Sophos XG v17

Next-Generation Firewall

Stefan Burkhardt
klopfer datennetzwerk gmbh
29. Mai 2018

Agenda

- Überblick Sophos XG v17
- Hardware, Lizenzen und Integration
- Funktionen und Module
- Synchronized Security - eine Firewall, die Bescheid weiß
- Den Gegner ernst nehmen - moderne Abwehrmaßnahmen
- Live-Demo: XG in Aktion

- umfassende Next-Generation Firewall Protection
- blockiert unbekannte Bedrohungen
  - IPS, ATP, Sandboxing, dualer Antivirus, Web & App Control
- reagiert automatisch auf Vorfälle
  - identifiziert die Quelle einer Infektion automatisch und kann Zugriffe beschränken
- deckt verborgene Risiken auf
  - erkennt unbekannte Bedrohungen und verdächtiges Verhalten
- Kommunikation zwischen Firewall und Endpoint (Security Heartbeat)
- leistungsstark, effektiv, schnell
  - basieren auf Intel-Multicore-Technologie und SSDs
- einfache Verwaltung mehrerer Firewalls
- umfangreiches Reporting

Was ist neu in XG v17?

- verbesserter Einrichtungsassistent
- How-To-Anleitungen
- Keywords in Webfiltern
- verbesserte IPS-Richtlinien, auch speziell für Linux
- optimierte Firewall-Regeln und umfassendes Reporting
- Testsimulator für Regeln und Richtlinien
- VPN: IKEv2-Unterstützung, Wildcard, optimierte NAT-Regeln
- Snychronized Security in Discover-Modus
- Synchronized AppControl
- HA-Szenarien in Microsoft Azure

LIZENZIERUNG

Bereitstellung

Hardware

Sophos XG-Geräten

Software

Intel-kompatible Hardware

Virtuell

HyperV
Vmware
XenServer
KVM

Cloud

Azure

- Essential Firewall wird Base License
- Wireless Protection und VPN-Funktionen bereits integriert
- nicht mehr kostenlos, aber in Hardware-Preis enthalten

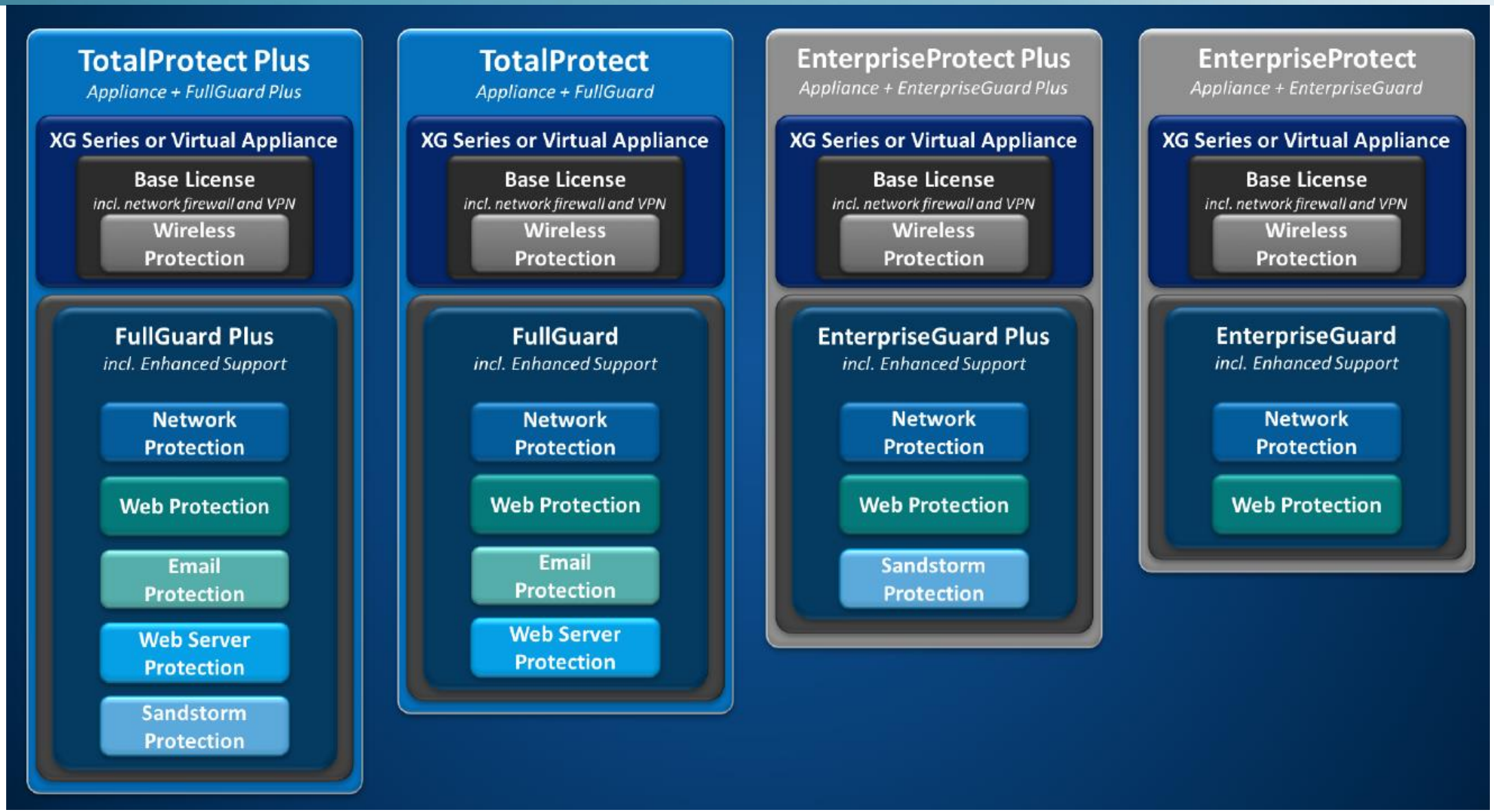
UTM Essential Firewall	XG Firewall Base License
Kosten: im Hardware Preis enthalten **Kosten**: In der SW/VM Appliance enthalten	**Kosten**: Im Hardware Preis enthalten **Kosten**: Einmaliger Preis für SW/VM Appliance
Enthält: • Firewall • Basic VPN (L2TP, PPTP)	**Enthält:** • Firewall • VPN (IPsec and SSL VPN) – keine Renewals notwendig – IPSec Clients separat erhältlich • Wireless Protection

- doppelte IP-Adresszählung für den gleichen Benutzer
- Anpassung aufgrund der neuen Base License

Sophos UTM	
Hardware	SW / Virtual
One-time payment	Per IP/users
Incl. Essential Firewall	Incl. Essential Firewall

XG Firewall	
Hardware	SW / Virtual
One-time payment	Per (v)Core / (v)RAM
Incl. Base License	One-time fee for Base

Lizenzierung Module



Sophos-Support – einfach und umfassend

Wir entwickeln Produkte, die einfach und gleichzeitig umfassend sind. Diesen Ansatz verfolgen wir auch bei unserem Support. Unser Angebot reicht von technischem Basis-Support bis hin zu Support-Plänen mit direktem Kontakt zu Senior Support Engineers und kundenspezifischen Services.

Lizenznamen	Standard Im Kaufpreis enthalten	Enhanced In allen Bundles enthalten	Enhanced Plus
Support Per Telefon und E-Mail	90 Tage inklusive (nur zu Geschäftszeiten)	Inklusive (24x7)	VIP-Zugriff (24x7)
Sicherheitsupdates und Patches Über die Lebensdauer des Produkts	Enthalten in aktiver Software-Subscription	Enthalten in aktiver Software-Subscription	Enthalten in aktiver Software-Subscription
Software-Feature-Updates und Upgrades	90 Tage inklusive	Inklusive	Inklusive
Beratung & Consulting Remote-Beratung zu Ihrer Firewall-Konfiguration und -Sicherheit durch einen Sophos Senior Technical Support Engineer			Inklusive (bis zu 4 Stunden)
Garantie und Vorabaustausch-Service Für alle Hardware-Appliances	1 Jahr (Return/Replace)	Vorabaustausch (max. 5 Jahre)	Vorabaustausch (max. 5 Jahre)
Technical Account Manager Persönlicher Ansprechpartner im technischen Support		Optional (Aufpreis)	Optional (Aufpreis)

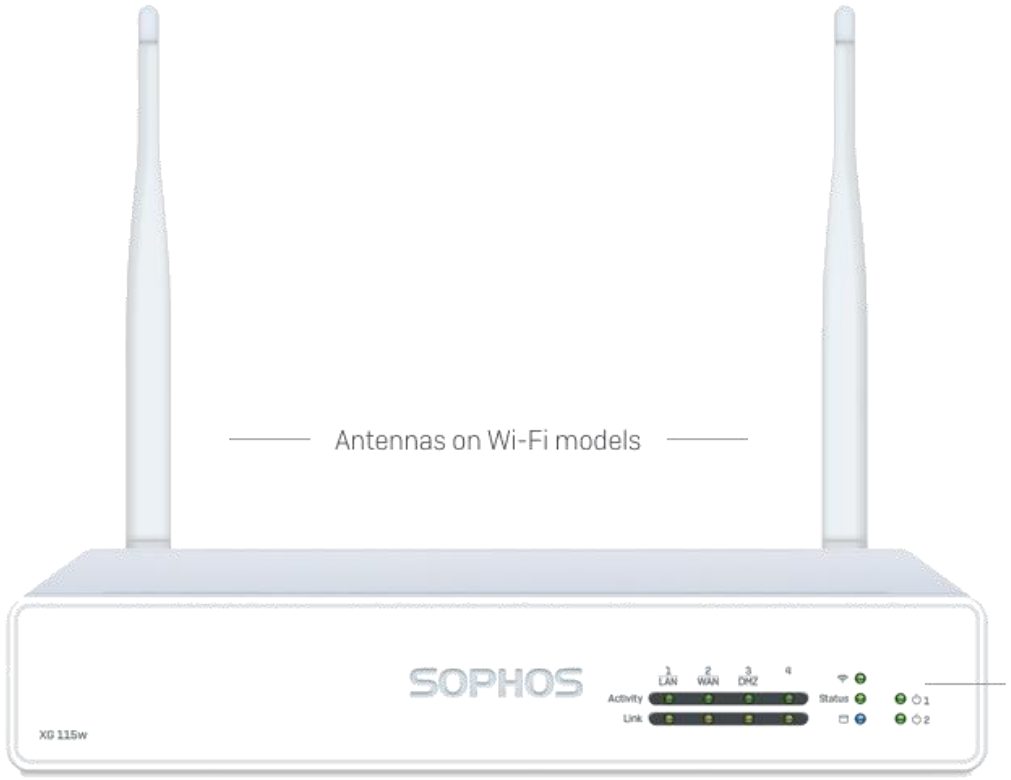
- **Active / Active**
  - für jede Appliance ist eine entsprechene Lizenz erforderlich
  - für jede Appliance muss ein separater Support-Plan gekauft werden

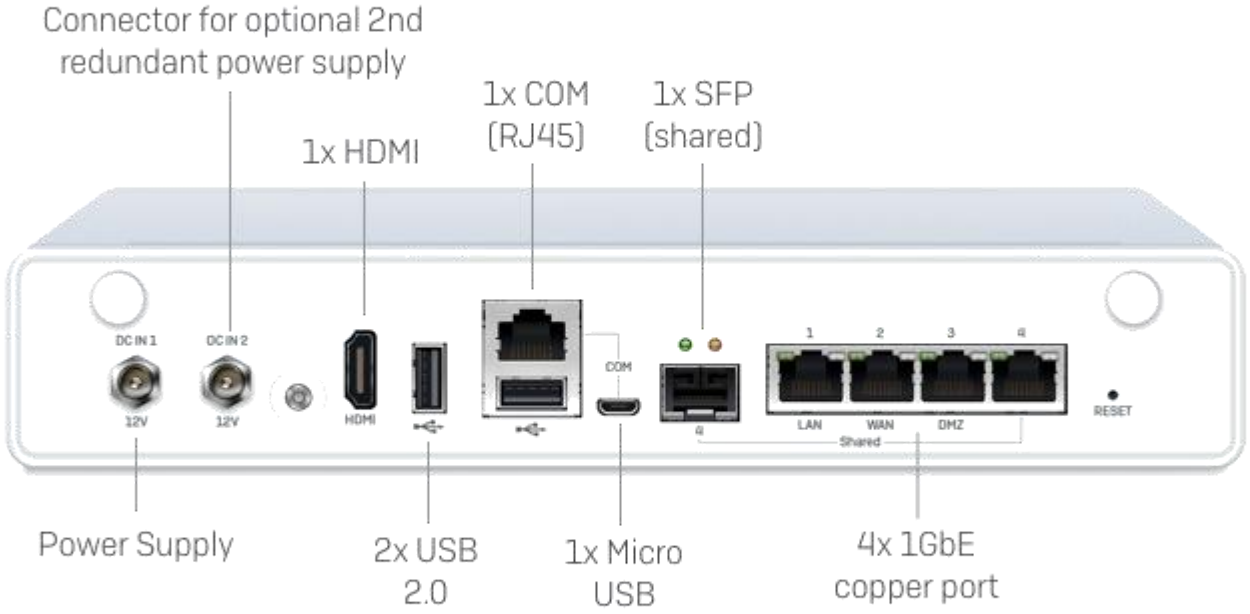
- **Active / Passive**
  - Subscription nur einmal erforderlich
  - technischer Support für passive Einheit, wenn Enhanced oder Enhanced Plus erworben wurde
  - Enhanced Plus ist erforderlich, wenn für die passive Einheit Austausch und erweiterte Garantie gewünscht ist

HARDWARE

- Desktop-Modelle
  - XG85, XG105(w), XG115(w), XG125(w), XG135(w)
  - neue Revision 3 (April 2018)
- 1U-Modelle
  - XG210, XG230, XG310, XG330, XG430, XG450
  - Revision 2
- 2U-Modelle
  - XG550, XG650, XG750
  - Revision 2

Desktop-Appliances Rev. 3





- redundante Stromversorgung
- Performance-Steigerung durch neue CPU
- integriertes AC-WLAN
- Management über microUSB oder COM
- Monitor-Verbindung über HDMI

- XG85(w)
  - 4xGigabit Kupfer, 2 USB
  - MicroUSB, COM Management
  - **802.11ac WiFi-Option**
- XG105 / 115(w)
  - 4xGigabit Kupfer, 2 USB, **HDMI**
  - **1x SFP-Port, z.B. für DSL-Modem**
  - **redundante Stromversorgung**
  - MicroUSB, COM Management
  - **802.11ac WiFi-Option**
- XG125 / 135(w)
  - 8xGigabit Kupfer, 2 USB, **HDMI**
  - **1x SFP-Port, z.B. für DSL-Modem**
  - **redundante Stromversorgung**
  - **Erweiterungseinheit für 3G/4G-Modul bzw. 2. WLAN-Modul**
  - MicroUSB, COM Management
  - 802.11ac Wi-Fi Option

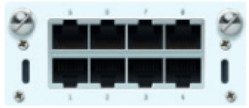
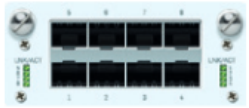
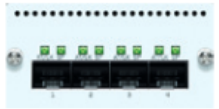
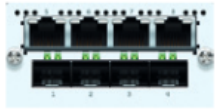
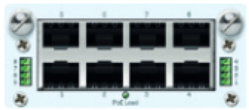
- 1U-Modelle: XG2xx, XG3xx, XG4xx
- 2U-Modelle: XG550, XG650, XG750
- integrierte Kupfer- und Glasfaserports
- LAN Bypass-Funktion
- modulare FlexiPort-Erweiterungen, z.B. 10GbE-SFP+
- redundante Stromversorgung (optional, 2 U-Modelle Serie)
- ab XG450 zwei redundante SSD (2U-Modelle: HotSwap RAID1)
- Komponentenaustausch im laufenden Betrieb (2U-Modelle)

Übersicht Modelle

Modell			Technische Spezifikationen			Durchsatz[1]			
	Revision Nr.	Formfaktor	Ports/Slots (max. Ports)	w-Modell 802.11 wireless	Austauschbare Komponenten	Firewall (MBit/s)	VPN (MBit/s)	NGFW (MBit/s)	Antivirus-Proxy (MBit/s)
XG 85(w)	3	Desktop	4	a/b/g/n/ac	--	3.000	225	310	360
XG 105(w)	3	Desktop	4	a/b/g/n/ac	opt. ext. Stromvers.	3.500	360	480	450
XG 115(w)	3	Desktop	4	a/b/g/n/ac	opt. ext. Stromvers.	4.000	490	1.000	600
XG 125(w)	3	Desktop	9/1 (9)	a/b/g/n/ac	opt. ext. Stromvers., 3G/4G	6.500	700	1.100	700
XG 135(w)	3	Desktop	9/1 (9)	a/b/g/n/ac	opt. ext. Stromvers., 3G/4G, WLAN*	8.000	1.180	1.200	1.580
XG 210	3	1U	8/1 (16)	--	opt. ext. Stromvers.	16.000	1.450	2.200	2.300
XG 230	2	1U	8/1 (16)	--	opt. ext. Stromvers.	20.000	1.700	3.000	2.800
XG 310	2	1U	12/1 (20)	--	opt. ext. Stromvers.	28.000	2.750	4.000	3.300
XG 330	2	1U	12/1 (20)	--	opt. ext. Stromvers.	33.000	3.200	5.500	6.000
XG 430	2	1U	10/2 (26)	--	opt. ext. Stromvers.	41.000	4.800	6.000	6.500
XG 450	2	1U	10/2 (26)	--	opt. int. Stromvers.	50.000	5.500	7.500	7.000
XG 550	2	2U	8/4 (32)	--	Stromvers., SSD, Lüfter	65.000	8.400	9.000	10.000
XG 650	2	2U	8/6 (48)	--	Stromvers., SSD, Lüfter	85.000	9.000	10.000	13.000
XG 750	2	2U	8/8 (64)	--	Stromvers., SSD, Lüfter	100.000	11.000	11.800	17.000

* zweite WLAN-Modul-Option nur auf 135w (XG v17 MR6 erforderlich)

XG Erweiterungsmodule

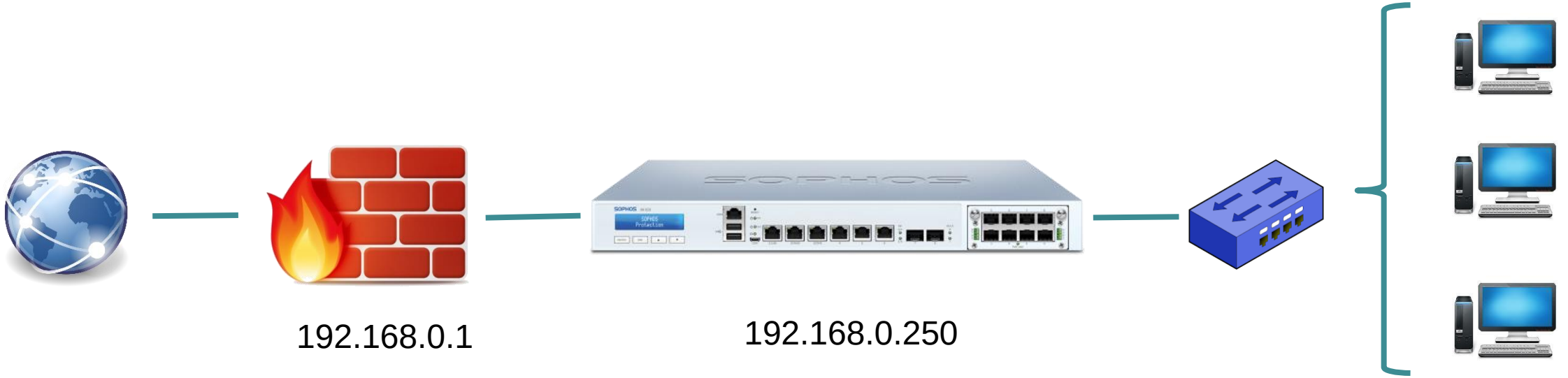
FleXi-Port-Module für 1U		FleXi-Port-Module für 2U	
	8-Port GbE Kupfer FleXi-Port-Modul (nur für SG/XG 2xx/3xx/4xx)		8-Port GbE Kupfer FleXi-Port-Modul (nur für XG 750 und SG/XG 550/650 Rev. 2)
	8-Port GbE SFP FleXi-Port-Modul (nur für SG/XG 2xx/3xx/4xx)		8-Port GbE SFP FleXi-Port-Modul (nur für XG 750 und SG/XG 550/650 Rev. 2)
	2-Port 10 GbE SFP+ FleXi-Port-Modul (nur für SG/XG 2xx/3xx/4xx)		2-Port 10 GbE SFP+ FleXi-Port-Modul (nur für XG 750 und SG/XG 550/650 Rev. 2)
	4-Port 10 GbE SFP+ FleXi-Port-Modul (nur für SG/XG 2xx/3xx/4xx)		4-Port 10 GbE SFP+ FleXi-Port-Modul (nur für XG 750 und SG/XG 550/650 Rev. 2)
	FleXi-Port-Modul, 2-Port 40 GbE QSFP+ (nur für SG/XG 210 Rev. 3 und SG/ XG 230, 3xx und 4xx Rev. 2)		4-Port GbE SFP plus 4-Port GbE Kupfer LAN Bypass FleXi-Port-Modul (nur für XG 750 und XG 550/650 Rev. 2)
	PoE -FleXi-Port-Modul, 4-Port GbE Kupfer (nur für SG/XG 210 Rev. 3 und SG/ XG 230, 3xx und 4xx Rev. 2)		FleXi-Port-Modul, 2-Port 40 GbE QSFP+ (nur für XG 750 und SG/XG 550/650 Rev. 2)
	PoE -FleXi-Port-Modul, 8-Port GbE Kupfer (nur für SG/XG 210 Rev. 3 und SG/ XG 230, 3xx und 4xx Rev. 2)		

Hinweis: Transceiver (Mini-GBICs) sind separat erhältlich.

BEREITSTELLUNG

- Bridge-Modus
  - hinter bestehender Firewall, teilweise mit eingeschränkter Funktion
- Gateway-Modus
  - ersetzt vorhandene Firewall-Lösung
- Mixed-Modus
- Discover-Modus (TAP-Mode)

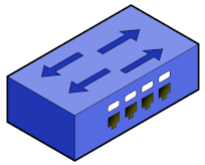
Bridge-Modus



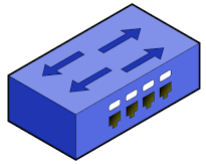
<u>als Layer 2 - Bridge</u>
unterstützt Packet-Inspection, IPS, Antivirus, Antispam

Gateway Modus

LAN 192.168.0.1
DMZ 172.20.56.1
WAN 217.225.101.24



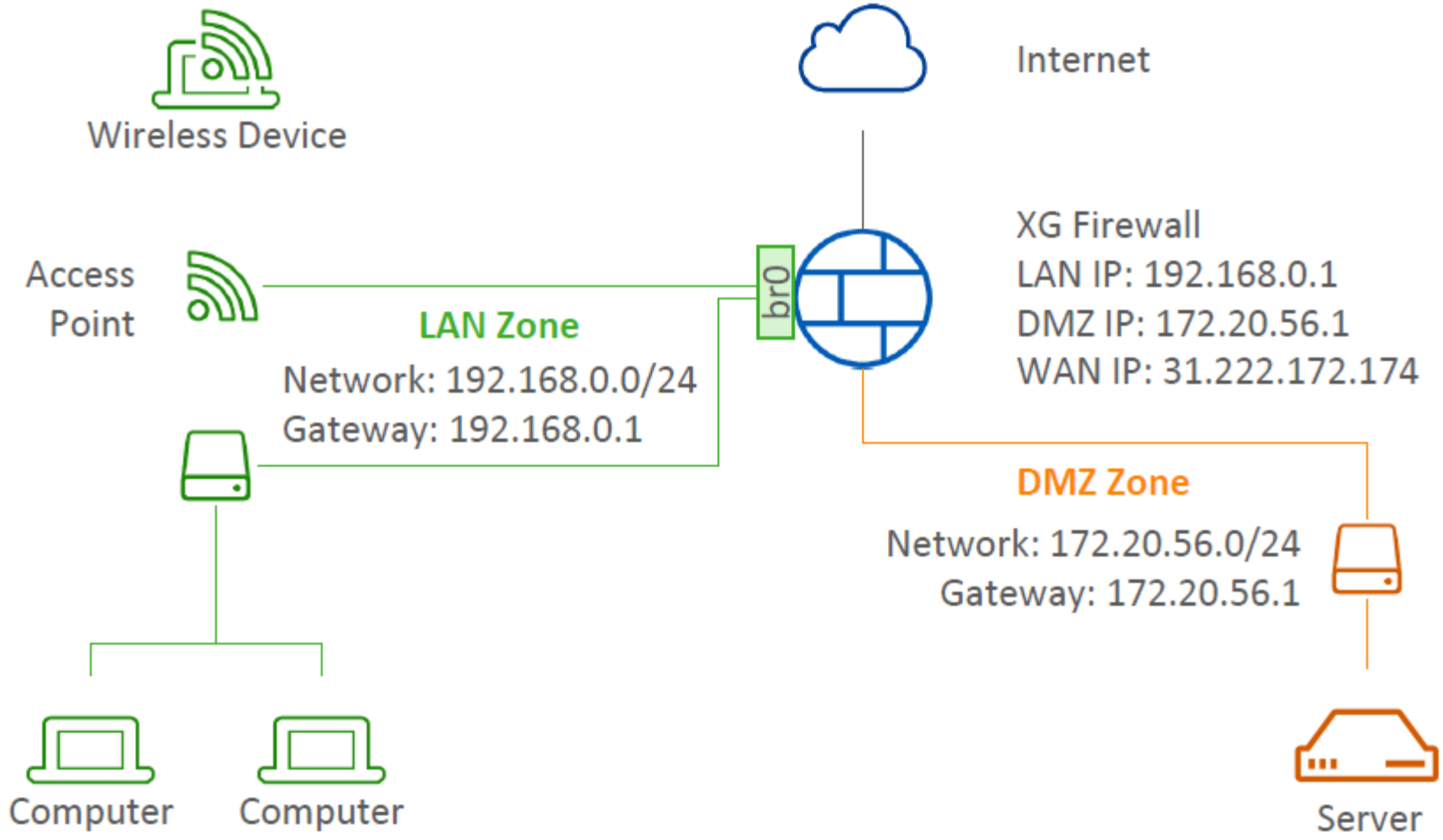
LAN Zone
Network 192.168.0.0 /24
GW 192.168.0.1



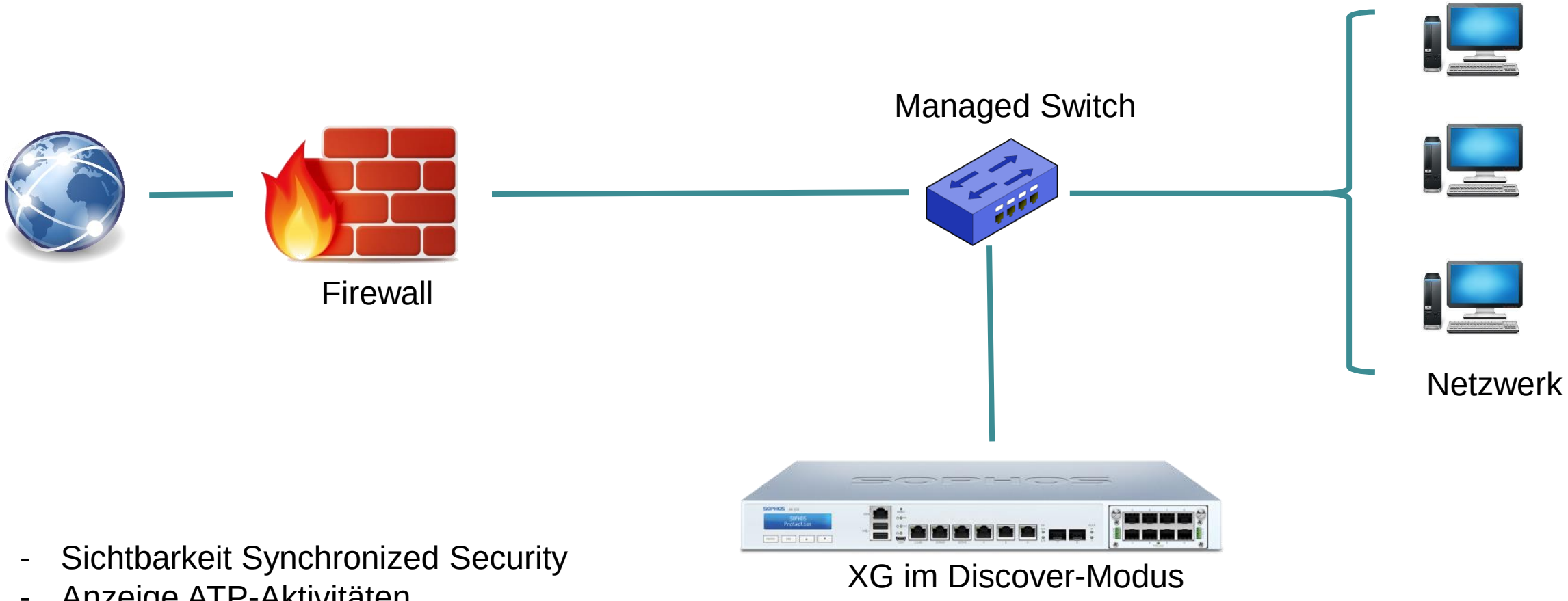
DMZ Zone
Network 172.20.56.0 /24
GW 172.20.56.1

- ersetzt vorhandene Firewall-Lösung
- zonenbasiertes Routing
- VPN-Konzentrator
- Multiple-WAN-Link
- Hochverfügbarkeit

Mixed Mode


Wireless Device
Internet
Access
Point
br0
XG Firewall
LAN IP: 192.168.0.1
DMZ IP: 172.20.56.1
WAN IP: 31.222.172.174
LAN Zone
Network: 192.168.0.0/24
Gateway: 192.168.0.1
DMZ Zone
Network: 172.20.56.0/24
Gateway: 172.20.56.1
Computer
Computer
Server

Discover- / TAP-Modus



- Sichtbarkeit Synchronized Security
- Anzeige ATP-Aktivitäten
- Root Cause Analyse für ATP
- umfassendes Reporting

FUNKTIONEN & MODULE

Funktionen und Module

klopfer datennetzwerk gmbh

Network Protection

- Intrusion Prevention (IPS)
- Advanced Threat Prot. (ATP)
- Security Heartbeat
- RED VPN
- Clientless VPN

Base Firewall

- Stateful Firewall
- User/Netzwerk Regelwerk
- **Wireless**
- **Site-to-Site VPN**
- **Remote VPN**
- Basic QoS

Web Protection

- HTTP/S Proxy
- Dual AntiVirus
- URL Filtering
- Application Control
- Synchronized AppControl

Web Server Protection

- Reverse Proxy
- Web Application Firewall
- Dual Antivirus

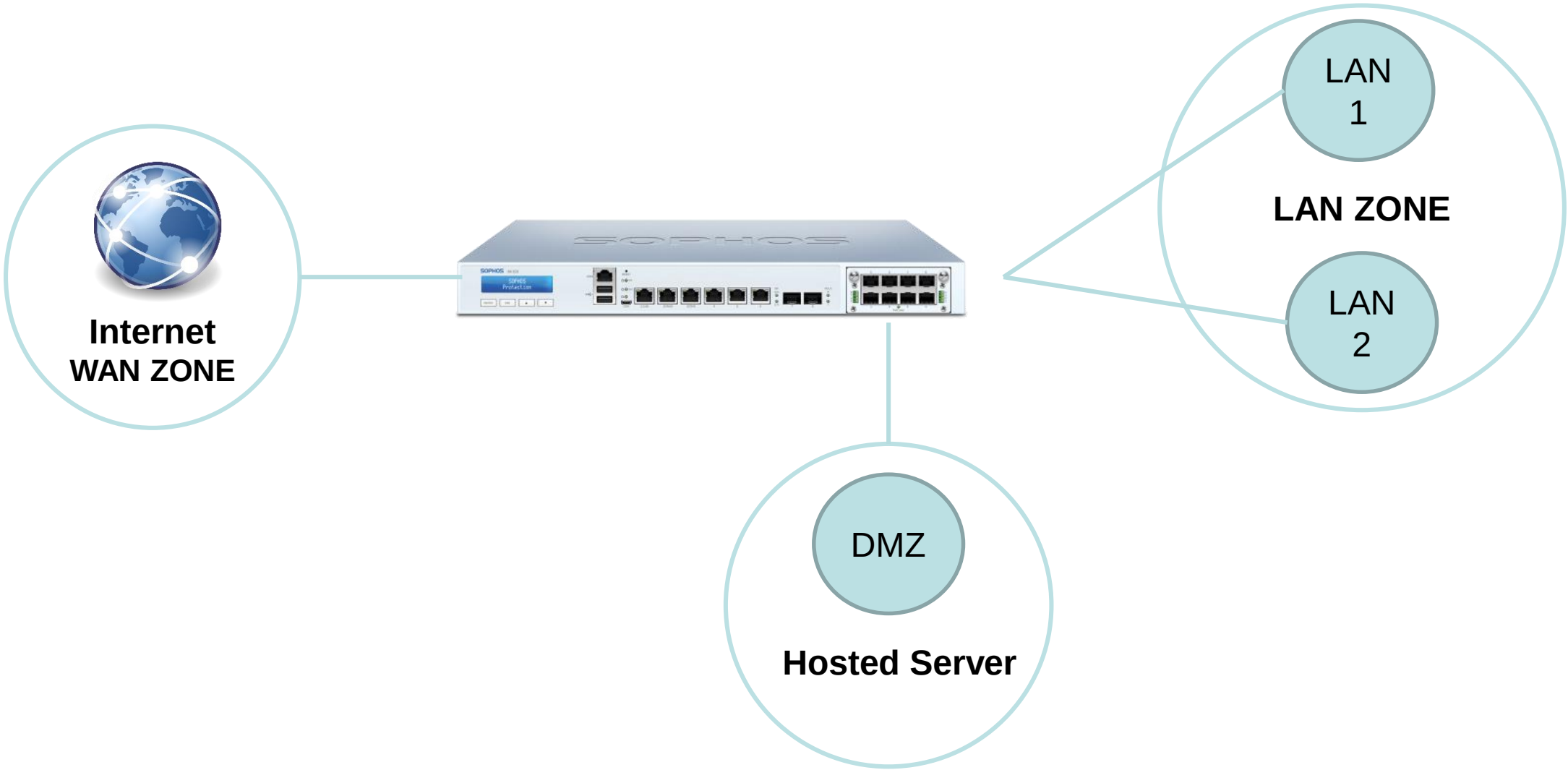
Sandstorm Protection

- Cloud-basierte Sandbox-Lösung
- Erkennen von unbekannten Bedrohungen

Mail Protection

- Anti Spam & Phishing
- Dual AntiVirus
- DLP & Encryption

Zonenkonzept

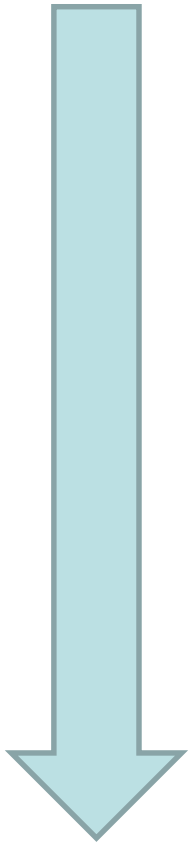


- **Benutzer / Netzwerk-Regel**
  - basiert auf Identitäten, IP/MAC
  - Web Filter
  - ApplicationControl
  - Bandbreitenmanagement (Traffic Shaping)

- **Business Application Regel**
  - Webserver: Web Application Firewall / ReverseProxy
  - Email-Server mit Email Protection
  - interne Server / Dienste via NAT

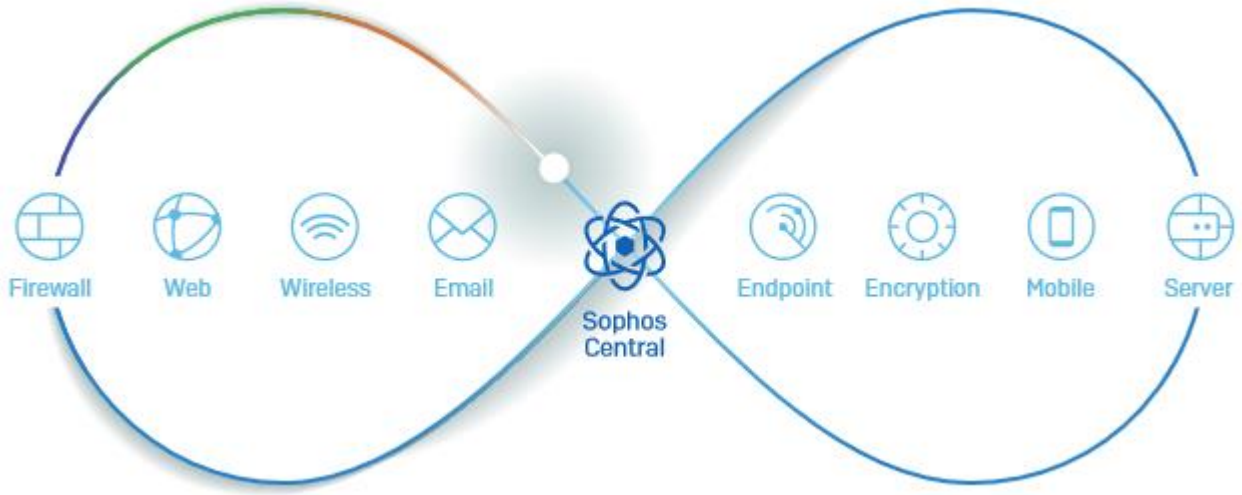
- Active Directory
- eDirectory
- RADIUS
- TACACS+
- LDAP/S

- Clientless User
- SSO
  - Sophos Transparent Authentication Suite
  - Sophos Authentication for Terminal Clients
  - SSO Client (Logonskript auf DC)
  - VPN
  - RADIUS
  - NTLM
- Authentication Agent
- Captive Portal



SYNCHRONIZED SECURITY

Synchronized Security



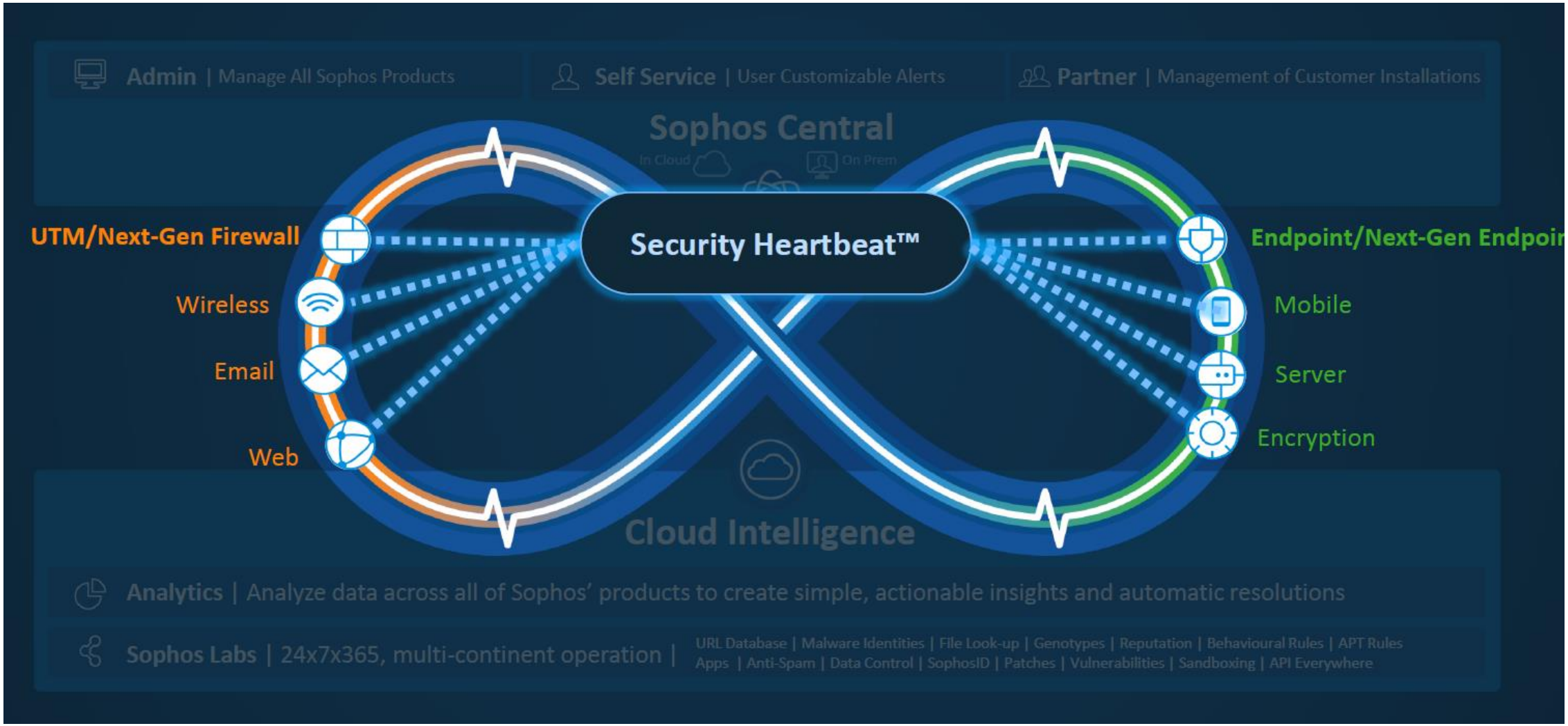
- wachsende Bedrohungslage
- komplexe IT-Infrastrukturen

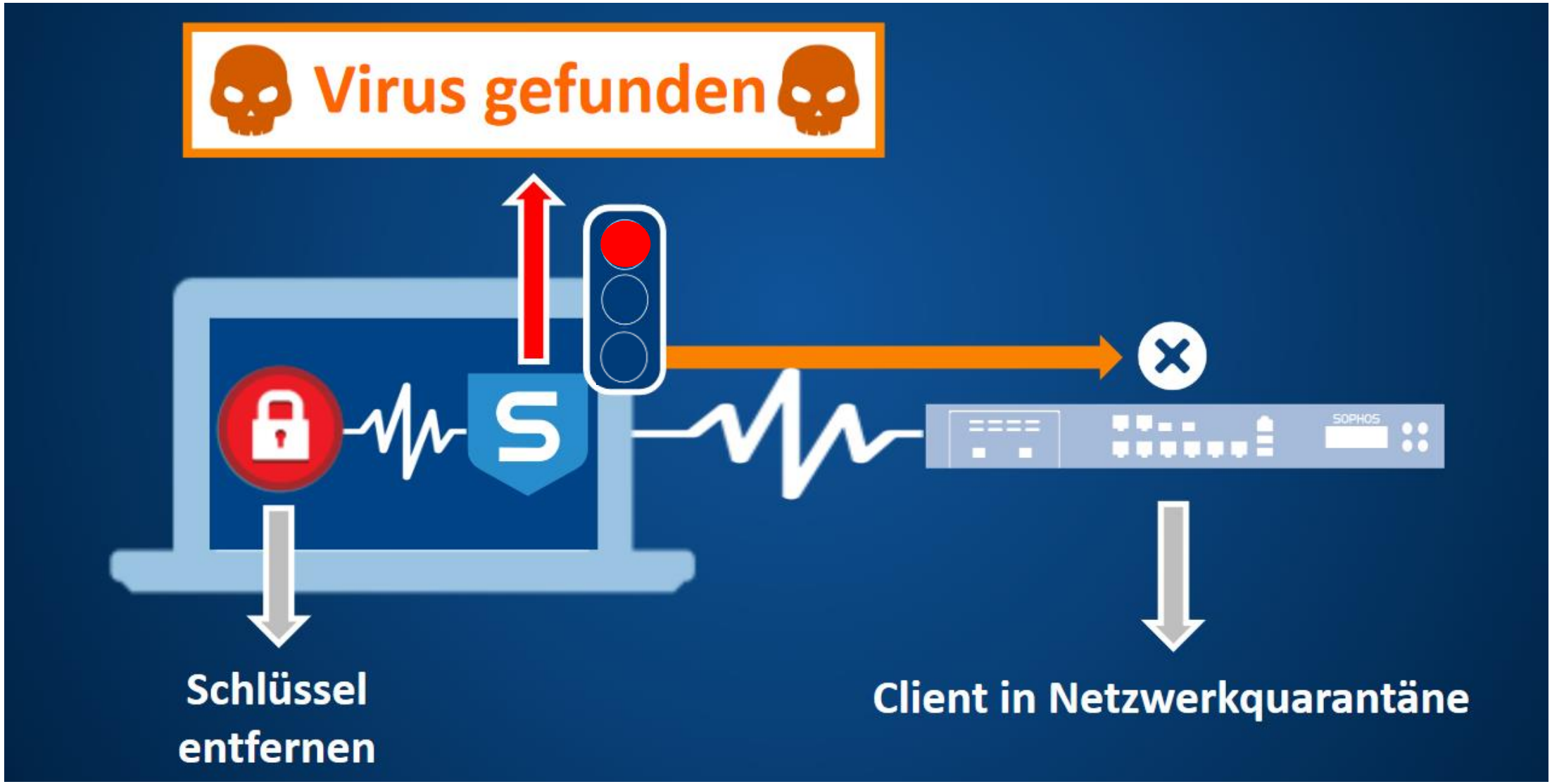
- integrierte Produkte, die dynamisch Bedrohungs-, Integritäts-, Sicherheitsinformationen austauschen
- automatisierte Reaktion auf Ereignisse
- Schutz für alle Systeme und Endgeräte

- Echtzeit-Datenaustausch zwischen Endpoint und Firewall
- Synchronisierung des Sicherheitssystems
  - Informationsaustausch über sicheren Kanal
- schnelle Erkennung moderner Bedrohungen
  - durch Kommunikation wird der Prozess erkannt und gestoppt
- aktive Identifizierung
- automatische Reaktion
  - z.B. Internetverbindung trennen, Client-Isolation, Stonewalling (vsl. v17.2)
- Warnmeldungen in Echtzeit mit Ampel-System

Voraussetzungen:

- Sophos Firewall OS (XG, Software, virtuell, Azure)
- Subscription **Network Protection**
- Sophos Central Endpoint Advanced


Admin | Manage All Sophos Products
Self Service | User Customizable Alerts
Partner | Management of Customer Installations
Sophos Central
In Cloud
On Prem
UTM/Next-Gen Firewall
Wireless
Email
Web
Security Heartbeat™
Endpoint/Next-Gen Endpoir
Mobile
Server
Encryption
Cloud Intelligence
Analytics | Analyze data across all of Sophos' products to create simple, actionable insights and automatic resolutions
Sophos Labs | 24x7x365, multi-continent operation |
URL Database | Malware Identities | File Look-up | Genotypes | Reputation | Behavioural Rules | APT Rules
Apps | Anti-Spam | Data Control | SophosID | Patches | Vulnerabilities | Sandboxing | API Everywhere


Virus gefunden
SOPHOS
Schlüssel entfernen
Client in Netzwerkquarantäne

XG LIVE

FRAGEN?!

Vielen Dank für Ihre Aufmerksamkeit!