SWS
COMPUTERSYSTEME
Member of ACP Group

SWS Computersysteme AG

SWS COMPUTERSYSTEME
Member of ACP Group

Cisco Secure Network Analytics und Cisco Secure Firewall - Visibility im Netzwerk

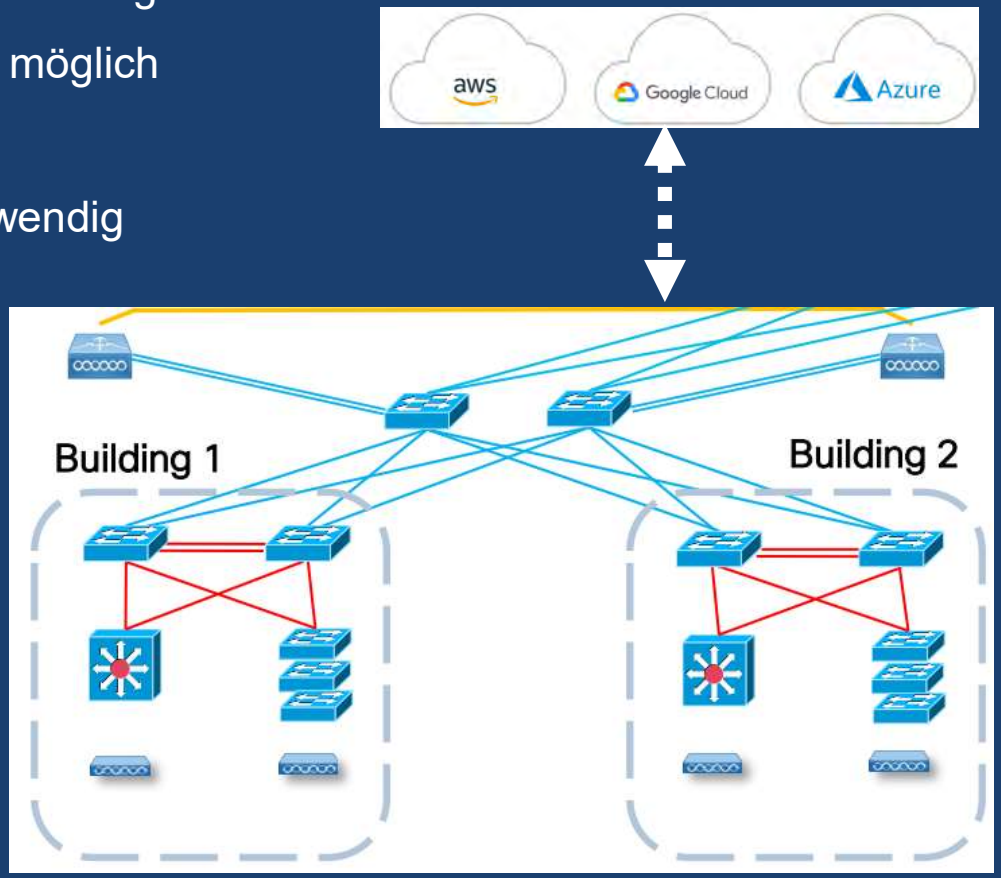
SWS COMPUTERSYSTEME
Member of ACP Group

Agenda

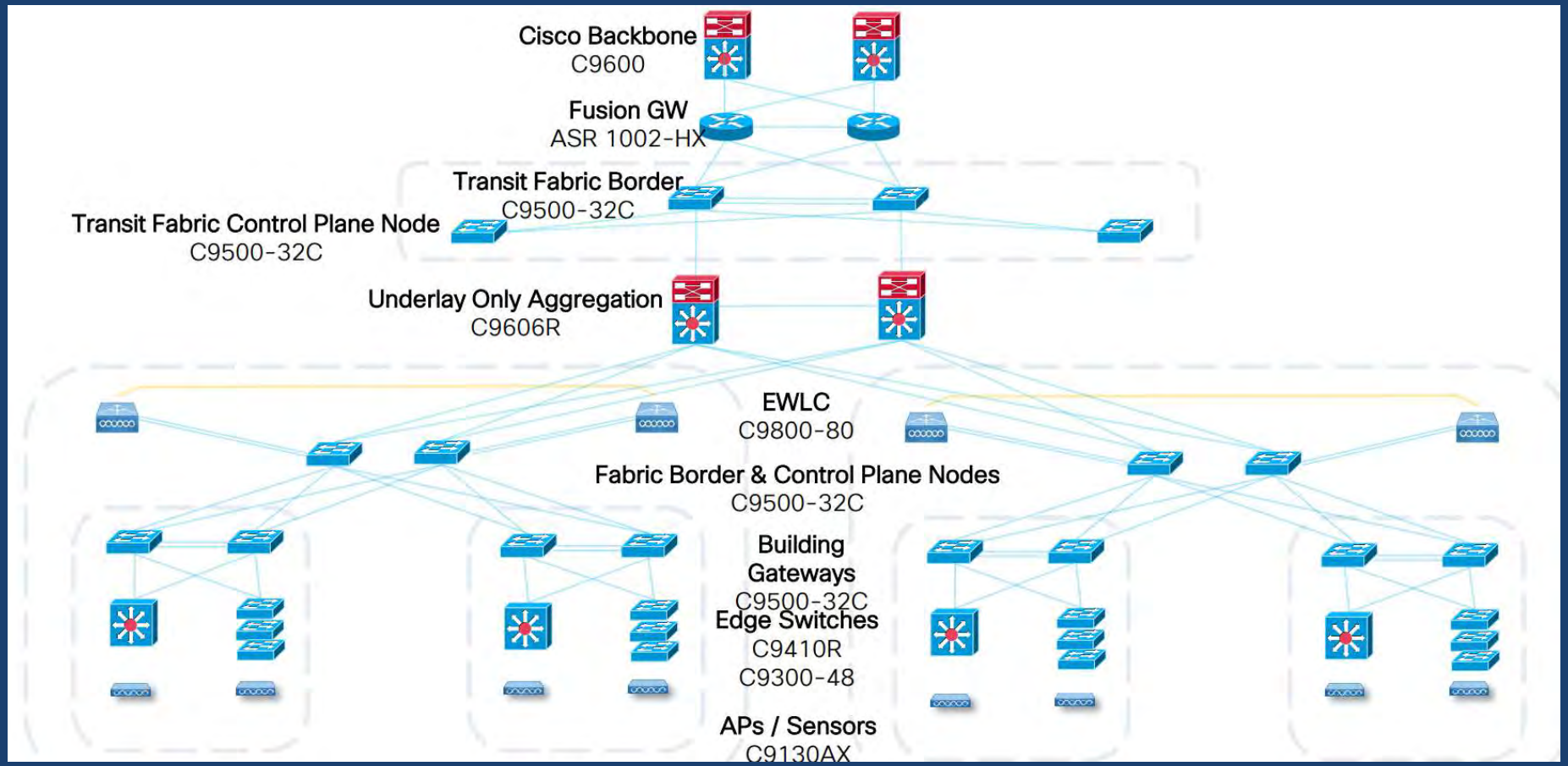
- Traditionelle Netzwerk Designs und Challenges
- Cisco Secure Analytics
- Cisco Secure Network Analytics - Demo
- Cisco Secure Firewall
- Cisco Secure Firewall - Demo
- Q&A

Traditionelle Netzwerk Designs und Challenges

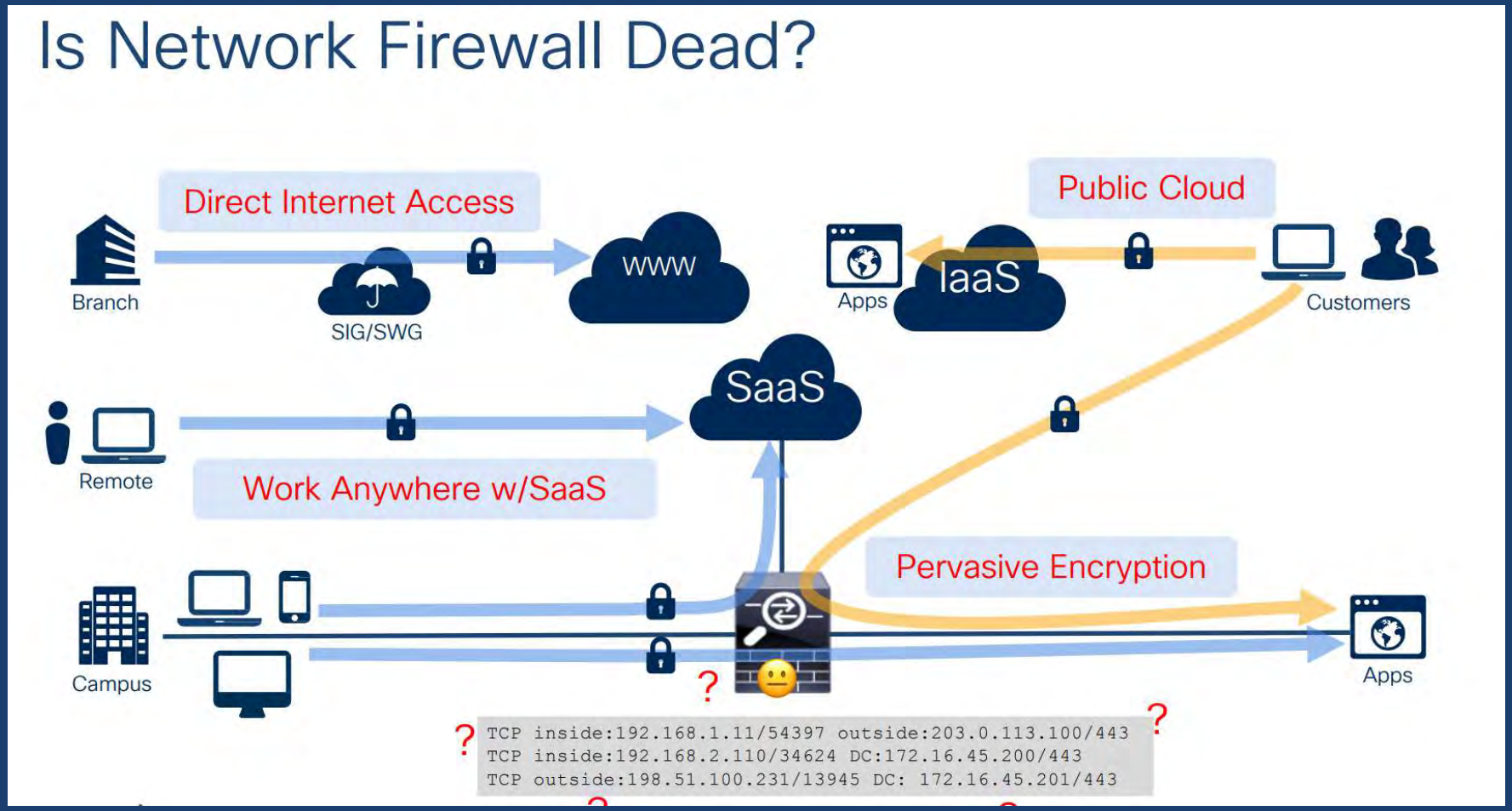
- Kommunikation im Netzwerk sind quasi nicht nachverfolgbar
- Policy Enforcement teils nur mit Endpoint Agents möglich
- Cloud Provider Visibility
- Komplexe Integrationen oder Capture Points notwendig



Traditionelle Netzwerk Designs und Challenges



Traditionelle Netzwerk Designs und Challenges



Die Antwort?

- Cisco Secure Analytics
- Cisco Secure Firewall

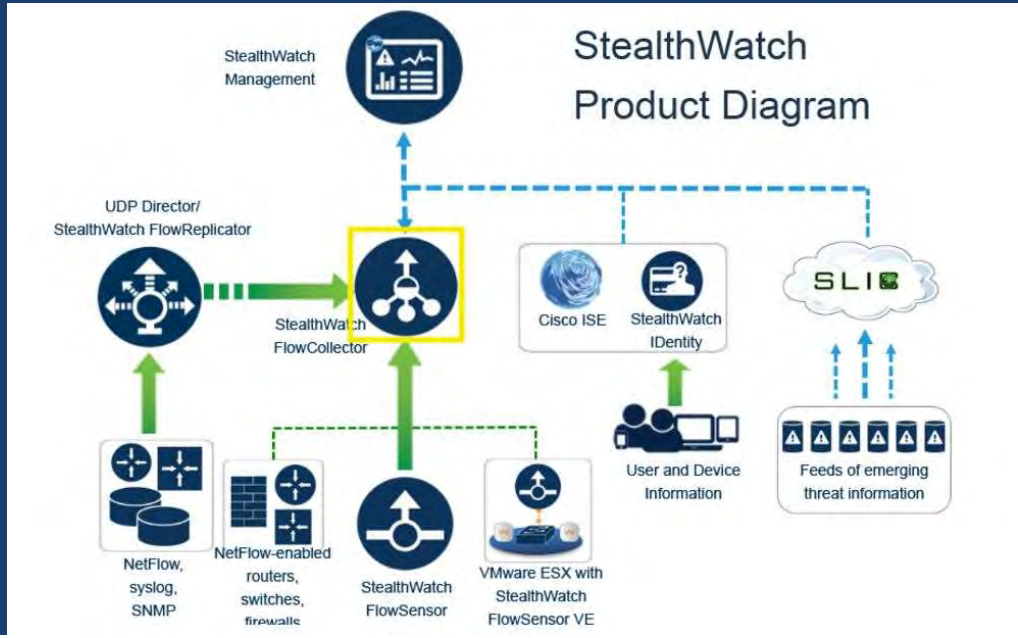
SWS COMPUTERSYSTEME
Member of ACP Group

Agenda

- Traditionelle Netzwerk Designs und Challenges
- Cisco Secure Analytics
- Cisco Secure Network Analytics - Demo
- Cisco Secure Firewall
- Cisco Secure Firewall - Demo
- Q&A

Netflow v9 / IPFIX (Netflow v10)

- Netflows werden von Flow Exporters (Switch, Router,..) erstellt und zu Flow Collectors gesendet
  - Ein Netflow wird für jede Verbindung erstellt und enthält verschiedene Informationen, abhängig vom Exporter
- Flow Collectors „stitchen“ Netflows zusammen und stellen Daten einem Flow Analyzer zur Verfügung
  - Somit können Anomalien, Maliziöse Zugriffe, usw. Erkennt werden
  - Machine Learning und Policies bilden das Fundament

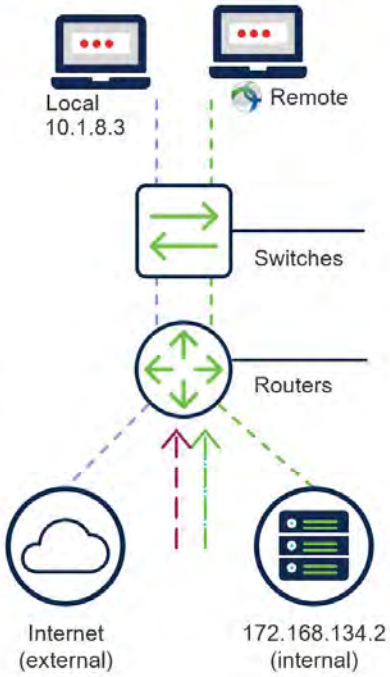


Cisco Secure Analytics - Überblick

The network as the source of truth

See it ALL!

- A Trace of every conversation
- Agentless information collection
- Remote worker endpoint data collection
- Cloud Telemetry ingest
- East west and north south visibility
- Light meta data collection using the existing infrastructure
- Capture enhanced NetFlow for encrypted traffic analysis from Cisco ASR, ISR and Catalyst 9000 platforms



Flow information	Packets
Source address	10.1.8.3
Destination address	172.168.134.2
Source port	47321
Destination port	443
Interface	Gi0/0/1
IP TOS	0x00
IP protocol	6
Next hop	172.168.25.1
TCP flags	0x1A
Source SGT	100
:	:
ETA meta data	IDP | SPLT
Application name	NBAR SECURE-HTTP
Process Name	chrome.exe
Process Account User	Acme/john

Cisco Secure Analytics - Überblick

End-to-end visibility infrastructure

NetFlow Export is available across the Cisco portfolio

Switch
Catalyst 2960-X (v9/IPFIX)
Catalyst 3650/3850 (v9/IPFIX)
Catalyst 4500E (v9/IPFIX)
Catalyst 6500E (v9/IPFIX)
Catalyst 6800 (v9/IPFIX)
Catalyst 9200 (v9/IPFIX)
Catalyst 9300/9400 (v9/IPFIX ETA)
Catalyst 9500 (v9/IPFIX)
Catalyst 9600 (v9/IPFIX)
IE3000 (v9/IPFIX)
IE4000 (v9/IPFIX)
IE5000 (v9/IPFIX)

Router
Cisco ISR 4000 (v9/IPFIX ETA)
Cisco CSR 1000v (v9/IPFIX ETA)
Cisco ASR 1000 (v9/IPFIX ETA)
Cisco ASR 9000 (v9/IPFIX)
Cisco WLC 5520, 8510, 8540 (v9 Enhanced)
Catalyst 9800 (v9/IPFIX ETA)

Firewall
ASA 5500-X (NSEL)
FTD (NSEL,Syslog)
Meraki MX/Z1 (v9 Enhanced v14.5)

Data center switch
Nexus 1000v (v9/IPFIX)
Nexus 3000 (sFlow)
Nexus 7000 (M Series modules – (v9/IPFIX)
Nexus 7000 (F Series modules – (v9/IPFIX sampled)
Nexus 9000 Series (sFlow)
Nexus 9000 Series EX/FX (v9)

Servers, software
SNA Flow Sensor (v9/IPFIX ETA)
Cisco UCS VIC (v9/IPFIX)

Cloud
AWS
(VPC Flow Logs via CTB)

Endpoint
AnyConnect (IPFIX)

Cisco Secure Analytics - Überblick

Secure Cloud Analytics
(Stealthwatch Cloud)

Suitable for monitoring public cloud as well as private networks. Simple deployment and automated tuning.

SaaS based with a lightweight sensor for telemetry collection.

Usage-based pricing determined by volume of log data or endpoint count.

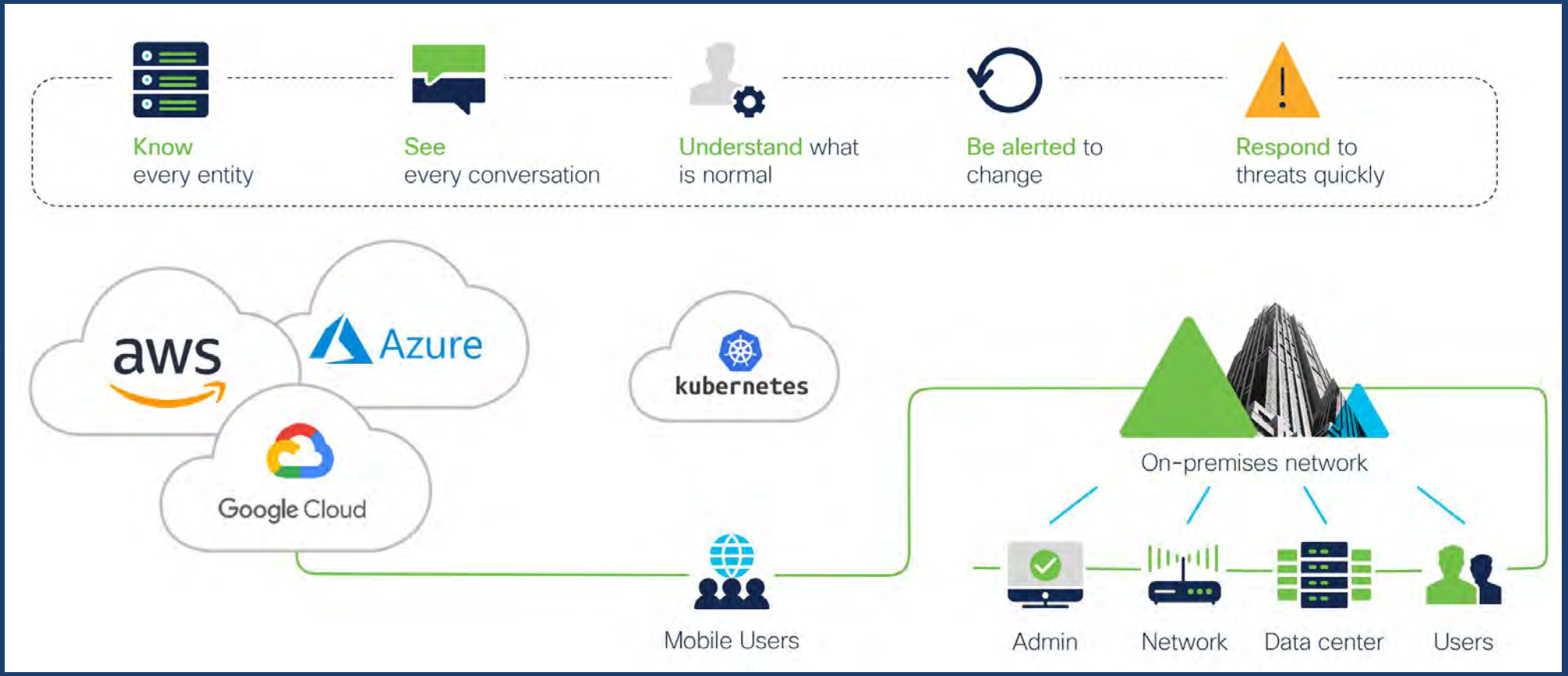
Secure Network Analytics
(Stealthwatch Enterprise)

On-premises data storage, granular tuning, SecOps and NetOps use cases, air-gapped networks

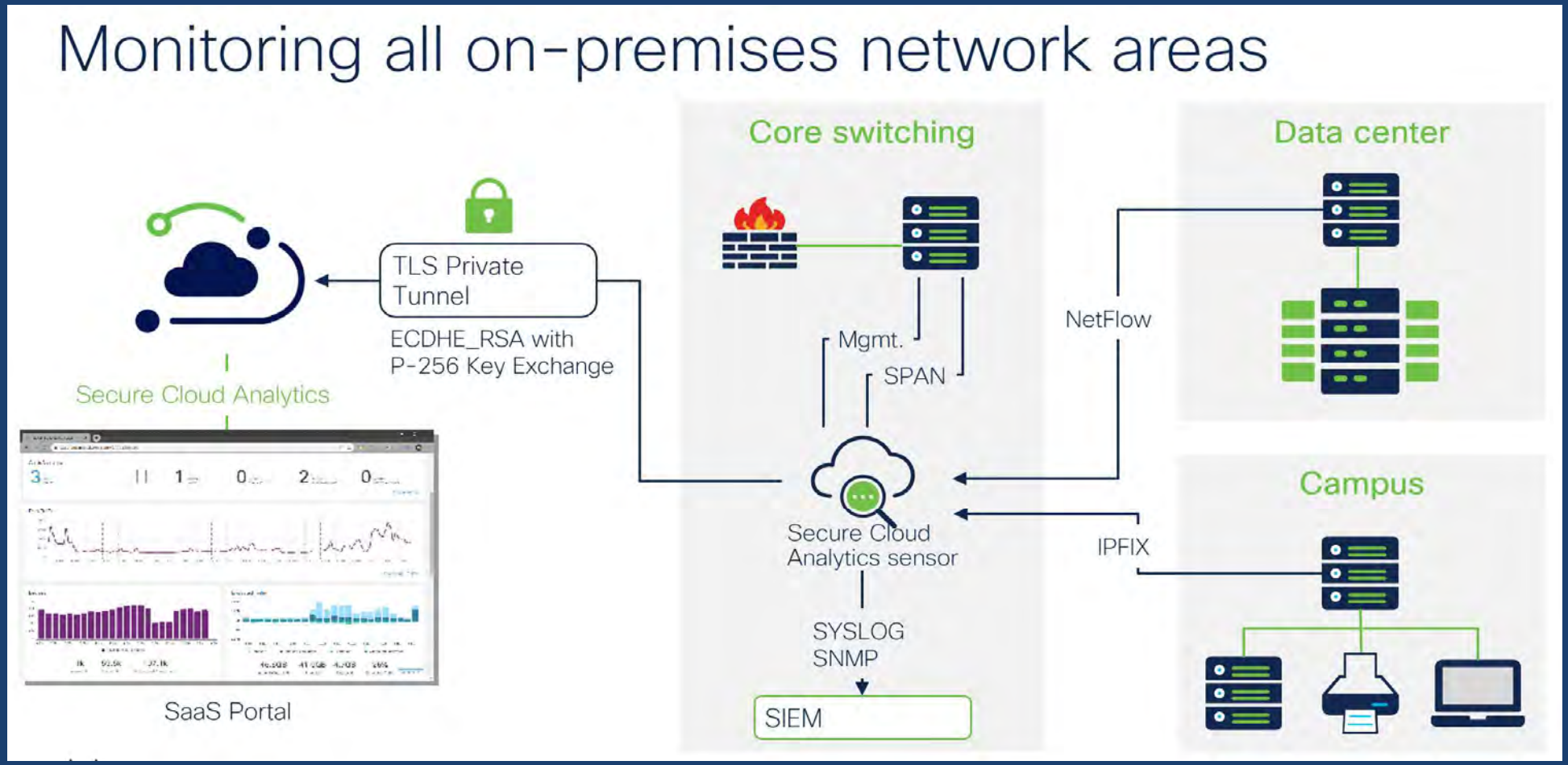
Hardware or virtual appliance

Priced by FPS (flows per second)

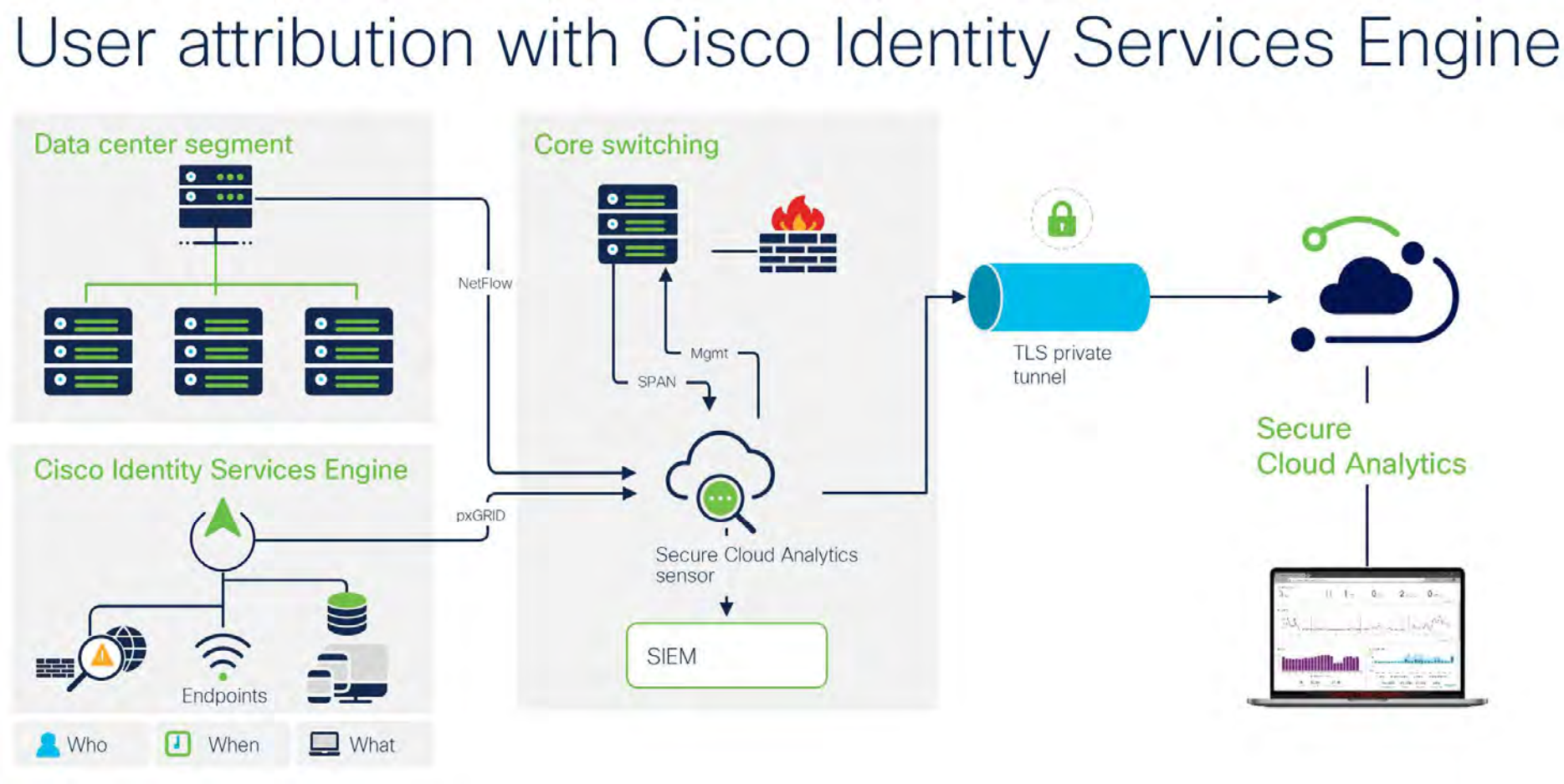
Cisco Secure Cloud Analytics - Einsatzgebiete



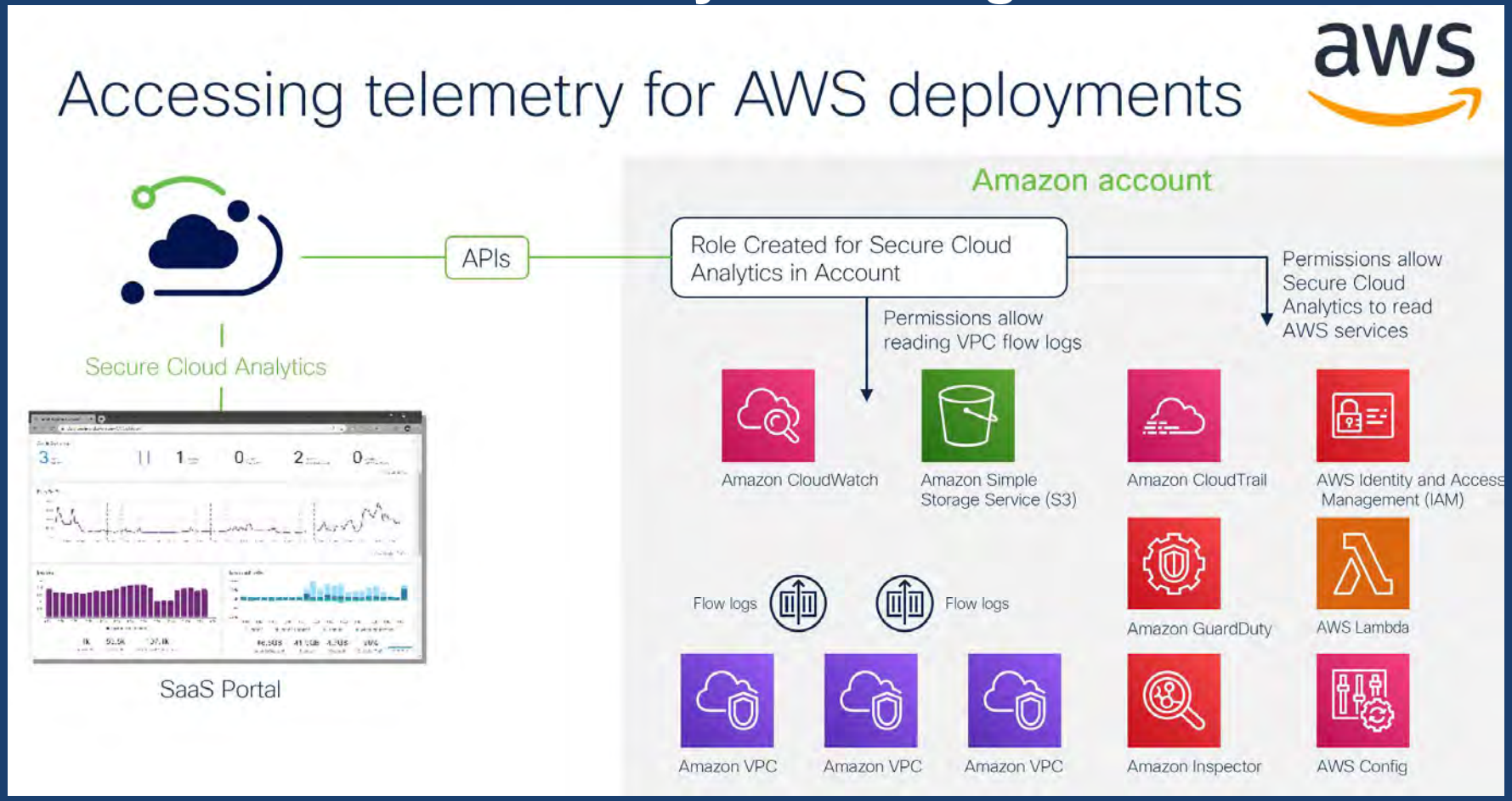
Cisco Secure Cloud Analytics - Einsatzgebiete



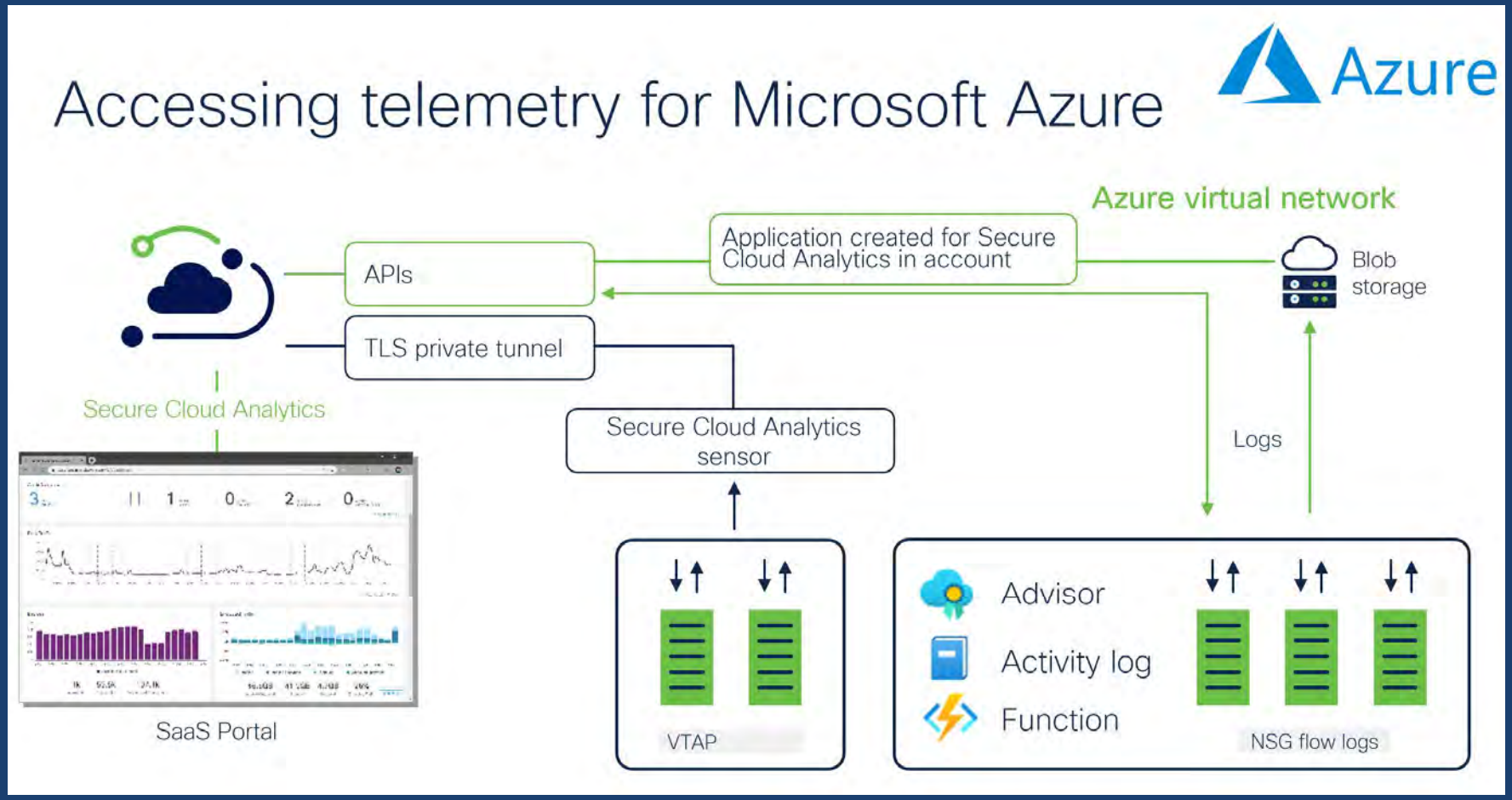
Cisco Secure Cloud Analytics - Integrationen



Cisco Secure Cloud Analytics - Integrationen



Cisco Secure Cloud Analytics - Integrationen



Cisco Secure Analytics - Überblick

Secure Cloud Analytics
(Stealthwatch Cloud)

Suitable for monitoring public cloud as well as private networks. Simple deployment and automated tuning.

SaaS based with a lightweight sensor for telemetry collection.

Usage-based pricing determined by volume of log data or endpoint count.

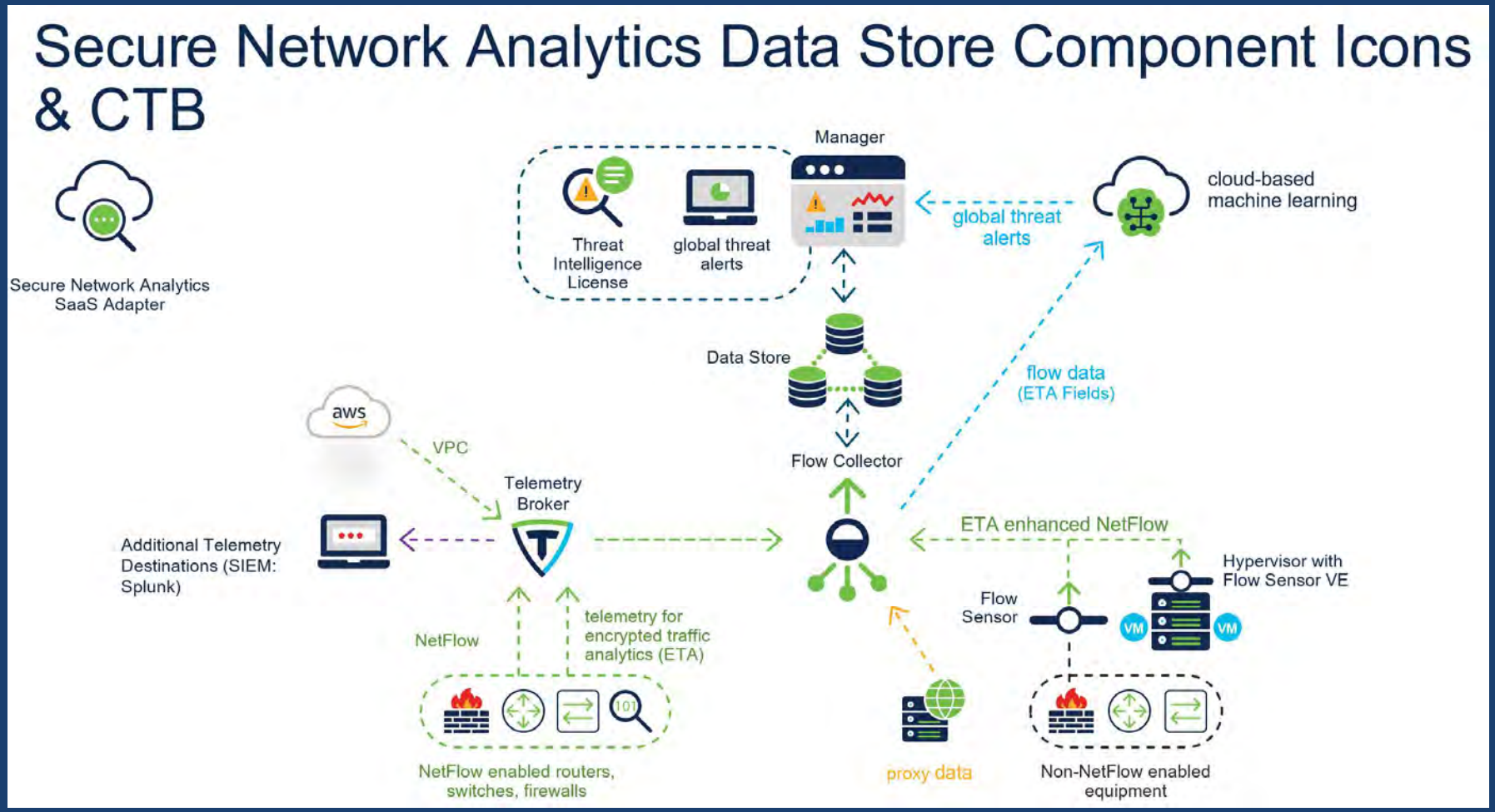
Secure Network Analytics
(Stealthwatch Enterprise)

On-premises data storage, granular tuning, SecOps and NetOps use cases, air-gapped networks

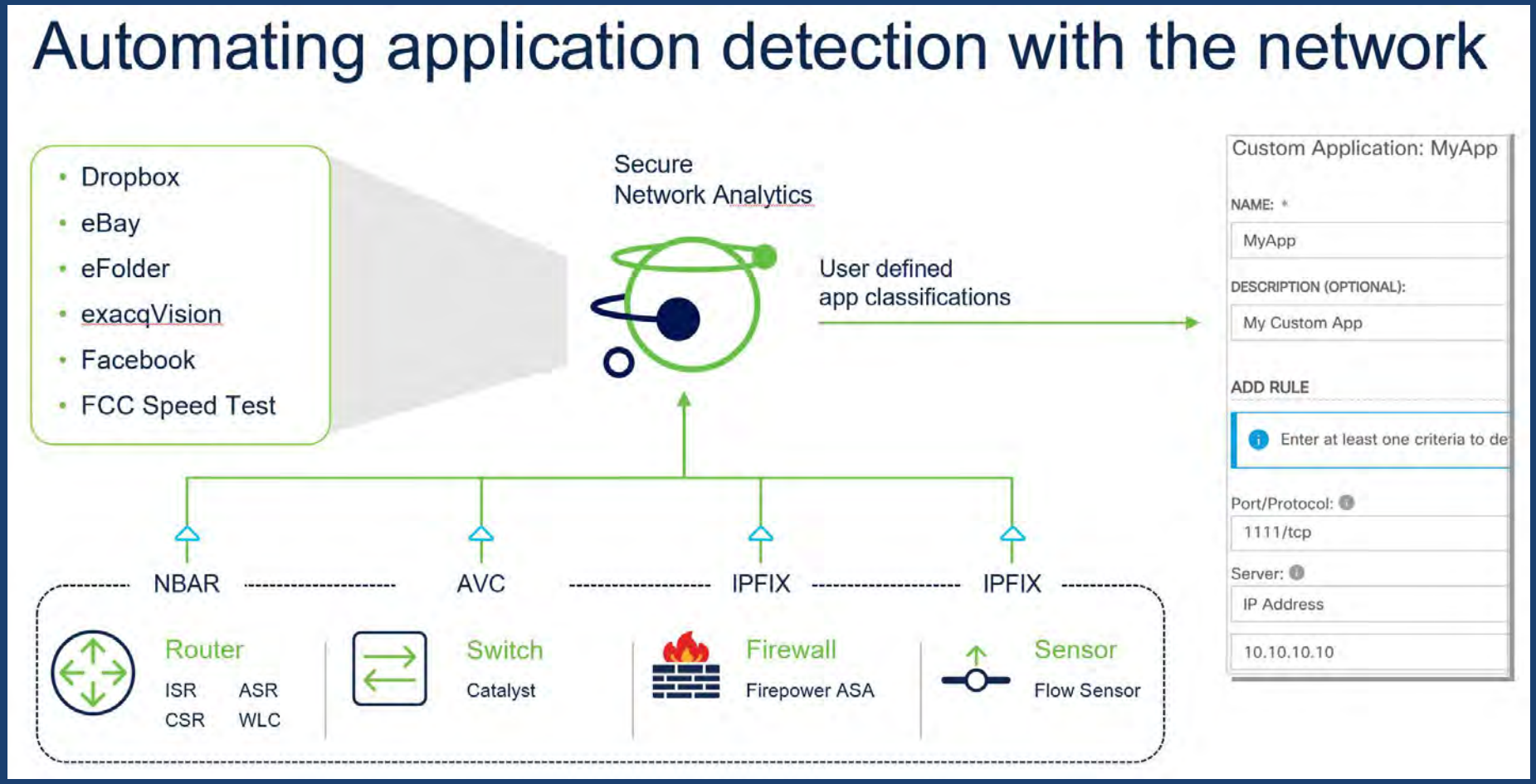
Hardware or virtual appliance

Priced by FPS (flows per second)

Cisco Secure Network Analytics - Überblick



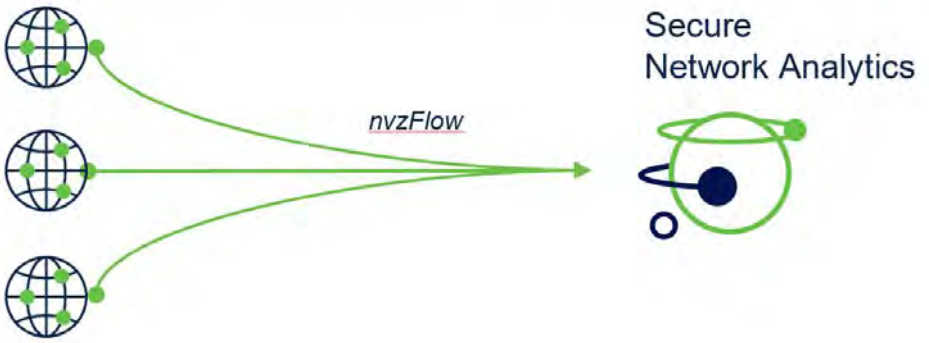
Cisco Secure Network Analytics - Module



Cisco Secure Network Analytics - Module

Visibility extended to client endpoint processes

VPN with Network Visibility Module



- Extend Visibility to the Endpoint
- Know the Process that Generated the Flow

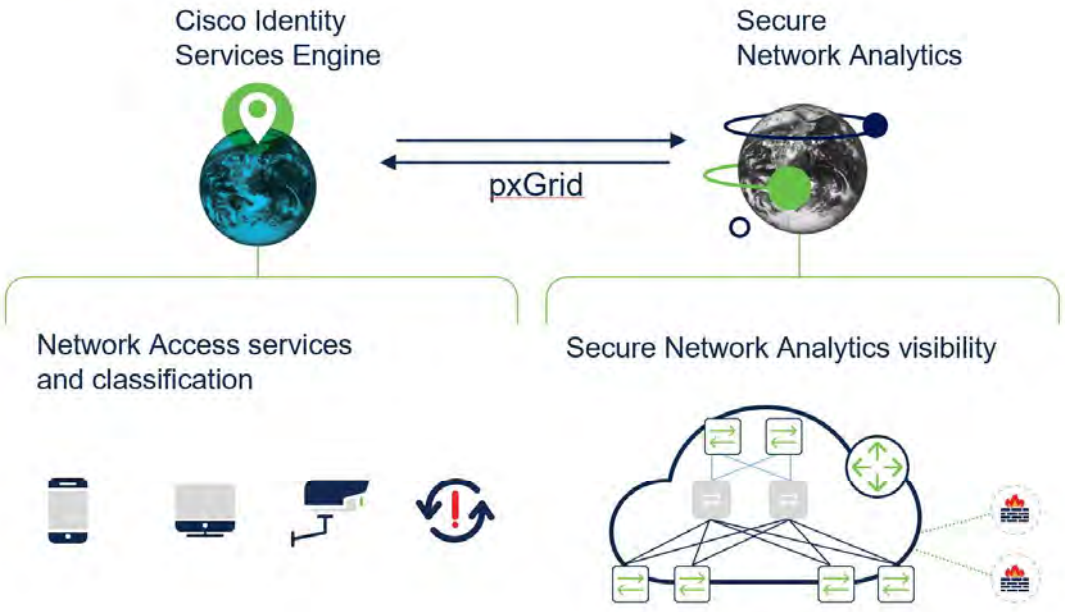
Attributing a flow to:

- Process name
- Process hash
- Process account
- Parent process name
- Parent process hash
- Parent process account

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT PR...	SUBJECT FILE...	SUBJECT PAR...	SUBJECT PAR...	APPLICATION	PEER IP ADDR...
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UD	Ex. "catch All"	Ex. chrome.ex	Ex. c8c0fc569	Ex. chrome.ex	Ex. c8c0fc569	Ex. "Corporate	Ex. 10.255.25
Mar 25, 2021 11:51:23 AM (38min ago)	37min 23s	10.100.10.100	55757/TCP	Remote VPN IP Pool , Main Campus VPN	tor.real	830CA7B335662FD4C30F4D3E8E07B08C4AE6CF41F8008BFD9E77067B72595619	firefox	19CF386F6E2A6217A6C92AB54137E1C57F3274EB4A2746796158ED23C028B5FE	Undefined TCP	85.17.88.177

Cisco Secure Network Analytics - Integrationen

Secure Network Analytics and network access integration



Secure Network Analytics integrates with ISE to get mitigation capabilities and apply different ANC policies to an endpoint

Device Id	Trustsec name
Domain Id	Last update time
Active	InterfaceDevicePortId
Start active time	InterfaceDeviceIp
Endpoint IP	Vlan
Username	MAC address
SGT Tag	Session ID

Info from ISE

Secure Network Analytics also integrates with ISE-PIC
using pxGrid to get endpoint contextual information

Active	Username
Start active time	Last update time

Info from ISE – PIC

Cisco Secure Network Analytics - Integrationen

Proxy integration

Web proxy

Secure Network Analytics

SYSLOG information	Packets
Timestamp	1456312345
Elapse time	12523
Source IP	192.168.2.100
Source port	4567
Destination IP	65.12.56.123
Destination port	80
Bytes	400
URL	http://cisco.com
Username	john

Web URL visibility

- Cisco WSA
- Bluecoat proxy
- Squid
- McAfee web gateway

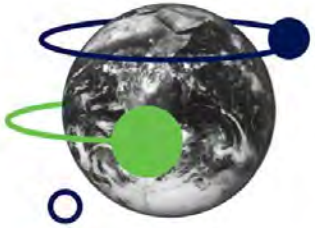
Cisco Secure Network Analytics - Integrationen

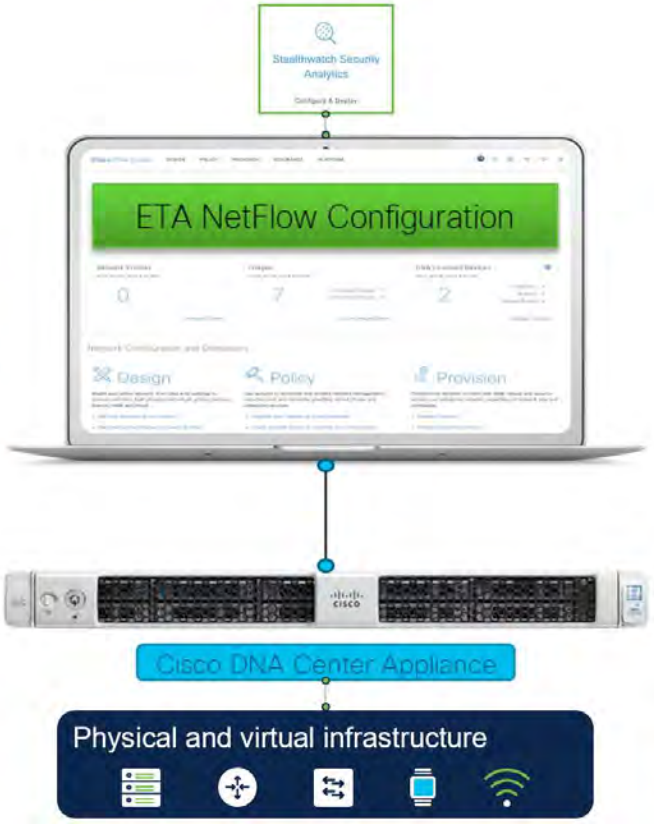
Security analytics integration with Cisco DNA Center

Secure Network Analytics app

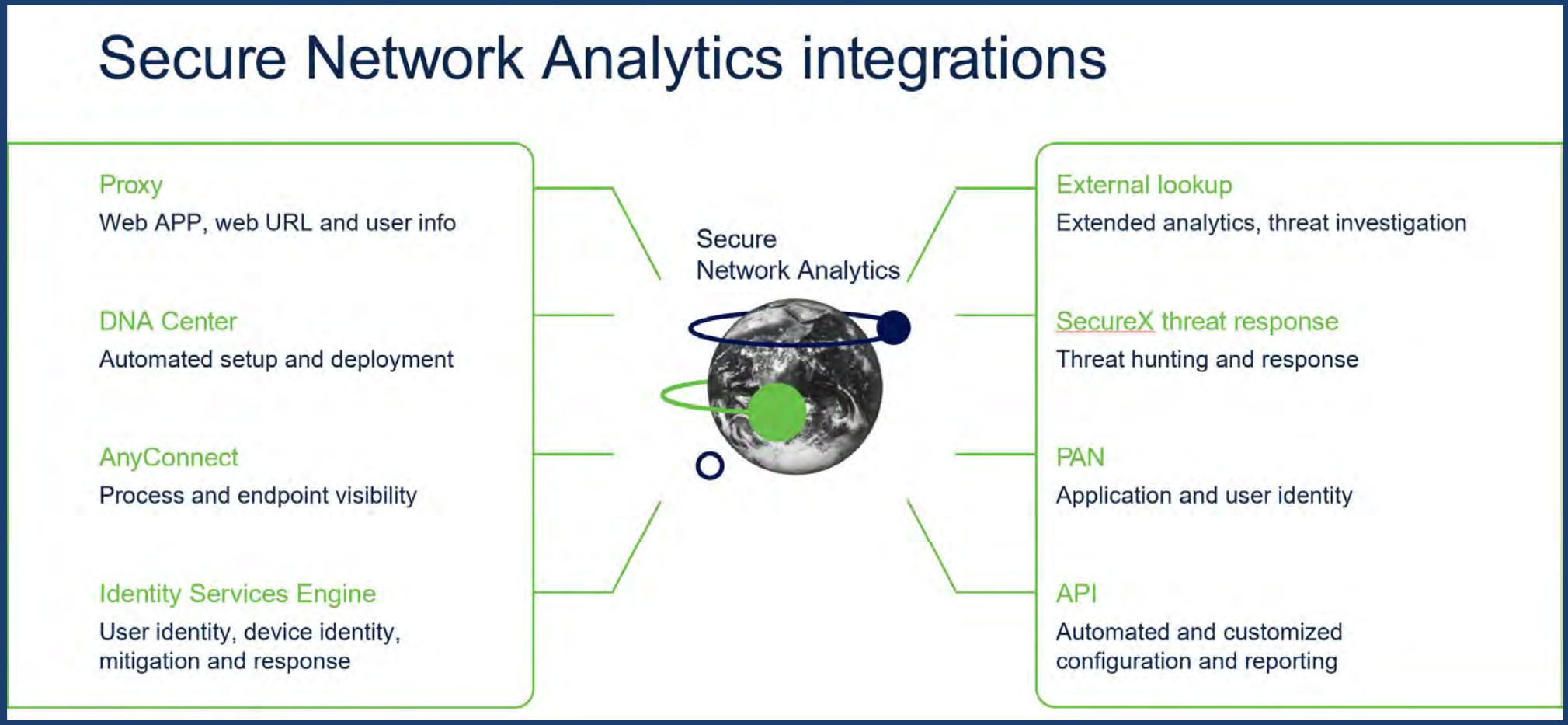
Deploy ETA in minutes!

- Guided workflow makes it easier for networking teams to enable Secure Network Analytics within the enterprise
- Site based provisioning
  - Traditional wired networks
  - SD-access fabrics
- Automated readiness check
- Visibility of deployment status
- Security endpoint assurance





Cisco Secure Network Analytics - Integrationen



SWS COMPUTERSYSTEME
Member of ACP Group

Agenda

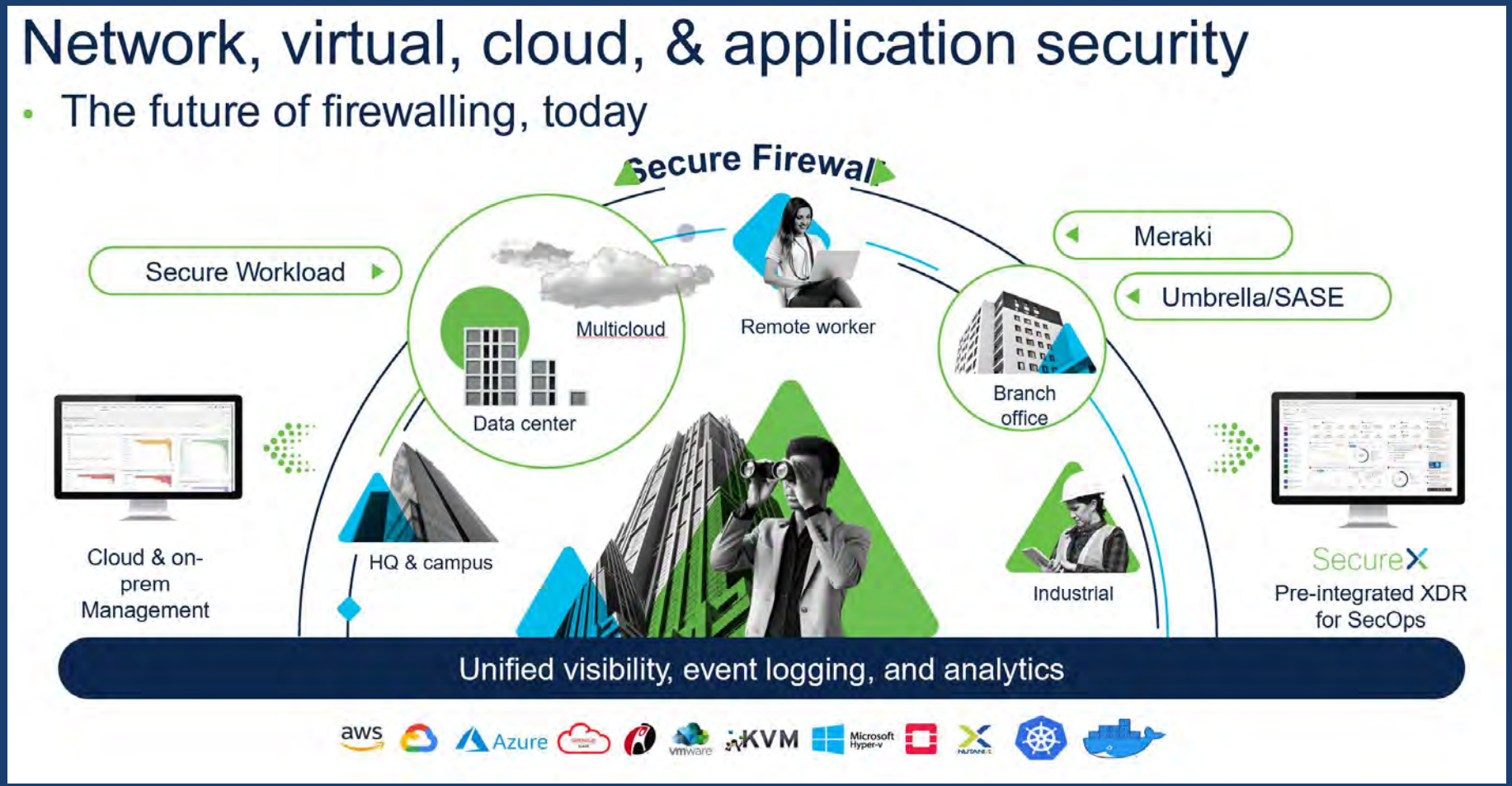
- Traditionelle Netzwerk Designs und Challenges
- Cisco Secure Analytics
- Cisco Secure Network Analytics - Demo
- Cisco Secure Firewall
- Cisco Secure Firewall - Demo
- Q&A

SWS COMPUTERSYSTEME
Member of ACP Group

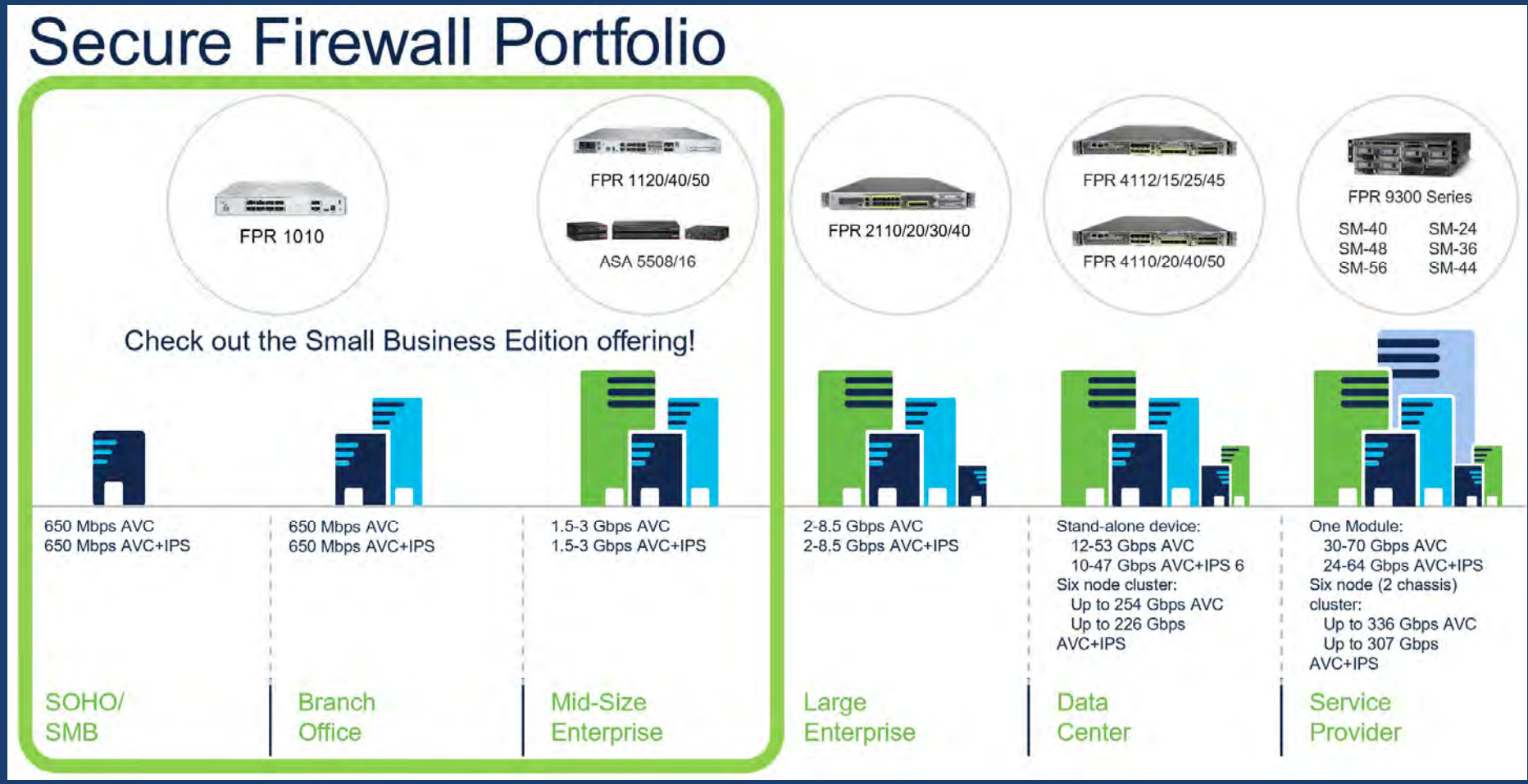
Agenda

- Traditionelle Netzwerk Designs und Challenges
- Cisco Secure Analytics
- Cisco Secure Network Analytics - Demo
- Cisco Secure Firewall
- Cisco Secure Firewall - Demo
- Q&A

Cisco Secure Firewall - Überblick



Cisco Secure Firewall - Überblick



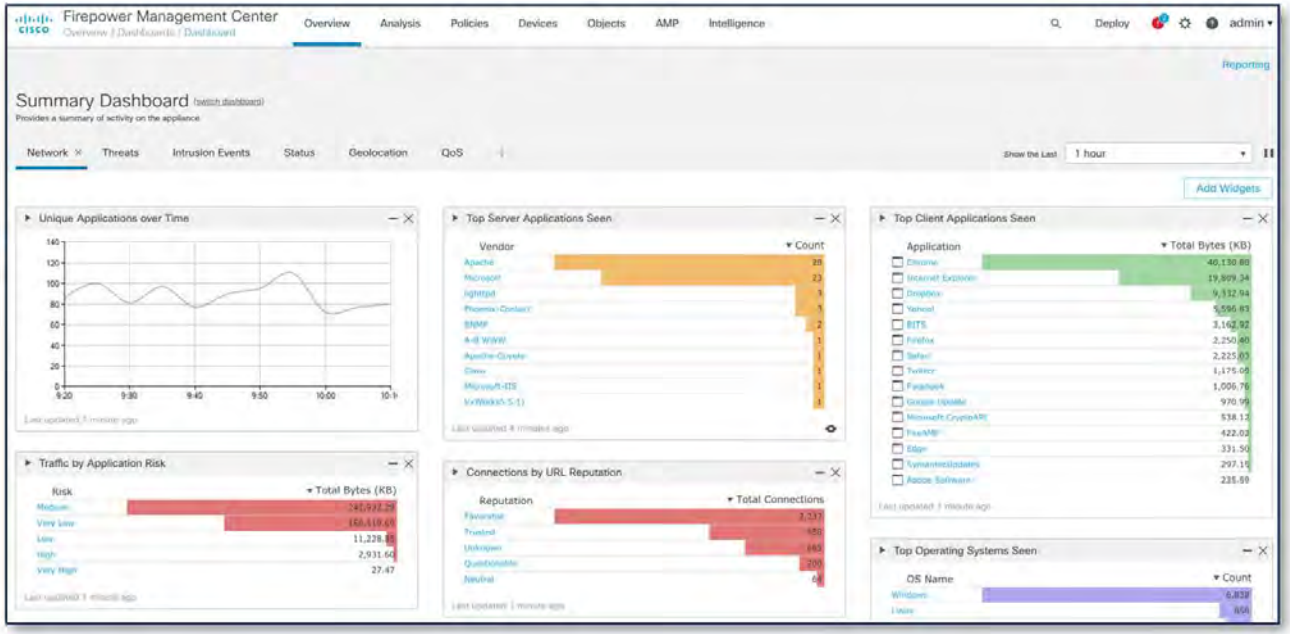
SWS COMPUTERSYSTEME
Member of ACP Group

Cisco Secure Firewall - Verwaltung

What is Firewall Management Center (FMC)?

On-premise, centralized management for multi-site deployments

- Key Benefits
  - Manage across many sites
  - Control access and set policies
  - Investigate incidents
  - Prioritize response
  - Available in physical and virtual options
- Features
  - Multi-domain management
  - Role-based access control
  - High availability
  - APIs and pxGrid integration
  - Policy & device management
  - Endpoint
  - Security intelligence



Cisco Secure Firewall - Verwaltung

Cisco Defense Orchestrator Overview

Consistently manage policies across your cisco security products.

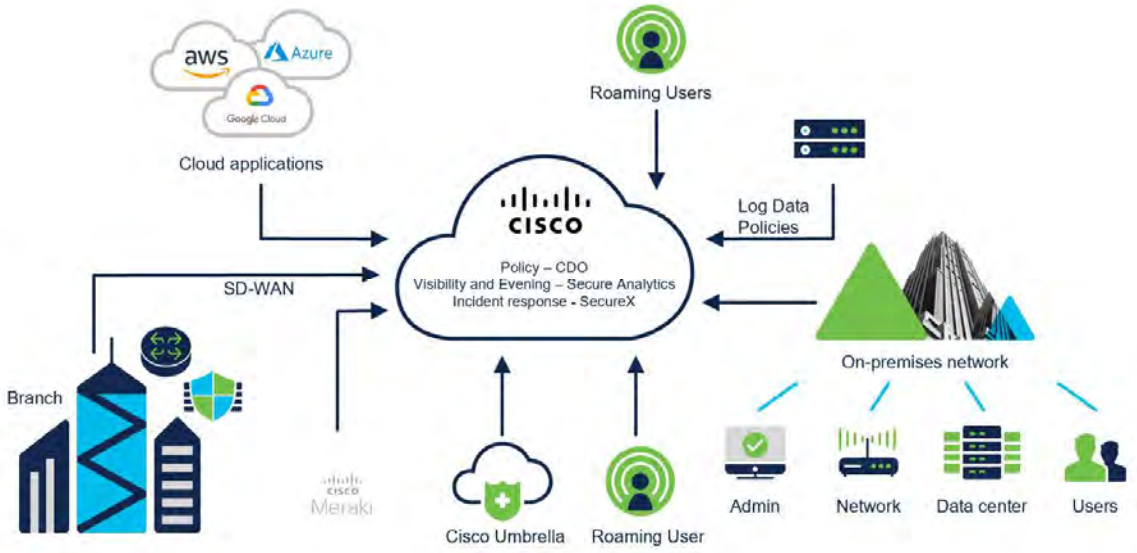
CDO is a Cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

Key Benefits

- Streamline security management
- Reduce time spent on security management tasks up to 90%
- Achieve better security while reducing complexity
- Prioritize response

Features

- Consistent policy enforcement
- Faster device deployments
- Configuration management

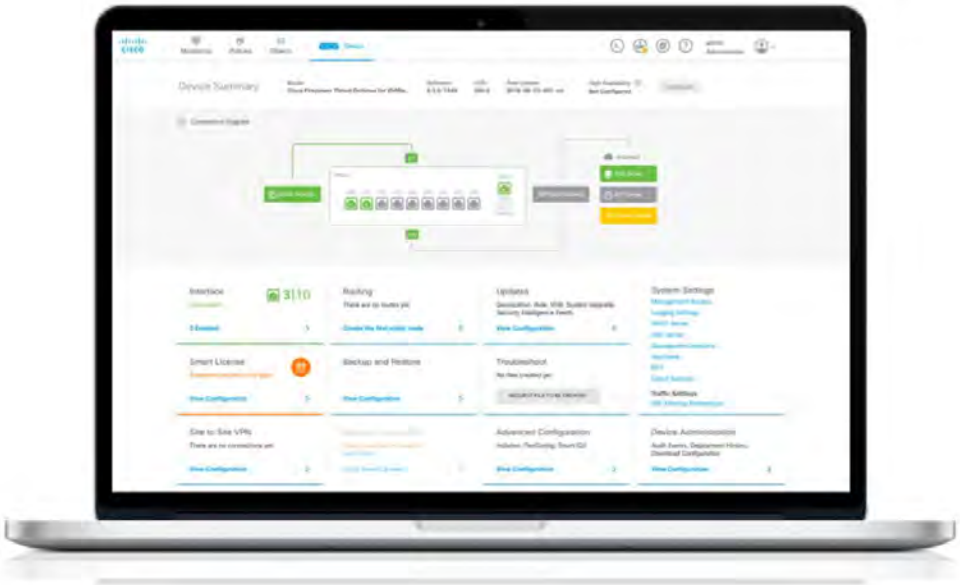


Cisco Secure Firewall - Verwaltung

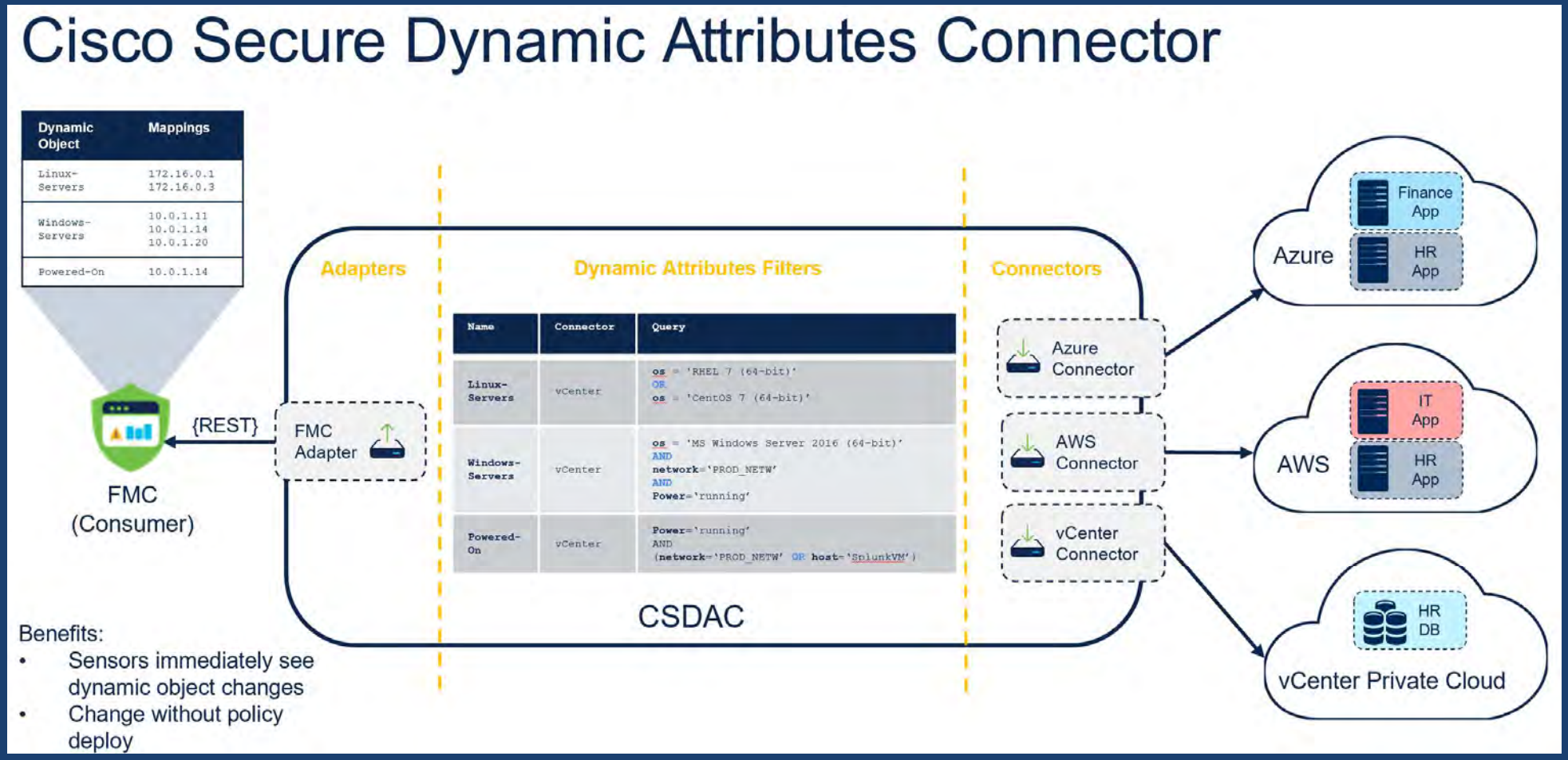
What is Secure Firewall Device Manager (FDM)

On-box manager and API platform

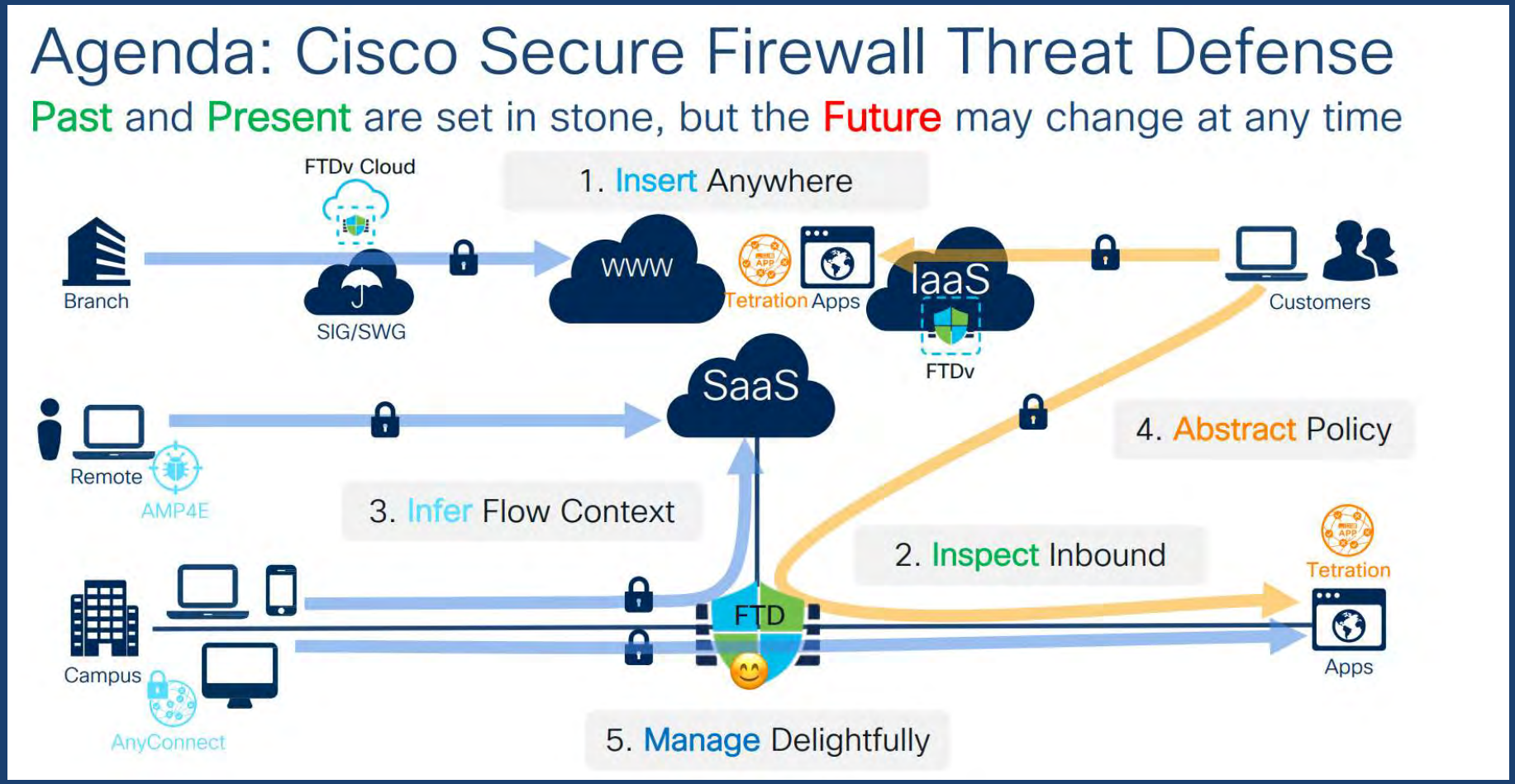
- Key Benefits
  - Easy set up
  - Control access and set policies
  - Automate configuration
  - Enhanced control
- Features
  - Role-based access control
  - High availability
  - NAT and routing
  - Intrusion and malware protection
  - Device monitoring
  - VPN support



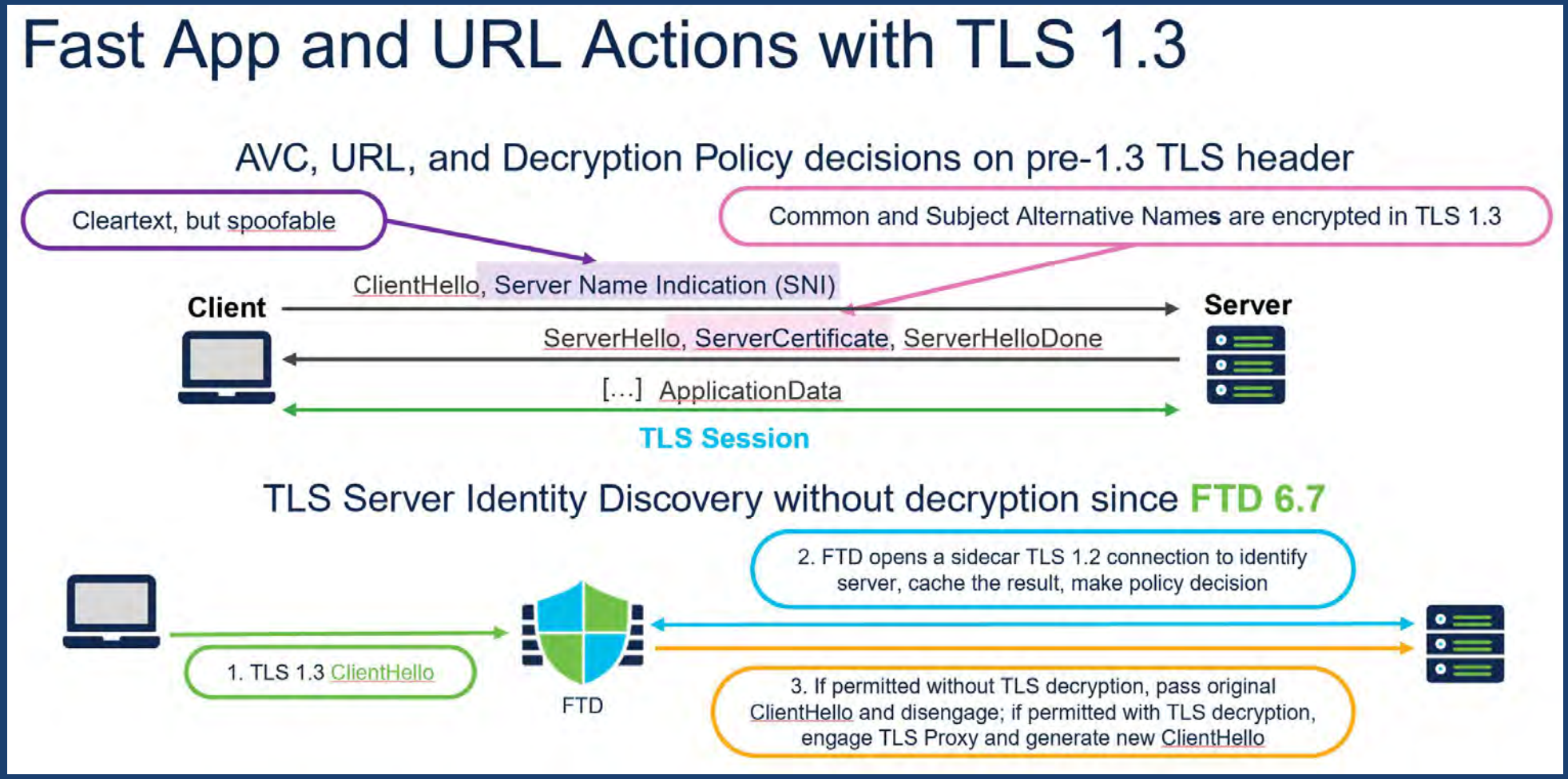
Cisco Secure Firewall – Verwaltung Add-ONs



Cisco Secure Firewall - Features



Cisco Secure Firewall - Features



SWS COMPUTERSYSTEME Member of ACP Group

Cisco Secure Firewall - Features

Encrypted Visibility Engine

- Experimental feature in release 7.1
- Utilizes machine learning to determine the application (client process) generating the Client Hello packet
- Identifies known processes/browsers
- Identifies malware based on Secure Malware Analytics fingerprints

SWS COMPUTERSYSTEME
Member of ACP Group

Cisco Secure Firewall - Features

2022-02-22 22:33:21	Connection	Allow	10.0.50.1	51.124.78.146	3070 / tcp	443 (https) / tcp	Microsoft

Event Type:	Connection	**SSL Flow Messages:**	SERVER_HELLO_DONE, SERVER_CERTIFI...	**Ingress Interface:**	client-inside
Time:	2022-02-22 22:33:21	**Application Protocol:**	HTTPS	**Egress Interface:**	transfer-outside
Last Packet:	2022-02-22 22:33:21	**Application Protocol Category:**	network protocols/services	**Ingress Virtual Router:**	Global
Action:	Allow	**Application Protocol Tag:**	file sharing/transfer, SSL protocol, opens p...	**Egress Virtual Router:**	Global
Source IP:	10.0.50.1	**Client Application:**	SSL client	**Initiator Packets:**	15
Source User:	lukas.schwarzfischer (ad-smr-service.lan\...	**Client Application Category:**	web browser	**Responder Packets:**	15
Destination IP:	51.124.78.146	**Client Application Tag:**	SSL protocol, evasive	**QoS-Dropped Initiator Packets:**	0
Destination Continent:	Europe	**Web Application:**	Microsoft	**QoS-Dropped Responder Packets:**	0
Destination Country:	NLD	**Web Application Category:**	web services provider, business	**Initiator Bytes:**	1,564
Ingress Security Zone:	client-inside	**Web Application Tag:**	office 365, NSG, SSL protocol	**Responder Bytes:**	3,974
Egress Security Zone:	transfer-lan	**Application Risk:**	Medium	**QoS-Dropped Initiator Bytes:**	0
Source Port / ICMP Type:	3070 / tcp	**Business Relevance:**	Low	**QoS-Dropped Responder Bytes:**	0
Destination Port / ICMP Code:	443 (https) / tcp	**URL:**	https://settings-win.data.microsoft.com	**TLS Fingerprint Process Name:**	microsoft office
SSL Status:	Do Not Decrypt	**Intrusion Events:**	0	**TLS Fingerprint Process Confidence Score:**	82%
SSL Flow Error:	Success	**Files:**	0	**TLS Fingerprint Malware Confidence:**	Very Low
SSL Actual Action:	Do Not Decrypt	**Access Control Policy:**	Default	**TLS Fingerprint Malware Confidence Score:**	0%
SSL Expected Action:	Do Not Decrypt	**Access Control Rule:**	to internet - filtered	**Detection Type:**	AppID
SSL Certificate Status:	Invalid Issuer	**Network Analysis Policy:**	Basic-NAP	**NAT Source IP:**	10.0.0.240
SSL Version:	TLSv1.2	**Prefilter Policy:**	Default Prefilter Policy	**NAT Destination IP:**	51.124.78.146
SSL Cipher Suite:	TLS_ECDHE_RSA_WITH_AES_128_GCM...	**Source SGT:**	sgt_domain_user		
SSL Policy:	default-ssl	**Endpoint Profile:**	Workstation:Microsoft-Workstation:Windo...		

SWS COMPUTERSYSTEME Member of ACP Group

Cisco Secure Firewall - Integrationen

Gain an Integrated Security Portfolio

Need: As IT infrastructure continues to become more diverse, the job of securing it becomes more dynamic. The perimeter becomes flexible, which requires a broader portfolio of security solutions.

Cisco offering:

Get more from your existing network

Tightly integrate existing investments, including Cisco Application-Centric Infrastructure (ACI) and Network Access with your Firewall solution.

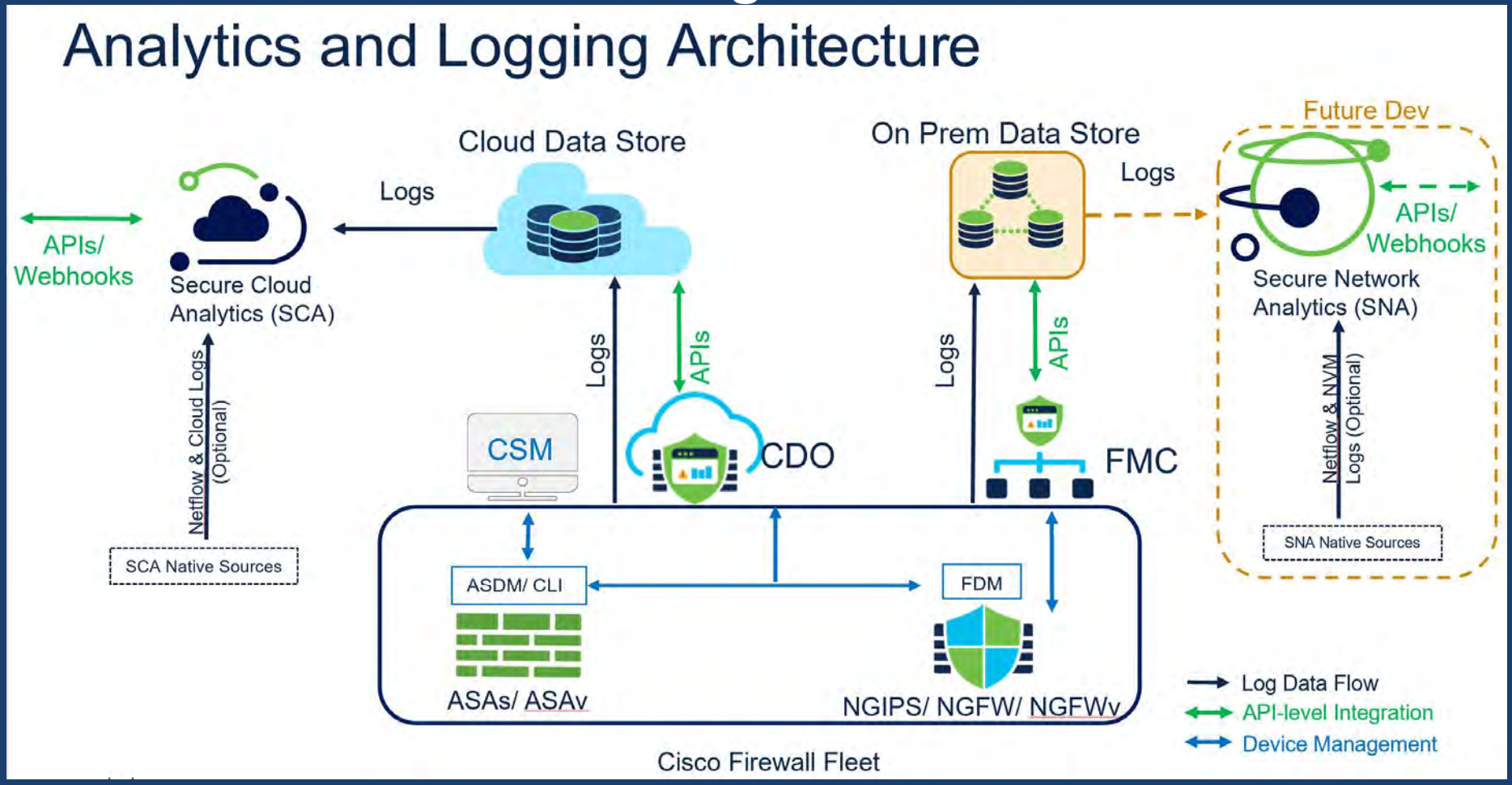
Greater security control points

Enforce polices across your entire environment, including any device administered by the organization.

Extend protection

Remove blind spots, protect users anywhere they go and anywhere they access the internet.

Cisco Secure Firewall - Integrationen



Cisco Secure Firewall - Integrationen

Cisco Rapid Threat Containment

Proven approach to reduce time and impact of threat

- Automatic network threat containment using the network as an enforcer
- Threat-centric network access determines network access based on IoCs
- Richer visibility from bidirectional data sharing with the network access

Cisco Secure Firewall - Integrationen

Protect Your Network Using AMP

Understand the motion and behavior of files through network and endpoint visibility.

Breadth and Control points

Email Endpoints Web Network IPS Devices

Threat Visibility

Retrospective Detection

Behavioral IoCs

File Trajectory

Threat Hunting

Telemetry Stream

File and Network I/O

Process Information

File Fingerprint and Metadata

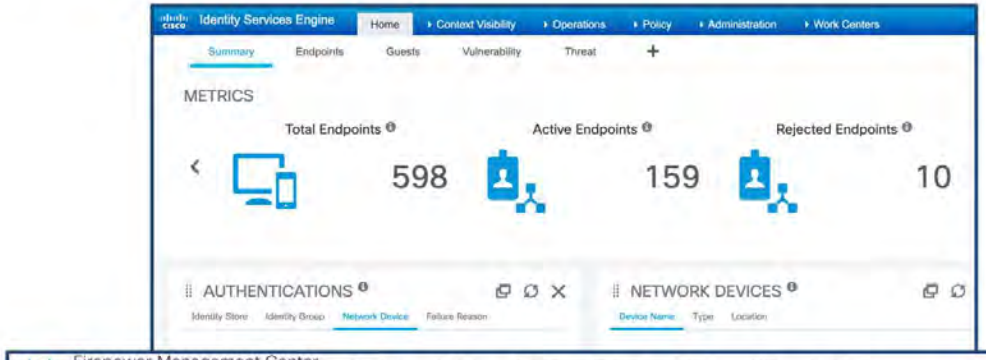
Talos and Malware Analytics Intelligence

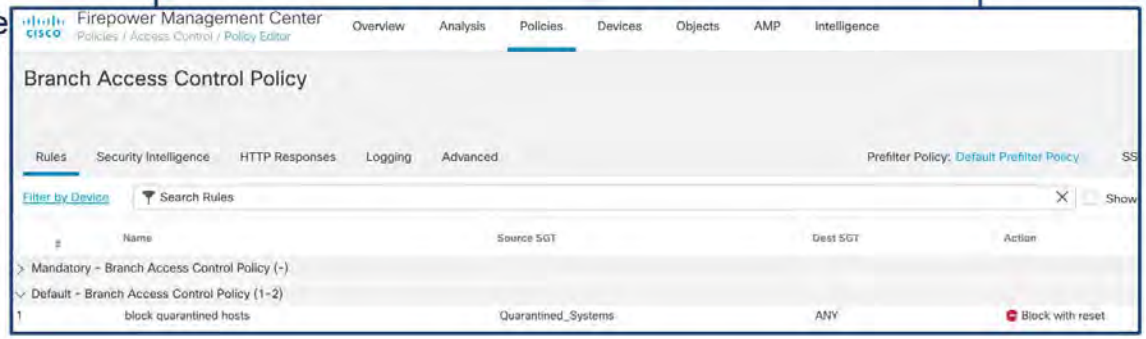
SWS COMPUTERSYSTEME Member of ACP Group

Cisco Secure Firewall - Integrationen

Control Traffic Based on User Awareness

- Use Active Directory users and groups in policy configuration
- Use Cisco Identity Services Engine to provide identity
  - TrustSec Security Group Tag (SGT)
  - Device type (endpoint profiles) and location
  - Identity Mapping Propagation & device level filtering
- Examples
  - Block HR users from using personal iPads
  - Create rules for quarantined iPhones





Cisco Secure Firewall - Integrationen

Simplify Security Management with TrustSec

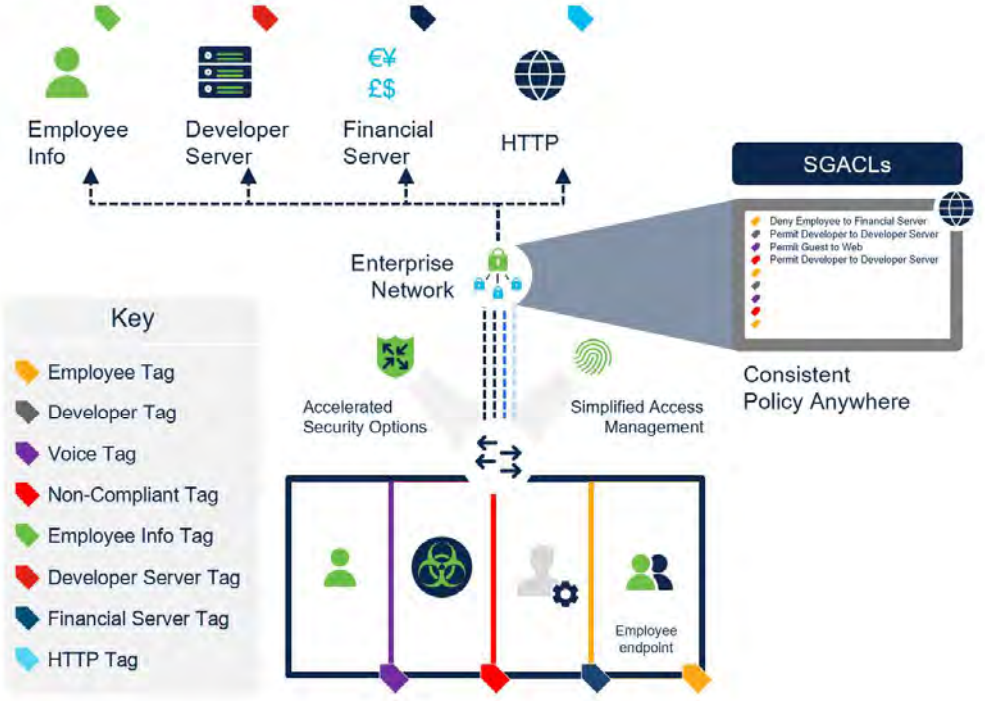
Leverage the network and investment

- Scalable and agile segmentation technology in over 40 different Cisco product families
- Enables dynamic, role-based policy enforcement anywhere on your network
- Extend TrustSec policies over Firepower Threat Defense with SRC & DST SGT matching

Simplified Access Management
Manage policies using plain language and maintain compliance by regulating access based on business role

Rapid Security Administration
Speed-up adds, moves, and changes, simplifying firewall administration to speed up server onboarding

Consistent Policy Anywhere
Control all network segments centrally, regardless of whether devices are wired, wireless or on VPN



Cisco Secure Firewall - SecureX

What is SecureX threat response?

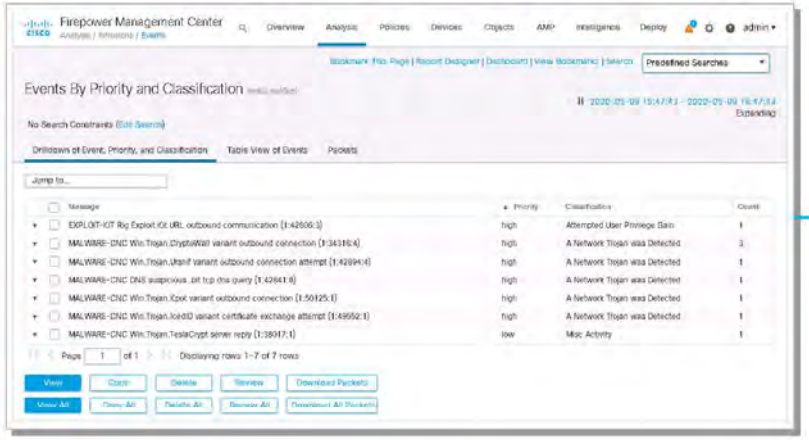
Automates integrations across networks, endpoints, and Cloud environments

- Key Benefits
  - Out of box integrations
  - Speed cyber investigations
  - Included with Cisco security product licenses
  - Reduce burden of other security products
- Features
  - Aggregated threat intelligence
  - Automated enrichment
  - Incident tracking
  - Seamless drill down
  - Direct remediation

Cisco Secure Firewall - SecureX

Leverage a Seamless Workflow

FTD supplies security events to SecureX threat response



- Limited data is stored in cloud
- FMC can send IPS events to SecureX threat response
- Any IP, domain, file hash or IoC seen in FMC can queried in SecureX threat response, reducing complexity and time for threat hunting
- Continuous analysis with retrospection facilitates remediation and enhances forensics

SWS COMPUTERSYSTEME
Member of ACP Group

Agenda

- Traditionelle Netzwerk Designs und Challenges
- Cisco Secure Analytics
- Cisco Secure Network Analytics - Demo
- Cisco Secure Firewall
- Cisco Secure Firewall - Demo
- Q&A

SWS COMPUTERSYSTEME
Member of ACP Group

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?

Wir freuen uns auf Ihre weitere Anmeldung für unsere Webinar Serie:

- NAC und MFA