IT Sicherheit als Managed Service mit Sophos MSP Connect

Michael Gutsch
Head of MSP CEEMEA

SOPHOS

MSP Markt

SOPHOS

Managed Service Provider Modell

Managed Services

Ein Managed Services Provider (MSP) ist ein Informations-Technologie-Dienstleister, der die Verantwortung für die Bereitstellung einer **definierten Reihe von Dienstleistungen** für seine Kunden übernimmt und verwaltet.



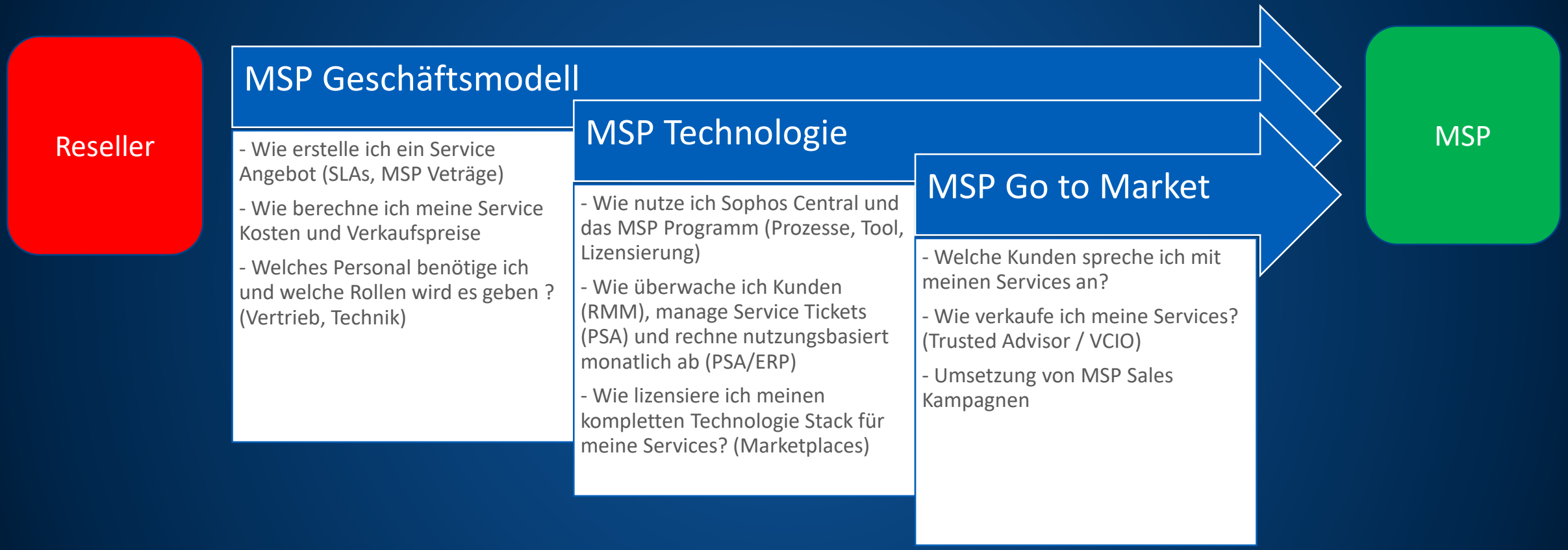
Virtual CIO

Vorteile des MSPs

- Wiederkehrende Umsätze
- Neue Kunden
- Kundenbindung
- Hohe Profitabilität

SOPHOS

Transformation – Vom Reseller zum MSP



Managed Services Markt – War treibt Kunden um?

IT Sicherheit wird immer aufwändiger

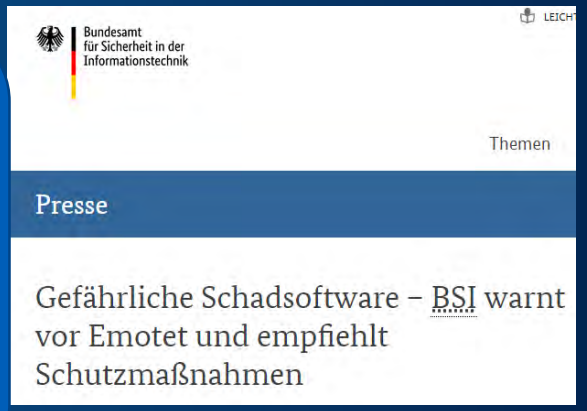
- Steigende Compliance(DSGVO) und IT Sicherheits Anforderungen
- Komplexere Cyber Angriffe, die Bedrohungslage ändert sich ständig



Steigendes Schade

- Digitalisierung zentra
  im Mittelstand!
- IT & Daten immer wi

In 2022 wird der globale Markt für Managed Services etwa 268 Milliarden $ sein. (Wachstum ca. 11.3% pro Jahr). **Etwa 1/3 des Marktes werden Managed Security Services sein.***



Fachkräftemangel

- Mangel an in House Know how
- Fachkräft sind teuer und schlicht nicht zu finden



Hohe Kosten für Managed Services / Mangelndes Vertrauen in den MSSP

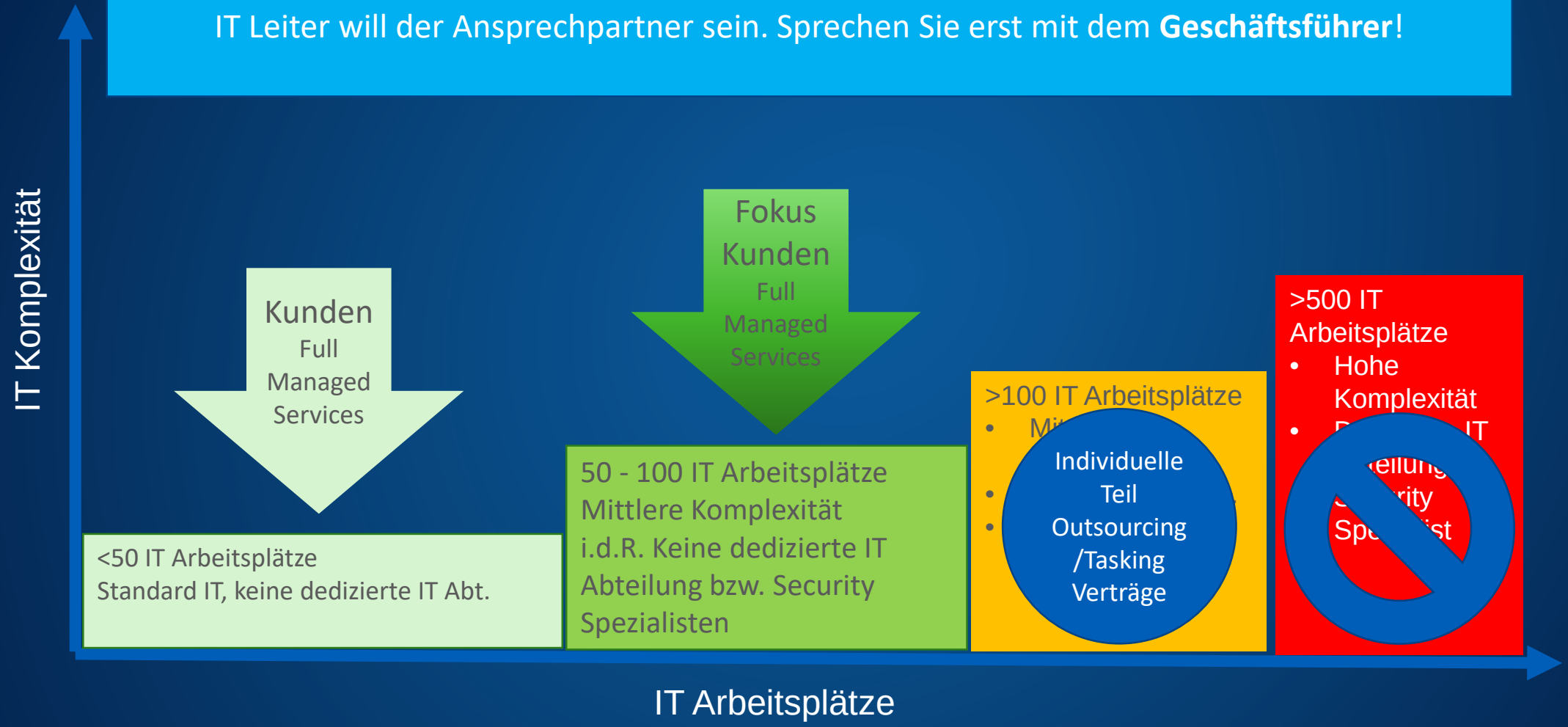
- Kleine und mittlere Unternehmen scheuen die Kosten für Managed Security Services*
- Große Unternehmen trauen MSSPs nicht zu, Ihre komplexe Infrastruktur zu schützen*

SOPHOS

* IDC / *Mordor Intelligence
*IDG Studie Managed Security 2018

Managed Services – Zielkunden für schnelles Wachstum

IT Leiter will der Ansprechpartner sein. Sprechen Sie erst mit dem **Geschäftsführer**!



SOPHOS

Neue Managed Service Kunden gewinnen

Bestandskunden

- Kein oder nur 1 Administrator
- Beschwert sich über hohe Investitionen / Rechnungen
- Kunden, die bereits Security Incidents hatten aufgrund von mangelndem Know How
- DSGVO Compliance

Neukunden

- Email Marketing Kampagnen aufsetzen DSGVO, Ransomware, Phishing etc.(Sophos Kampagnen nutzen)
- Gezielte Call Out Days -> sprechen Sie KMU Kunden in der Region an
- Sprechen Sie über Risiken, nicht über Features

Neue Managed Security Service Verträge ☺

Security Probleme der Kunden erkennen



Problem:

Administratoren haben den Fokus auf dem Anwender:

- Alle Applikationen im Griff -> Alle MAs arbeiten damit / Geschäftsbetrieb hängt davon ab!
- Druckerprobleme, Excel, Word, Telefon -> Turnschuhadministration füllt den Tag



Was leidet, ist die Infrastruktur unter den Applikationen:

- Backup ungetestet
- IT Sicherheit ohne Monitoring
- Sicherheitsrisiken werden nicht regelmäßig geprüft und beobachtet!
- Admin reaktiv (Feuerwehr)

Security Probleme der Kunden lösen



Lösung:

IT Security proaktiv betreiben

→ Ihre Managed Security Services

- Up to date Technologie -> bester Schutz gegen aktuelle Bedrohungen
- Monitoring, Helpdesk und garantierte SLAS -> kontinuierlicher Betrieb
- Umfassende Service Pakete zu einem planbaren Preis

Managed Services mit Sophos – Comp4U



ServicePlus Server

Basismodul für jeden Netzwerk-Service: Exakt abgestimmte Parameter werden 24h am Tag überwacht. Sobald Abweichungen auftreten, können wir aktiv werden. Lange bevor daraus eine Störung werden kann.
Einfach kalkulierbar als Managed-Service!

ServicePlus Backup

Wir prüfen ständig Status, Funktion und Ergebnisse Ihrer Datensicherung. Durch regelmäßige Recoverytests wird sichergestellt, dass im Falle eines Falles die Daten auch nutzbar und vollständig sind.
Einfach kalkulierbar als Managed-Service!

ServicePlus Online-Backup

Die bequemste Form der Datensicherung, direkt in unser Rechenzentrum. Hochverfügbar und unabhängig von Ihrer Infrastruktur. Schnellste Wiederherstellung ohne aufwändige Datenträgerauslagerung.
Günstige Volumentarife!

ServicePlus Firewall

99% aller Angriffe gegen Firewalls sind nicht zielgerichtet und erfolgen zufällig gegen bekannte Schwachstellen. Kontinuierliche Überwachung und regelmäßige Aktualisierung der Systeme schützt die sensibelste Technik in Ihrem Netzwerk.
Einfach kalkulierbar als Managed-Service!

ServicePlus AntiVirus

Heute so wichtig wie noch nie: Zusammen mit der Firewall bieten gute AV-Systeme hohen Schutz. Performante AV-Systemwartung und Patternservice ohne Zeitverzug für Server und zentrale AV-Systeme.
Einfach kalkulierbar als Managed-Service!

ServicePlus Desktop

Unsere bequemste Option: Pflege aller Desktops und Notebooks. Sicherheitsaktualisierung des Betriebssystems, Patches von Standard-Software und Überwachung von Systemparametern. Inklusive Fernwartung und Anwendersupport.
Einfach kalkulierbar als Managed-Service!

ServicePlus Kontingent

Für Ihre zusätzlichen Wunschleistungen wählen Sie Servicestunden als individuelles Kontingentpaket zum fairen Vorteilspreis. Kontingente verfallen nicht und sind für viele Leistungen nutzbar. Zubuchbar zu allen ServicePlus-Paketen.
Preisvorteil bis 35%

ServicePlus Dokumentation

Wir erfassen alle Systeme in einer professionellen Dokumentation: Hard- und Software, Einrichtungs- und Betriebsparameter, Infrastruktur- und Benutzerdaten. Ständig aktualisiert und jederzeit abrufbar.
Einfach kalkulierbar als Flatrate!

ServicePlus 24h

Benötigen Sie Service auch nachts oder am Wochenende? Kein Problem mit unseren Notdienst-Services: Rund um die Uhr, auch an Wochenenden oder Feiertagen, sind wir auf Wunsch für Sie erreichbar.
Lassen Sie sich gleich beraten!

	ServicePlus **Basis**	ServicePlus **Standard**	ServicePlus **Premium**
ServicePlus Server	✓	✓	✓
ServicePlus Backup	✗	✓	✓
ServicePlus AntiVirus	✗	✓	✓
ServicePlus Firewall	✗	✓	✓
ServicePlus Arbeitsplatz	✗	✗	✓
ServicePlus Kontingent	✗	8 Zeiteinheiten à 15 Minuten	Flatrate
ServicePlus Dokumentation	✗	✗	✓
ServicePlus Online-Backup	✗	✗	✓
Garantierte Reaktionszeit	8 Stunden	4 Stunden	2 Stunden
Hotlinezeiten	9-17 Uhr	7:30 - 18:30 Uhr	24 Stunden
Zugang zum Ticketsystem	✗	✗	✓
Anfahrten für Vor-Ort-Service	✗	1 enthalten	Alle enthalten
	JETZT ANFRAGEN	JETZT ANFRAGEN	JETZT ANFRAGEN

SOPHOS

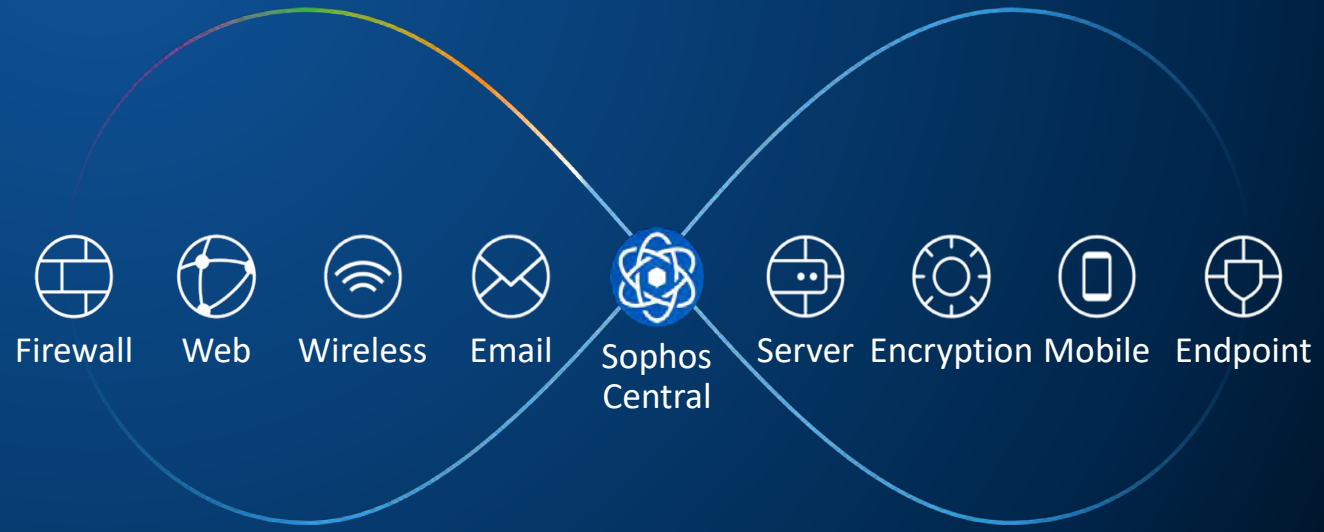
EIN Anbieter für Ihre kompletten IT Security Services

SOPHOS

Sophos im Überblick

- 1985 in Oxford, UK gegründet
- $711 Millionen Umsatz in FY19
- 11% Wachstum/Jahr - vgl. IT-Security-Markt = 7%
- > 3.000 Mitarbeiter, davon ca. 500 in DACH
- 300.000+ Kunden
- 100+ Millionen User
- 39.000+ Channel Partner
- Gartner: Marktführer in den Bereichen Endpoint, Firewall & Verschlüsselung





SOPHOS

Synchronized Security – Der Sophos Vorteil

Admin| Manage All Sophos Products

Self Service | User Customizable Alerts

Partner | Management of Customer Installations

Sophos Central



Cloud Intelligence

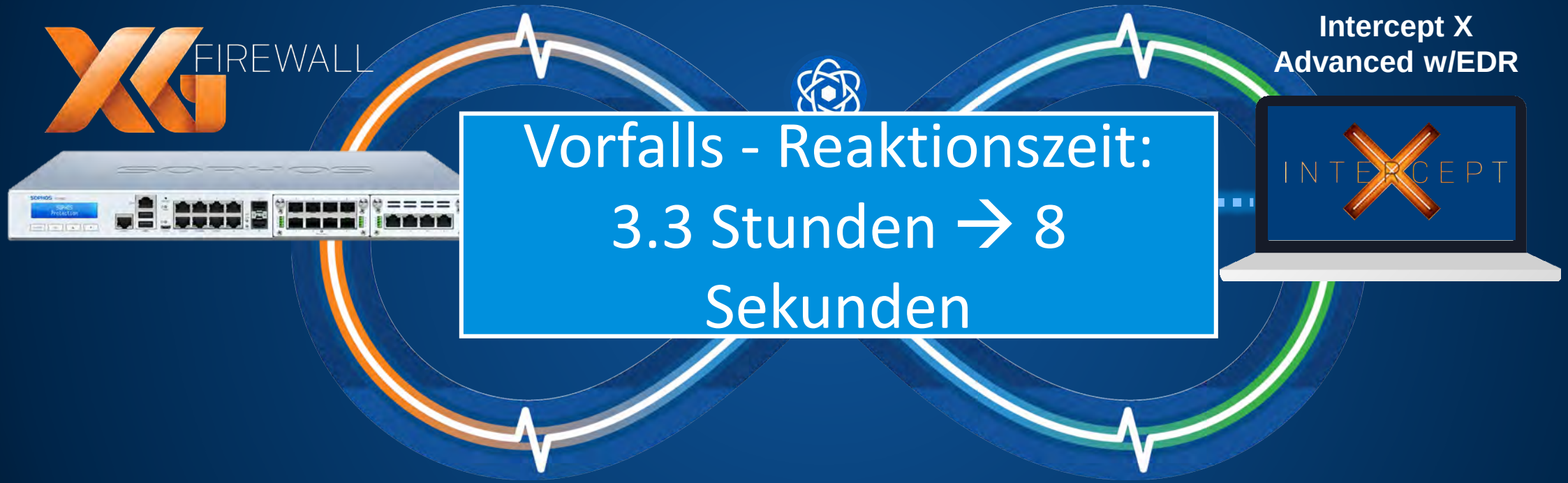
Analytics| Analyze data across all of Sophos' products to create simple, actionable insights and automatic resolutions

Sophos Labs| 24x7x365, multi-continent operation | Malware Identities | URL Database | Machine Learning | Threat Intelligence | Genotypes | Reputation | Behavioral Rules | APT Rules | App Identities | Anti-Spam | DLP | SophosID | Sandboxing | API Everywhere

SOPHOS

Die ultimative Kombination

Für Bedrohungsanalyse und automatisierte Reaktionen



SOFORT
Bedrohungs Identifizierung

100%
App Identifizierung und Kontrolle

AUTO
Bedrohungsreaktion

Sophos Intercept X

Stoppt unbekannte Bedrohungen mit Deep Learning



"One of the ***best performance scores*** we have ever seen in our tests."

Maik Morgenstern, CTO, AV-TEST

Schützt vor Ransomware mit CryptoGuard



"Intercept X is brilliant at ransomware. Since implementation we haven't had one infection."

Aaron Harris, IT Manager, Oxford Metrics Group

Stoppt Hacker durch Exploit Prevention



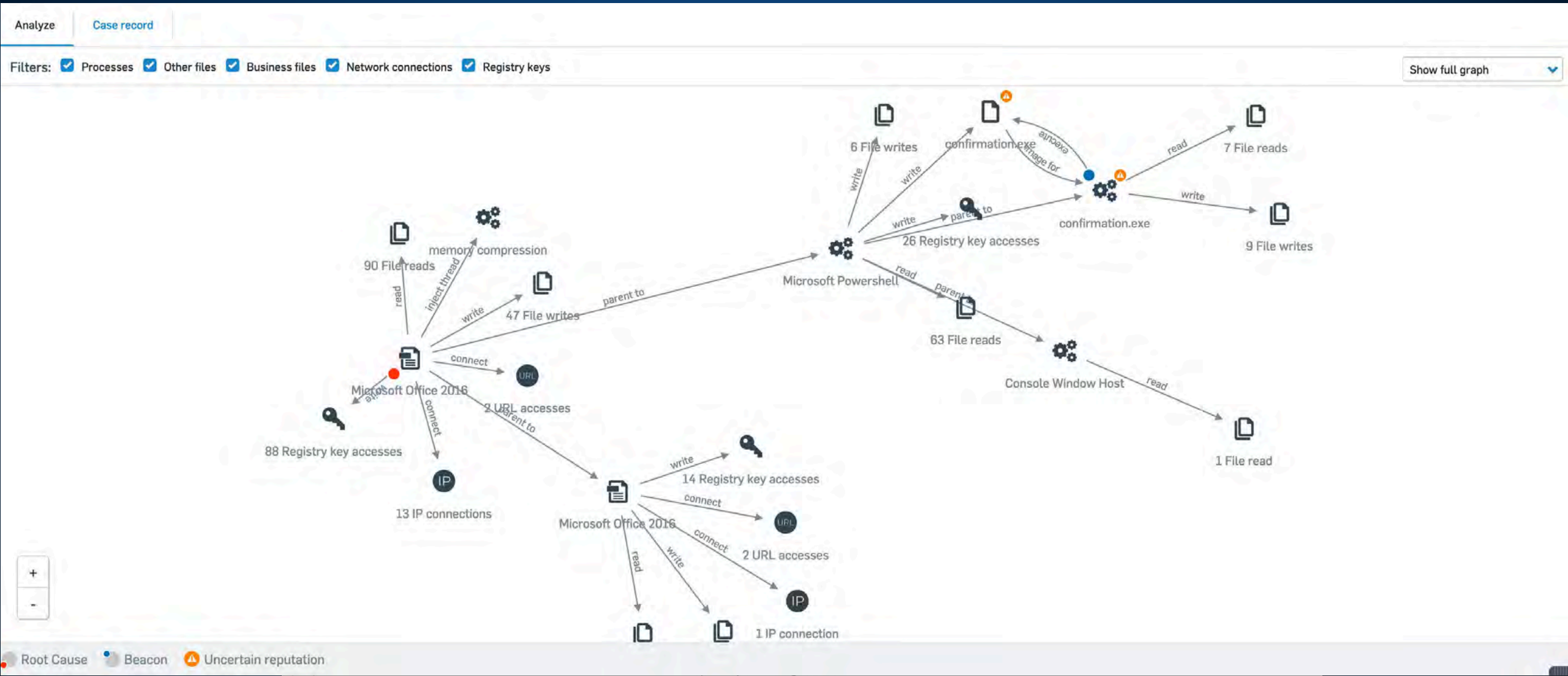
"Based on the exploit and anti-exploit protection tests, Sophos Intercept X performed the best."

MRG Effitas

*Source: The State of Endpoint Security Today Survey
^Based on VirusTotal submissions (12/31/17 – 1/6/18)

Threat Cases

Überblick über das wer, was, wann, wo, warum und wie



1 IP connection
Root Cause
Beacon
Uncertain reputation

SOPHOS

Sophos Intercept X vs. Mitbewerb

SOPHOS Intercept X

Sophos Intercept X is the world's best endpoint protection.

SOPHOS INTERCEPT X 3RD PARTY REVIEWS	
NSS Labs[1]	Ranked #1 security effectiveness, #1 for TCO
SE Labs Enterprise Protection Test[2]	Ranked 1st - 100% total accuracy rating
SE Labs Small Business Protection Test[3]	Ranked 1st - 100% total accuracy rating
MRG Effitas 360 Assessment[4]	100% threat protection, 100% PUA detection w/default settings
MRG Effitas Exploit Protection[5]	Ranked 1st. Missed 1 out of 35 exploits
MRG Effitas Malware Protection[6]	Ranked 1st (99.2% malware detection, 95% PUA detection, 0.05% false positive rate)
AV-Comparatives[7]	Ranked 1st malware protection
AV-Test Windows[8]	"Top Product" (6/6 Protection, 6/6 Usability, 5.5/6 Performance)
AV-Test Mac[9]	Perfect Score (6/6 Protection, 6/6 Usability, 6/6 Performance)
AV-Test Mobile[10]	Perfect Score (6/6 Protection, 6/6 Usability)
PC Magazine[11]	Editor's Choice, Best Ransomware Protection
Gartner 2019 Endpoint Protections Platform Magic Quadrant[12]	11-time Leader, 2019 Leader
Forrester Wave[13]	Leader Since 2013, 2019 Leader
Forrester Now Tech MDR Report[14]	Top Tier (full scale forensics)

NSS Labs RECOMMENDED · SE Labs BEST Small Business Endpoint WINNER 2019 · MRG Effitas EFFICACY ASSESSMENT & ASSURANCE · AV comparatives · AV-TEST The Independent IT-Security Institute · Gartner · FORRESTER®

Source:
[1] NSS Labs 2019 Advanced Endpoint Protection (AEP) Security Value Map
[2] SE Labs Enterprise Endpoint Protection, July - Sept 2019
[3] SE Labs Small Business Endpoint Protection, July - Sept 2019
[4] MRG Effitas 360 Degree Assessment & Certification, Q2 2019
[5] MRG Effitas Exploit Protection Assessment
[6] MRG Effitas Comparative Malware Protection Assessment
[7] AV-Comparatives Factsheet Business Test (March-April 2019)
[8] AV-Test Windows 10: April 2019
[9] AV-Test MacOS Mojave: June 2019
[10] AV-Test Android May 2019
[11] PC Magazine 2019 Best Ransomware Protection for Businesses
[12] Gartner 2019 Endpoint Protection Platforms Magic Quadrant
[13] Forrester Wave: Endpoint Security, Q3 2019
[14] Forrester Now Tech: Managed Detection and Response (MDR) Services, Q2 2018

SE Labs BEST Small Business Endpoint WINNER 2019 · SE Labs AAA ENTERPRISE ENDPOINT PROTECTION JUL-SEP 2019 · SE Labs AAA SMALL BUSINESS ENDPOINT PROTECTION JUL-SEP 2019

- Awarded Best Small Business Endpoint: 2019 Annual Report
- AAA Rated by SE Labs since April 2018
- Sophos achieved a 100% Total Accuracy Rating from SE Labs for enterprise endpoint protection
- Sophos achieved a 100% Total Accuracy Rating from SE Labs for small business endpoint protection
- "Sophos Intercept X Advanced blocked all of the public and targeted attacks." – SE Labs

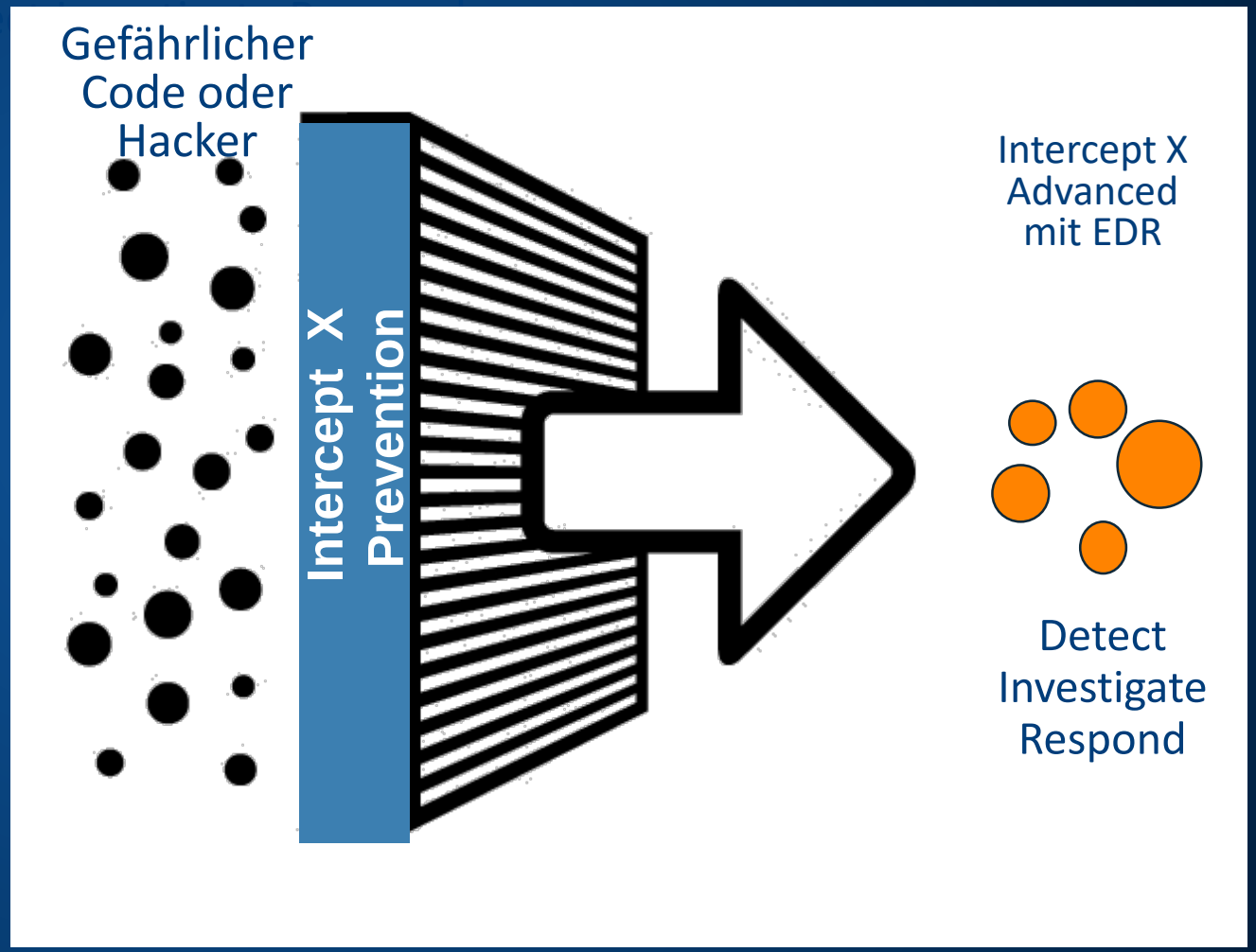
TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Sophos Intercept X	1,136	100%	AAA
Kaspersky Endpoint Security	1,135	100%	AAA
McAfee EndPoint Security	1,135	100%	AAA
Symantec Endpoint Security Enterprise Edition	1,134	100%	AAA
Microsoft Windows Defender ATP's Antivirus	1,126	99%	AAA
ESET Endpoint Security	1,123	99%	AAA
Crowdstrike Falcon	1,120	99%	AAA
Trend Micro OfficeScan, Intrusion Defense Firewall	1,117	98%	AAA
Bitdefender Gravity Zone Endpoint Security	1,098	97%	AAA
VIPRE Endpoint Security	1,088	96%	AAA

Source: SE Labs SMB Endpoint Protection Test July– September 2019


INTERCEPT X
NOW WITH EDR
THE BEST JUST GOT BETTER

Stopt Angriffe bevor Sie starten

- Verringert die Angriffsfläche
- Verringert wesentlich den EDR Arbeitsaufwand
- Optimiert Resourcen
- Reduziert das Grundrauschen



Ergänzen Sie Wissen, aber keine Mitarbeiter

Die erste Detection and Response Lösung für IT Generalisten



Security Analyst

Aufspüren und priorisieren von verdächtigen Events



Malware Analyst

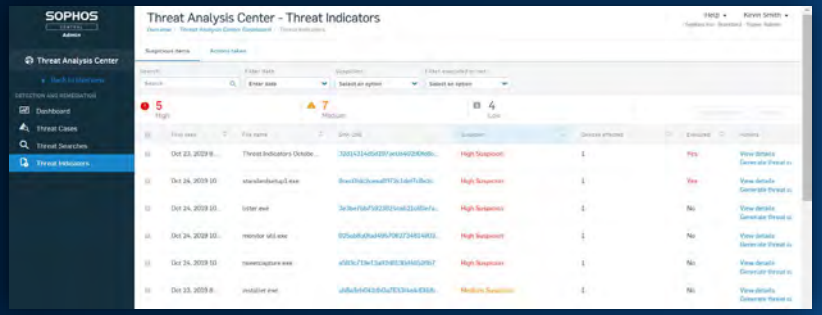
Reverse Engineering von verdächtigen Dateien



Threat Intelligence Analyst

Intergrieren und Interpretieren von Bedrohungs Feeds

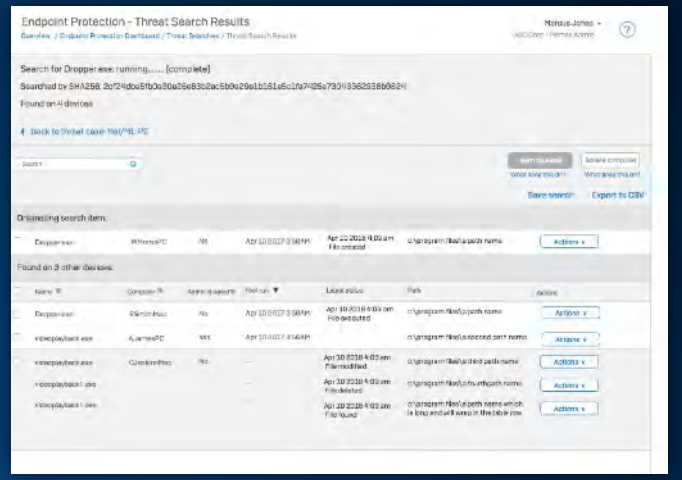
Ein Tag im Leben das Analysts



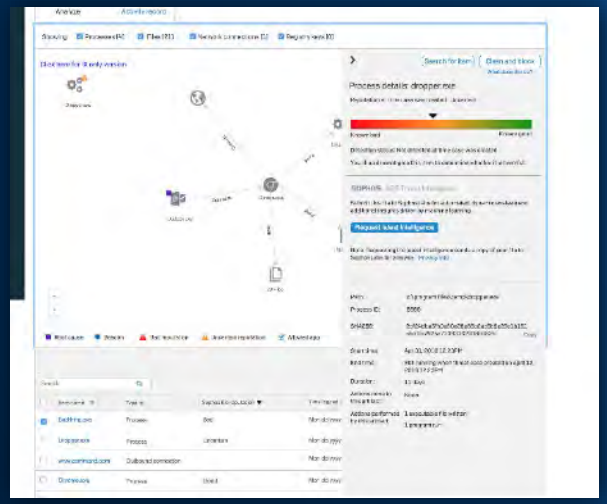
Identifiziert “Dropper.exe” als top Vorfall via “Bedrohungsindikatoren”



Erkennt, dass Dropper.exe malware verteilt hat (welche geblockt wurde)



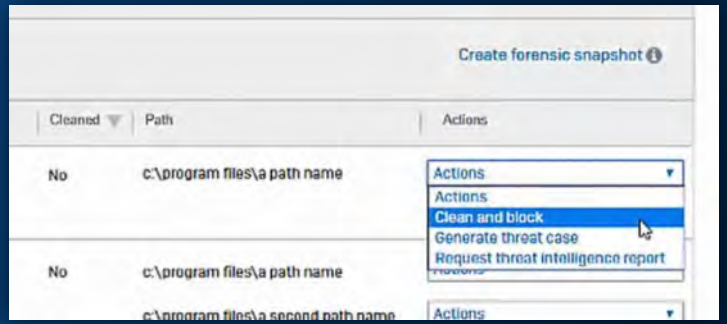
Bestimmt, wo Dropper.exe sonst noch existiert



Fordert weitere Details von SophosLabs an



Nutzt Deep Learning um festzustellen, dass die File böswillig ist



Entfernt Bedrohung per “Clean and block”

SOPHOS

*Coming in 2019

SOPHOS

Managed Threat Response

Sophos MTR fuses machine learning technology and expert-led analysis to take targeted actions against even the most sophisticated threats.

ENDPOINT DETECTION AND RESPONSE TOOLS

1. Intercept X with EDR Monitors for Threats
2. Machine Learning Prioritizes Suspicious Activities
3. Confirmed Malicious Activities are Automatically Terminated

HUMAN THREAT HUNTERS AND RESPONSE EXPERTS

4. Human Analysts Investigate Suspicious Events
5. Threat Hunts are Conducted to Find New Threats
6. Response Experts Take Action to Neutralize Threats

©Copyright 2019. Sophos Ltd. All rights reserved.

SOPHOS

Sophos Central Device Encryption



Setup und Installation mit wenigen Klicks

- *Einfache Lösung, um Windows BitLocker und macOS FileVault Festplatten Verschlüsselung zu verwalten*
- *Geteilter Agent mit Sophos Endpoint*
- *Keine zusätzliche Installation notwendig*



Sophos Mobile

Unified Endpoint Management

Standard

DEVICES

- iOS, Android, Win10, macOS
- Configuration and policies
- Inventory and asset management
- Reporting

APPS

- Install, remove, view apps
- Enterprise app store
- App control
- Whitelist/blacklist

Advanced

CONTENT

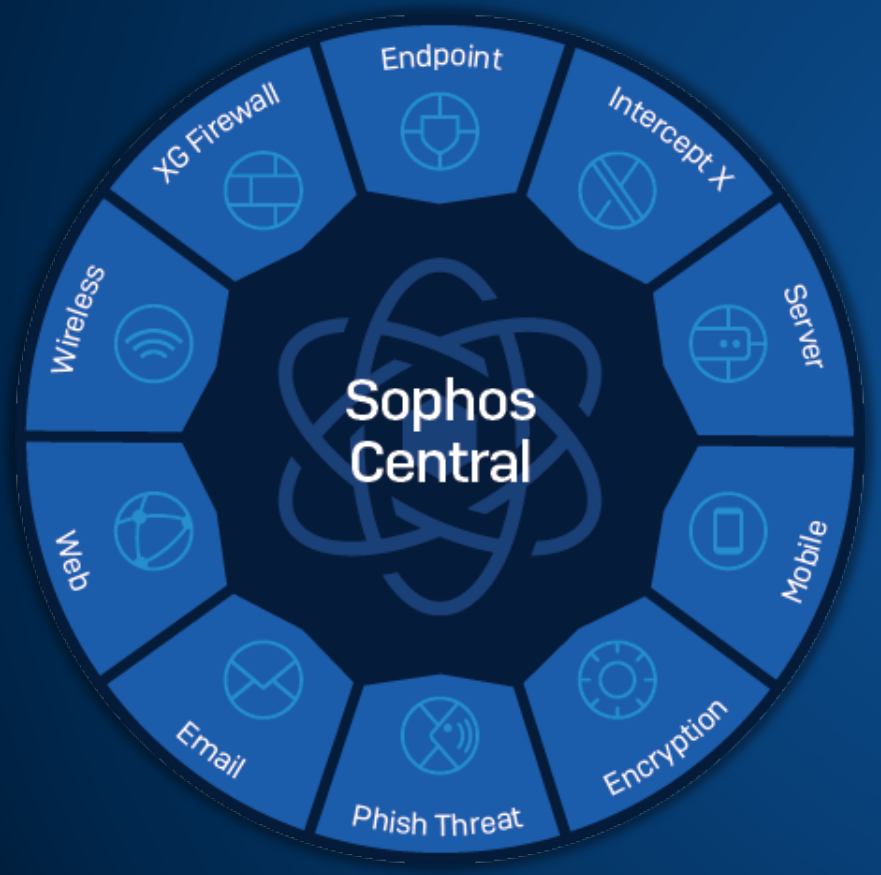
- Email and document container
- Publish content
- Container-only Management
- Native OS containerization

SECURITY

- Compliance rules and remediation
- Deep Learning Malware & ransomware detection, PUA detection
- Anti-phishing, Web protection, web filtering, MiTM detection

Phish Threat Highlights

Macht Phishing Simulationen und Security Training einfach



#1

Nutzungsbasiert abgerechnet

Only pay monthly subscription when you send a campaign

#2

Keine Grenzen

Freedom to run unlimited campaigns

#3

500+ Vorlagen

Customizable attacks fed by latest threat intelligence

#4

60+ Kurse

Range of training covering security and compliance

#5

Komplettes Reporting

Measure success by organization, group or individual

#6

Sophos Central

One console, full cybersecurity portfolio

SOPHOS

Intercept X

For Server with EDR

Server sind die wichtigsten Endpoints

Ransomware	• Höhere Kosten , wenn Server verschlüsselt werden
CryptoMining	• Server Farmen und Clouds haben den höchsten Wert für CryptoJacking
Server Exploits	• Größerer Schaden durch Diebstahl persönlicher Daten, privilege escalation, or code cave
Data Exfiltration	• Organisationsweite proprietäre Daten führen zu größerem Schaden

Automatisierte Bedrohungsanalyse und Antwort

Endpoint Detection and Response (EDR)

- Aktives aufspüren von beweglichen Bedrohungen
- Verständis für das Ausmaß des Security Vorfalls



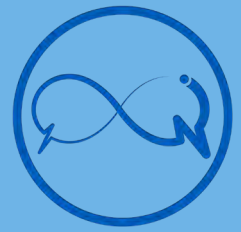
Erkennen und sichern von cloud workloads

- Erkennen Sie cloud workloads (AWS/Azure)
- Erhalten Sie Einblicke in und schützen Sie diese (AWS/Azure/Google)



Synchronized Application Control *(mit XG Firewall)*

- 100% Sichtbarkeit von auf Servern ausgeführten Applikationen
- Hindern sie unbekannte Apps an der Kommunikation nach aussen



Kontrolle über Ihre Server

Server Lockdown

Schützt die Konfiguration Ihrer Server mit einem Klickbutton

File Integrity Monitoring (FIM)

Identifiziert jede unauthorisierte Veränderung von kritischen Dateien

Powerful Policies, Easy Deployment

Schnell aufgesetzt und Policies können auch in gemischten Umgebungen ausgerollt werden

Public Cloud Security Vorfälle

In 2020 werden

95%

der Cloud Security Fehler durch Fehler des Kunden ausgelöst

Source: Gartner, Clouds Are Secure: Are You Using Them Securely? by Jay Heiser

6 Millionen PII Aufzeichnungen

Telecommunications company

200k Gesprächsaufzeichnungen Zugänglich

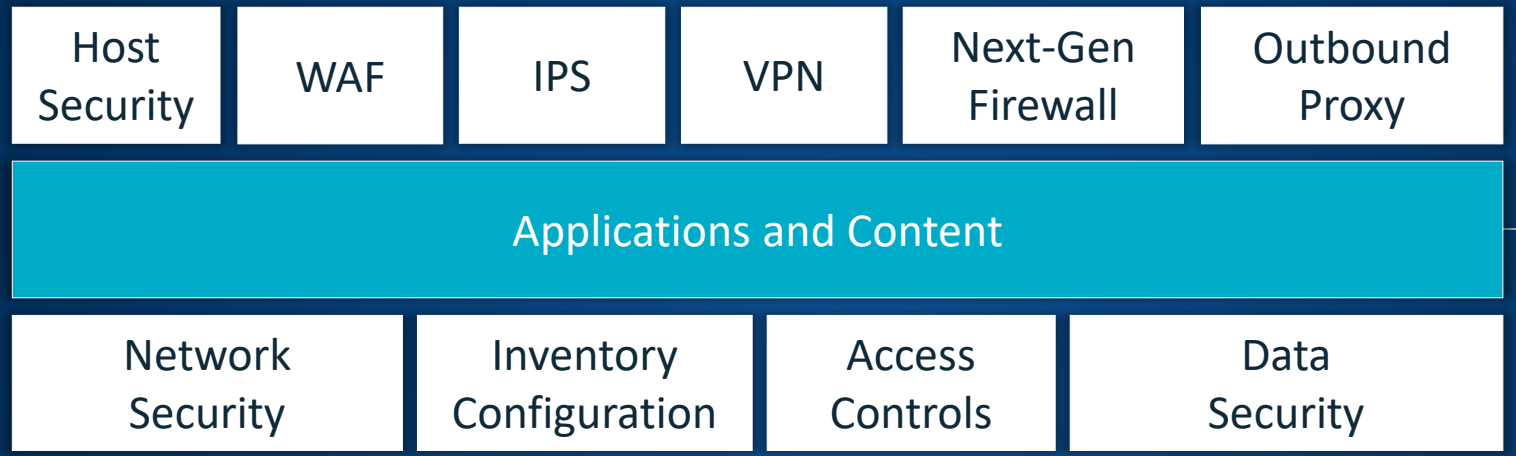
Holiday booking service

20K Kunden Datensätze

Large discount brokerage firm

Cloud Security ist eine geteilte Verantwortung

Security **IN** der Cloud



Ihre Verwantwortung als MSP

Security **aus** der Cloud



Cloud Provider Verantwortung
AWS, Azure, Google

Public Cloud Sichtbarkeit und Bedrohungsreaktion

Cloud Optix

- Identifizieren, beantworten und verhindern Sie Cloud Security und Compliance Lücken
- Sichern Sie AWS, Microsoft Azure, und Google Cloud





AI Powered Security Analytics and Monitoring



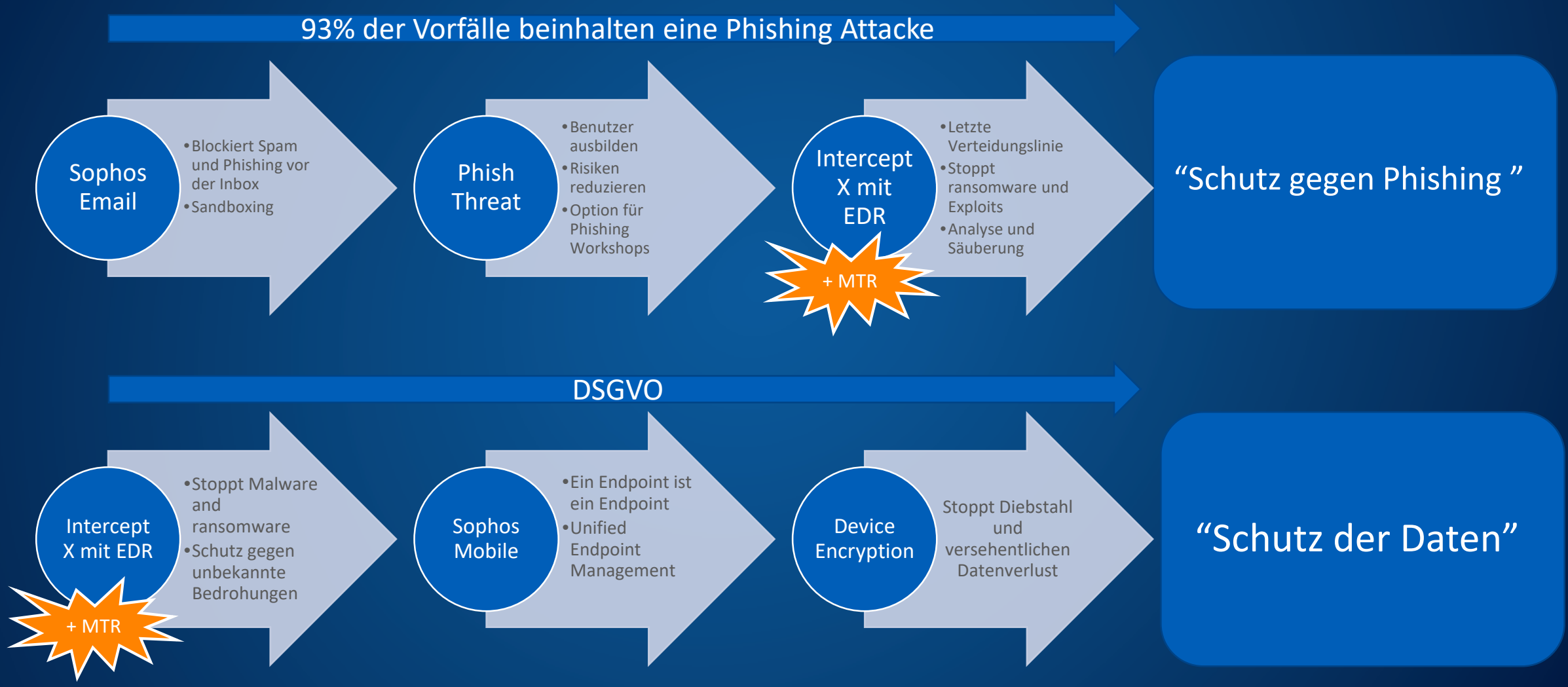
Governance, Risk and Compliance



Secure DevOps

Beispiel Service Pakete Sophos

Erstellen Sie next Gen Managed Security Services



XG – Firewall as a Service

- HaaS -> MSP besitzt die FW und vermietet die Appliance
- Amortisierung durch Mindestvertragslaufzeit
- Durch OPEX Modell können KMU Kunden gewonnen werden



Beispiel – FWaaS

- XG 125 Firewall HW – bis zu. ca. ~ 20 User mit Enterprise Guard (Network & Web Protection)
- MSRP 795,- / Partner Rabatt “authorized” Level : 25% -> XG Partner Preis = 596,25 Euro

MSP

Kosten für HaaS : 49,69 pro Monat
Kosten XG Lizenz : 49,59 pro Monat
Enterprise Guard (Network Protection, Web Protection und Enhanced Support)
Kosten Managed Service für die FW: 50,- (fiktiv)
Installation, Monitoring, Patch Management, LvL 1 S.

199,- VK
Jahr 1: 137,22 Kosten
31% Marge *
Ab Jahr 2: 87,53 Kosten
56% Marge *

Kunde

FWaaS inkl. Hardware: 199,- Euro pro Monat (keine Einzelpreise ausweisen!)
Bei 12 Monaten Mindesvertragslaufzeit

SOPHOS

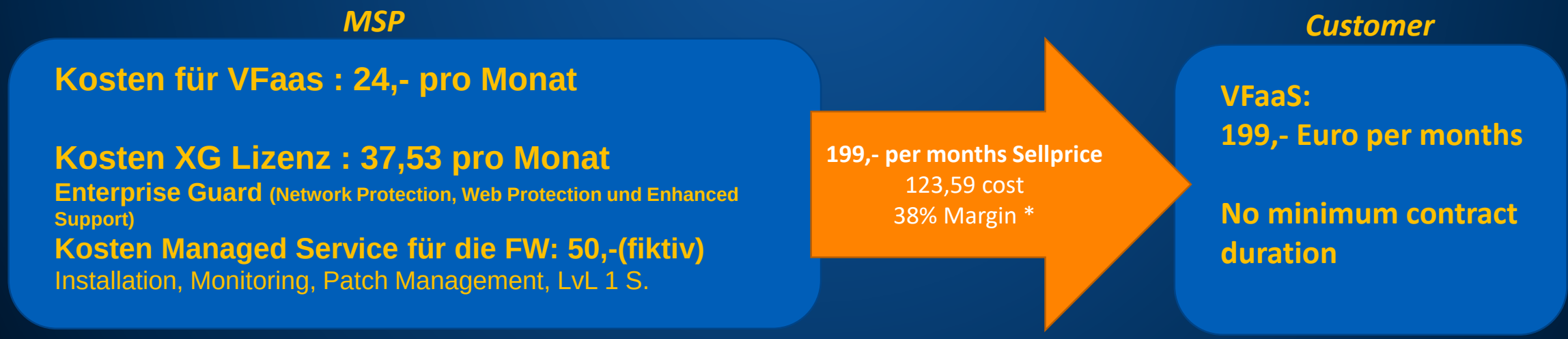
* Marge steigt durch besseres Preisband über Zeit

XG – Virtual Firewall as a Service

- Hoster & Cloud Provider betreibt virtuelle XG im Rechenzentrum
- Syncronize Security als Service Differentiator (second layer firewall <-> Server)
- Komplettes OPEX Model, einfach zu skalierendes Geschäftsmodell

Beispiel – VFaaS

- 1 Core 4GB Ram XG virtual Firewall -> bis zu ~20 User mit Enterprise Guard (Network & Web Protection)



SOPHOS

* Marge steigt durch besseres Preisband über Zeit

Hersteller Management vereinfachen – Kosten einsparen

SONICWALL

cisco Meraki

intel Security

UMBRELLA by OpenDNS

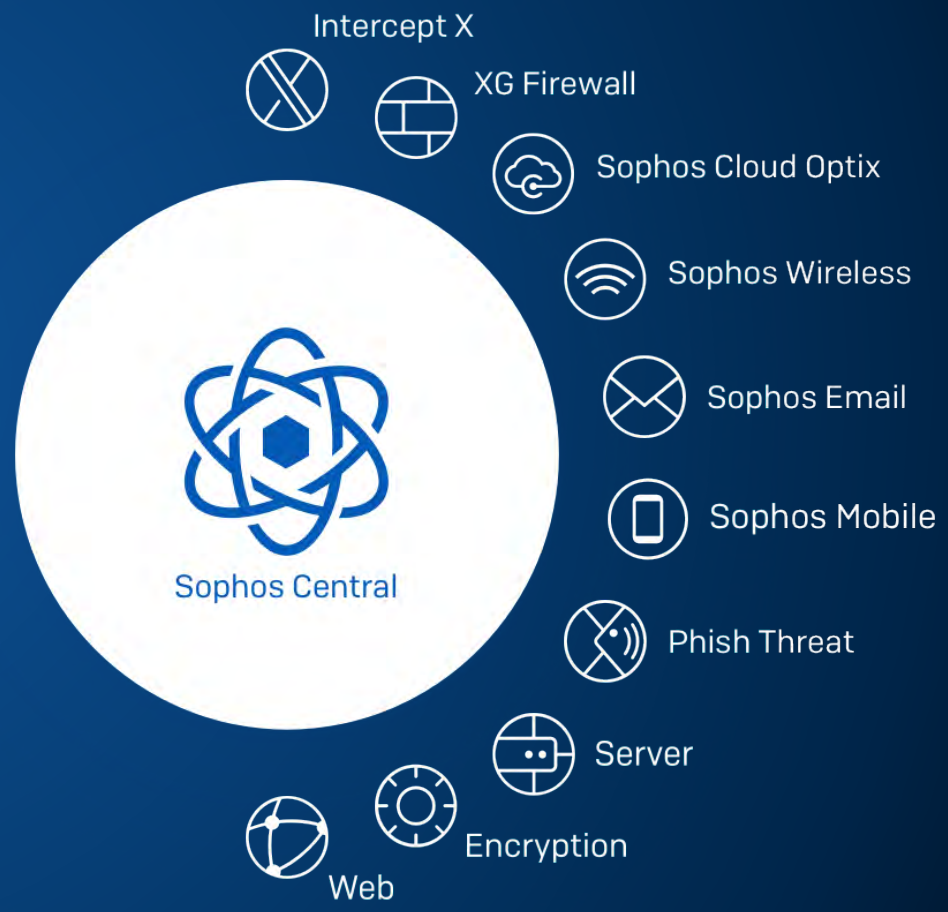
SOPHOS

MaaS360 by Fiberlink, an IBM company

WEBROOT

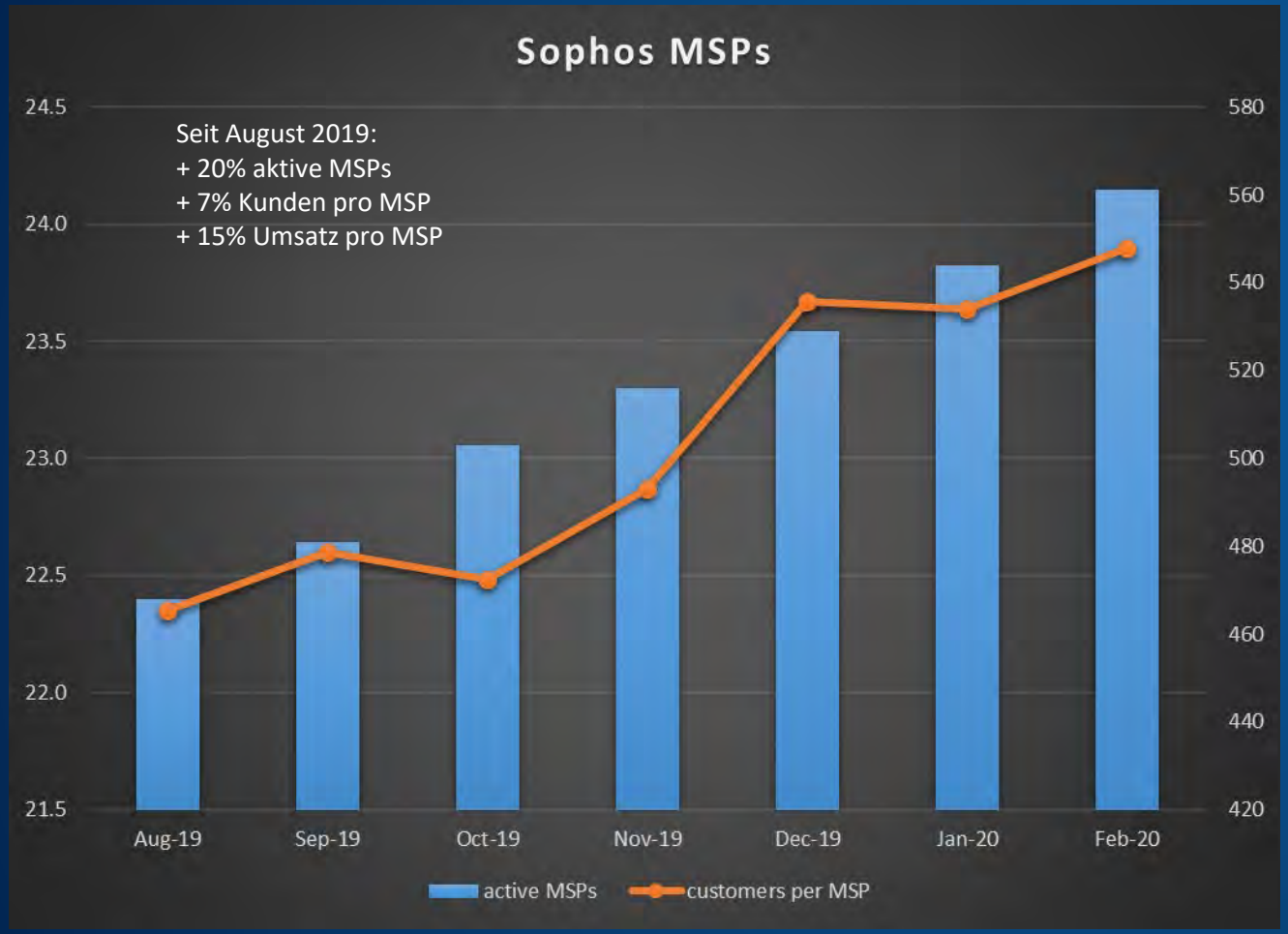
Greenfield





Sophos MSP Connect Program

Stark wachsende Partnerbasis in DACH:



Vorteile als Sophos MSP:

- **Bessere Kontrolle** durch eine einfache, integrierte Sicherheitslösung
- **Höhere Transparenz** durch Cloudbasierte Verwaltung mit Sophos Central
- **Flexibilität** durch nutzungsbasierte, monatliche Abrechung -> pay as you go
- **Erstklassige Security Produkte:** Endpoint(next gen), Mobile, Device Encryption, Server, XG Firewalls, Wireless, Web & Email Gateways

SOPHOS

Klare Ausrichtung auf das Geschäftsergebnis des MSPs



Steigerung des Umsatzes

- Möglichkeit zum Verkauf ergänzender oder höherwertiger Sicherheitsdienstleistungen
- Erweiterung des Angebotsportfolios des MSP
- Erhöhung der Profitabilität durch aggregierte Abrechnung



Senkung der Kosten

- Reduzierung von Zeit und Ressourcen für Vendor Management
- Wandel von Investitionskosten zu Betriebskosten



Effizienzoptimierung der betrieblichen Abläufe

- Integration in das Ökosystem des MSP
- EINE Dashboard-Anzeige ermöglicht die Steuerung der Sicherheit von Endgeräten und Netzwerk
- Bedarfsgerechte Konfiguration ermöglicht gezieltes Hinzufügen von Kunden

Steigerung Ihrer Umsätze – Wie unsere erfolgreichsten MSPs

Die 20 größten MSPs in DACH

nutzen 6.1 verschiedene Sophos Produkte

50%
nutzen Endpoint und Netzwerk Security
-> syncronized security

Steigern Ihren monatlichen Umsatz um 5-10% pro Monat

MSP - Erfolgsgeschichten

StarCom-Bauer GmbH



Luithle + Luithle IT-Services



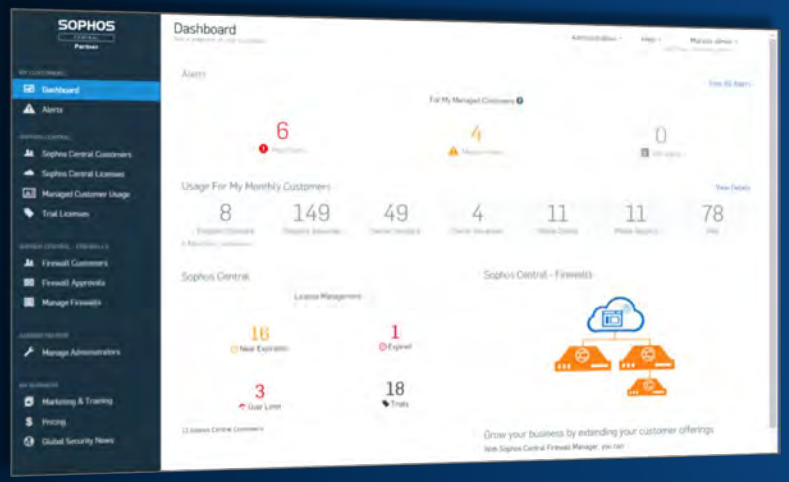
EFFIZIENZ + **PRODUKTIVITÄT** + **PROFITABILITÄT**

Einfache MSP Kundenverwaltung mit Sophos Central

SOPHOS

Sophos Central

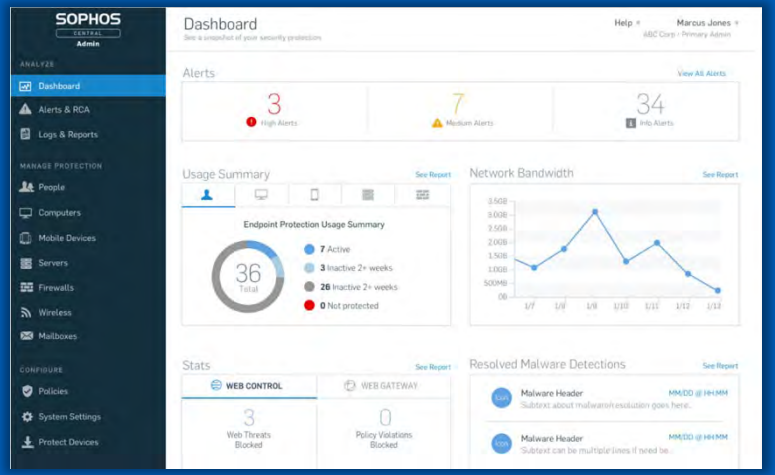
Partner Dashboard



Verwaltung aller Kunden

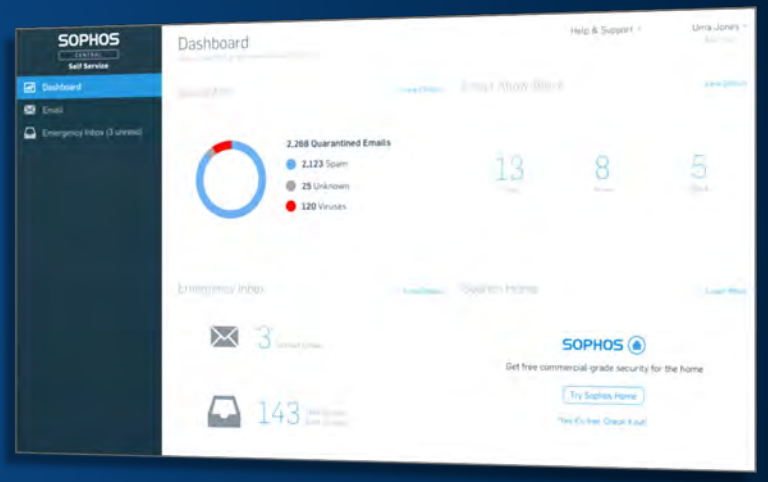
- Lizenzen
- Administration
- Trials
- Sicherheitsereignisse
- MSP

Admin



- Endpoint
- Mobile
- Server
- Verschlüsselung
- Wireless
- Web Gateway
- Email Security
- Firewall

Self Service



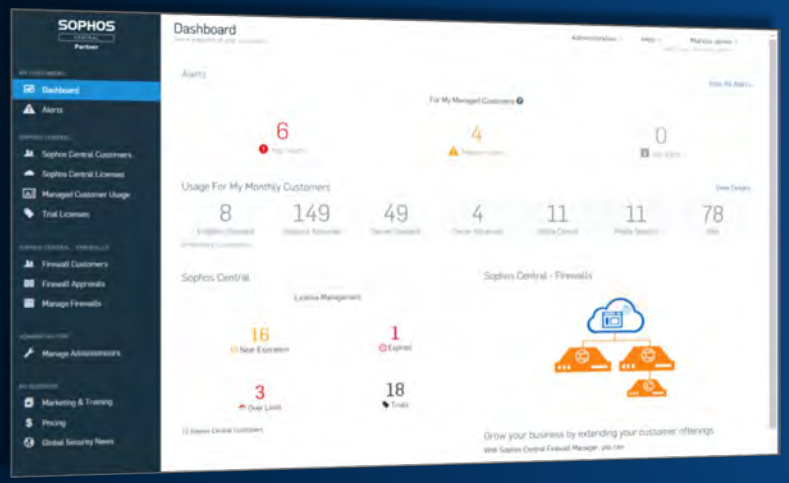
Benutzer-Zugriff

- Email-Quarantäne
- Verschlüsselungs-Recovery
- BYOD Mobilgeräte
- Notfall-Inbox

SOPHOS

Sophos Central Partner Dashboard - Highlights

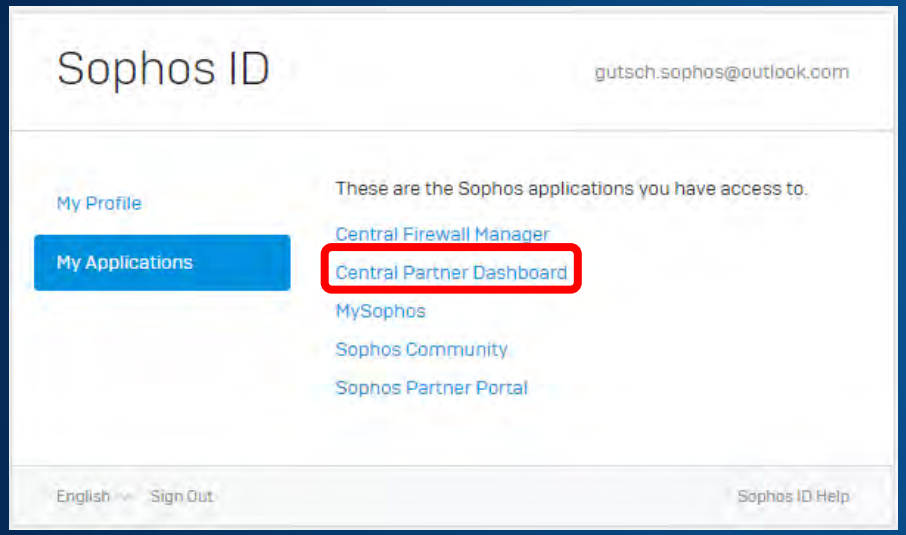
Optimiert für MSPs – Automatisierung und Kundenverwaltung



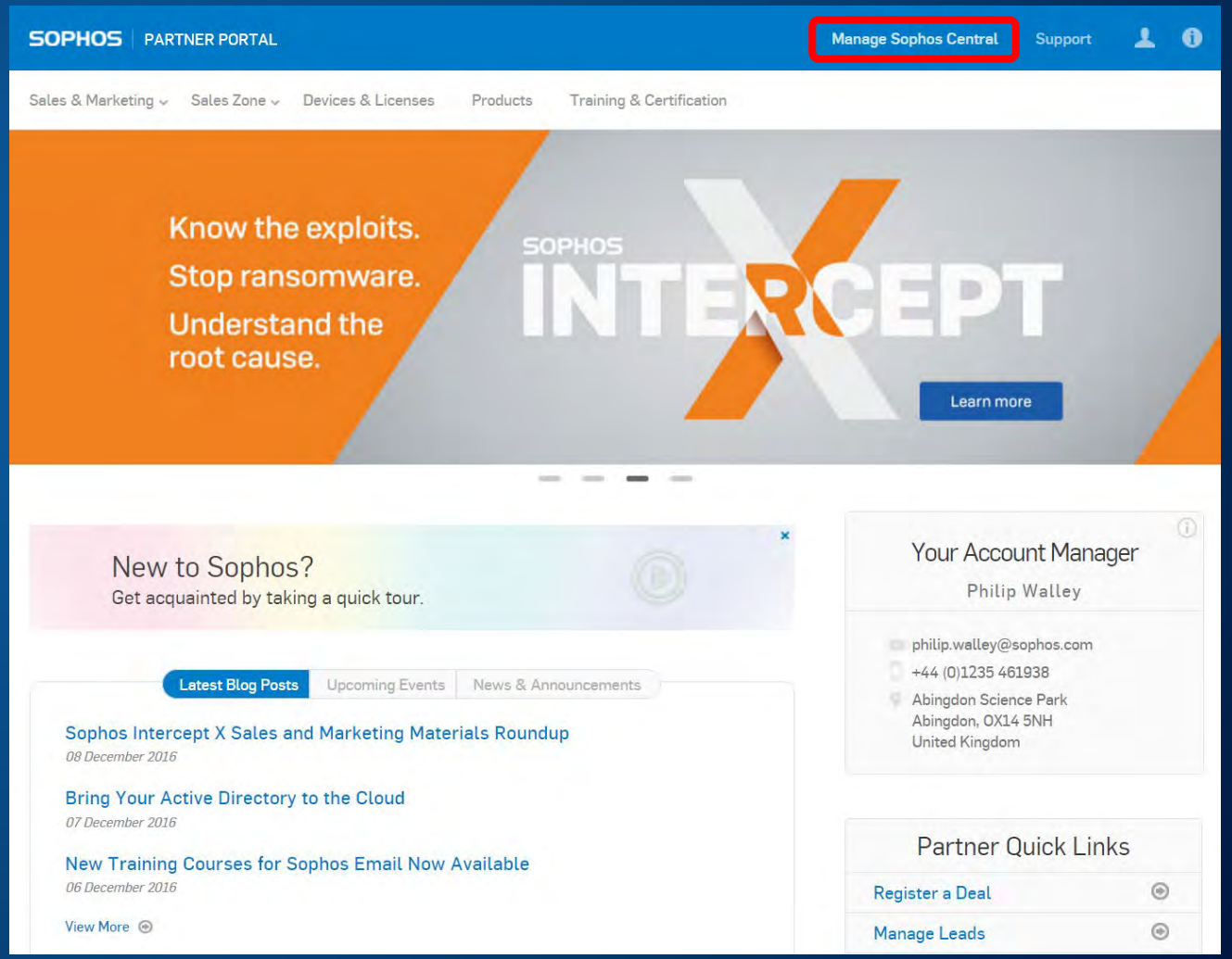
- **Cloud basiertes MSP Management** -> keine eigenen Management Server notwendig
- **Flexible Nutzerrollen mit 2FA** -> Abbildung Ihrer Teams im Partner Dashboard mit sicherem Login
- **Monatliche Kunden erstellen** in wenigen Sekunden
- **Einfacher Überblick über die Kundenbasis** -> Lizenzierung und Nutzungsdaten
- **Globale Vorlagen** -> Vorlagen auf mehrere Kunden gleichzeitig anwenden
- **Flexible Alarm Benachrichtigungen per Email** -> Stellen Sie Häufigkeit, Filterung (nach Priorität, Produkt, Typ). Rest API verfügbar für eine Integration in SIEM/RMM
- **XG Firewall Verwaltung** -> einfach zu verwalten in Sophos Central
- **Effizientes deployment** -> Scripte für die gängigen RMM stehen zur Verfügung (Datto, Kaseya, ServerEye, Connectwise Automate)
- **Native PSA Integration** mit Connectwise und Autotask (Nutzungsdaten)
- **APIs** für Provisionierung, Monitoring und Management

Management Dashboard - Login

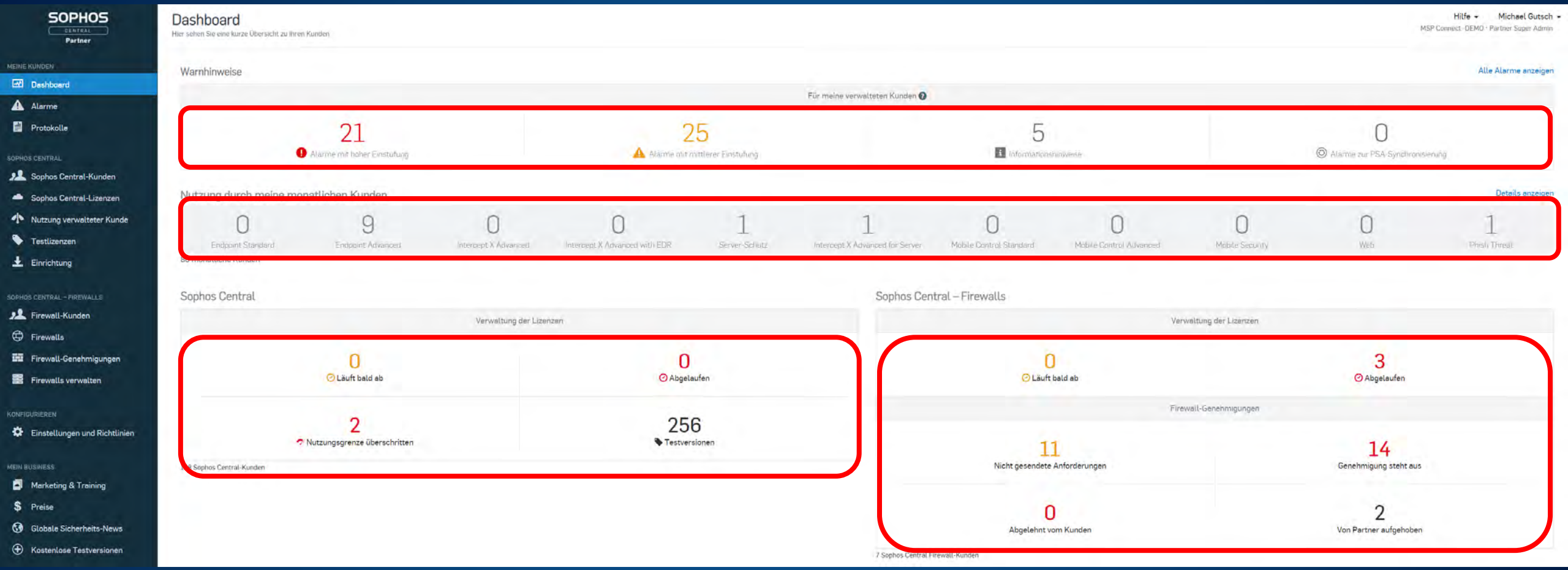
https://id.sophos.com



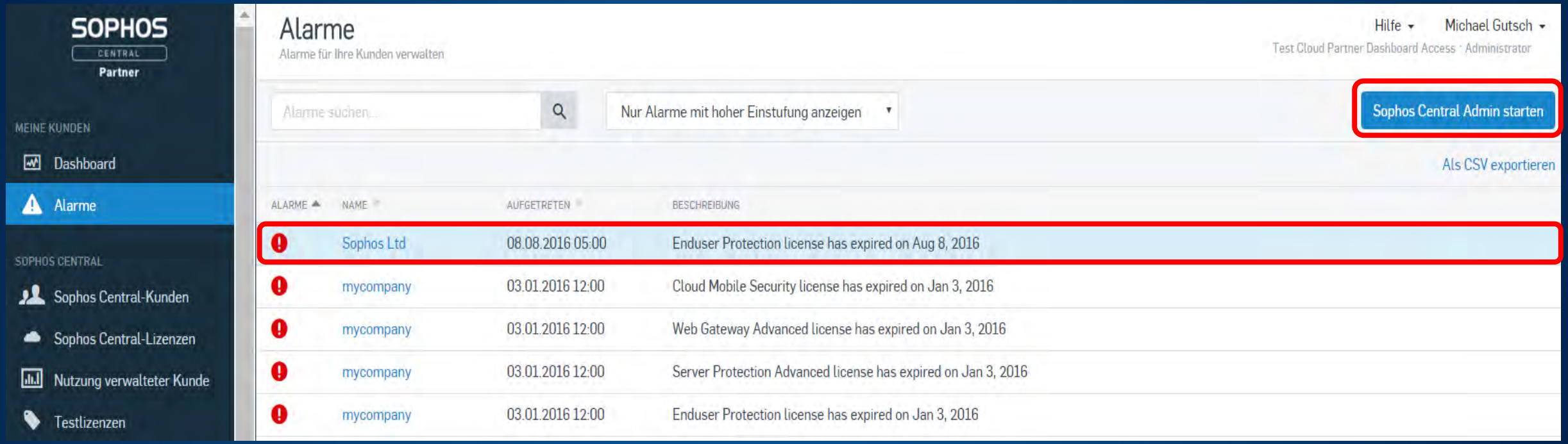
https://partnerportal.sophos.com/



Management Dashboard



Alarme für verwaltete Kunden

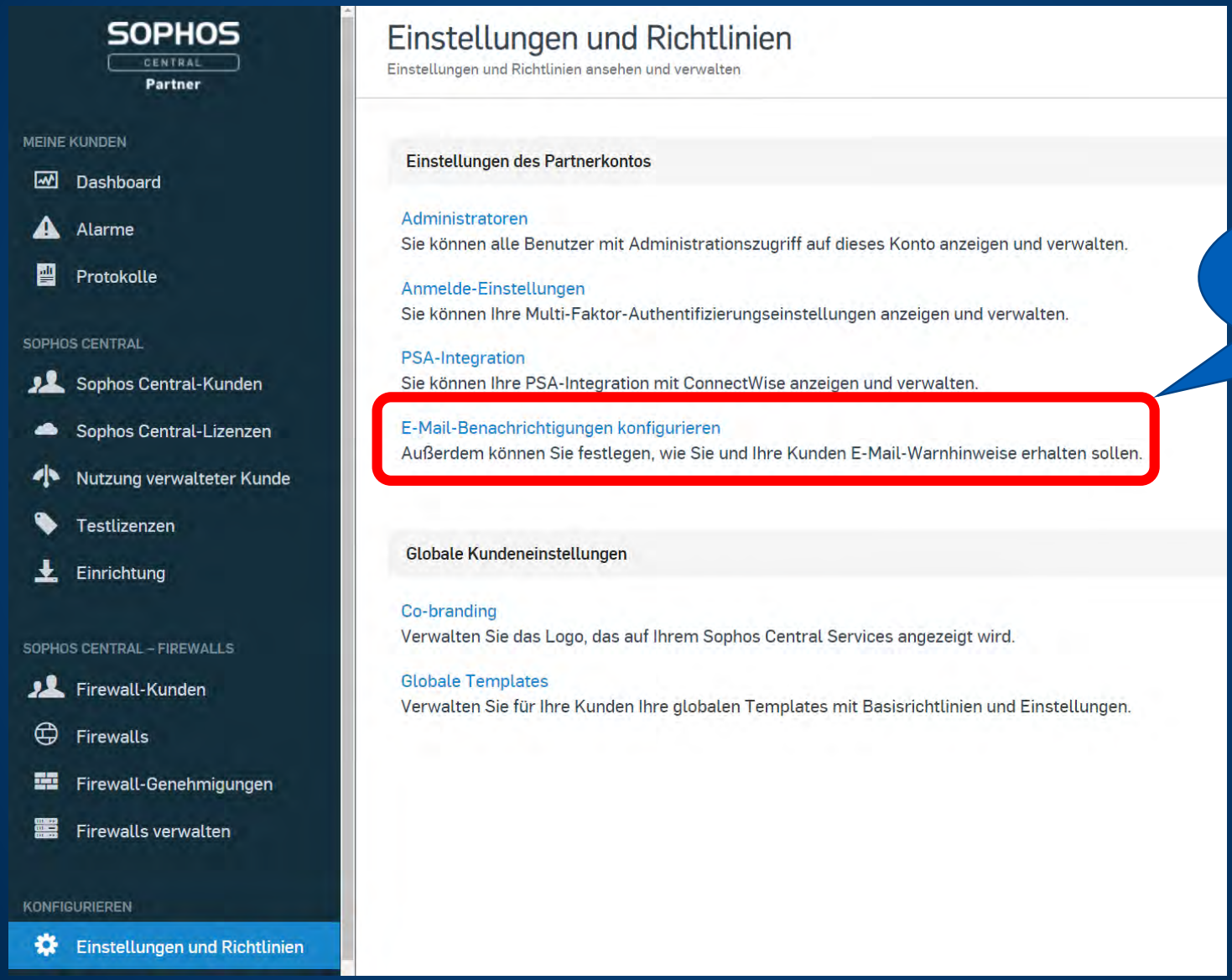


Email Benachrichtigungen



- Alarme können gefiltert werden -> Sie erhalten nur Alarme, die für Sie wichtig sind
- Ausnahmen wo Sie gebraucht werden
- Unterschiedliche Benachrichtigungen pro Team für Produkte, die relevant sind
- Steuerbar für alle Kunden via Partner Dashboard

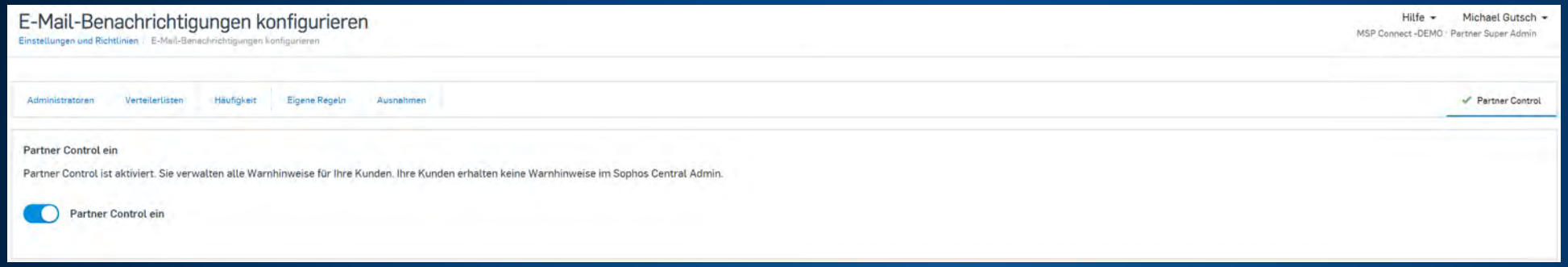
Einstellungen und Richtlinien

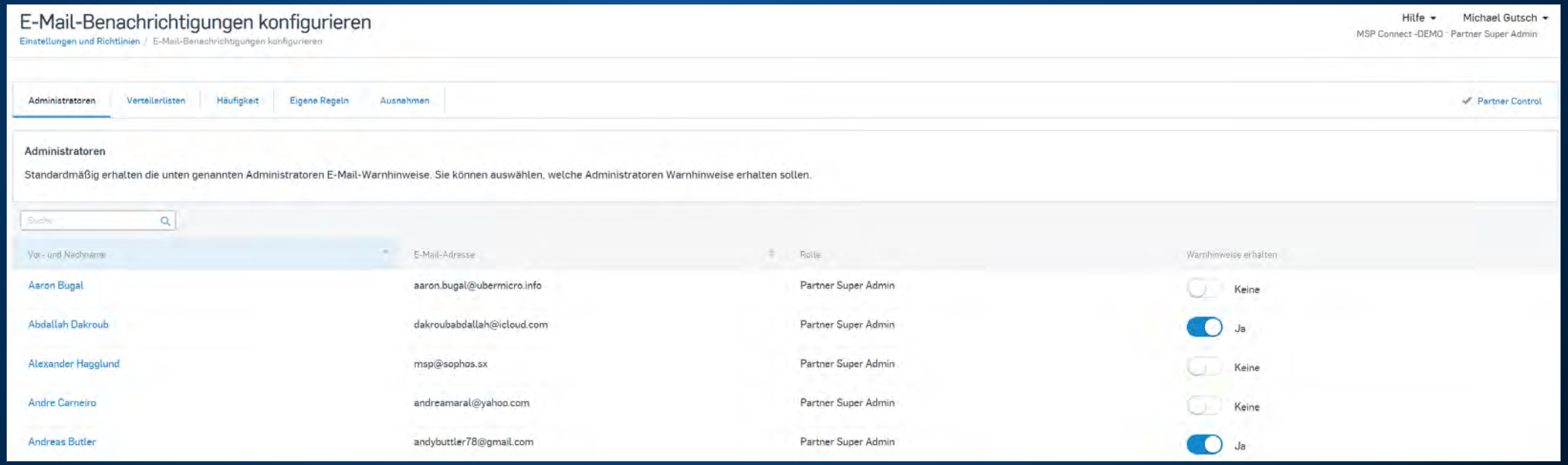


Alarm
Benachrichtigungen

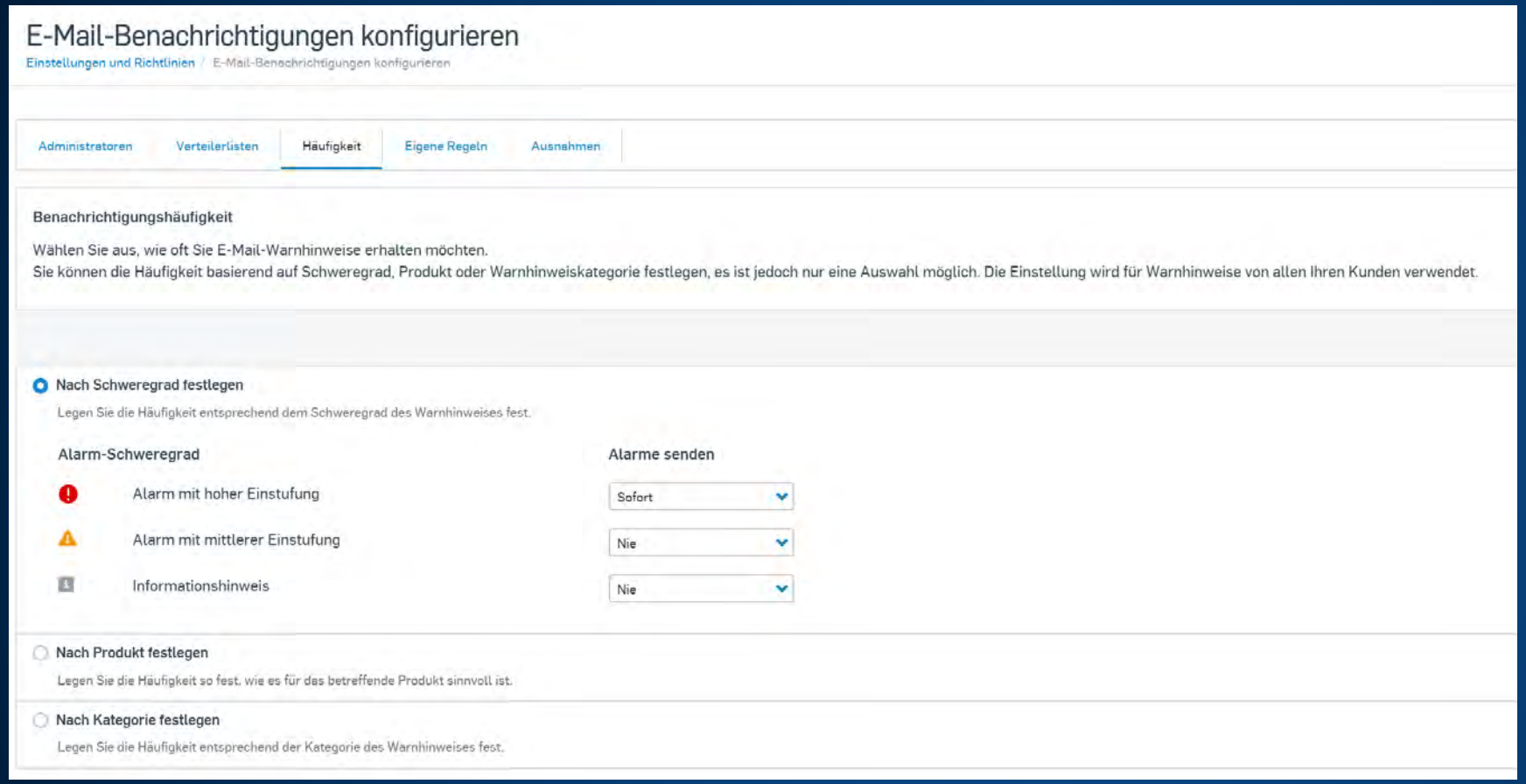
Alarm Benachrichtigungen steuern

Partner Dashboard: Kontrolle über alle Kunden Alarme





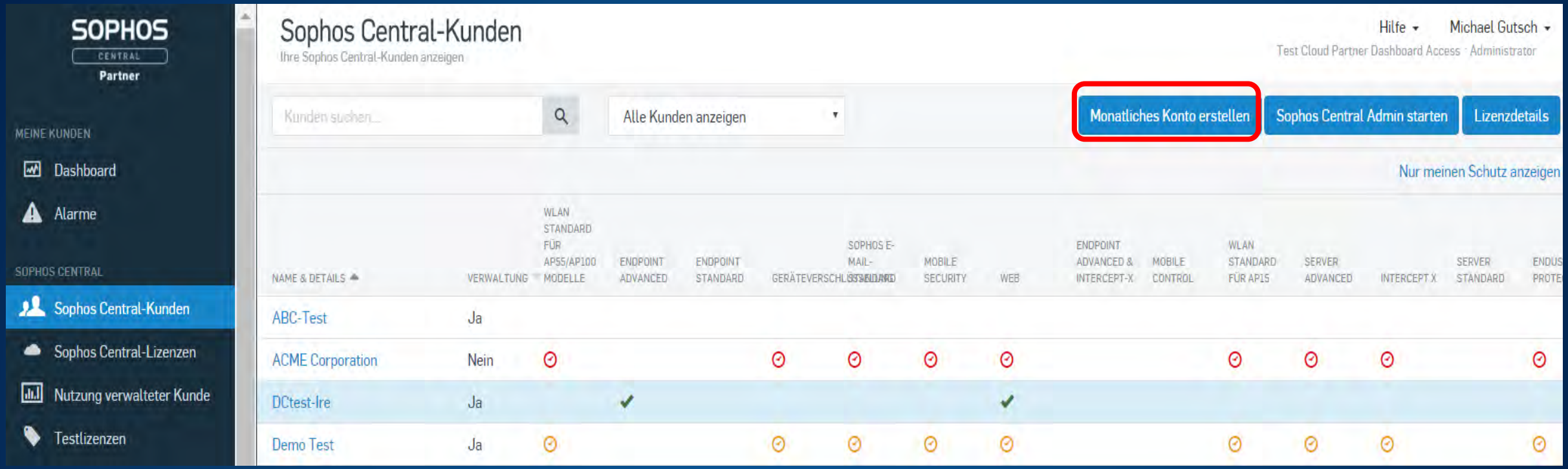
Alarm Benachrichtigungen steuern



Sie steuern genau, welche Alarme Sie erhalten:

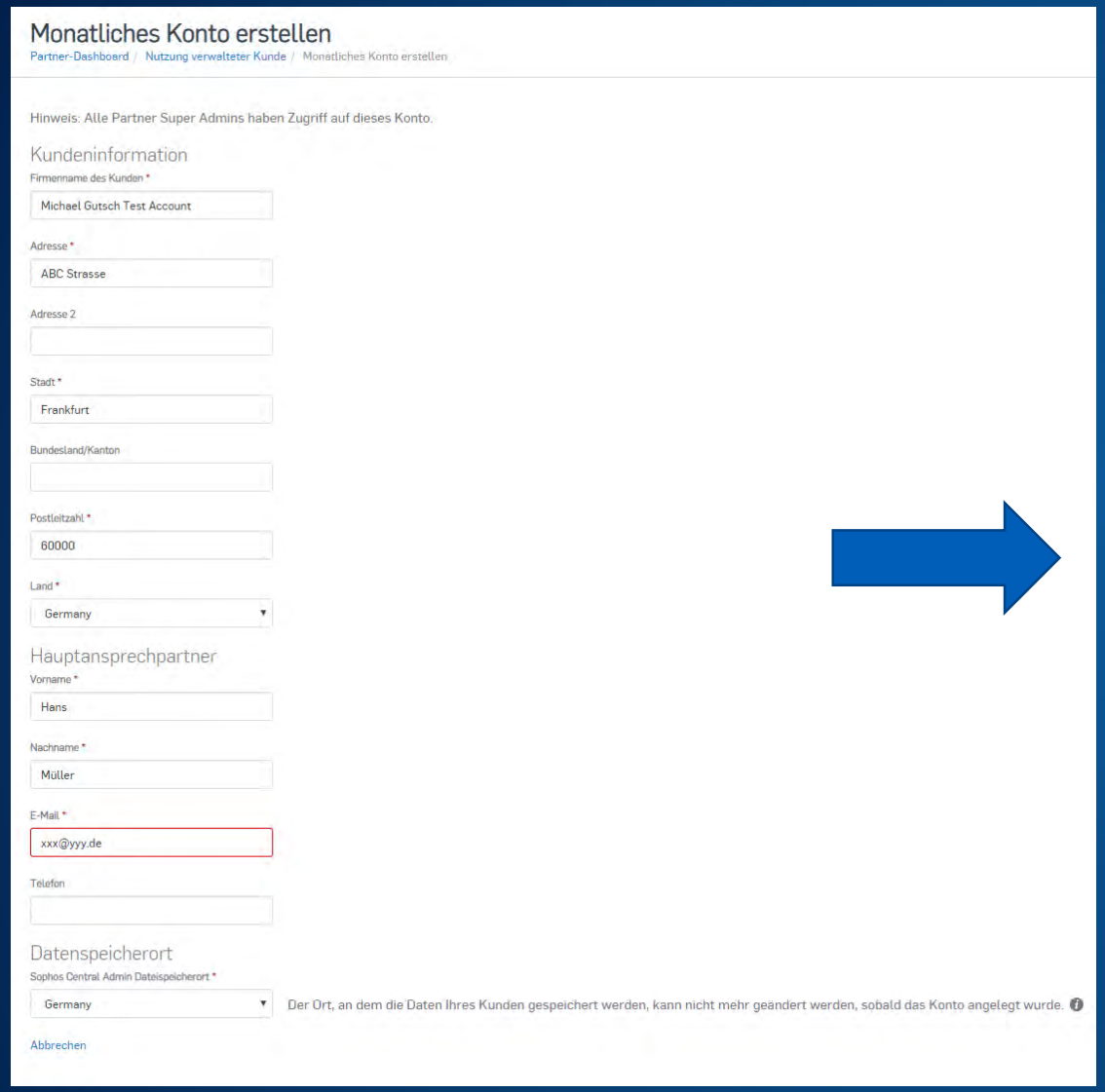
- Nach Schweregrad
- Nach Produkt
- Nach Kategorie

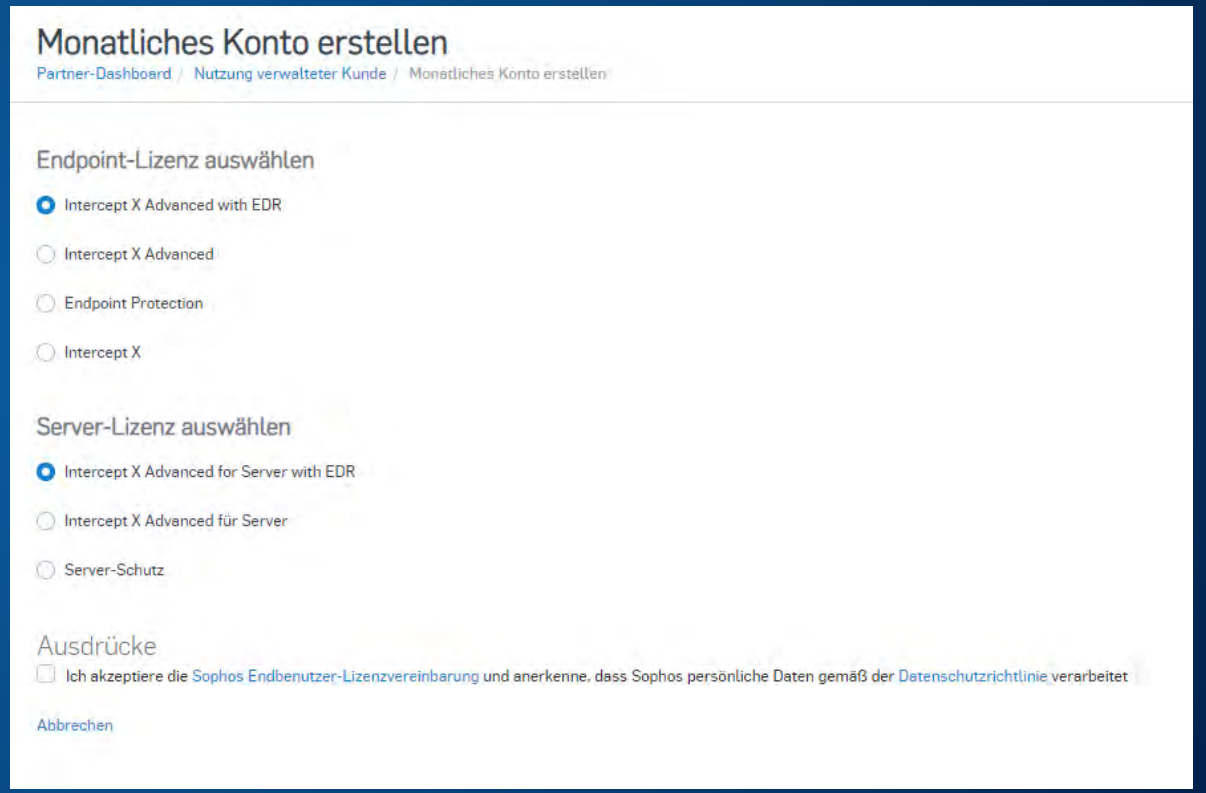
MSP Connect Flex – Anlegen neuer monatlicher Kunden



- Lizenz in Betrieb gesetzt und in Benutzung
- Aktuelle Testphase des Kunden
- Virtuelle Lizenzen in Betrieb gesetzt
- Test Lizenz abgelaufen
- Lizenznutzung oberhalb des Grenzwertes
- Test Lizenz läuft bald ab

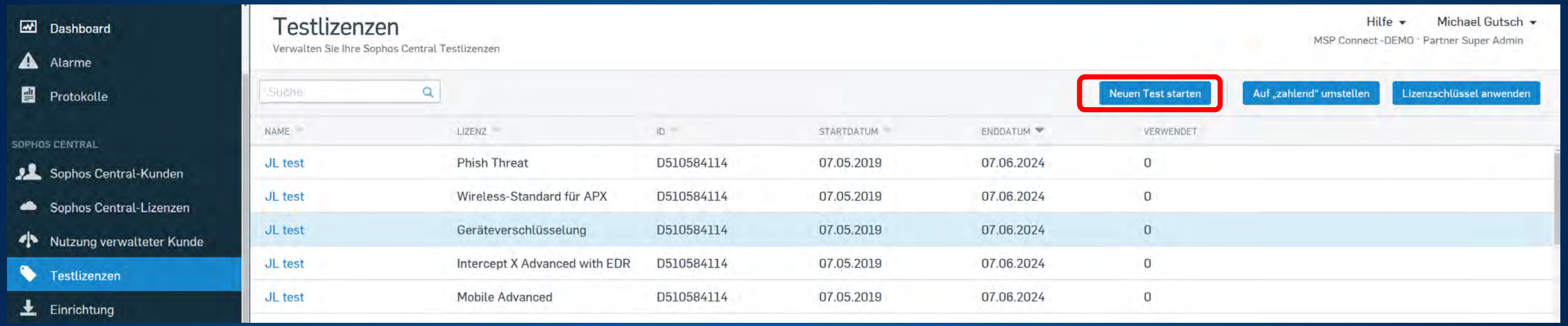
MSP Connect Flex - Anlegen neuer monatlicher Kunden





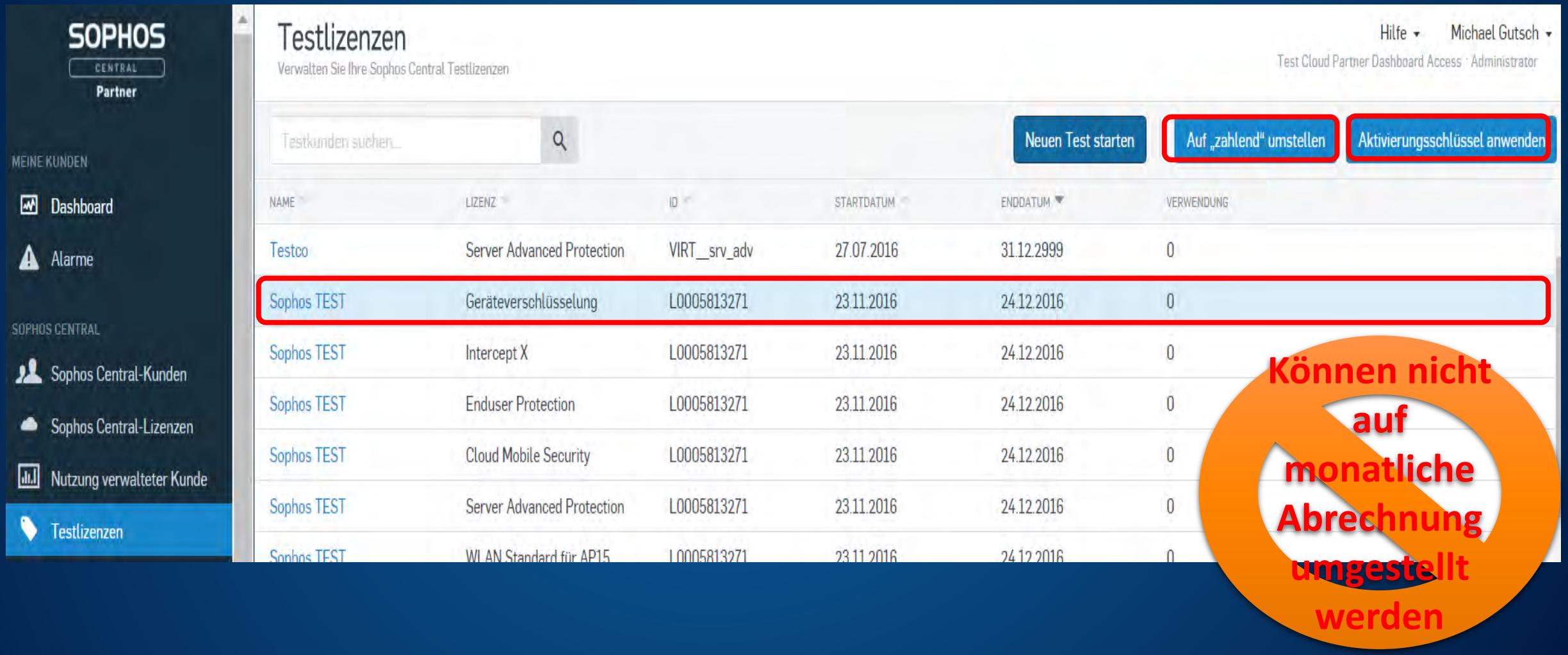
SOPHOS

MSP Connect Laufzeit Testlizenzen

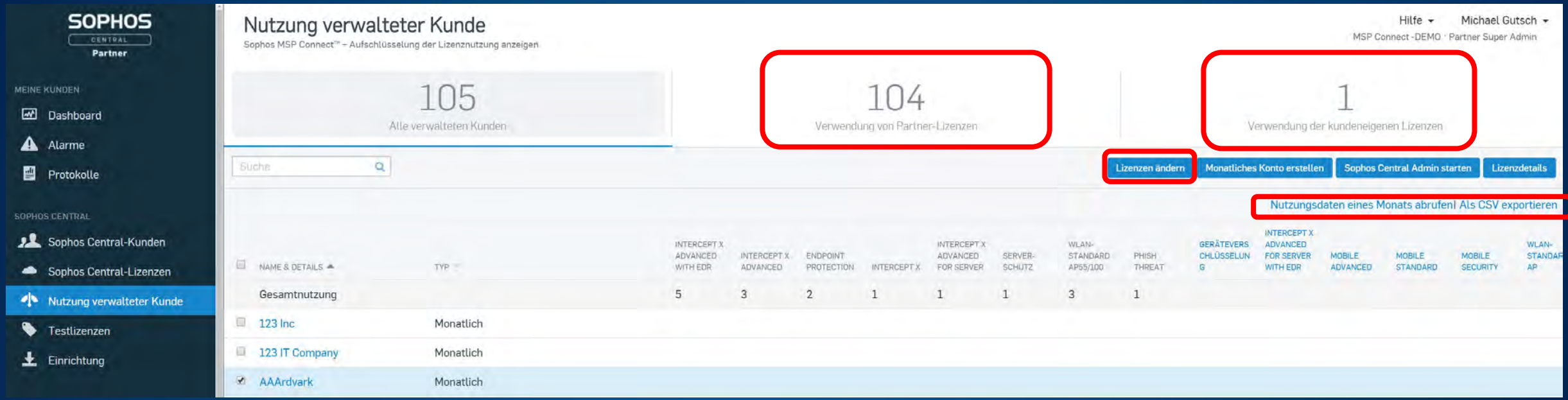


SOPHOS

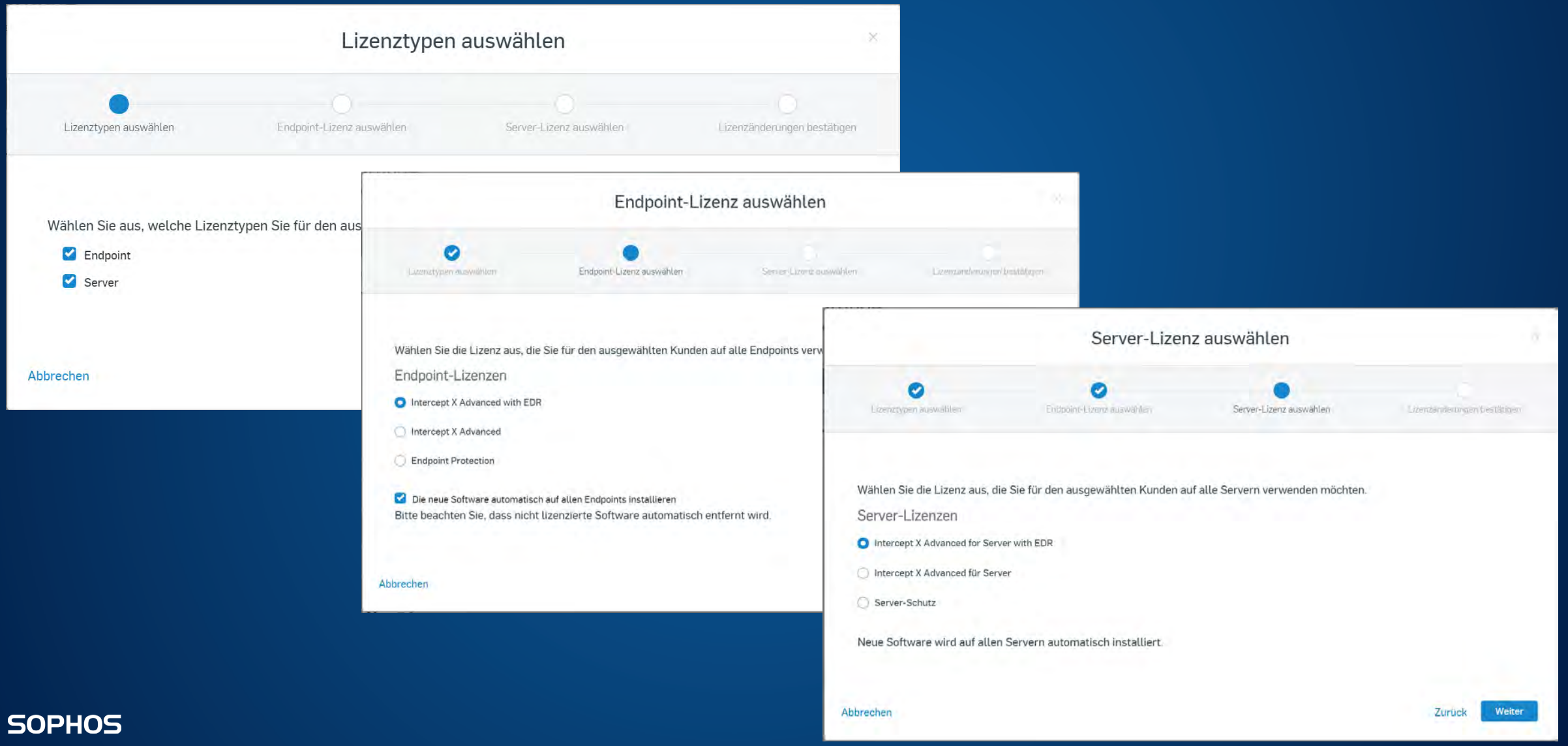
MSP Connect Testlizenzen – Umstellung auf zahlend



MSP Kunden Nutzungsdaten & Lizenztyp ändern



Endpoint & Server Lizenztyp ändern

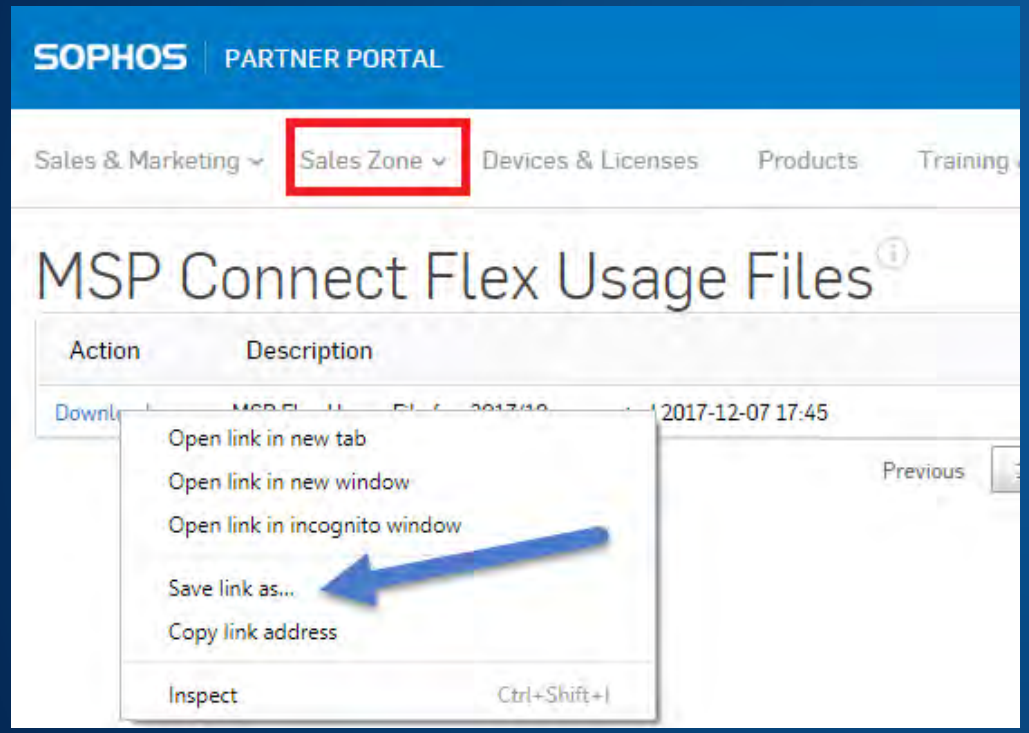


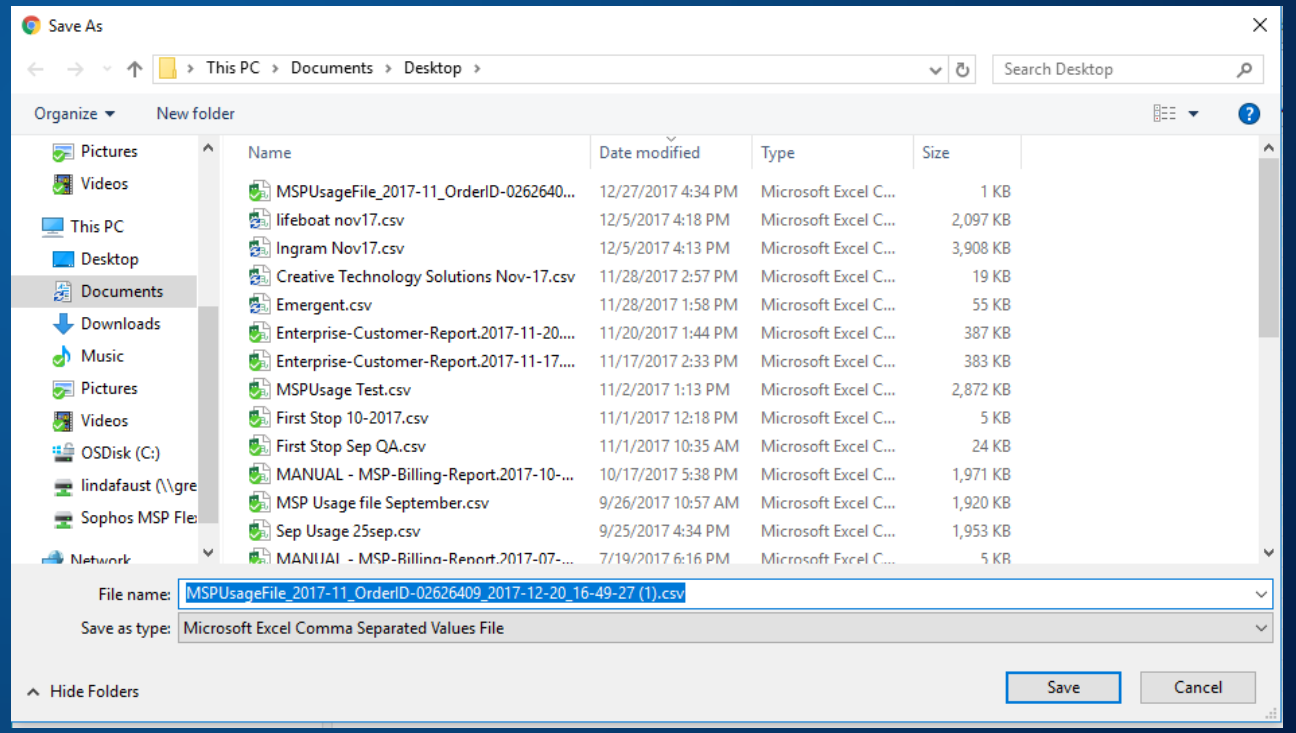
SOPHOS

MSP Nutzungsdaten – Verfügbar im Partner Portal

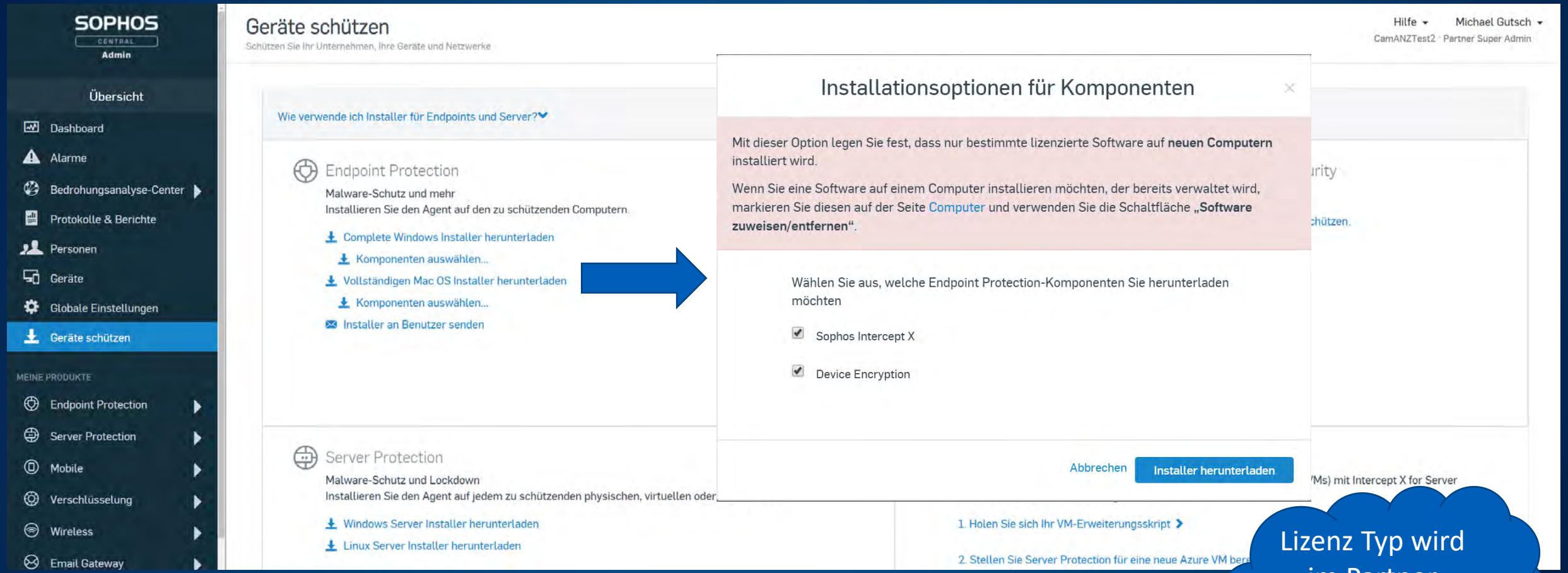
So können Sie den monatlichen Nutzungsreport herunterladen:

1. Auf Sales Zone im Partner Portal klicken und danach auf die verfügbaren Dateien
2. Rechte Maustauste klicken auf den Download link und Datei speichern unter klicken
3. Speichern als CSV oder XML Datei
4. Datei öffnen mit Excel oder anderem Tool



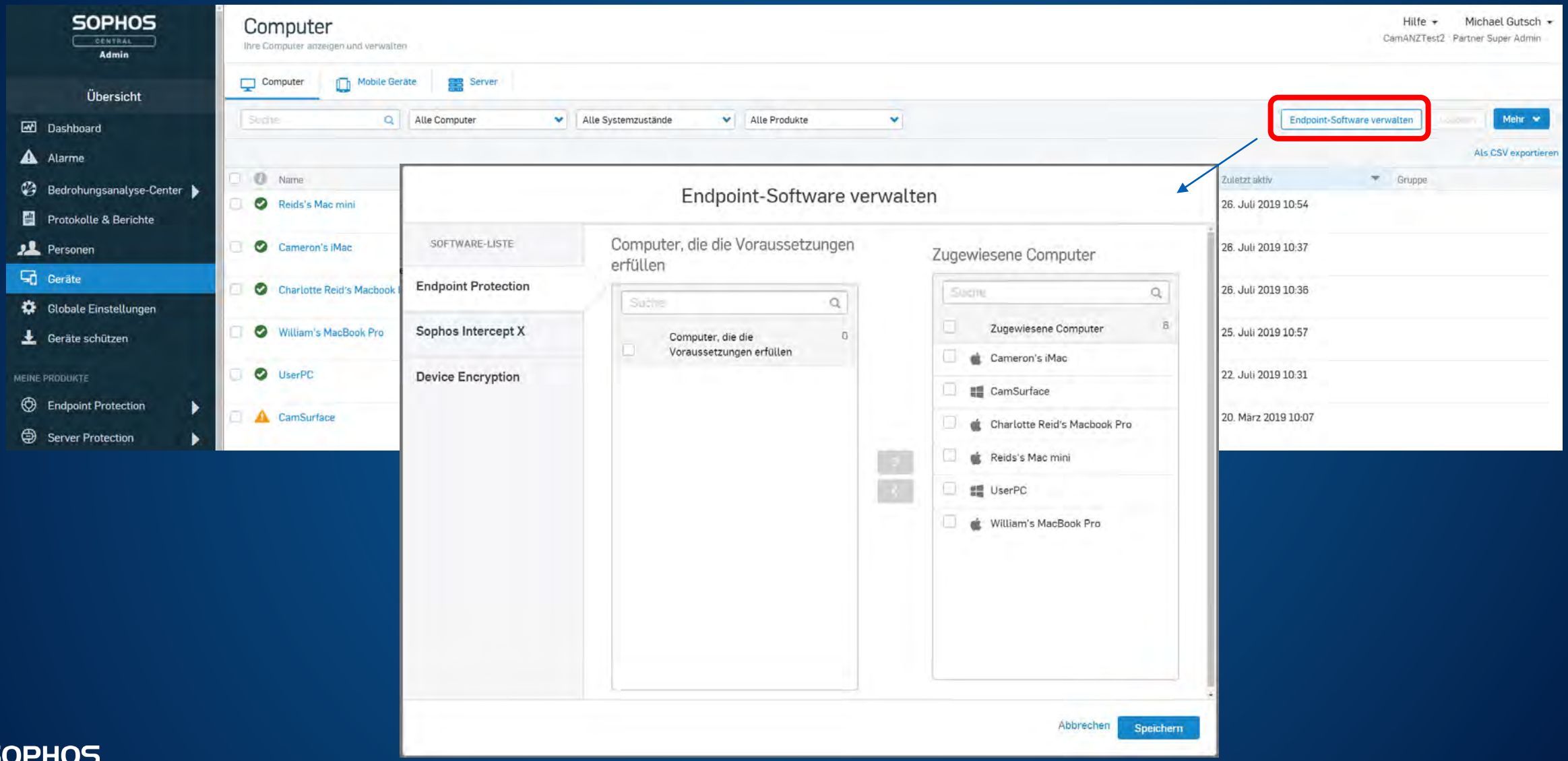


Sophos Central Admin – Systeme installieren - Beispiel



Lizenz Typ wird im Partner Dashboard eingestellt

Sophos Central Admin – Installation Produktauswahl



Sophos Central Live MSP Integrations

ConnectWise Automate®

Sophos Central Deployment Addon for CW Automate

ConnectWise Manage®

Sophos / ConnectWise Billing Integration for MSPs

Kaseya®

Sophos Central Thin Installer for Kaseya VSA

datto | AUTOTASK

Sophos / Autotask Billing Integration for MSPs

datto | RMM

Sophos Central Deployment through Datto RMM

BrightGauge

a ConnectWise solution

BrightGauge + Sophos Deliver Precision and Efficiency

liongard™

Sophos Central Inspector

servereye

Endlich! Sophos XG ins Monitoring inkludieren

auvik

XG SNMP Monitoring by Auvik Collector

Sophos Central Dashboard – Endpoint/Server Deployment via Thin Installer

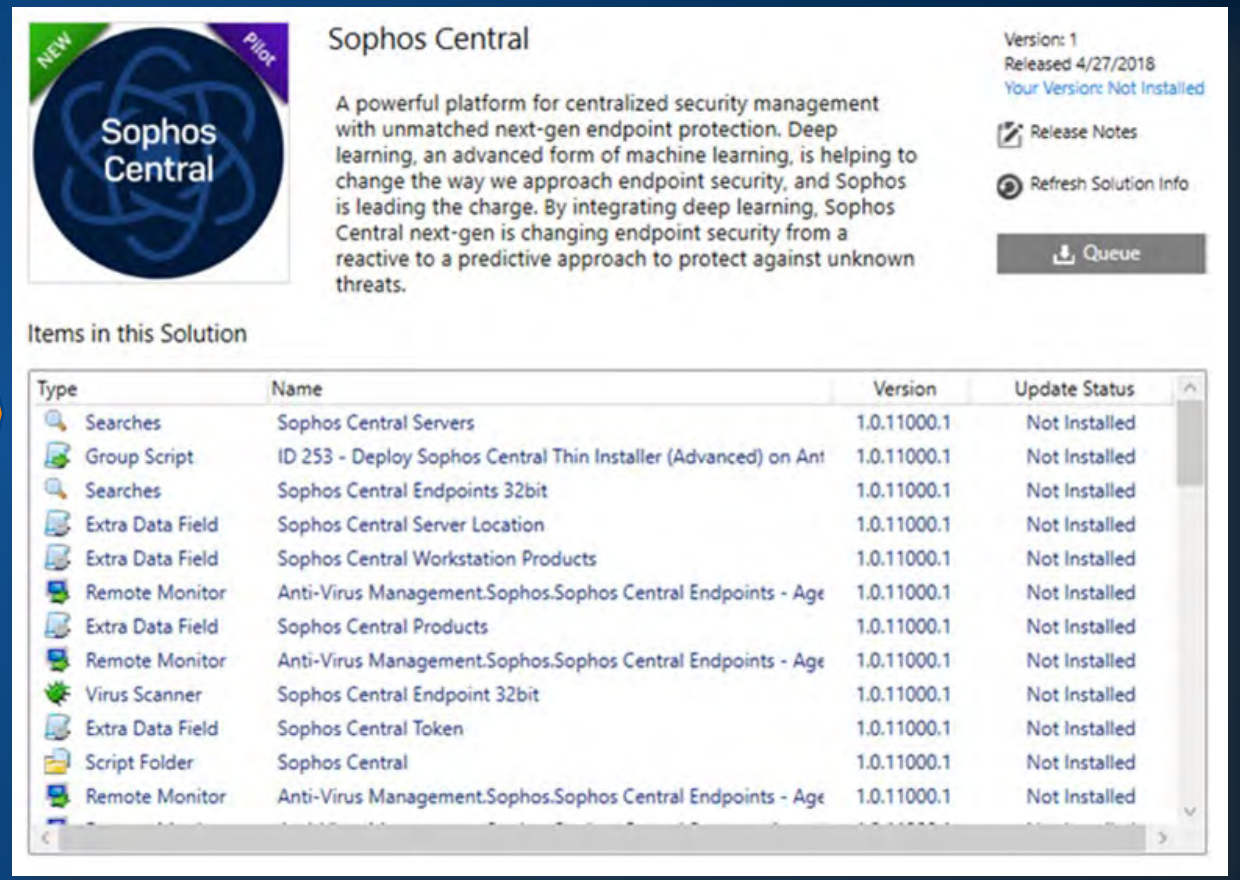


Weitere Informationen zur Command Line: https://community.sophos.com/kb/en-us/127045

ConnectWise Automate Solution Center (Certified)

- ConnectWise Automate Solutions Center
- Auto-Deployment of the Endpoint Agent
- Service Monitoring of Critical Agent

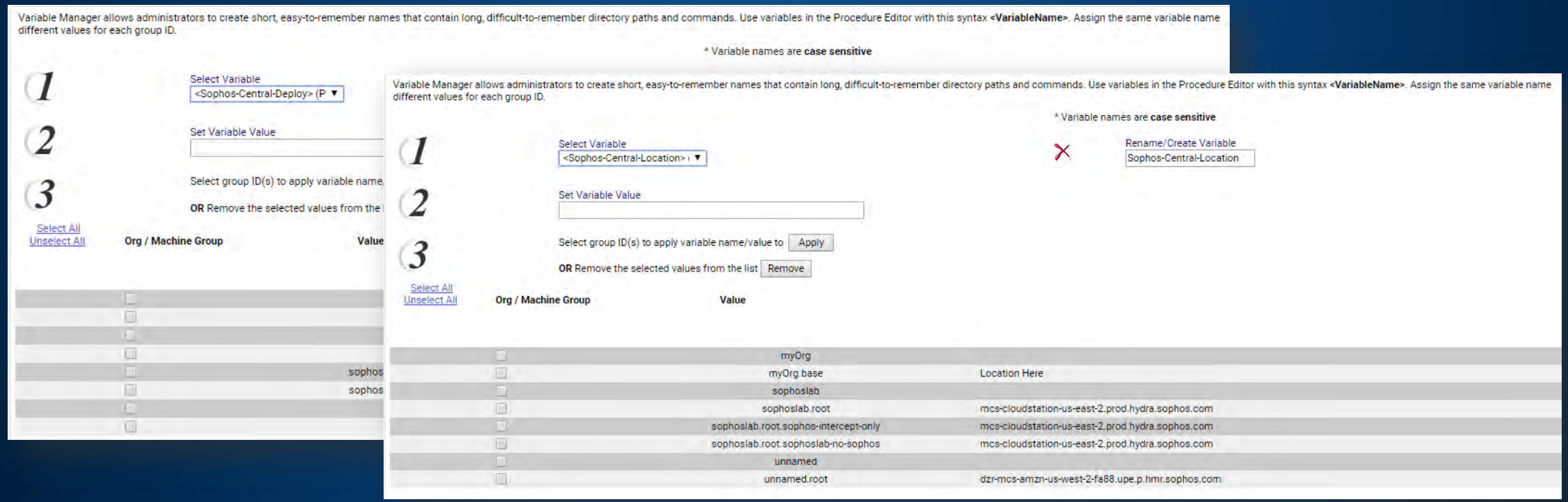
  Services
- Reboot Pending Monitoring
- Ticket Creation on Error



"My tech just came over and was ecstatic after reading through your docs. The Sophos integration far exceeded what he had expected. You should hype your integration to anyone else you know of that's using ConnectWise! 😉"

Kaseya

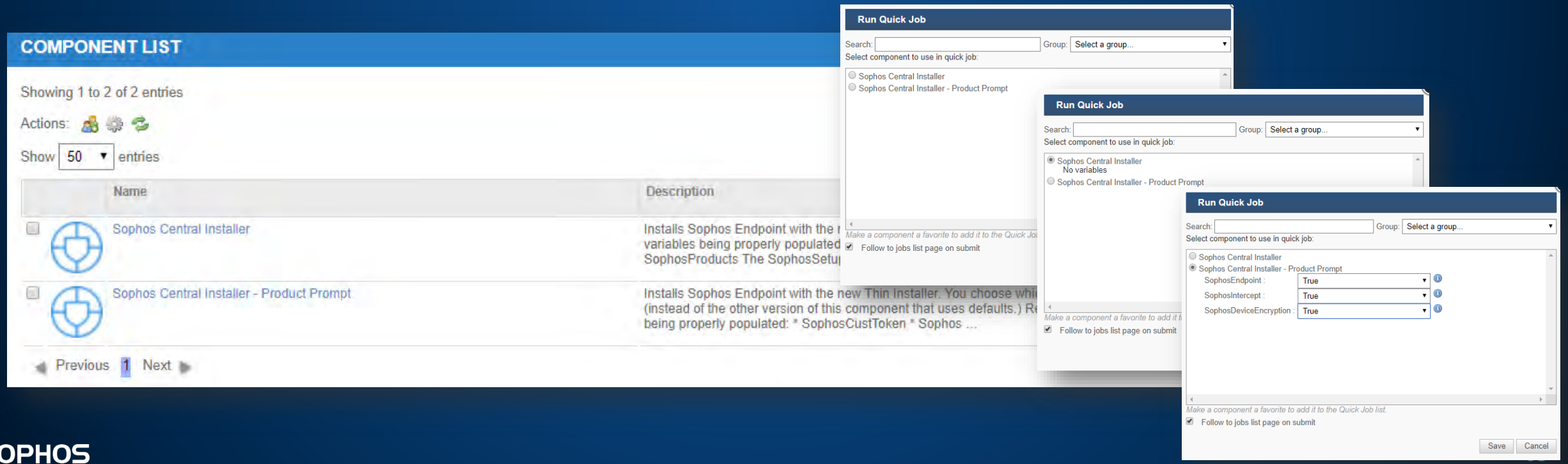
- Deployment Agent Procedure using Managed Variables
  - This allows for deployment via a Single Agent Procedure for all Customers
  - The Script pulls the Managed Variables entered to be run against the Workstation or Server based on the Machine Group it belongs to.



This script is currently only available to be manually run against the workstations and servers.

Datto RMM

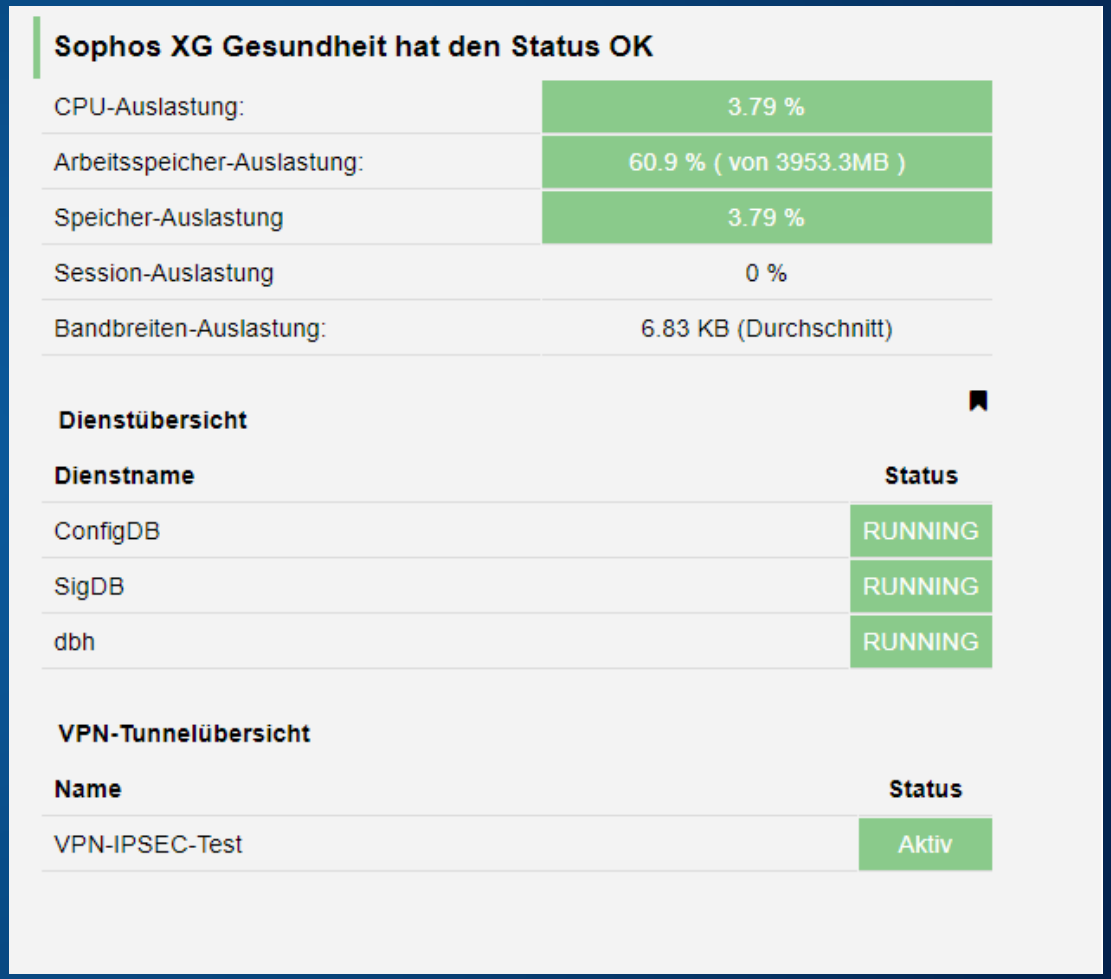
- Deployment Components using Site Level Variables
- Two Scripts available
  - One that takes all three variables and deploys with pre-defined products
  - The second that prompts for which Products should be installed
- Both can be scheduled



RMM Integration - Server Eye

Sensor für die Sophos XG:

- Performance (CPU, Arbeitsspeicher, Speicherauslastung)
- Dienste der XG
- Ausgewählte Schnittstellen
- Ausgewählte VPN Tunnel
- HA-Modus



Sophos XG Gesundheit hat den Status OK

CPU-Auslastung:	3.79 %
Arbeitsspeicher-Auslastung:	60.9 % (von 3953.3MB)
Speicher-Auslastung	3.79 %
Session-Auslastung	0 %
Bandbreiten-Auslastung:	6.83 KB (Durchschnitt)

Dienstübersicht

Dienstname	Status
ConfigDB	RUNNING
SigDB	RUNNING
dbh	RUNNING

VPN-Tunnelübersicht

Name	Status
VPN-IPSEC-Test	Aktiv

RMM Integration - Server Eye

Statusüberwachung für Sophos Cloud AV:

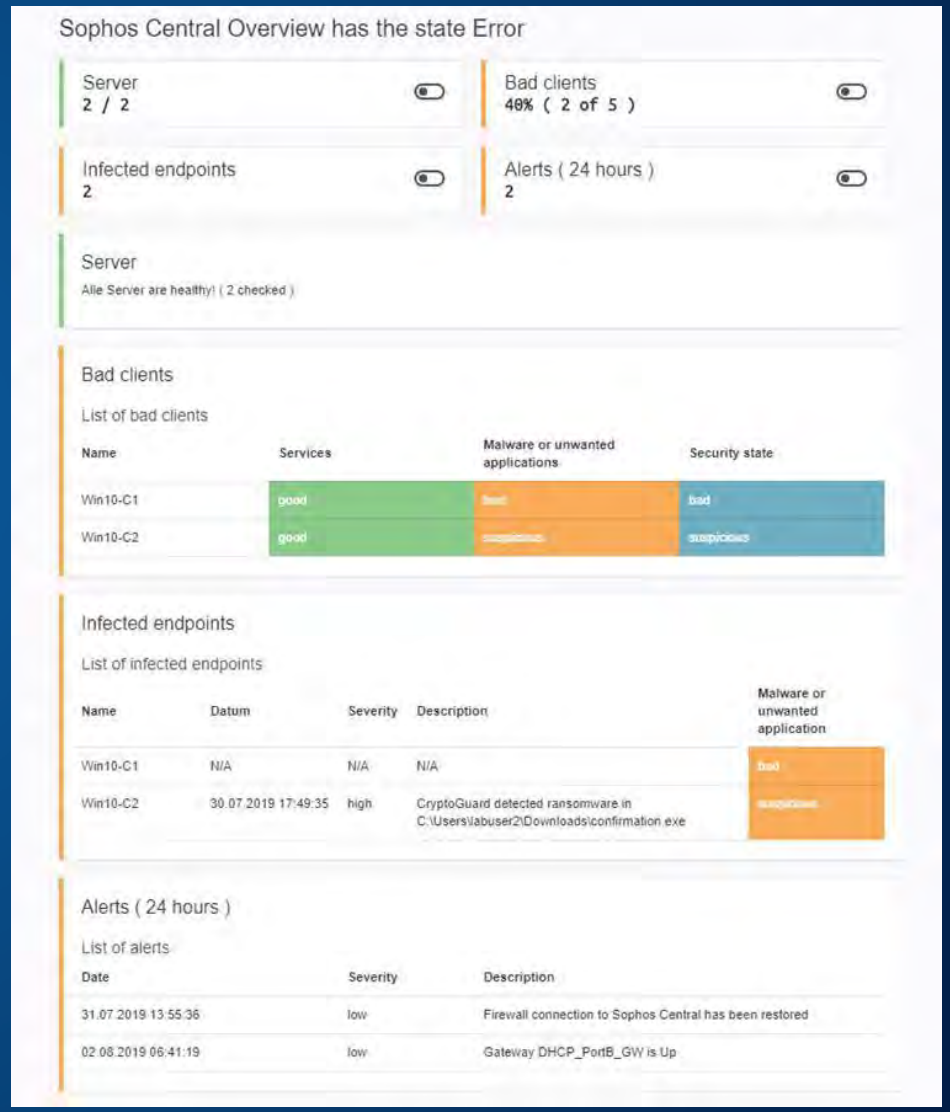
- Zugriff auf Sophos Central über die neue API
- Überwachung eines ausgewählten Kunden auf folgende Punkte:

Servergesundheit

- Gesamtstatus
- Dienste Status
- Infektionsstatus
- Alarmierung ab dem ersten Server

Clientgesundheit

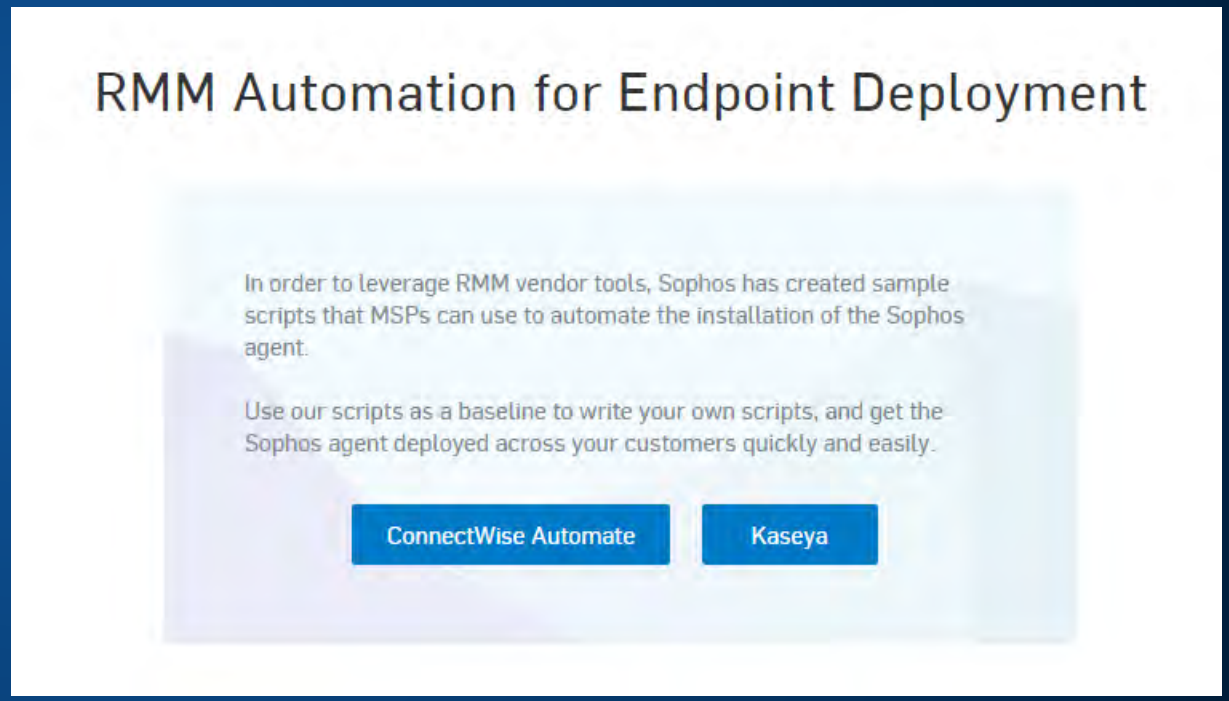
- Gesamtstatus
- Dienste Status
- Infektionsstatus
- Alarmierung erst ab xx Prozent fehlerhafter Clients.
- **Unbehandelte Vireninfektionen**
- Detaillierte Anzeige der Infektion (falls verfügbar)
- Ansonsten Anzeige des infizierten Systems
- Anzeige der Alarme der letzten 24 Stunden (nach Benachrichtungsgrad Mittel oder Hoch)



RMM Deployment Integrationen

Deployments scripts und Guides verfügbar:

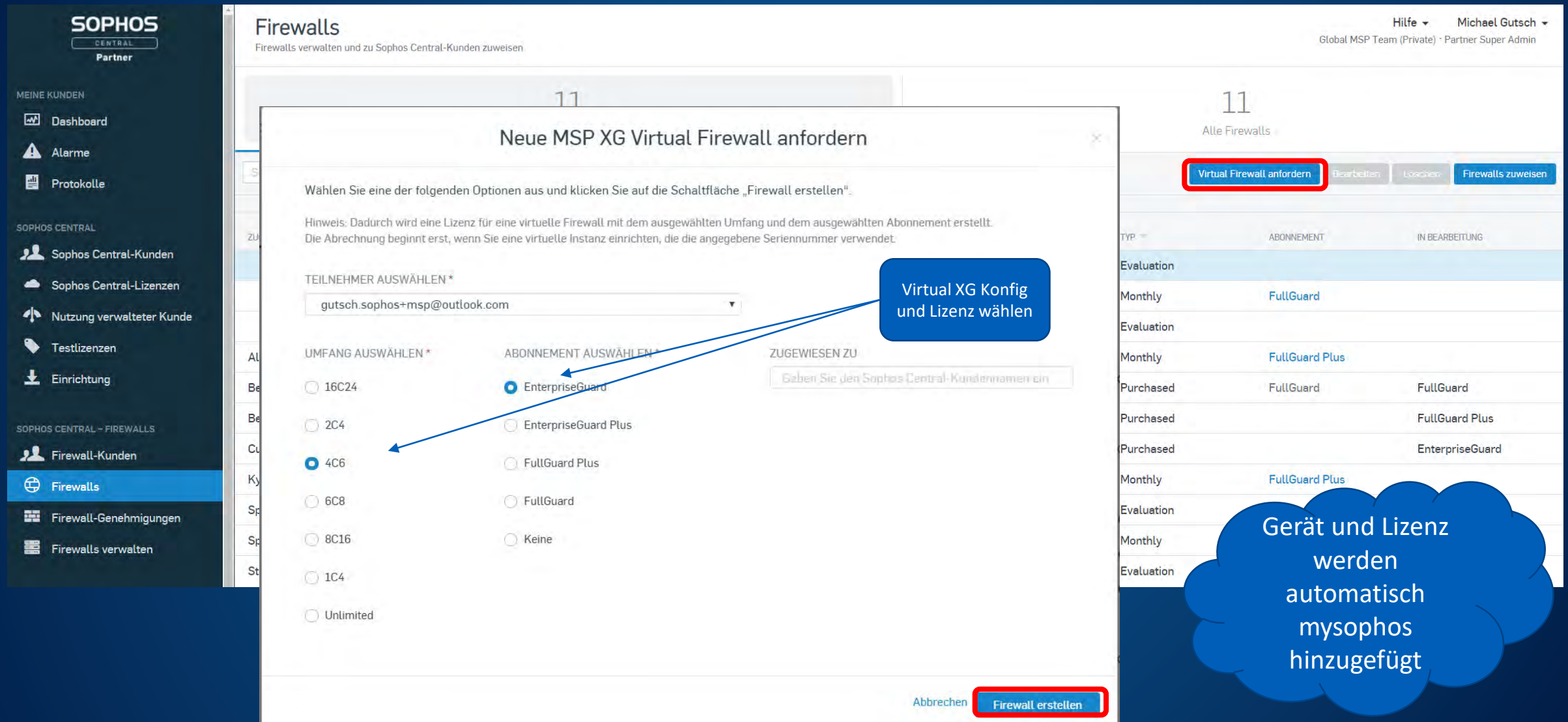
- **Verfügbar:**
  - **ConnectWise Automate Certified**
  - **Kaseya**
  - **Server Eye**
  - **Datto RMM**
- **In Bearbeitung:**
  - **Autotask AEM (CentraStage)**
  - **SolarWinds/N-Able**
  - **Continuum**



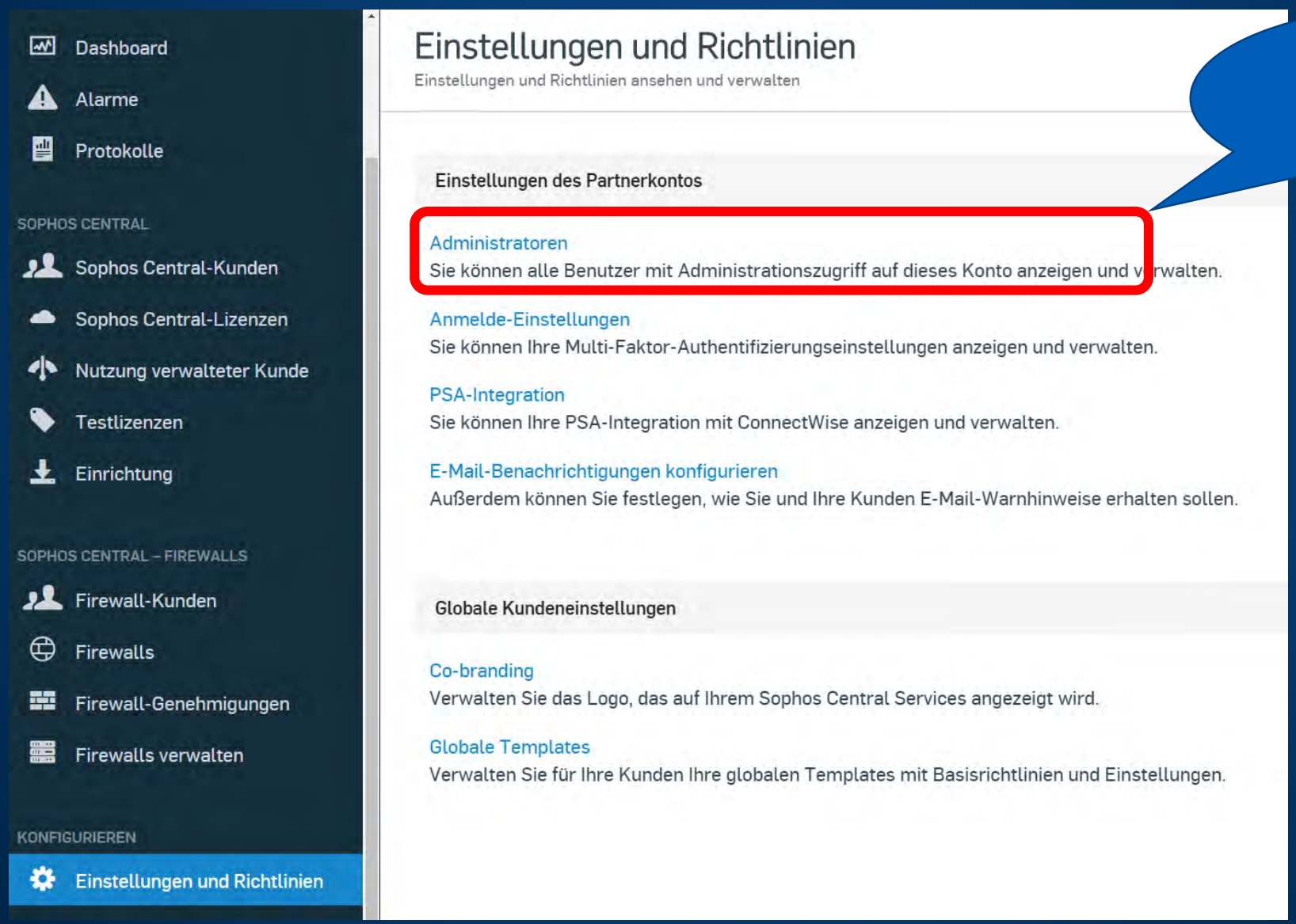
MSP Hub im Partner Portal

MSP HUB - https://partnerportal.sophos.com/en-us/msp-hub.aspx

Virtual XG Firewall as a Service



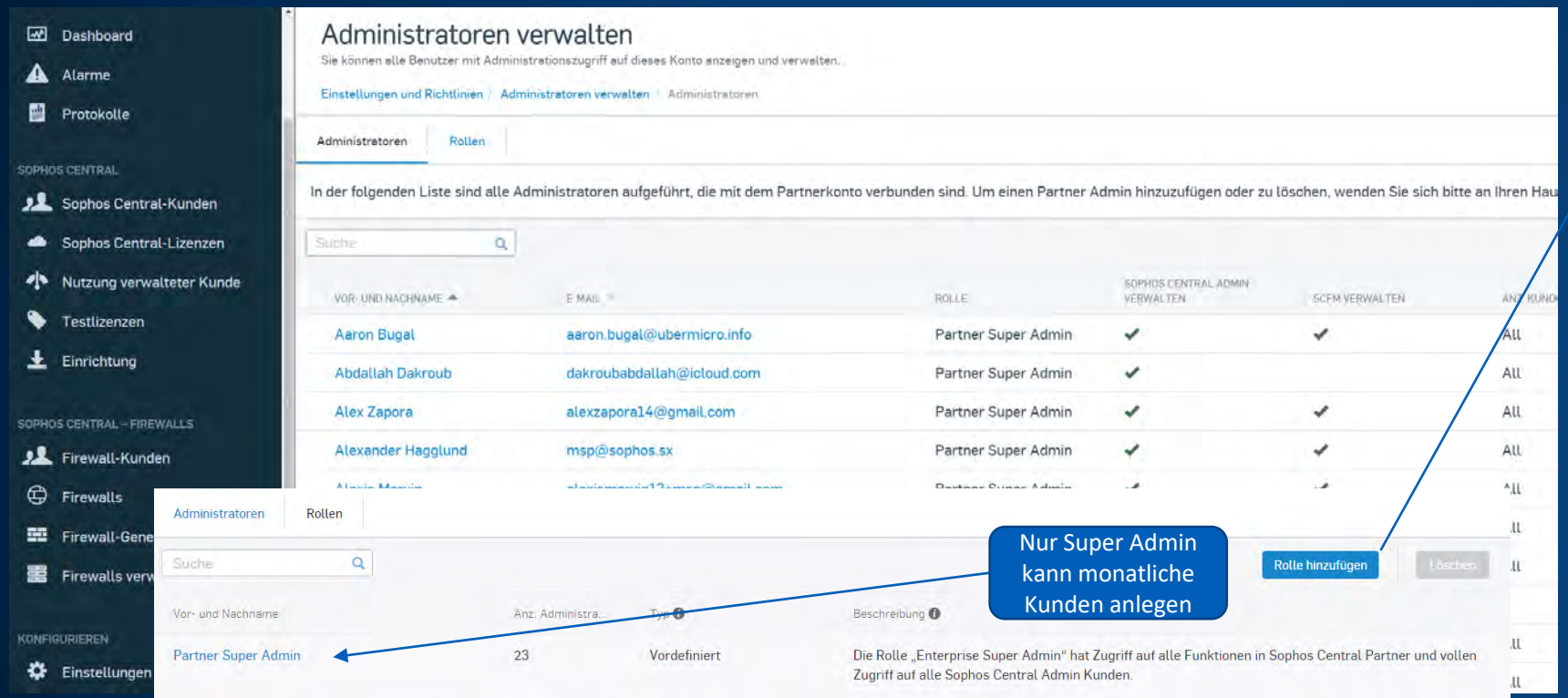
Einstellungen und Richtlinien - Administratoren



Administratoren verwalten

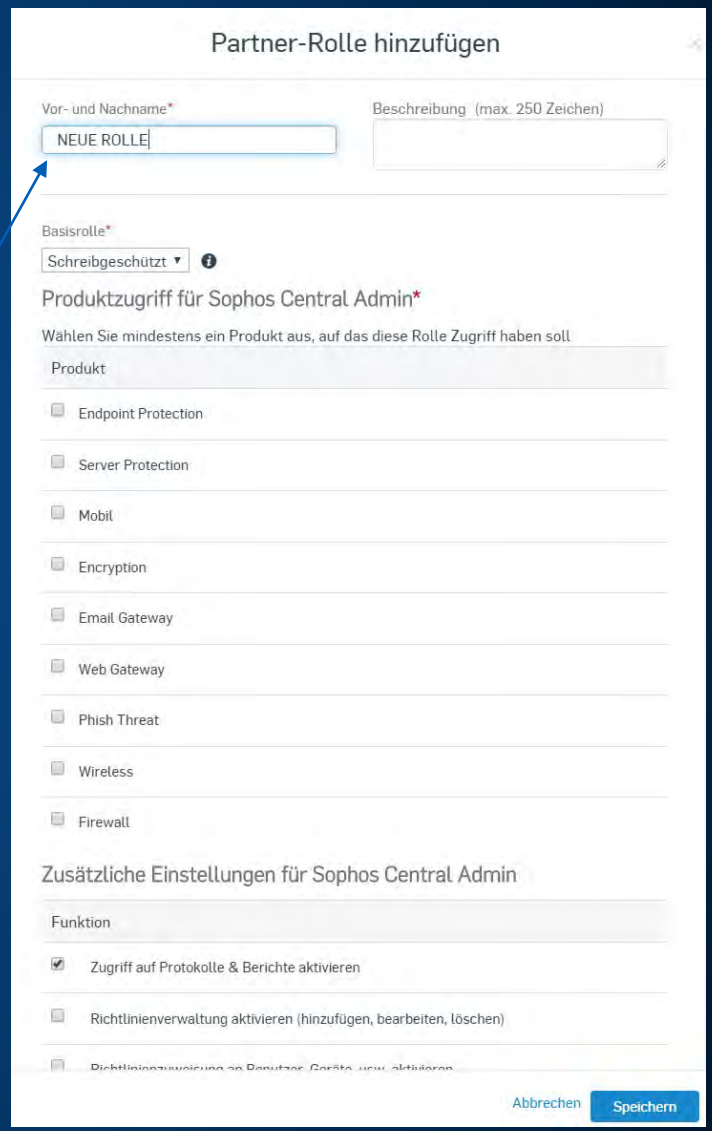
SOPHOS

Einstellungen und Richtlinien – Administratoren (RBAC v2)



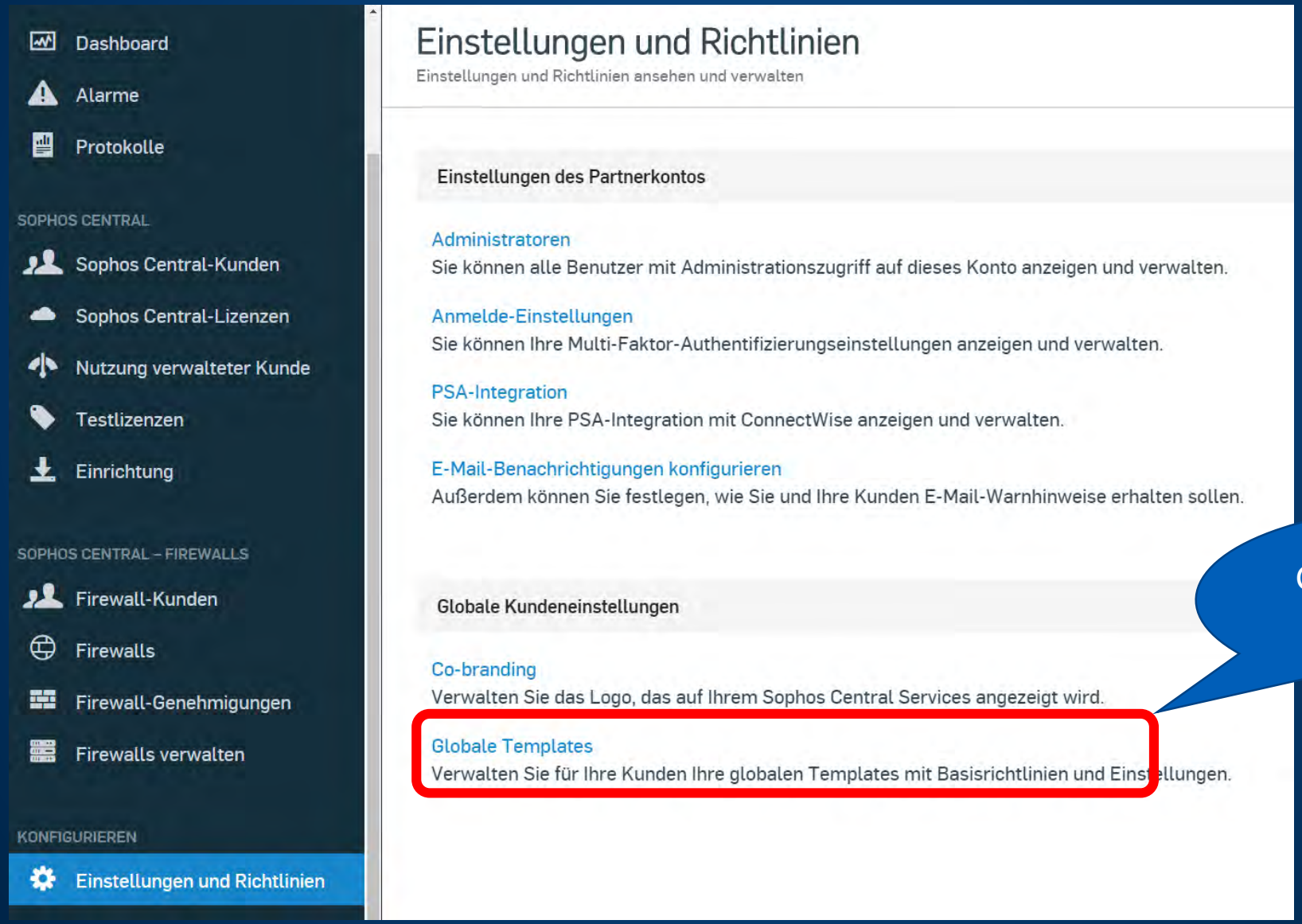


Nur Super Admin kann monatliche Kunden anlegen



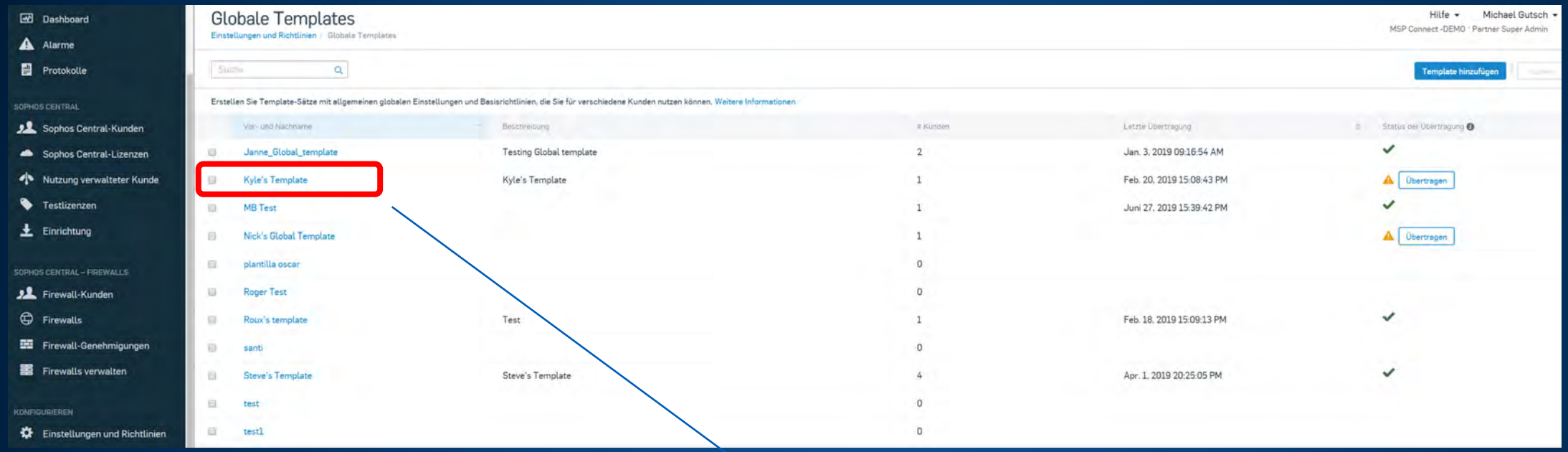
SOPHOS

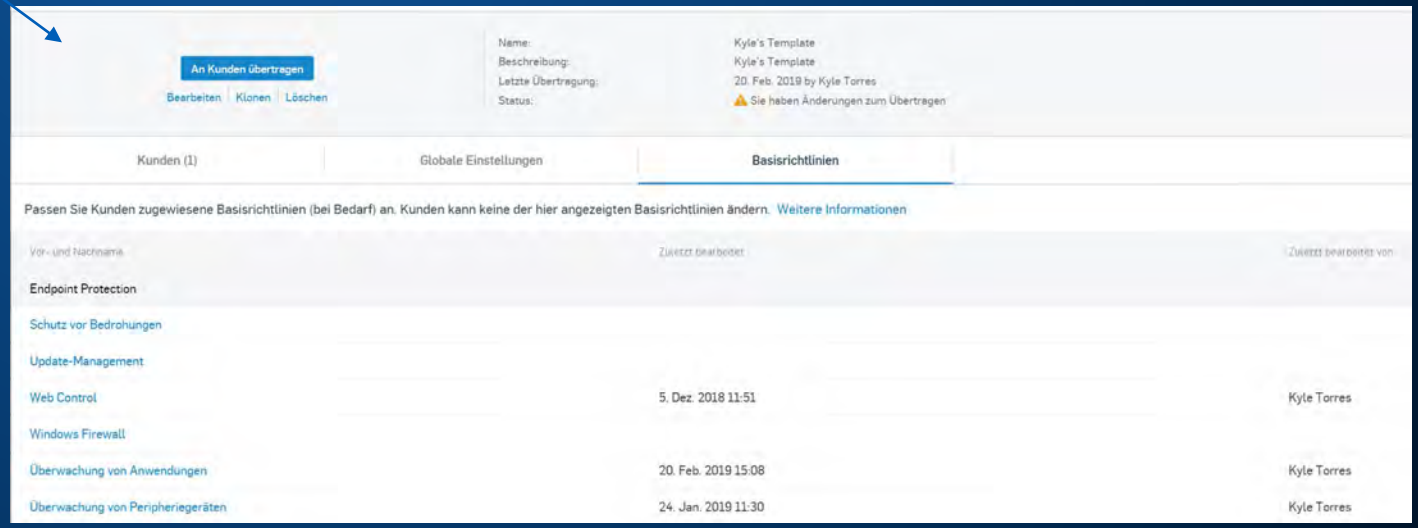
Einstellungen und Richtlinien – Globale Templates



SOPHOS

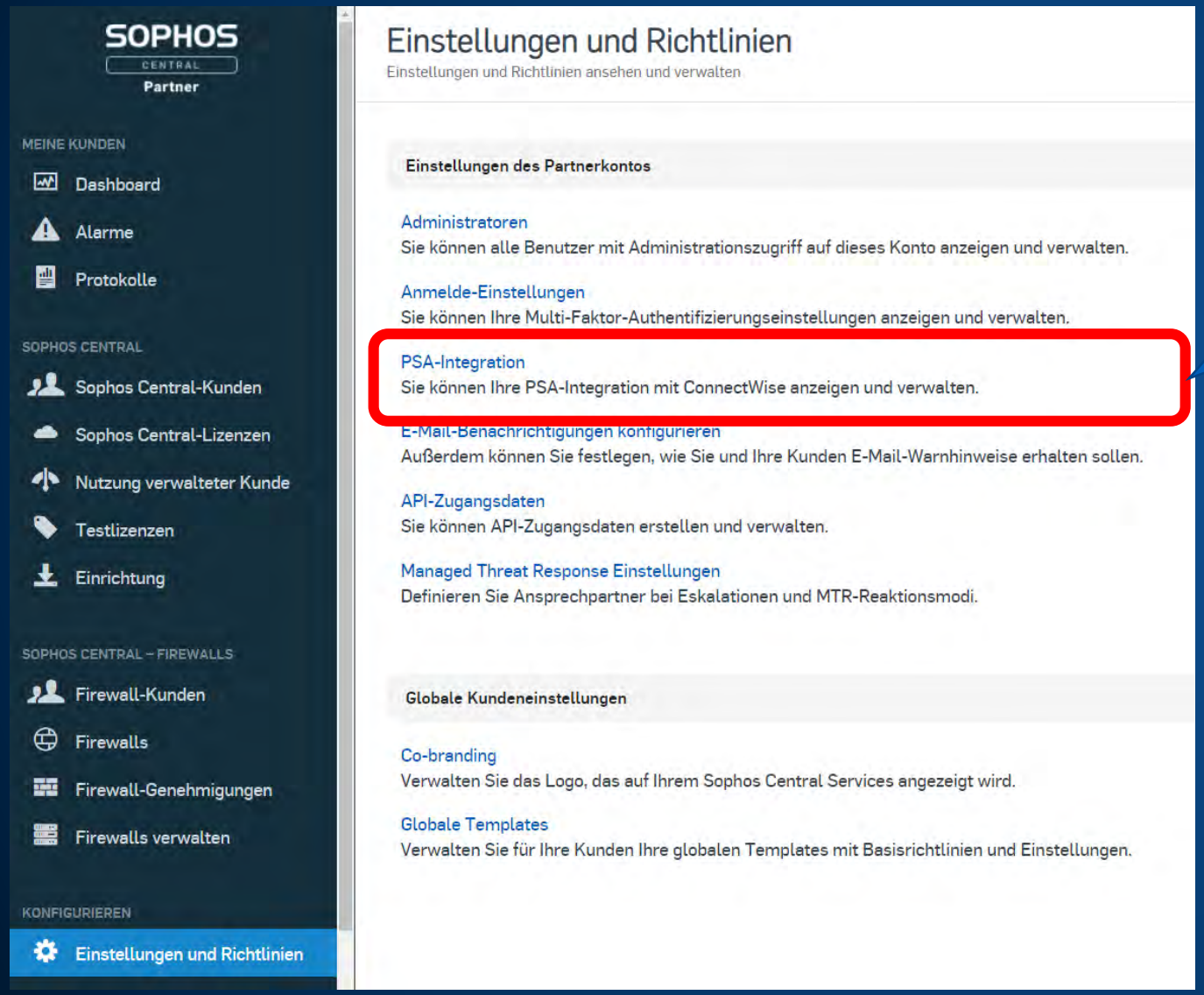
Einstellungen und Richtlinien – Globale Templates





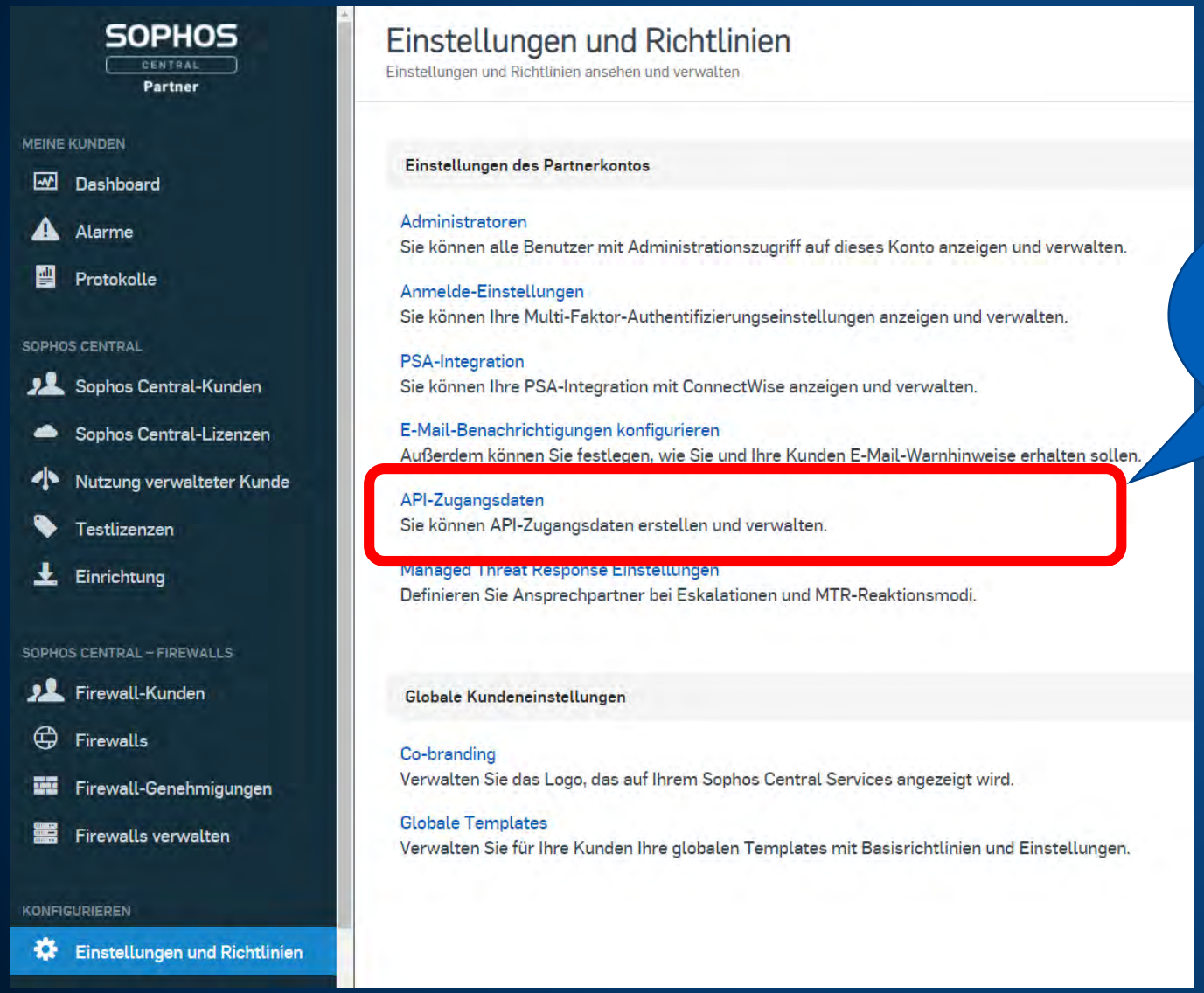
SOPHOS

Einstellungen und Richtlinien – PSA Integration



Connectwise / Autotask PSA Abrechnungs - Integration einrichten

Einstellungen und Richtlinien – API



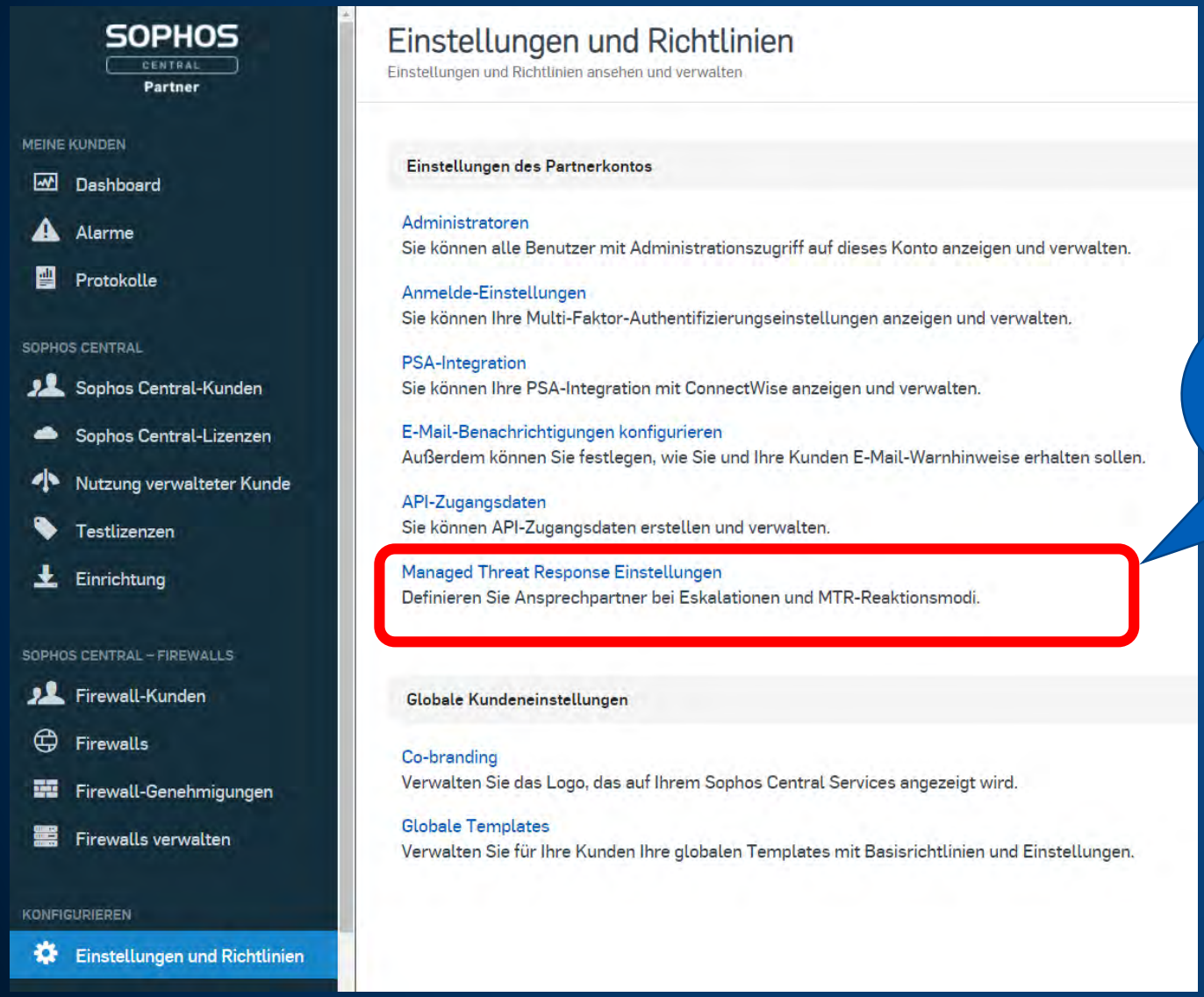
API Konfiguration

Monitoring & Management APIs

- **Endpoint & Server Status API**
  - Query device details such as IP addresses, OS, last user logged in, last seen, last reboot, etc
  - Query product state such as installed products, tamper protect status, last update, last scan, running/failed services, etc.
  - Query health state, including latest threats, active threats, and overall derived health status.
- **Endpoint & Server Management API**
  - Enable/disable tamper protection per endpoint
  - Run a scan
  - Run a product update
  - Lock down a server
- **Interactive Alerts Management API**
  - Retrieve all alerts by account/sub-estate
  - Retrieve individual alerts by Alert ID and Group ID
  - Pre-filtered alert retrieval by Severity, Product, and Category
  - Clear individual alerts by Alert ID

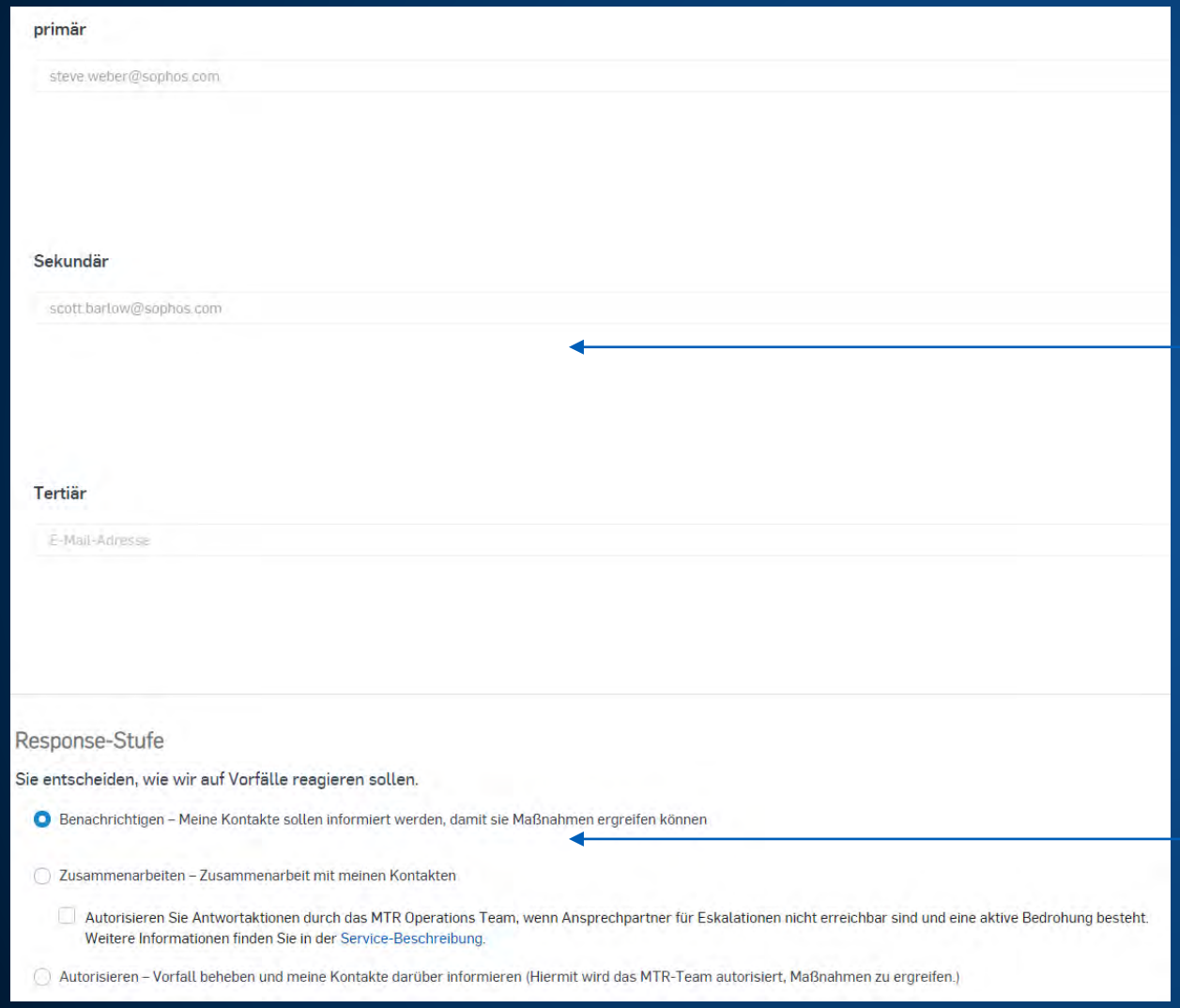
How to Guide available here: https://developer.sophos.com/getting-started

Einstellungen und Richtlinien – MTR



MTR
Konfiguration

Einstellungen und Richtlinien – MTR

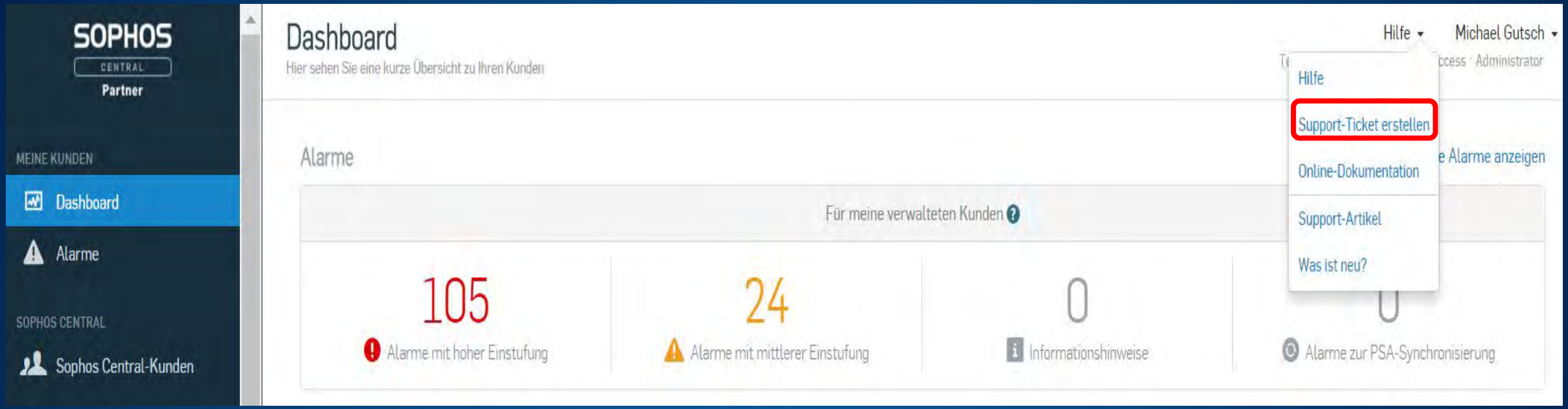


Kontakte festlegen

Modus der Zusammenarbeit

SOPHOS

MSP Support



Email: Support:
msp.support@sophos.com

Telefon Support:
+49-611-58581020

EIN flexibles Programm

SOPHOS

Sophos MSP Connect Highlights

Ausgerichtet an Ihrem MSP Geschäftsmodel – echtes pay per Use



- **Einfacher Zugang zum Program** -> nur 2 Online Trainings notwendig
- **Monatliche, nutzungsbasierte Abrechnung** -> echtes pay per use Model, keine Mindestabnahmemengen, keine Bestellungen notwendig
- **Volumen basierte Rabatte auf Basis aggregierter Nutzung** -> sinkende Preise für Sie mit steigender Lizenznutzung über alle Kunden
- **End to End Security Portfolio aus einer Hand** -> einfaches Hersteller Management, eine Abrechnung
- **Virtual Firewall as a Service** -> kein Vorabinvestment für virtuelle Firewalls, skalierbares OPEX Model
- **LvL2 Support für MSPs** -> priorisierter Support für MSPs
- **Dediziertes MSP Team beim Hersteller** -> wir verstehen Ihr MSP Business

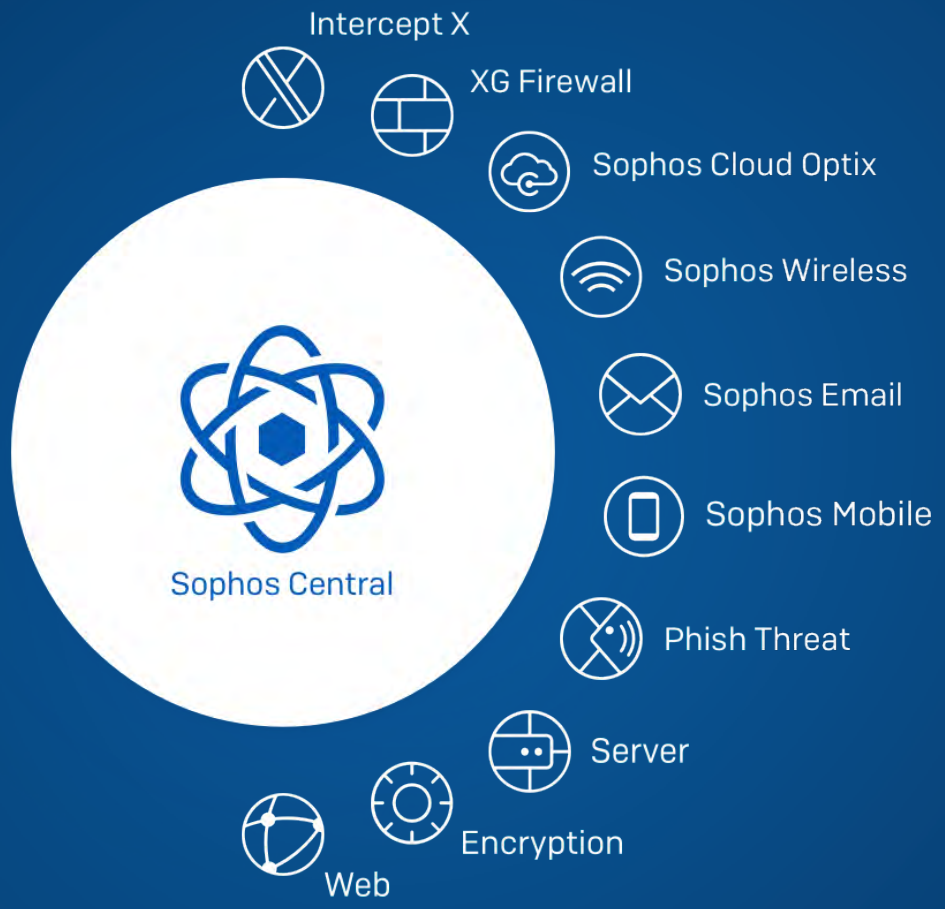
End-to-end Schutz mit einem Hersteller

XG Firewall
Perimeter Schutz mit der optimalen enterprise Firewall

Server Protection
Für Server-Umgebungen optimierter Schutz (physikalisch oder virtuell)

InterceptX Advanced for Server
Alle Standard features + Next-Gen

Wireless Standard
Sicheres, einfaches WI-Fi



InterceptX Advanced (PC/Mac)
Standard + Next-Gen Schutz in einem Produkt

Mobile
Sicherheit für Smartphones und Tablets
MDM, Containerization, Kiosk

Device Encryption (PC/Mac)
Verschlüsselung ermöglicht effiziente letzte Schutzlinie gegen Datenverlust

Phish Threat
Security Awareness Training für Benutzer des Endkunden

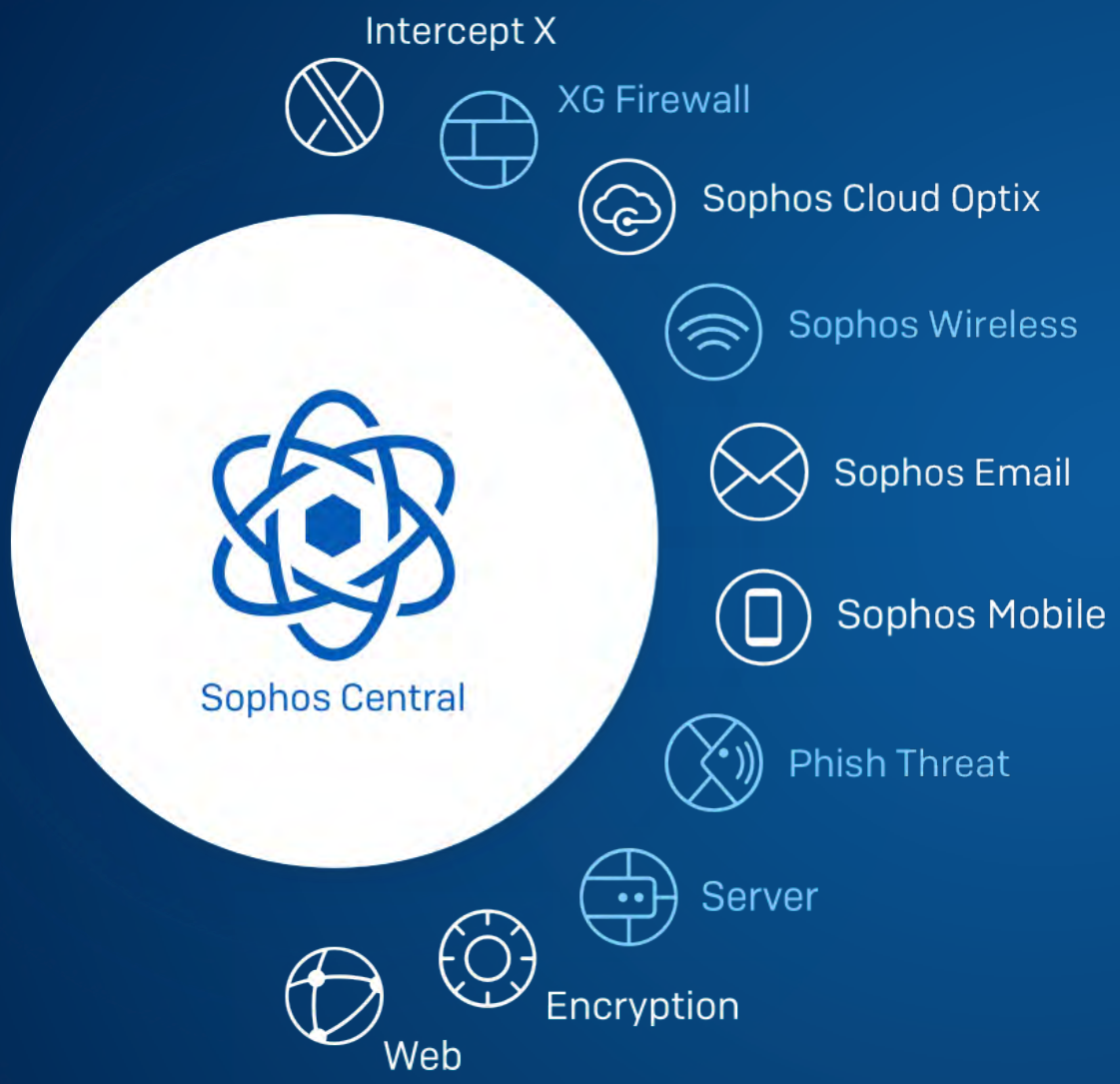
Cloud Optix
Cloud security Überwachung, Analyse und Automatisierung

EDR/MTR
Managed threat hunting, detection, und response for Server and Endpoint

Email Advanced
Keine Chance für Email-Bedrohungen und Phishing-Angriffe dank transparenter Email-Filterung

SOPHOS

End-to-end Schutz mit einem Hersteller



D

Perimeter Schutz XG FW
Perimeter Schutz mit der optimalen enterprise Firewall

S

Server Schutz
Für Server-Umgebungen optimierter Schutz (physikalisch oder virtuell),
Application Control / CrypoGuard

W

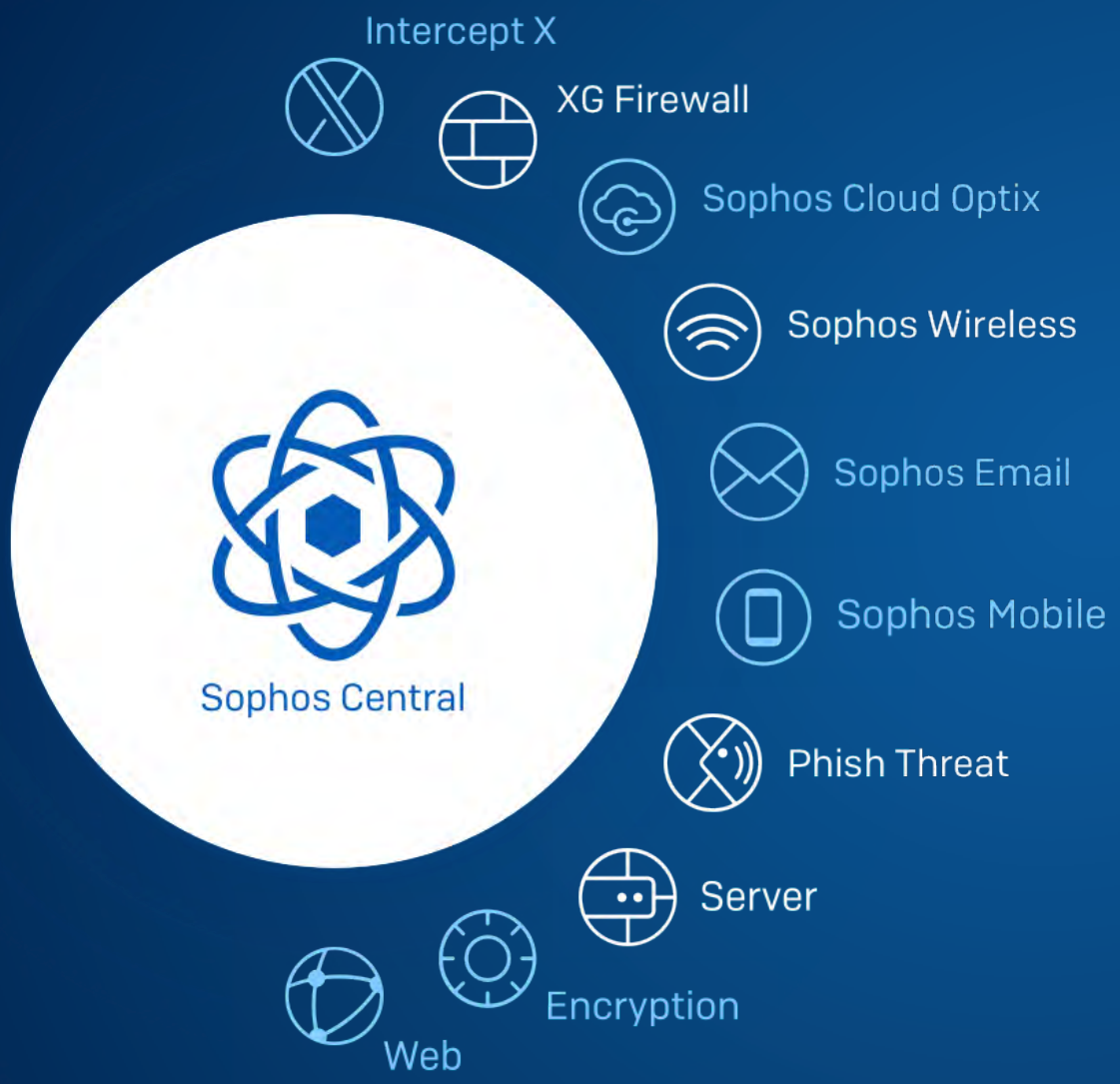
Sicheres Wi-Fi
Sicheres, einfaches WI-Fi

C

Cloud Optix
Cloud security Überwachung, Analyse und Automatisierung

SOPHOS

End-to-end Schutz mit einem Hersteller



U

Secure the Endpoint (PC/Mac)
Next Gen Endpoint security
Schutz gegen Ransomware und Exploits, Ursachenanalyse, MTR, EDR

U

Phish Threat
Security Awareness Training für Benutzer des Endkunden

U

Mobile (IOS, Android)
Sicherheit für Smartphones und Tablets
MDM, Containerization, Kiosk

U

Device Encryption (PC/Mac)
Verschlüsselung ermöglicht effiziente letzte Schutzlinie gegen Datenverlust

U

Email Sicherheit
Proven email security for business continuity

SOPHOS

Lizensierung Beispiel



Kunde A

200 User
10 Server
5 Wireless
2 Devices



Kunde B

120 User
5 Server
48 Wireless



Kunde C

300 User
10 Server
15 Devices
1 Cloud



Kunde D

500 User
8 Server
9 Devices

=

MSP aggregierte Nutzung

1120 User
33 Server
26 Devices
53 Wireless
1 Cloud

SOPHOS

Aggregierte Lizenz Abrechnung

User Licenses: Endpoint, Intercept X, EDR, MTR, Mobile, Encryption, Phish Threat, Email
1 -99 user licenses
100-499 user licenses
500-999 user licenses
1,000-4,999 user licenses
5,000-9,999 user licenses
10,000+ user licenses

Device: XG Firewall
1-24 devices
25-99 devices
100-199 devices
200 -499 devices
500-999 devices
1,000 + devices

1120 User
33 Server
26 Devices
53 Wireless
1 Cloud

Server Licenses: Standard and Advanced
1 -24 server licenses
25-99 server licenses
100-249 server licenses
250-499 server licenses
500-999 server licenses
1,000 + server licenses

Wireless: APX, AP15, AP55, AP100
1-24 access points
25-99 access points
100-199 access points
200 -499 access points
500-999 access points
1,000 + access points

Cloud: Cloud Optix
1-24 assets
25-99 assets
100-199 assets
200 -499 assets
500-999 assets
1,000+ assets

SOPHOS

MSP Lizenzierung – FAQ

Der Abrechnungs Zyklus geht vom 23ten des Monats zum 22ten des Folgemonats -> Sophos wertet die Nutzungsdaten am **22ten** jedes Monats aus.

Sophos bietet Nutzer basierte Lizensierung:

- **Nutzer können mehrere Geräte registriert haben, trotzdem fällt nur 1 Lizenz an. (getrennt pro Produkt)**
  - BEISPIEL: 1 Nutzer hat 2 Geräte (Laptop und PC Workstation) und beide sind durch Sophos Endpoint geschützt. Es wird trotzdem nur 1 Lizenz gezählt.
- **Was passiert, wenn mehrere Nutzer sich ein Gerät teilen? (Call Center Szenario)** -> Wir berechnen nur den User, der zuletzt am jeweiligen Gerät angemeldet war. Die anderen haben kein Gerät zugeordnet und werden nicht abgerechnet.
  - BEISPIEL: 200 Nutzer, die sich abwechselnd auf 50 PCs im Call Center anmelden, werden nur 50 Lizenzen konsumieren.
- **Aktive vs. Passive Nutzer** -> Wir rechnen nur aktive Nutzer ab, d.h. Diese müssen mind. 1 mal in Abrechnungszyklus angemeldet gewesen sein.
  - BEISPIEL: PC wurde am 18ten des Monats mit Intercept X installiert und der Nutzer hat sich 19ten angemeldet -> Es wird eine Lizenz fällig im aktuellen Abrechnungszyklus
  - BEISPIEL: PC wurde am 21ten des letzten Monats mit Intercept X installiert und der User hat sich am 21ten des letzten Monats angemeldet, danach aber nicht mehr -> Es wird keine Lizenz im aktuellen Abrechnungszyklus fällig

MSP Lizenzierung – FAQ

Phish Threat:

- Wir rechnen die Anzahl der einzigartigen Nutzer, die eine Kampagne im aktuellen Abrechnungsmonat erhalten haben.
  - BEISPIEL: MSP hat 3 Kunden mit jeweils 50 Nutzern. Jeder Nutzer erhält 2 Kampagnen im aktuellen Abrechnungsmonat - > Es werden 150 Lizenzen berechnet im aktuellen Abrechnungsmonat (3*50)

Server:

- **Advanced Lizenzen** können nur genutzt werden, wenn die Advanced Funktionen für das genutzte Server OS unterstützt werden. Liste der unterstützen Features pro Server OS: https://community.sophos.com/kb/en-us/113278

XG Firewall:

- **Jede XG, die im aktuellen Abrechnungsmonat aktiv ist, wird eine Lizenz nutzen** (Aktiv -> sendet Daten)
- **Active/Passive HA Cluster** -> Es wird nur 1 Lizenz benötigt für die active XG.
  - Monatliche Lizenzen enthalten den Enhanced Support, daher sind aktive und passive XG abgedeckt
  - APs und REDs – Sofern für der XG ein gültiger Servicer Vertrag besteht, sind RED and Aps abgedeckt
- **Virtuelle Basis Lizenz ändern** -> bitte passende Upgrade SKU bestellt werden und Key auf der XG einspielen. Danach die virtuelle Machine neu starten.

MSP Lizenzierung – FAQ

Managed Threat Response:

- MTR Service greift nur auf Daten zu, die erfasst wurden während MTR aktiviert war. Daher muss MTR bereits aktiv sein, um eine Bedrohung ausführlich analysieren zu können. Es kann nicht nachträglich eingeschaltet werden, um Kosten zu sparen.

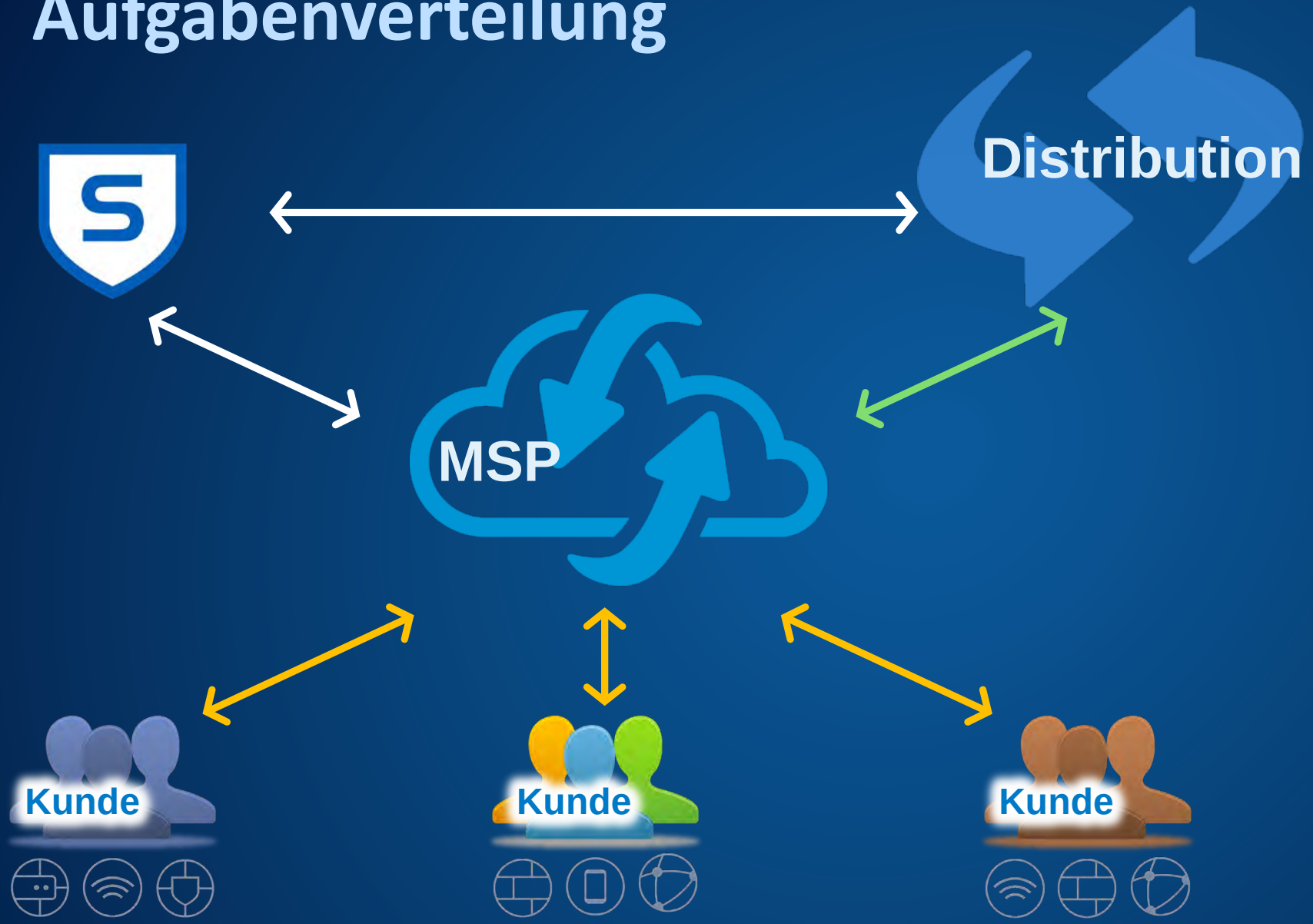
Cloud Optix:

- Lizenziert pro **Cloud Asset**

  Definition: Cloud Asset meint eine einzelnen virtuelle Machinen Instanz, inclusive jeder Server oder Datenbank Instanz, die in einer Cloud Umgebung läuft, die vom Service profitiert oder auf dessen Konfiguration vom Service zugegriffen wird.

  Zur Zeit wird folgendes als Clou Asset gezählt:
  AWS EC2, AWS RDS, Azure VM, Azure SQL Server, Azure DB Server, Google VM, Google SQL, Kubernetes Nodes
  Um Duplizierung zu vermeiden, werden K8s Knoten nicht gezählt, wenn sie bereits als AWS EC2 VM / Azure VM / GCP VM gezählt wurden.

Aufgabenverteilung



Sophos

- Rechtliche Beziehung mit MSP
- Schulung und Zertifizierung der MSP
- Synchronized Security
- Level 2 Support für MSP

Distributor

- Übernahme Hardware-Logistik
- Bereitstellung MSP-Bedingungen
- Rechnungsstellung an MSP
- Zahlung an Sophos

MSP

- Level 1 Support für Kunden
- Bereitstellung und Konfiguration
- Rechnungsstellung an Kunden
- Kauf über Distribution

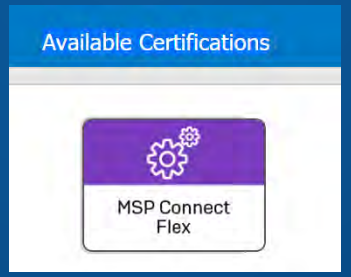
Der Weg zum MSP Connect Flex Partner

SOPHOS
MSP Connect Flex

Managed Services Geschäfts - Modell

MSP Connect Anmeldung

Partner Portal -> Training & Certification:



Erforderliche Sales consultant Trainings:

Sales fundamentals (SC 01)

Sophos MSP Connect - Sales Consultant (MSP01)

Sophos & Distributor genehmigen monatliche Abrechnung



Anmeldung unter: www.Sophos.de/msp

SOPHOS

XG Firewall Hardware Bestellung/Inbetriebname

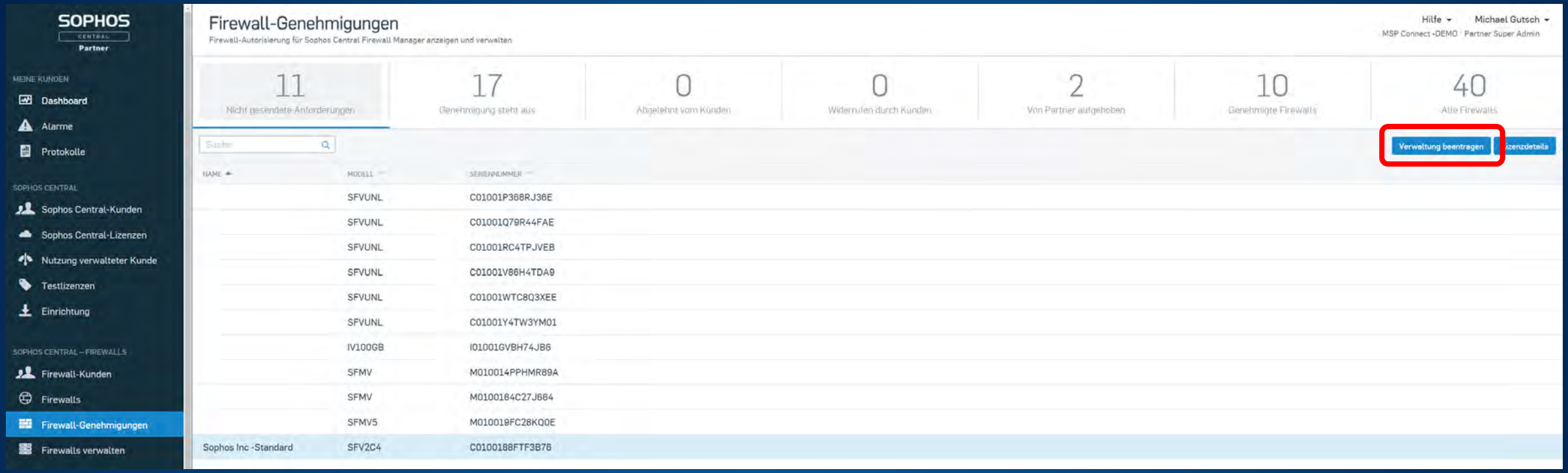
SOPHOS

Hardware - Bestellung

- Hardware muss vorab gekauft werden – Keine monatliche Abrechnung verfügbar
- Hardware unterliegt unseren gewöhnlichen Bestellprozessen und Discount-Richtlinien
- Rabatte auf HW richten sich nach dem Partnerstatus im Sophos Partner-Programm.
- Projektmeldung ist bei Bestellungen für MSP Hardware möglich ohne Nennung des Endkunden
  - Bei HaaS (MSP Besitzt die Hardware) -> ohne Nennung de
  - Projektmeldung über Formular bei der Distribution

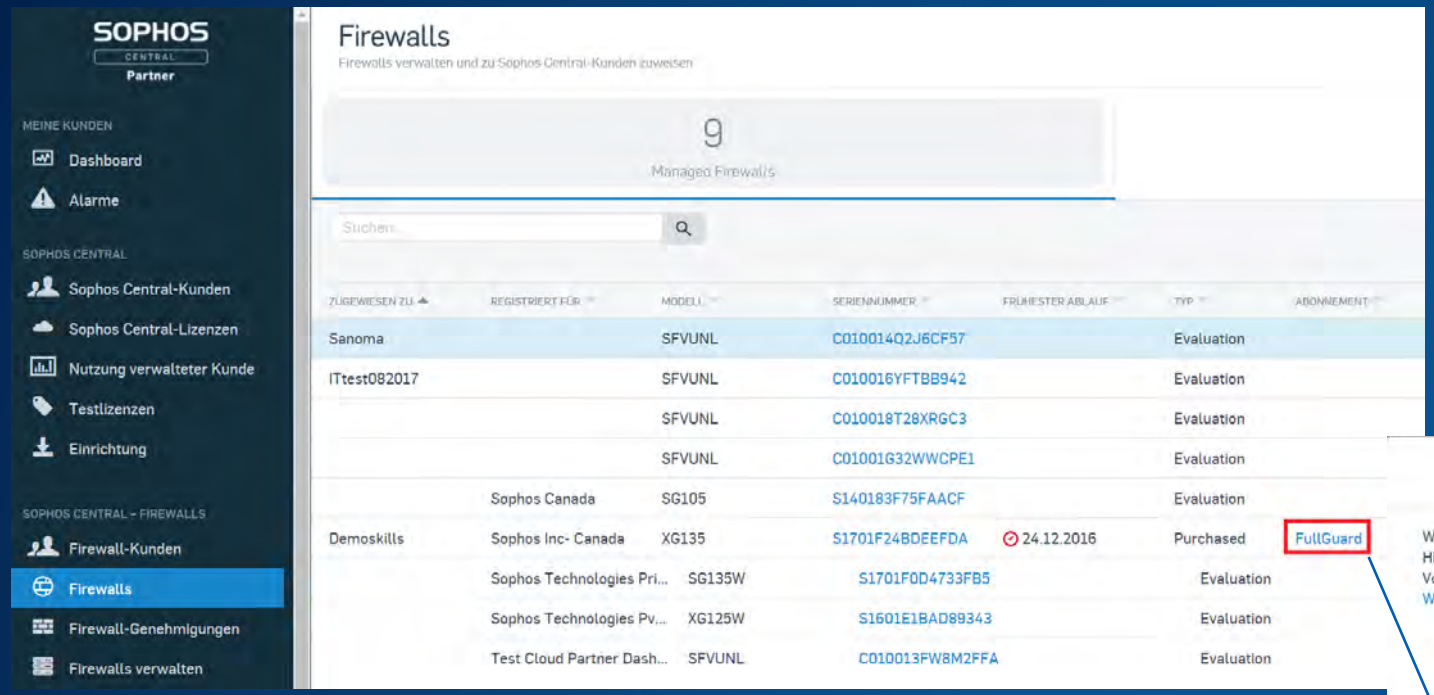


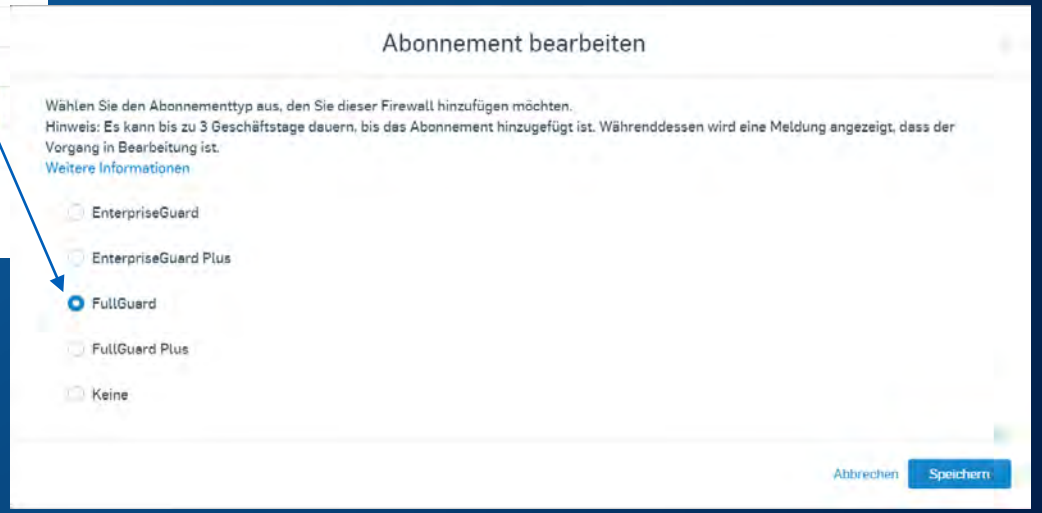
XG FW Managemnt Zugang einrichten



- Sie müssen nun zum Firewall Genehmigungs Menü navigieren und die Genehmigung für das Managen der Firewall anfordern **->** die Anfrage wird an die Email Adresse Ihrer Sophos ID gehen, die genutz wurde, um die Firewall zu registrieren. Der Empfänger muss dann diese genehmigen,
  - Die Anfrage wird an Ihren Kunden gehen, wenn der Kunde diese besitzt und der Kunde diese registriert hat
  - **Oder** an die Email der Sophos ID, auf die die XG registriert wurde (deswegen empfehlen wir eine gemeinsame Sophos ID für Ihre Organisation, siehe Schritt 2. Dann genehmigen Sie alle Anfragen in einer Sophos ID)

Monatliche Firewall Lizenzen - Bestellprozess

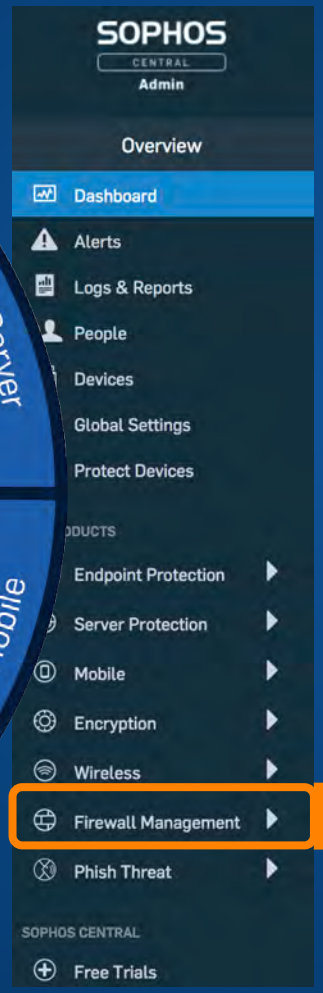


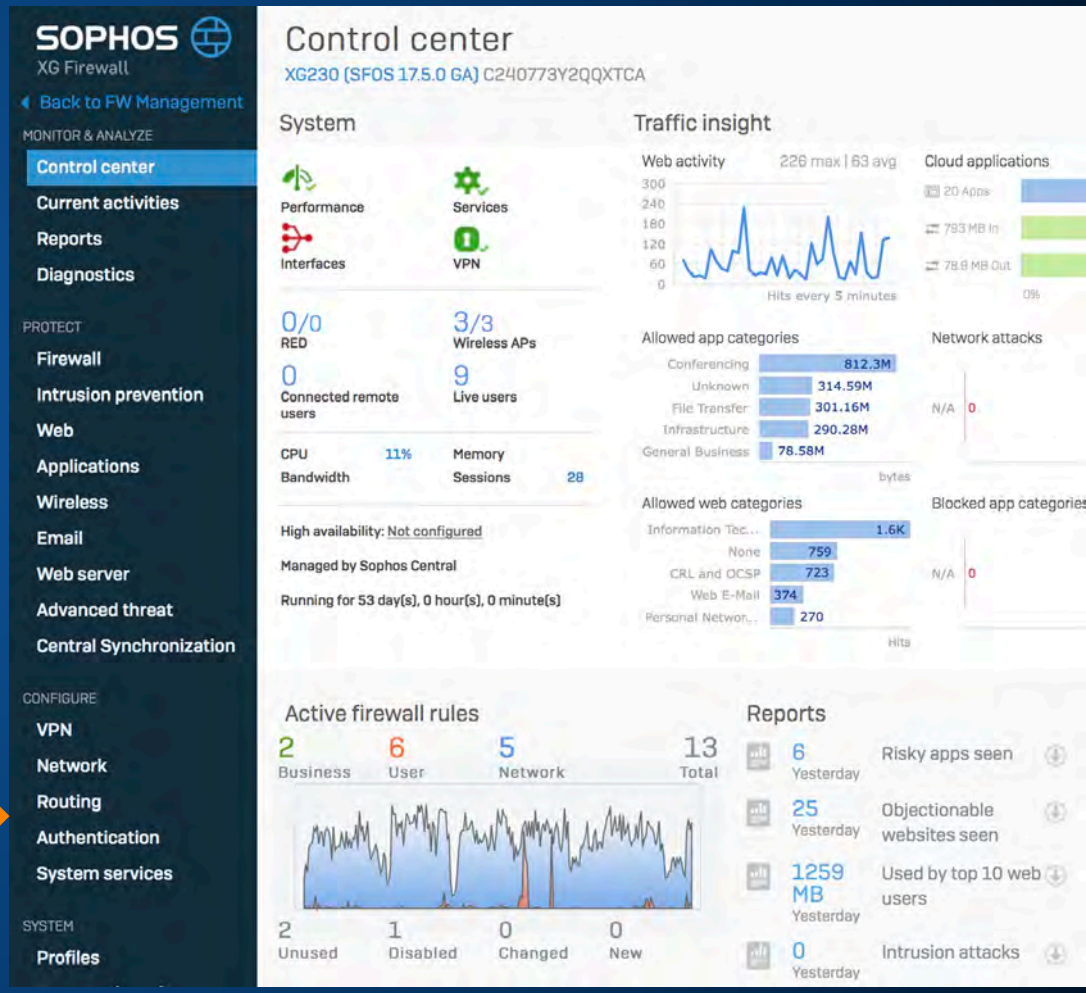


- Wenden Sie den Lizenzschlüssel in Ihrem Mysophos account an.
- Nachdem Sie die XG hinzugefügt und registriert haben, können Sie diese nun mit dem Sophos Central Firewall Manager (SCFM) verwalten.
- Dieses Video zeigt Ihnen, wie Sie die XG im **Sophos Central Firewall Manager** aufsetzen: LINK
- Anleitung zum Sophos Central Firewall Manager: Sophos XG Firewall: Information on managing customer's firewall through Sophos Central Firewall Manager: https://community.sophos.com/kb/en-us/123715

Central Admin XG Firewall Management v1







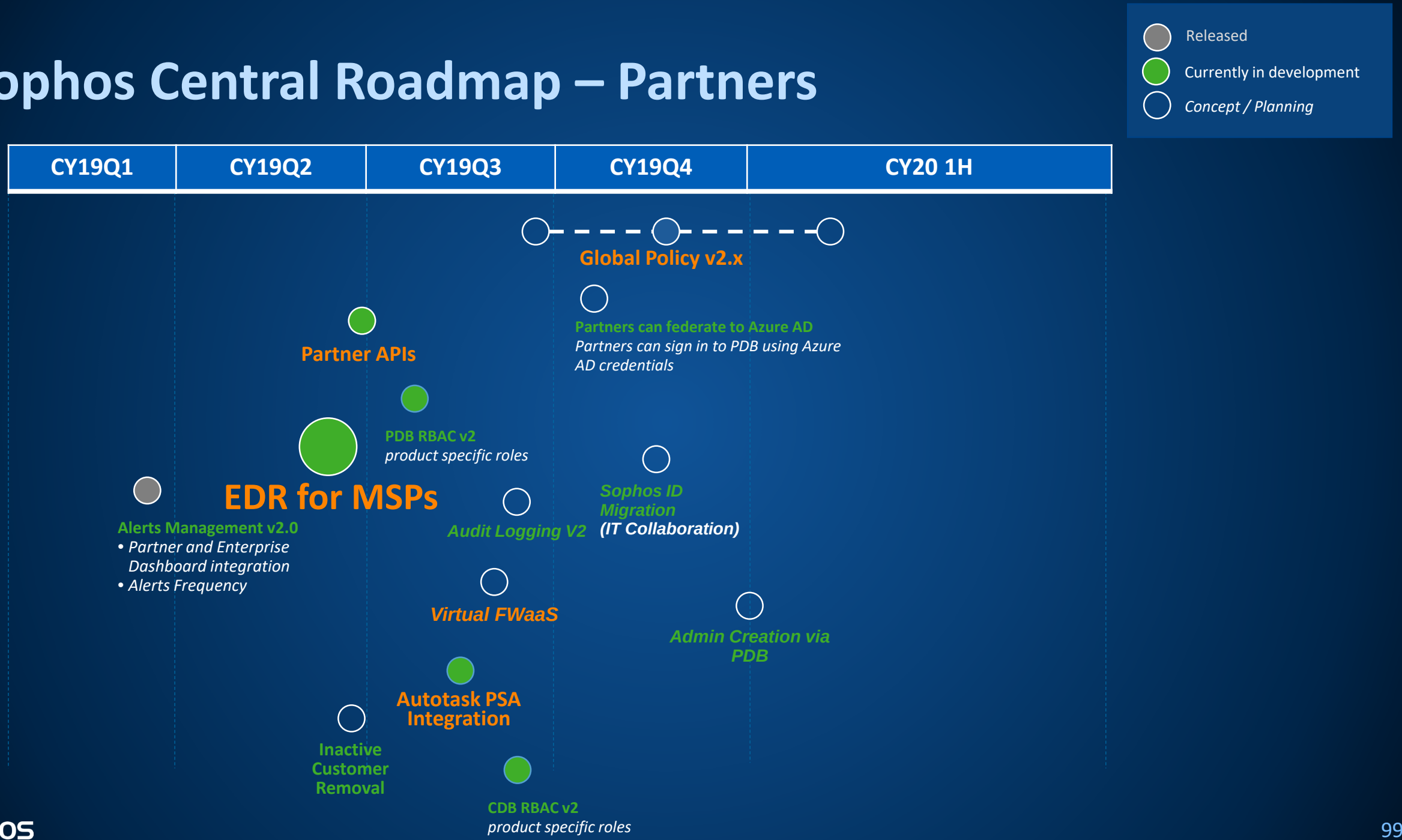
MSP Roadmap

Top Roadmap Prioritäten



- Partner Usability
- 3rd Party Integration
  - Provisioning
  - RMM integration
  - Autotask
- Globales Management
- Virtual Firewall as a Service (VFWaaS)
- Partner RBAC v2

Sophos Central Roadmap – Partners



MSP Informationen

SOPHOS

MSP Hub auf dem Partner Portal

- MSP Connect Program
- MSP Program Overview
- MSP Connect FAQs
- MSP Connect Flex Licer
- MSP Connect Flex XG M
- MSP Connect Partner L

Get Pricing
Based in the U.S.A., C
Click here to access p
If you are based anyw
Sophos account mana

Partner Dashboard

The intuitive Sophos Ce
and manage all your cu
the video tour to learn h
fantastic resource

MSP Connect Flex Trai

To join the MSP Connec
billings you will need to
Consultant level:

- Sophos and Synchro
- MSP Connect
- Sophos Central

Product Training Cours

Our easy-to-follow cour
need to maximize your
then either the Sales Co
level.

Start Training

Sophos Central Manage

- Set up a Sophos Centr
- Transition a term acc
- Add an administrator
- Remove an administra
- Disable tamper protec
- Set up co-branding fo
- Access MSP Connect
- Access the MSP Conn
- Self-administer in the
- Configure email alert
- Integrate Sophos Cen

Endpoint, Intercept X, Se

- Download the Sophos
- Change a license from
- Change a license from
- Assign or remove end
  including Intercept X
- Deploy Endpoint Prote
  Installer

Demand Gen Campaigns

Use these campaigns with your customers and prospects to grow your Sophos revenue. They give you everything you need to generate leads and progress deals for Sophos solutions. Take advantage of our full-range of co-marketing support to help you maximize the success of your activities.



The Anatomy of a Hack



Cryptojacking



Intercept X


Sophos XG Firewall


Stop the Phishing



EU General Data Protection Regulation (GDPR)


Phish Threat Cross-Sell


Encryption Cross-Sell


Mobile Cross-Sell



Sophos Case Studies

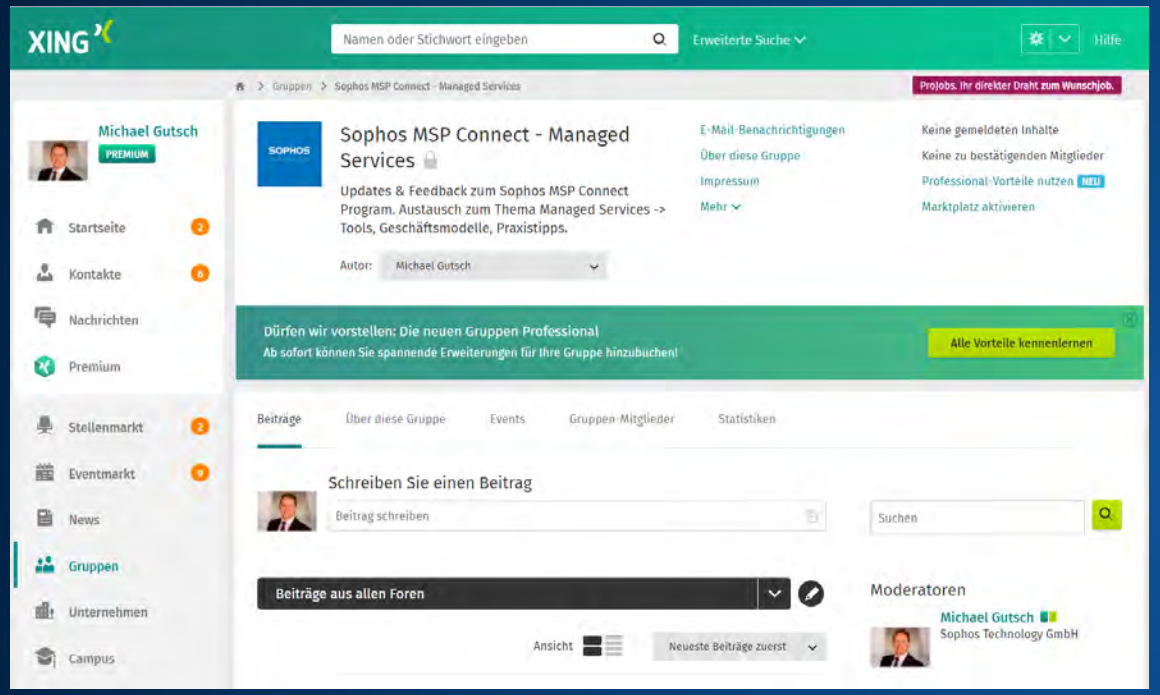


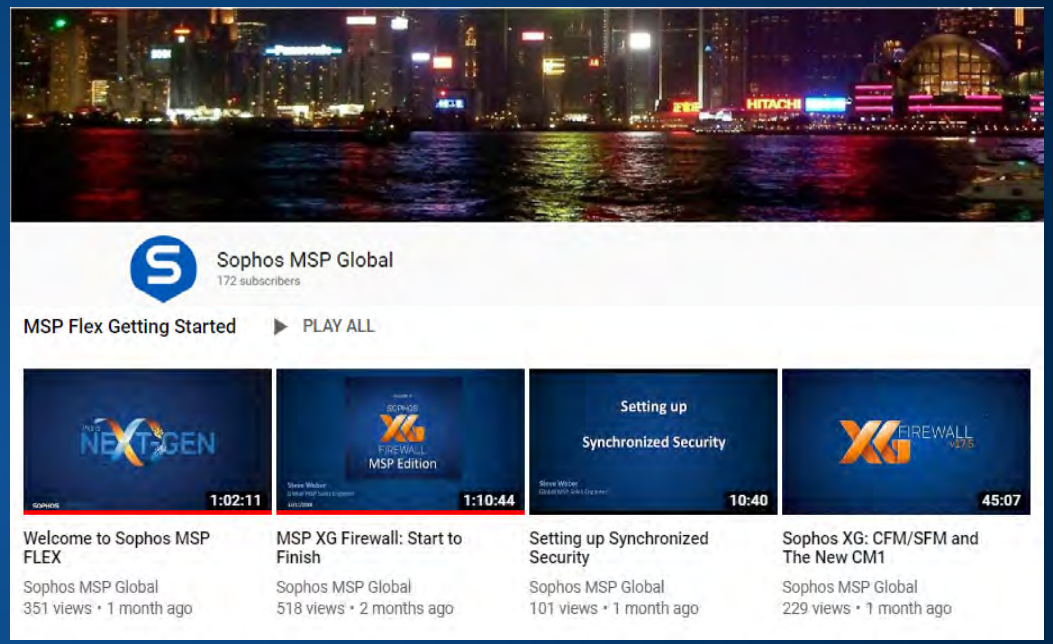
Wanna Ransomware


Sophos UTM 9.5 Expanded

https://partnerportal.sophos.com

Nehmen Sie an unserer MSP XING Gruppe und unserem YouTube Kanal teil





https://www.xing.com/communities/groups/sophos-msp-connect-managed-services-1bae-1095112

https://www.youtube.com/c/SophosMSPGlobal

Webinar-Reihe Sophos MSP Connect – Monatliche Infos und Tipps

Ab März immer am zweiten Donnerstag im Monat, 14:00-15:00

Webinar-Termine in 2020:

- ✓ Freitag, 14. Februar 2020, 11:30 - 12:30
- ✓ Donnerstag, 12. März 2020, 14:00 - 15:00
- ✓ Donnerstag, 9. April 2020, 14:00 - 15:00
- ✓ weiter geht’s



Sie müssen sich für die ganze Serie nur EINMAL registrieren. Laden Sie auch Ihre Kollegen ein https://register.gotowebinar.com/register/6507285142953475331

SOPHOS

Sophos MSP Team DACH



Scott Barlow
Vice President Global MSP

Scott.Barlow@Sophos.com



Michael Gutsch
Head of MSP CEEMEA

Telefon: +49 611 5858-1679
Mobil: +49 173 90 80 357
Michael.Gutsch@Sophos.com



Andreas Buttler
Channel Account Manager
MSP DACH & Eastern Europe

Telefon: +49 611 5858-1624
Andreas.Buttler@Sophos.com



Lars Arndt
Channel Account Executive
MSP DACH & Eastern Europe

Telefon: +49 611 5858-1504
Mobil: +49 174-3440538
Lars.Arndt@Sophos.com

MSP Team Email Kontakt:
MSP.Sales.DACH@sophos.com

SOPHOS

Managed Services mit Sophos MSP Connect

Ein Anbieter, der Ihren IT Security Bedarf deckt :

- Vereinfachtes Anbieter Management -> reduziert Kosten
- Erweitern Sie Ihr Security Service Angebot -> erhöht den Umsatz
- Nutzen Sie die Automatisierung durch Syncronized Security -> erhöht die Effizienz

Einfache Kundenverwaltung mit Sophos Central:

- Einfach zu nutzen, Cloud basiert, keine on premise management Infrastruktur nötig
- Automatisierung: Script gesteuerte Installation, PSA Integration (Abrechnung), APIs

Flexibles und faires MSP Programm:

- Nutzungsbasierte monatliche Abrechnung-> kein Bestellungen, spart Zeit
- Einfacher Start, kein Minimum Umsatz erforderlich
- Volumen basierte Rabatte, aggregierte Abrechnung -> steigende Profitabilität

Wie gehts weiter?

- Melden sie sich zum MSP Programm an unter:
  - https://partners.sophos.com/English/register_email.aspx
  - Das Sophos MSP Team kontaktiert Sie und führt Sie durch den Onboarding Prozess

- Kontaktieren sie uns bei weiteren Fragen unter:
  - MSP.Sales.DACH@Sophos.com (DACH Partner)


Q
A

SOPHOS

Cybersecurity made simple.