umsetzungsgesetz EU aus 2019 (2. DSAnpUG-EU), das den bereichsspezifischen Bundesdatenschutz an die Vorgaben der DSGVO anpasst
- die Digitale-Inhalte-Richtlinie der EU (DID-RL) aus 2019 und die entsprechenden, zurzeit für Deutschland im Gesetzgebungsverfahren befindlichen nationalen Umsetzungsgesetze
- GmbHG, § 43 der vorschreibt, dass die Geschäftsführer tG im gleichen Maßstab für die Organisation, Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder vor...
- Telekommunikationsgesetz
- ...

Ganzheitliche IT Security

Mensch

Security Bewusstsein und Skills

Organisation

Prozesse & Compliance

Technik

Werkzeuge und Technologien

Wie schützen wir uns?

...




Anti-Virus Firewall Intrusion Prevention Web Security

...

Etablierte Sicherheitsmechanismen

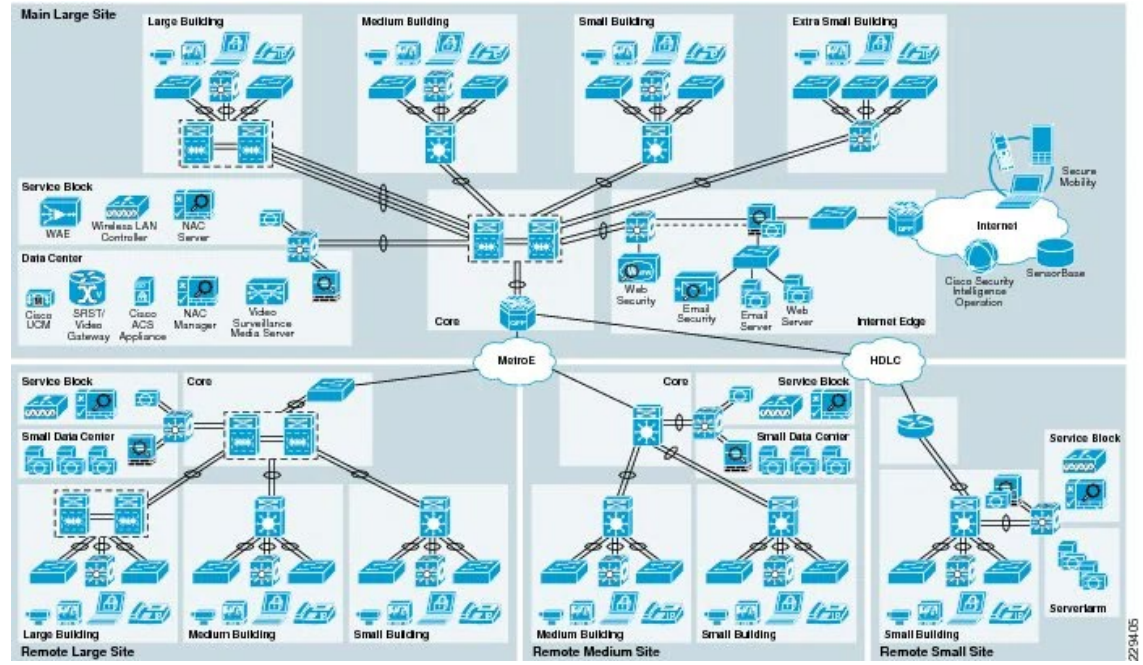
Neue Sicherheitsmechanismen



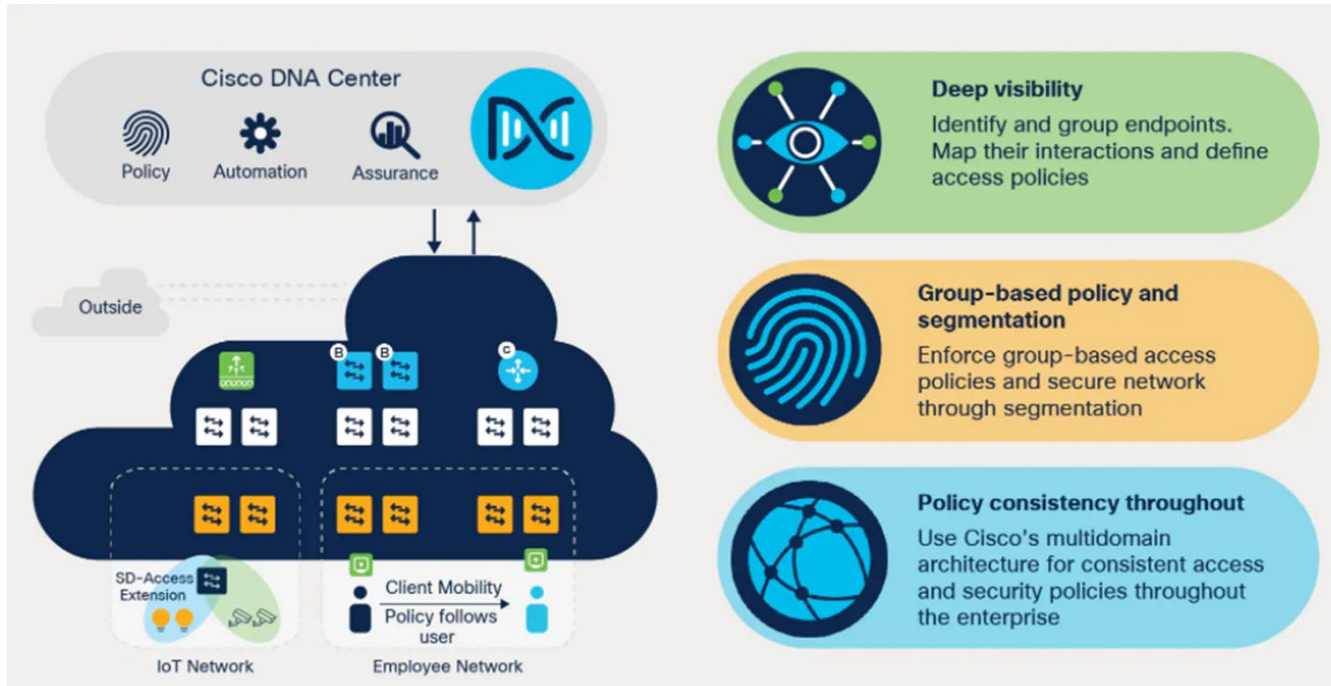
DNS Security Threat Intelligence Flow Analytics SIEM

...

Wo beginnen wir?



Segmentierung

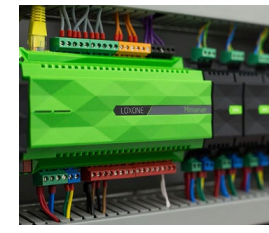
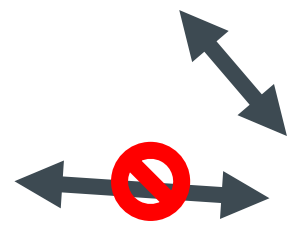
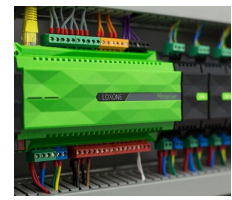
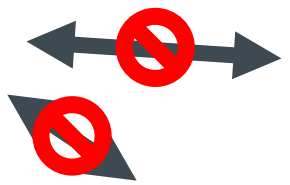
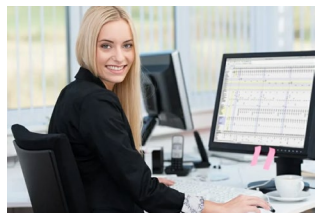


Deep visibility
Identify and group endpoints. Map their interactions and define access policies

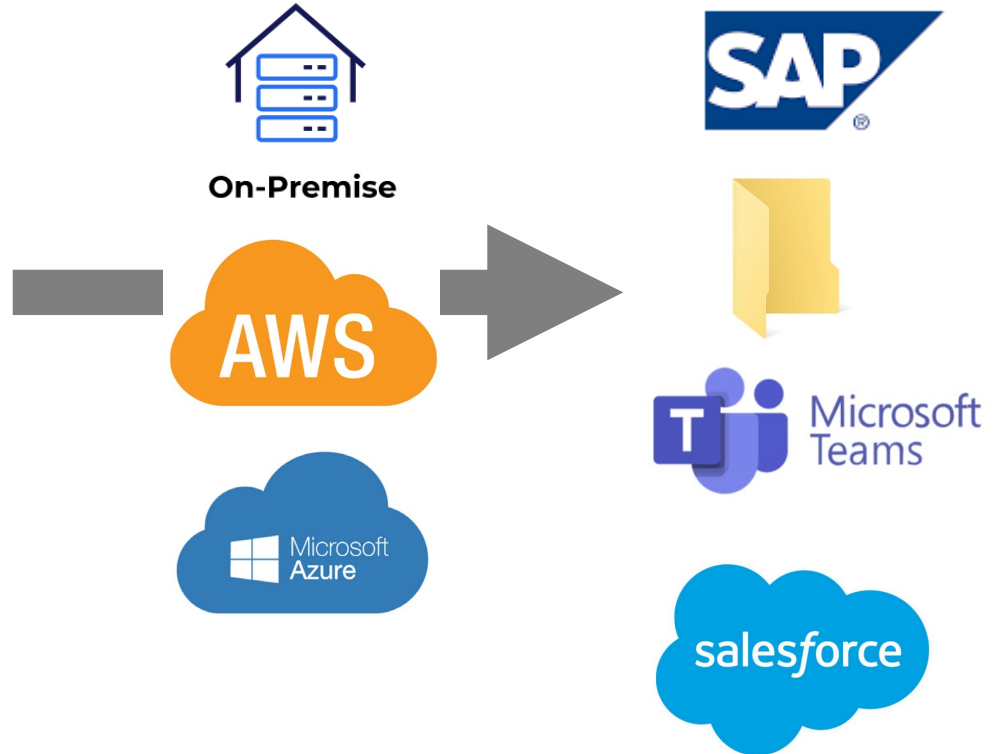
Group-based policy and segmentation
Enforce group-based access policies and secure network through segmentation

Policy consistency throughout
Use Cisco's multidomain architecture for consistent access and security policies throughout the enterprise

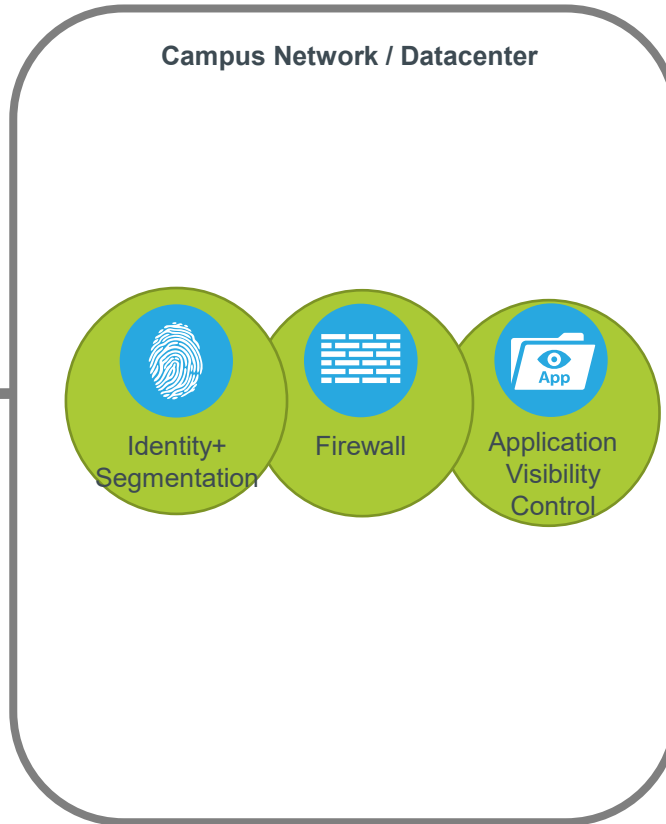
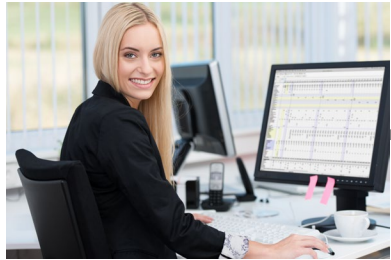
Angriffsfläche verkleinern



Business Flows absichern!



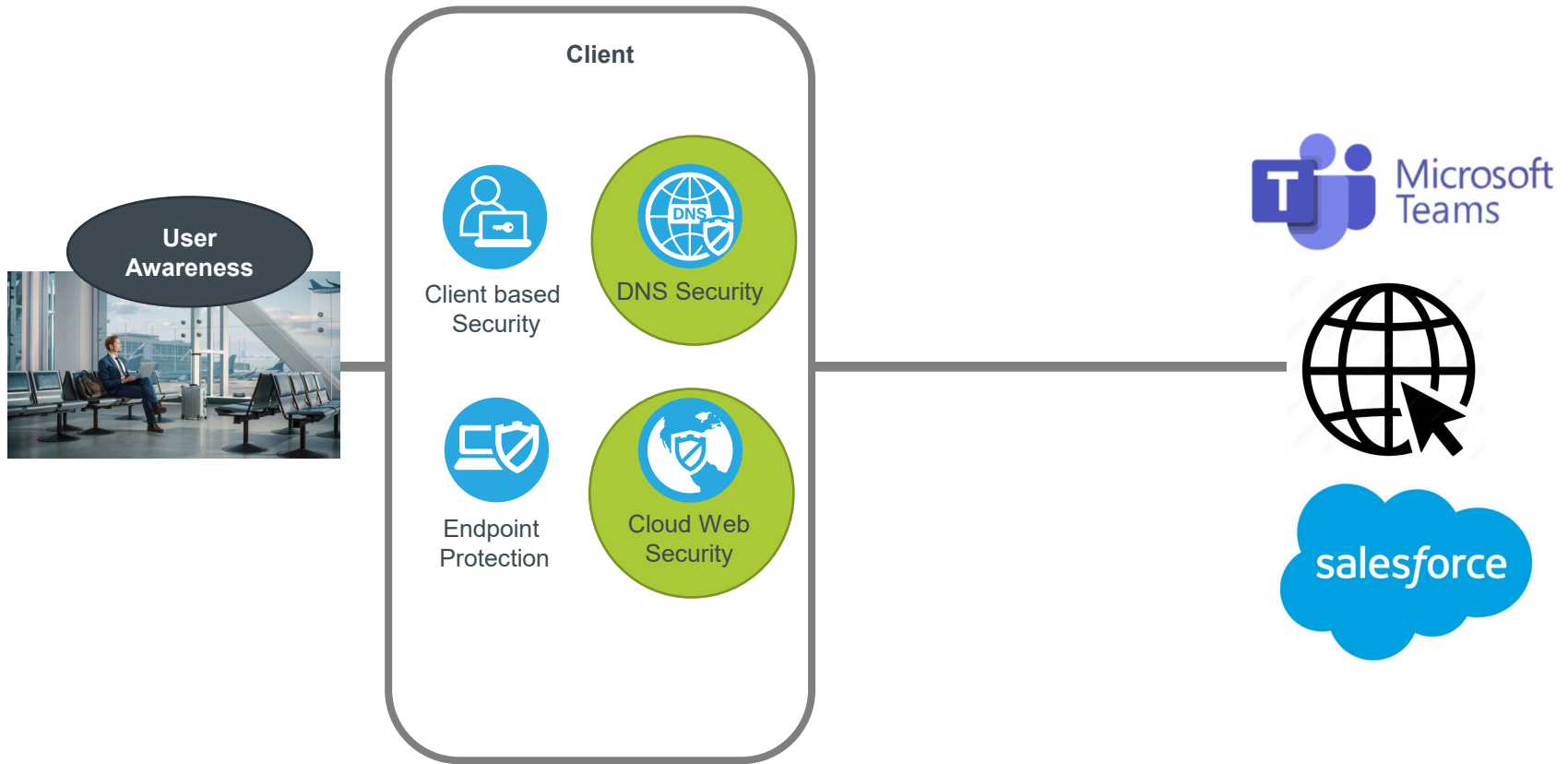
Office Client



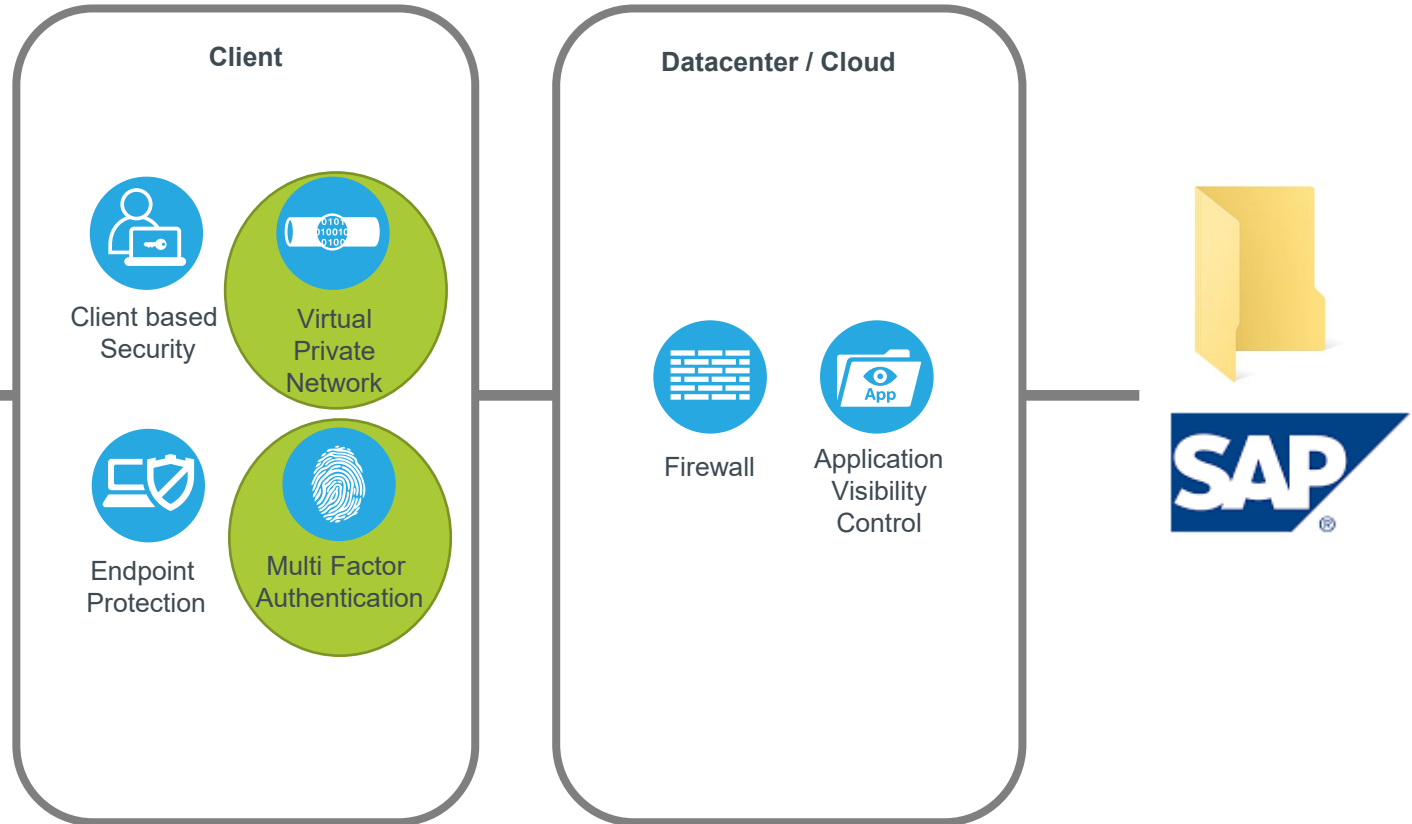
E-Mail



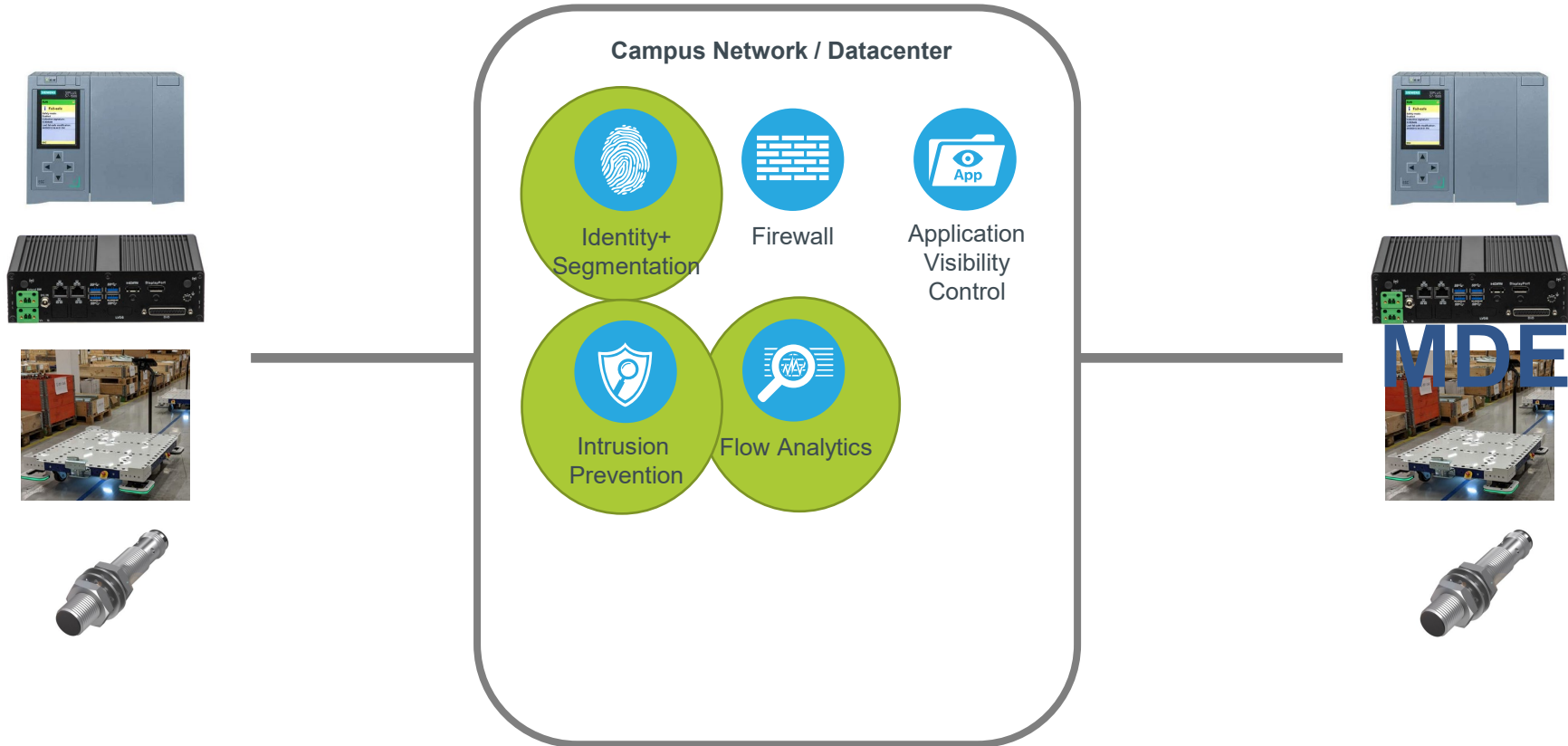
Der Vertriebsmitarbeiter



Der Vertriebsmitarbeiter

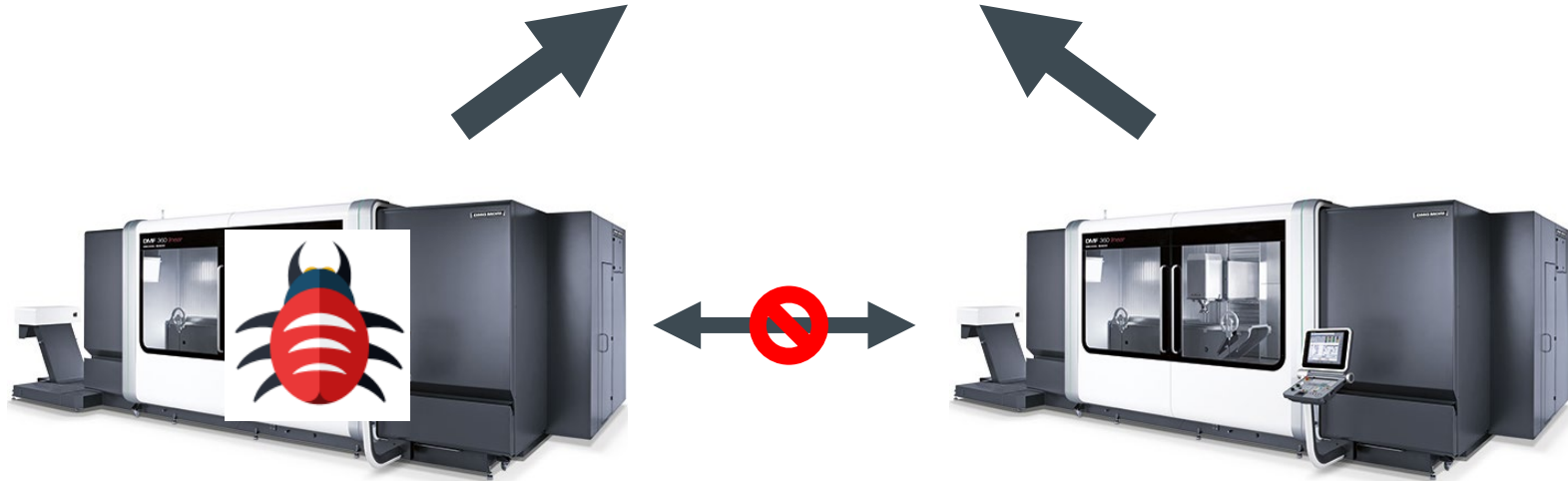


Produktionsumgebungen

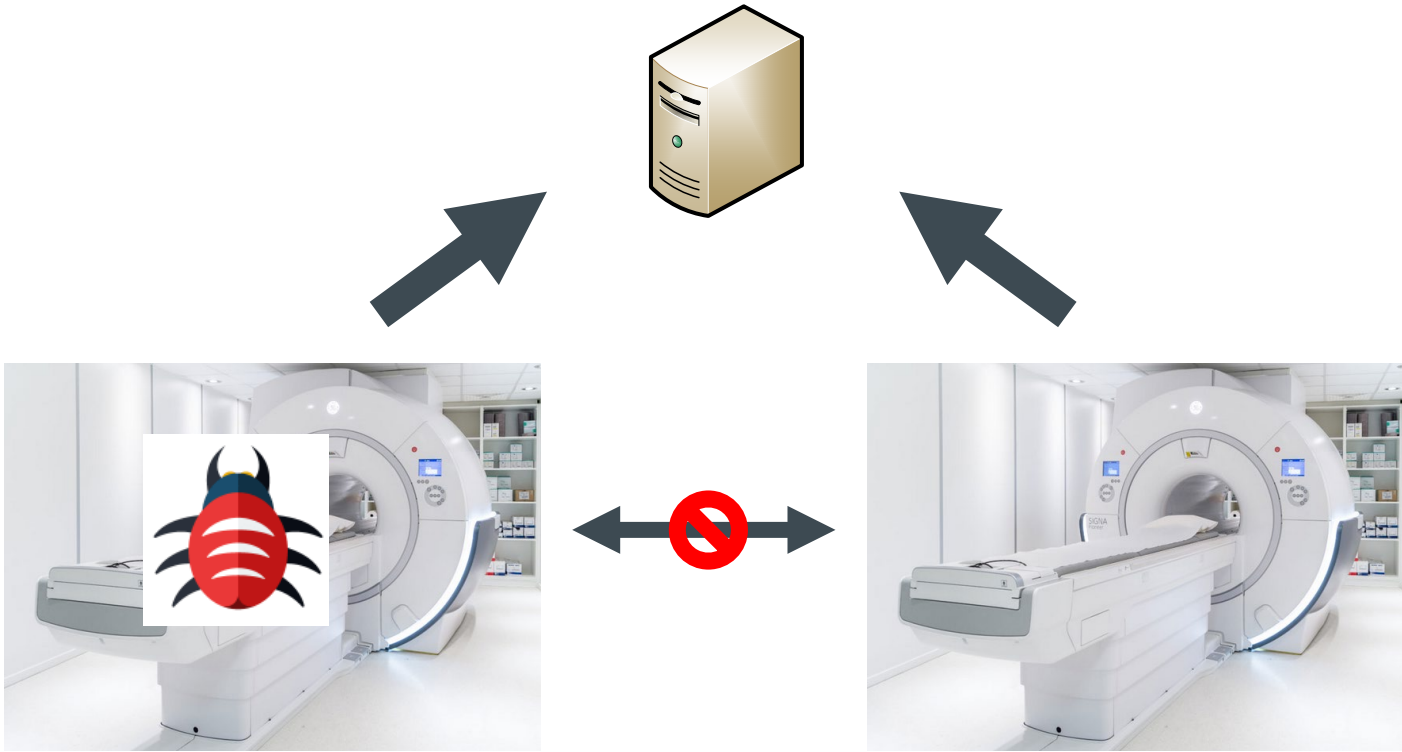


Produktionsumgebungen

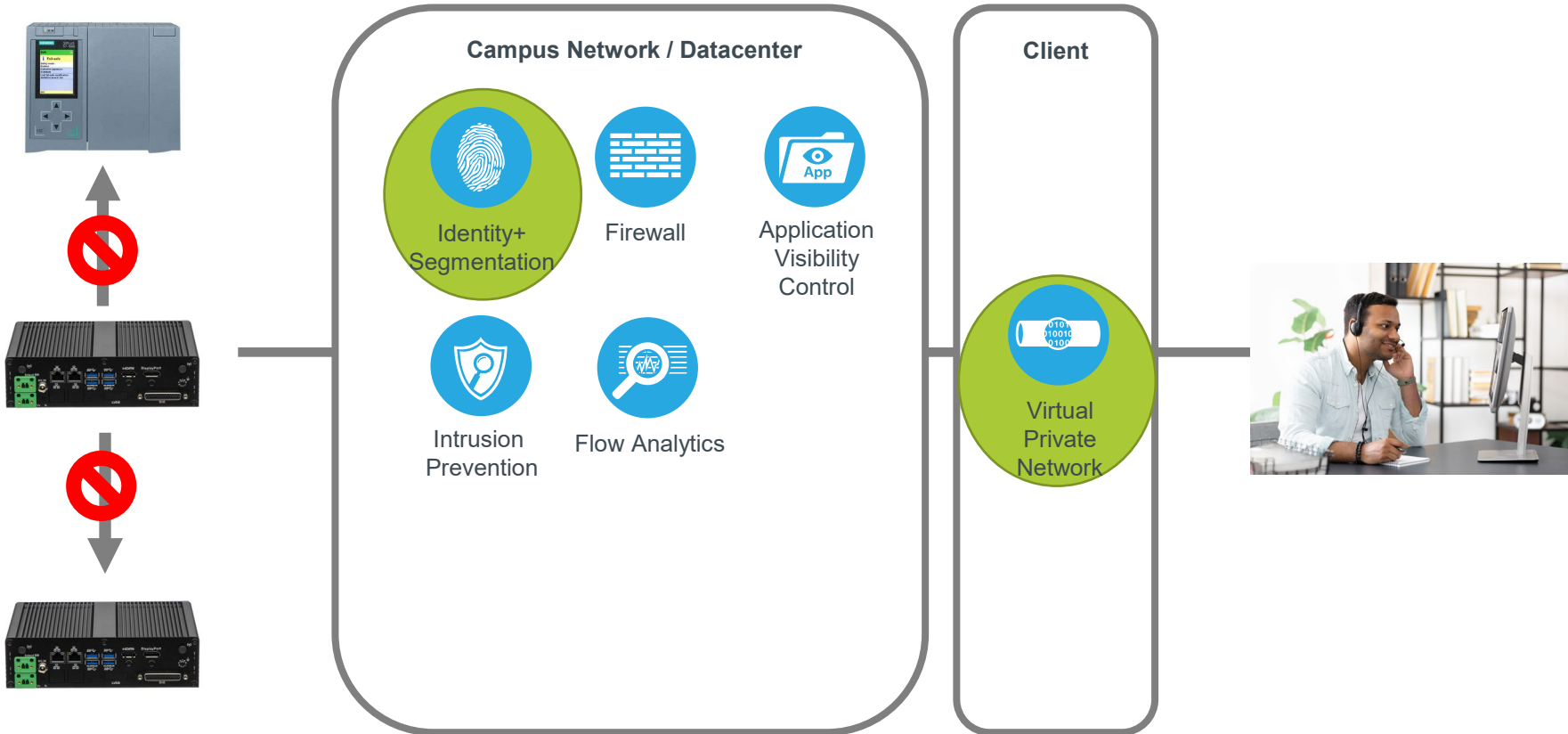
MDE



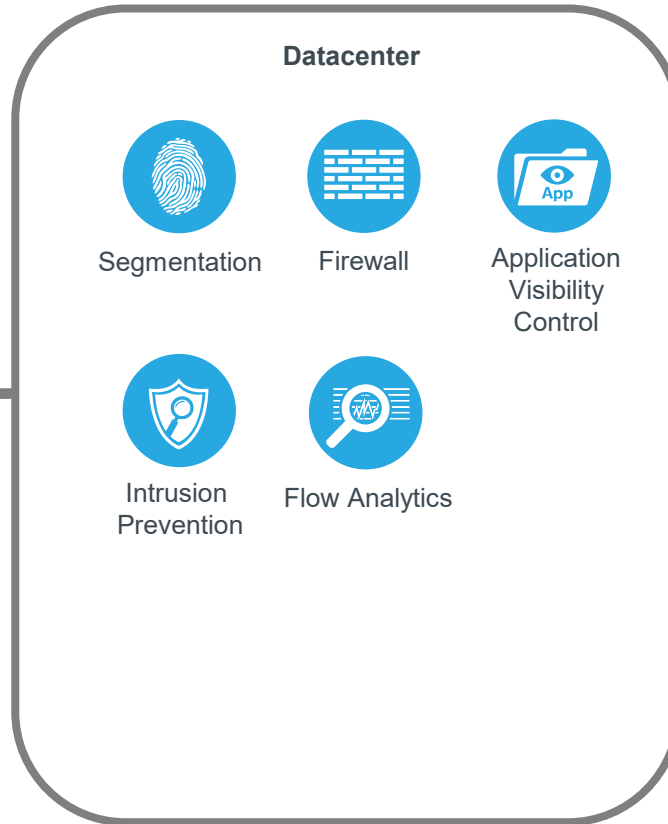
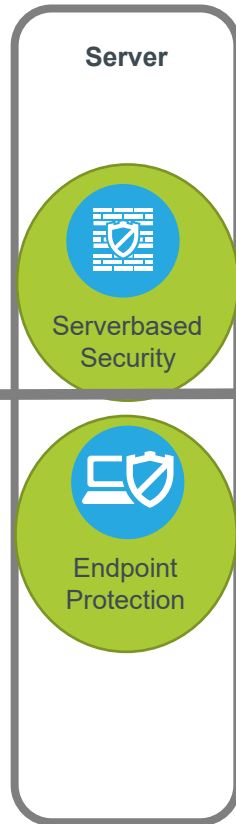
Produktionsumgebungen



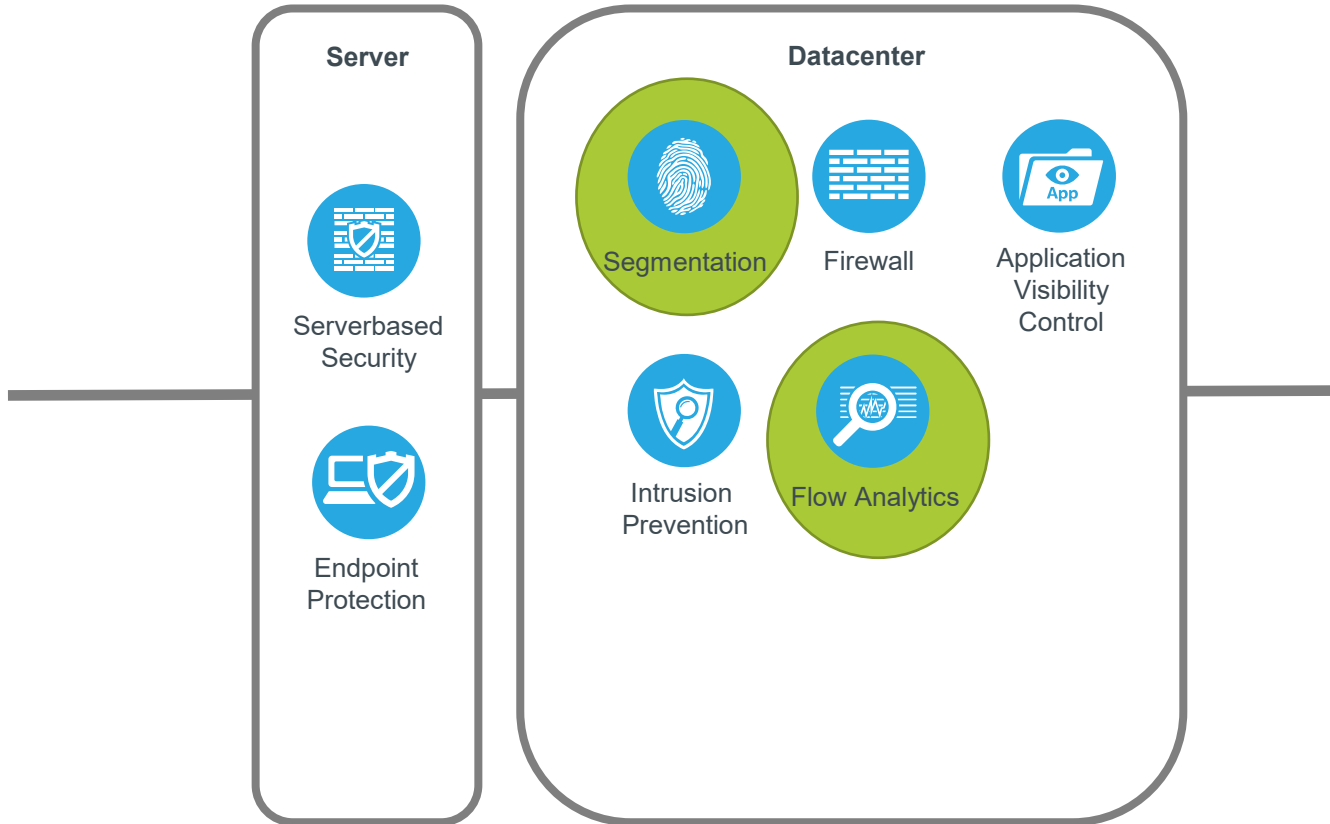
Der externe Servicetechniker



Server to Server



Server to Server



Transparenz / Nachvollziehbarkeit



Log-Daten!



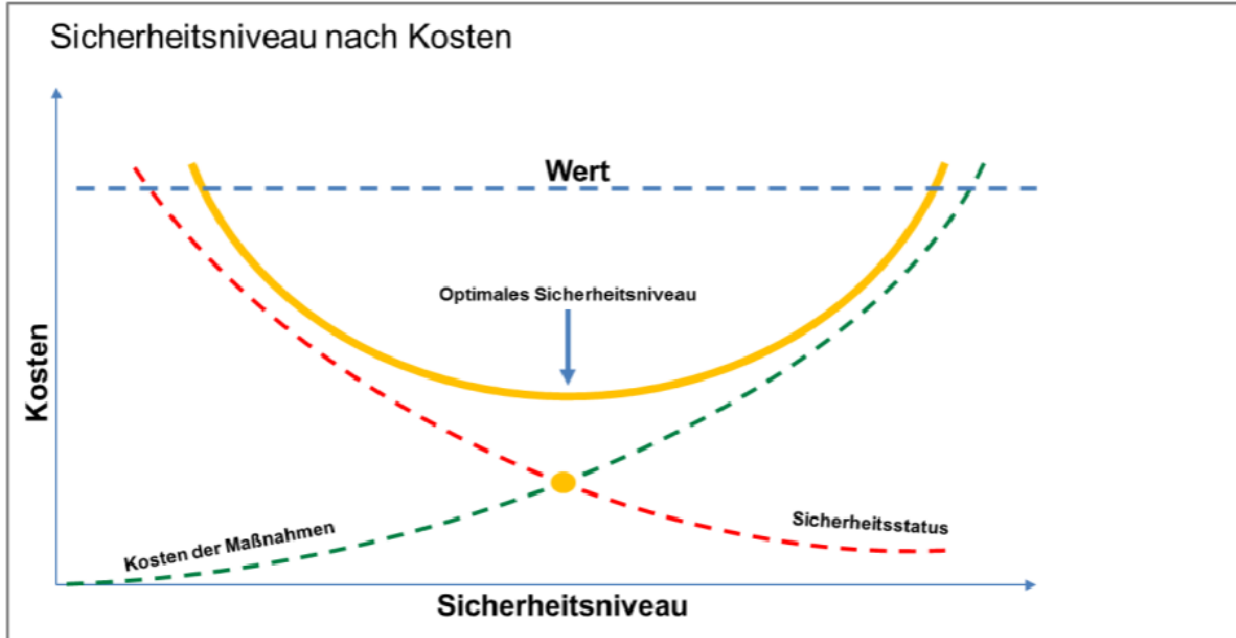
Security Betrieb



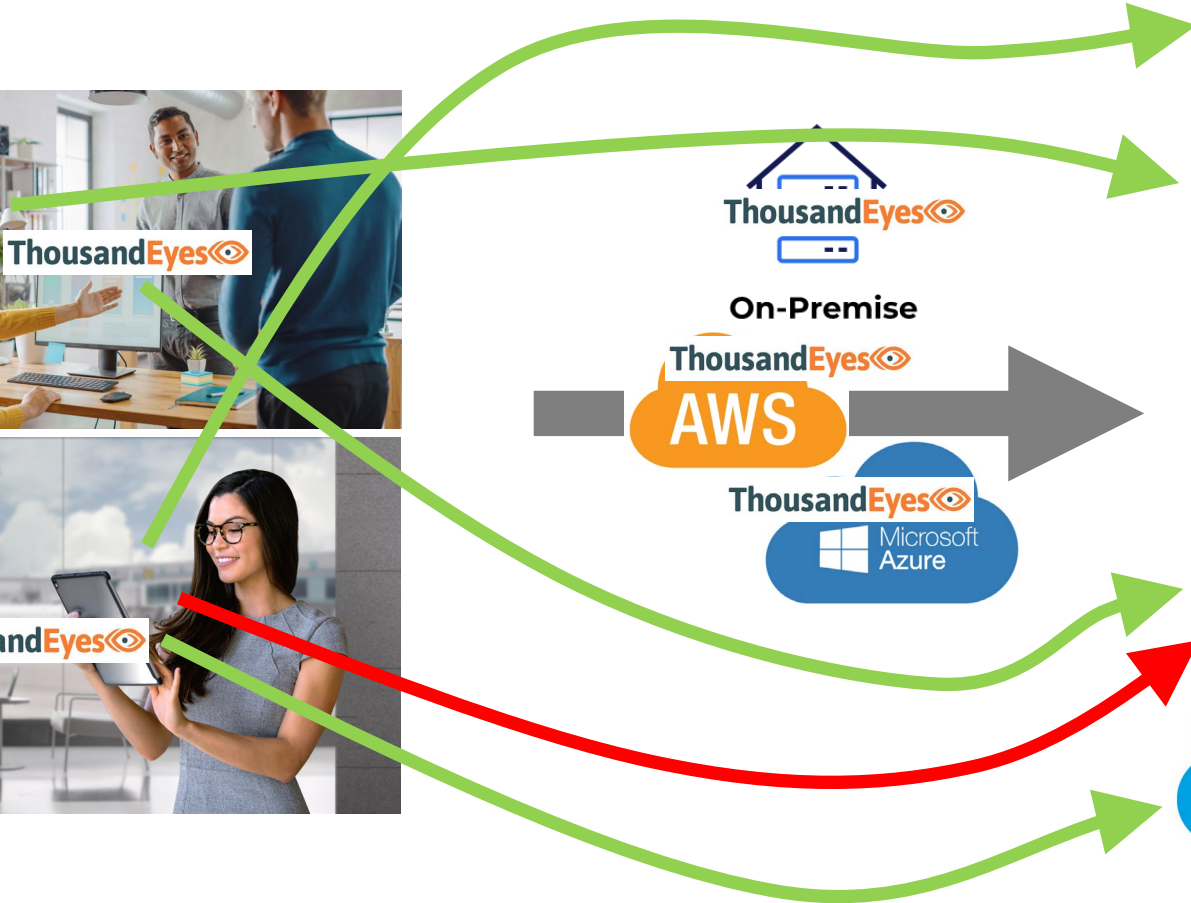
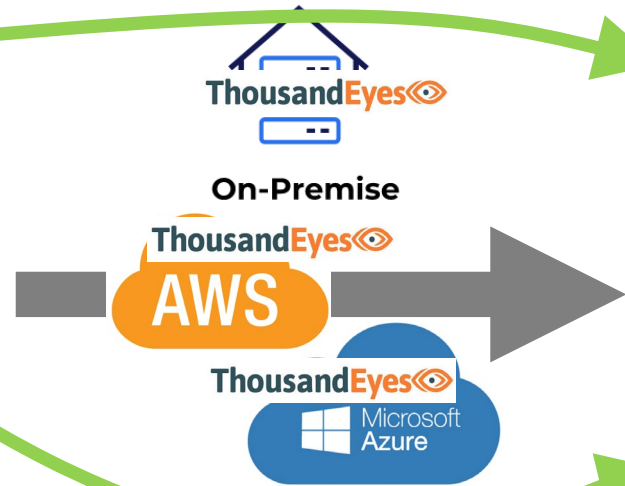
Identity + Segmentation	Firewall	Application Visibility Control	Virtual Private Network
Intrusion Prevention	Anti-Malware	Threat Intelligence	Multi Factor Authentication
Flow Analytics	Endpoint Protection	DNS Security	Cloud Web Security

SIEM
Security Information and Event Management

IT-Security Kosten



Quality of Experience



Thousand Eyes

Path Visualization

0 hops 22 hops

Showing: **6 of 6 Agents** ▾ Hide IP Address labels ▾

Grouping: **Agents by Agent** ▾ Interfaces by IP Address ▾ Destinations by IP Address ▾

Highlighting: **Forwarding Loss > 5 % (4 nodes)** ▾ Link Delay ▾

Selecting: Click a node or link **Info (2)** ▾

Highlight nodes that match all / any

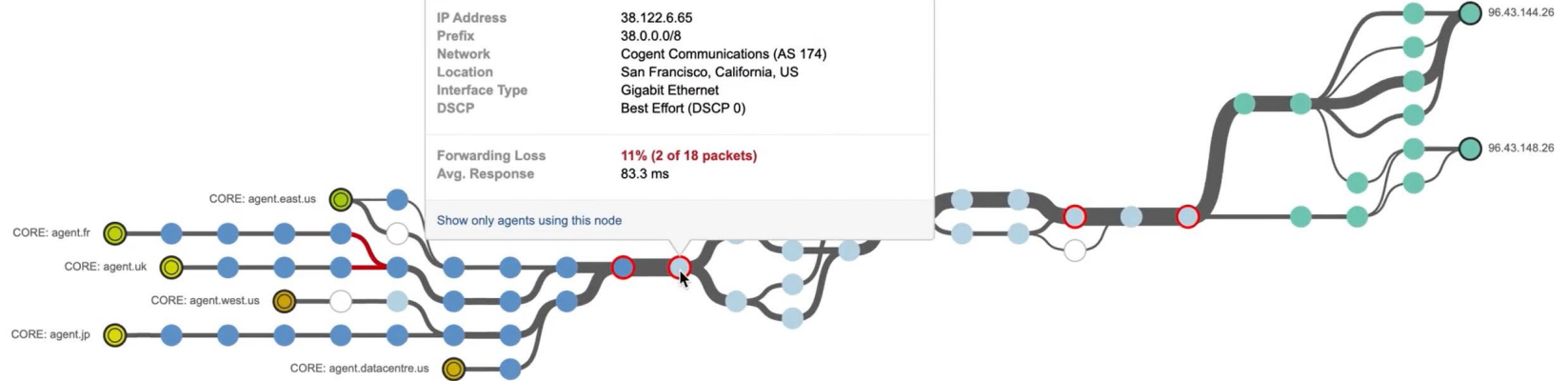
○ Node (with forwarding loss)

gi0-0-0-19.209.nr11.b001900-0.sfo01.atlas.cogentco.com

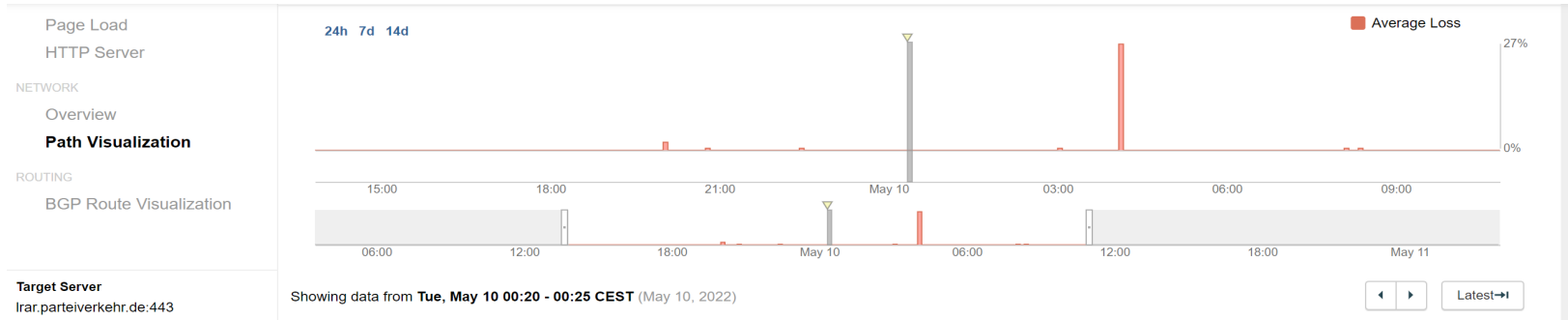
IP Address	38.122.6.65
Prefix	38.0.0.0/8
Network	Cogent Communications (AS 174)
Location	San Francisco, California, US
Interface Type	Gigabit Ethernet
DSCP	Best Effort (DSCP 0)

Forwarding Loss	11% (2 of 18 packets)
Avg. Response	83.3 ms

Show only agents using this node



Thousand Eyes



Path Visualization

Showing: **4 of 4 Agents** ▼ Hide IP Address labels ▼

Grouping: Agents by **Agent** ▼ Interfaces by **IP Address** ▼ Destinations by **IP Address** ▼

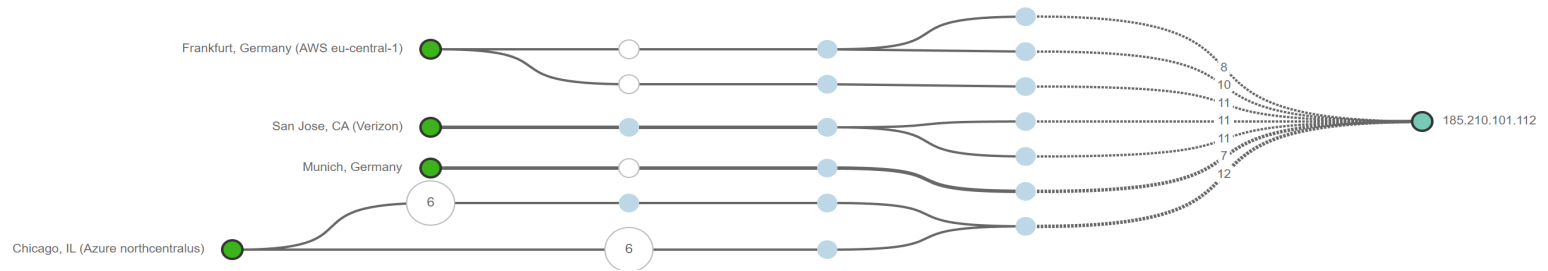
Highlighting: **Forwarding Loss > 10 %** (0 nodes) ▼ **Link Delay > 100 ms** (0 links) ▼

Selecting: Click a node or link **Info (1)** ▼

Highlight nodes that match **all / any**

Search on Network, Country, IP address, Prefix, or Title... 🔍

3 hops 0 hops





**Vielen Dank für eure
Aufmerksamkeit.**

Fragen?

**IT for
innovators.**

Member of ACP Group