SOPHOS | discover

NEXT-GEN

Next Generation IT Security

Synchronized Security vs. Best-of-Breed

Christoph Riese
Manager Sales Engineering

SOPHOS

Sophos – mehr als 30 Jahre Erfahrung

1985
GRÜNDUNG
OXFORD, UK

534.9
UMSATZ
(FY16)

3.000
MITARBEITER

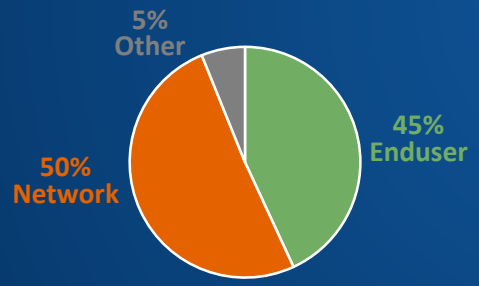
400
in DACH

HQ
ABINGDON, UK

200,000+
KUNDEN

100M+
ANWENDER

20,000+
CHANNEL
PARTNER



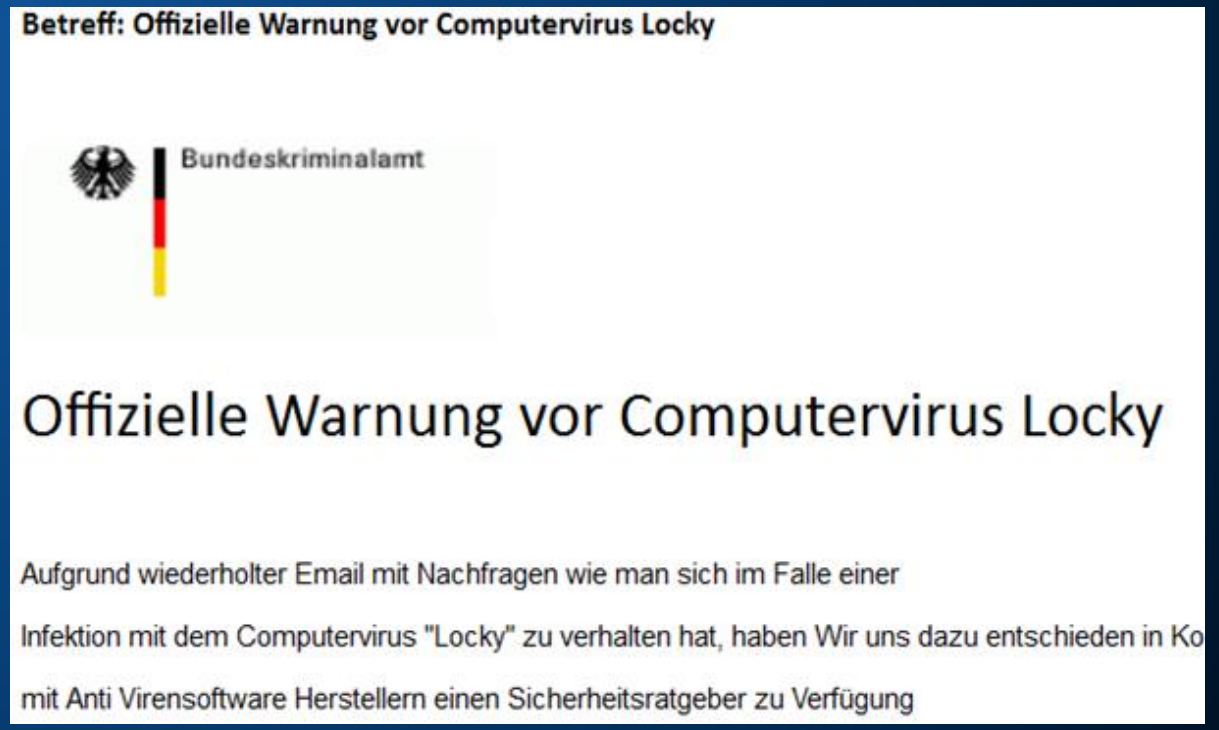
- Akquisition u.a. von Utimaco 2009, Astaro 2011, Dialogs 2012, Cyberoam 2014, Mojave 2014, Reflexion 2015, SurfRight 2015, Barricade 2016, Invincea 2017
- Gartner: Marktführer in den Bereichen Endpoint, Verschlüsselung & UTM

Warum waren die Krypto-Trojaner so erfolgreich?

SOPHOS

Gründe für Infektionen trotz Best-of-Breed Security

- Office-Dokumente und PDFs in E-Mails oft zugelassen
- Technologisch fortgeschrittene Schädlinge
- Hochprofessionelle Angreifer
- Geschicktes Social Engineering
- Sicherheitssysteme fehlen oder falsch konfiguriert
- Sicherheitssysteme agieren nicht als System



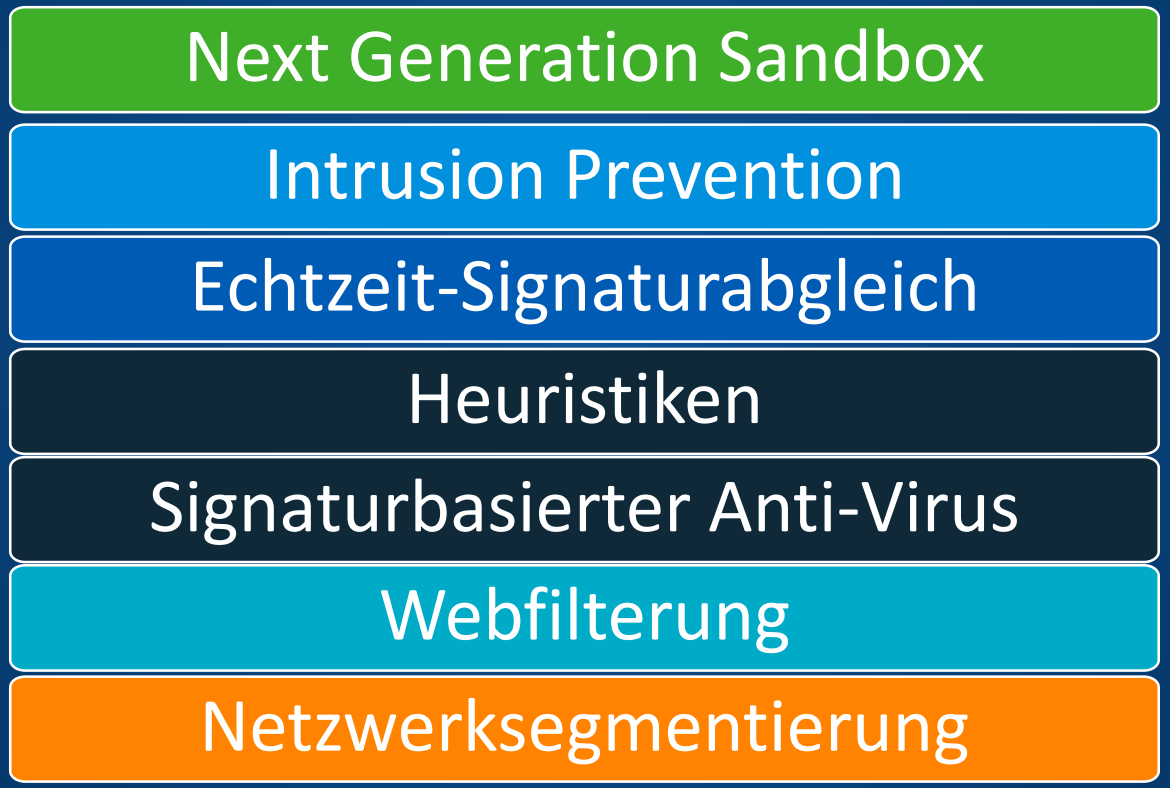
Neue Sicherheitskonzepte sind notwendig

SOPHOS

Verteidigungslinie 1
Gateway

SOPHOS

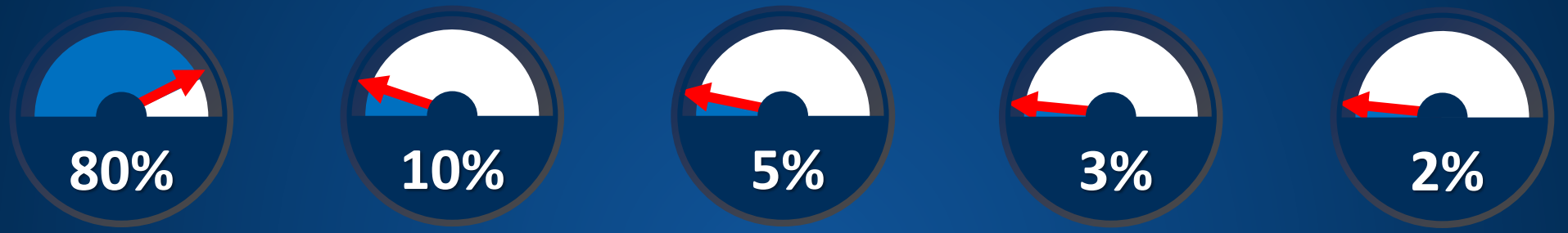
Sicherheitsmaßnahmen am Gateway



Verteidigungslinie 2
Endpoint Protection

SOPHOS

Wo Malware am Endpoint aufgehalten wird



Angriffsfläche reduzieren	Analyse vor Ausführung	Signaturen	Laufzeit	Exploit Erkennung
URL-Filterung Download Reputation Device Control	Heuristiken Regelbasiert	Bekannte Malware-Familien	Verhaltens-erkennung	Identifizierung von Techniken

Traditionelle Malware

Moderne Bedrohungen

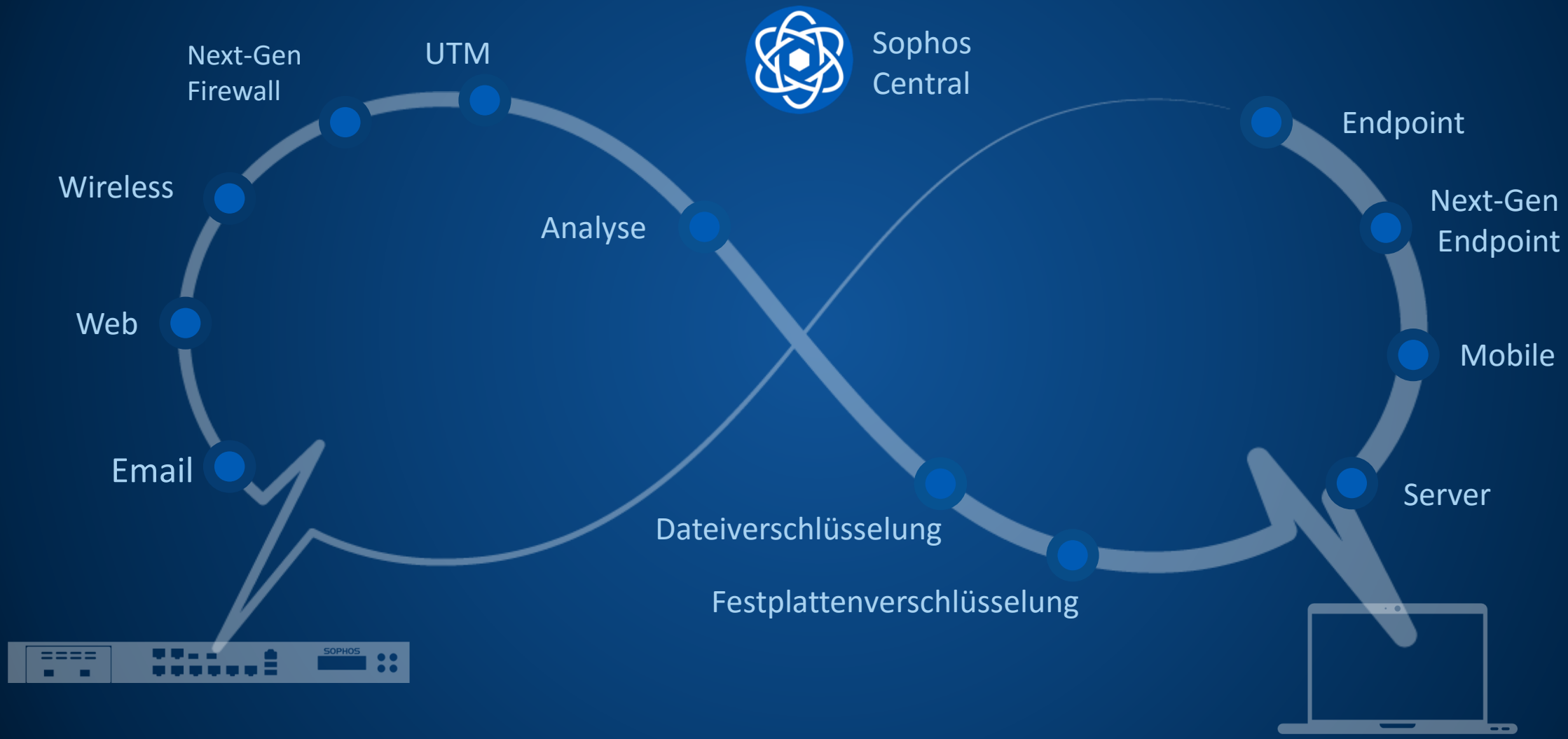
SOPHOS

Finale Verteidigungslinie
Sicherheit als System

Synchronized Security

SOPHOS

Synchronized Security – Teamplay statt Best-of-Breed

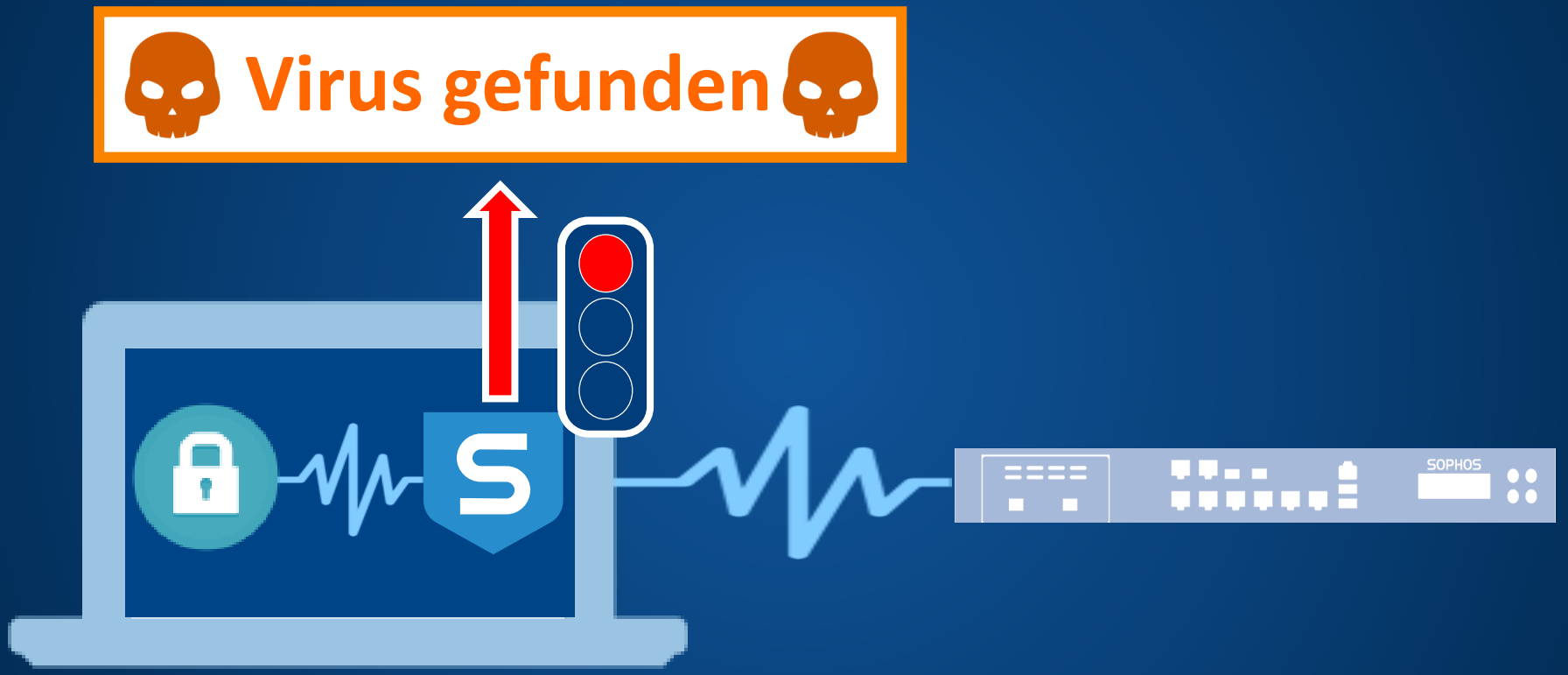


Security Heartbeat

Synchronized Security

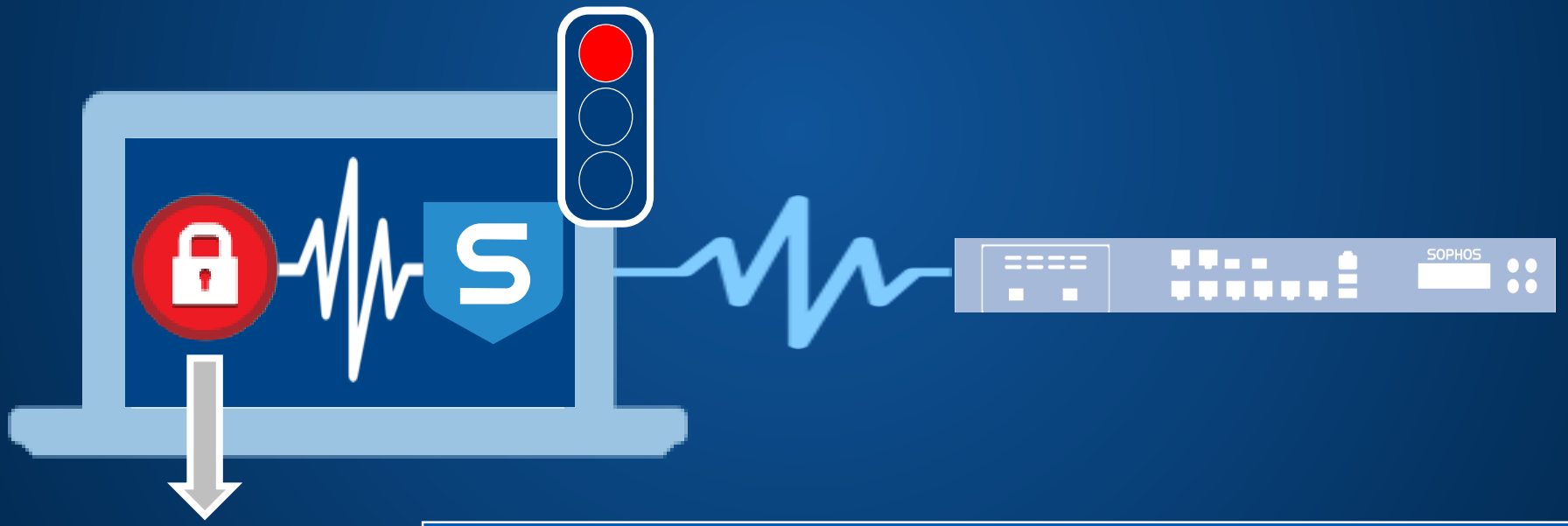
SOPHOS

Security Heartbeat – Beispiel Vireninfektion (1)



1. Sophos Endpoint Protection oder Intercept X erkennt eine Bedrohung
2. Der Sicherheitsstatus des Clients ändert sich auf rot – der Endpoint ist momentan nicht sicher

Security Heartbeat – Beispiel Vireninfektion (2)

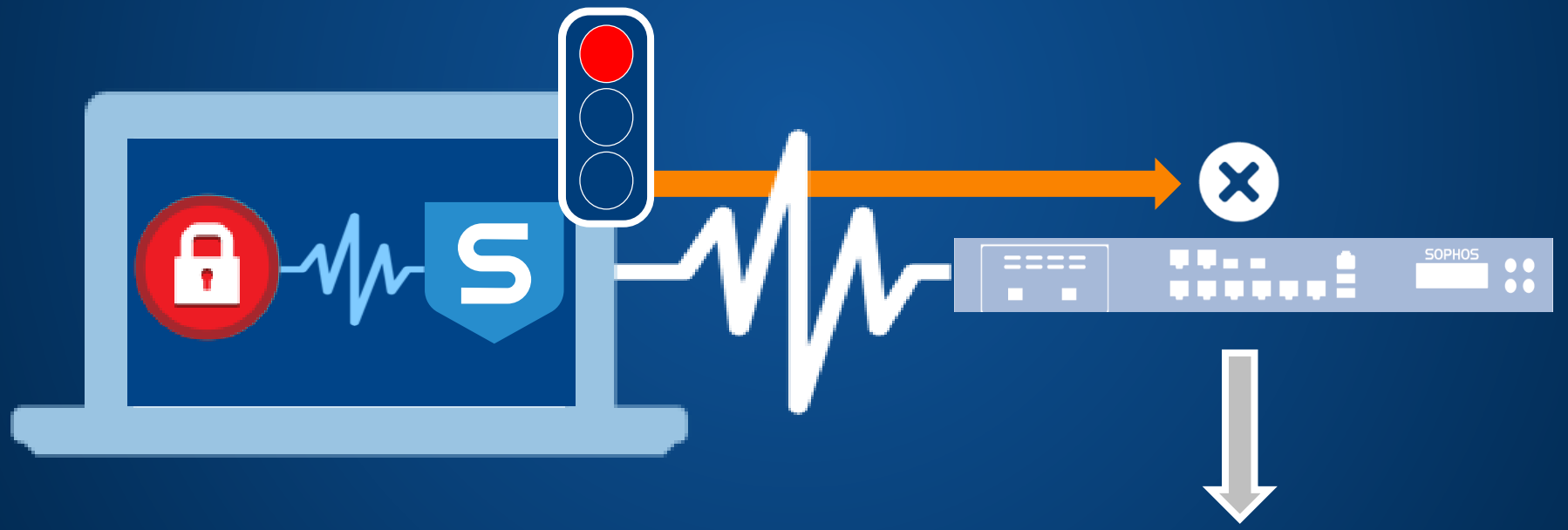


Schlüssel entfernen

3. Über den internen SecurityHeartbeat wird der Verschlüsselungsclient informiert, dass der Endpoint momentan nicht sicher ist
4. Die Schlüssel werden entfernt, damit keine Daten gestohlen werden können

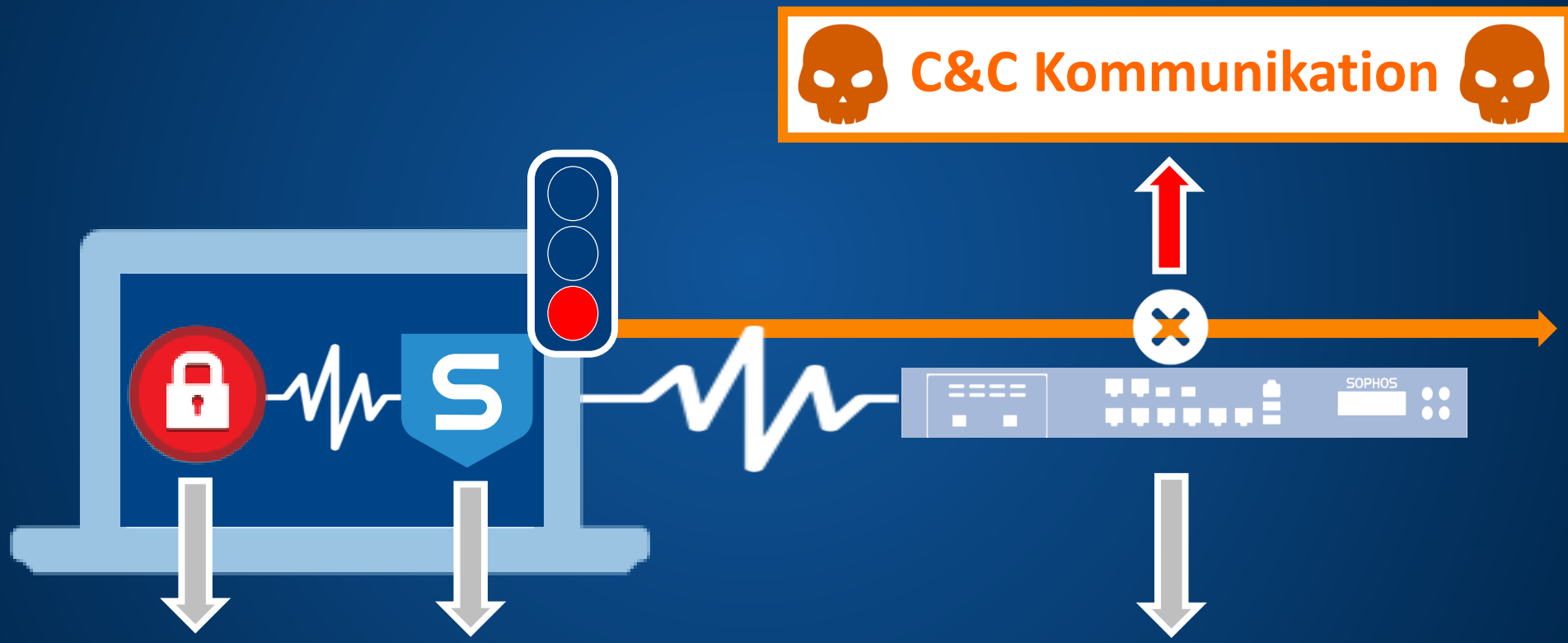
Security Heartbeat – Beispiel Vireninfektion (3)

5. Über den SecurityHeartbeat erfährt die NextGen-Firewall, dass der Endpoint nicht sicher ist
6. Die NextGent-Firewall nimmt den Endpoint solange in Netzwerkquarantäne, bis die Bedrohung beseitigt ist

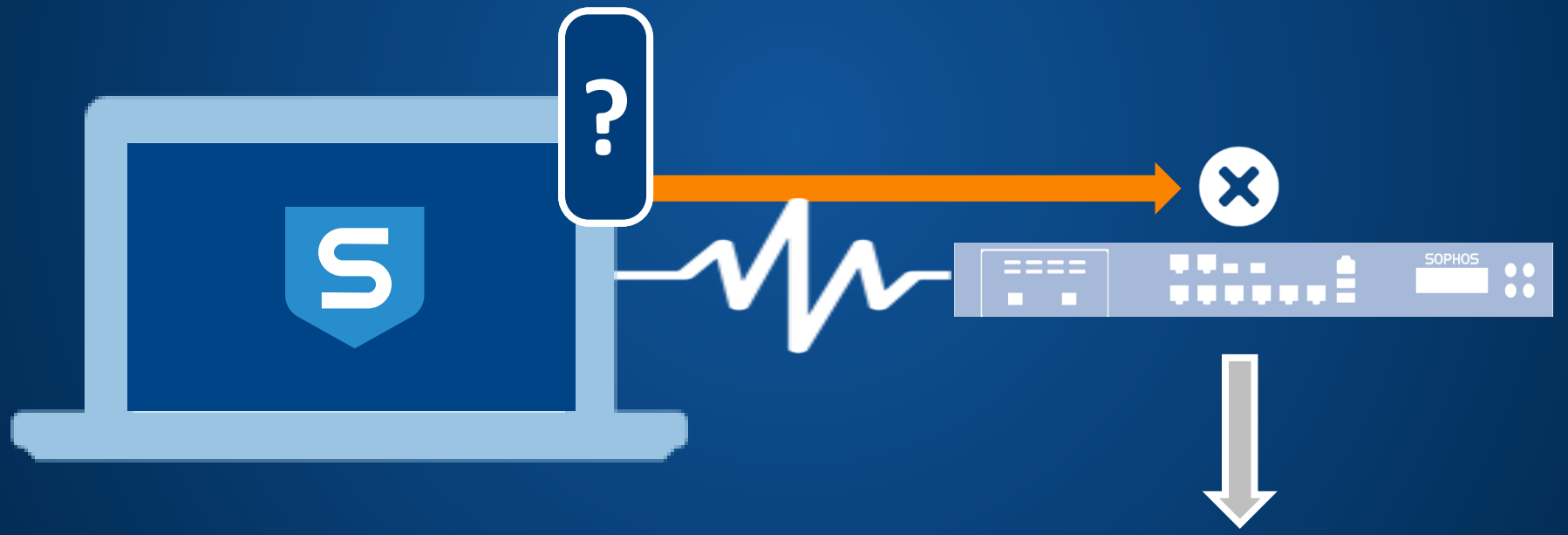


Client in Netzwerkquarantäne

Security Heartbeat – Botnet C&C-Verkehr erkannt

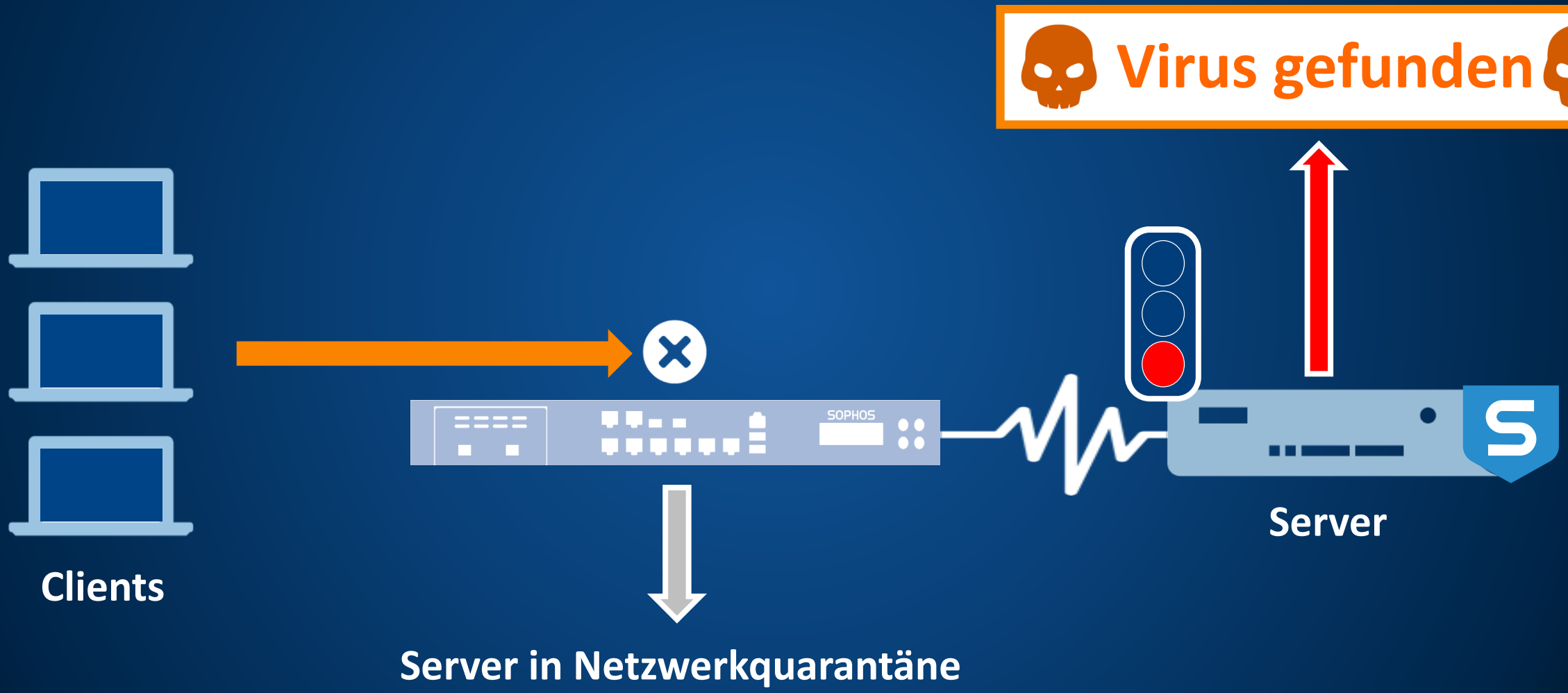


Security Heartbeat – fehlender Heartbeat



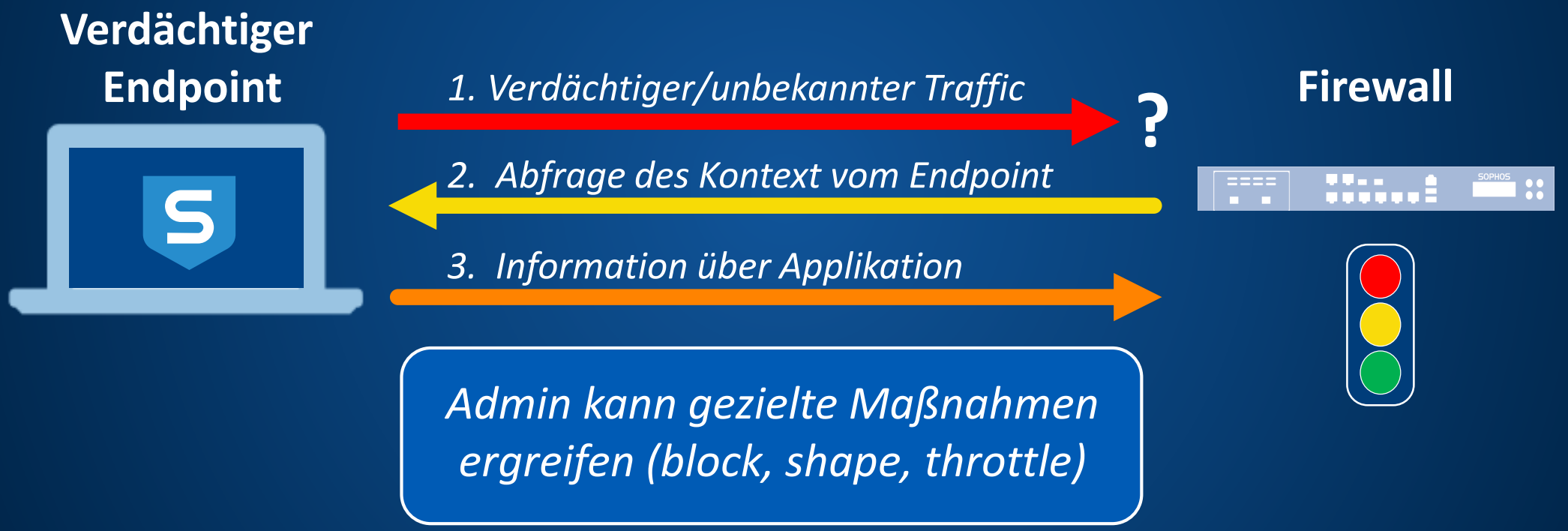
Client in Netzwerkquarantäne

Security Heartbeat – Server Heartbeat



Security Heartbeat – Applikationskontext

Informationen und Kontrolle über unbekannte Apps



Synchronized Encryption

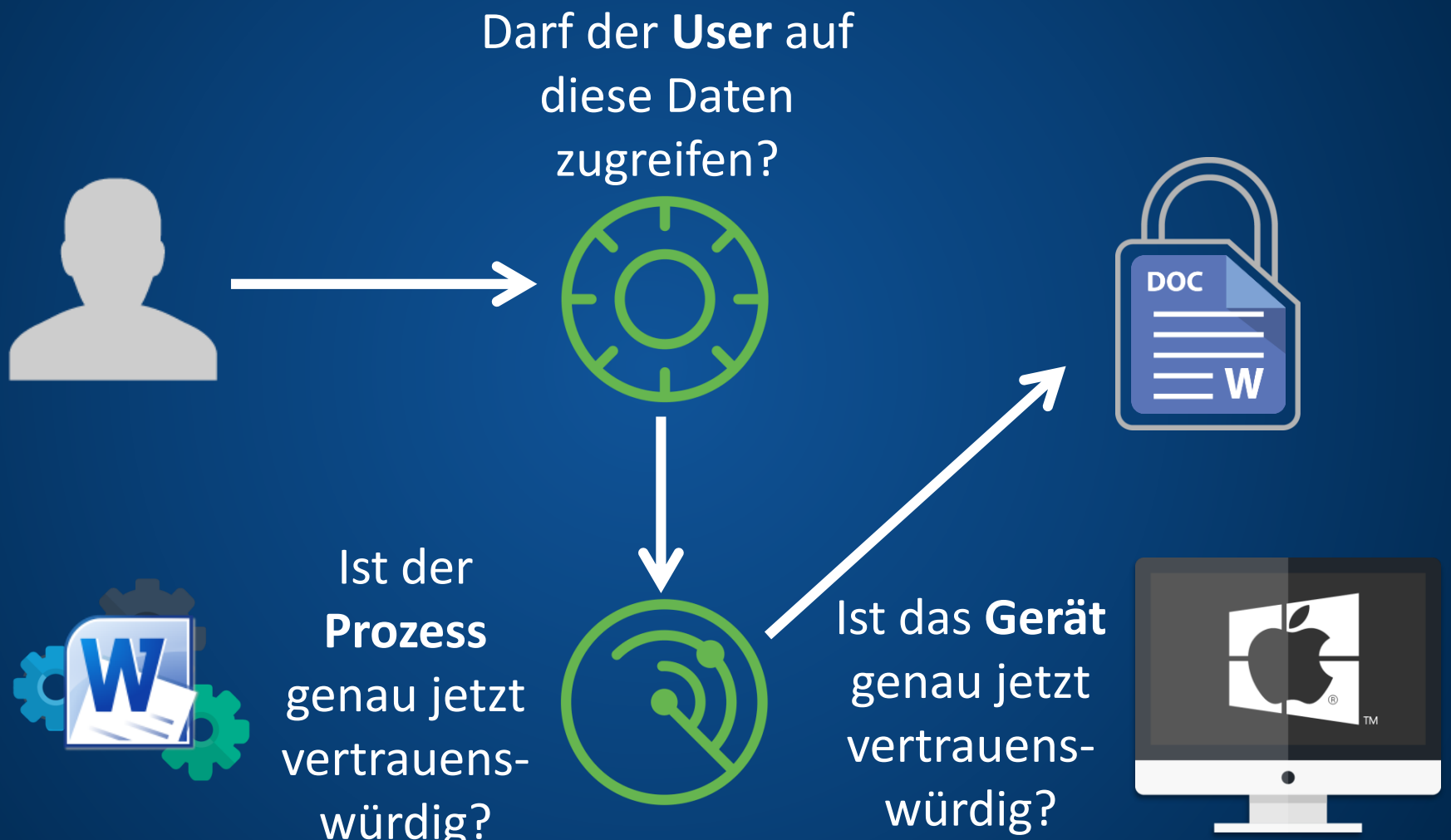
Synchronized Security

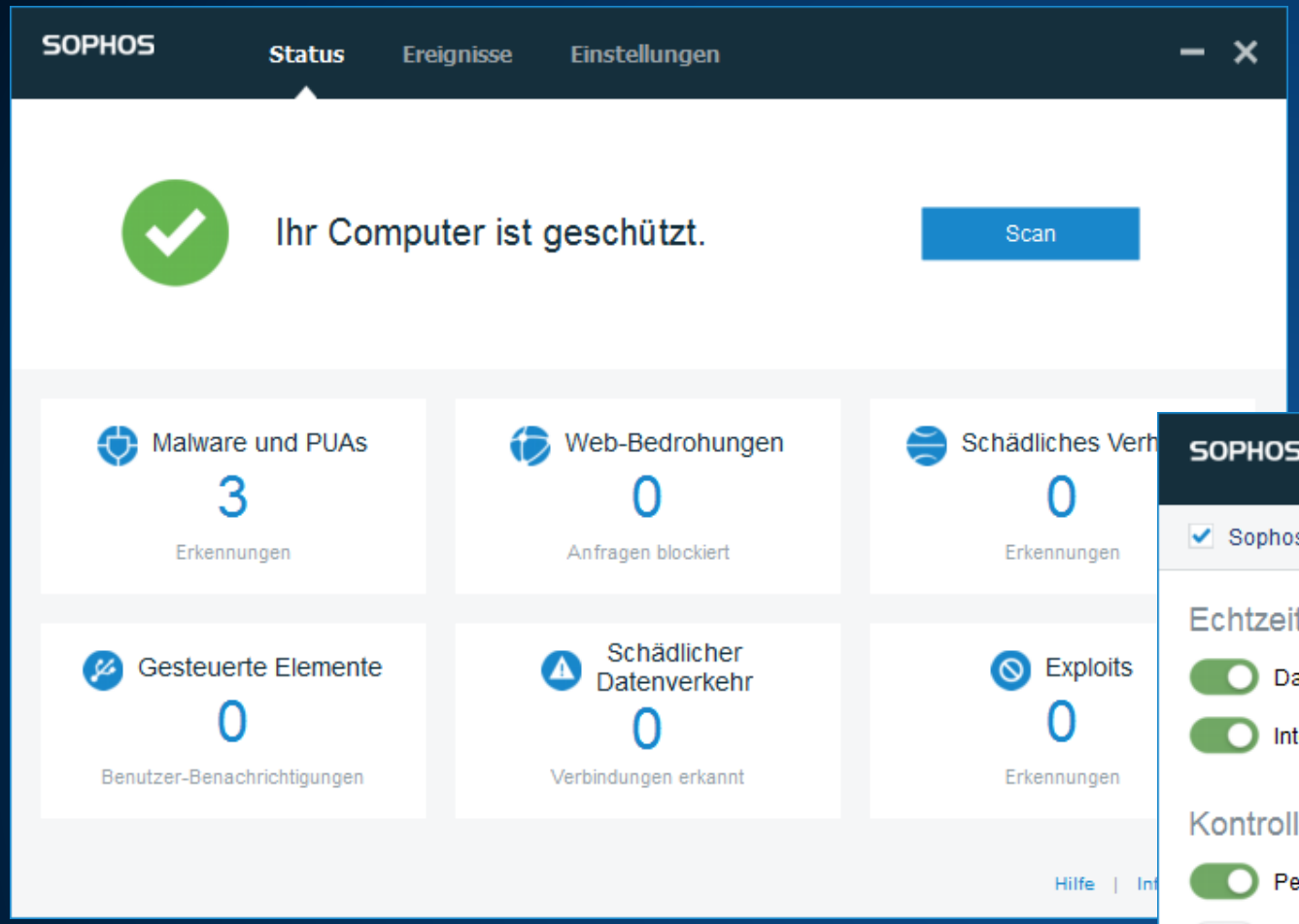
SOPHOS

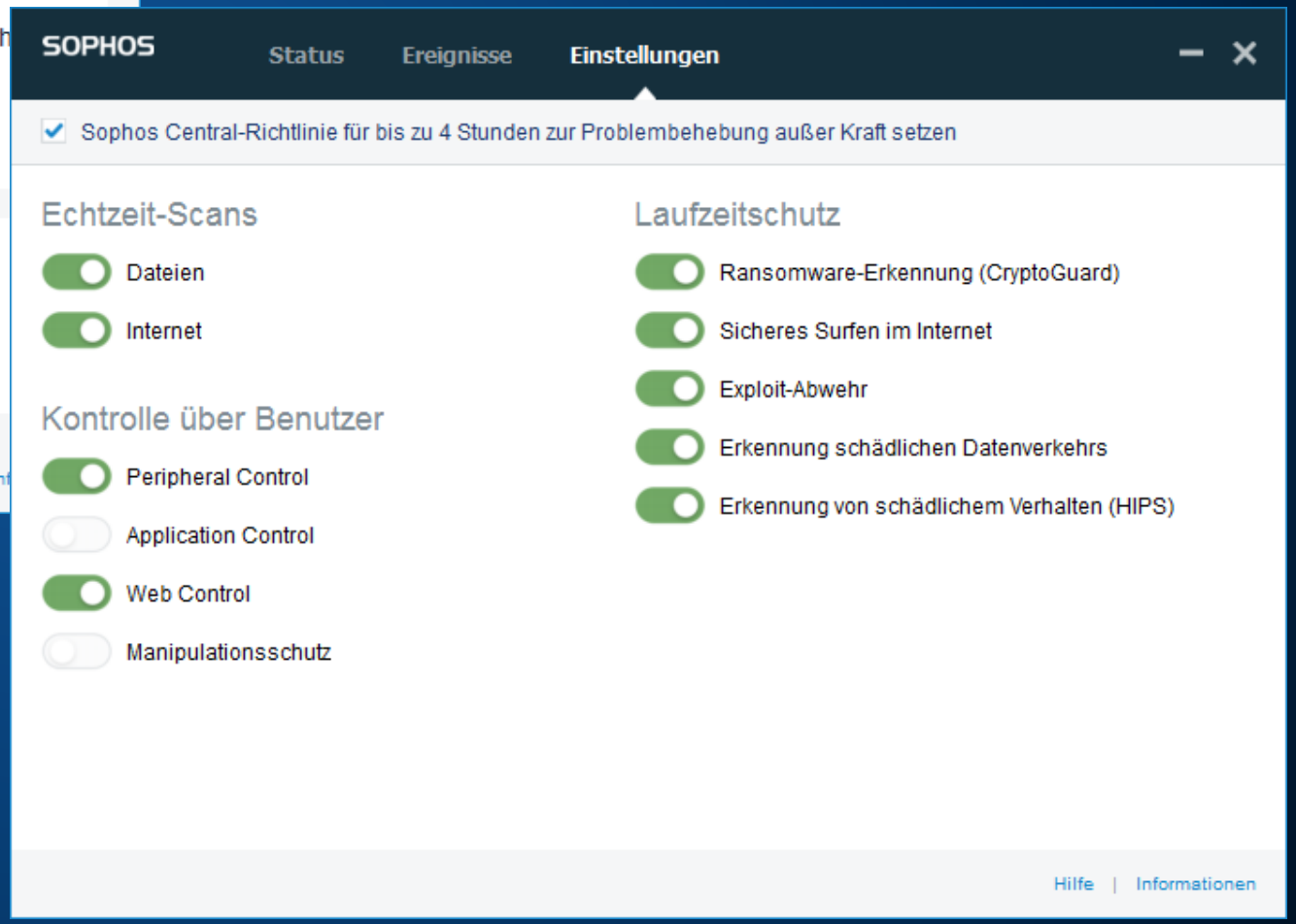
SafeGuard Enterprise – Verschlüsselung überall

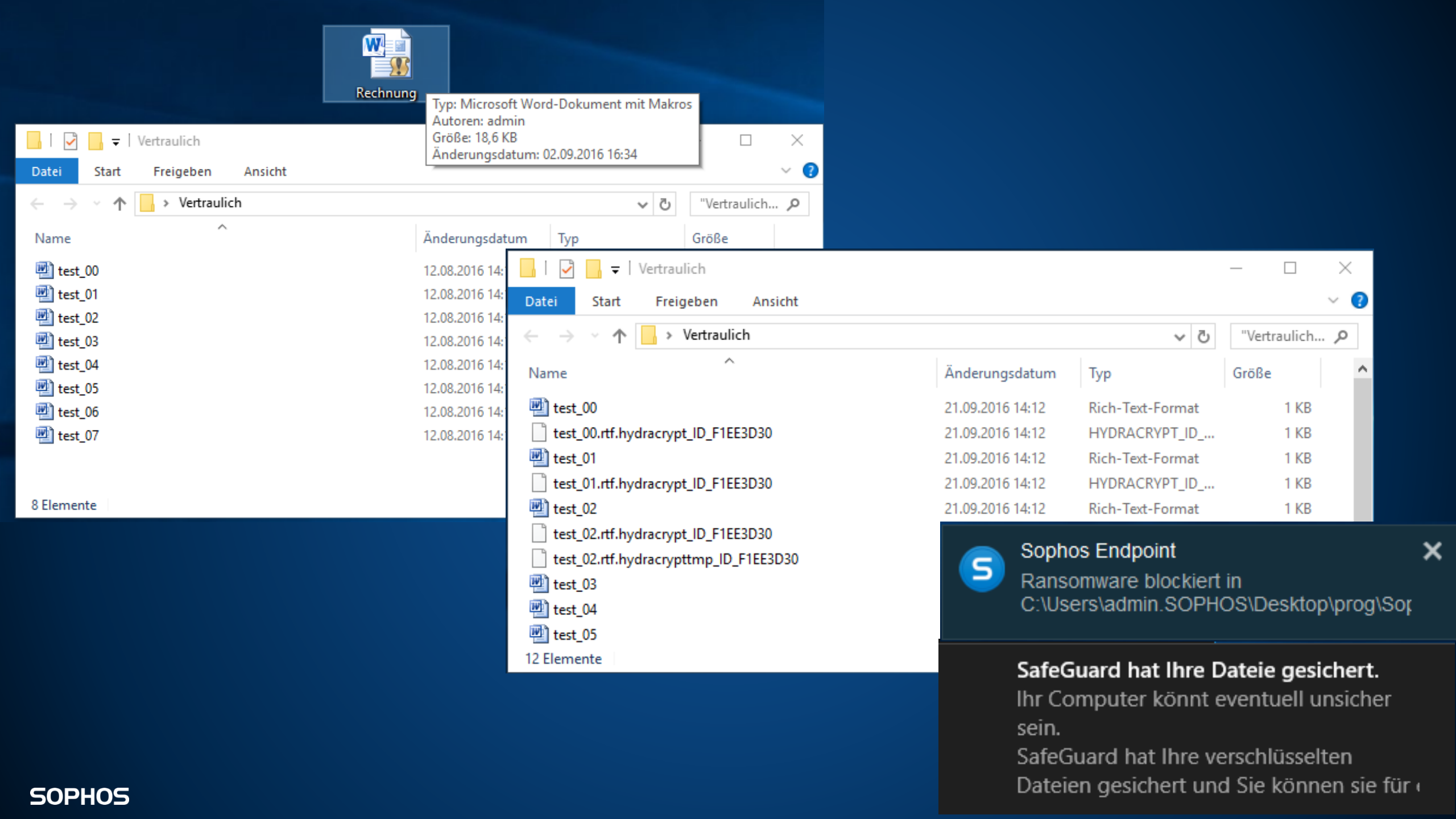
SOPHOS

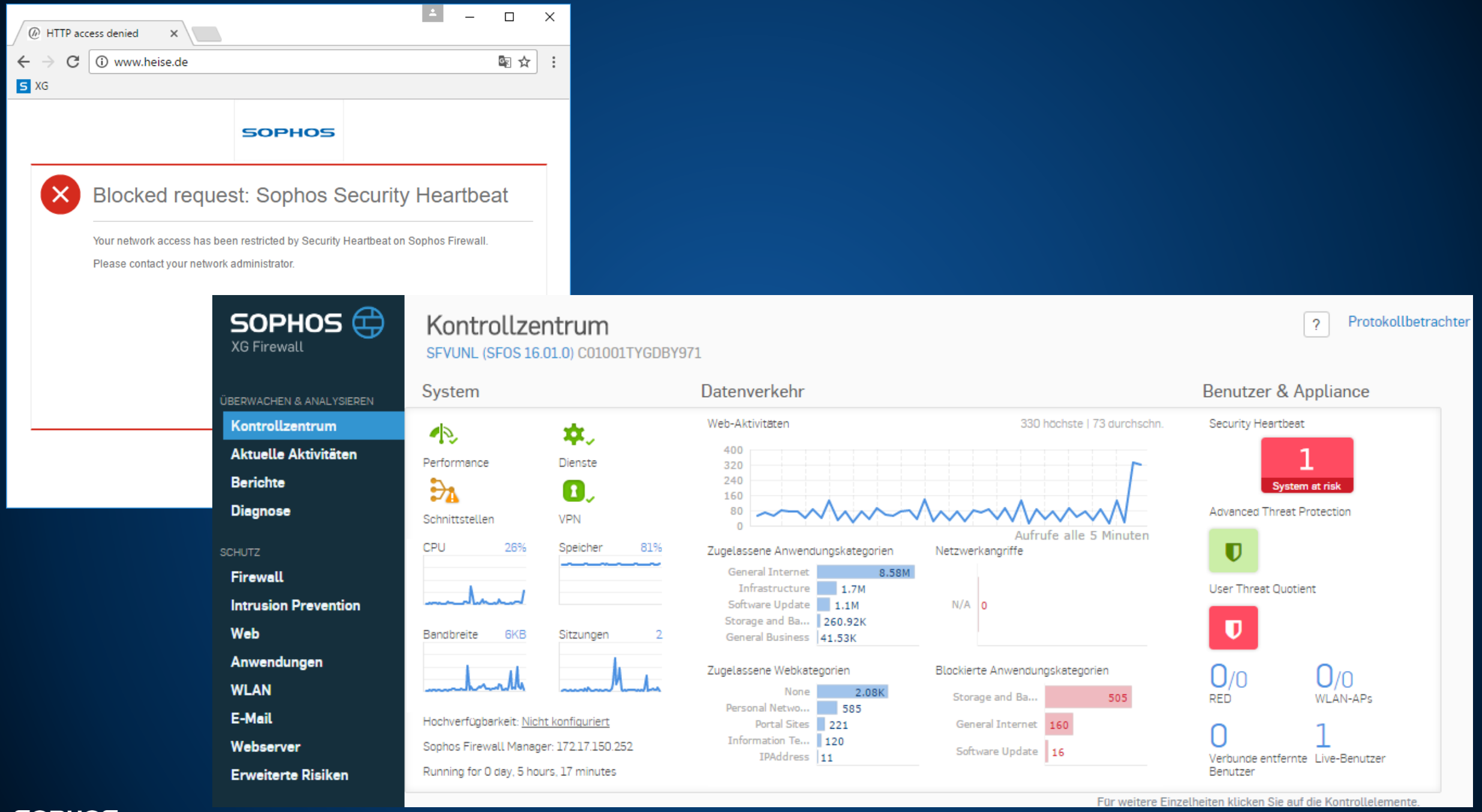
Ablauf beim Zugriff auf verschlüsselte Daten

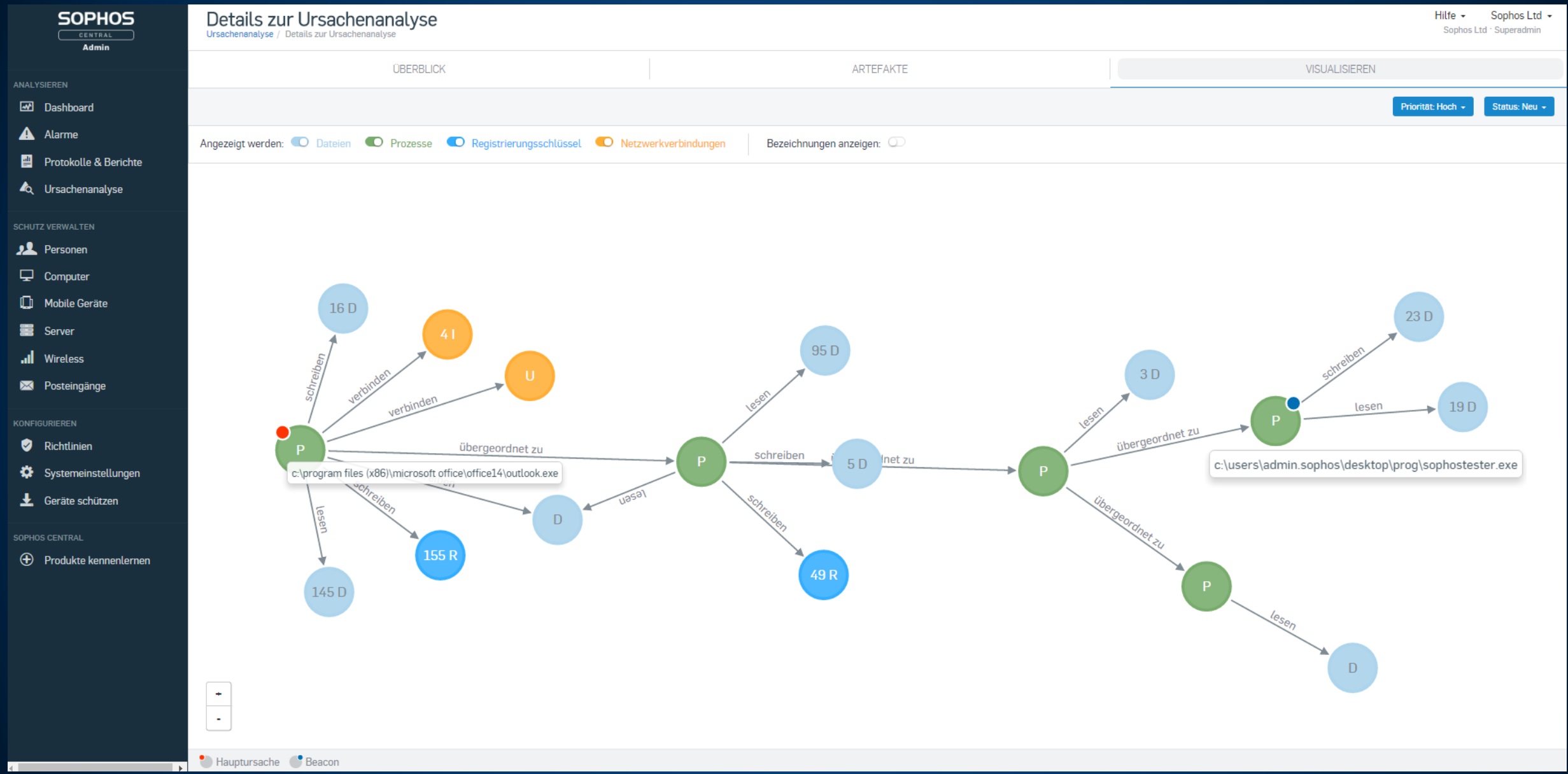



SOPHOS
Status
Ereignisse
Einstellungen
Ihr Computer ist geschützt.
Scan
Malware und PUAs
3
Erkennungen
Web-Bedrohungen
0
Anfragen blockiert
Schädliches Verh
0
Erkennungen
Gesteuerte Elemente
0
Benutzer-Benachrichtigungen
Schädlicher Datenverkehr
0
Verbindungen erkannt
Exploits
0
Erkennungen
Hilfe

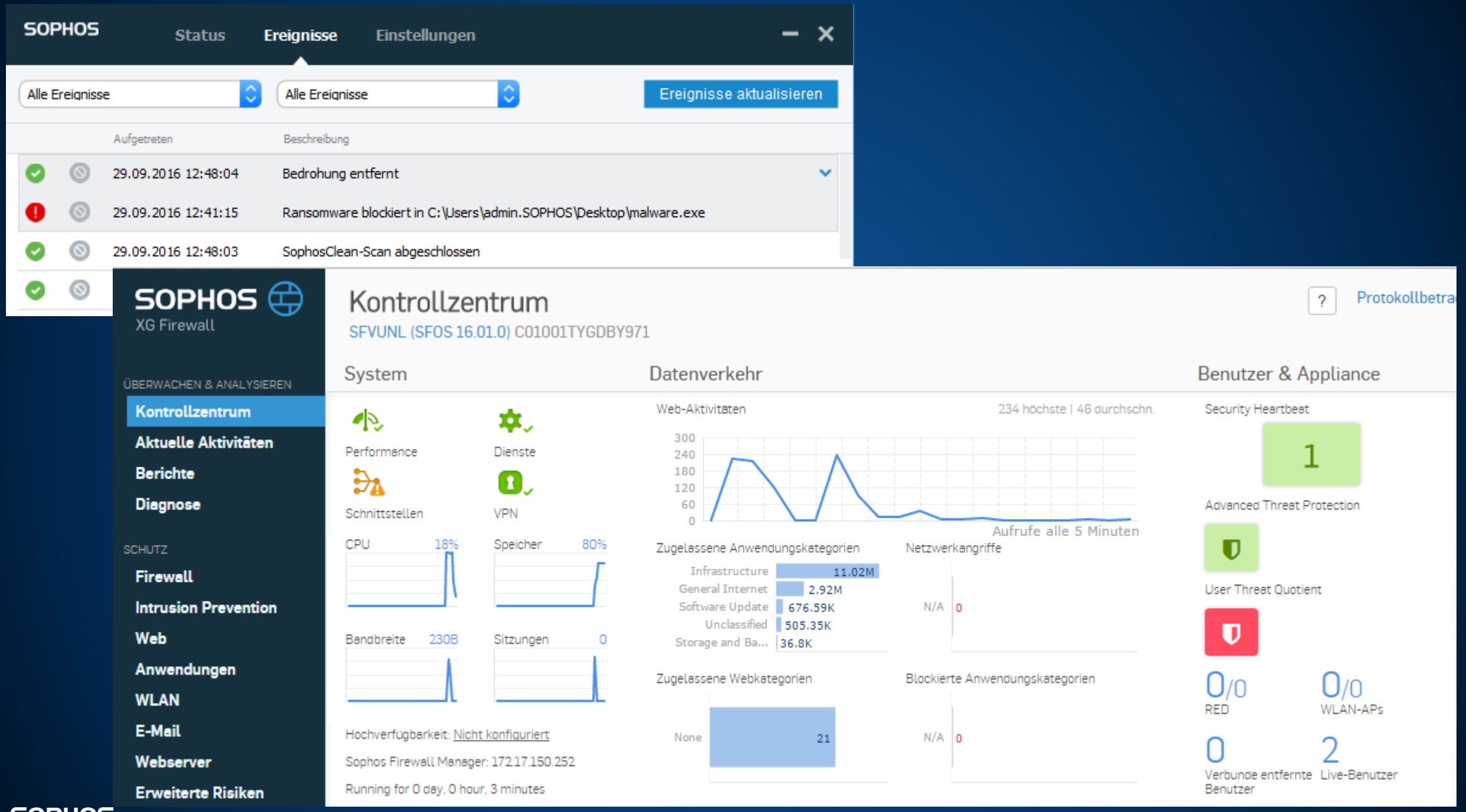

SOPHOS
Status
Ereignisse
Einstellungen
Sophos Central-Richtlinie für bis zu 4 Stunden zur Problembehebung außer Kraft setzen
Echtzeit-Scans
Dateien
Internet
Kontrolle über Benutzer
Peripheral Control
Application Control
Web Control
Manipulationsschutz
Laufzeitschutz
Ransomware-Erkennung (CryptoGuard)
Sicheres Surfen im Internet
Exploit-Abwehr
Erkennung schädlichen Datenverkehrs
Erkennung von schädlichem Verhalten (HIPS)
Hilfe
Informationen


Rechnung
Typ: Microsoft Word-Dokument mit Makros
Autoren: admin
Größe: 18,6 KB
Änderungsdatum: 02.09.2016 16:34
Vertraulich
Datei
Start
Freigeben
Ansicht
Vertraulich
"Vertraulich...
Name
Änderungsdatum
Typ
Größe
test_00
test_01
test_02
test_03
test_04
test_05
test_06
test_07
8 Elemente
Vertraulich
Datei
Start
Freigeben
Ansicht
Vertraulich
"Vertraulich...
Name
Änderungsdatum
Typ
Größe
test_00 21.09.2016 14:12 Rich-Text-Format 1 KB
test_00.rtf.hydracrypt_ID_F1EE3D30 21.09.2016 14:12 HYDRACRYPT_ID_... 1 KB
test_01 21.09.2016 14:12 Rich-Text-Format 1 KB
test_01.rtf.hydracrypt_ID_F1EE3D30 21.09.2016 14:12 HYDRACRYPT_ID_... 1 KB
test_02 21.09.2016 14:12 Rich-Text-Format 1 KB
test_02.rtf.hydracrypt_ID_F1EE3D30
test_02.rtf.hydracrypttmp_ID_F1EE3D30
test_03
test_04
test_05
12 Elemente
Sophos Endpoint
Ransomware blockiert in
C:\Users\admin.SOPHOS\Desktop\prog\Sop
SafeGuard hat Ihre Dateie gesichert.
Ihr Computer könnt eventuell unsicher sein.
SafeGuard hat Ihre verschlüsselten Dateien gesichert und Sie können sie für
SOPHOS

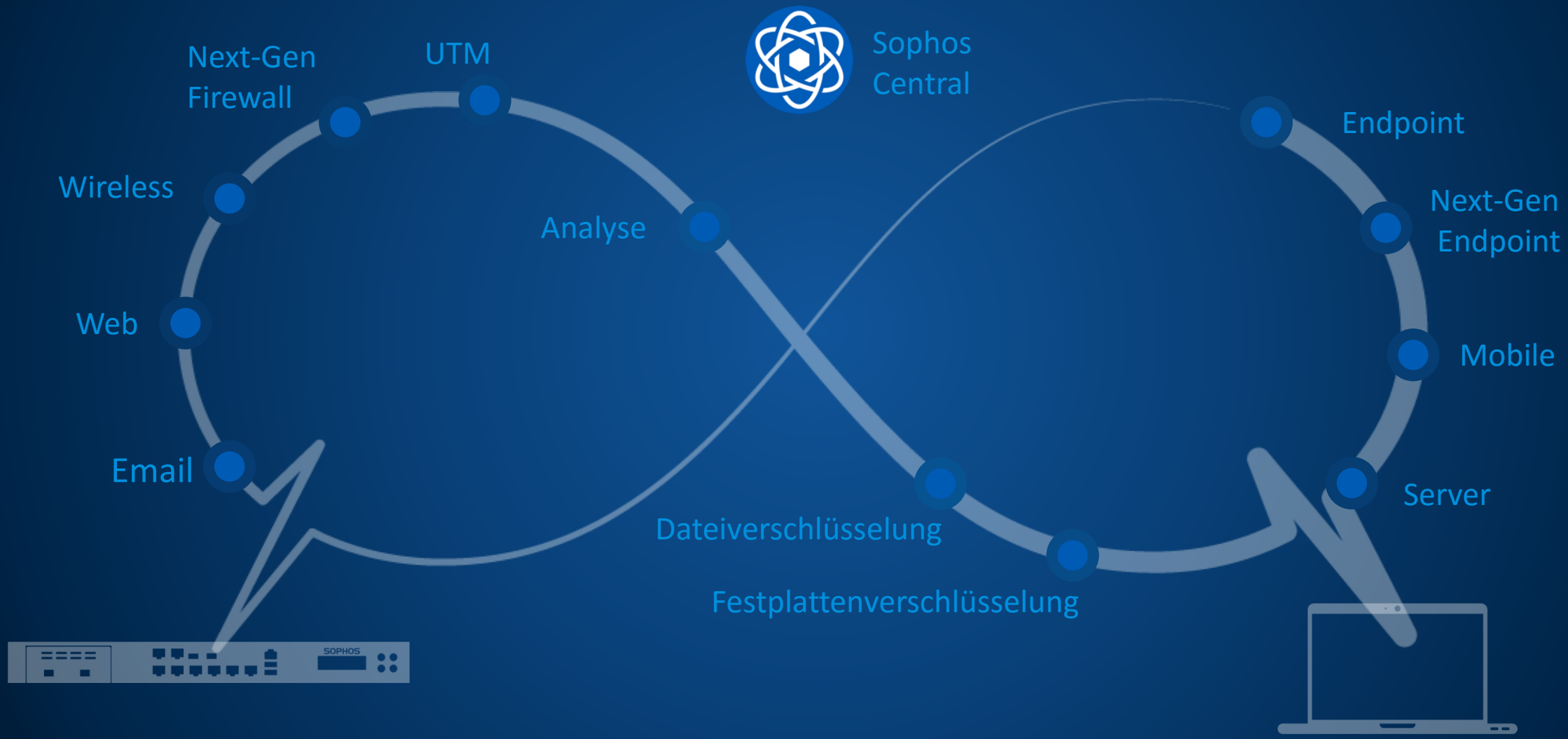

HTTP access denied
www.heise.de
XG
SOPHOS
Blocked request: Sophos Security Heartbeat
Your network access has been restricted by Security Heartbeat on Sophos Firewall.
Please contact your network administrator.
SOPHOS
XG Firewall
ÜBERWACHEN & ANALYSIEREN
Kontrollzentrum
Aktuelle Aktivitäten
Berichte
Diagnose
SCHUTZ
Firewall
Intrusion Prevention
Web
Anwendungen
WLAN
E-Mail
Webserver
Erweiterte Risiken
Kontrollzentrum
SFVUNL (SFOS 16.01.0) C01001TYGDBY971
Protokollbetrachter
System
Performance
Dienste
Schnittstellen
VPN
CPU 26%
Speicher 81%
Bandbreite 6KB
Sitzungen 2
Hochverfügbarkeit: Nicht konfiguriert
Sophos Firewall Manager: 172.17.150.252
Running for 0 day, 5 hours, 17 minutes
Datenverkehr
Web-Aktivitäten
330 höchste | 73 durchschn.
400
320
240
160
80
0
Aufrufe alle 5 Minuten
Zugelassene Anwendungskategorien
General Internet 8.58M
Infrastructure 1.7M
Software Update 1.1M
Storage and Ba... 260.92K
General Business 41.53K
Netzwerkangriffe
N/A 0
Zugelassene Webkategorien
None 2.08K
Personal Netwo... 585
Portal Sites 221
Information Te... 120
IPAddress 11
Blockierte Anwendungskategorien
Storage and Ba... 505
General Internet 160
Software Update 16
Benutzer & Appliance
Security Heartbeat
1
System at risk
Advanced Threat Protection
User Threat Quotient
0/0
RED
0/0
WLAN-APs
0
Verbunde entfernte Benutzer
1
Live-Benutzer
Für weitere Einzelheiten klicken Sie auf die Kontrollelemente.


SOPHOS
CENTRAL
Admin
ANALYSIEREN
Dashboard
Alarme
Protokolle & Berichte
Ursachenanalyse
SCHUTZ VERWALTEN
Personen
Computer
Mobile Geräte
Server
Wireless
Posteingänge
KONFIGURIEREN
Richtlinien
Systemeinstellungen
Geräte schützen
SOPHOS CENTRAL
Produkte kennenlernen
Details zur Ursachenanalyse
Ursachenanalyse / Details zur Ursachenanalyse
Hilfe
Sophos Ltd
Sophos Ltd · Superadmin
ÜBERBLICK
ARTEFAKTE
VISUALISIEREN
Priorität: Hoch
Status: Neu
Angezeigt werden:
Dateien
Prozesse
Registrierungsschlüssel
Netzwerkverbindungen
Bezeichnungen anzeigen:
16 D
4 I
U
95 D
3 D
23 D
19 D
5 D
155 R
145 D
49 R
D
schreiben
verbinden
lesen
übergeordnet zu
c:\program files (x86)\microsoft office\office14\outlook.exe
c:\users\admin.sophos\desktop\prog\sophostester.exe
Hauptursache
Beacon

SOPHOS


SOPHOS
Status
Ereignisse
Einstellungen
Alle Ereignisse
Alle Ereignisse
Ereignisse aktualisieren
Aufgetreten
Beschreibung
29.09.2016 12:48:04
Bedrohung entfernt
29.09.2016 12:41:15
Ransomware blockiert in C:\Users\admin.SOPHOS\Desktop\malware.exe
29.09.2016 12:48:03
SophosClean-Scan abgeschlossen
SOPHOS
XG Firewall
Kontrollzentrum
SFVUNL (SFOS 16.01.0) C01001TYGDBY971
Protokollbetra
ÜBERWACHEN & ANALYSIEREN
Kontrollzentrum
Aktuelle Aktivitäten
Berichte
Diagnose
SCHUTZ
Firewall
Intrusion Prevention
Web
Anwendungen
WLAN
E-Mail
Webserver
Erweiterte Risiken
System
Performance
Dienste
Schnittstellen
VPN
CPU 18%
Speicher 80%
Bandbreite 230B
Sitzungen 0
Hochverfügbarkeit: Nicht konfiguriert
Sophos Firewall Manager: 172.17.150.252
Running for 0 day, 0 hour, 3 minutes
Datenverkehr
Web-Aktivitäten
234 höchste | 46 durchschn.
300
240
180
120
60
0
Aufrufe alle 5 Minuten
Zugelassene Anwendungskategorien
Infrastructure 11.02M
General Internet 2.92M
Software Update 676.59K
Unclassified 505.35K
Storage and Ba... 36.8K
Netzwerkangriffe
N/A 0
Zugelassene Webkategorien
None 21
Blockierte Anwendungskategorien
N/A 0
Benutzer & Appliance
Security Heartbeat
1
Advanced Threat Protection
User Threat Quotient
0/0
RED
0/0
WLAN-APs
0
Verbunde entfernte Benutzer
2
Live-Benutzer

Synchronized Security – Teamplay statt Best-of-Breed



Synchronized Security von Sophos

- Best-of-Breed wird ersetzt durch Security als System
- Kommunikation von Netzwerk-, Endpoint-, Server- und Verschlüsselungslösungen
- Erkennung hochentwickelter Bedrohungen
- Identifizierung kompromittierter Systeme
- Automatische Reaktion auf Vorfälle
- Analyse der Infektions- und Verbreitungswege
- Kommend: Security Heartbeat Überprüfung auf WLAN-APs
  Security Heartbeat auf Smartphones & Tablets
  ...

SOPHOS

Security made simple.