SOPHOS

# EVOLVE

it-sa 2019

## Neue Technologien gegen Ransomware und Co.
## Sicherheit als System ersetzt Best-of-Breed

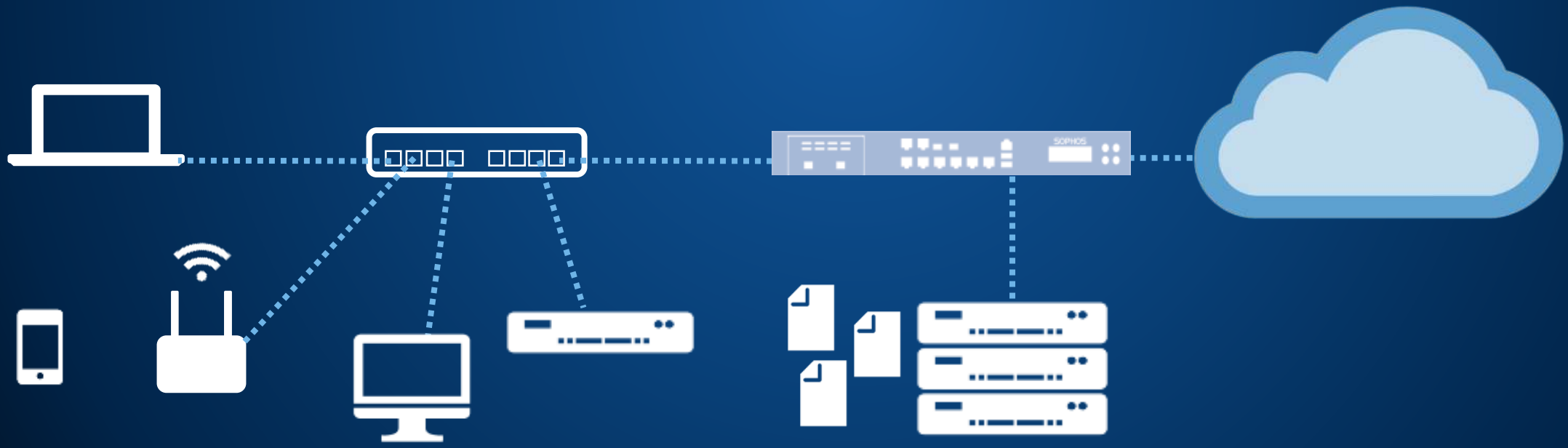
Christoph Riese
Senior Manager Sales Engineering

# Warum Synchronized Security?

SOPHOS

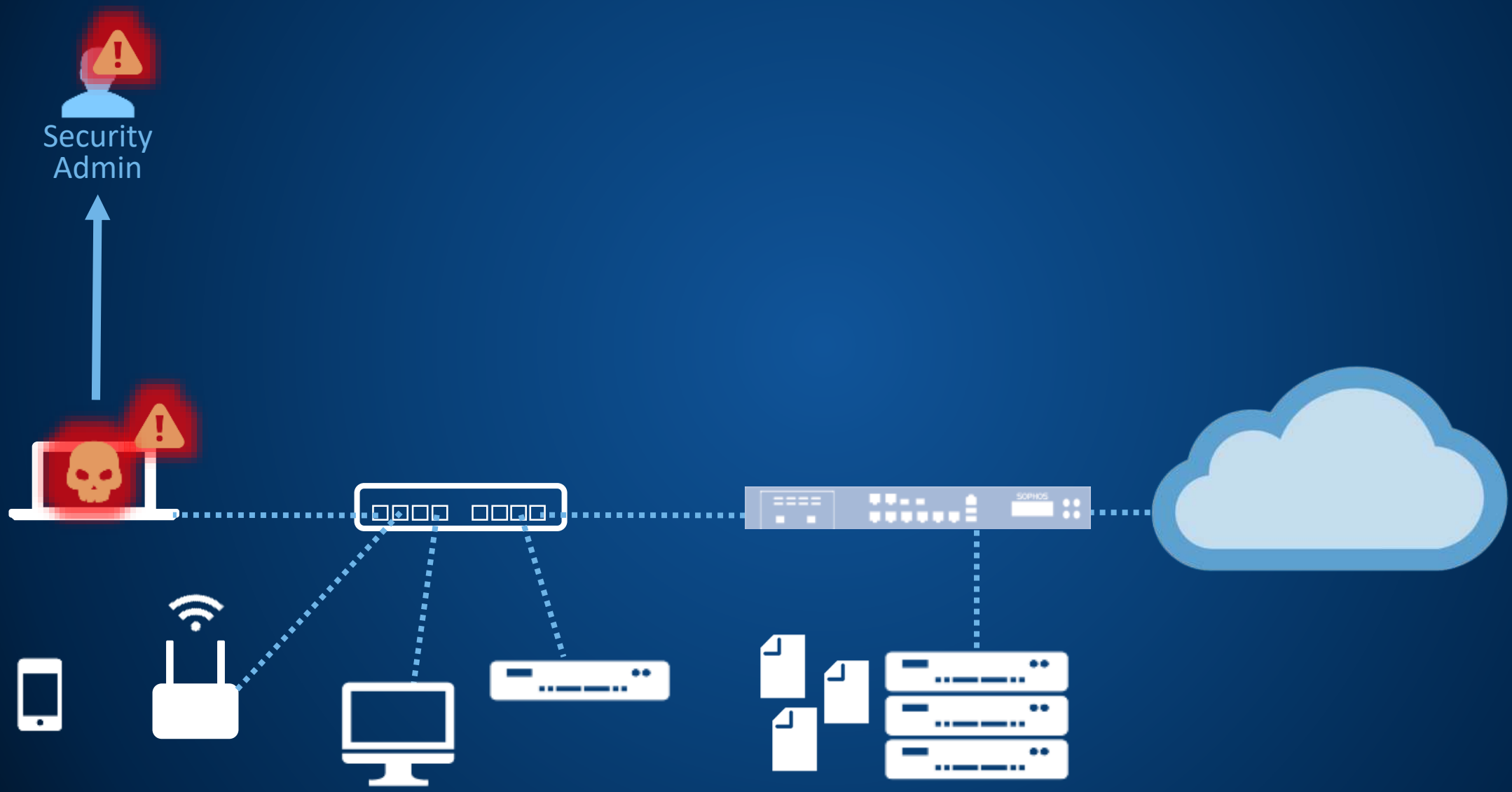

IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

# Vorgehen bei Bedrohungen ohne Synchronized Security



SOPHOS

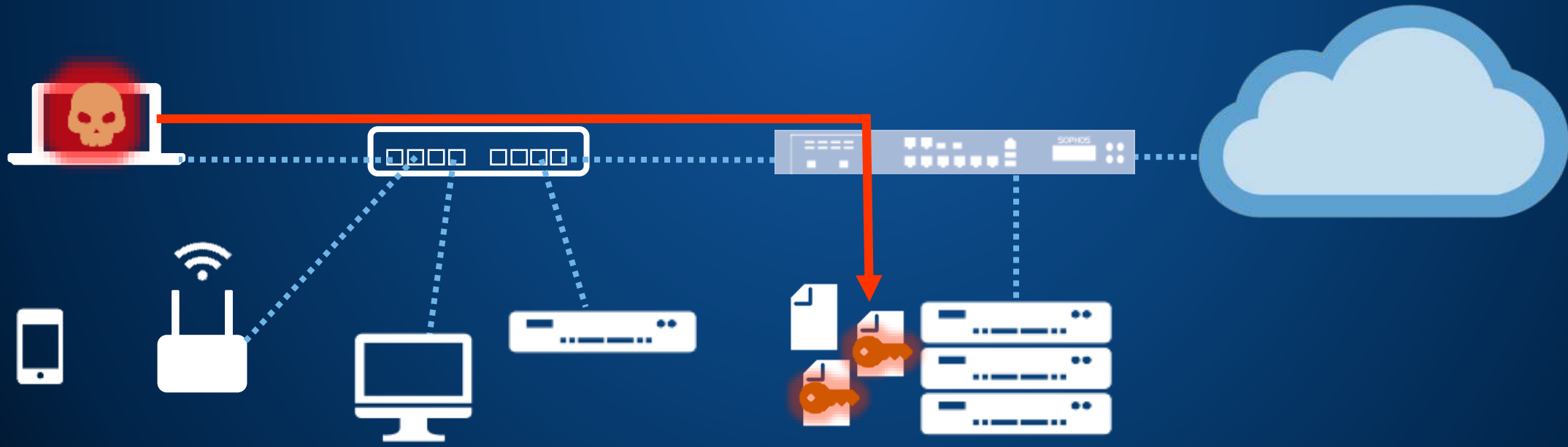
# Die Bedrohung wird erkannt



# ..und analysiert

Security Admin

Es wurden Dateien auf dem Fileserver verschlüsselt

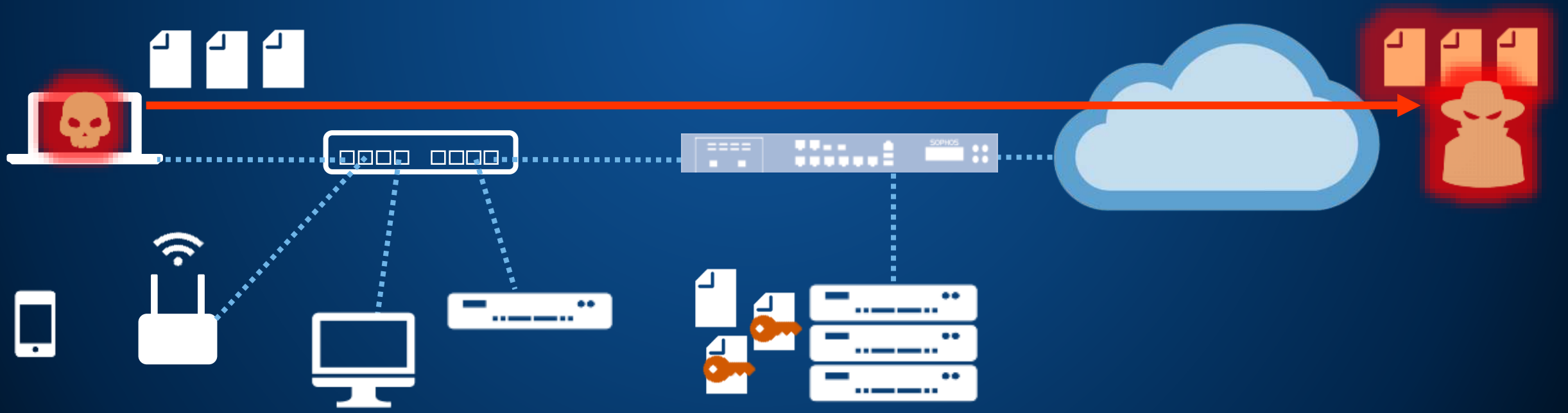


SOPHOS

# ..und analysiert

Security Admin

..und vertrauliche Daten an einen Angreifer im Internet geschickt

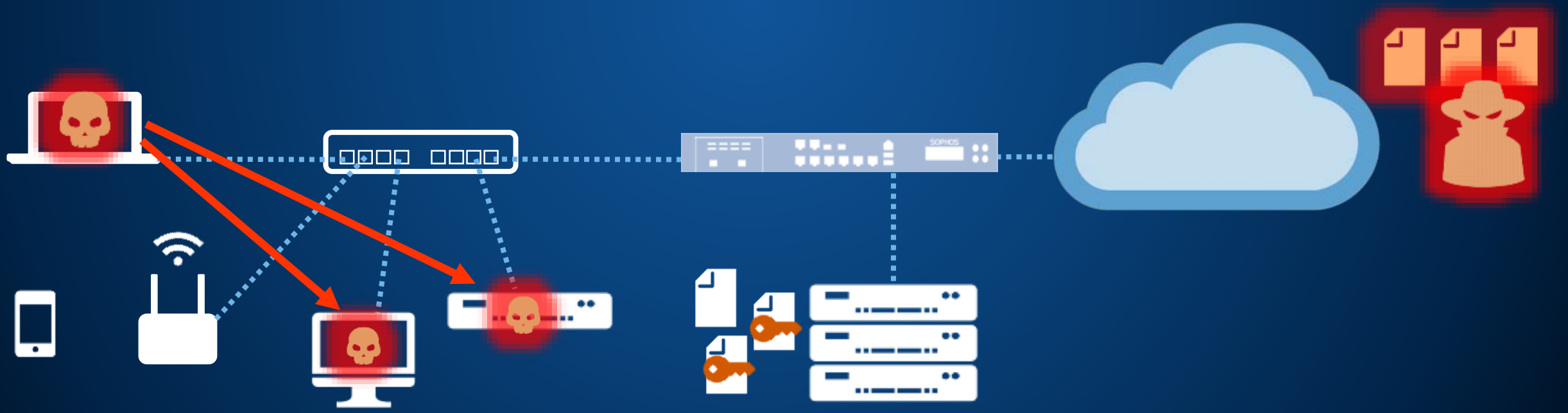


SOPHOS

# ..und analysiert

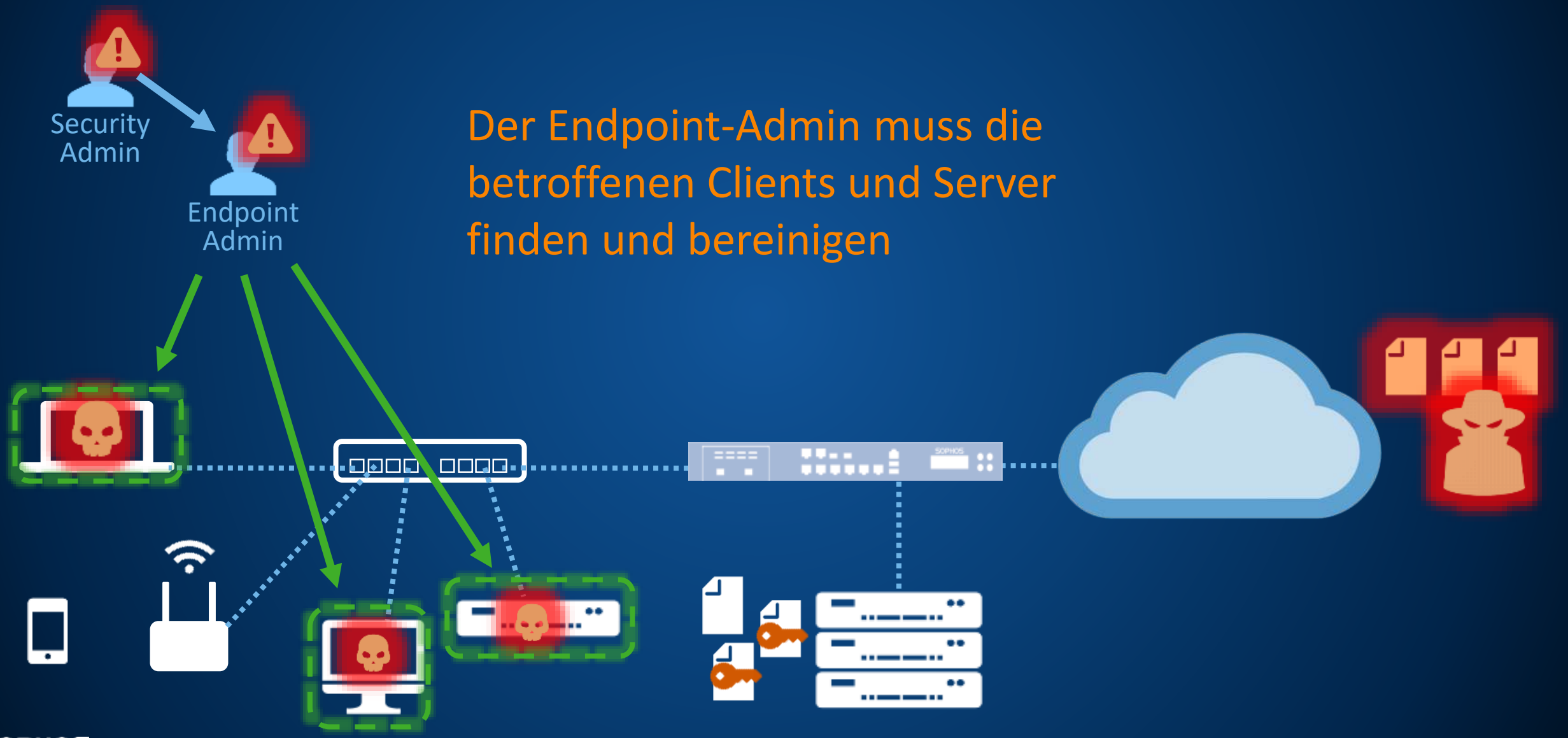
Security Admin

..außerdem wurden weitere Endpoints und Server infiziert



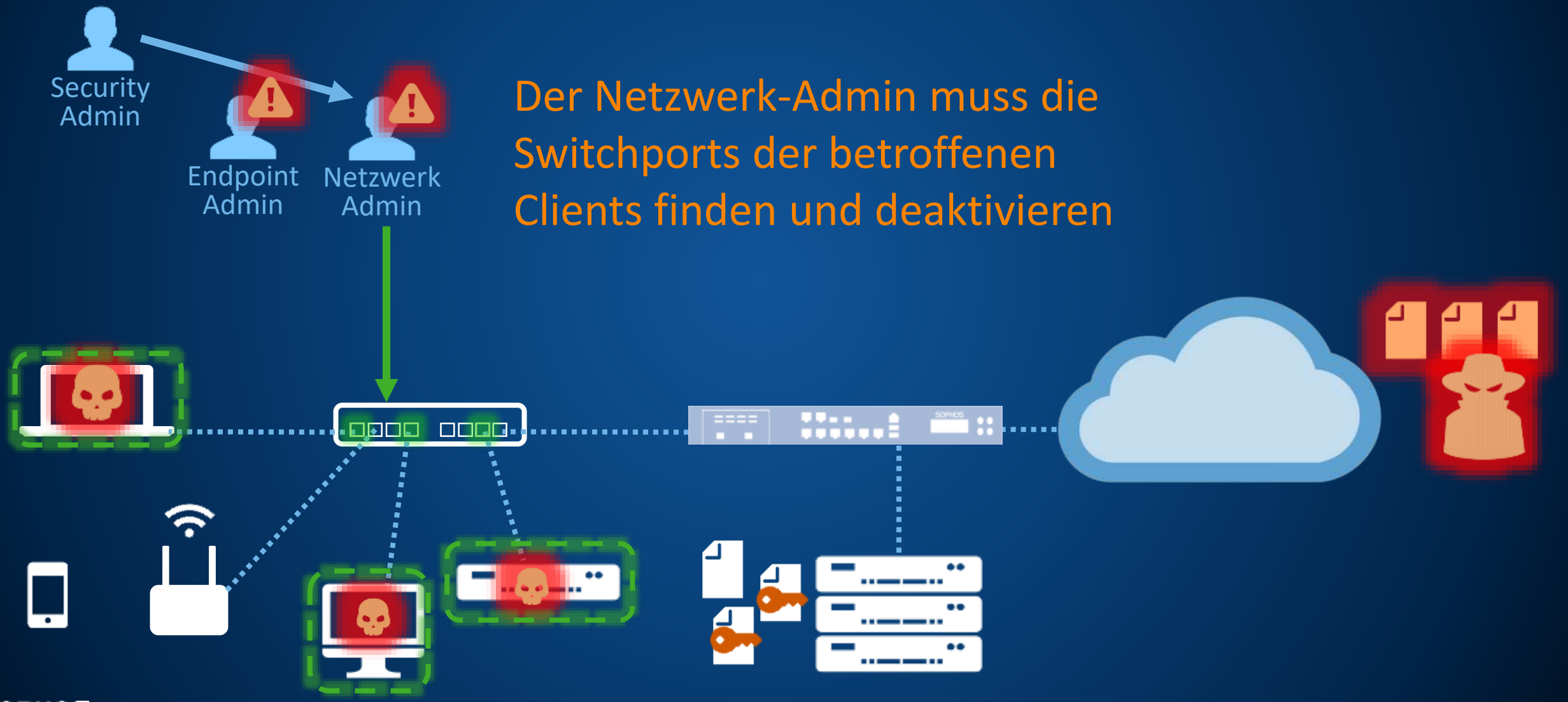
SOPHOS

# Action!!!



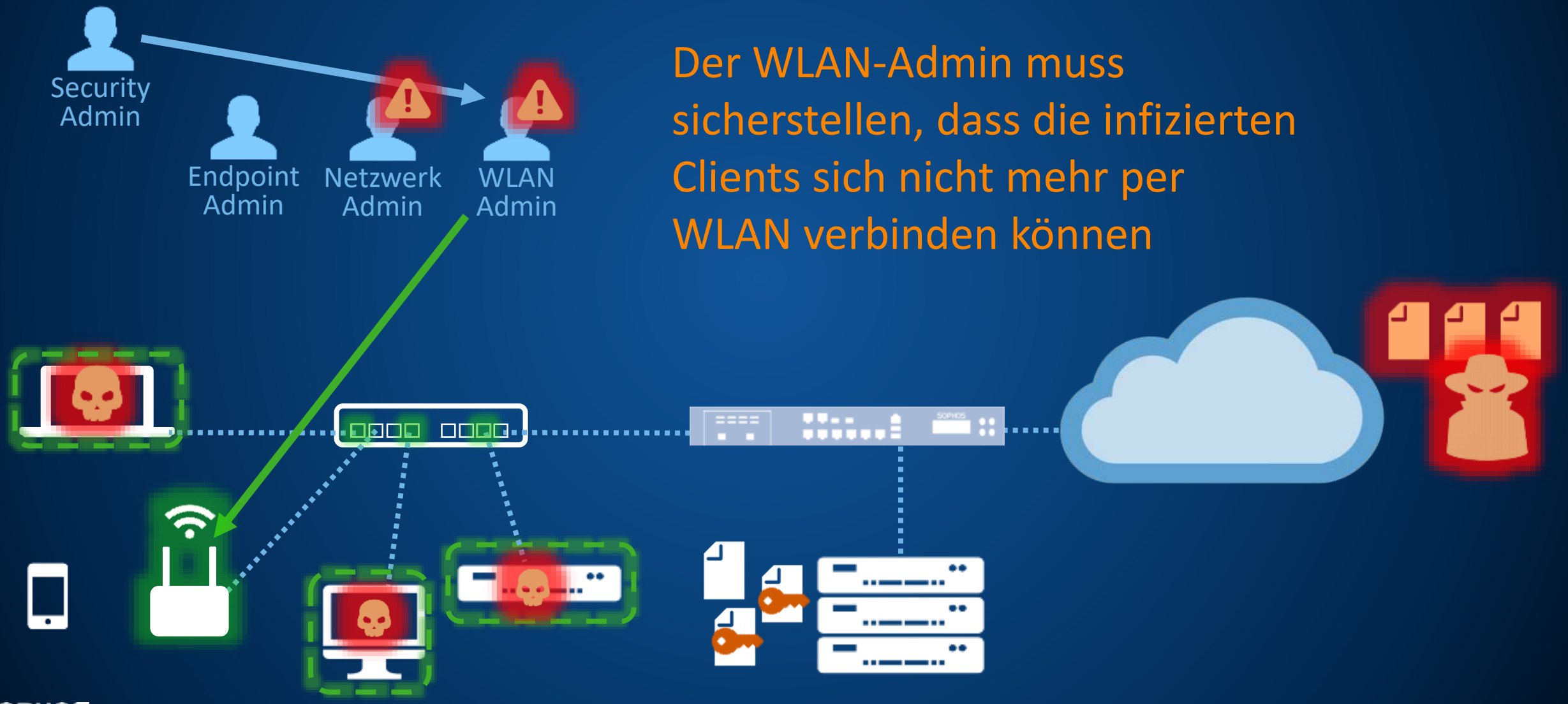

Der Endpoint-Admin muss die betroffenen Clients und Server finden und bereinigen

# Action!!!



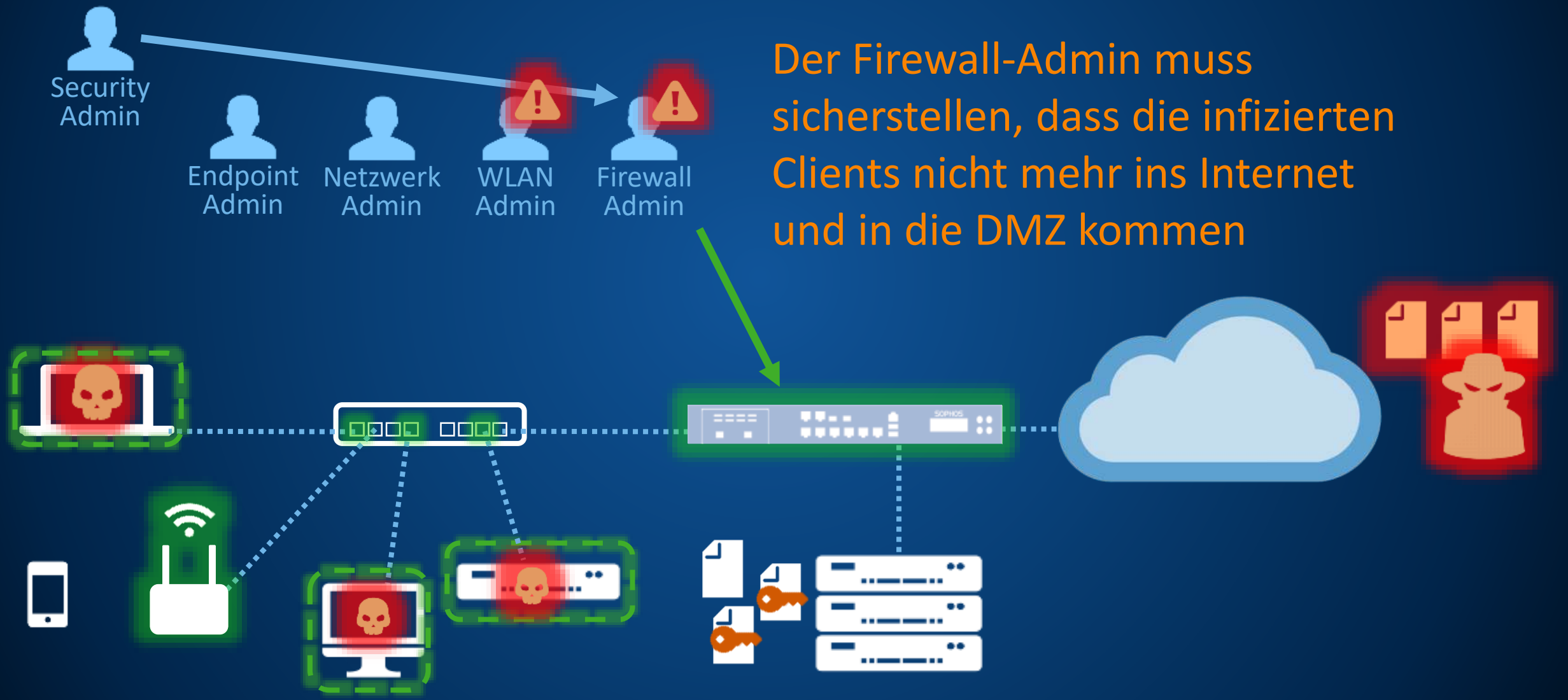

Der Netzwerk-Admin muss die Switchports der betroffenen Clients finden und deaktivieren

# Action!!!



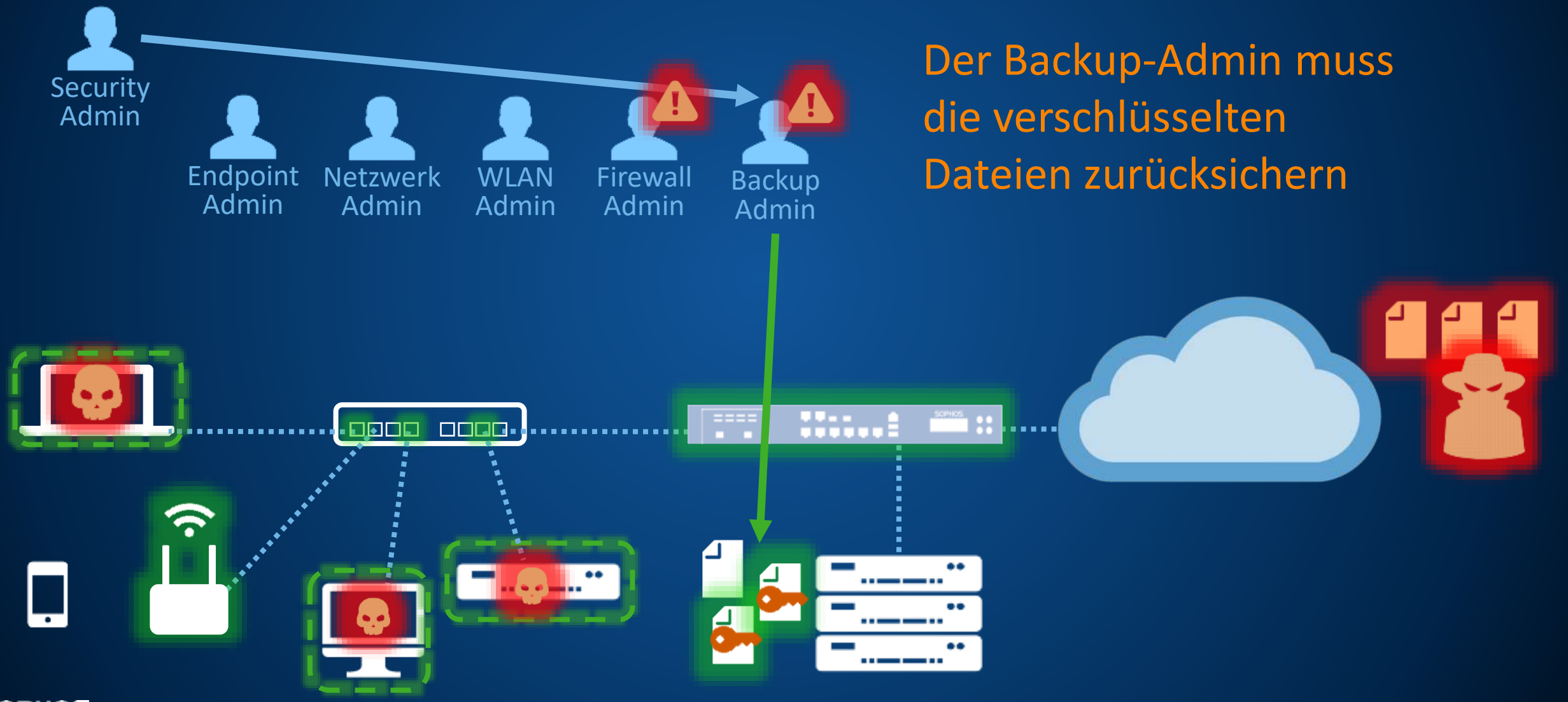

Der WLAN-Admin muss sicherstellen, dass die infizierten Clients sich nicht mehr per WLAN verbinden können

# Action!!!




Der Firewall-Admin muss sicherstellen, dass die infizierten Clients nicht mehr ins Internet und in die DMZ kommen

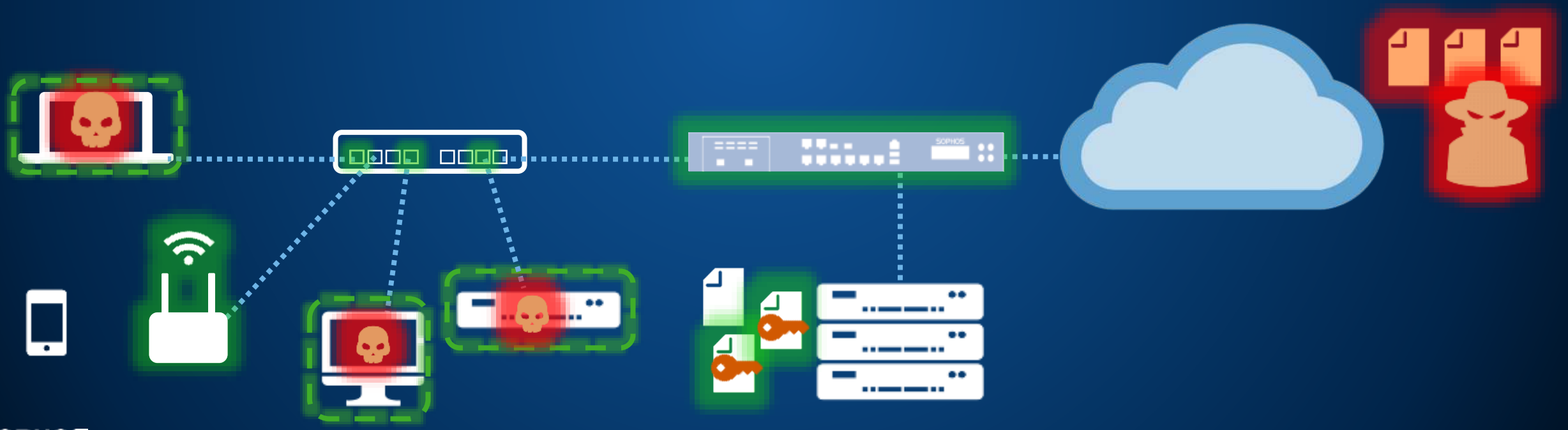
# Action!!!




Der Backup-Admin muss die verschlüsselten Dateien zurücksichern

# Action!!!


Jetzt wird der CISO informiert..



SOPHOS

# Action!!!

Security Admin

Endpoint Admin

Netzwerk Admin

WLAN Admin

Firewall Admin

Backup Admin

CISO

CEO

..der die Leitung informiert, dass Daten gestohlen wurden

SOPHOS

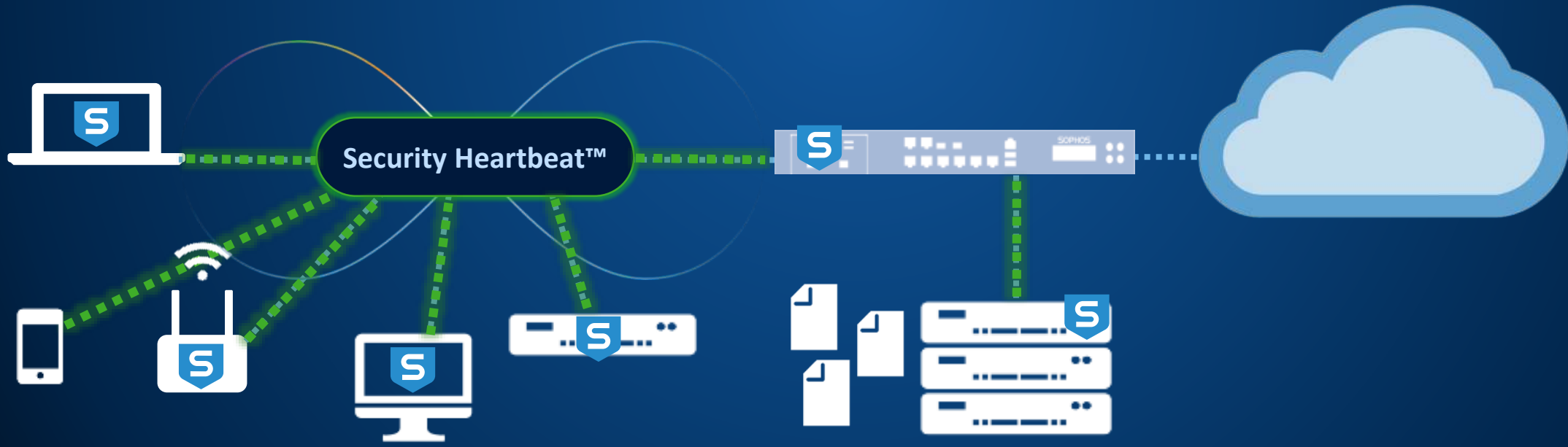
# Die IT vor dem Wochenende

# Vorgehen bei Sicherheitsvorfällen
# mit
# Synchronized Security

SOPHOS

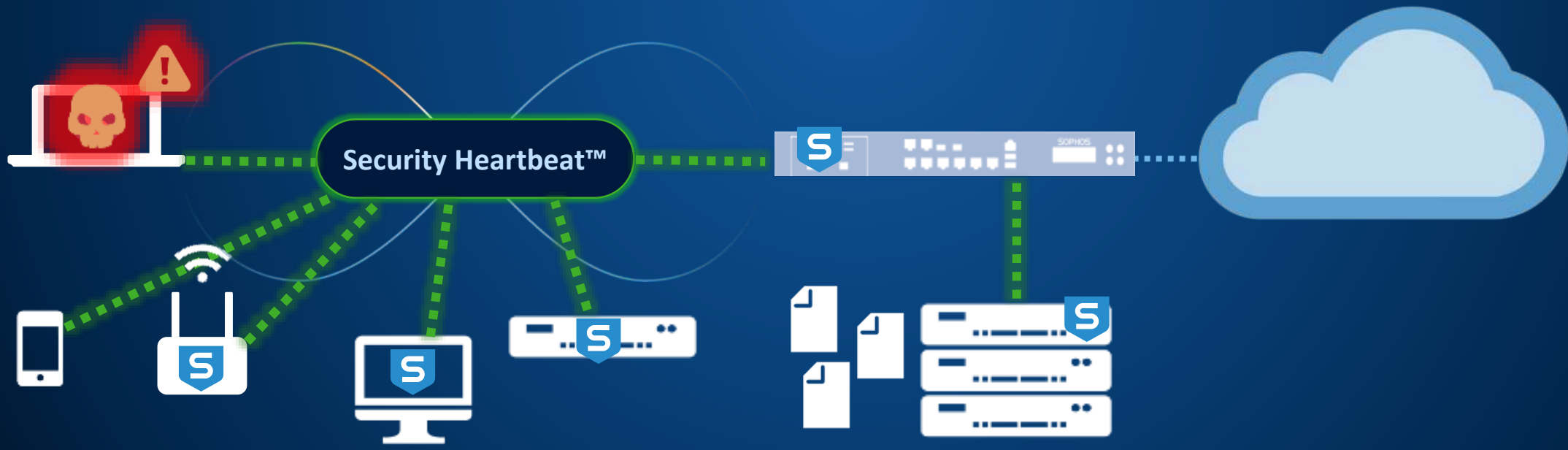
# Vorgehen bei Bedrohungen mit Synchronized Security

Clients, Server, Mobilgeräte, WLAN-APs
und Firewall kommunizieren per
SecurityHeartbeat direkt miteinander



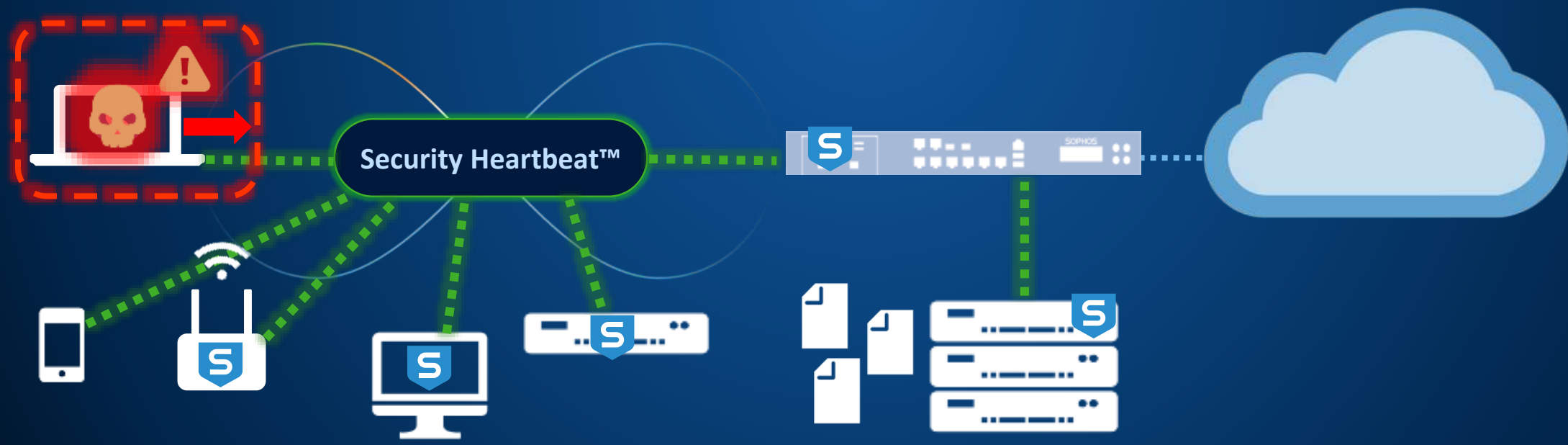
# Vorgehen bei Bedrohungen mit Synchronized Security

Bei einer Bedrohung werden alle Komponenten informiert und reagieren automatisch



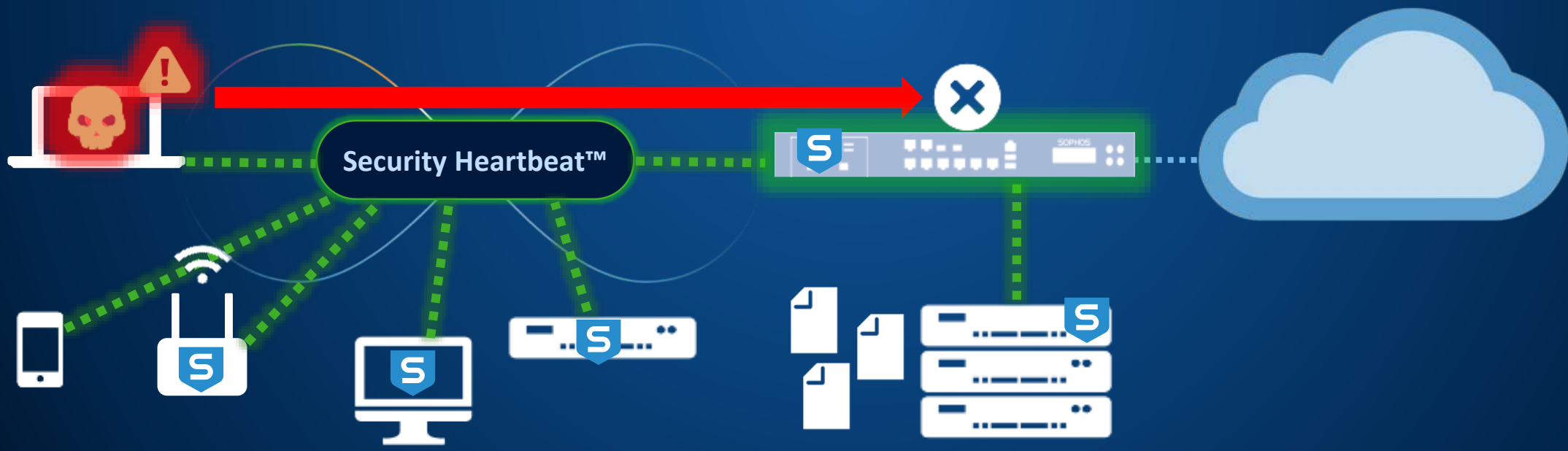
# Vorgehen bei Bedrohungen mit Synchronized Security

Der Client isoliert sich selbst..



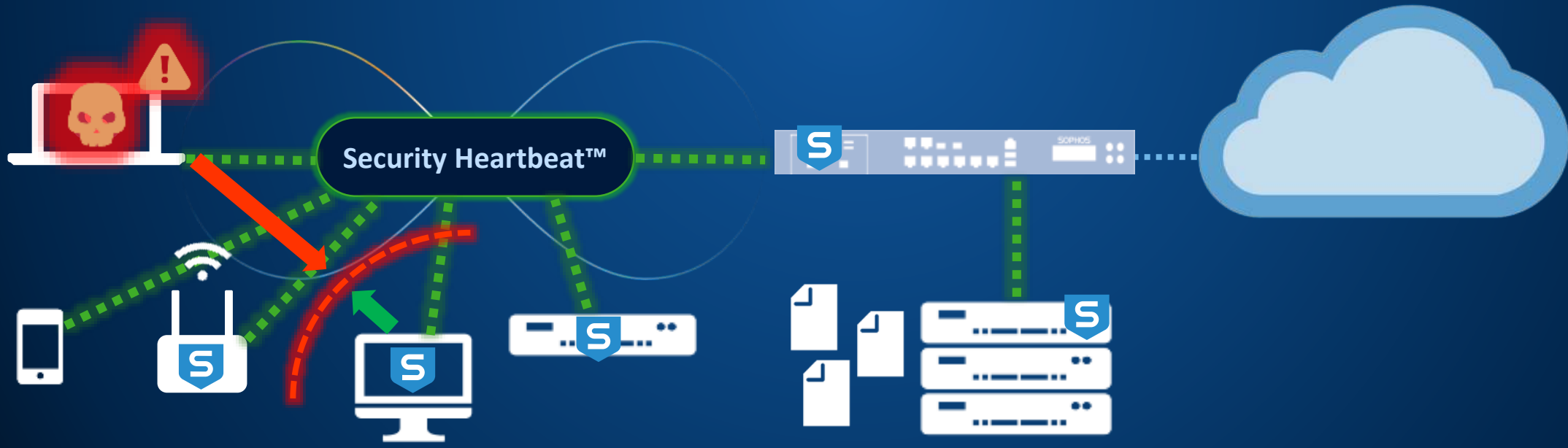
# Vorgehen bei Bedrohungen mit Synchronized Security

Die Firewall nimmt den Client in Netzwerkquarantäne und verhindert Kommunikation ins Internet oder die DMZ



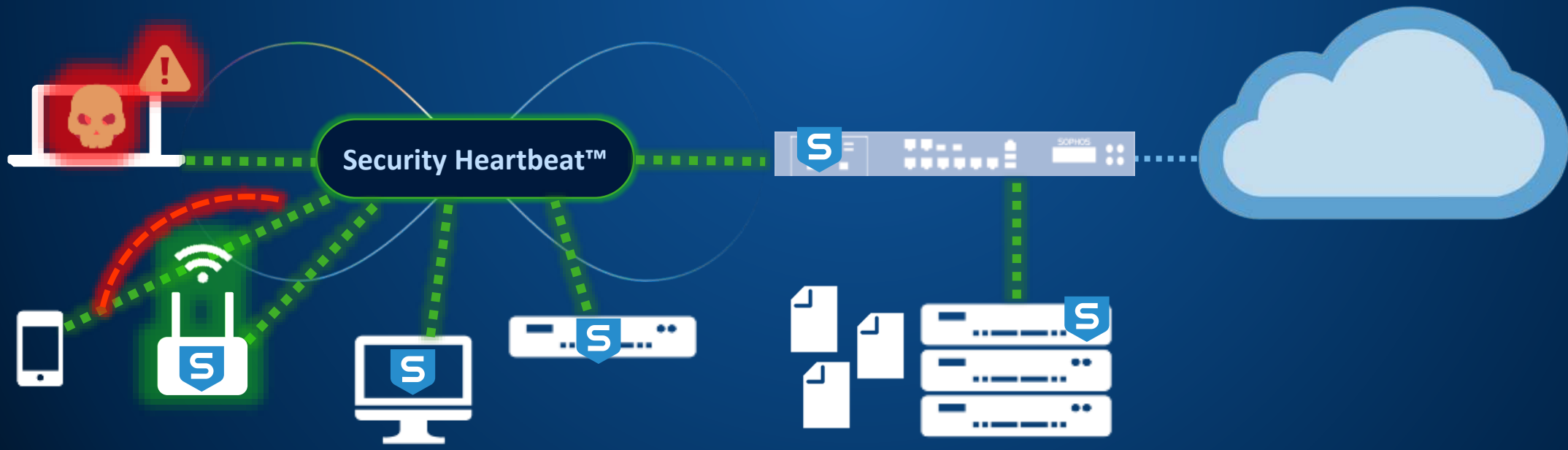
# Vorgehen bei Bedrohungen mit Synchronized Security

Die Clients und Server im selben Netz kommunizieren nicht mehr mit dem infizierten Client



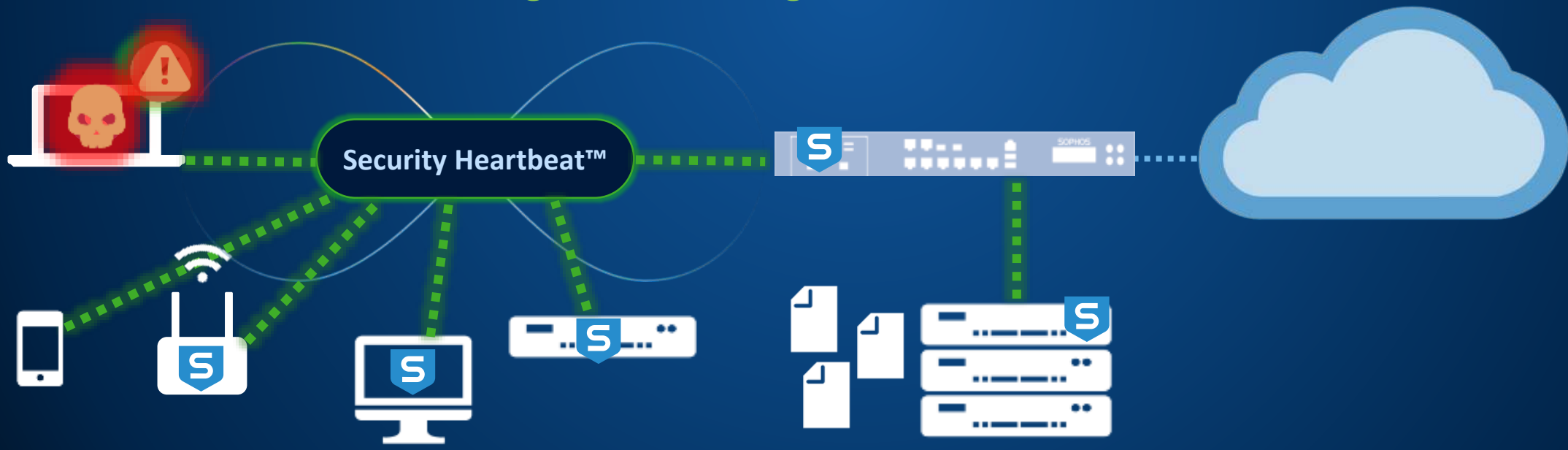
# Vorgehen bei Bedrohungen mit Synchronized Security

Der WLAN Access Point lässt
den infizierten Client nicht
mehr ins interne WLAN

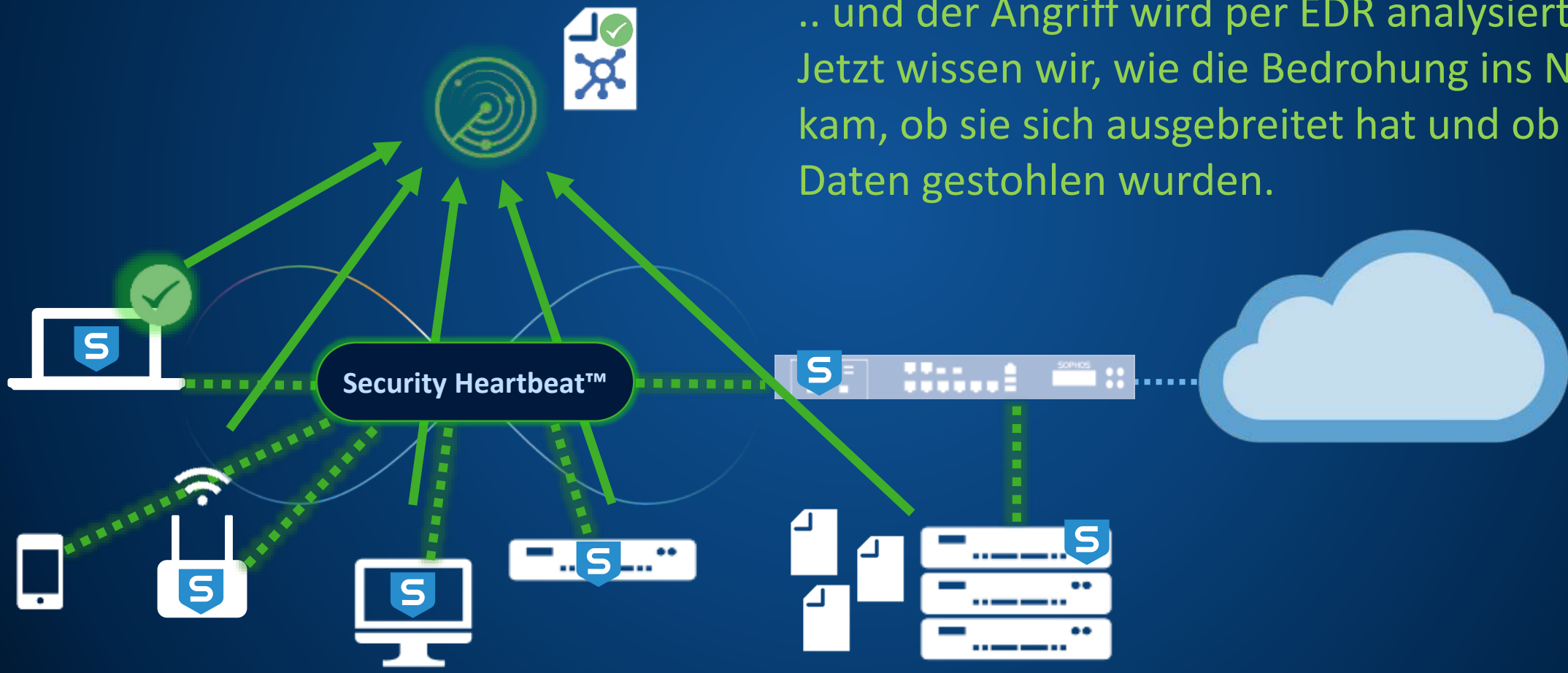


# Vorgehen bei Bedrohungen mit Synchronized Security

..die Bedrohung wird bereinigt..

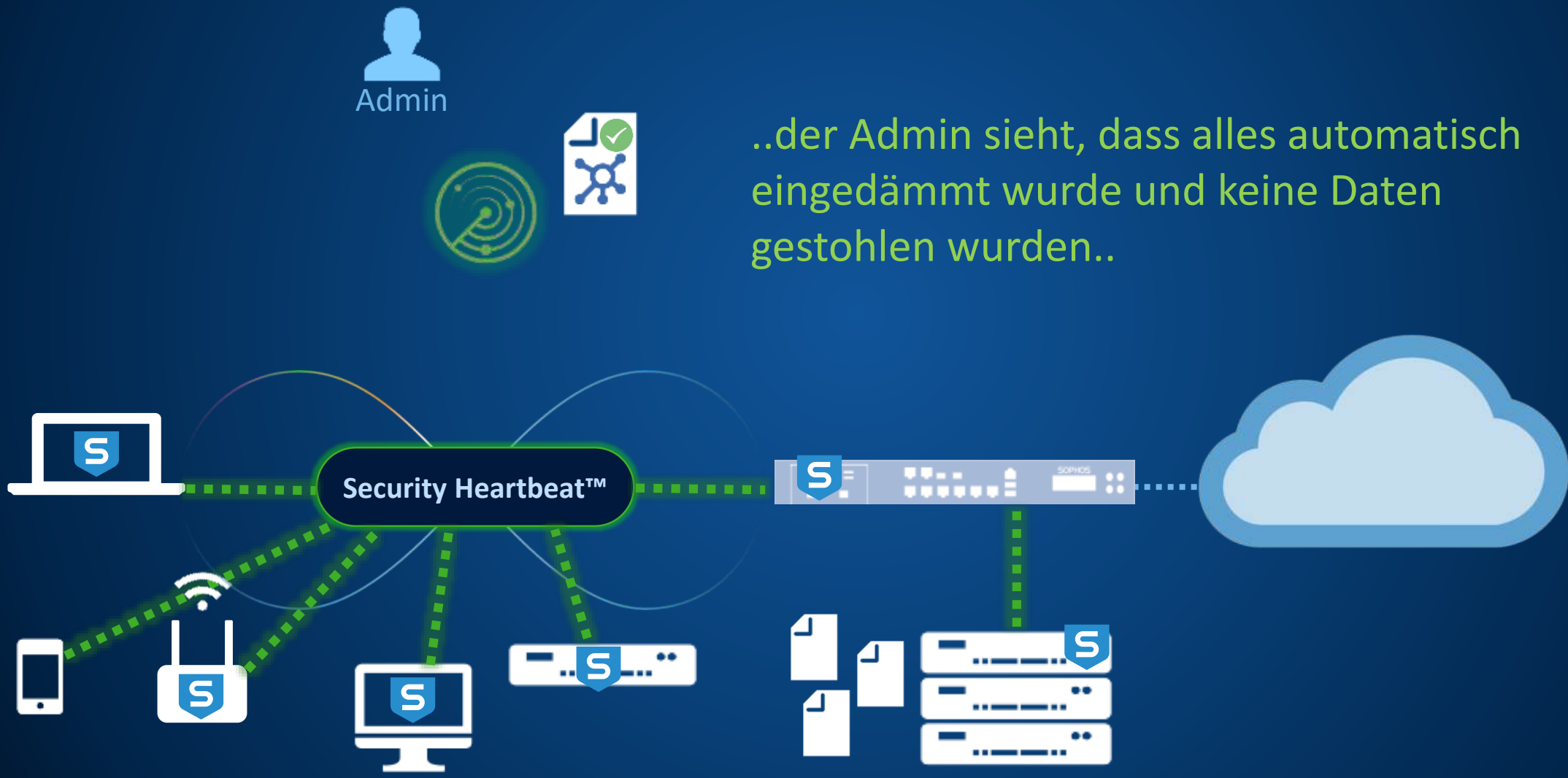


# Vorgehen bei Bedrohungen mit Synchronized Security




.. und der Angriff wird per EDR analysiert. Jetzt wissen wir, wie die Bedrohung ins Netz kam, ob sie sich ausgebreitet hat und ob Daten gestohlen wurden.

# Vorgehen bei Bedrohungen mit Synchronized Security



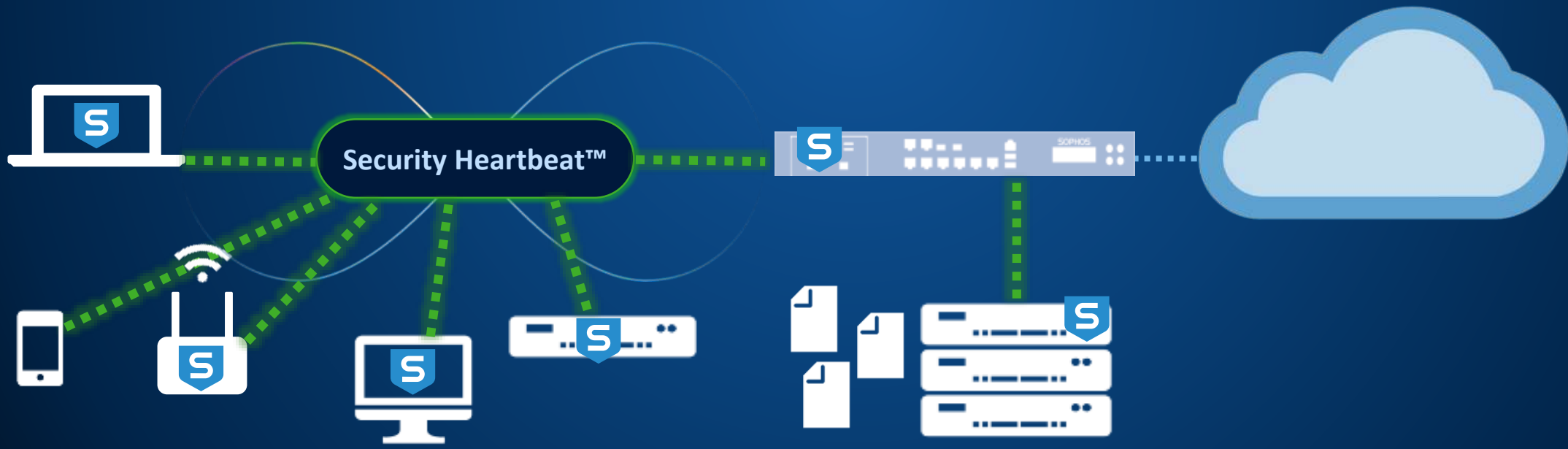

..der Admin sieht, dass alles automatisch eingedämmt wurde und keine Daten gestohlen wurden..

# Vorgehen bei Bedrohungen mit Synchronized Security

Admin

CEO

..und der Chef ist zufrieden, dass die
IT Sicherheit einfach funktioniert.

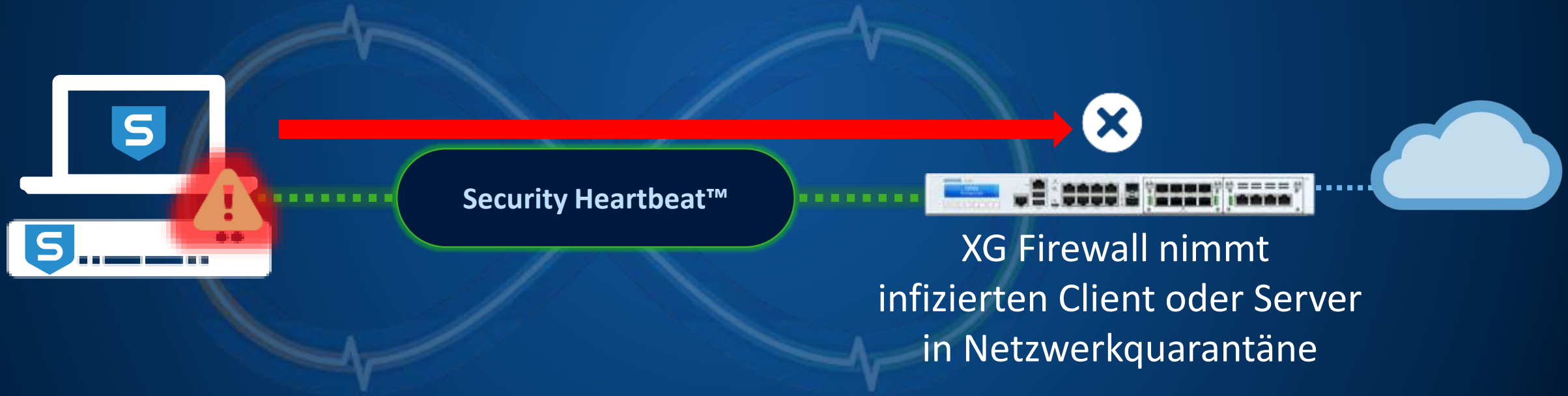


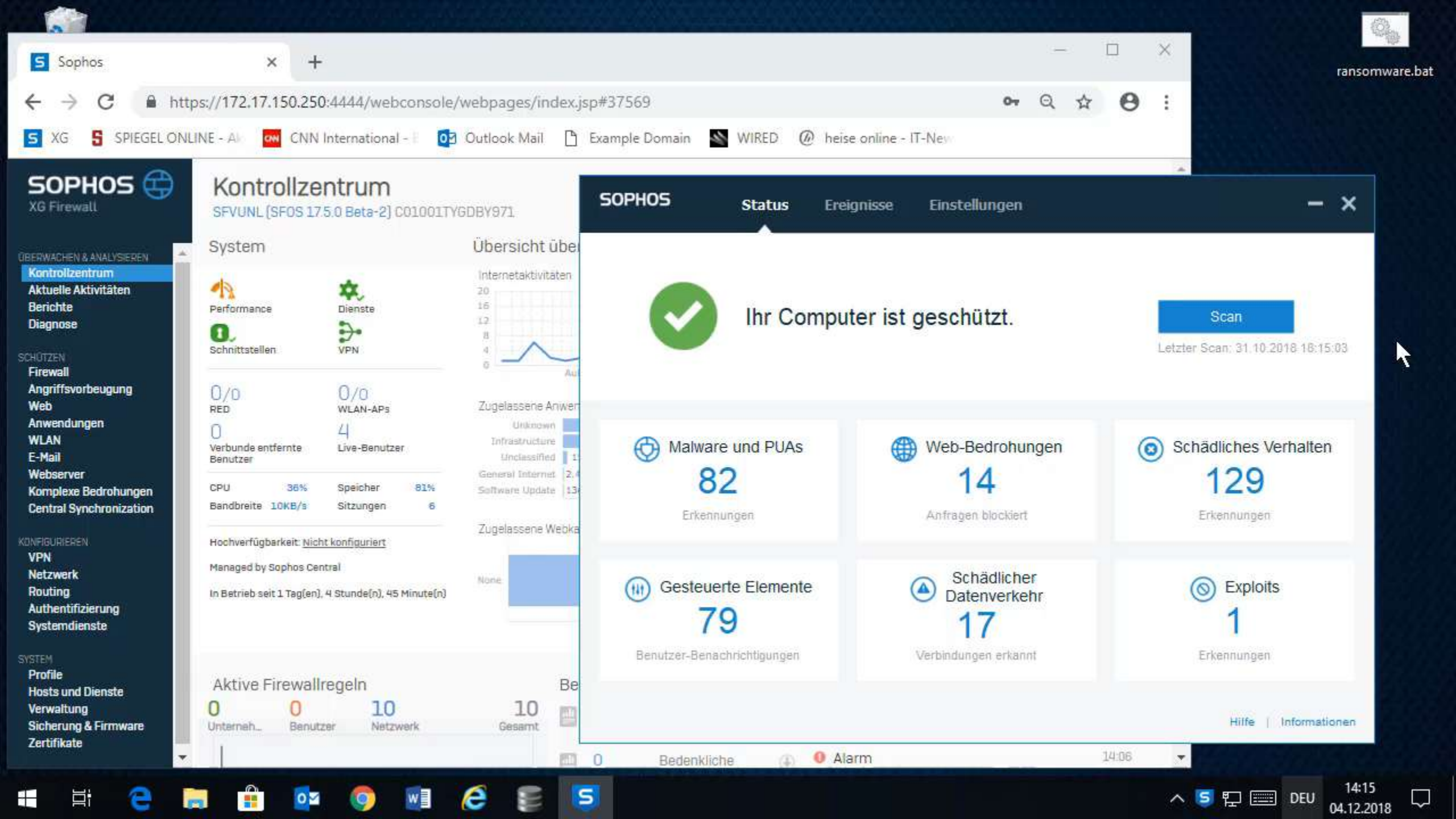

SOPHOS

# Synchronized Security - Konzept

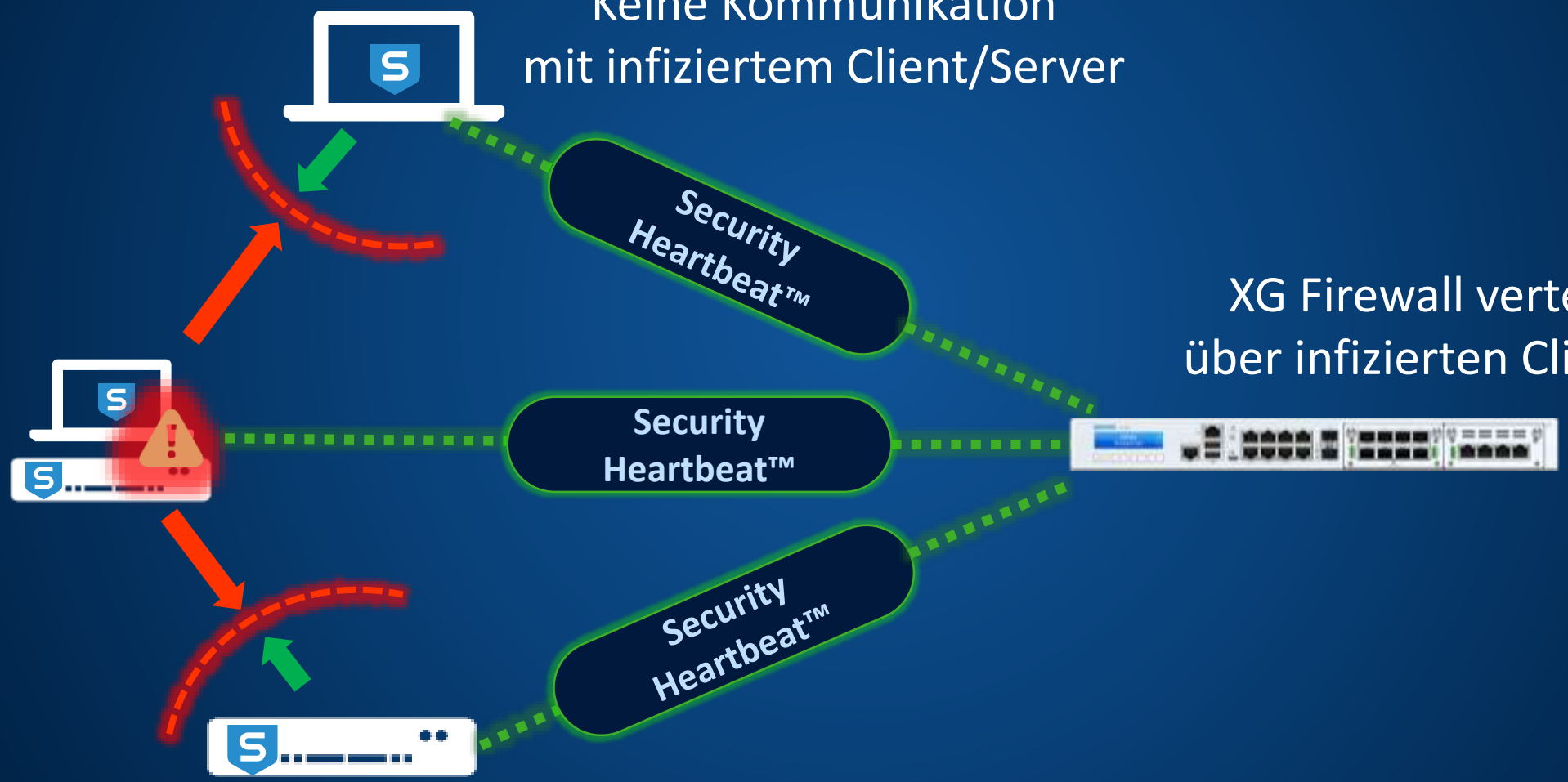
- Gateway und Endpoint agieren als System und tauschen aus
  - Sicherheitsstatus von Geräten
  - Anwendungsverkehr
  - Benutzerkontext
- Ziele
  - Bessere Erkennung von Bedrohungen und Hackeraktivitäten
  - Automatische Eindämmung von Bedrohungen
  - Schutz kritischer Daten

# Automatische Netzwerkquarantäne




ransomware.bat
Sophos
https://172.17.150.250:4444/webconsole/webpages/index.jsp#37569
XG
SPIEGEL ONLINE - A
CNN International - E
Outlook Mail
Example Domain
WIRED
heise online - IT-Ne
SOPHOS
XG Firewall
Kontrollzentrum
SFVUNL (SFOS 17.5.0 Beta-2) C01001TYGDBY971
ÜBERWACHEN & ANALYSIEREN
Kontrollzentrum
Aktuelle Aktivitäten
Berichte
Diagnose
SCHÜTZEN
Firewall
Angriffsvorbeugung
Web
Anwendungen
WLAN
E-Mail
Webserver
Komplexe Bedrohungen
Central Synchronization
KONFIGURIEREN
VPN
Netzwerk
Routing
Authentifizierung
Systemdienste
SYSTEM
Profile
Hosts und Dienste
Verwaltung
Sicherung & Firmware
Zertifikate
System
Performance
Dienste
Schnittstellen
VPN
0/0
RED
0/0
WLAN-APs
0
Verbunde entfernte Benutzer
4
Live-Benutzer
CPU 36%
Speicher 81%
Bandbreite 10KB/s
Sitzungen 6
Hochverfügbarkeit: Nicht konfiguriert
Managed by Sophos Central
In Betrieb seit 1 Tag(en), 4 Stunde(n), 45 Minute(n)
Übersicht über
Internetaktivitäten
Zugelassene Anwen
Unknown
Infrastructure
Unclassified
General Internet
Software Update
Zugelassene Webka
None
Aktive Firewallregeln
0
Unterneh...
0
Benutzer
10
Netzwerk
10
Gesamt
Be
0
Bedenkliche
Alarm
14:06
SOPHOS
Status
Ereignisse
Einstellungen
Ihr Computer ist geschützt.
Scan
Letzter Scan: 31.10.2018 18:15:03
Malware und PUAs
82
Erkennungen
Web-Bedrohungen
14
Anfragen blockiert
Schädliches Verhalten
129
Erkennungen
Gesteuerte Elemente
79
Benutzer-Benachrichtigungen
Schädlicher Datenverkehr
17
Verbindungen erkannt
Exploits
1
Erkennungen
Hilfe | Informationen
DEU
14:15
04.12.2018

# Lateral Movement Protection



# Synchronized App Control

*Ich möchte gerne kommunizieren*

**Security Heartbeat™**

*← Welche Applikation?  Das ist Anwendung XY →*

**Priorisieren**

**Drosseln**

**Blockieren**

# Synchronized Security - Vorteile

- Unerreichte Sichtbarkeit – was passiert im Netzwerk?
- Automatische Reaktion erkauft Zeit
- Keine 24x7-Bereitschaft mehr notwendig
  –> Mitarbeiter können sinnvoller eingesetzt werden
- Stressfreie IT!
- Modular – je mehr Sophos-Komponenten, desto einfacher die Verwaltung und Automatisierung der IT-Sicherheit

SOPHOS

# Synchronized Security

SOPHOS

SOPHOS

Stand 426 - Halle 9