MEHR SICHERHEIT IM ZUSAMMENSPIEL

WIE CISCO-LÖSUNGEN MICROSOFT E3 SINNVOLL ERGÄNZEN

Manuel Götz

ACP IT Solution AG - Hauzenberg

IT Security Consultant

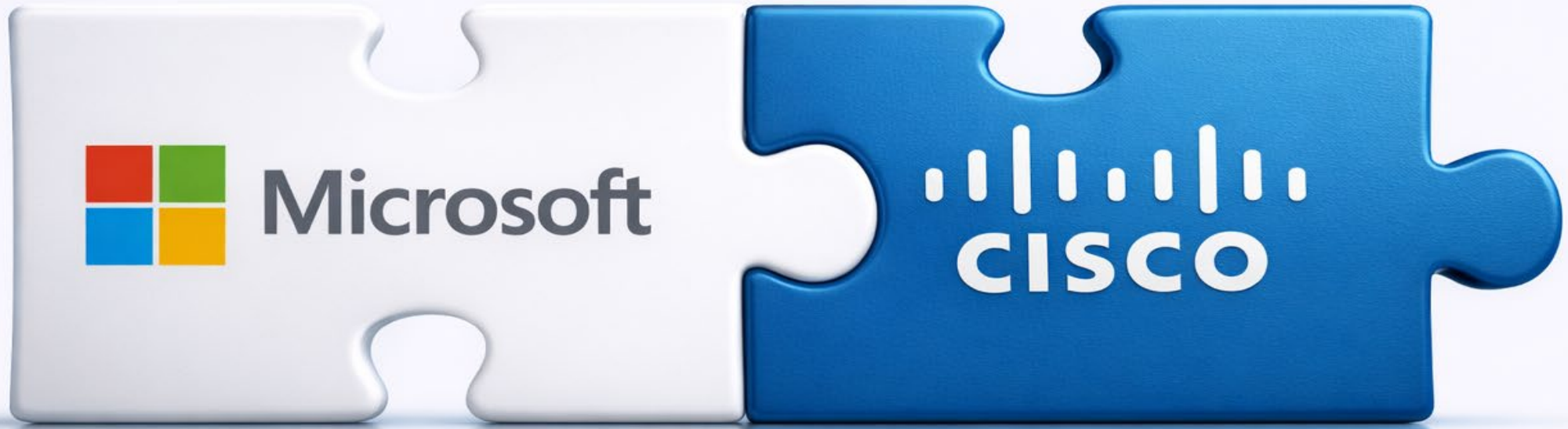
CCNP Security

manuel.goetz@acp.de

+49 8586 9604 223

+49 173 589 47 54

IT for innovators.



AGENDA

| DIE HERAUSFORDERUNG

END-TO-END SECURITY

| DAS ZUSAMMENSPIEL

MICROSOFT & CISCO

| DIE LÖSUNGEN VON CISCO

EMAIL THREAT DEFENSE

SECURE ACCESS

IDENTITY SECURITY

XDR

Haben Sie bereits Microsoft Security Lösungen im Einsatz?

- Nein
- E3 Lizenzen
- E5 Lizenzen
- Suiten

Wie viel Prozent aller IT-Angriffe zielen auf den User ab?

- 50%
- 65%
- 80%
- 95%

80% ALLER ANGRIFFE AUF USER GERICHTET

Social Engineering

Phishing Mail

Browser basierter Angriff

Malicious Website

Passwort Diebstahl

MFA Angriff

Deep Fakes

- IT Security ist fragmentiert
- Angriffe werden komplexer
- User arbeiten überall

IT Security muss End-to-End gedacht werden

Einzelne Security Produkte reichen nicht mehr aus. Wir brauchen eine ganzheitliche Security!

- Identity
- Endpoint
- Access / Traffic
- Detection / Response

Schutz in jeder Ebene nötig

Microsoft sieht den User und das Gerät

-> Das ist die Basis

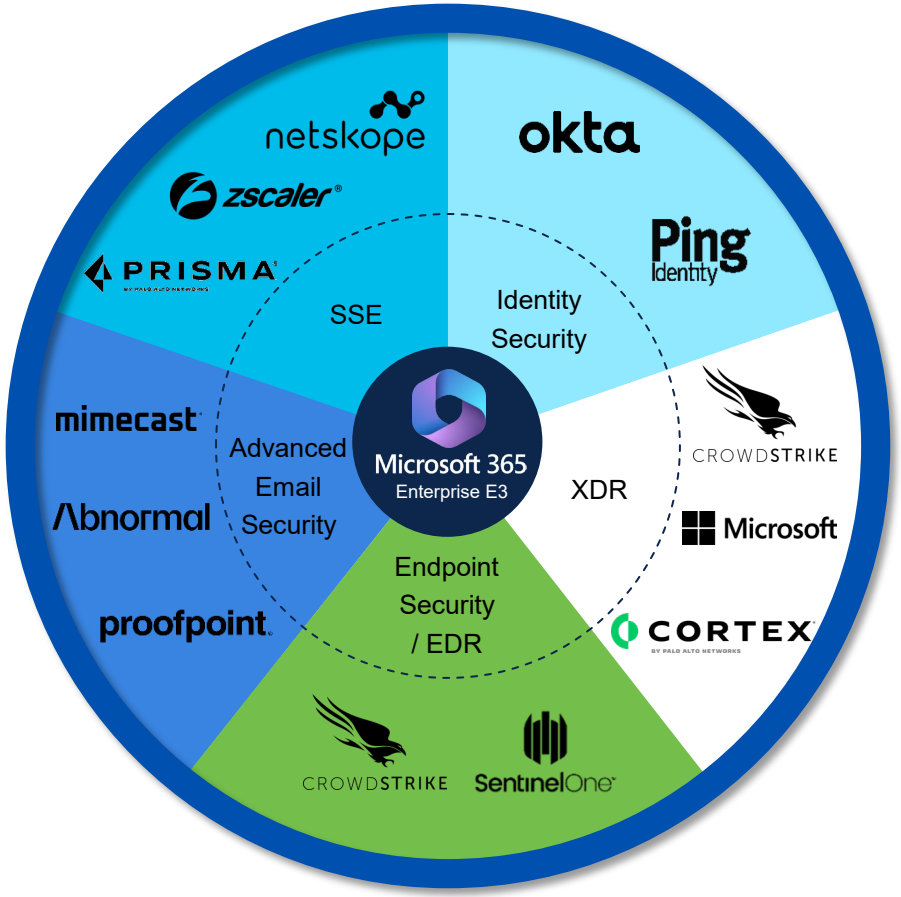
Cisco ergänzt:

-> Sicheren Zugriff & Traffic

-> Detection & Response

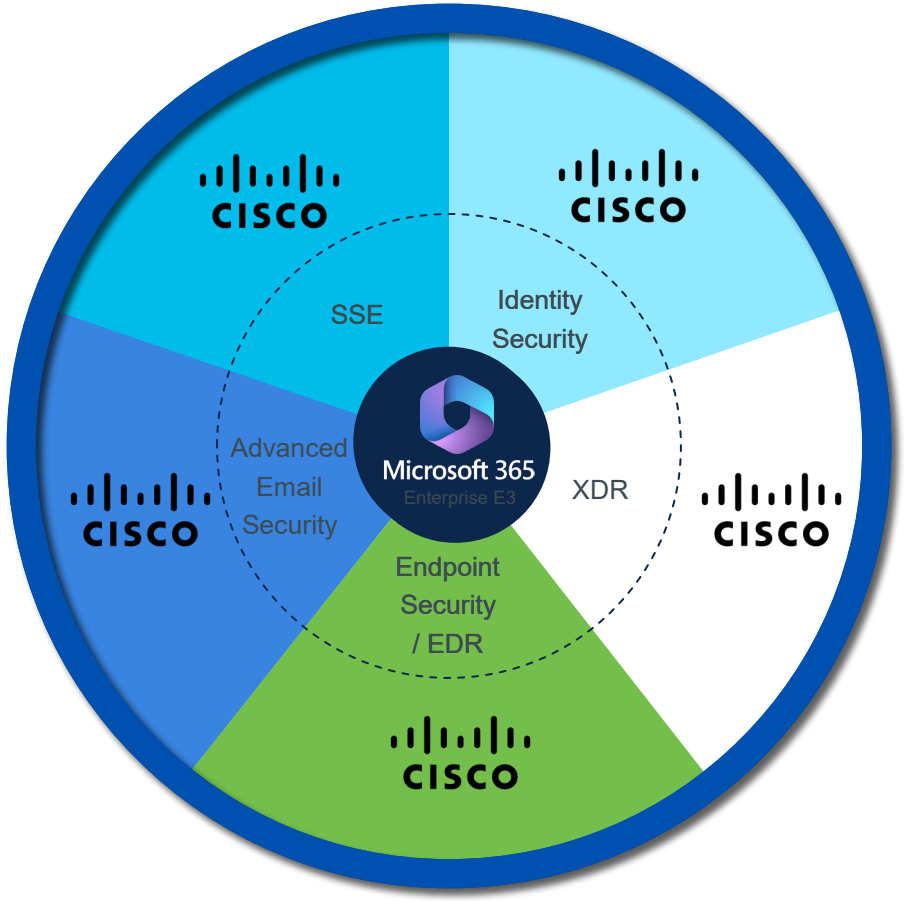
Gemeinsam entsteht echte
End-to-End Security

DAS ZUSAMMENSPIEL



- Microsoft E3 Lizenz (July 2026)
- Advanced Email Security
- Defender Suite
- Entra Suite
- Digital Experience Monitoring
- NAC
- NDR
- Identity Security

DAS ZUSAMMENSPIEL



- Cisco User + Breach Protection Suite
- Advanced Email Security
- EDR
- SSE
- NAC
- XDR
- NDR

Cisco ergänzt und ersetzt nicht

USER PROTECTION SUITE -> Access

- Zugriff absichern
- Zero Trust

BREACH PROTECTION SUITE -> Detection

- Bedrohungen erkennen
- Response automatisieren

User Protection Suite

SECURE SERVICE EDG E

Secure Internet Access

ZTNA for SaaS and Private Apps

Experience Insights

VPNaaS

Identity Security

Posture & Auth Management

Network Access Control

IoT Protection

Breach Protection Suite

Email Security

Endpoint Security

Threat Detection and Response

Network Visibility and Analytics

Incident Response

Managed Services

User Protection Suite secures *all*

- Users
- Applications
- Devices

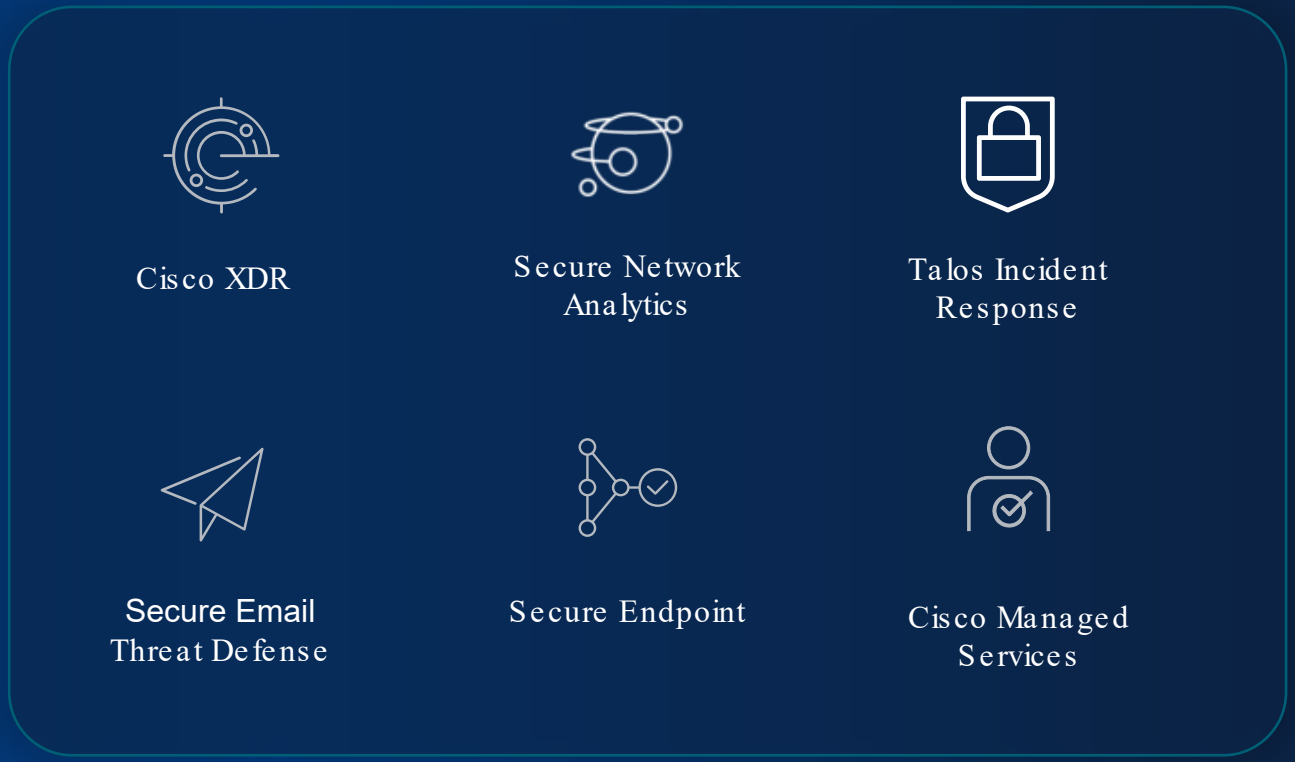
Cisco User Protection Suite & Microsoft: Better Together

Microsoft E3: Workplace infrastructure & productivity solution with light security

		Identity	Zero Trust Access	Email	Endpoint & Server
Why are organizations buying E3?	IT Infrastructure & Productivity	Entra ID Active Directory	Enterprise Applications & Devices	Microsoft 365 Enterprise Email	Microsoft Windows
What security products are included?	Basic Security in E3	Basic MFA	*Not included* *(Entra suite only)*	Basic blocking (spam & phishing)	Defender for Endpoint P1 (AV) *(excludes servers)*
What capabilities does Cisco provide?	Cisco User Protection Suite	Duo + Cisco Identity Intelligence	Cisco Secure Access & ISE	Email Threat Defense	Secure Endpoint
	**Better together Zero Trust strategy**	MFA + Identity Security	Secure Service Edge + Network Access Control	Anti-spam + Advanced Threat Protection	EPP + EDR

Breach Protection Suite enhances resiliency

- AI Driven
- Telemetry Rich
- Platform Powered



Breach Protection Suite + Microsoft E3

Microsoft E3: Workplace infrastructure & productivity solution with light security

		Email	Endpoint & Server	NDR	XDR	MDR
Why are organizations buying E3?	IT Infrastructure & Productivity	Microsoft 365 Enterprise Email	Microsoft Windows	Network	Network & Cloud	Network & Cloud
What security products are included?	Basic Security in E3	Basic blocking (spam & phishing)	Defender for Endpoint P1 (AV)	*Not included*	*Not included*	*Not included*
What capabilities does Cisco provide?	Cisco Breach Protection Suite	Email Threat Defense	Secure Endpoint	Cisco Secure Network analytics	Cisco XDR	Managed XDR / Talos hours
	Better together Zero Trust strategy	Anti-spam + Advanced Threat Protection	EPP + EDR	NDR	XDR	24x7 monitoring, detection and response

Breach Protection Suite

Cisco & Microsoft: Better Together

Microsoft E3: Workplace infrastructure & productivity solution with light security

		Identity	Zero Trust Access	Email	Endpoint & Server	XDR & NDR
Why are organizations buying E3?	IT Infrastructure & Productivity	Entra ID Active Directory	Enterprise Applications & Devices	Microsoft 365 Enterprise Email	Microsoft Windows	Network & Cloud
What security products are included?	Basic Security in E3	Basic MFA	*Not included (Entra suite only)*	Basic blocking (spam & phishing)	Defender for Endpoint P1 (AV)	*Not included*
What capabilities does Cisco provide?	Cisco User Protection Suite	Duo + Cisco Identity Intelligence	Cisco Secure Access & ISE	Email Threat Defense	Secure Endpoint	Cisco XDR & Secure Network Analytics
	**Better together Zero Trust strategy**	MFA + Identity Security	Secure Service Edge + Network Access Control	Anti-spam + Advanced Threat Protection	EPP + EDR	XDR + NDR

User Protection Suite

Breach Protection Suite

DAS ZUSAMMENSPIEL

User Protection Suite

Essentials

- Secure Access Essentials
  (Secure Internet + Secure Private Access)
- Duo Advantage
- Email Threat Defense

Advantage

Everything in Essentials Plus

- Secure Access Advantage
  (Secure Internet + Secure Private Access)
- ISE Premier
- Secure Endpoint Advantage

Breach Protection Suite

Essentials

- Cisco XDR Essentials
- Secure Endpoint Advantage
- Email Threat Defense

Advantage

Everything in Essentials Plus

- Cisco XDR Advantage
- Secure Endpoint Premier
- Secure Network Analytics
- Cisco Telemetry Broker

Premier

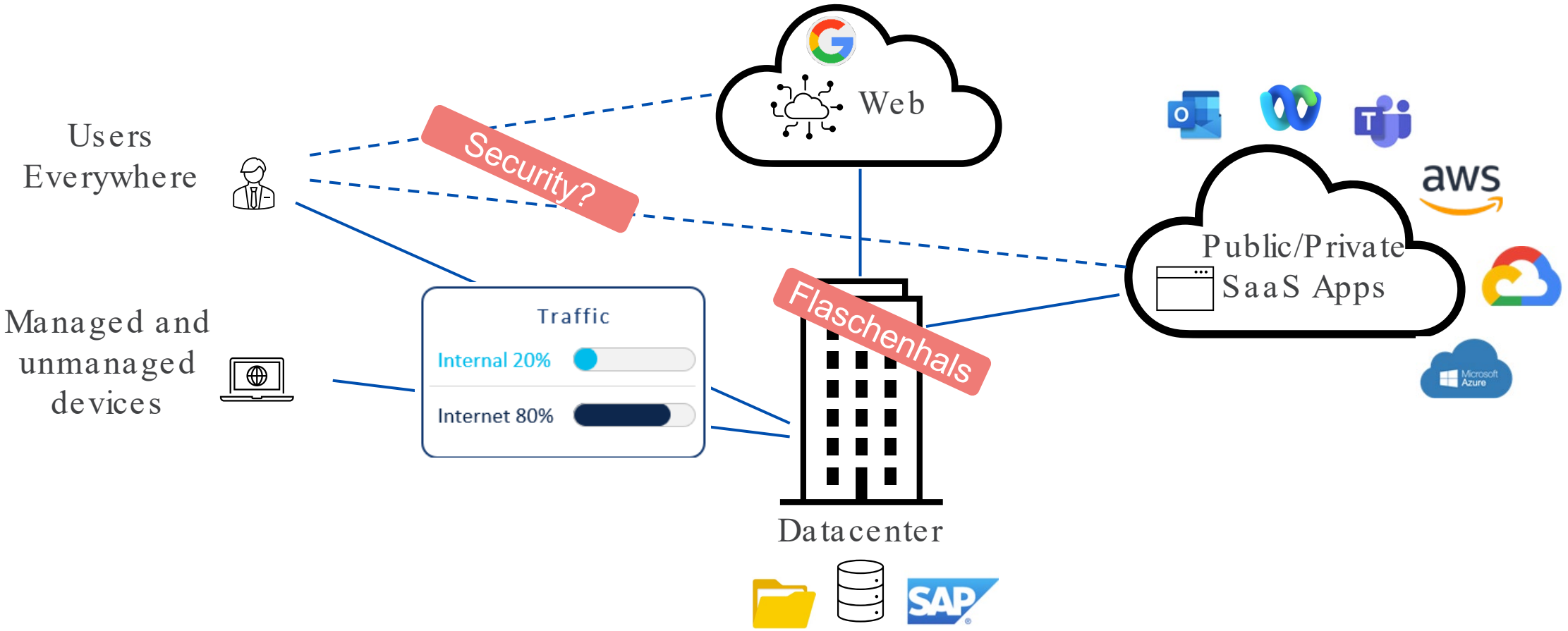
Everything in Advantage Plus

- Cisco XDR Premier (Managed XDR)
- Cisco Talos Incident Response
- Cisco Technical Security Assessments

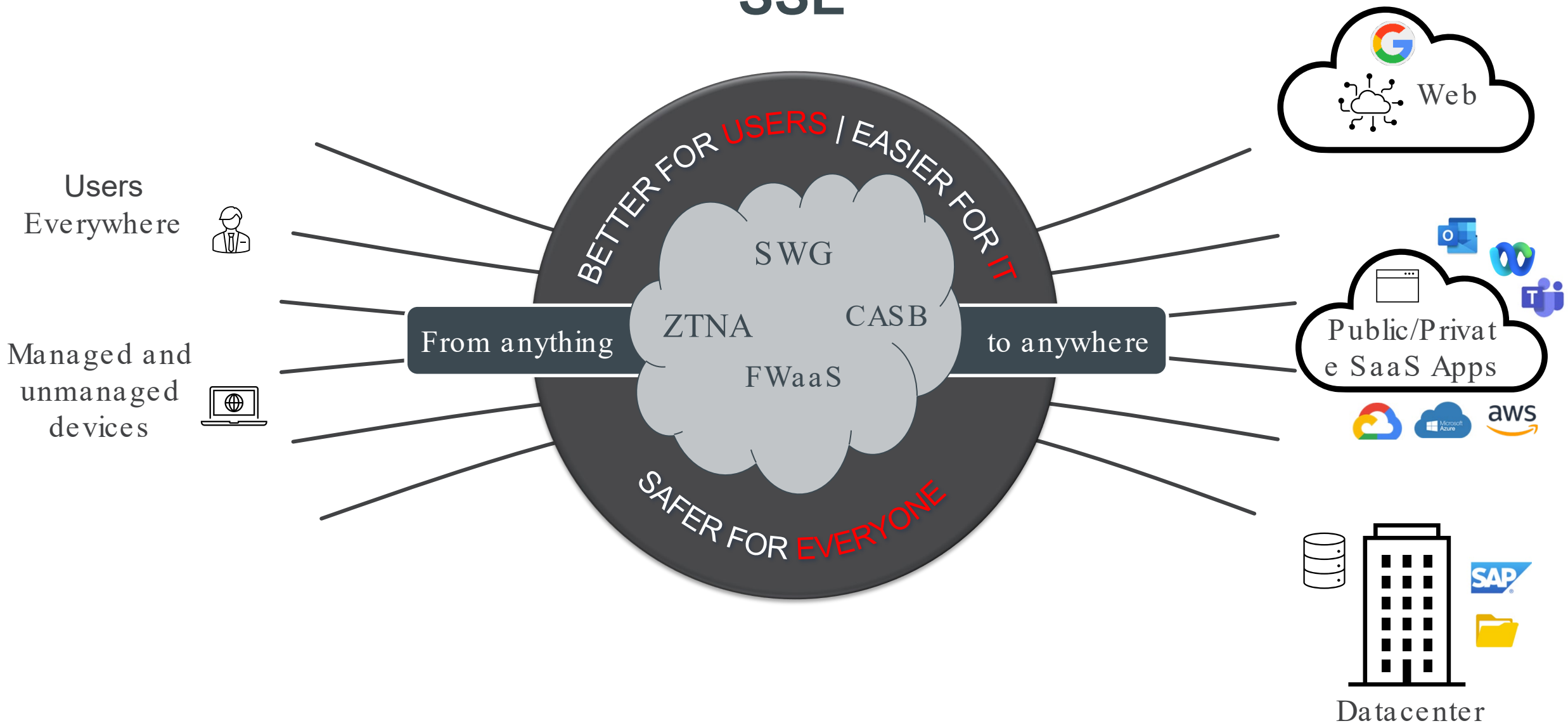
CISCO SECURE ACCESS

SSE-PLATTFORM FÜR SICHEREN ZUGRIFF AUF ANWENDUNGEN

Traditional Infrastructure



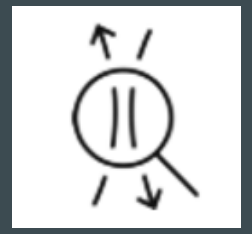
Secure Service Edge
SSE



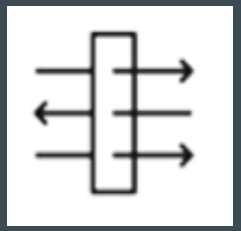
Secure Service Edge - Kernbausteine

Zero Trust Network Access

Cloud Access Security (CASB & DLP)



Secure Web Gateway



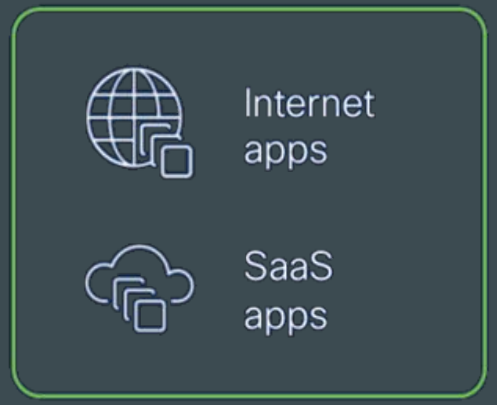
Firewall as a Service (IPS)

Secure Service Edge – AddOn´s

- DNS Security
- SDWAN Integration
- Advanced Malware Protection
- File Sandbox
- Remote Browser Isolation
- Digital Experience Monitoring
- VPN as a Service
- AI Assistant

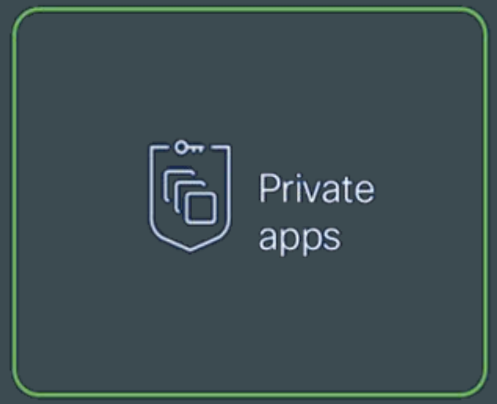
Use Cases unserer Kunden

Secure Internet Access



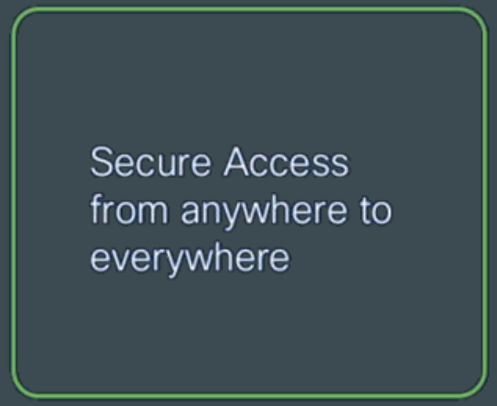
+

Secure Private Access

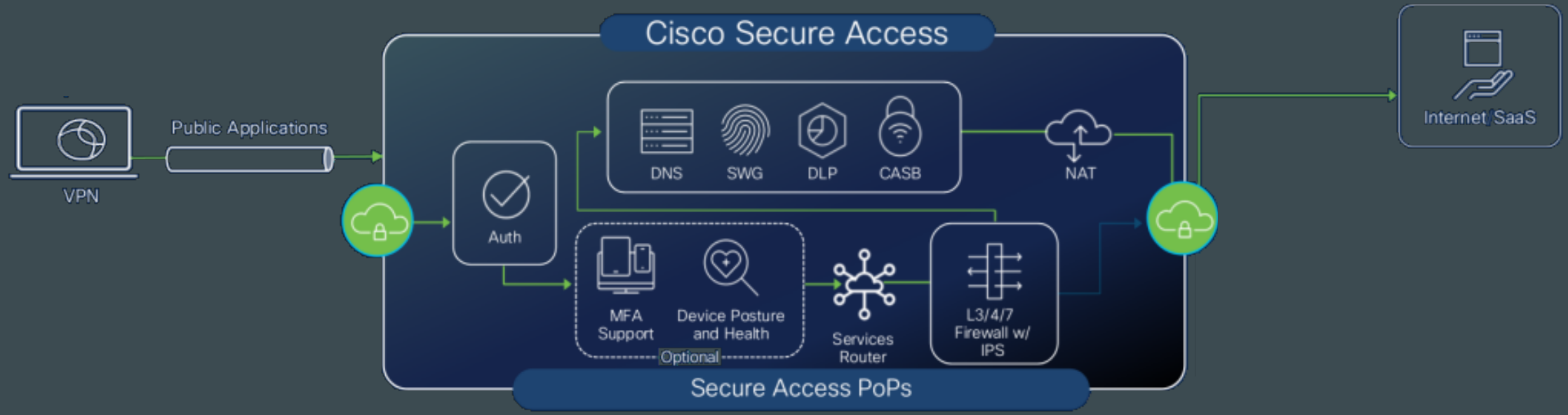


=

Secure Service Edge (SSE)



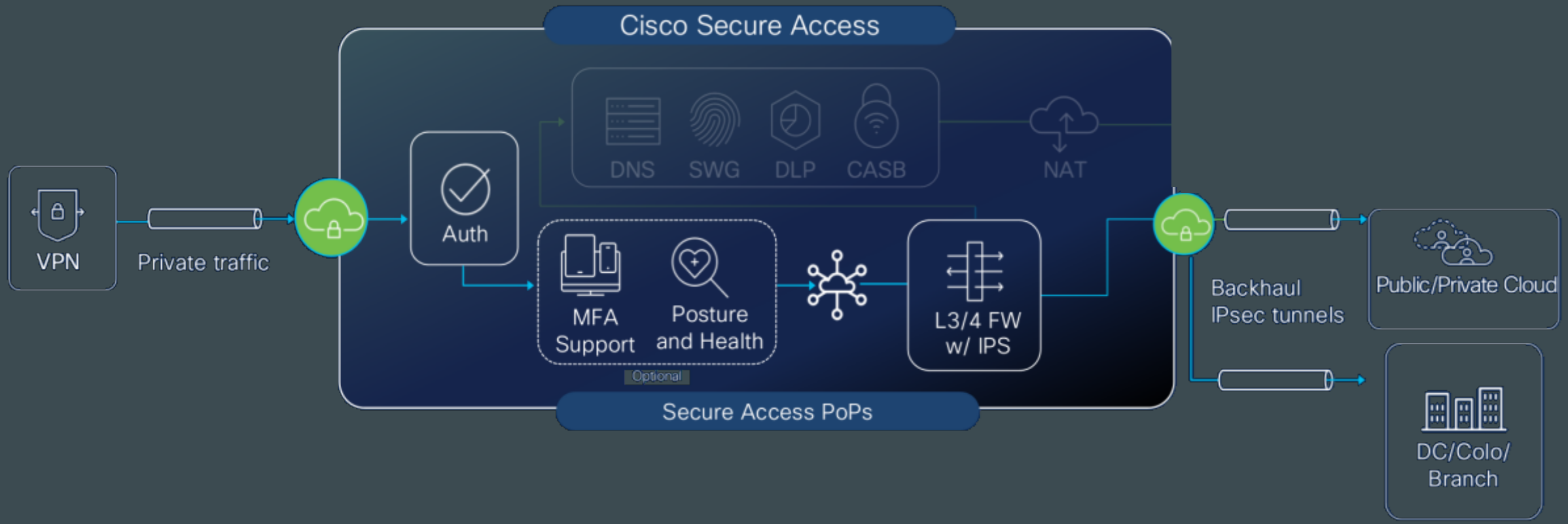
Secure Internet Access



Capabilities

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- IPS
- Single Inline inspection
- Application policy

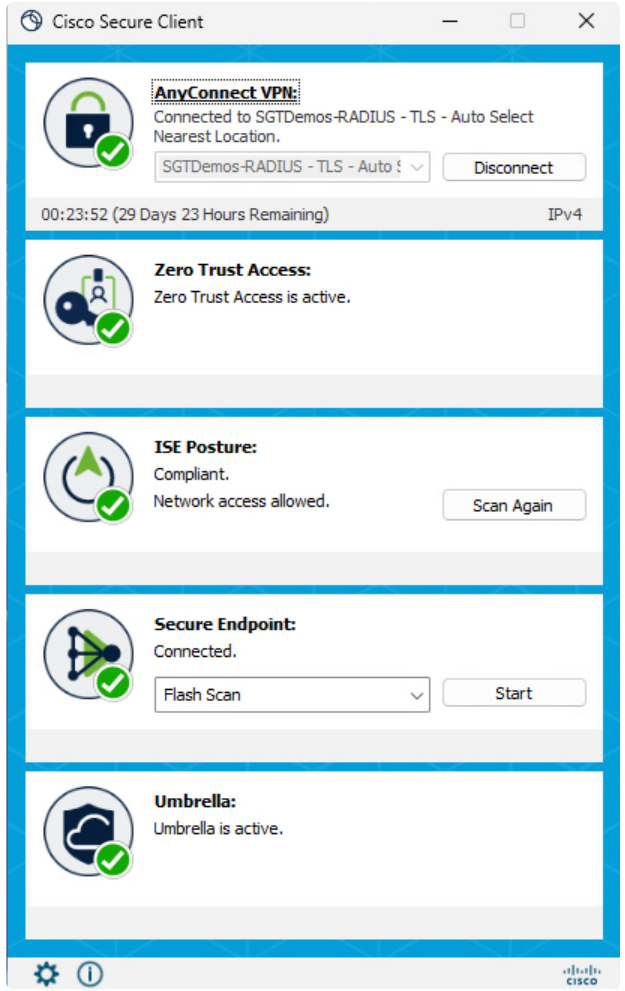
Secure Private Access



Benefits

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- Trusted Network Detection
- Start before logon
- IPS
- Granular context-based control

Cisco Secure Client



Network Visibility Module
Network Detection & Response

Secure Access
VPN-as-a-Service

Secure Access
Secure Private Access

ISE
Device authentication and posture

Secure Endpoint
Endpoint Detection & Response

Secure Access
Secure Internet Access

EMAIL THREAT DEFENSE

ERWEITERTE EMAIL-SICHERHEIT DURCH ZUSÄTZLICHE DETECTION, VISIBILITY UND RESPONSTE

Anton Scheibenzuber

ACP IT Solution AG - Hauzenberg

Support Engineer

CCNP Security

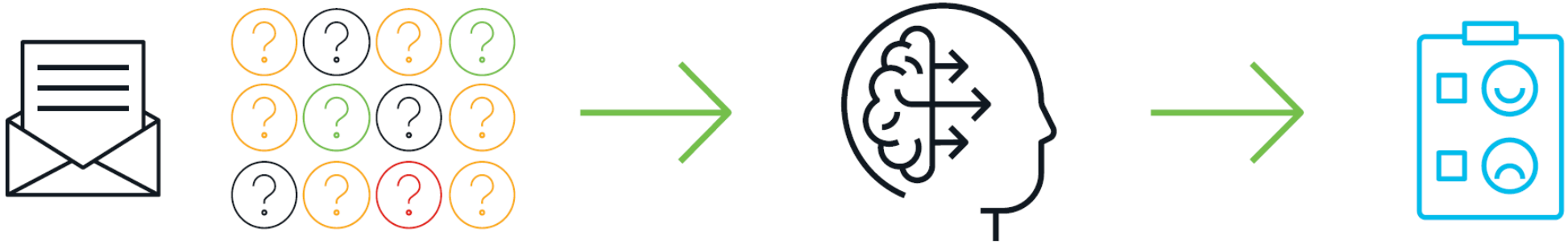
anton.scheibenzuber@acp.de

+49 8586 9604 195

IT for innovators.

Comprehensive Email Protection

Jede E-Mail wird auf eine Vielzahl unabhängiger Signale überprüft

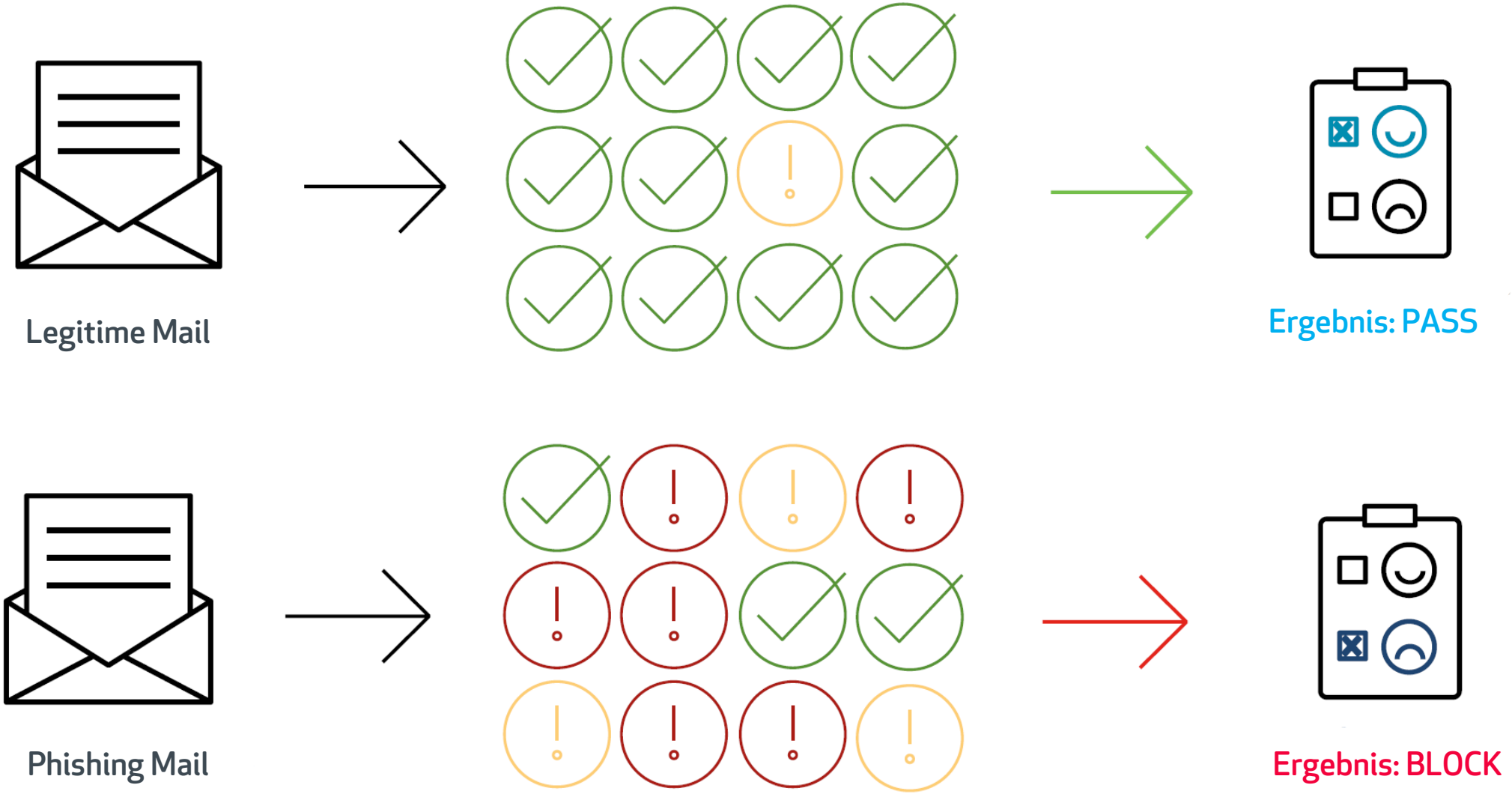


Die endgültige Entscheidung erfolgt durch das Zusammenführen aller Signale.

ETD – DAS STECKT DAHINTER

- Brand impersonation
- Call to action
- Data input request
- Disposable sender address
- Domain brand impersonation
- Email address in subject
- Email without text
- External admin
- External support
- Fake reply
- Frequent sender
- Frequent sender for recipient
- Frequent sender for recipient's domain
- Hidden text
- Hidden text injection
- Image-only email
- Inferred greeting
- Internal email
- Link masquerade
- Link visit request
- Low content reputation
- Low-reputation TLD
- Malicious HTML attachment
- Malicious URL
- Masqueraded file extension
- Open redirect
- QR code
- Rare sender address
- Rare sender domain
- Rare sender domain for recipient
- Rare sender domain for recipient domain
- Rare sender for recipient
- Rare sender for recipient domain
- References to cryptocurrency
- Reply
- Request for contact details
- Request for credentials
- Request to open attachment
- Reused URL
- Sender IP reputation
- Sender domain brand impersonation
- Sender domain reputation
- Sender name brand impersonation
- Sender name impersonation
- Sender name mismatch
- Shortened URL
- Suspicious button
- Suspicious sender address
- Suspicious sender domain
- Unicode masquerade
- Urgency
- User impersonation
- Username in subject
- Victim impersonation
- Victim specific URL
- Young domain

ETD – DAS STECKT DAHINTER



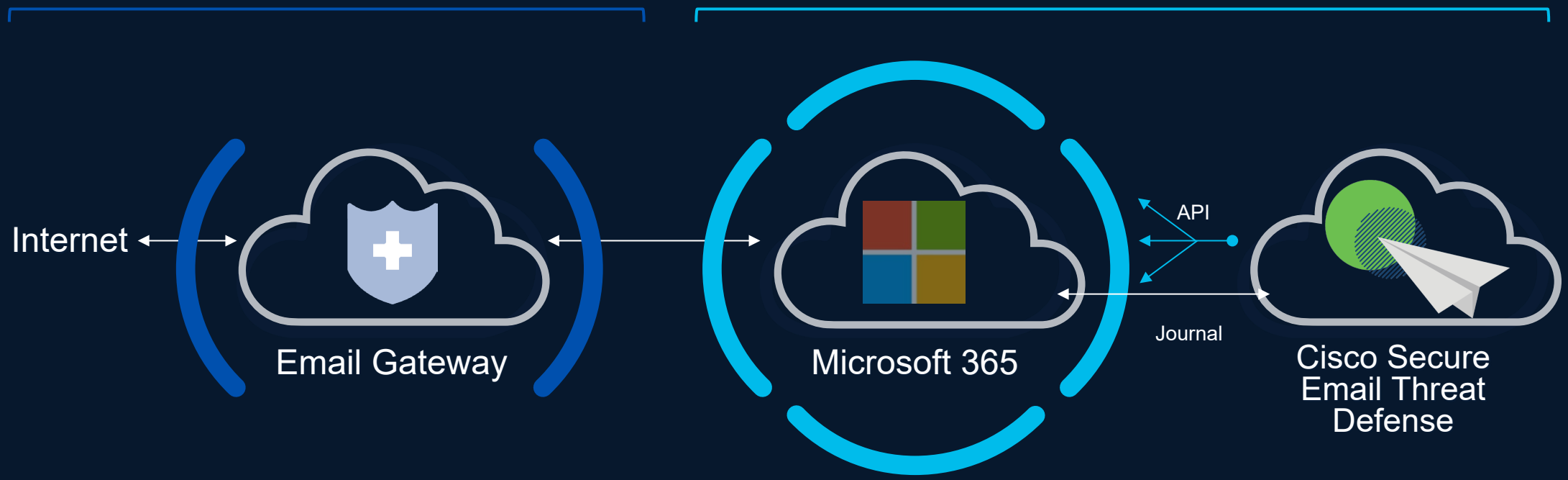
Complete visibility & protection for all messages

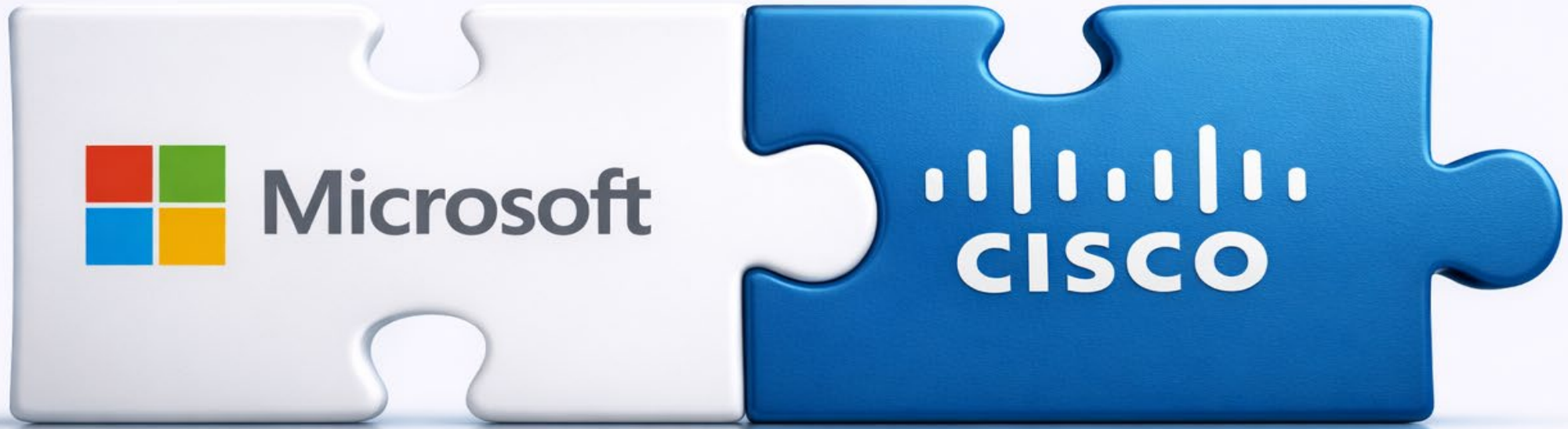
Secure Email Gateway

Modifies and filters **inbound** and **outbound** messages that cross the perimeter

Cisco Secure Email Threat Defense

Has complete visibility of **inbound, outbound and internal** messages

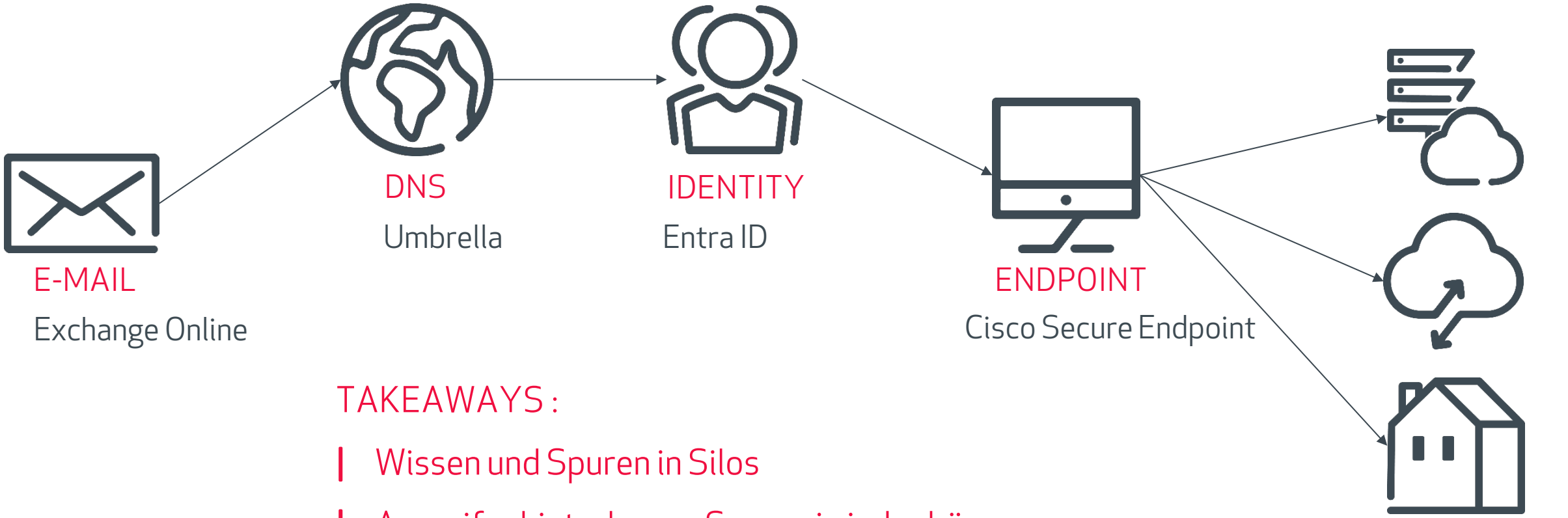




CISCO XDR

ZENTRALE SECURITY-OPERATIONS-PLATTFORM ZUR ERKENNUNG, ANALYSE UND REAKTION AUF BEDROHUNGEN

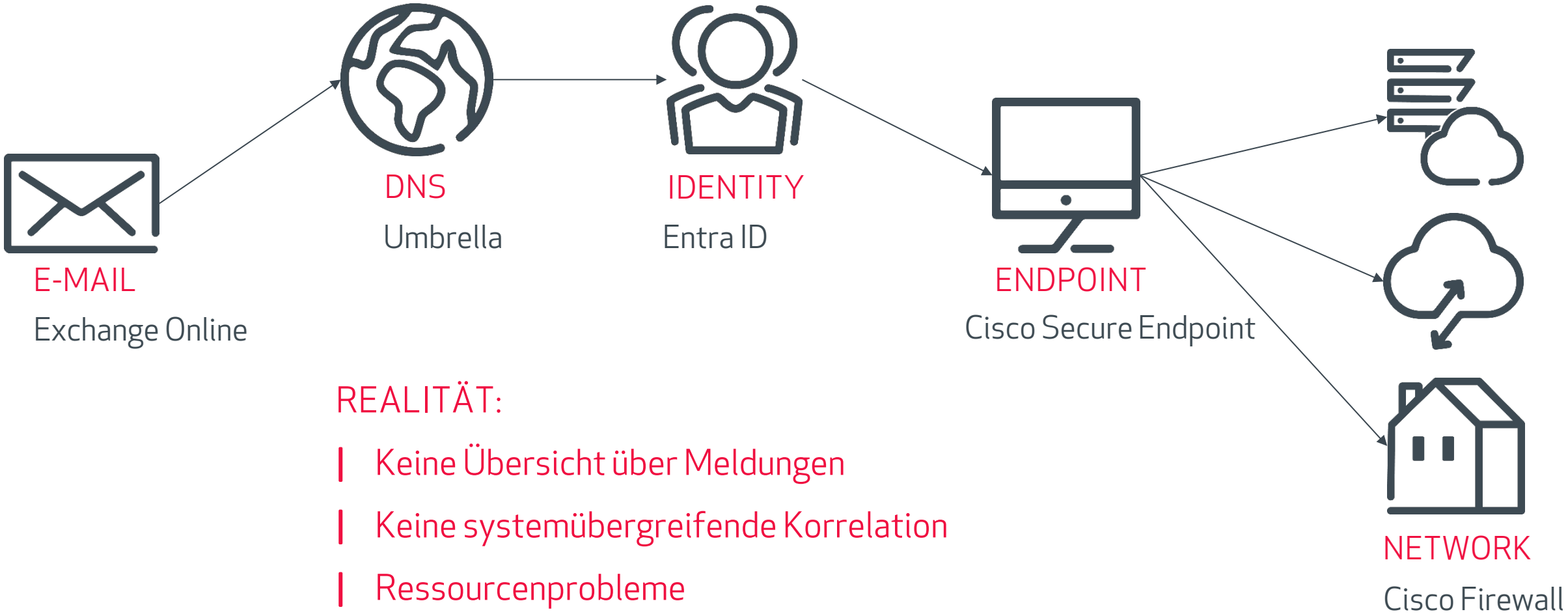
ALLTÄGLICHE GEFAHREN



TAKEAWAYS :

- Wissen und Spuren in Silos
- Angreifer hinterlassen Spuren in jeder Lösung
- Aufklärung von Vorfällen erfordert Sichtbarkeit

ALLTÄGLICHE GEFAHREN



REALITÄT:

- Keine Übersicht über Meldungen
- Keine systemübergreifende Korrelation
- Ressourcenprobleme

IM EINSATZ: CISCO XDR

Palo Alto Networks Cortex Cloud

CrowdStrike Falcon

Microsoft
Defender
For Endpoint

SentinelOne Singularity

Proofpoint Threat Protection

Ivanti Neurons for MDM

Microsoft Entra ID

Microsoft Cloud

VirusTotal

Trend Vision One

Observable Networks Appliance
On-Prem Sensors for Netflow, IPFIX and sFlow

Secure Firewall

Cisco Meraki

Cisco Secure Access

Umbrella

Secure Email Appliance

Cisco Duo

Secure Endpoint

IM EINSATZ: CISCO XDR

← Incidents

850 New **Suspicious Endpoint Activity and Registry Commands Detected**

Reported by **Cisco XDR Analytics** on 2025-06-25T15:55:19.029Z

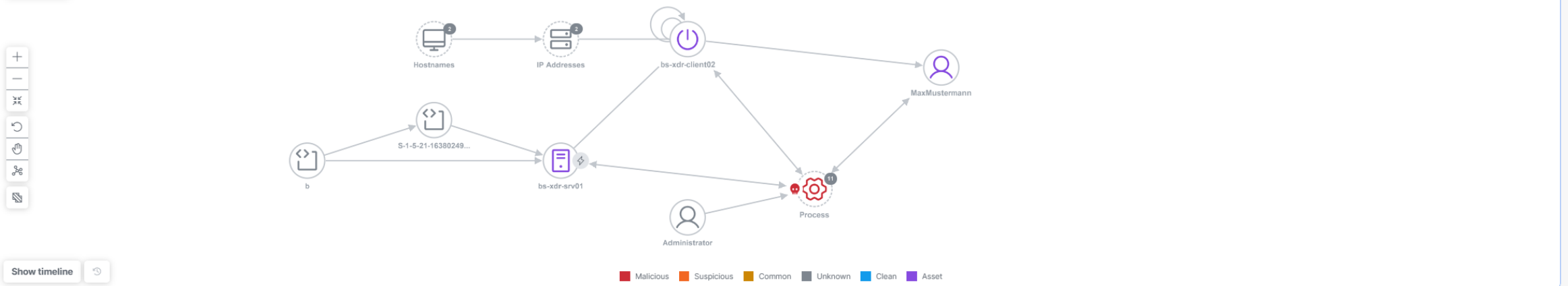
Unassigned

View detailed description

The incident occurred on Jun 25 2025. Suspicious endpoint activity was identified by Cisco Secure Cloud Analytics and suspicious registry commands were flagged by Microsoft Defender for Endpoint. Observables included an endpoint **bs-xdr-client02** and a user **maxmustermann**, a... AI-generated more

Overview Detection Response Worklog Report

Expand



3 Assets View all

TOP ACTIVE

10 Device
bs-xdr-client02 3 events

User
MaxMustermann 3 events

Endpoint
bs-xdr-srv01 2 events

52 Observables View all

TOP ACTIVE

IP Address
192.168.1.77 3 events

SHA1 Hash
8baa602fdc6ba67545c0717e2b9063a0bfe3f278 2 events

File Path
C:\Windows\explorer.exe 2 events

Process UID
ef7568900063a1b033717008848671fc322f8708 2 events

File Name
Rechnung #45323432.exe 2 events

5 Indicators View all

TOP ACTIVE

Microsoft Defender for Endpoint
An active 'ClickFix' malware in a command line was prevented from executing 1 event

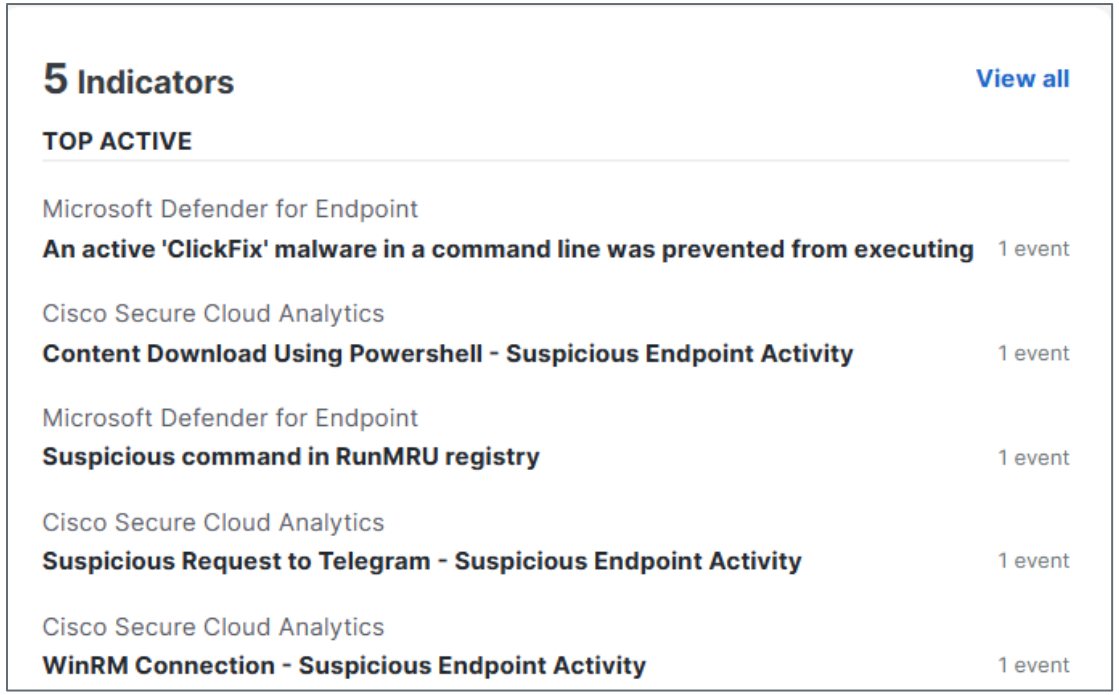
Cisco Secure Cloud Analytics
Content Download Using Powershell - Suspicious Endpoint Activity 1 event

Microsoft Defender for Endpoint
Suspicious command in RunMRU registry 1 event

Cisco Secure Cloud Analytics
Suspicious Request to Telegram - Suspicious Endpoint Activity 1 event

Cisco Secure Cloud Analytics
WinRM Connection - Suspicious Endpoint Activity 1 event

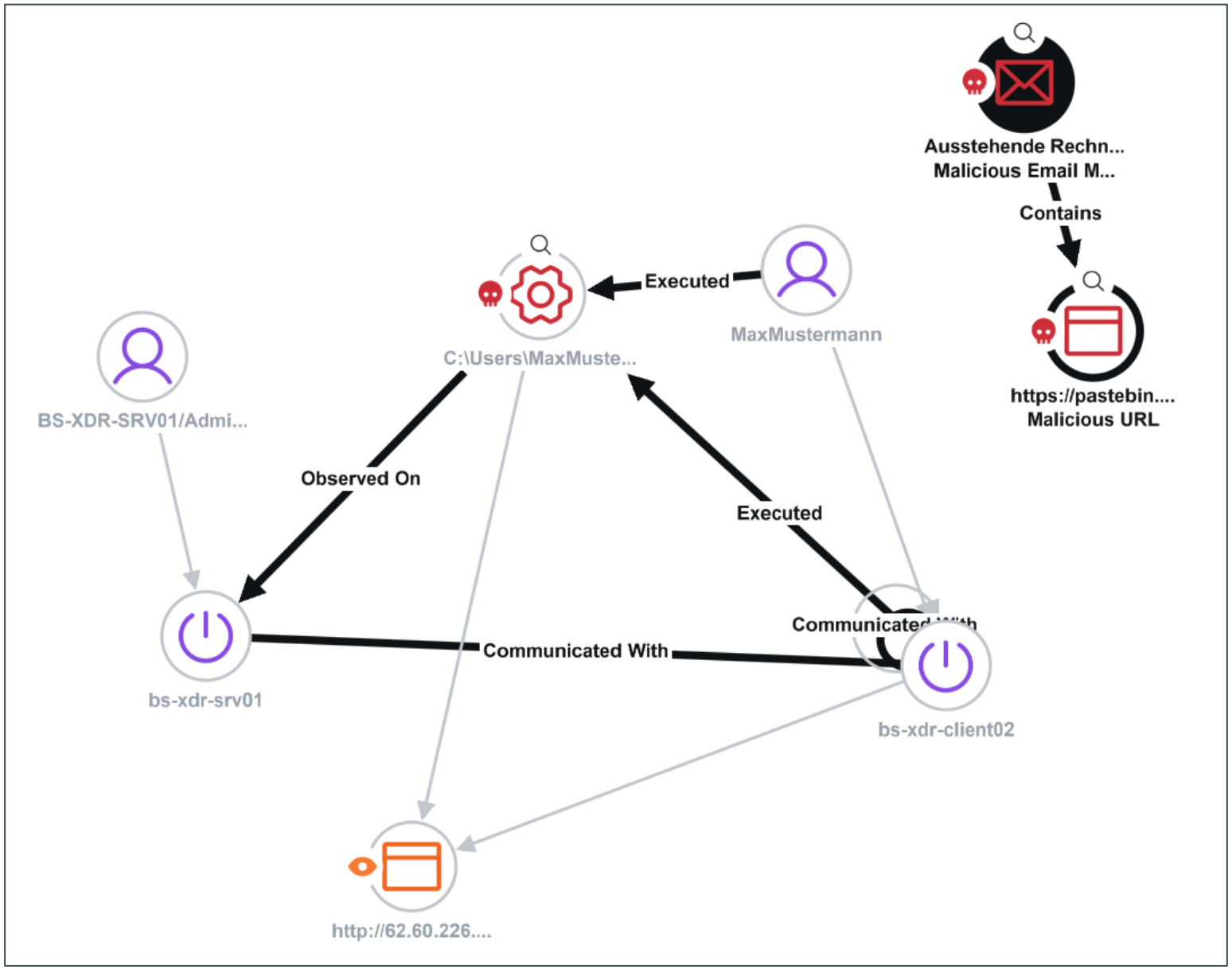
IM EINSATZ: CISCO XDR



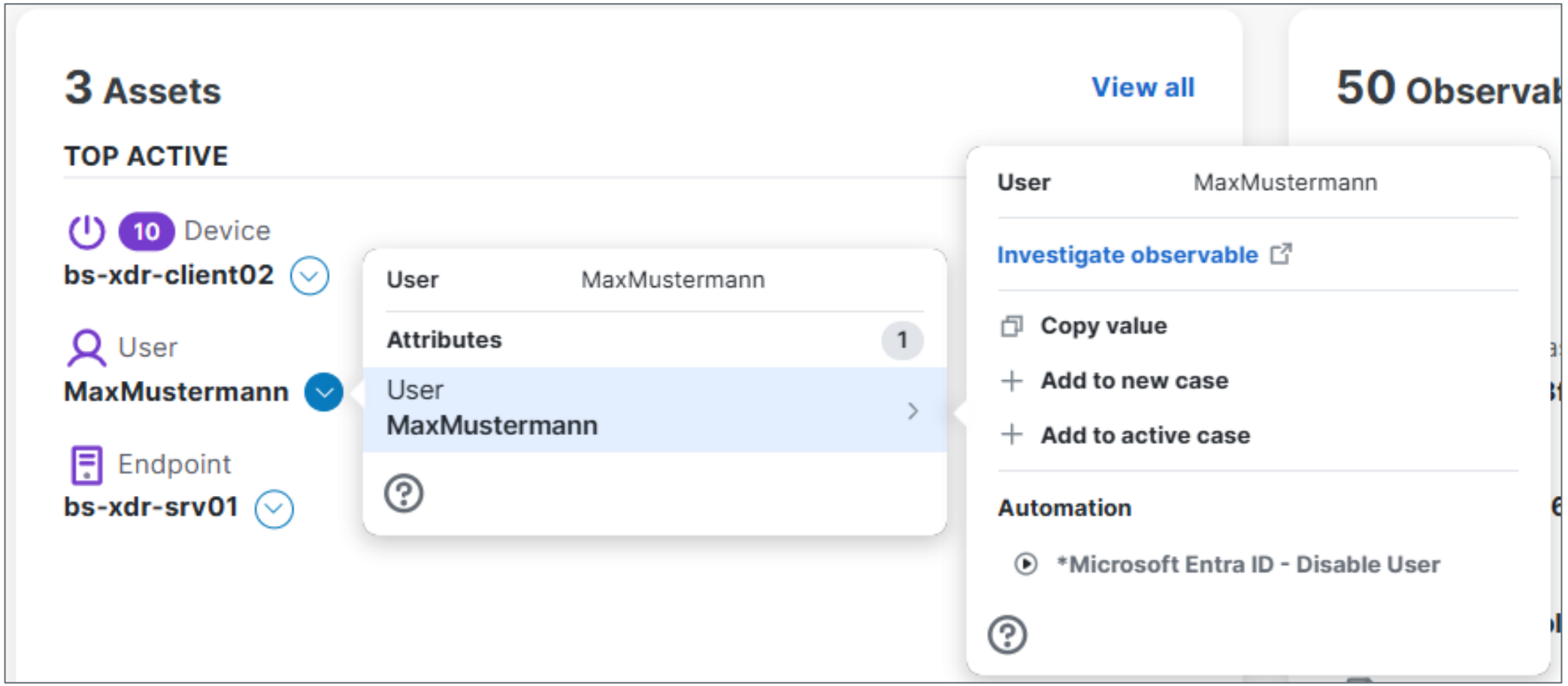
IM EINSATZ: CISCO XDR

First seen	Severity	Source	Indicators	Observables	Assets
2025-06-25T15:14:48.000Z	None	Microsoft Defender for Office 365	—	melanie@soc.swsrz.de https://pastebin.com/VnLagzSq Ausstehende Rechnung #24874 - bitte melden +4 more	10 Max Mustermann
2025-06-25T15:20:44.308Z	Info	Microsoft Defender for E...	'Tisar' malware was detected	96df96f572dd8ff7ede2d054390a005c... 12135 C:\Users\Administrator\Downloads\BrainShar... 3c6c4a7684215608b4388272b106a3c... ab6c1 +7 more	10 bs-xdr-srv01 BS-XDR-SRV01/Administrato
2025-06-25T15:29:41.000Z	High	XDR Endpoint	Suspicious Endpoint Activity	96df96f572dd8ff7ede2d054390a005c... 12135 MaxMustermann 037b2108d3e9efb02bc84111df82fe5e66d1c... +7 more	10 bs-xdr-client02 bs-xdr-client02
2025-06-25T15:31:33.000Z	Critical	XDR Endpoint	Content Download Using Powershell - Sus...	-NoProfile -ExecutionPolicy ByPass Invoke-W... 96df96f572dd8ff7ede2d054390a005c... 12135 C:\Users\MaxMustermann\Downloads\Rechn... +10 more	10 bs-xdr-client02 MaxMustermann
2025-06-25T15:14:47.000Z	None	Secure Email Threat Defe...	—	melanie@soc.swsrz.de https://pastebin.com/VnLagzSq Ausstehende Rechnung #24874 - bitte melden +5 more	10 Max Mustermann
2025-06-25T15:51:27.000Z	Medium	Secure Endpoint	Gen:Heur.Bodegun.23	96df96f572dd8ff7ede2d054390a005c... 12135 dc4fdcd96efe7b41e123c4cba1905916... 7bf58 \\?\C:\Users\MaxMustermann\AppData\Local\... +2 more	10 bs-xdr-client02
2025-06-25T15:51:37.000Z	Medium	Secure Endpoint	Gen:Heur.Bodegun.23	96df96f572dd8ff7ede2d054390a005c... 12135 dc4fdcd96efe7b41e123c4cba1905916... 7bf58 7zFM.exe +2 more	10 bs-xdr-client02

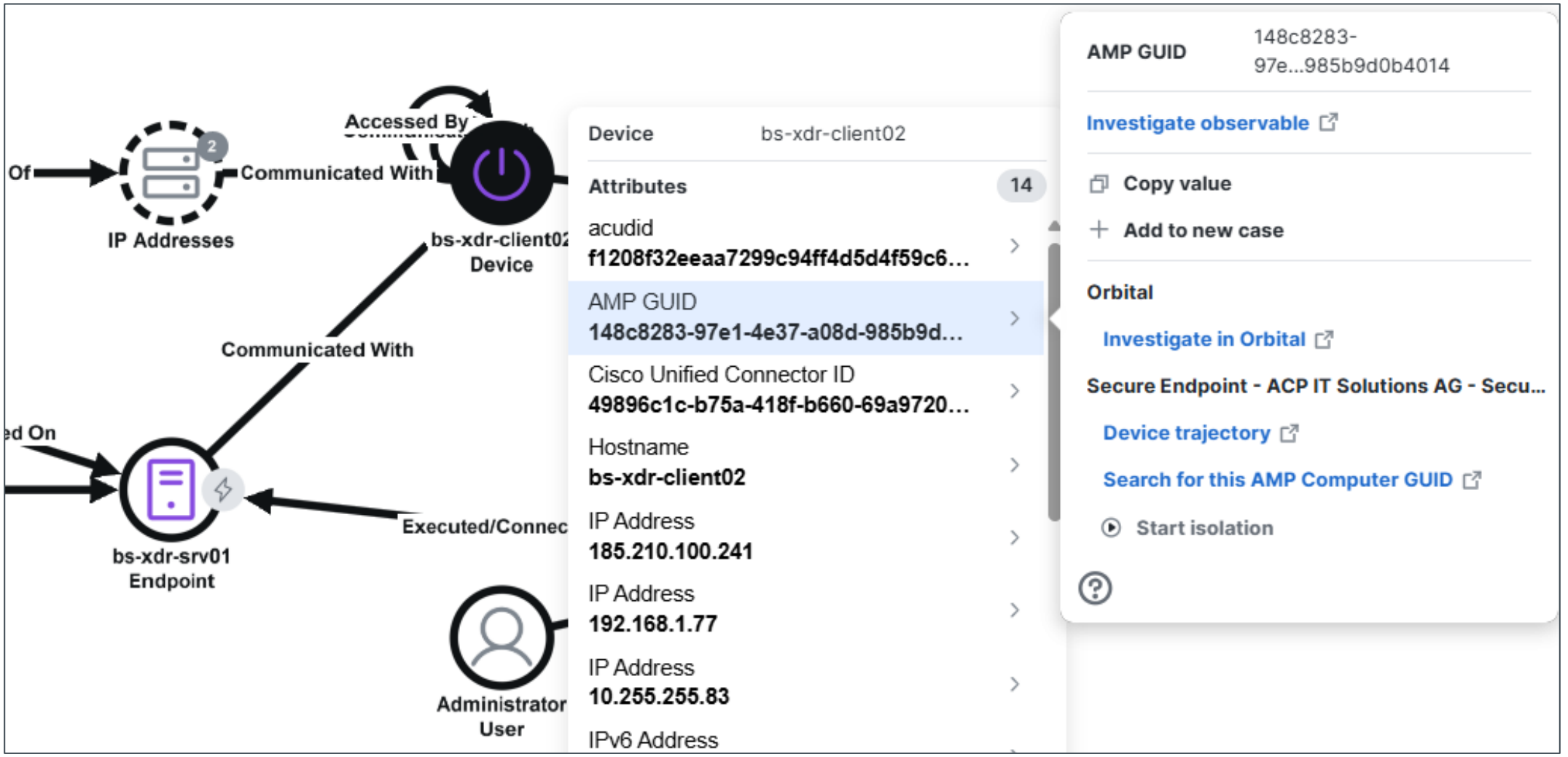
IM EINSATZ: CISCO XDR



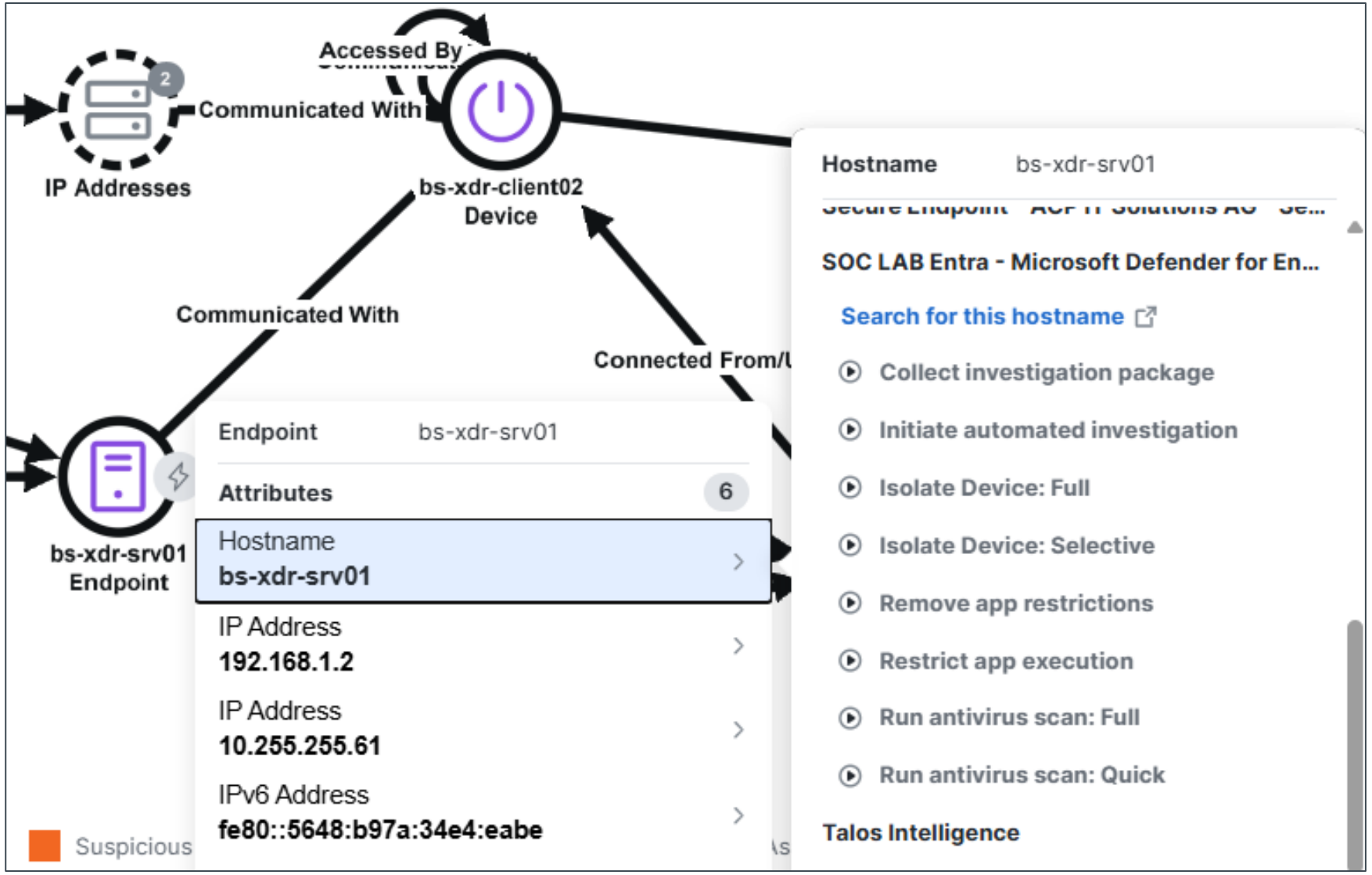
IM EINSATZ: CISCO XDR



IM EINSATZ: CISCO XDR



IM EINSATZ: CISCO XDR



ALLES IM BLICK MIT CISCO XDR

PRODUKTÜBERGREIFEND

- Erkennungen: übersichtlich & strukturiert
- Reaktionen: einheitlich & automatisierbar

EINFACH UND SCHNELL ANBINDBAR

- „On-Top“ eigenständiger Lösungen
- Schnelle und einfache Einrichtung

ZEITSCHONENDER AUFBAU VON SOC FÄHIGKEITEN

- Vorgefertigte oder eigene Playbooks
- Automatisierung mit eigenen Workflows

Microsoft sieht den User und das Gerät

-> Das ist die Basis

Cisco ergänzt:

-> Sicheren Zugriff & Traffic

-> Detection & Response

Gemeinsam entsteht echte
End-to-End Security

Ganzheitliche IT-Security

Organisation	Firewall	DMZ	Web-Security
Email-Security	Security KI	Segmentierung	VPN und Zero-Trust Network Access
Endpoint und Server-Security	Datenträgerverschlüsselung	Mobile Device Management	Cloud Nutzung (SaaS)
Berechtigungs- und Zugriffsmanagement	Update Management	Identity Intelligence	SIEM / SOAR / XDR
Penetration-Tests	User-Awareness Trainings	IT-Notfallplan für Sicherheitsvorfälle (IR-Plan)	Backup
MFA	Visibility	Logging	Compliance

Ganzheitliche IT-Security

Organisation	Firewall	DMZ	Web-Security
Email-Security	Security KI	Segmentierung	VPN und Zero-Trust Network Access
Endpoint und Server-Security	Datenträgerverschlüsselung	Mobile Device Management	Cloud Nutzung (SaaS)
Berechtigungs- und Zugriffsmanagement	Update Management	Identity Intelligence	SIEM / SOAR / XDR
Penetration-Tests	User-Awareness Trainings	IT-Notfallplan für Sicherheitsvorfälle (IR-Plan)	Backup
MFA	Visibility	Logging	Compliance

VIELEN DANK

FÜR IHRE AUFMERKSAMKEIT

ACP | IT FOR INNOVATORS