SOPHOS | discover

NEXT-GEN

# Synchronized Security

## Teamplay vs. Best-of-Breed

**Michael Veit**
Technology Evangelist

SOPHOS

# Sophos – mehr als 30 Jahre Erfahrung

1985
GRÜNDUNG
**OXFORD, UK**

630M
**UMSATZ**
*(FY17)*

3.000
**MITARBEITER**

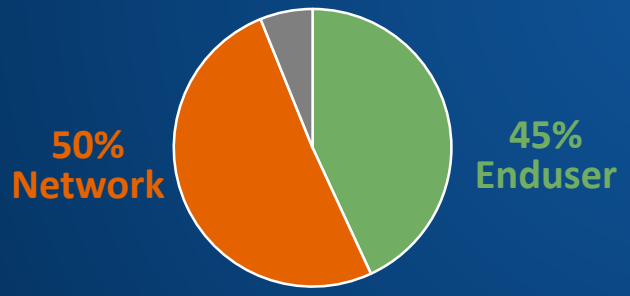
400
**in DACH**

HQ
**ABINGDON, UK**

200,000+
**KUNDEN**

100M+
**ANWENDER**

20,000+
**CHANNEL**
PARTNER



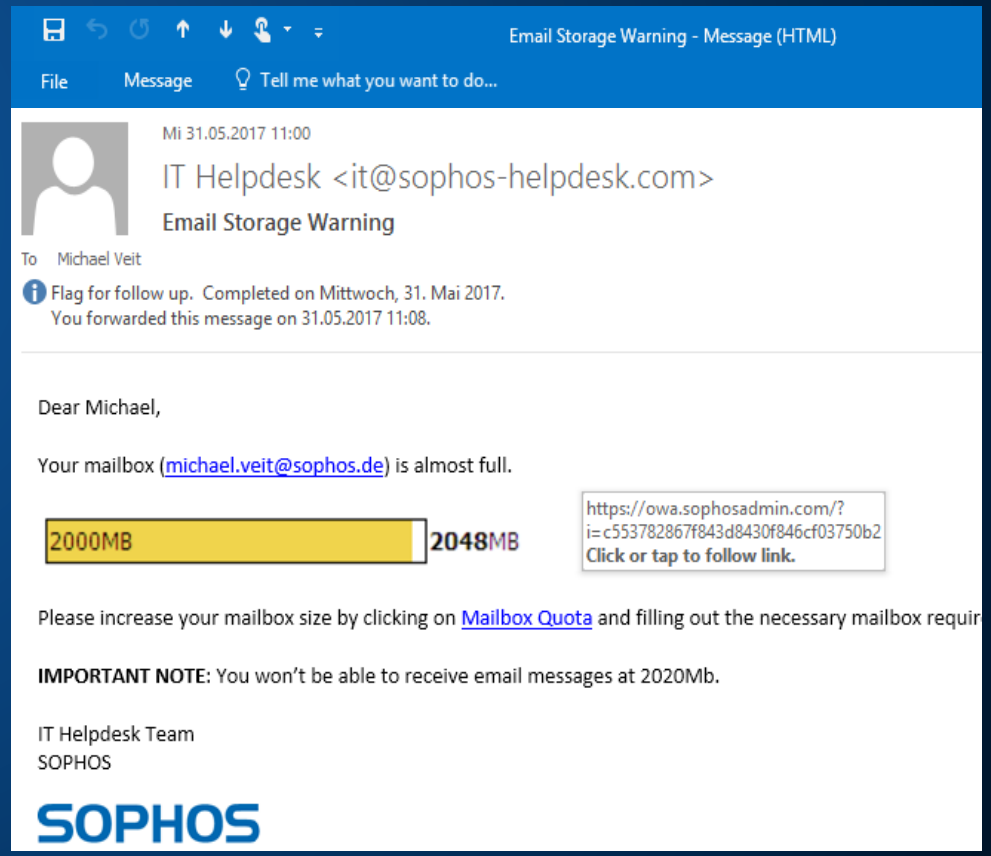

- Akquisition u.a. von Utimaco 2009, Astaro 2011, Dialogs 2012, Cyberoam 2014, Mojave 2014, Reflexion 2015, SurfRight 2015, Barricade 2016, Invincea 2017
- Gartner: Marktführer in den Bereichen Endpoint, Verschlüsselung & UTM

# Warum waren die Krypto-Trojaner so erfolgreich?

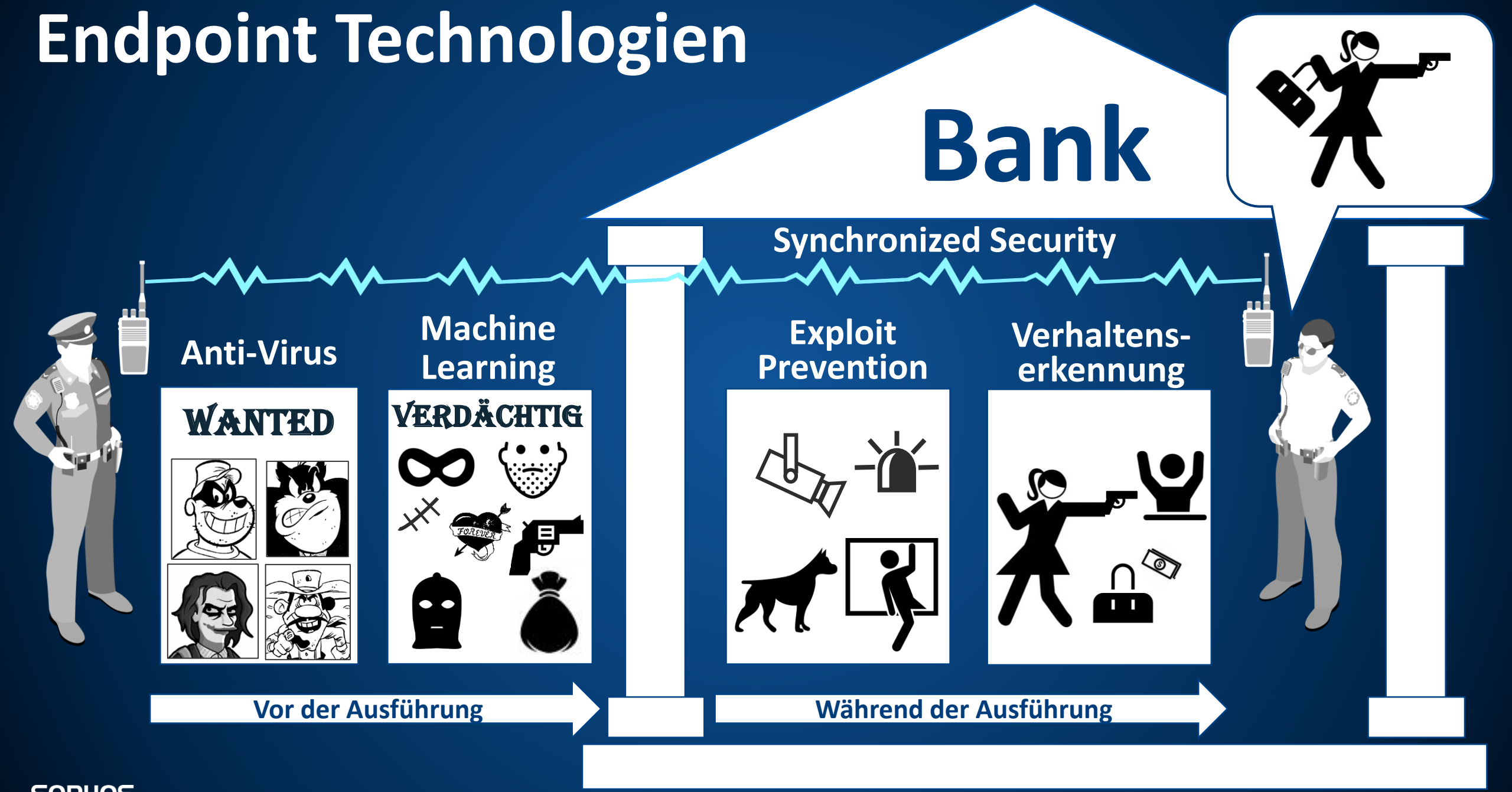
SOPHOS

# Gründe für Infektionen trotz Best-of-Breed Security

- Technologisch fortgeschrittene Schädlinge
- Hochprofessionelle Angreifer nutzen Löcher in Sicherheitskonzepten
- Patch-Strategie
- Geschicktes Social Engineering
- Sicherheitssysteme gegen moderne Bedrohungen fehlen
- Sicherheitssysteme agieren nicht als System



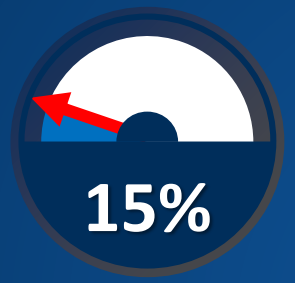
# Endpoint Technologien

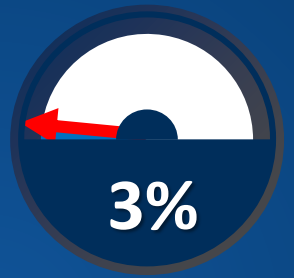


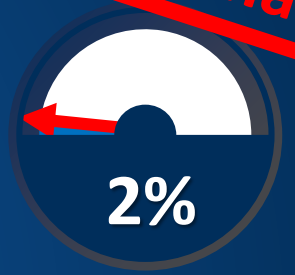

SOPHOS

# Wo Malware heute am Endpoint aufgehalten wird

400.000 neue Schädlinge / Tag


| Einfallsweg schließen | Analyse vor Ausführung | Exploit-Vehinderung | Verhaltens-Erkennung |
|---|---|---|---|
| • URL-Filterung<br>• Download Reputation<br>• Device Control<br>• App Control | • Signaturen<br>• Heuristiken<br>• Machine Learning | • Einbruchstechniken erkennen/verhindern<br>• Rechteausweitung verhindern | • Verschlüsselung<br>• Hacker-Aktivität<br>• Passwort- und Datendiebstahl |

INTERCEPT X

SOPHOS

# Sophos INTERCEPT X

**Zusätzlich zur Endpoint Protection**

## *Schutz gegen Ransomware & Co*

- **Deep Learning** erkennt unbekannte Malware
- **CryptoGuard** erkennt **Verschlüsselung** und stellt Originaldateien wieder her

## *Anti-Hacker*

- **Signaturloser Schutz** vor Zero-Day-Angriffen
- **Exploit**-Erkennung
- **Anti-Hacker** Technologien
- Schutz vor **Passwort-Diebstahl**

## *Erweiterte Bereinigung*

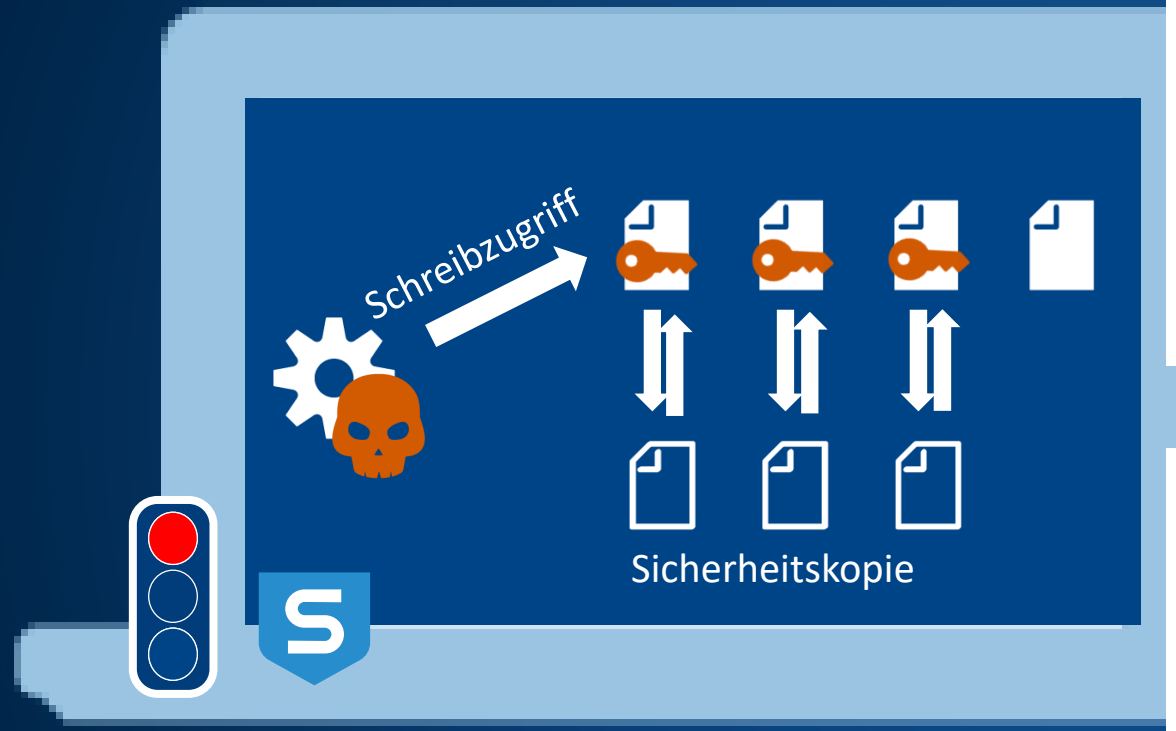
- **Signaturlose** Erkennung und **Entfernung** von bisher unbekannter Malware
- Stellt **Originaldateien** wieder her

## *Ursachenanalyse*

- **Grafische Analyse** der Infektions- und Verbreitungswege
- Was ist **passiert**?
- Was ist **gefährdet**?
- Wie **verhindere** ich das **zukünftig**?

SOPHOS

# CryptoGuard – Schutz vor lokaler Ransomware




| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | 7B | 5C | 72 | 74 | 66 | 31 | 5C | 61 | 6E | 73 | 69 | 5C | 61 | 6E | 73 | 69 | {\rtf1\ansi\ansi |
| 00000010 | 63 | 70 | 67 | 31 | 32 | 35 | 32 | 5C | 64 | 65 | 66 | 66 | 30 | 5C | 64 | 65 | cpg1252\deff0\de |
| 00000020 | 66 | 6C | 61 | 6E | 67 | 31 | 30 | 34 | 33 | 7B | 5C | 66 | 6F | 6E | 74 | 74 | flang1043{\fontt |
| 00000030 | 62 | 6C | 7B | 5C | 66 | 30 | 5C | 66 | 6E | 69 | 6C | 5C | 66 | 63 | 68 | 61 | bl{\f0\fnil\fcha |
| 00000040 | 72 | 73 | 65 | 74 | 30 | 20 | 56 | 65 | 72 | 64 | 61 | 6E | 61 | 3B | 7D | 7D | rset0 Verdana;}} |
| 00000050 | 5C | 72 | 5C | 6E | 5C | 76 | 69 | 65 | 77 | 6B | 69 | 6E | 64 | 34 | 5C | 75 | \r\n\viewkind4\u |
| 00000060 | 63 | 31 | 5C | 70 | 61 | 72 | 64 | 5C | 73 | 61 | 32 | 30 | 30 | 5C | 73 | 6C | c1\pard\sa200\sl |
| 00000070 | 32 | 37 | 36 | 5C | 73 | 6C | 6D | 75 | 6C | 74 | 31 | 5C | 6C | 61 | 6E | 67 | 276\slmult1\lang |
| 00000080 | 39 | 5C | 66 | 30 | 5C | 66 | 73 | 32 | 32 | 20 | 54 | 68 | 65 | 20 | 71 | 75 | 9\f0\fs22 The qu |
| 00000090 | 69 | 63 | 6B | 20 | 62 | 72 | 6F | 77 | 6E | 20 | 66 | 6F | 78 | 20 | 6A | 75 | ick brown fox ju |
| 000000A0 | 6D | 70 | 73 | 20 | 6F | 76 | 65 | 72 | 20 | 74 | 68 | 65 | 20 | 6C | 61 | 7A | mps over the laz |
| 000000B0 | 79 | 20 | 64 | 6F | 67 | 2E | 7D | | | | | | | | | | y dog.} |

Unverschlüsselte Datei vor Schreibvorgang

| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | 7D | EB | 10 | B2 | FD | 8E | EB | B9 | D1 | F6 | D8 | DE | CC | 9B | F6 | CB | }ë.²ýŽë¹ÑöØÞÌ›öË |
| 00000010 | C4 | D9 | C3 | F6 | CB | C4 | D9 | C3 | C9 | DA | CD | 9B | 98 | 9F | 98 | F6 | ÄÙÃöËÄÙÃÉÚÍ›˜Ÿ˜ö |
| 00000020 | CE | CF | CC | CC | 9A | F6 | CE | CF | CC | C6 | CB | C4 | CD | 9B | 9A | 9E | ÎÏÌÌšöÎÏÌÆËÄÍ›šž |
| 00000030 | 99 | D1 | F6 | CC | C5 | C4 | DE | DE | C8 | C6 | D1 | F6 | CC | 9A | F6 | CC | ™ÑöÌÅÄÞÞÈÆÑöÌšöÌ |
| 00000040 | C4 | C3 | C6 | F6 | CC | C9 | C2 | CB | D8 | D9 | CF | DE | 9A | 8A | FC | CF | ÄÃÆöÌÉÂËØÙÏÞšŠüÏ |
| 00000050 | D8 | CE | CB | C4 | CB | 91 | D7 | D7 | F6 | D8 | F6 | C4 | F6 | DC | C3 | CF | ØÎËÄË'××öØöÄöÜÃÏ |
| 00000060 | DD | C1 | C3 | C4 | CE | 9E | F6 | DF | C9 | 9B | F6 | DA | CB | D8 | CE | F6 | ÝÁÃÄÎžößÉ›öÚËØÎö |
| 00000070 | D9 | CB | 98 | 9A | 9A | F6 | D9 | C6 | 98 | 9D | 9C | F6 | D9 | C6 | C7 | DF | ÙË˜šš öÙÆ˜.œöÙÆÇß |
| 00000080 | C6 | DE | 9B | F6 | C6 | CB | C4 | CD | 93 | F6 | CC | 9A | F6 | CC | D9 | 98 | ÆÞ›öÆËÄÍ"öÌšöÌÙ˜ |
| 00000090 | 98 | 8A | FE | C2 | CF | 8A | DB | DF | C3 | C9 | C1 | 8A | C8 | D8 | C5 | DD | ˜ŠþÂÏŠÛßÃÉÁŠÈØÅÝ |
| 000000A0 | C4 | 8A | CC | C5 | D2 | 8A | C0 | DF | C7 | DA | D9 | 8A | C5 | DC | CF | D8 | ÄŠÌÅÒŠÀßÇÚÙŠÅÜÏØ |
| 000000B0 | 8A | DE | C2 | CF | 8A | C6 | CB | D0 | D3 | 8A | CE | C5 | CD | 84 | D7 | | ŠÞÂÏŠÆËÐÓŠÎÅÍ„× |

Verschlüsselte Datei nach Schreibvorgang

- Ursachenanalyse
- Erweiterte Bereinigung

SOPHOS

# Wo lauert die größere Gefahr?


# Schutz vor unbekannter Malware über Exploit-Prevention

## Exploit Schutz

- Signaturloser Schutz vor Zero-Day-Angriffen
- Keine Performanceeinbußen
- Verhindert das Ausnutzen von Sicherheitslücken in unsicheren / ungepatchten Anwendungen
- Stoppt den Angriff

> The bad guys will inevitably get through any single layer of endpoint security controls. But they are much less likely to get through multiple layers and their chances of success decrease proportionately to the number of layers (..). Security layers need to extend beyond the endpoint (..) and into central analytics engines that can contextualize and correlate suspect events across different attack vectors.

Avivah Litan, Gartner

# Technologien zum Schutz gegen Bedrohungen

Gateway-Technologien

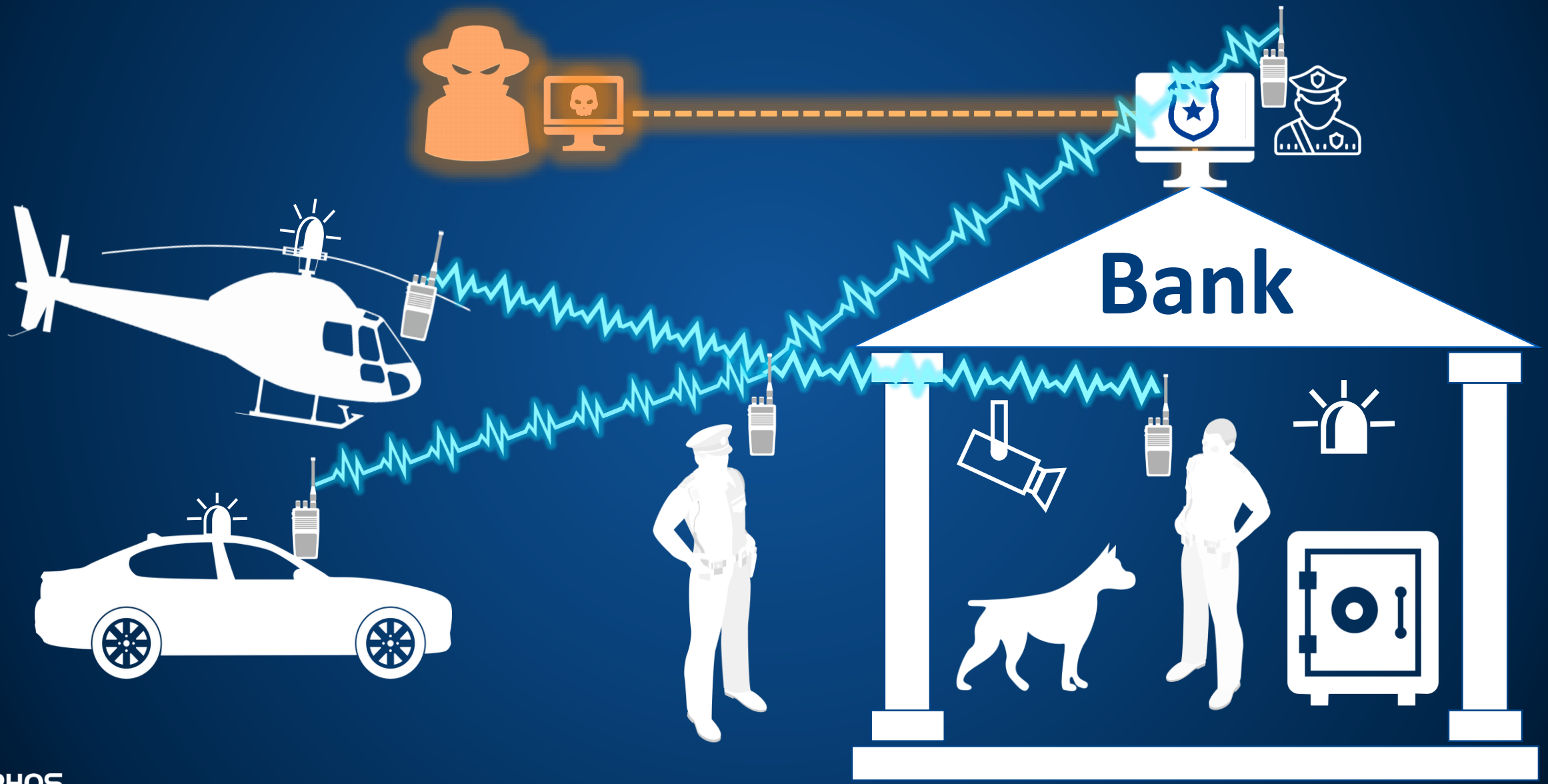
- Firewall / Netzwerksegmentierung
- Botnet-C&C-Erkennung
- Intrusion Prevention
- Web- und Emailfilterung
- Anti-Virus
- Web Application Firewall
- Next-Generation Sandbox

Endpoint-Technologien

- Anti-Virus
- Webfilter
- Device Control
- Application Control
- Verschlüsselung
- Whitelisting
- Machine Learning
- HIPS
- Verhaltenserkennung
- Exploit Prevention

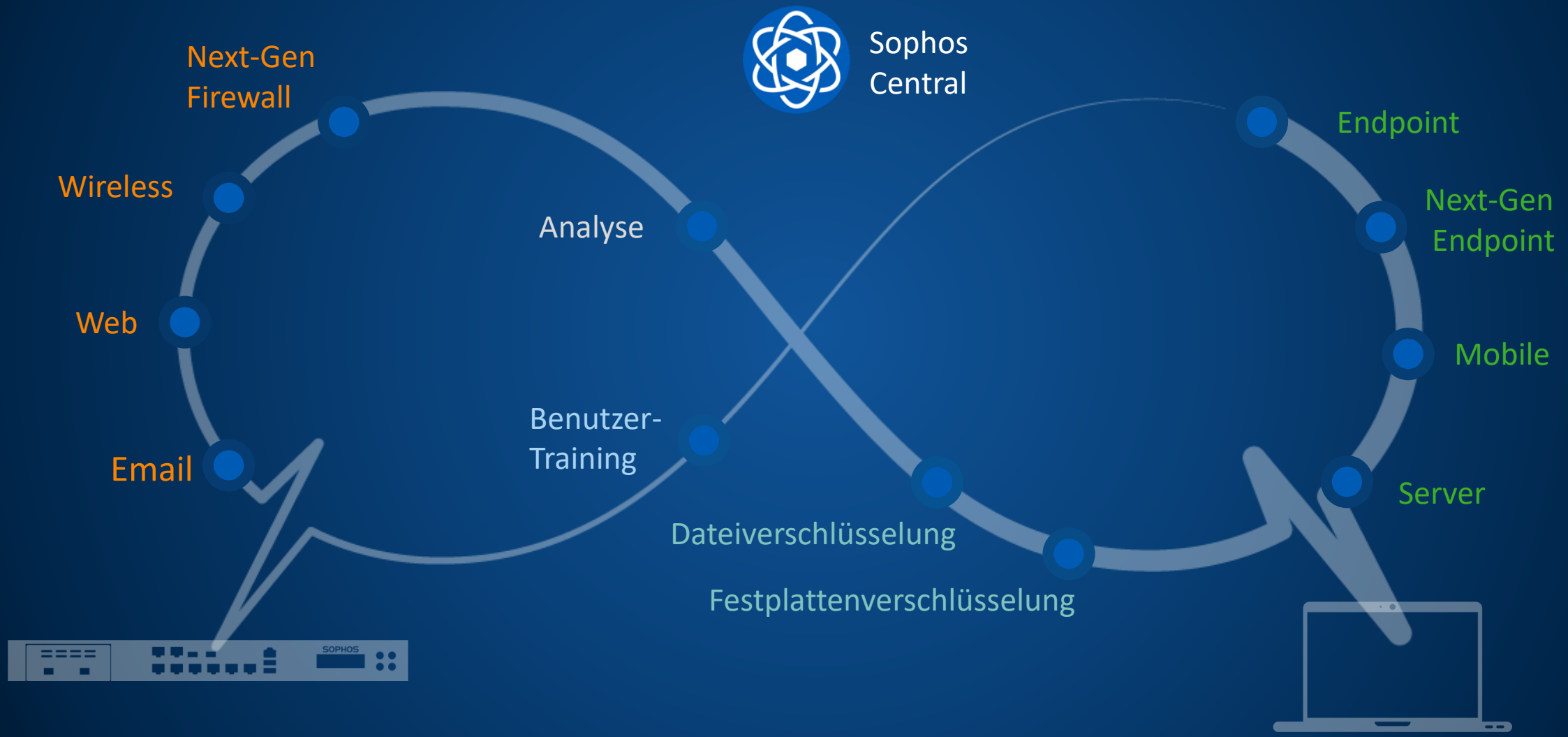
SOPHOS

# Sicherheit als System ersetzt Einzellösungen

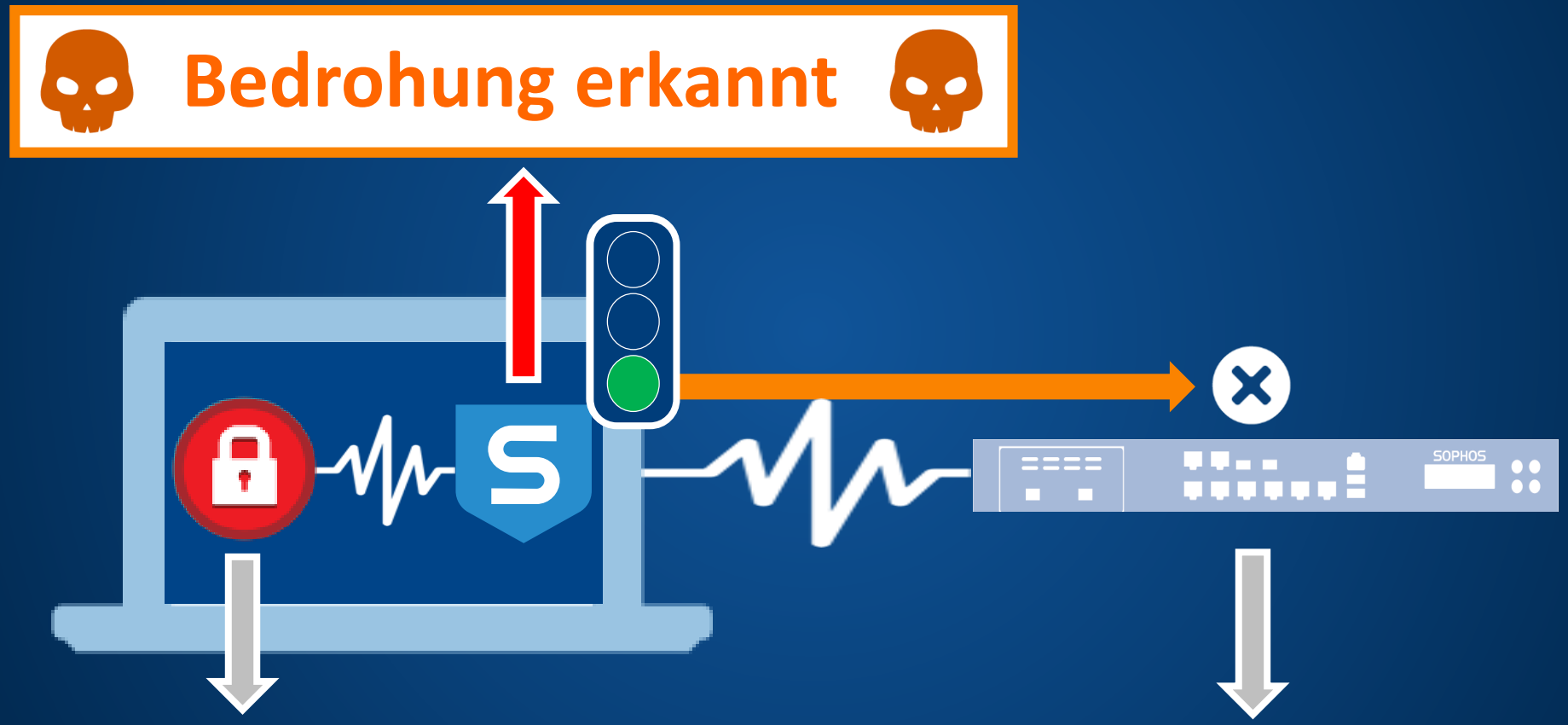



SOPHOS

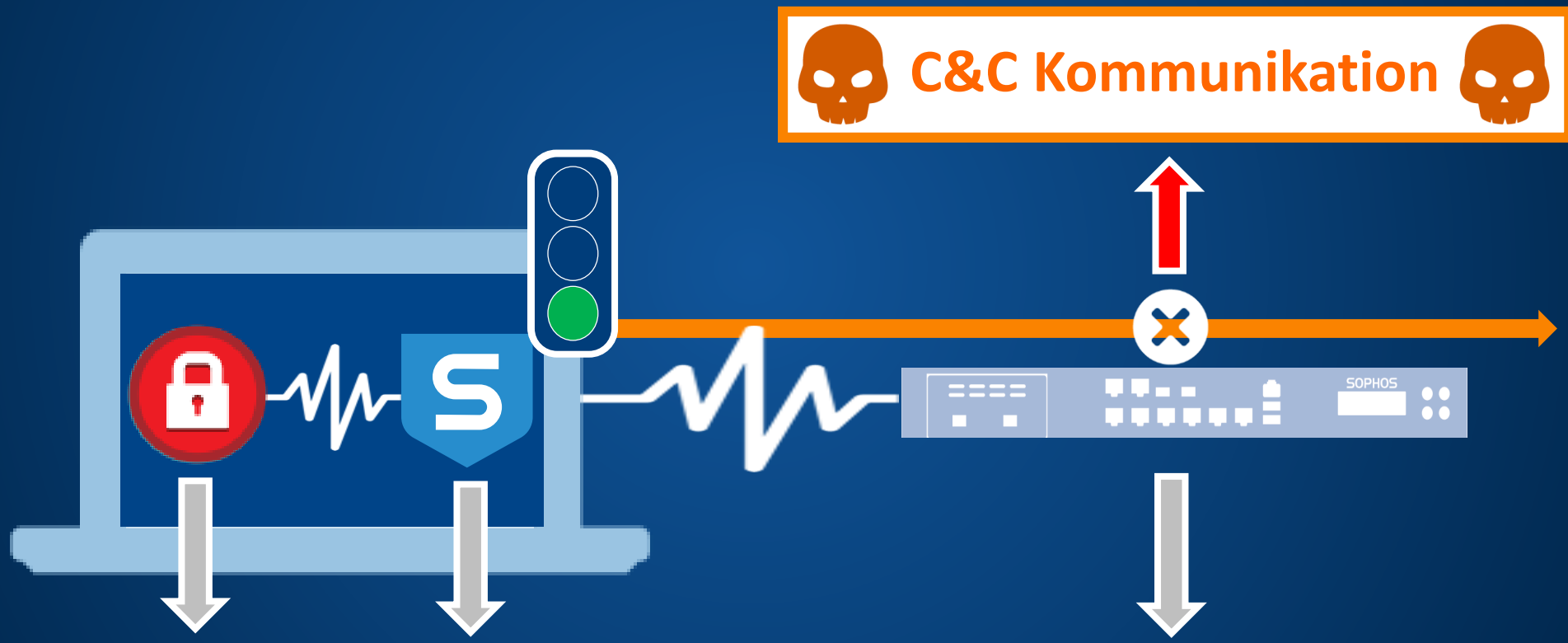
# Synchronized Security – Teamplay statt Best-of-Breed



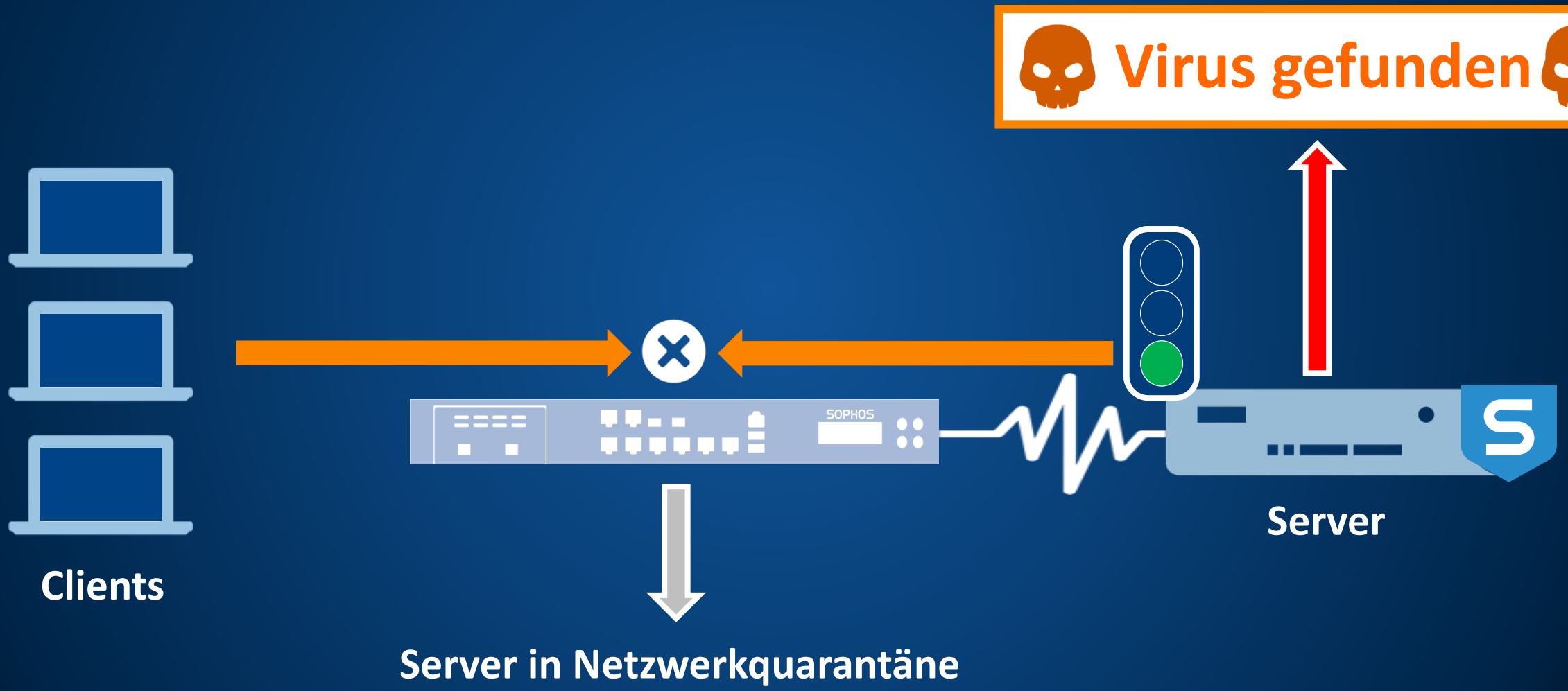
# Security Heartbeat – Zusammenspiel von Endpoint und Gateway



# Security Heartbeat – Botnet C&C-Verkehr erkannt

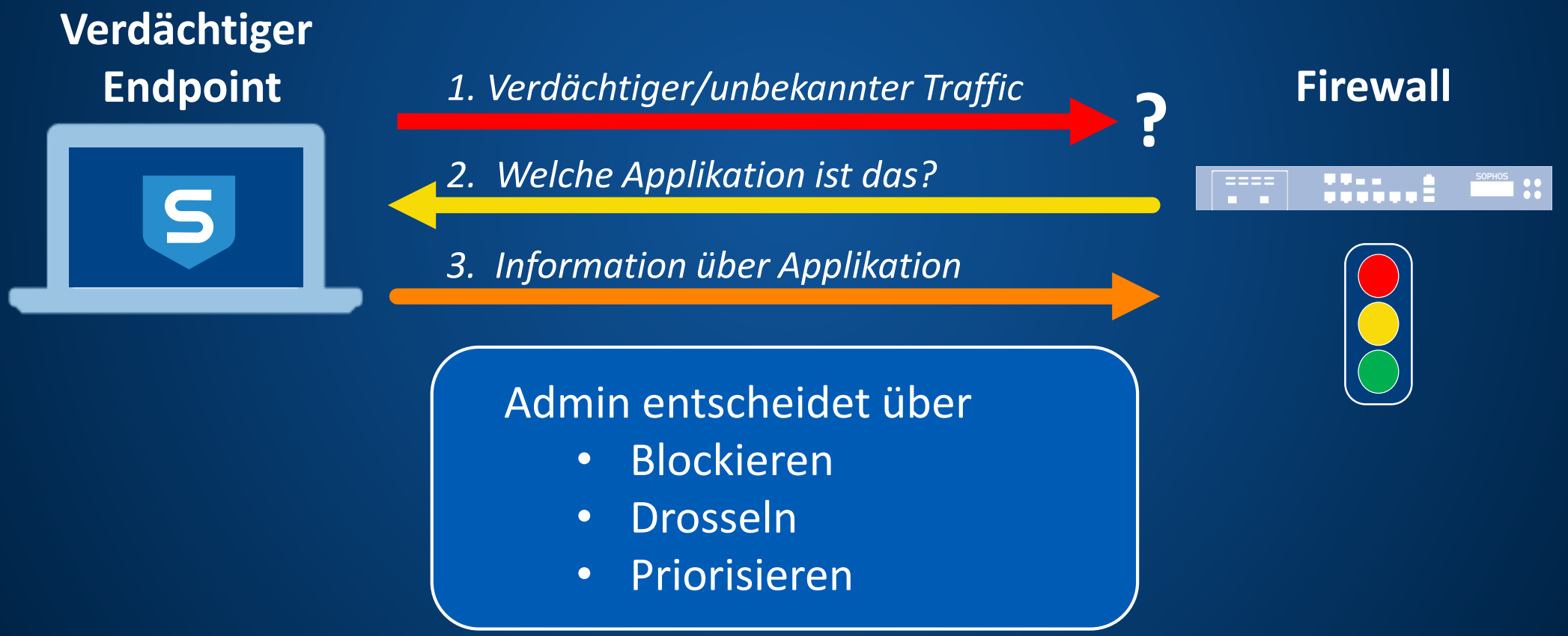


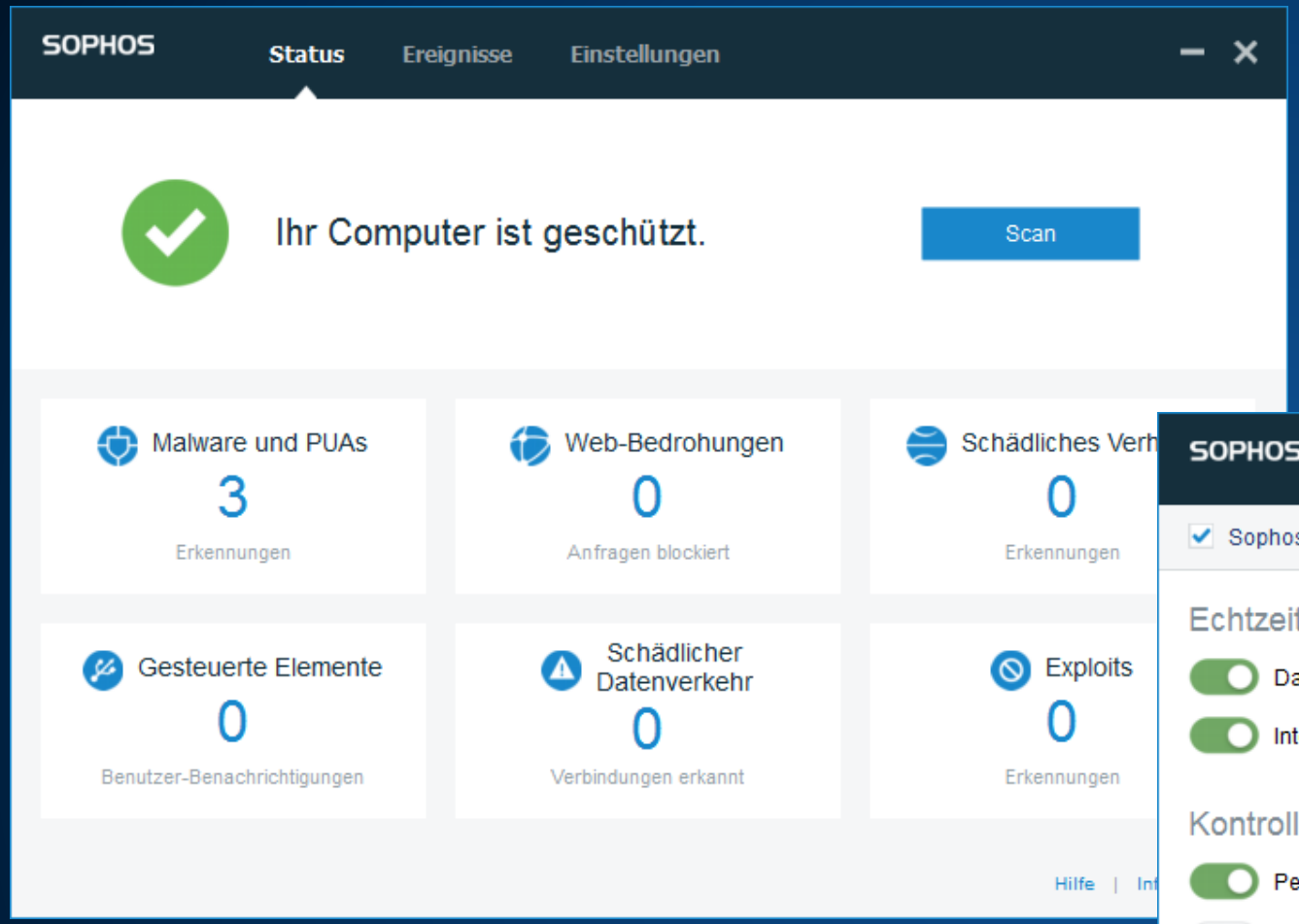
# Security Heartbeat – Server Heartbeat

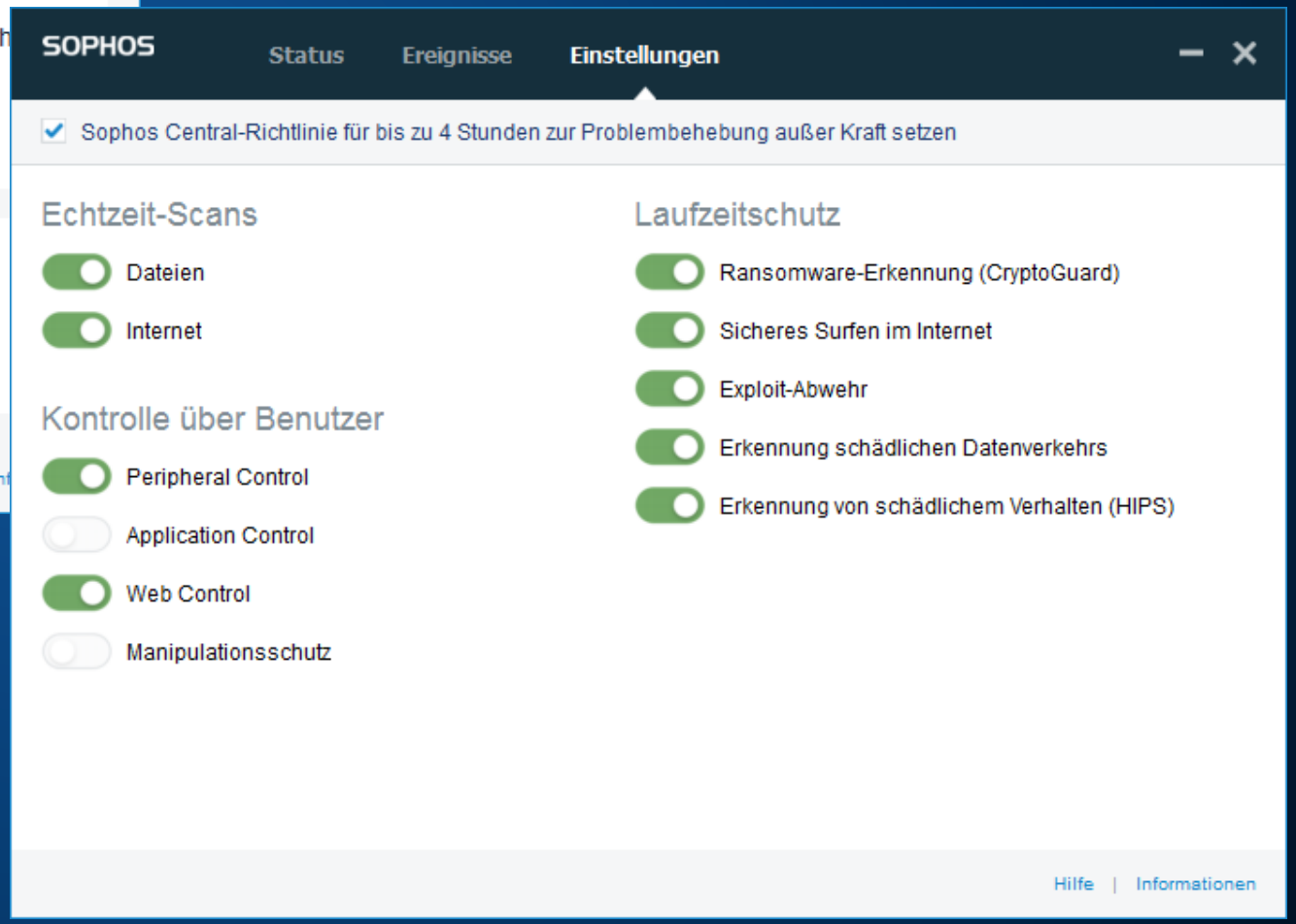


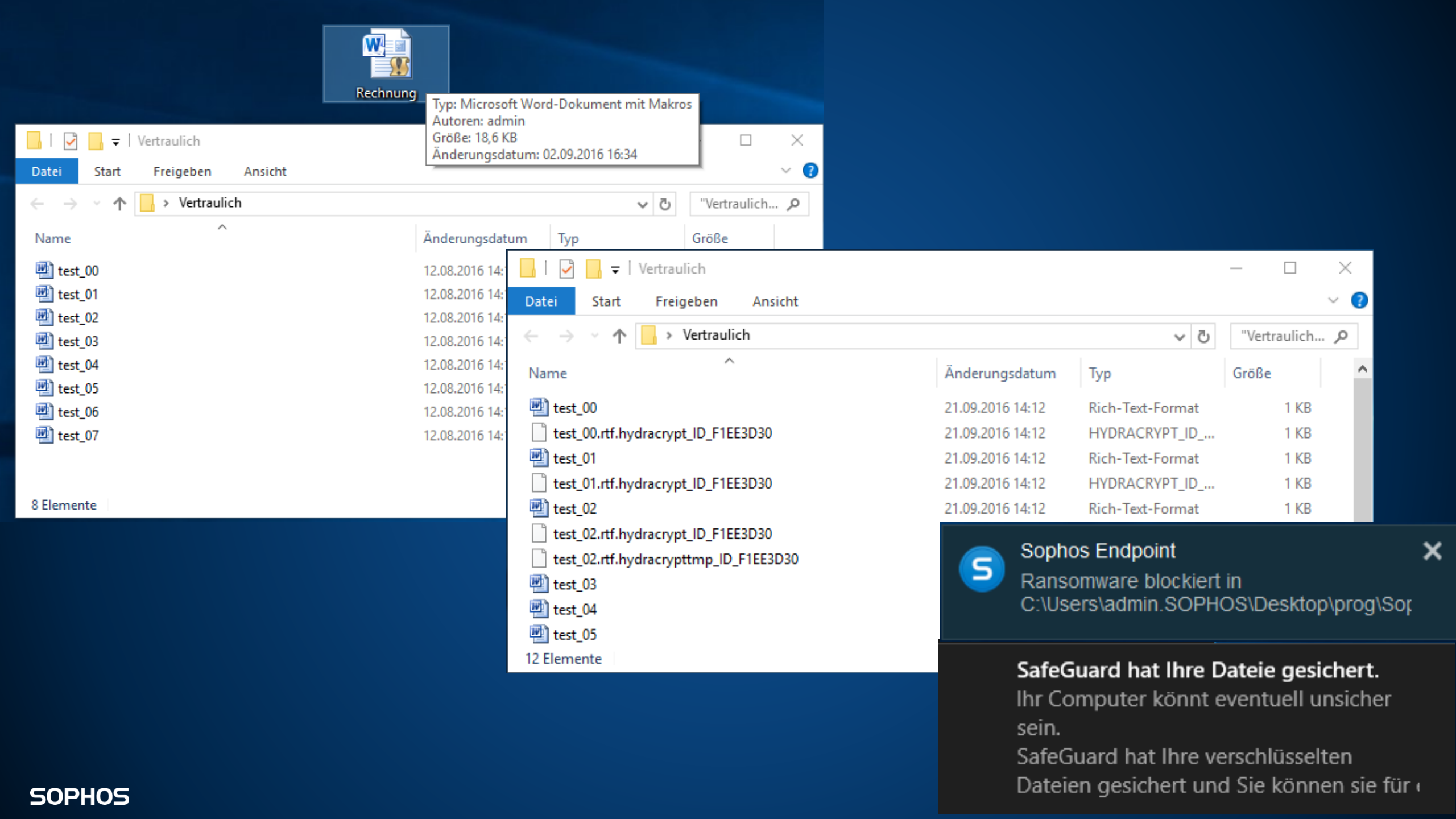
# Security Heartbeat – Applikationskontext (kommend)

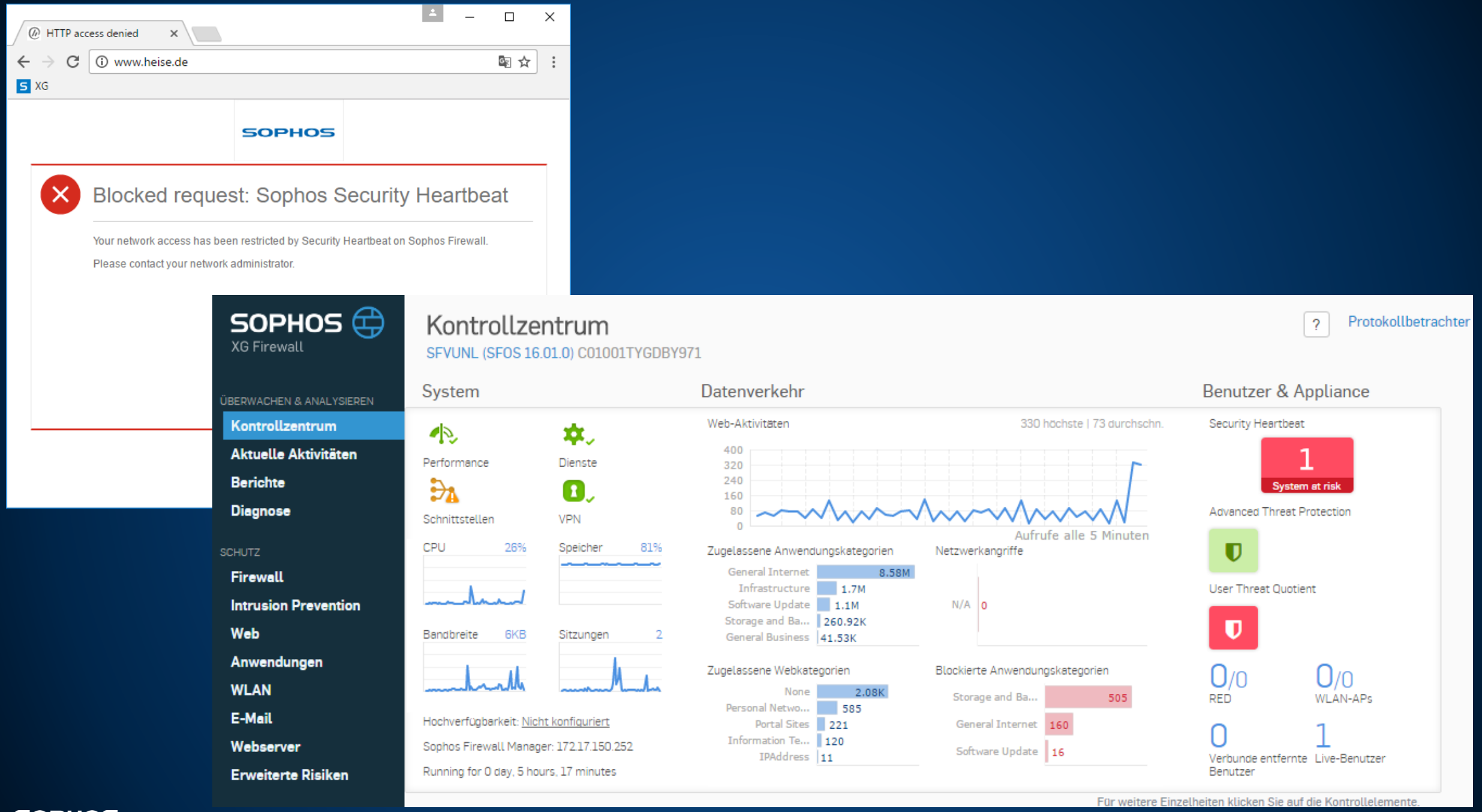
Informationen und Kontrolle über unbekannte Apps

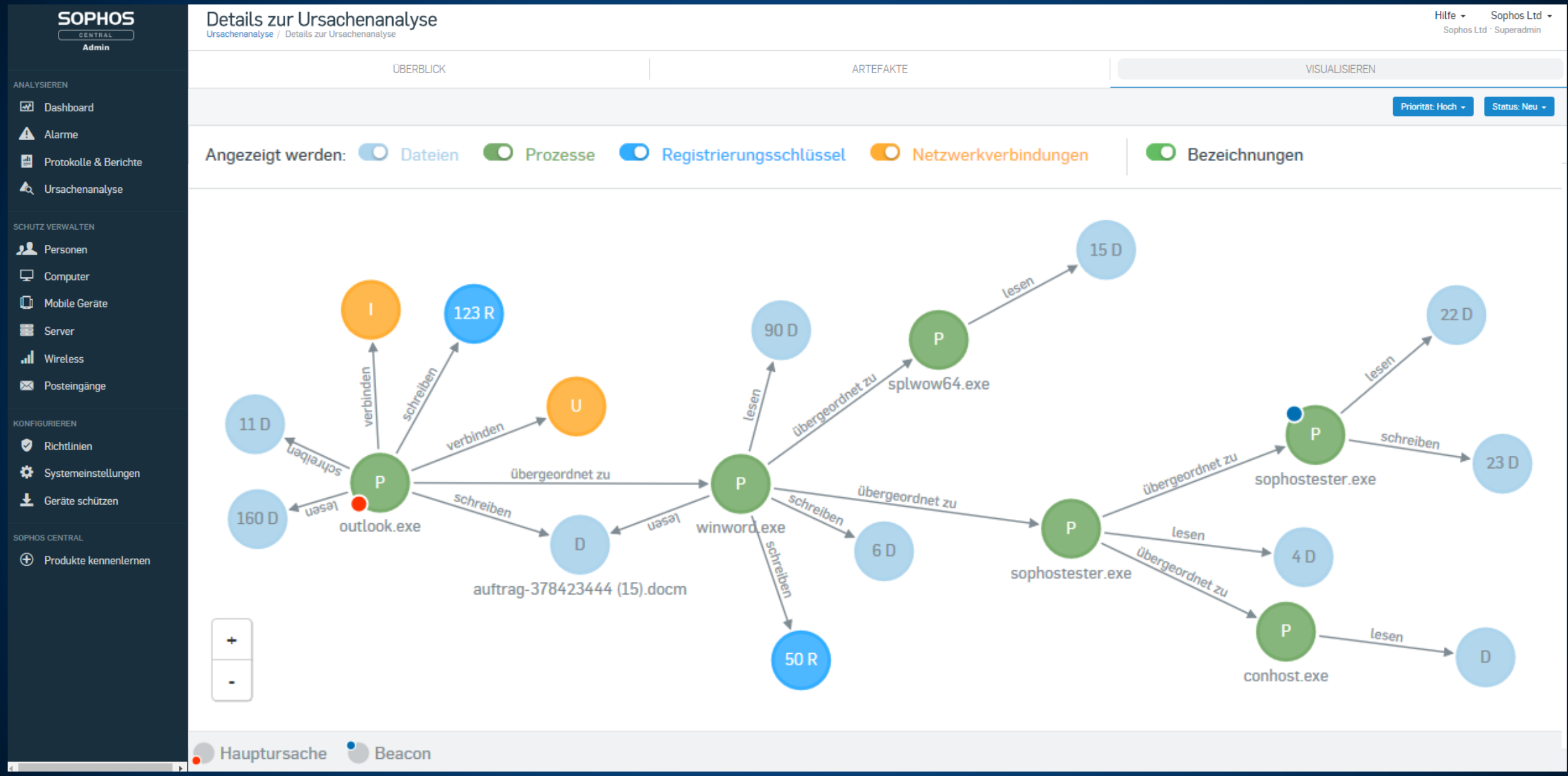



SOPHOS
Status
Ereignisse
Einstellungen
Ihr Computer ist geschützt.
Scan
Malware und PUAs
3
Erkennungen
Web-Bedrohungen
0
Anfragen blockiert
Schädliches Verh
0
Erkennungen
Gesteuerte Elemente
0
Benutzer-Benachrichtigungen
Schädlicher Datenverkehr
0
Verbindungen erkannt
Exploits
0
Erkennungen
Hilfe

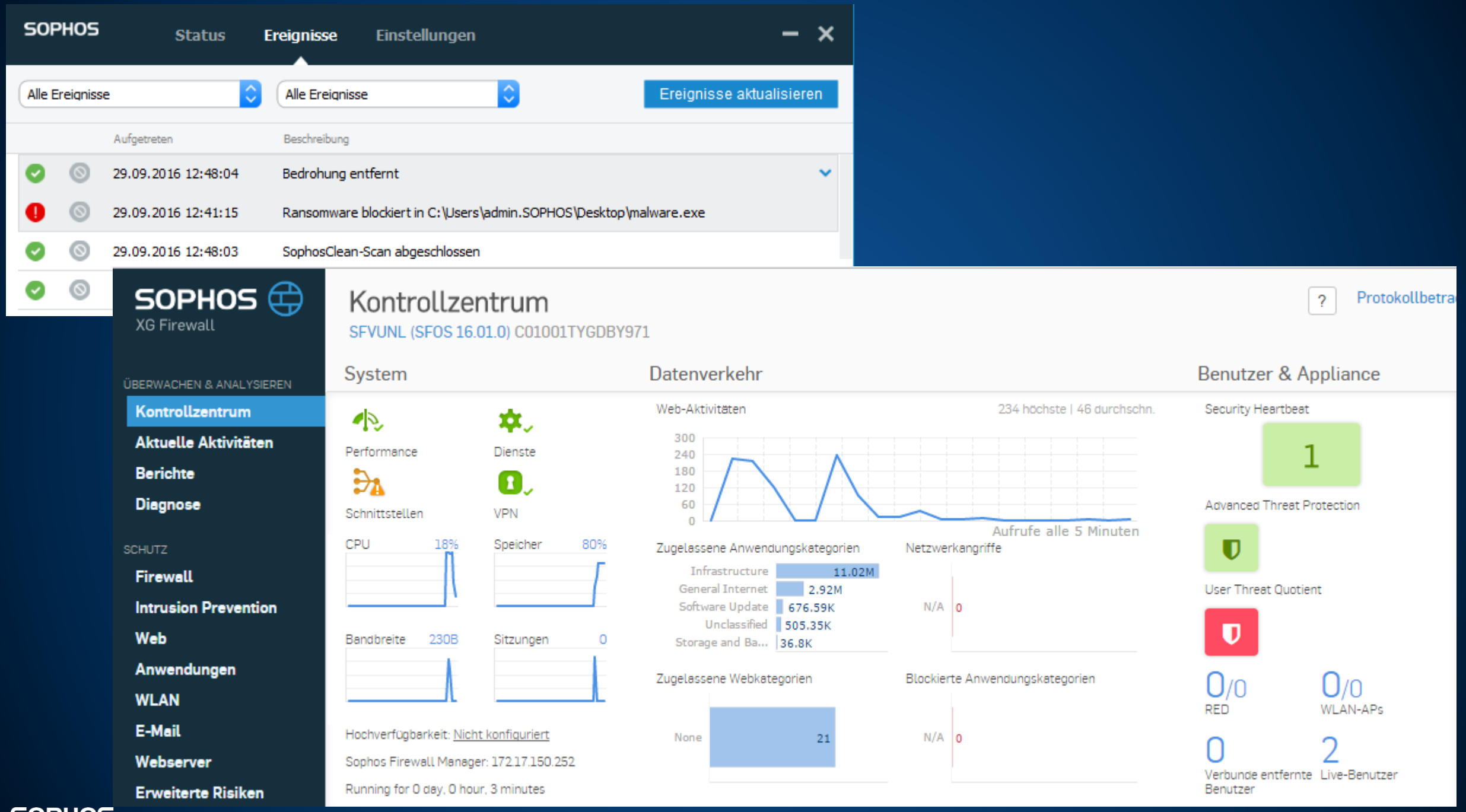

SOPHOS
Status
Ereignisse
Einstellungen
Sophos Central-Richtlinie für bis zu 4 Stunden zur Problembehebung außer Kraft setzen
Echtzeit-Scans
Dateien
Internet
Kontrolle über Benutzer
Peripheral Control
Application Control
Web Control
Manipulationsschutz
Laufzeitschutz
Ransomware-Erkennung (CryptoGuard)
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

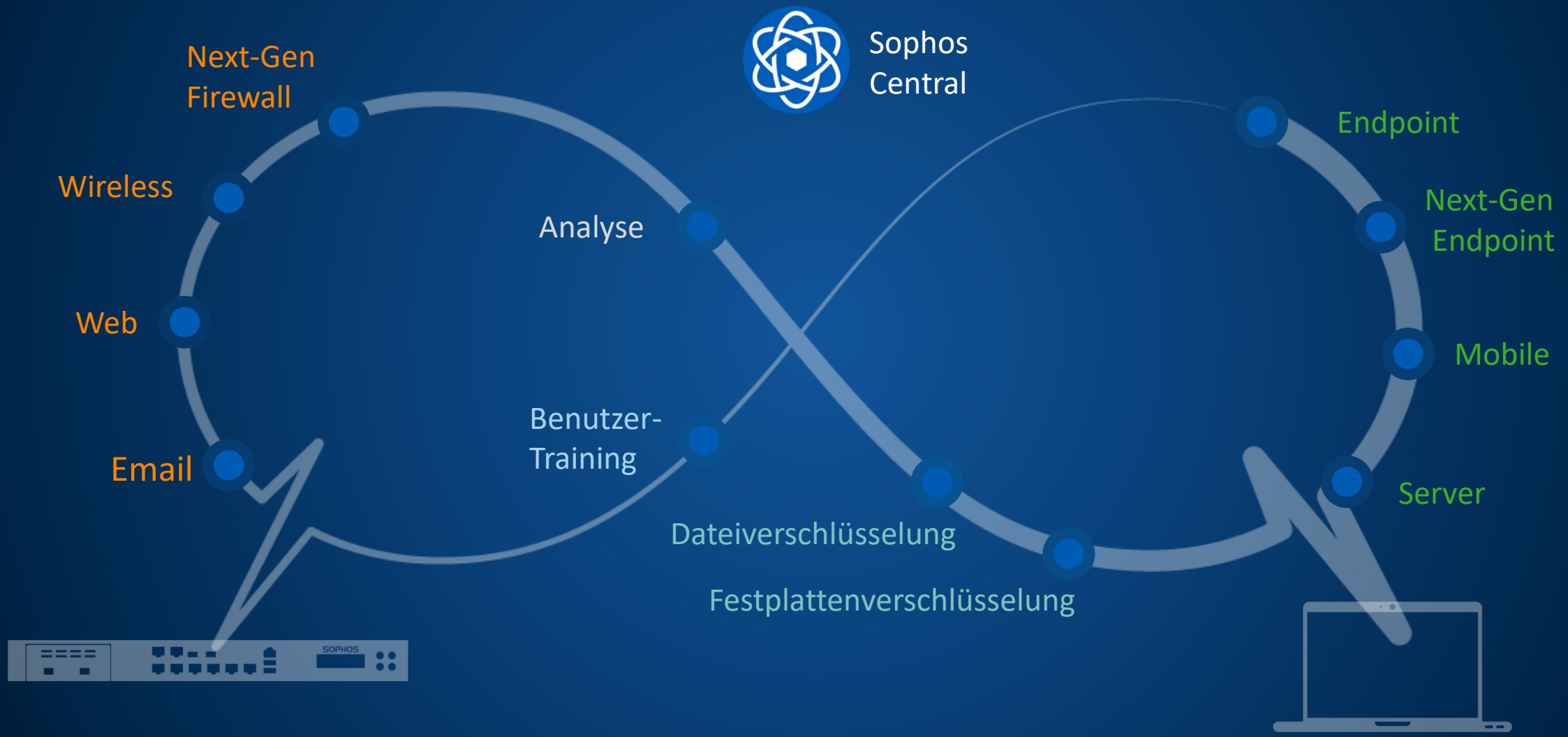

HTTP access denied
www.heise.de
XG
SOPHOS
Blocked request: Sophos Security Heartbeat
Your network access has been restricted by Security Heartbeat on Sophos Firewall.
Please contact your network administrator.
SOPHOS
XG Firewall
ÜBERWACHEN & ANALYSIEREN
Kontrollzentrum
Aktuelle Aktivitäten
Berichte
Diagnose
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
I
123 R
U
11 D
160 D
P
outlook.exe
verbinden
schreiben
verbinden
schreiben
lesen
übergeordnet zu
D
auftrag-378423444 (15).docm
90 D
lesen
übergeordnet zu
P
winword.exe
schreiben
6 D
schreiben
50 R
P
splwow64.exe
lesen
15 D
übergeordnet zu
P
sophostester.exe
lesen
22 D
schreiben
23 D
lesen
4 D
übergeordnet zu
P
conhost.exe
lesen
D
+
-
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 und Eindämmung von Hacker-Aktivitäten
- Automatische Reaktion auf Vorfälle
- Analyse der Infektions- und Verbreitungswege

SOPHOS

Security made simple.

michael.veit@sophos.de