

Workshop:



Martin Weiß

Senior Sales Engineer Public

SOPHOS

Kurze Vorstellungsrunde

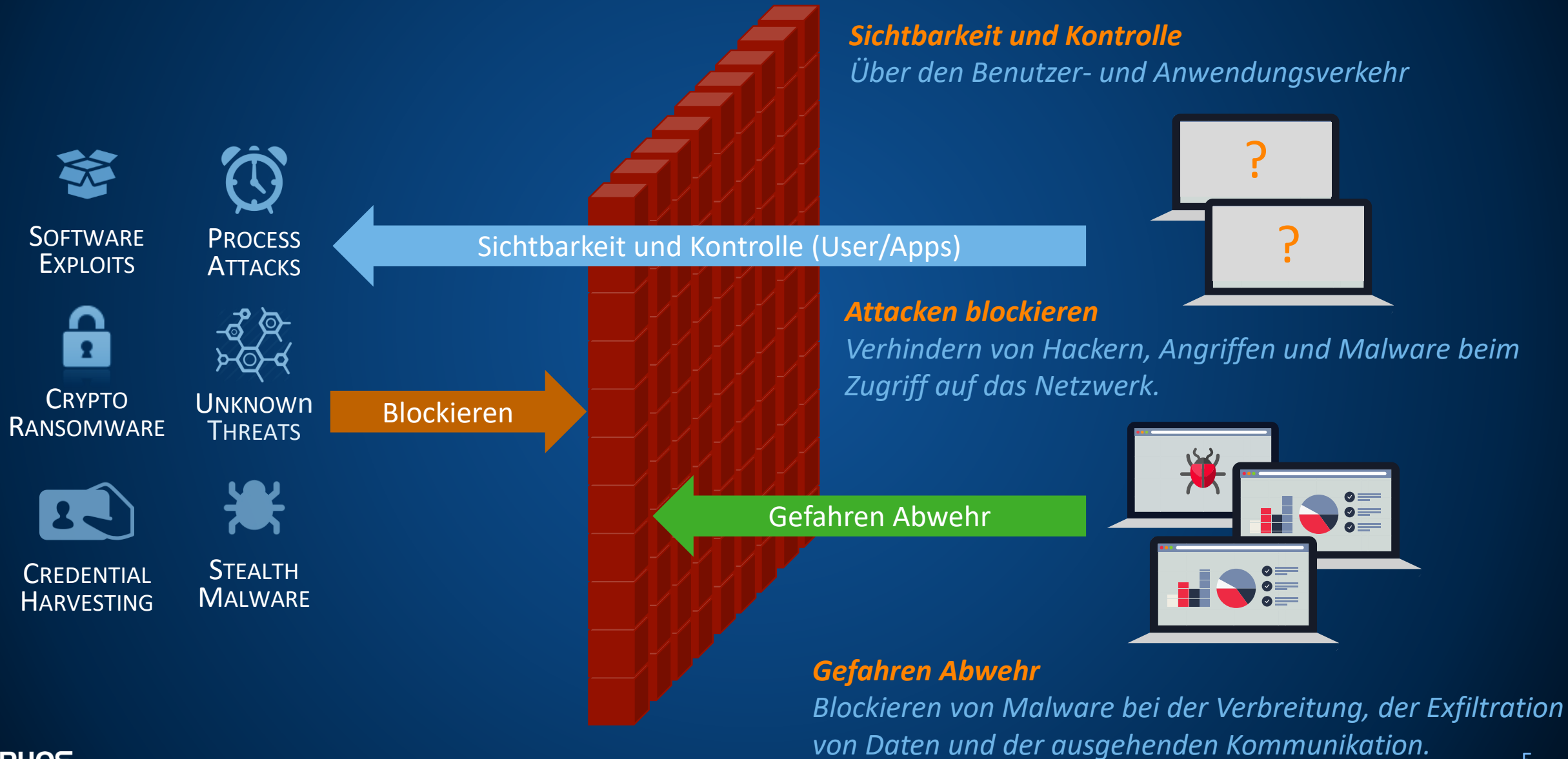
- Wer bin ich?
- Woher komme ich?
- Welche Erwartungen habe ich?

Traditional Firewall

Where are you coming from? **Phoenix**
Where are you going to? **San Francisco**
What are you? **A parcel**

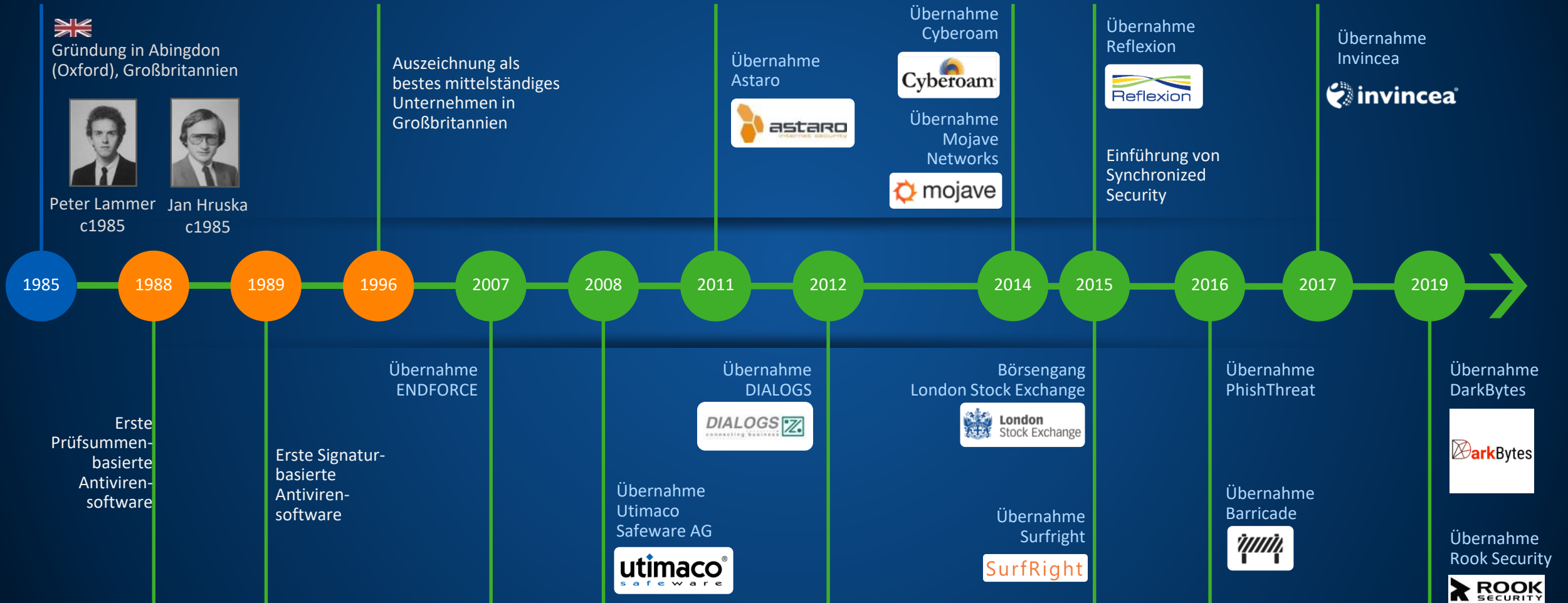


Die Next-Gen Firewall



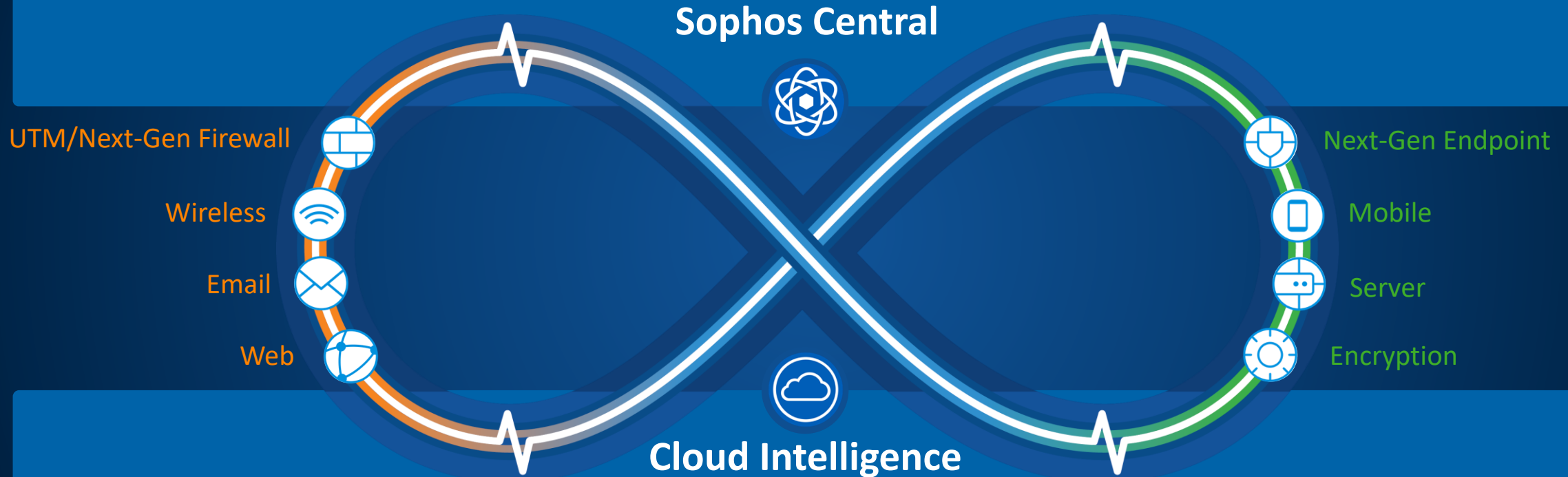
Sophos Geschichte

Entwicklung zur vollständigen Sicherheit




Synchronized Security Plattform und Strategie

 **Admin** | Manage All Sophos Products  **Self Service** | User Customizable Alerts  **Partner** | Management of Customer Installations



 **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

Zwei Plattformen

Sophos UTM



- Klassische UTM „All-In-One“ Firewall
- Vollumfängliche Sicherheitslösung
- Einfache Bedienung
- Bekannter Name
- Im Markt bewährt

Sophos XG Firewall



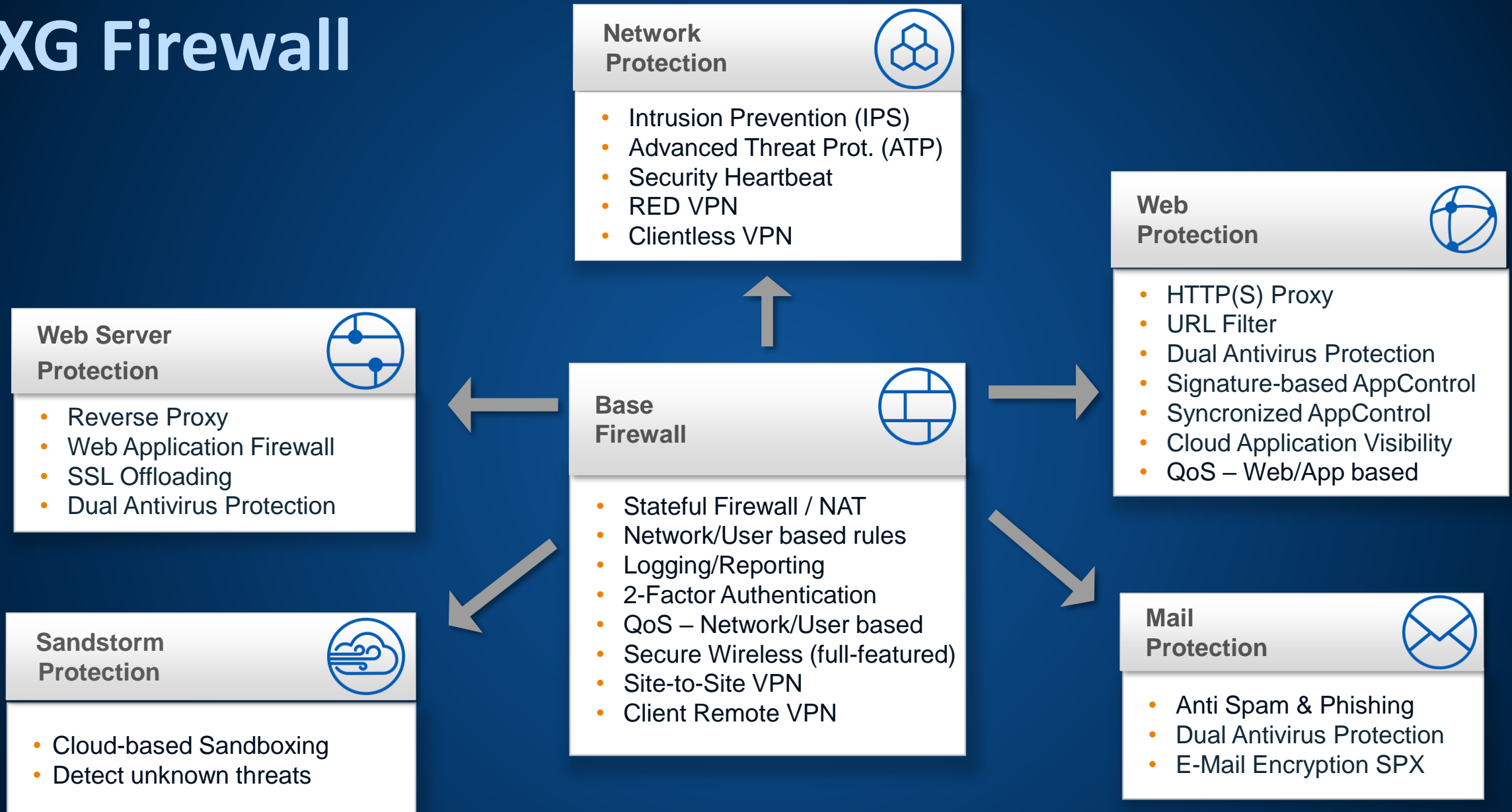
- Next Generation Firewall
- Userbasiertes Regelwerk
- Userbasiertes Reporting
- Synchronized Security
- Synchronized App Control
- Zentrale Verwaltbarkeit

SOPHOS

Sophos XG Firewall Features

SOPHOS

XG Firewall



XG Firewall Appliances (XG Serie)



XG 86

XG 106 XG 115

XG 125 XG 135

XG 210 XG 230

XG 310 XG 330

XG 430 XG 450

XG 550

XG 650

XG 750

Deployment Modes

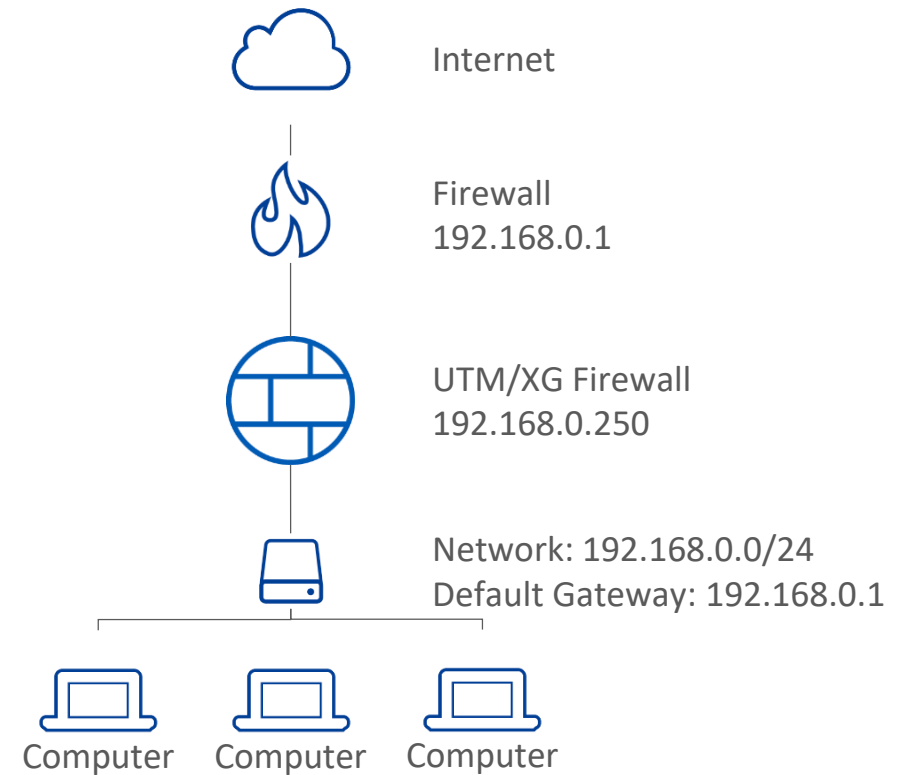
Bridge/Transparent Mode

Gateway Mode

Mixed Mode

Discover Mode

Transparent monitoring and scanning



Deployment Modes

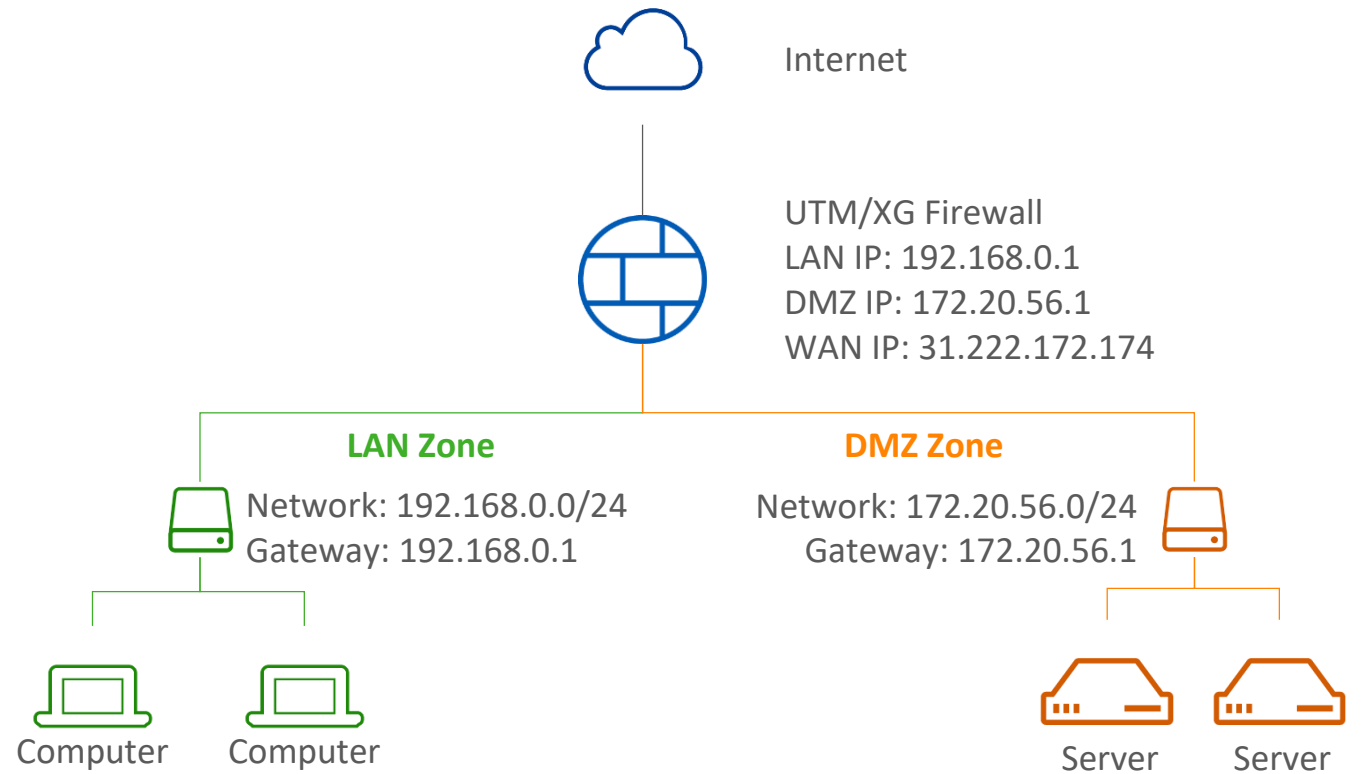
Bridge/Transparent Mode

Gateway Mode

Mixed Mode

Discover Mode

Zone-based filtering and scanning



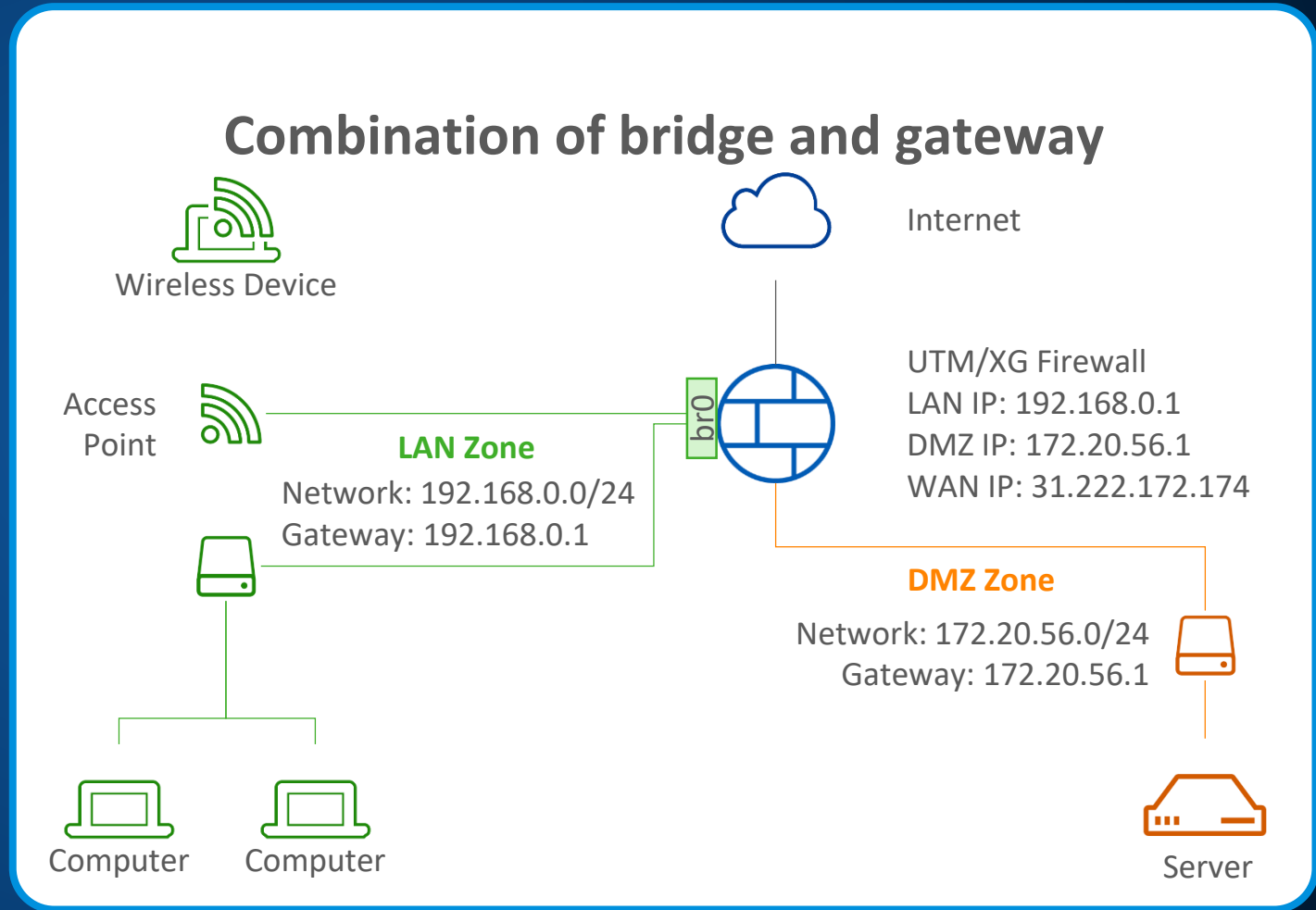
Deployment Modes

Bridge/Transparent Mode

Gateway Mode

Mixed Mode

Discover Mode



Deployment Modes

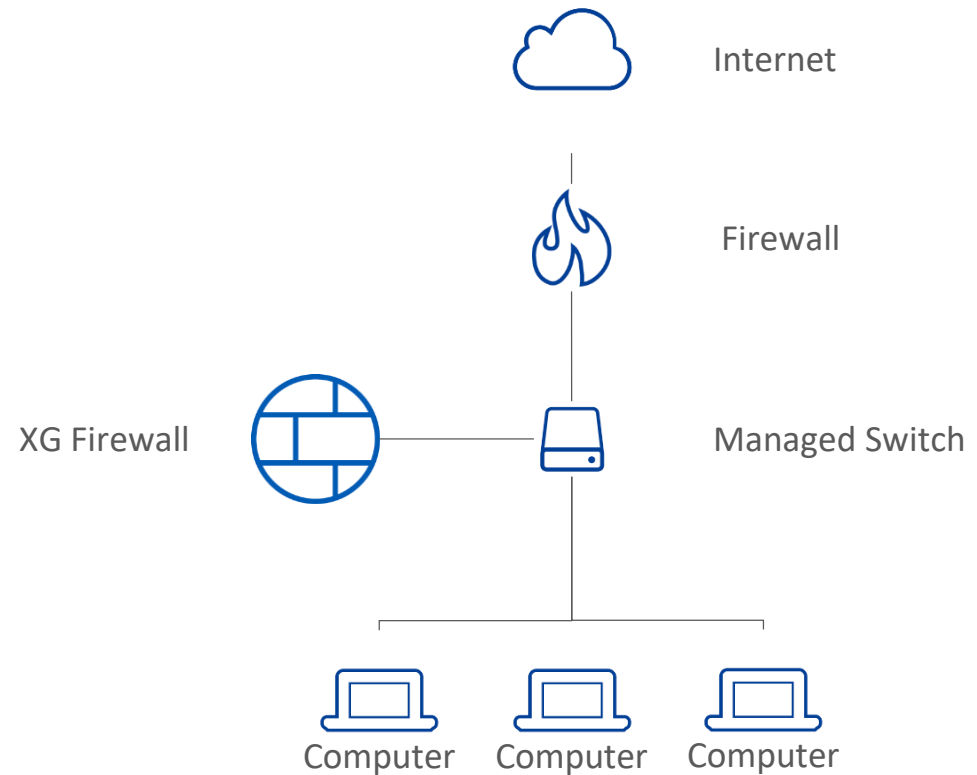
Bridge/Transparent Mode

Gateway Mode

Mixed Mode

Discover Mode

Non-intrusive monitoring of traffic



Die XG Firewall Design Philosophie

- Konzipiert für den durchschnittlichen mittelständischen IT-Manager
- Alles, was Sie am meisten interessiert - auf einen Blick mit Ampelanzeige
- 2-Klicks nach überall = Schneller Zugriff auf Detailinformationen
- Interaktive Widgets mit Flip-Card-Ansichten und Drill-Downs

Den Administratoren auf einen Blick Einblick in das Wesentliche geben

SOPHOS XG Firewall

Control Center

XG135w (SFOS 16.01.0) S1701F24746AC0C

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

SYSTEM

- Profiles
- Hosts and Services Administration
- Backup & Firmware
- Certificates

System

Performance Services

Interfaces VPN

CPU 8% Memory 39%

Bandwidth 140KB Sessions 21

High Availability: Not configured

Sophos Firewall Manager: Not configured

Running for 1 day, 20 hours, 28 minutes

Traffic Insight

Web Activity 124 highest | 22 avg

Hits every 5 minutes

Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Network Attacks

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

User & Device Insights

Security Heartbeat

2 Warnings 1 System at risk 1

Sandstorm

17 Suspect 4 Malicious 6 Clean

ATP UTQ

0/0 RED 4/4 Wireless APs

0 Connected Remote Users 7 Live Users

Click on widgets to open details

Active Firewall Rules

2 Business 13 User 13 Network 28 Total

6 Unused 2 Disabled 0 Changed 0 New

Reports

Yesterday Risky Apps seen

0 Yesterday Objectionable websites seen

6852 MB Yesterday Used by Top 10 Web users

0 Yesterday Intrusion Attacks

Messages

Warning 2d ago

HTTPS, SSH-based management is allowed from the W...

Welche ist die häufigste Anwendungskategorie, die die meisten Next-Gen-Firewalls erkennen?

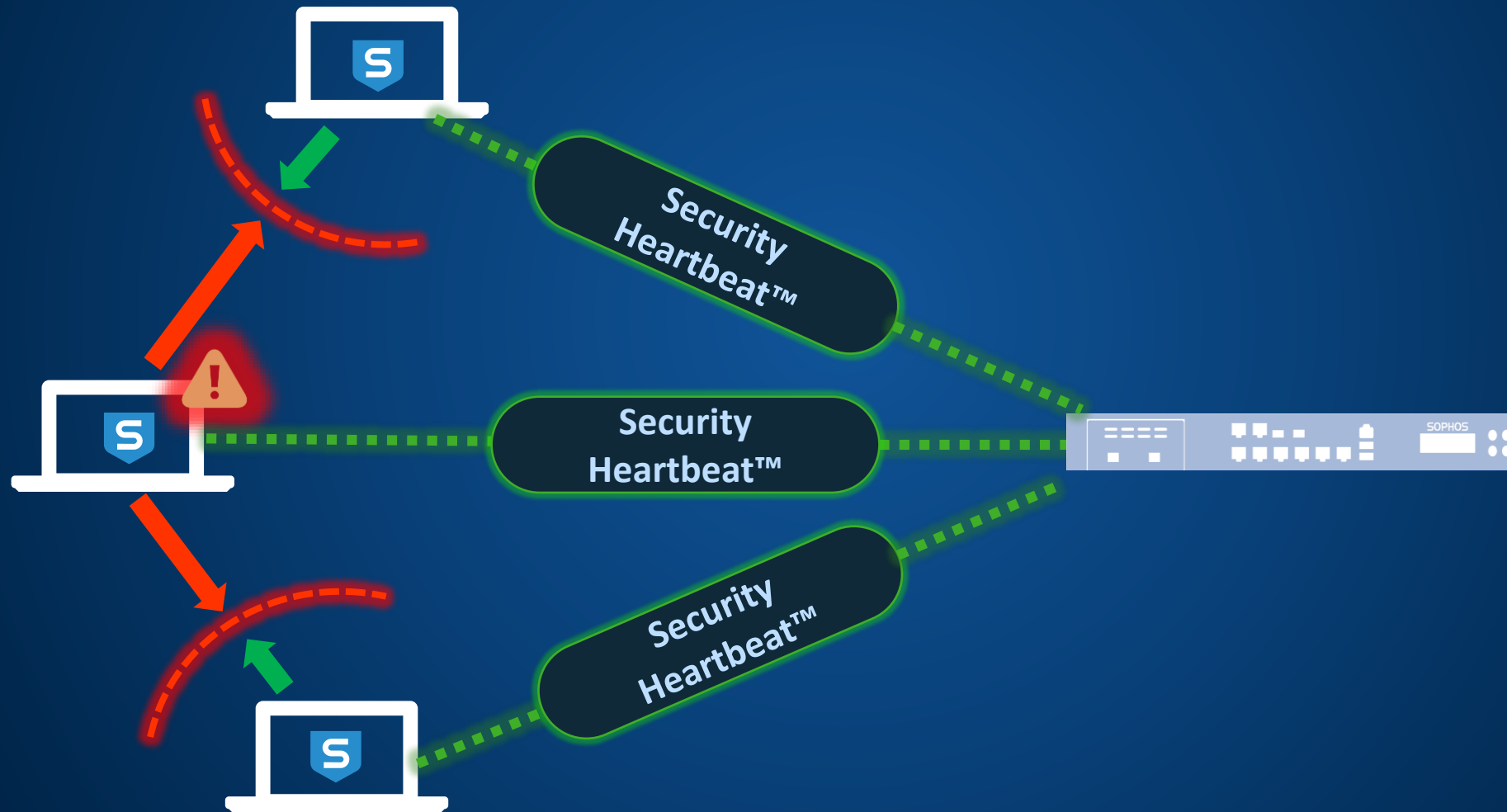
Synchronized App Control

Firewall erfährt die kommunizierende Applikation vom Client



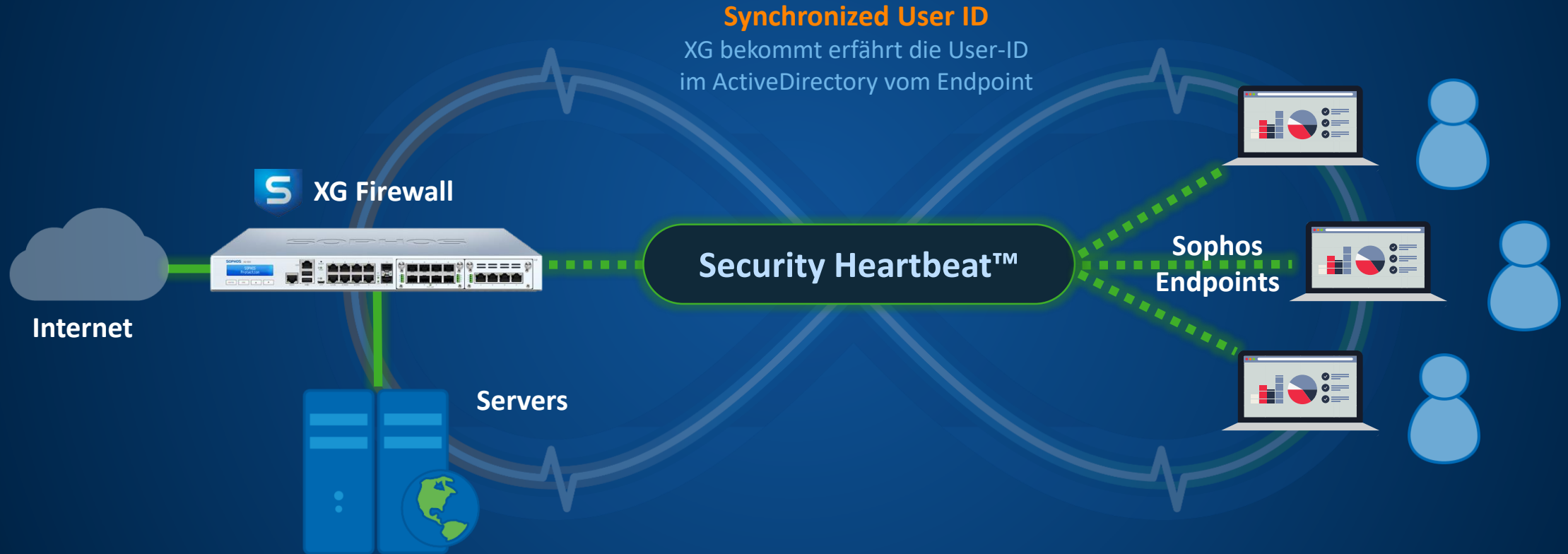
Synchronized Security - Lateral Movement Protection

XG Firewall verteilt Informationen über infizierte Clients per Security Heartbeat



Synchronized User ID

Benutzer-ID wird automatisch zwischen Endpoint und Firewall synchronisiert



Firewall Regel-Gruppierung

Automatische Gruppierung von Regeln für große Regelsätze

What's New

- Kriterien zur automatischen Gruppierung von Regeln können erstellt werden
- Neue Regeln werden manuell oder automatisch gruppiert

Add User/network rule How-to guides Log viewer Help admin Sophos

Rule name * Description

Rule position

Action Accept Drop Reject

Rule group

Source

Can't add the rule to an existing group based on the selected criteria.

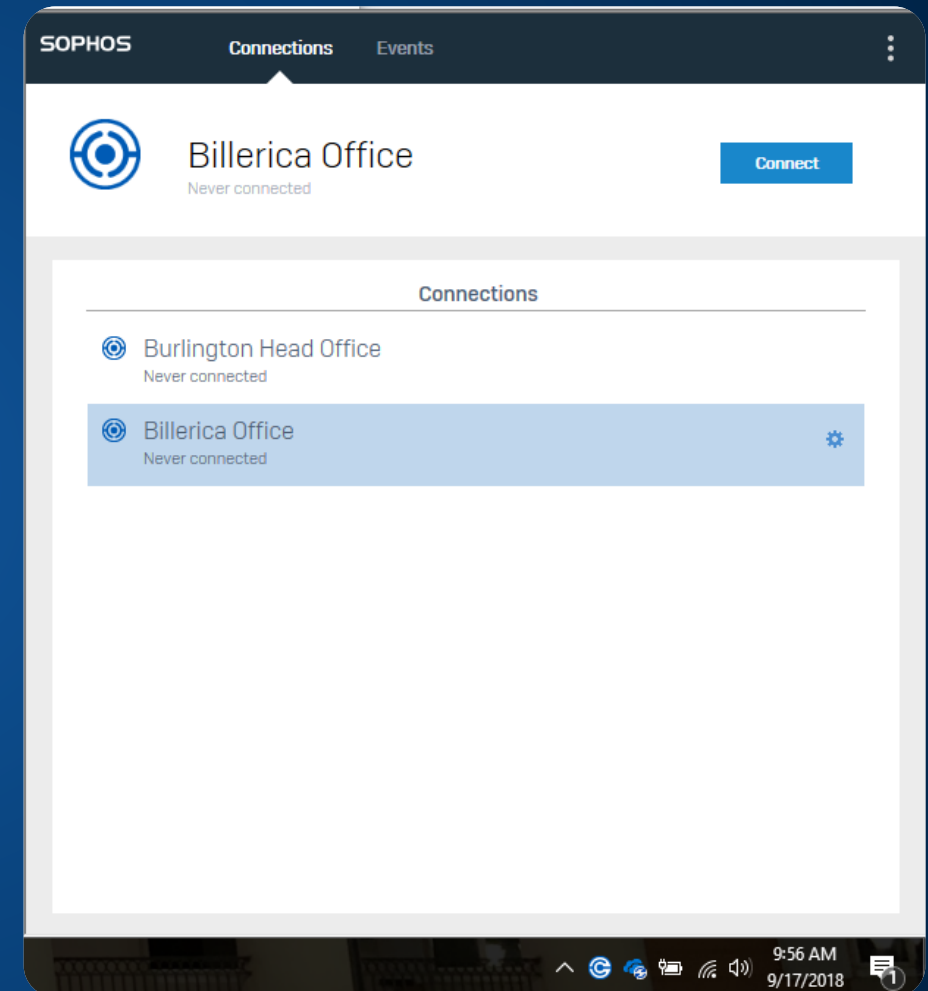
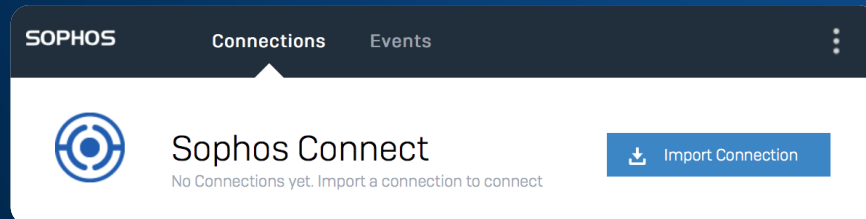
Sophos Connect IPsec Client

Neuer kostenloser IPSEC-Client

What's New

- Einfache Verteilung und Wartung
- MSI-Installationspaket kann via Active Directory oder Softwareverteilung installiert werden
- Einfache Verteilung der Konfiguration per Skript
- Keine Schulung der Endanwender notwendig

Kostenlos für Kunden und Partner!



APX – Wave 2 Access Points

Schnelleres und leistungsfähigeres WLAN

Höhere Geschwindigkeit – bis zu 2.3Gbps

High Capacity & High Density

Optimierte Performance



- **APX 740:** Top-Modell mit High Capacity und High Density für mittlere bis große Umgebungen
- **APX 530:** Hohe Performance für typische Büro-Umgebungen
- **APX 320:** Dual 5 GHz basierter Access Point für kleinere Büro- und Lehre-Umgebungen

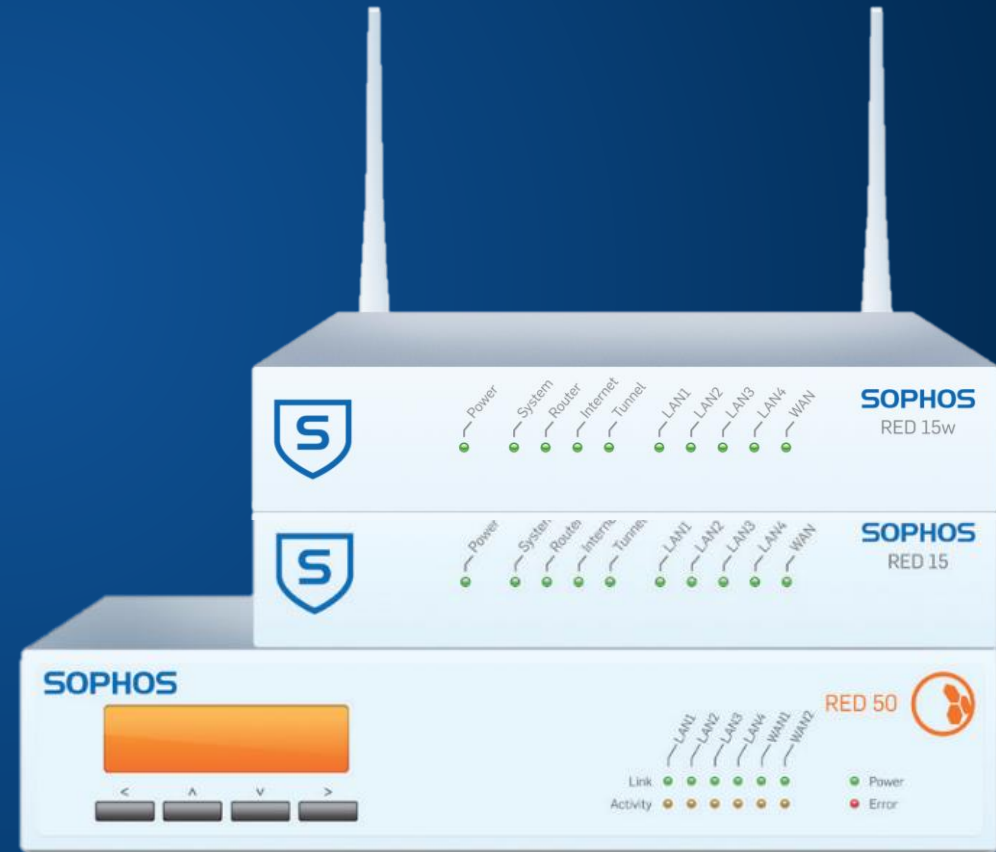
Sophos RED

(Remote Ethernet Device)

Sophos RED

Unternehmen mit vielen kleineren Zweigstellen benötigen einfach zu bedienende, kosteneffiziente und sichere Mechanismen, um Zweigstellen mit der Zentrale zu verbinden und deren Internet-Zugang abzusichern.

- Zweigstellen & Filialen
- Niederlassungen
- Vertriebsbüros
- Home Offices
- Baustellen, Produktionsstätten
- Remote Wartung von Maschinen
- Lieferanten
- ...



Sandstorm

SOPHOS

Sandstorm

- Abgeschottete Umgebung, in der unbekannte Dateien ausgeführt werden
- Verhaltensbasierte Analyse zur Erkennung von APTs und Zero-Days
- Untersucht über 40 Dateitypen unter Windows, Mac und Android
u.a. Office-Dokumente, PDFs, ausführbare Dateien, FLASH, Java, Javascript, HTML5
- Verfügbar als Security-as-a-Service per Zusatzlizenz in:
 - Sophos XG Firewall
 - Sophos UTM
 - Sophos Web Appliance
 - Sophos E-Mail Appliance



Sandstorm



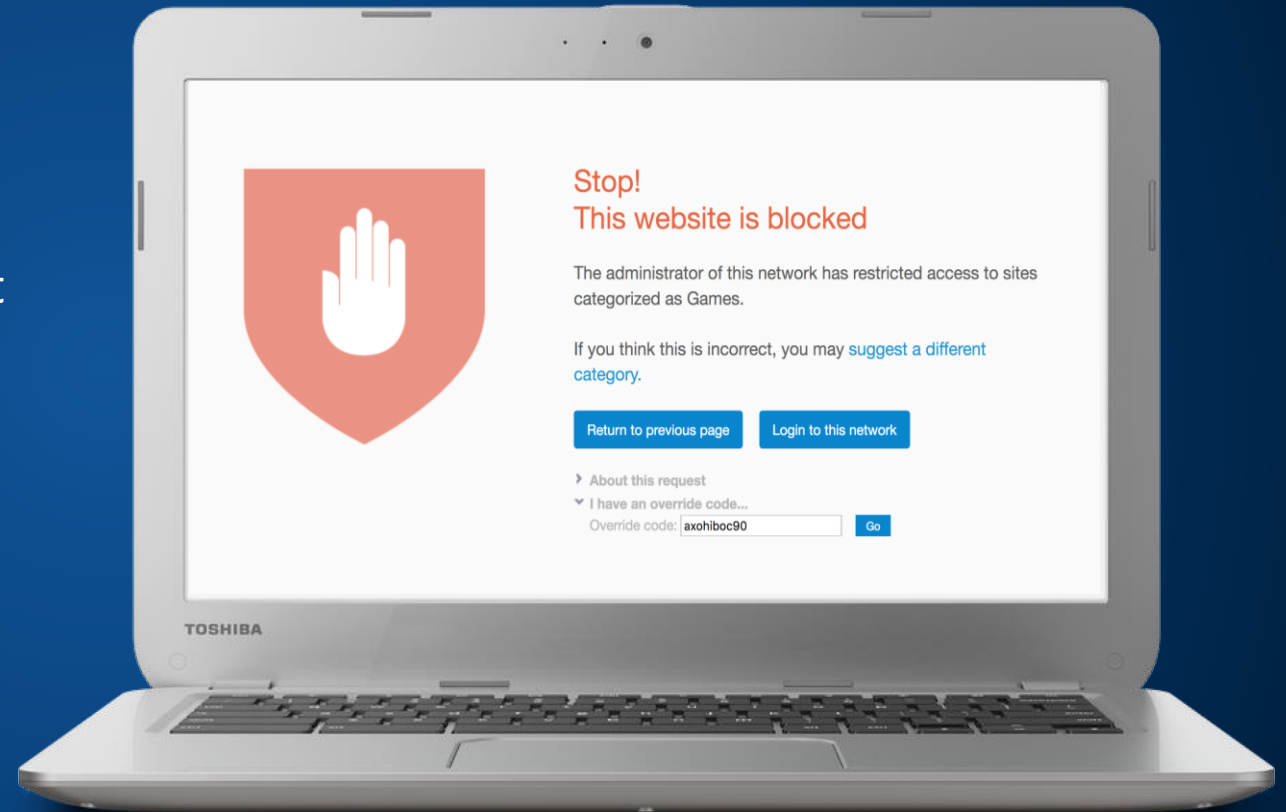
Maßgeschneidert für Bildungseinrichtungen

What's New

- SafeSearch and YouTube können jetzt regelbasiert auf Benutzer-/Gruppenebene gesteuert werden
- Freischaltcodes für Webseiten können vom Lehrpersonal über das Benutzerportal verwaltet werden

Web Filtering

- Leistungsstarke Web-Filter-Richtlinien
- Kinder- und Jugendschutz
- Kontextsensitives Web Filtering
- Erkennen gefährlicher Internet-Nutzung
- Automatische Reports für Lehrkräfte oder Sicherheitsbeauftragte



New Features & Ausblick 2020



Sophos Central



Sophos Central Management

Sophos Central Reporting

Real-time Flow Monitor

Alerts and Notifications

Extreme Performance



Extreme SSL Inspection

Network Flow Processing

New Streaming DPI Engine

Intelligent FastPath Offloading

SD-WAN and AWS



Synchronized SD-WAN

New SD-RED Appliances

Full IaaS Support in AWS

Routing, NAT, IF Enhancements

Sophos XG Firewall für Bildungseinrichtungen

Maßgeschneidert für Bildungseinrichtungen.

Die Sophos XG Firewall ist optimal auf die Bedürfnisse von Bildungseinrichtungen ausgelegt und bietet einzigartige Transparenz, erstklassige Sicherheit und Kontrolle sowie herausragende Reaktion auf Bedrohungen. Mit der Sophos XG Firewall wird die Verwaltung Ihrer Firewall, die Reaktion auf Bedrohungen und die Kontrolle von Aktivitäten in Ihrem Netzwerk jetzt noch einfacher und benutzerfreundlicher.



SOPHOS

Cybersecurity made simple.