SEE THE FUTURE

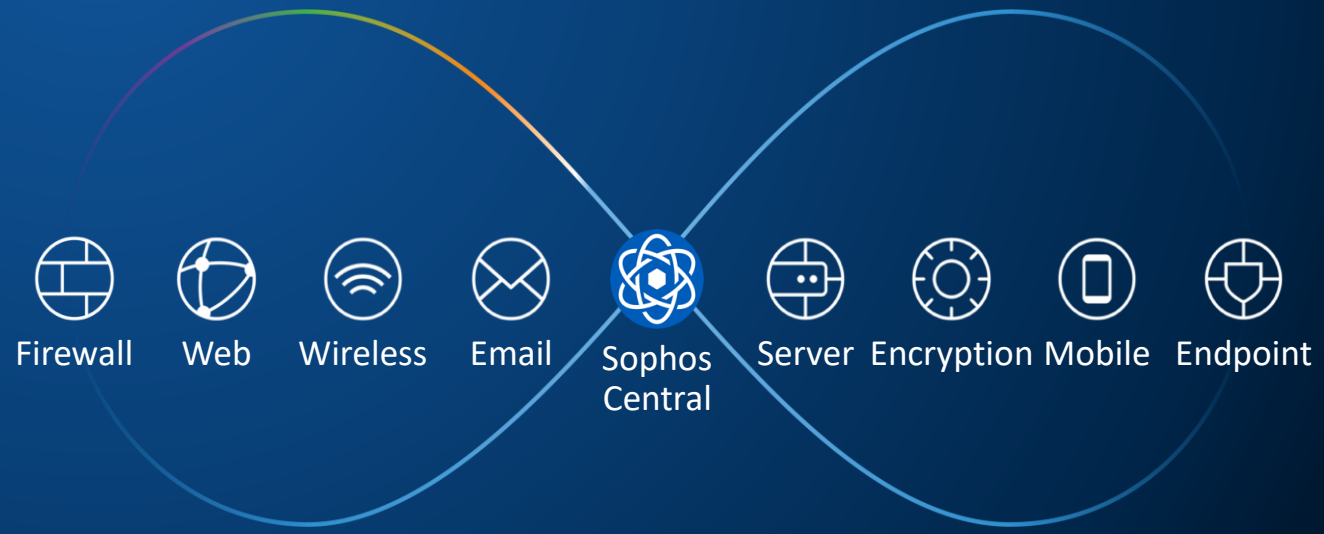
Künstliche Intelligenz in der IT-Sicherheit – Revolution oder Hype?

Michael Veit
Technology Evangelist, Sophos

SOPHOS

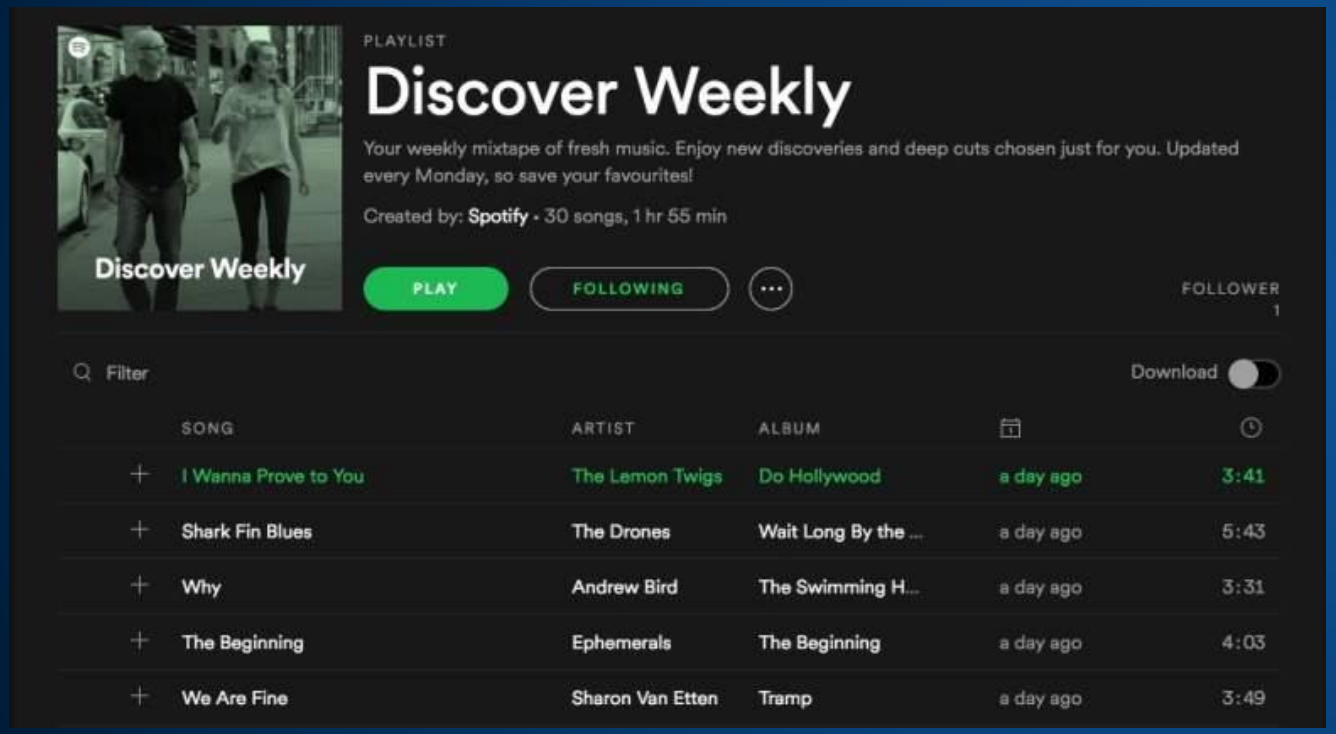
Sophos im Überblick

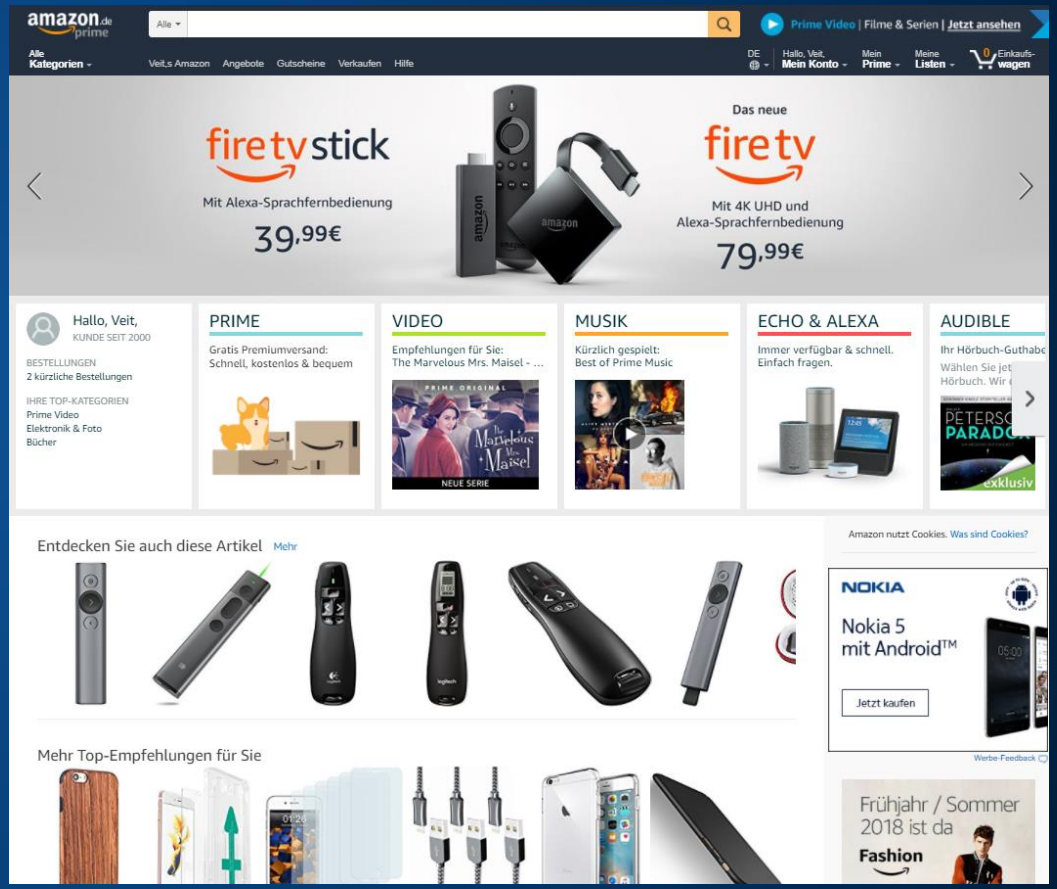
- 1985 in Oxford, UK gegründet
- $768 Millionen Umsatz in FY18
- 20% Wachstum/Jahr - vgl. IT-Security-Markt = 7%
- > 3.000 Mitarbeiter, davon ca. 500 in DACH
- 300.000+ Kunden
- 100+ Millionen User
- 39.000+ Channel Partner
- Gartner: Marktführer in den Bereichen Endpoint, Firewall & Verschlüsselung



SOPHOS

Machine Learning ist überall



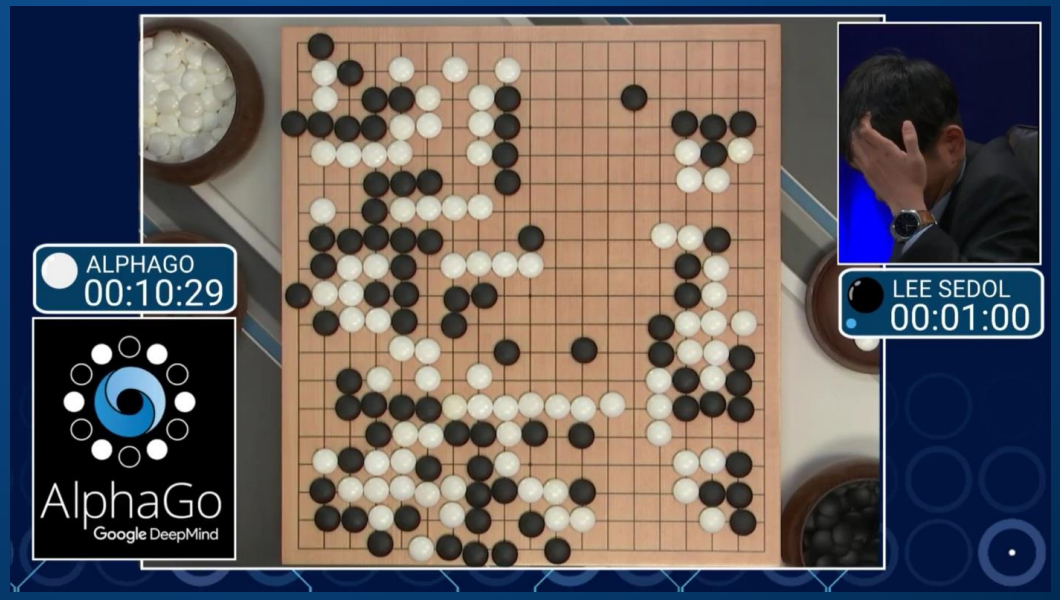


Machine Learning ist überall

KI für Spezialfälle

- Schach?

- Go!




YOLO v2
http://pjreddie.com/yolo

Machine Learning

„Maschinelles Lernen ist ein Forschungsbereich, der Computern die Möglichkeit gibt zu lernen, ohne explizit programmiert zu werden“

Arthur Lee Samuel (Pioneer der KI-Forschung)

Machine Learning-Modelle

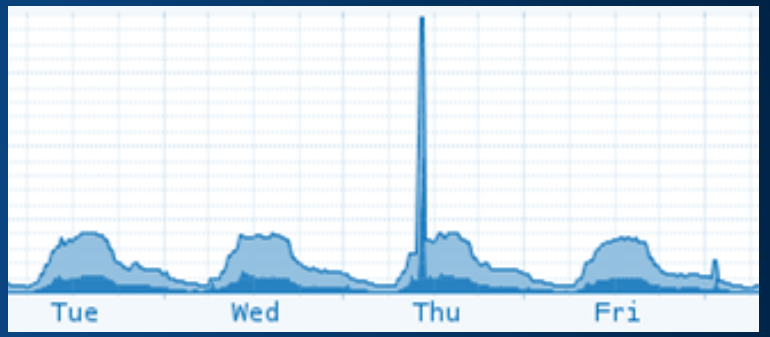
- analysieren viele Daten und erstellen eigene Regeln
- extrahieren Muster und Merkmale und treffen Vorhersagen
- automatisieren die Datenklassifizierung einer speziellen Aufgabe

Künstliche Intelligenz

- Der Versuch, intelligente Maschinen nach dem Vorbild des Menschen zu schaffen
- Teilbereich der Informatik, der sich mit selbstlernenden und problemlösenden Computersystemen beschäftigt
- Intelligent, kreativ

ML-Einsatzgebiete in der IT Security

- Erkennung von 0-Day Malware
- Anomalie-Erkennung
  - im Netzwerkverkehr
  - im Benutzerverhalten
  - in Dateizugriffen/-veränderungen
- Korrelation von Ereignissen verschiedener Sensoren
  - Erkennung von Hackeraktivität



Beispiel:
Machine Learning
in Endpoint Security

SOPHOS

BANK

$£€

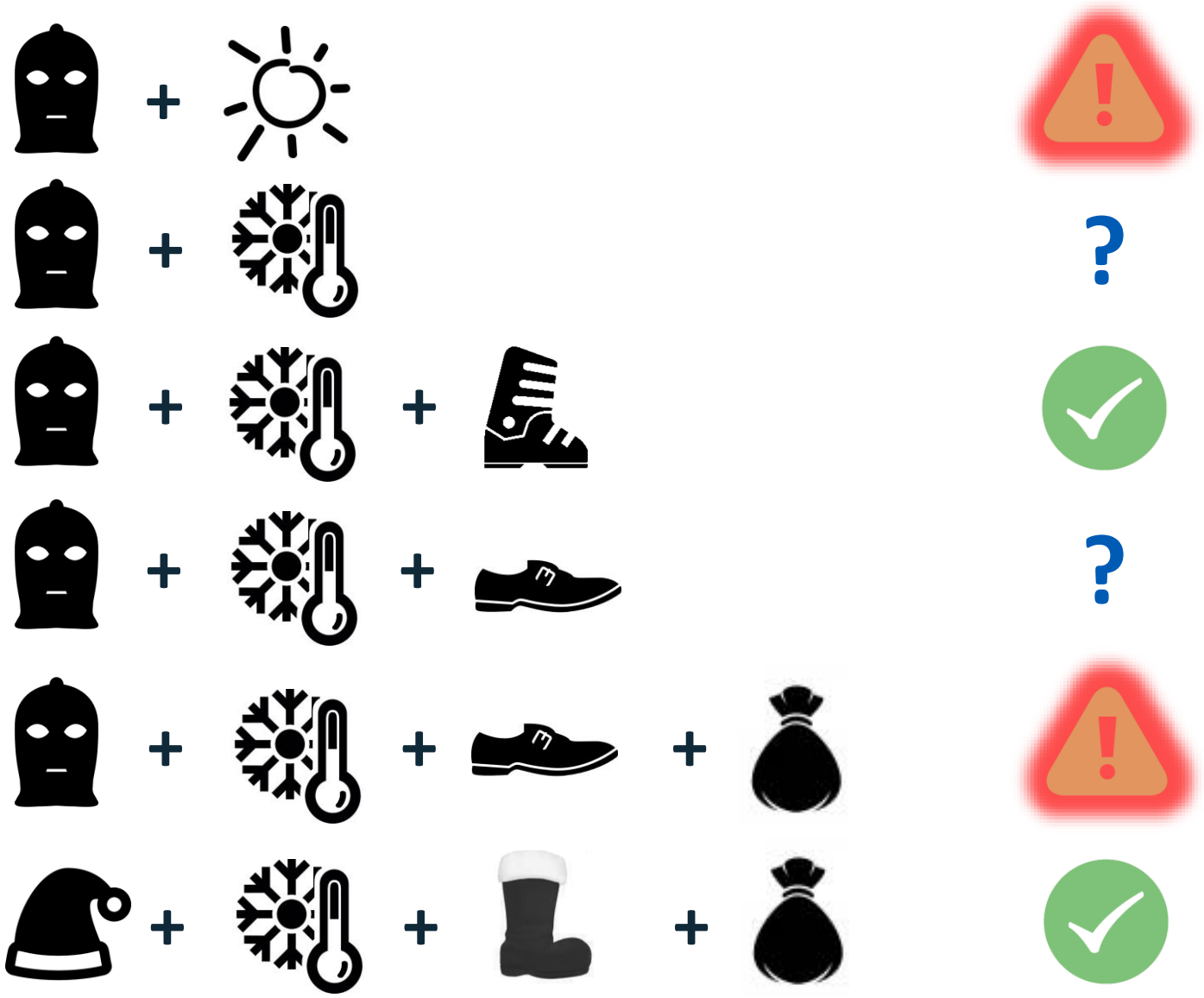
Anti Virus

Machine Learning

Vor der Ausführung

SOPHOS

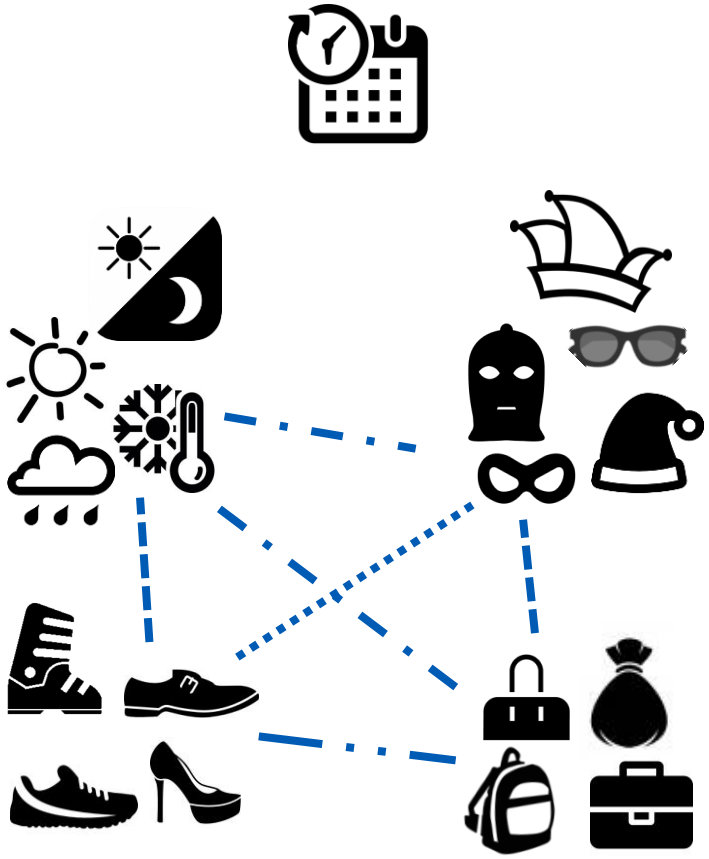
Machine Learning



Konventionelles Machine Learning

Menschlicher Analyst identifiziert Merkmale und definiert deren Beziehungen

Reagiert träge auf Veränderungen und wird bei vielen Eingabedaten sehr groß und langsam.



Deep Learning

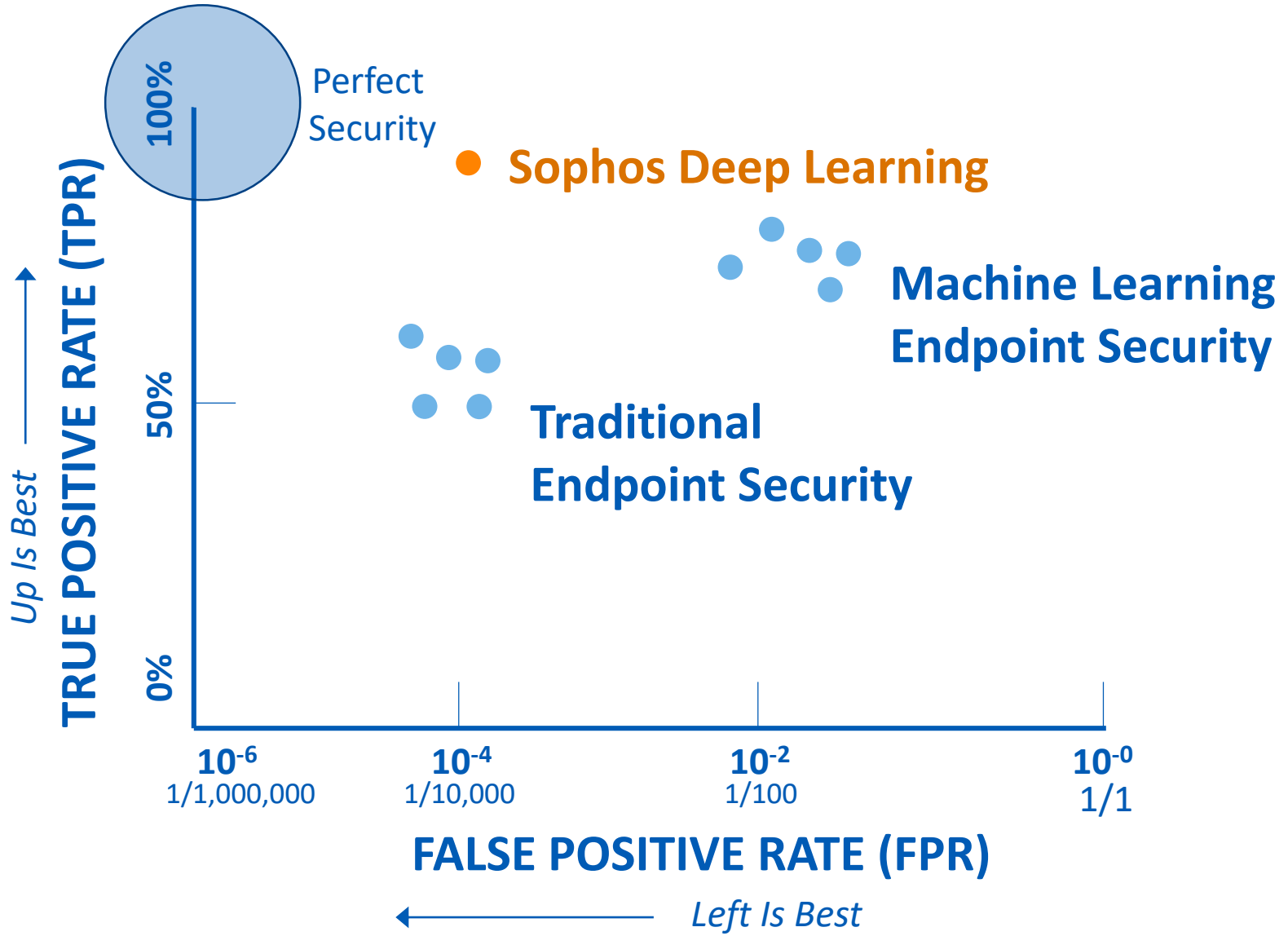
Neuronales Netz lernt selbstständig Merkmale und deren Beziehungen

Sehr performant, kann große Datenmengen verarbeiten, wird dadurch immer besser

Training, Training, Training

- Gut qualifizierte Daten
- Daten bereinigen
- False Positives und False Negatives beachten
- Modell nicht überfrachten
- Bestes Modell wählen:
  -> oft DeepLearning

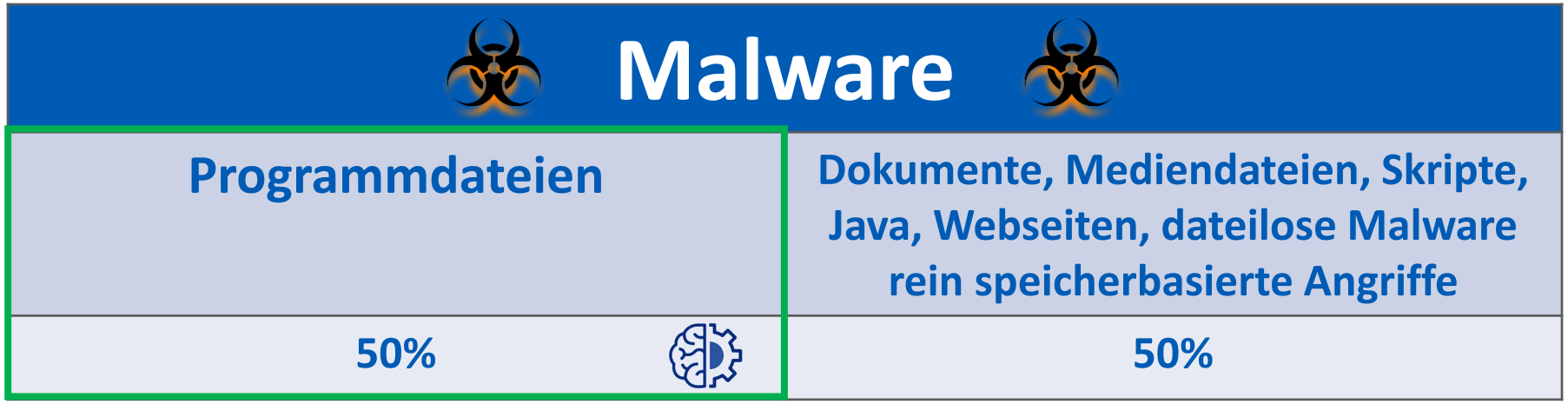
Sophos – beste Erkennung bei minimalen False Positives



Source: SophosLabs analysis of malware found in the wild

Machine Learning / Deep Learning

- Schützt vor den 50% der Malware, die als Programmdatei kommt
- Schützt nicht vor Infektionen per Exploit, speicherbasierter bzw. dateiloser Malware oder Dokumenten-Malware



Konsequenz:
Security braucht viele Schichten

SOPHOS

BANK

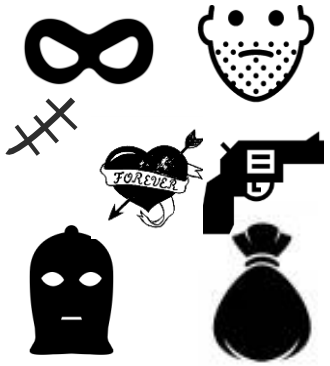
$£€

Anti Virus

GESUCHT!

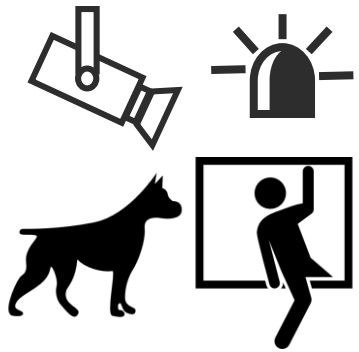
Deep Learning

Verdächtig!



Exploit Prevention

Techniken!



Verhaltens-Erkennung

Aktionen!

Vor der Ausführung

Nach der Ausführung

SOPHOS

Demo

SOPHOS

Schutzschichten am Endpoint

Einfallswege kontrollieren

- Web Control
- Device Control
- App Control
- Firewall

Vor der Ausführung

- Live-Schutz
- Web Security
- Signaturen
- Deep Learning
- Heuristiken
- Skript-Analyse
- Download Reputation

Während der Ausführung

- Exploit Prevention
- Host Intrusion Prevention
- Anti-Hacker
- Schutz vor Ransomware
- Speicher-Scan
- Schutz von Passwörtern
- Botnet-Traffic-Erkennung

Reaktion

- Blockieren
- Quarantäne
- Wiederherstellung
- Erweiterte Bereinigung
- Synchronized Security

Sichtbarkeit

- Logging & Reporting
- Alarmierung
- Zentrales Management
- Ursachen-Analyse
- Bedrohungs-Analyse
- Bedrohungs-Suche

SOPHOS

Konsequenz: Komponenten müssen als System agieren

Synchronized Security

SOPHOS

BANK

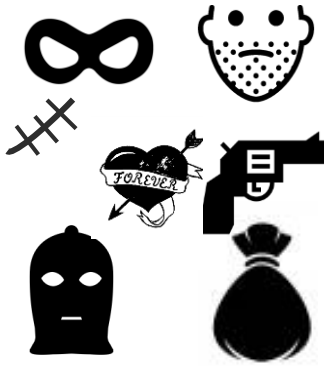
$£€

Anti Virus

GESUCHT!

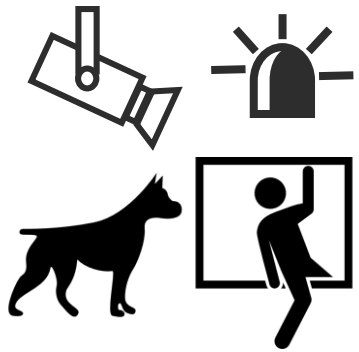
Deep Learning

Verdächtig!



Exploit Prevention

Techniken!



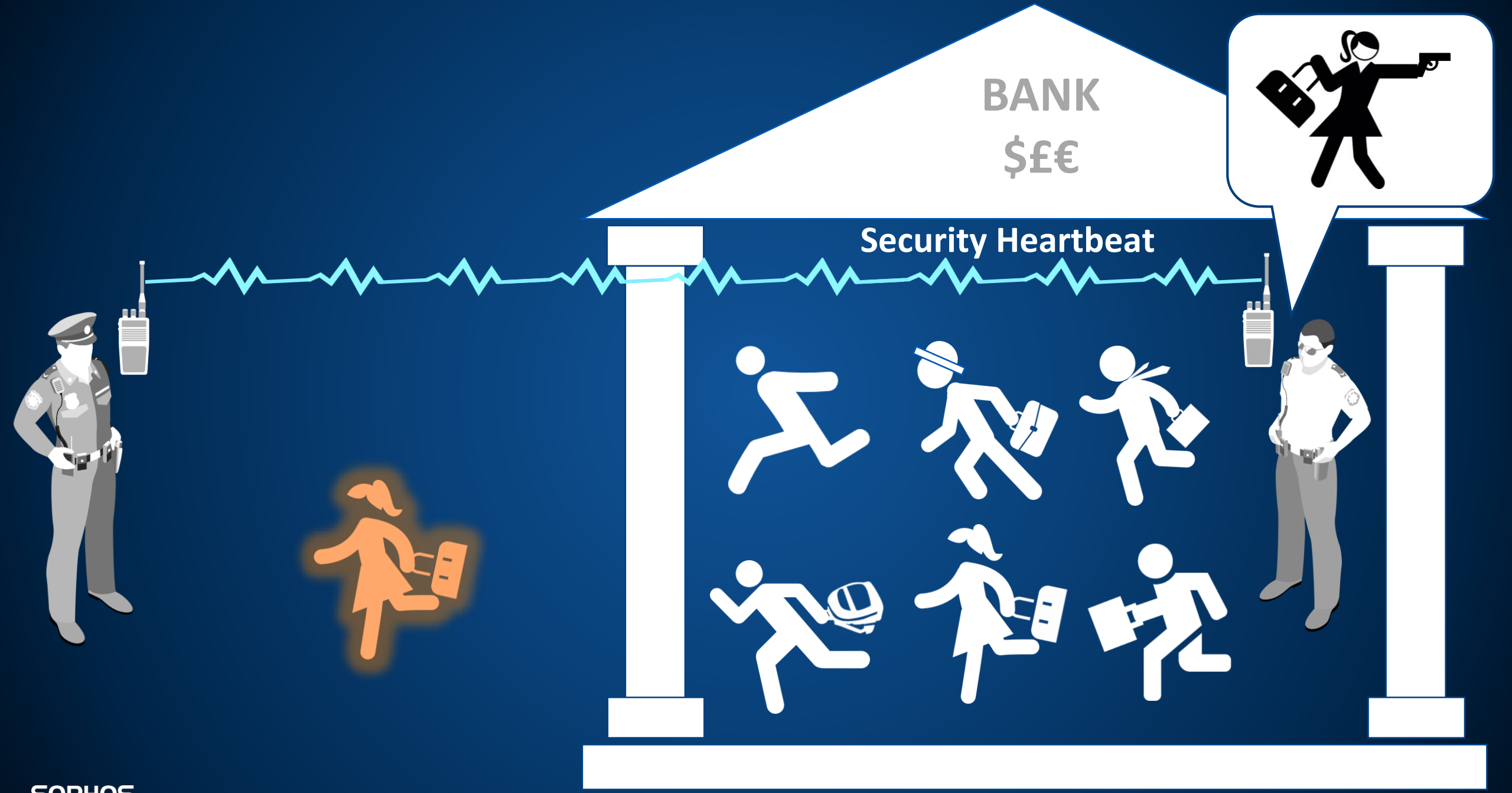
Verhaltens-Erkennung

Aktionen!

Vor der Ausführung

Nach der Ausführung

SOPHOS



SOPHOS

Synchronized Security - Konzept

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

Demo

Synchronized Security

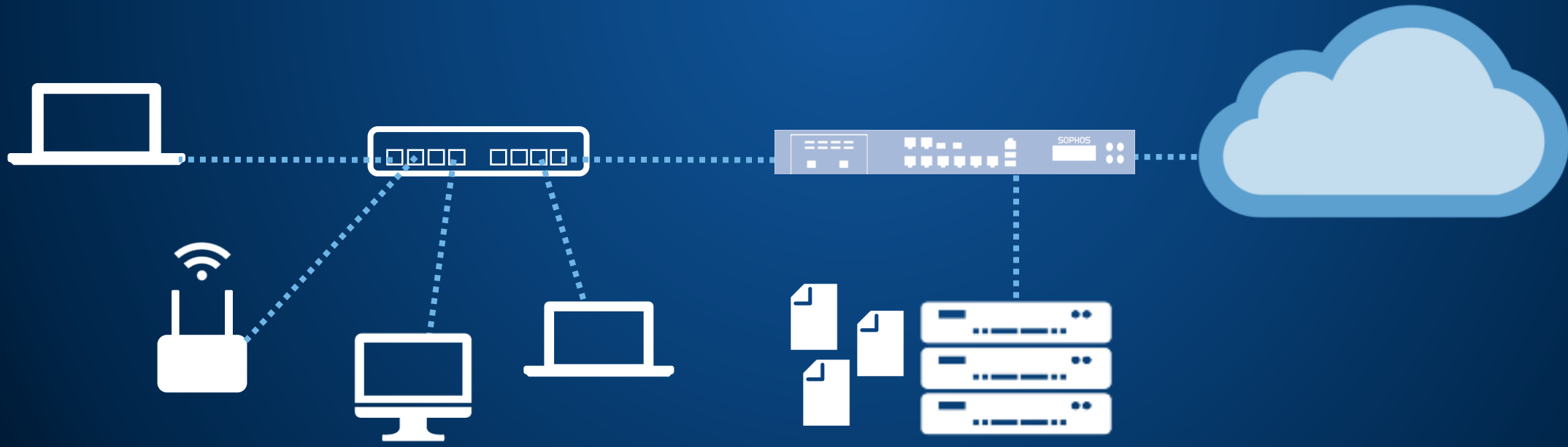
SOPHOS

Was passiert bei einem Angriff ohne Synchronized Security?

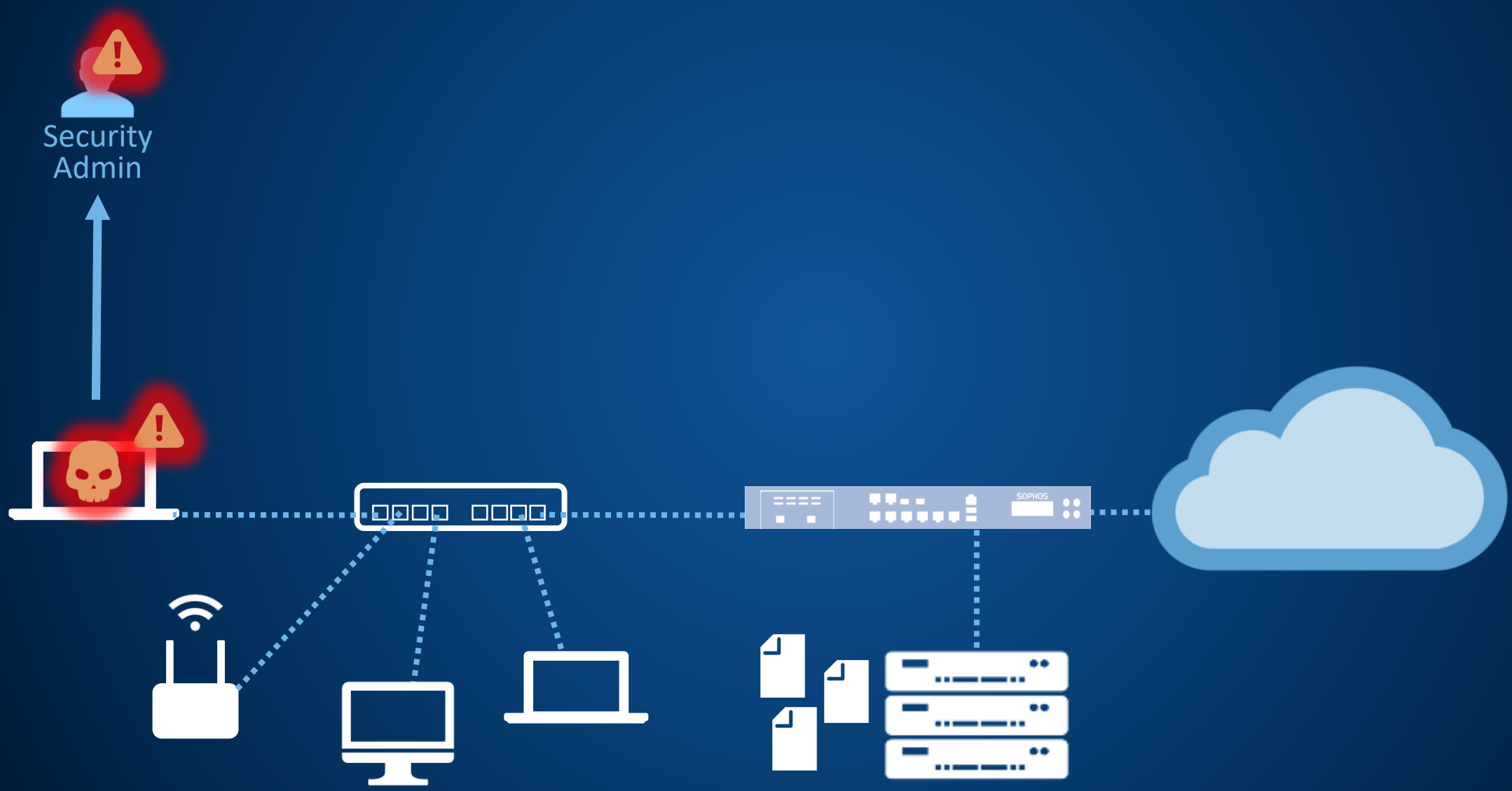
SOPHOS


IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

Vorgehen bei Bedrohungen ohne Synchronized Security



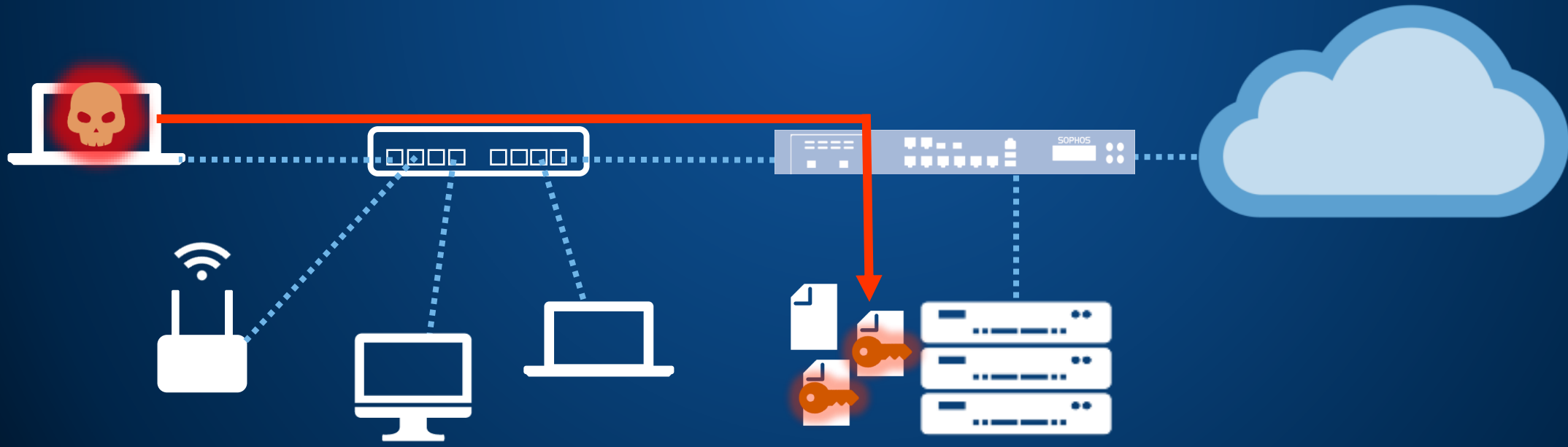
Die Bedrohung wird erkannt



..und analysiert

Security Admin

Es wurden Dateien auf dem Fileserver verschlüsselt

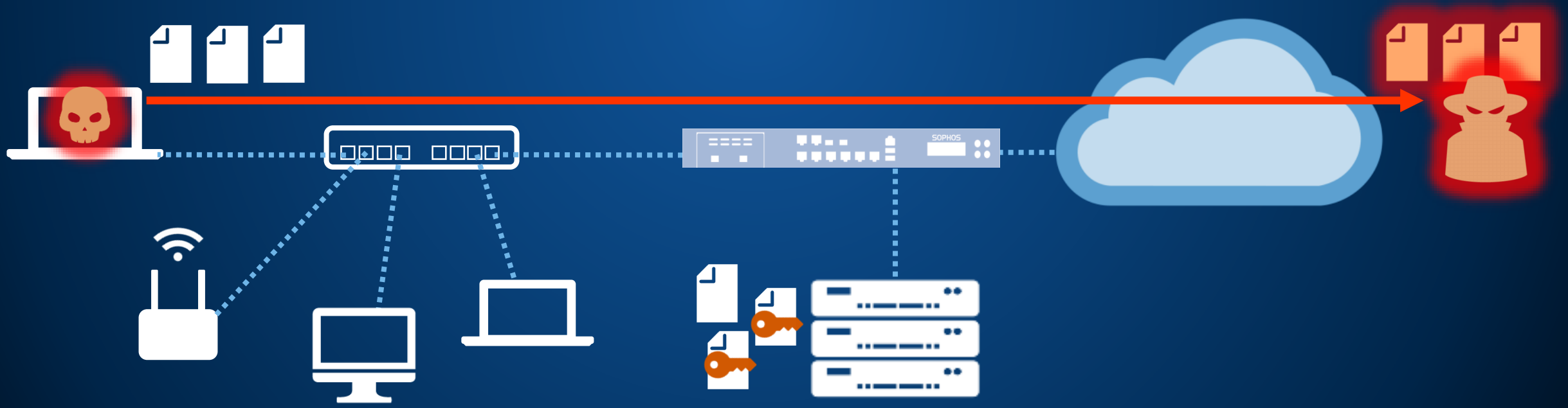


SOPHOS

..und analysiert

Security Admin

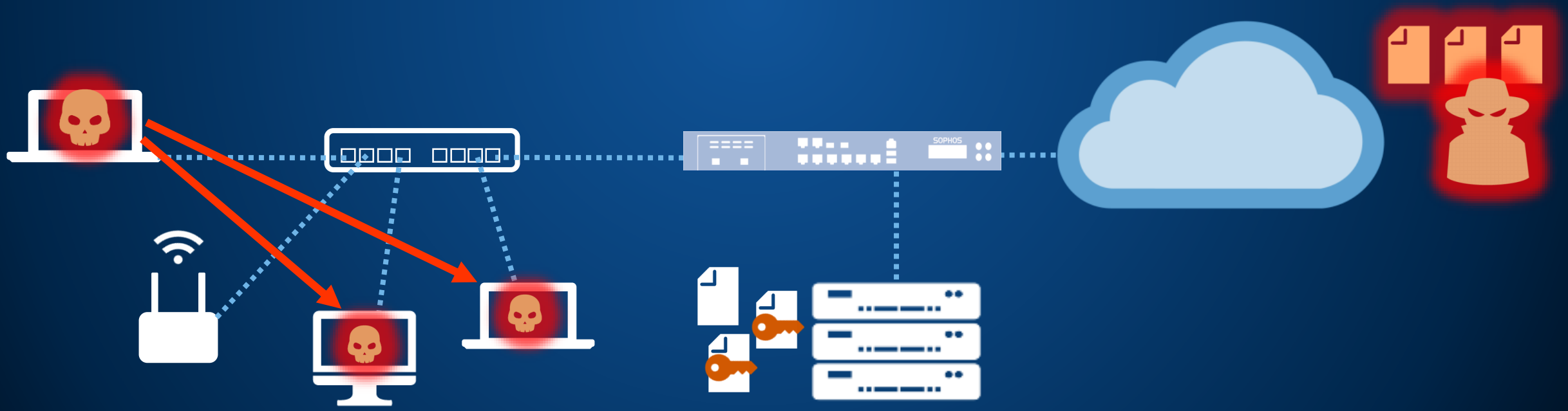
..und vertrauliche Daten an einen Angreifer im Internet geschickt



..und analysiert

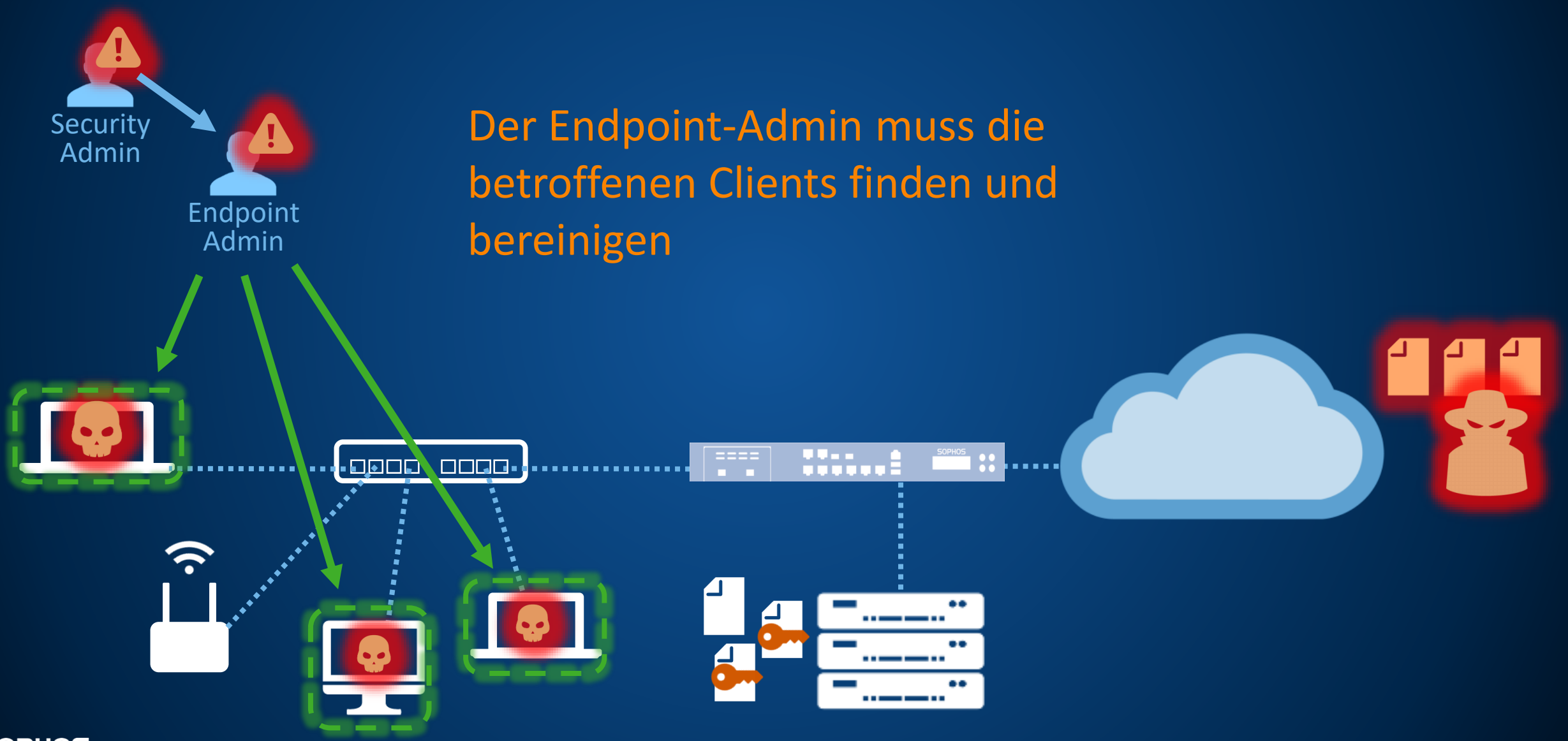
Security Admin

..außerdem wurden weitere Endpoints infiziert



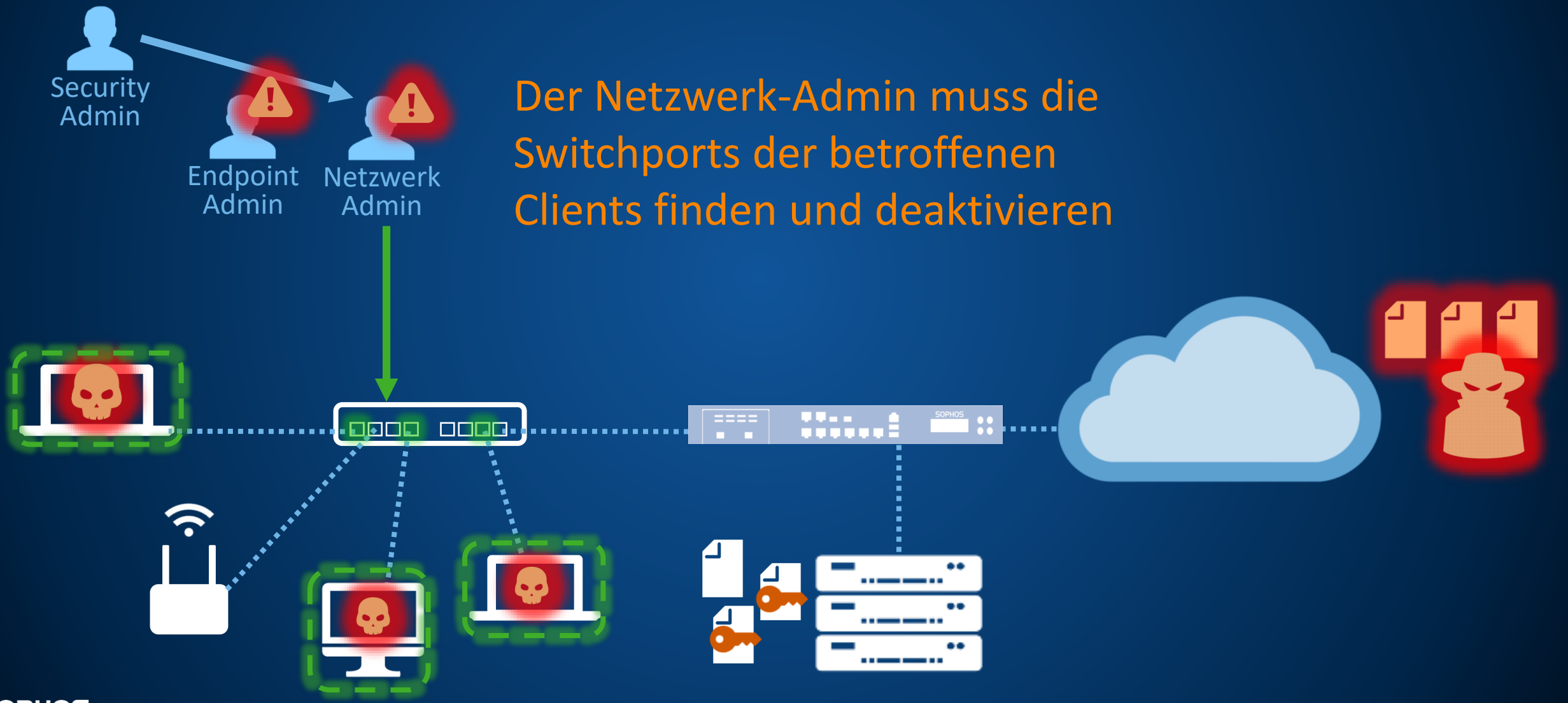
SOPHOS

Action!!!



Der Endpoint-Admin muss die betroffenen Clients finden und bereinigen

Action!!!

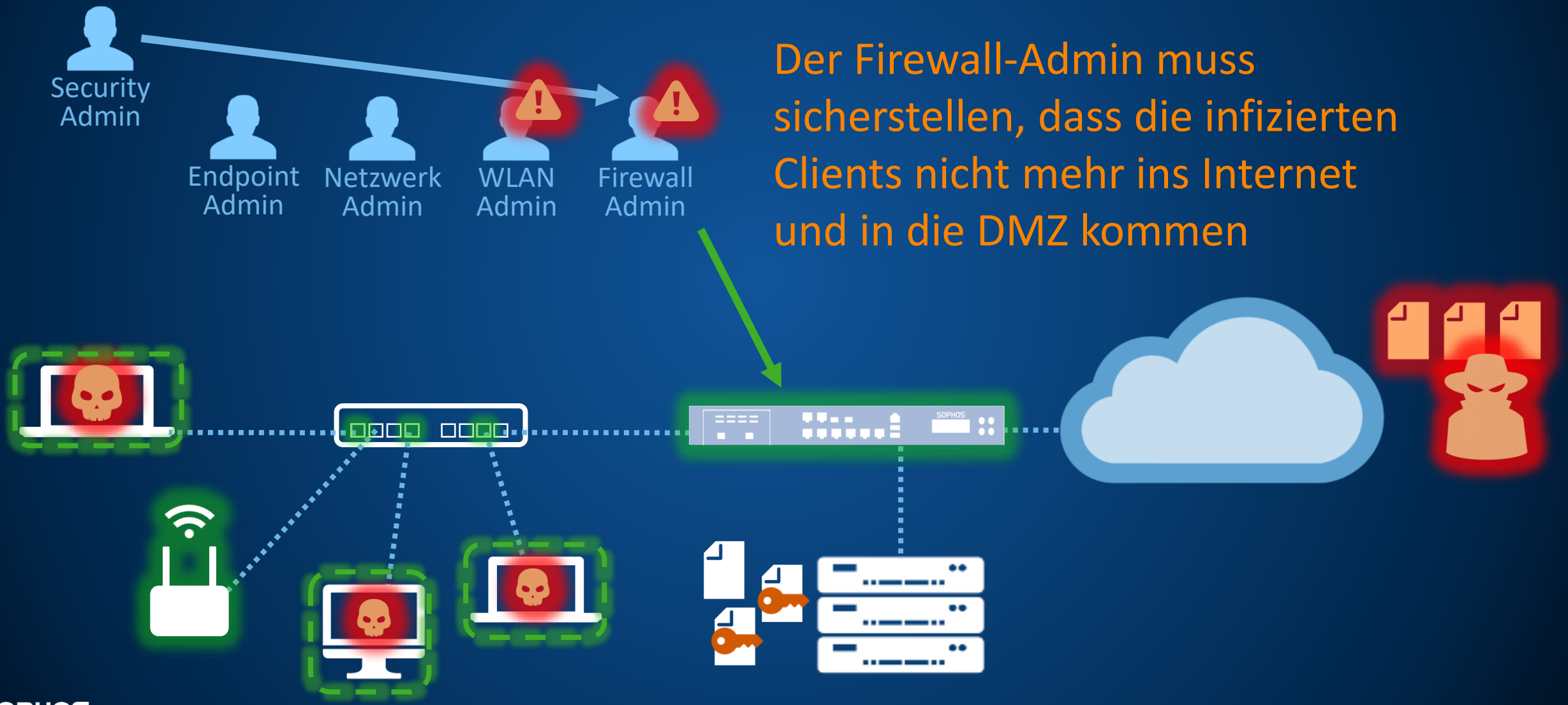


Der Netzwerk-Admin muss die Switchports der betroffenen Clients finden und deaktivieren

Action!!!

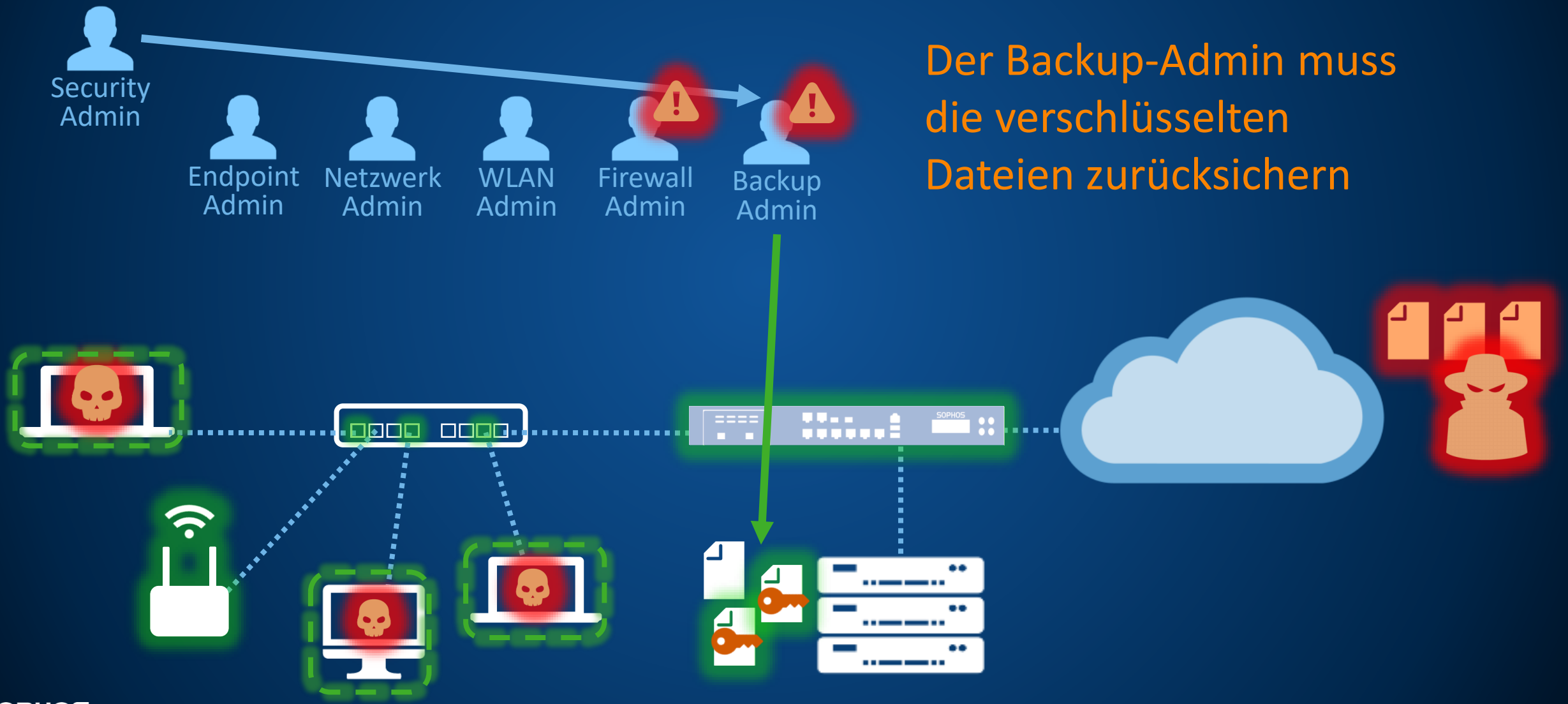
Der WLAN-Admin muss sicherstellen, dass die infizierten Clients sich nicht mehr per WLAN verbinden können

Action!!!



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

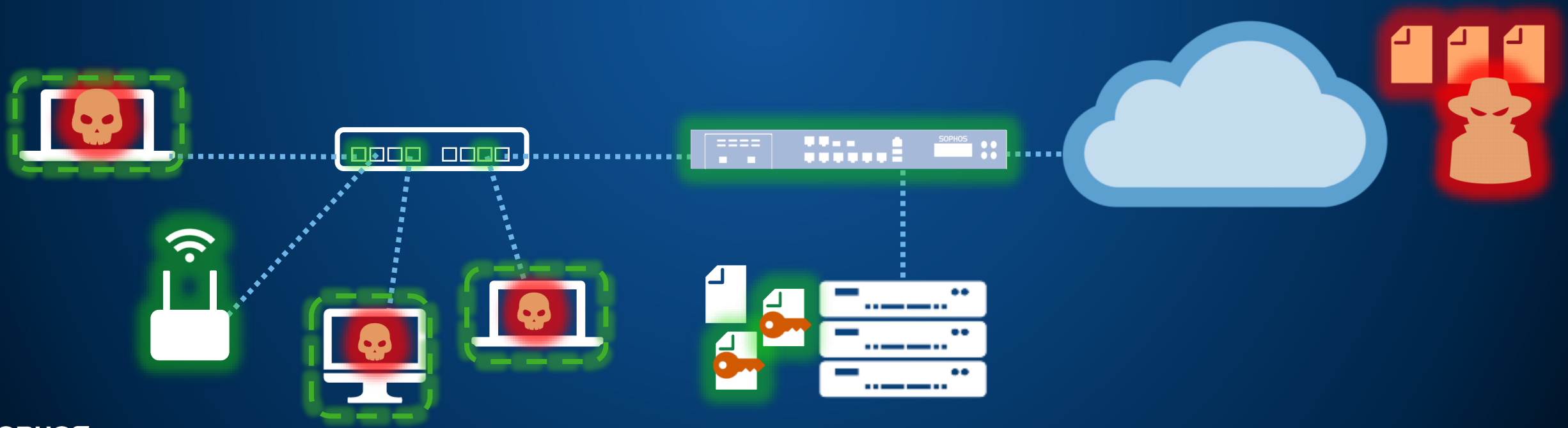
Action!!!



Der Backup-Admin muss die verschlüsselten Dateien zurücksichern

Action!!!

Jetzt wird der CISO informiert..



SOPHOS

Action!!!

Security Admin

Endpoint Admin

Netzwerk Admin

WLAN Admin

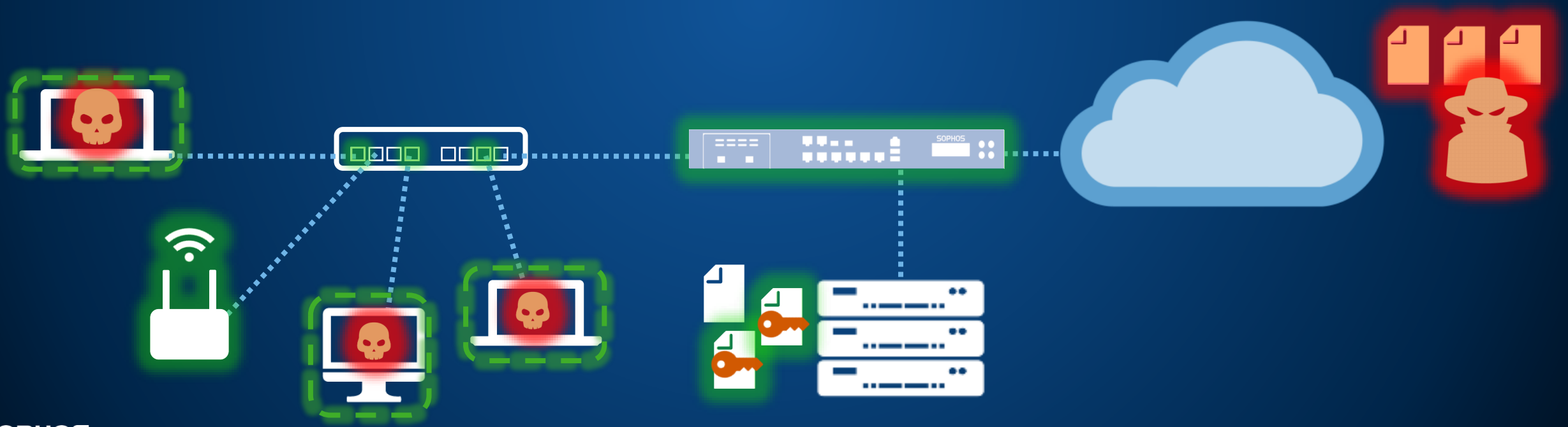
Firewall Admin

Backup Admin

CISO

CEO

..der den CEO informiert,
dass Daten gestohlen wurden

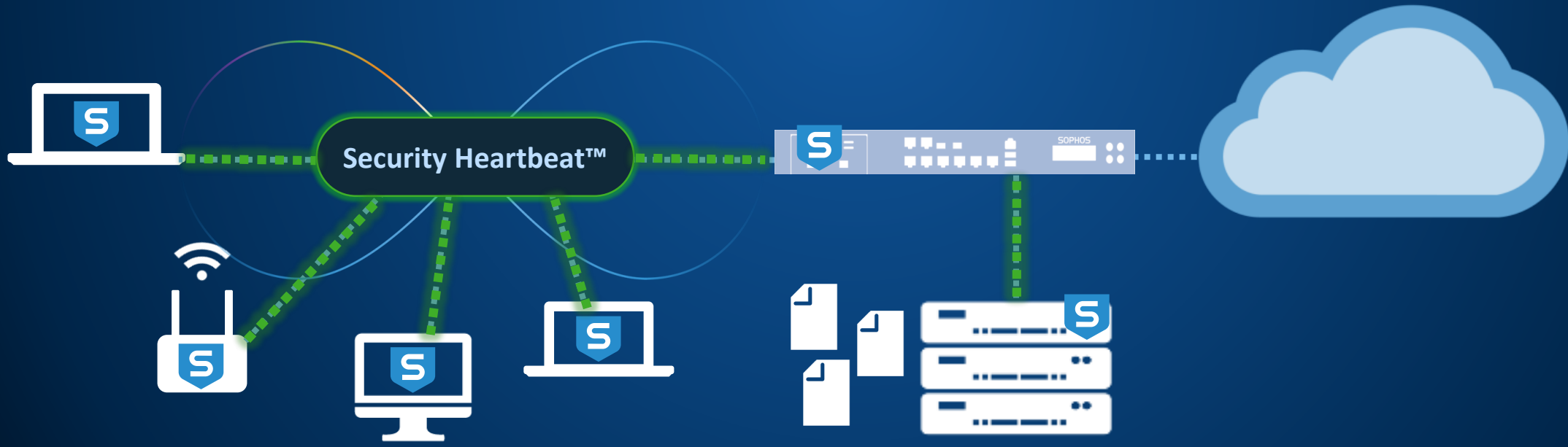


Und wie sieht es mit Synchronized Security aus?

SOPHOS

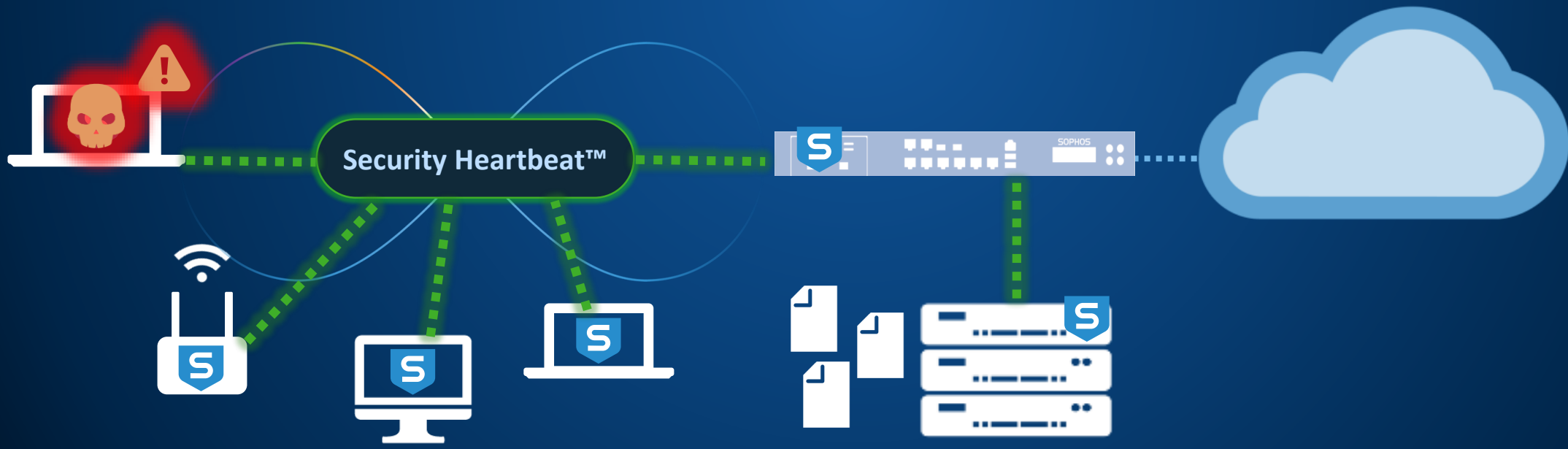
Vorgehen bei Bedrohungen mit Synchronized Security

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



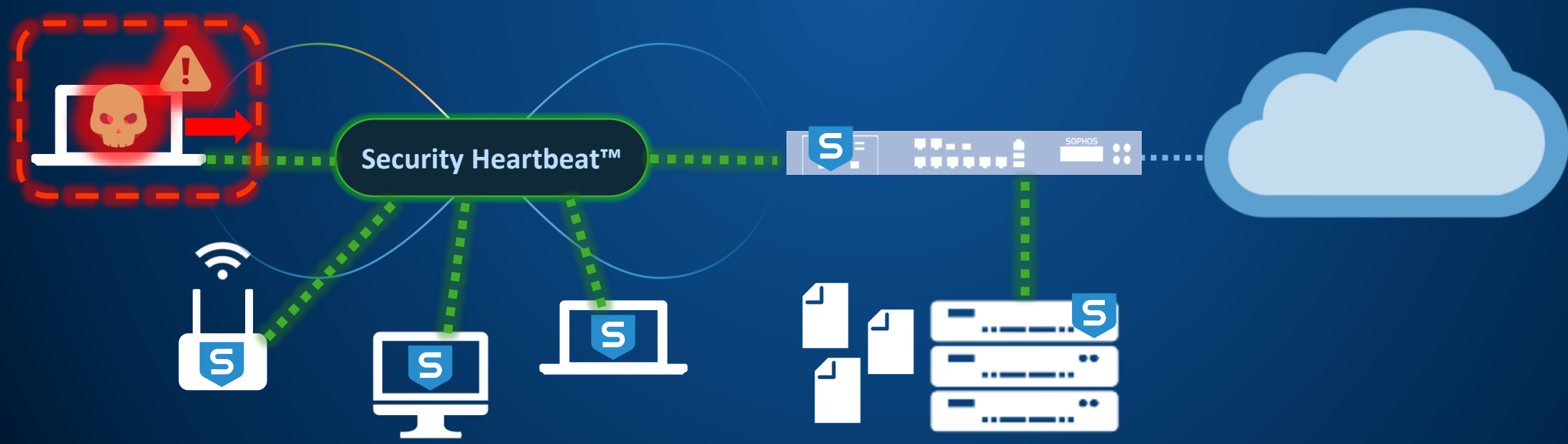
Vorgehen bei Bedrohungen mit Synchronized Security

Bei einer Bedrohung werden alle Komponenten informiert und reagieren automatisch



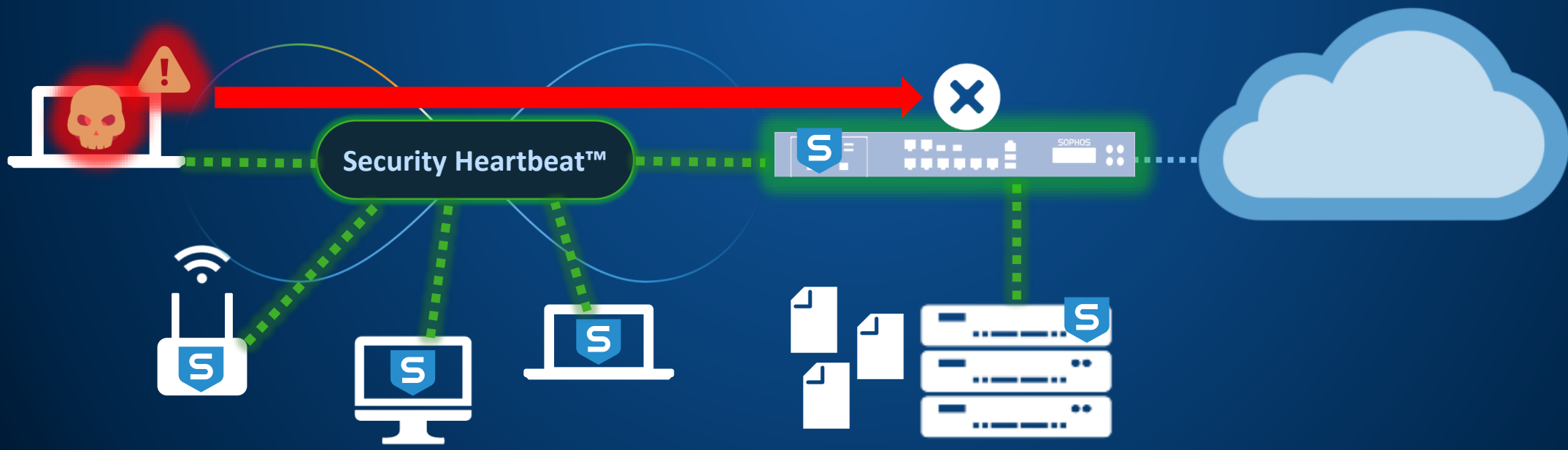
Vorgehen bei Bedrohungen mit Synchronized Security

Der Client isoliert sich selbst..



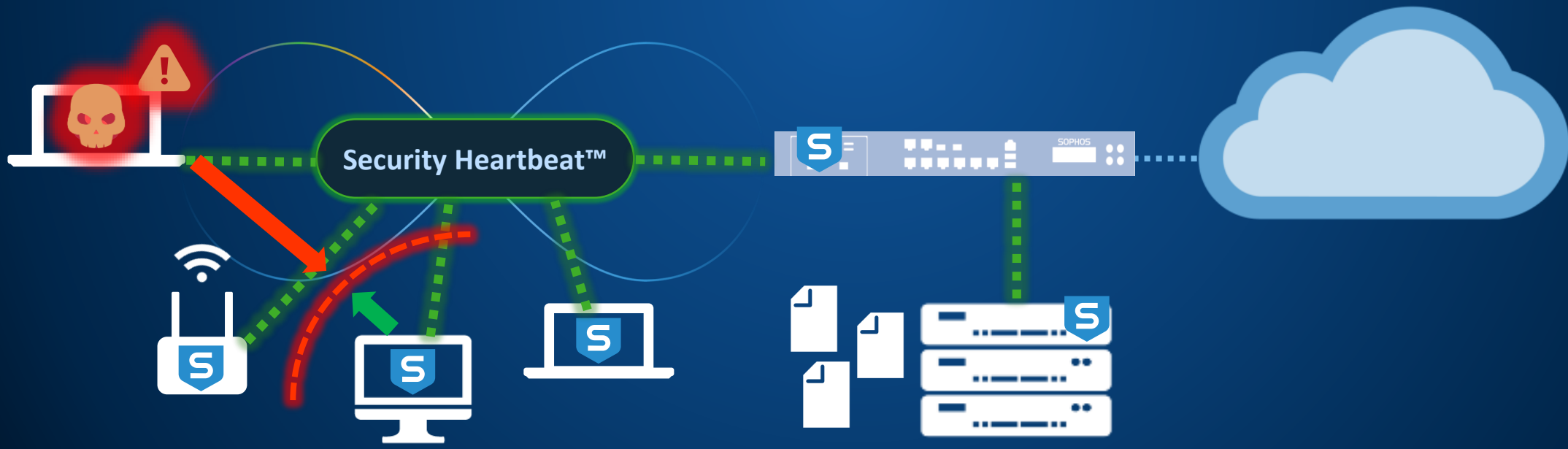
Vorgehen bei Bedrohungen mit Synchronized Security

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



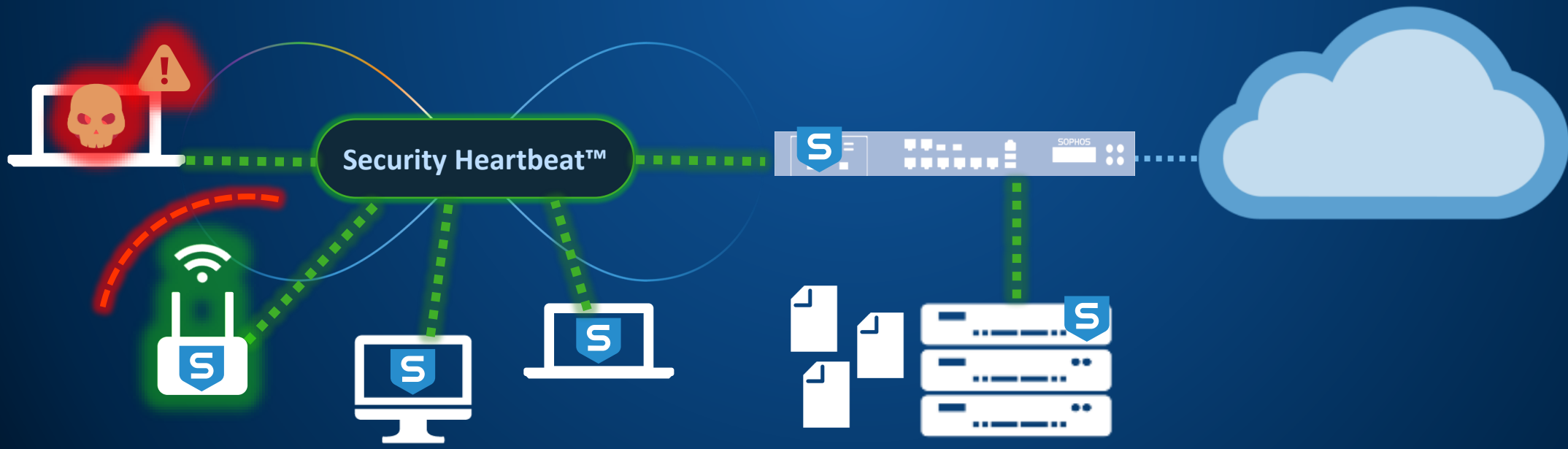
Vorgehen bei Bedrohungen mit Synchronized Security

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



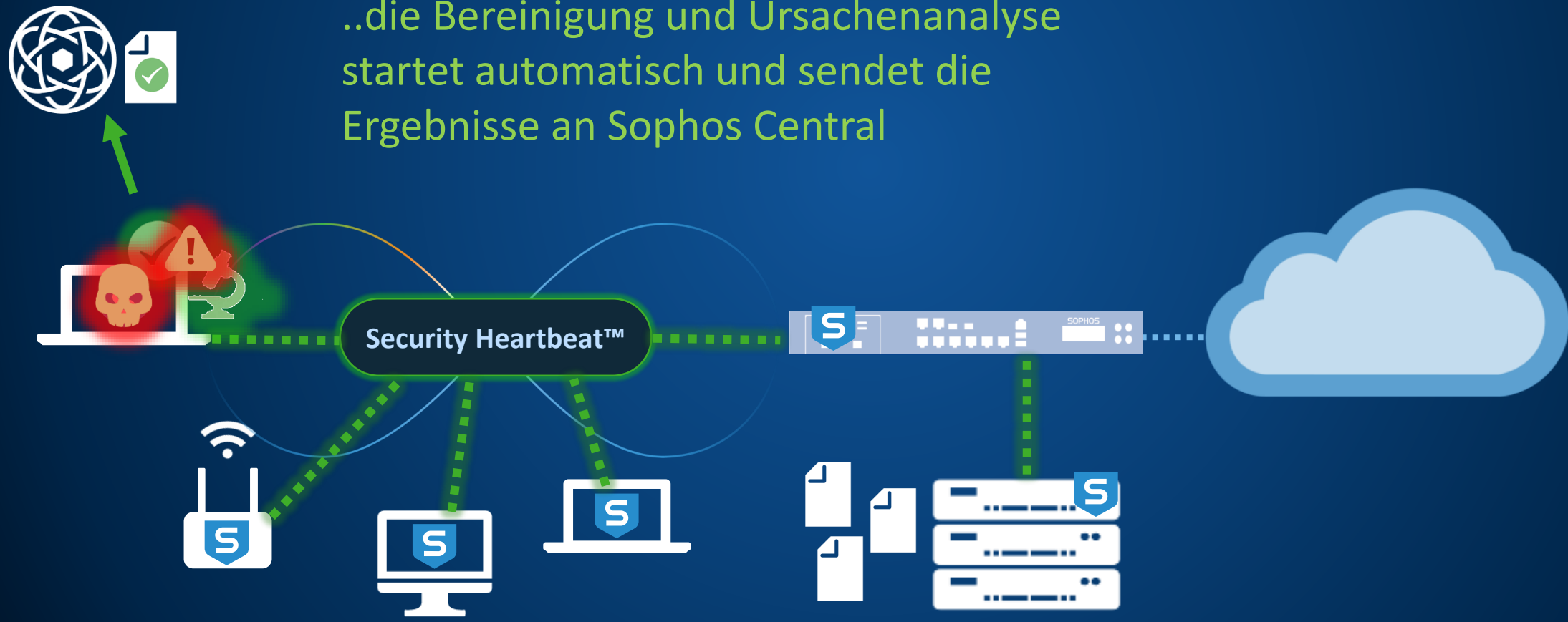
Vorgehen bei Bedrohungen mit Synchronized Security

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



Vorgehen bei Bedrohungen mit Synchronized Security

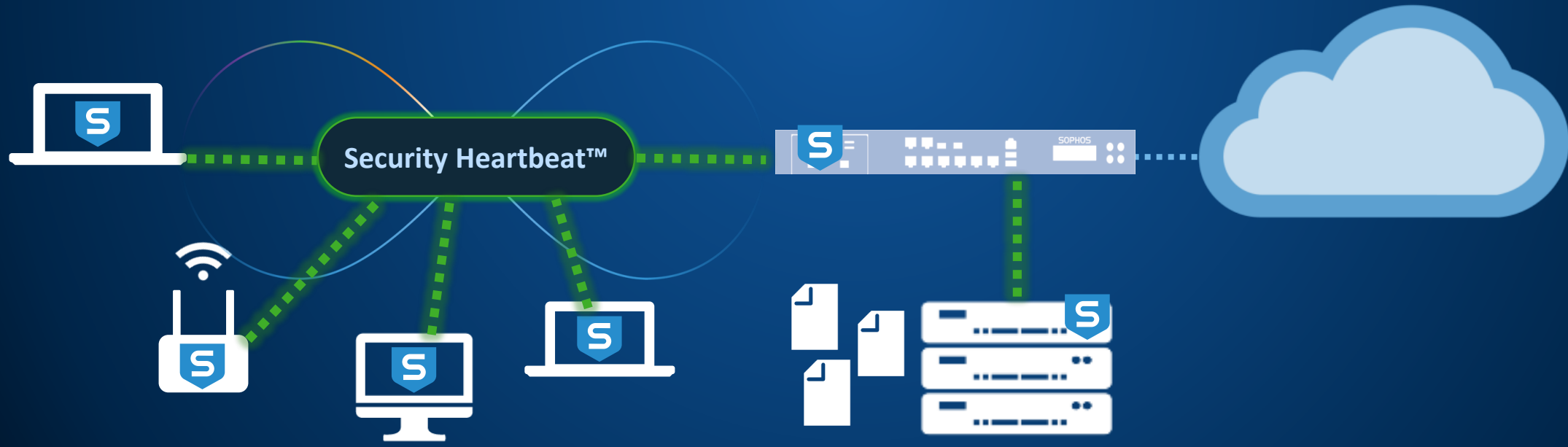
..die Bereinigung und Ursachenanalyse startet automatisch und sendet die Ergebnisse an Sophos Central



Vorgehen bei Bedrohungen mit Synchronized Security

Admin

..der Admin erhält den Bericht, dass die Bedrohung automatisch eingedämmt wurde und keine Daten gestohlen wurden



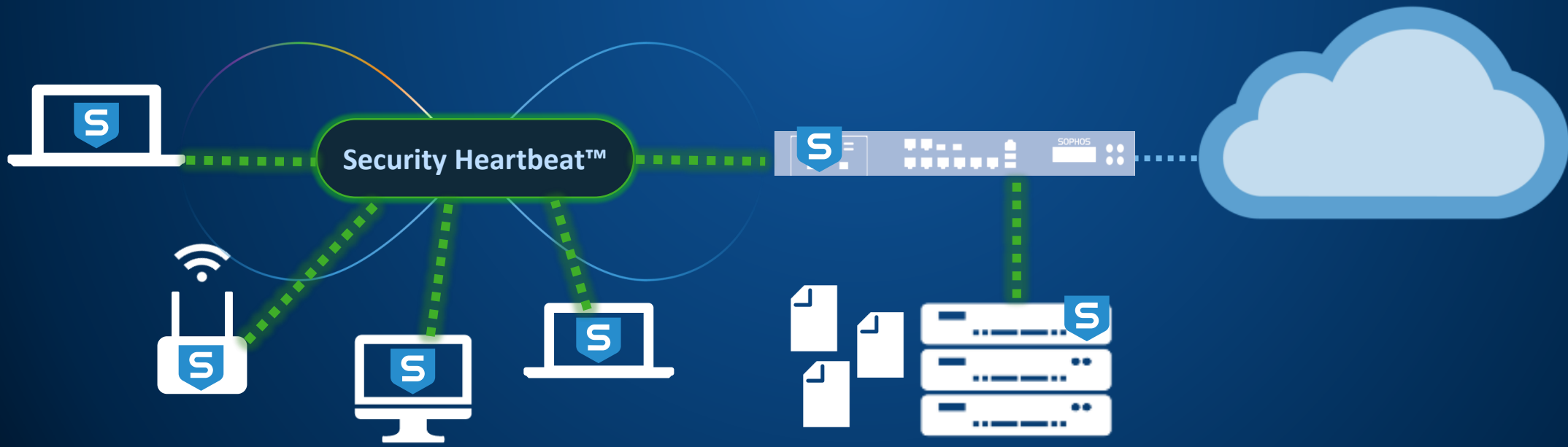
SOPHOS

Vorgehen bei Bedrohungen mit Synchronized Security

Admin

CEO

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



SOPHOS

Synchronized Security - Konzept

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

Und was ist mit KI/ML?

SOPHOS

Chancen des Machine Learning

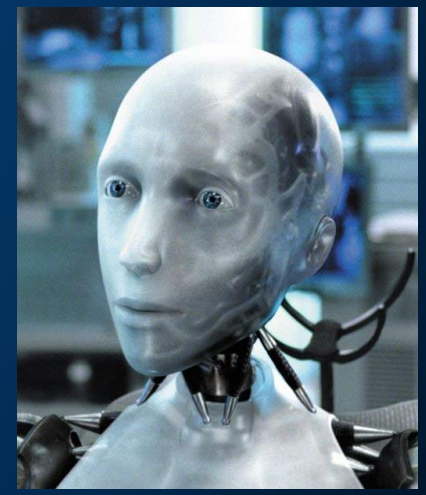
- Spezielle Aufgaben können effektiv gelöst werden
  - „Ist dieses Programm wahrscheinlich Malware?“
  - „Ist dieses Benutzerverhalten ungewöhnlich?“
- Große Datenmengen können verarbeitet und korreliert werden
  - „Welche Benutzer agieren riskant?“
  - „Ist im Netzwerk ein Hacker unterwegs?“

Aber..

SOPHOS

Grenzen des Machine Learning in der IT-Sicherheit

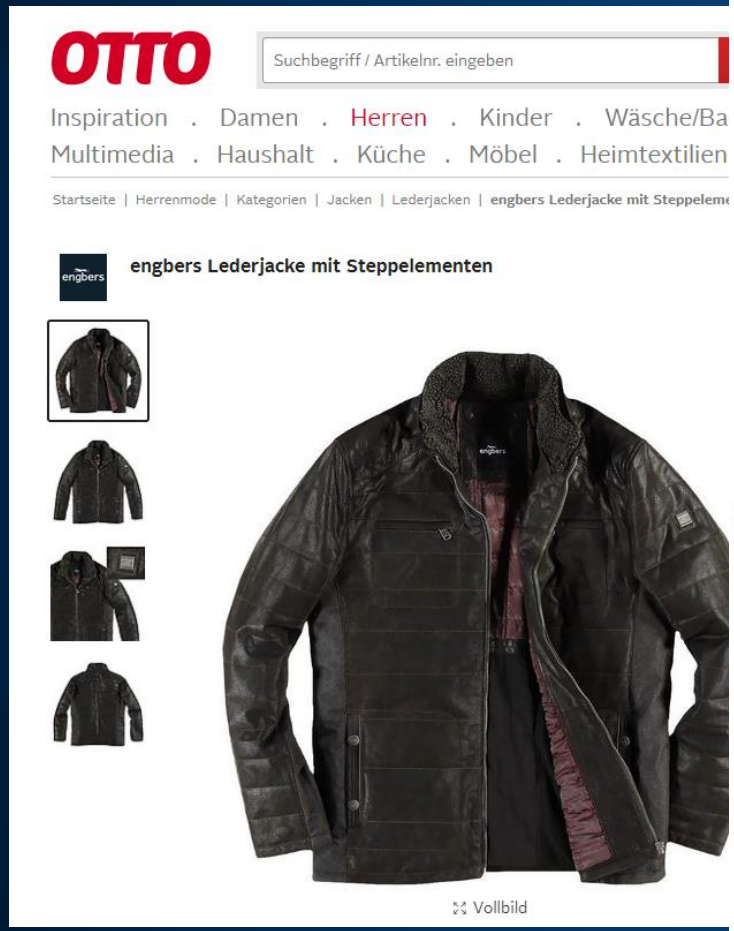
- Angreifer können einzelne Mechanismen umgehen, z.B.
  - ML-Endpoint Security
    - Qualitätssicherung bei der Malware-Entwicklung
  - Anomalie-Erkennung
    - Datendiebstahl wird in normalem Verkehr versteckt
    - Verlängerung des Zeitabstandes zwischen Aktionen
- Kreativität / Erkennung neuer Angiffsarten durch echte Künstliche Intelligenz gibt es heute (noch) nicht



Und in anderen Bereichen?

SOPHOS

Machine annoying!



Sexistische KI ?

MACHINE LEARNING

Amazon verwirft sexistisches KI-Tool für Bewerber

Weil es Frauen klar benachteiligte, hat Amazon die Arbeit an seinem Machine-Learning-gestützten Tool zur Beurteilung von Bewerbern eingestellt. Die KI hatte sich die Haltung selbst beigebracht.

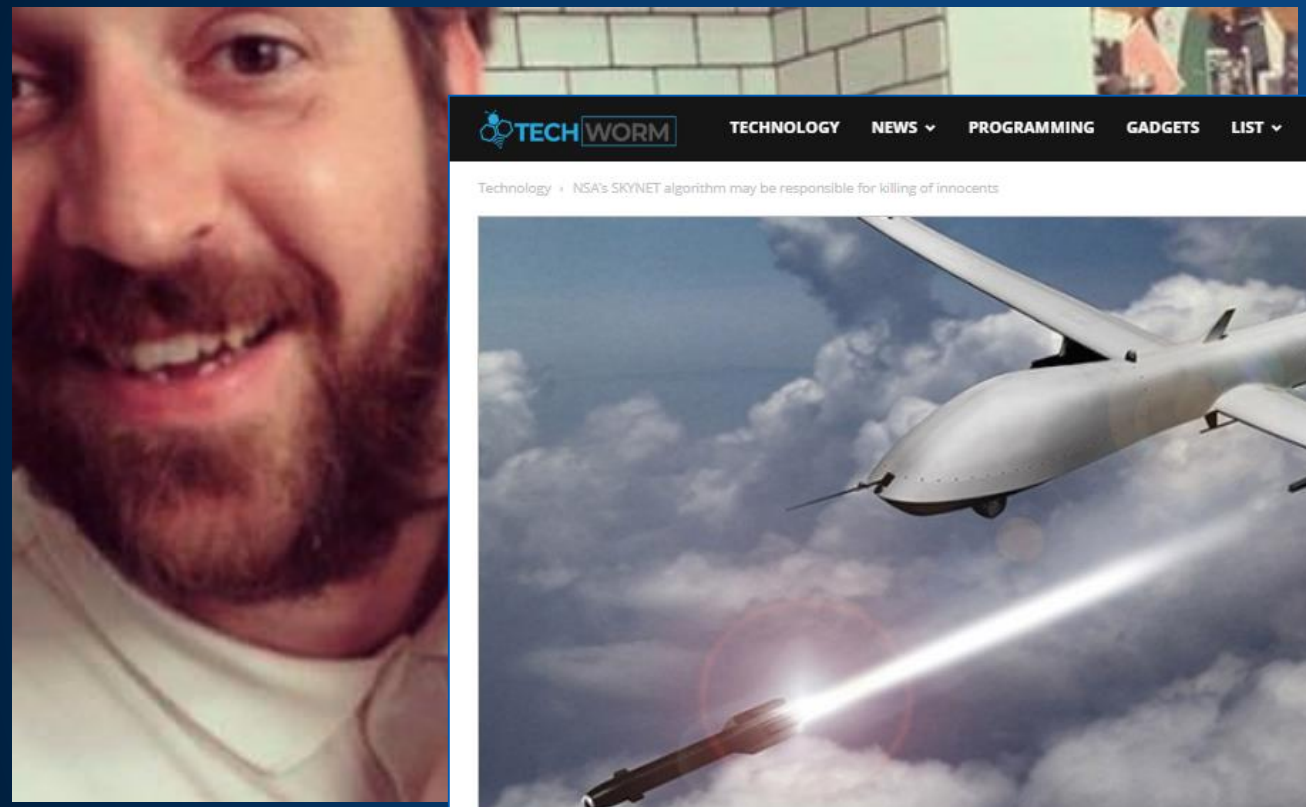
11. Oktober 2018, 13:00 Uhr, Oliver Nickel

(Bild: Pixabay.com/Montage: Golem.de/CC0 1.0)

Das Attribut Frau ist für Amazons Bewerberfilter negativ behaftet gewesen.

Amazon verwirft sein von Machine Learning gestütztes

Fehler akzeptabel?



heise online ⟩ News ⟩ 05/2016 ⟩ US-Justiz: Algorithmen benachteiligen systematisch Schwarze

24.05.2016 10:31 Uhr

US-Justiz: Algorithmen benachteiligen systematisch Schwarze

Software eingesetzt, die anhand verschiedener
von Angeklagten berechnen soll. Die funktioniert
wertet vor allem Afroamerikaner systematisch zu

384

TECHWORM TECHNOLOGY NEWS PROGRAMMING GADGETS LIST EXPLANATORY

Technology › NSA's SKYNET algorithm may be responsible for killing of innocents

Technology

NSA's SKYNET algorithm may be responsible for killing of innocents

By vijay

Recent Posts

WhatsApp iOS beta open for public; How to download it now

Greek ISPs Ordered To Block The Pirate Bay, 1337x, YTS And Other Domains

Facebook quietly launches Lasso, a TikTok-clone app to win teens over

Google confirms Dark Mode on Android

SOPHOS

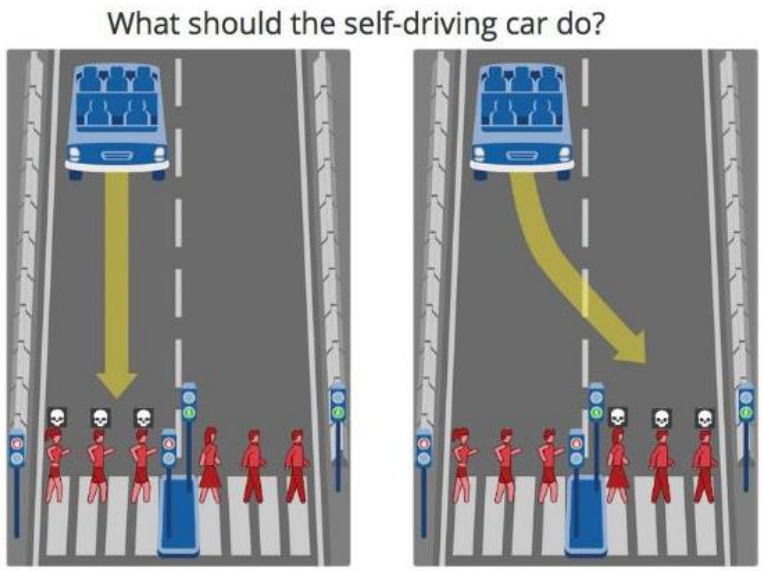
Moralische KI-Entscheidungen?

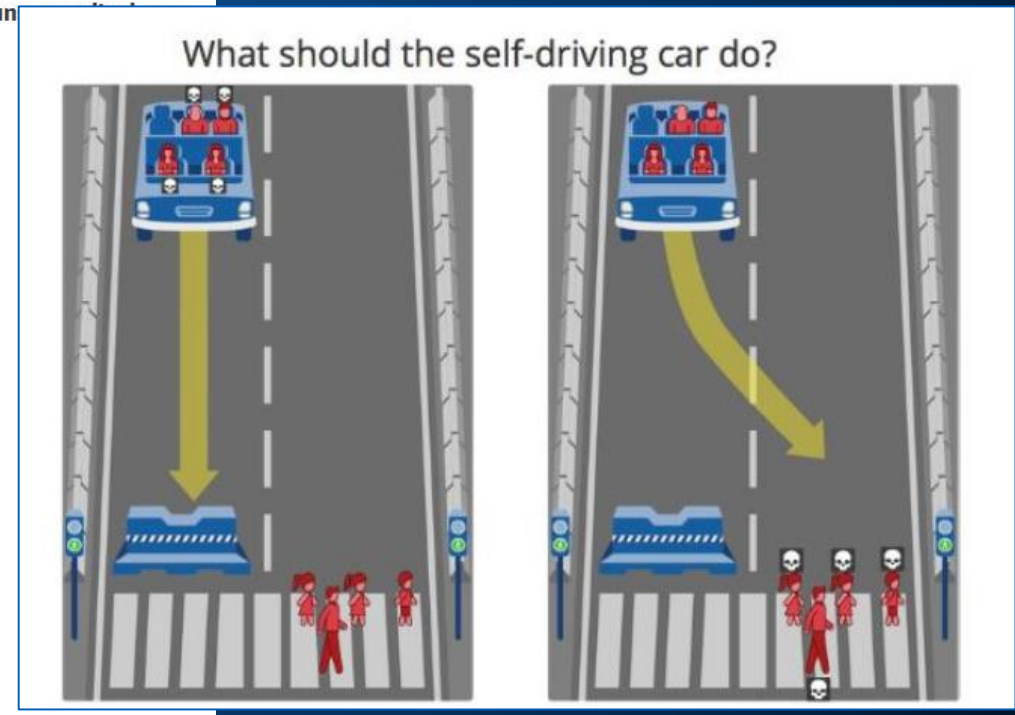
Autonomes Fahren

Was soll Ihr Auto jetzt tun?

Menschen werden selbstfahrenden Autos in Zukunft weitreichende Entscheidungen überlassen - wohl auch darüber, wer bei einer Kollision stirbt. Simuliert wird das in einem Online-Experiment, das un… Grenzen bringt.

Ein Interview von Christoph Stockburger





SOPHOS

Wirtschaftliche Dimension

- Bis 2030 über 150 Mrd USD zusätzlich Wertschöpfung durch KI
  40% durch Effizienzgewinn, 60% durch neue Angebote
- Seit 2012 mehr als 2300 Aquisitionen im Bereich KI weltweit
- Allein 2016 ca 20-30 Mrd. Investition in KI
- Besonders aktiv: Google, Facebook, Amazon, Microsoft, Apple, Baidu

Globale Dimension

Handelsblatt Premium
KOSTENLOS TESTEN »

Handelsblatt

HOME POLITIK UNTERNEHMEN FINANZEN TECHNIK AUTO KARRIERE ARTS & STYLE MEINUNG VIDEO SERVICE

IT + Internet Gadgets Forschung + Innovation Medizin Energie + Umwelt Edison

Handelsblatt > Technik > The Spark > Künstliche Intelligenz: Wie China zur Supermacht aufsteigt

Suchbegriff, WKN, ISIN

TECHNIK DER ZUKUNFT

Wie China bei der Künstlichen Intelligenz zur Supermacht aufsteigt

China setzt entschlossen auf die KI. Erstmals seit der industriellen Revolution könnte der Westen die Vorherrschaft bei einer globalen Schlüsseltechnologie verlieren.

Sha Hua, Thomas Jahn, Christof Kerkmann, Sebastian Matthes, Stephan Scheuer, Britta Weddeling

25.10.2018 - 20:10 Uhr • 1 Kommentar • 87 x geteilt

Putin - „Künstliche Intelligenz wird die Welt beherrschen“

Veröffentlicht am 01.09.2017 | Dauer 36 Sek

Wer immer einen Durchbruch bei der Entwicklung künstlicher Intelligenz erzielt, wird nach Ansicht des russischen Präsidenten künftig die Welt dominieren. Künstliche Intelligenz eröffne „kolossale Möglichkeiten und Bedrohungen“.

Wirtschaft 〉 Künstliche Intelligenz 〉 Emmanuel Macron setzt auf Künstliche Intelligenz

E-Paper ABONNEMENT

Frankfurter Allgemeine
Künstliche Intelligenz

Frankfurt am Main 9°

F.A.Z.-INDEX 2.207,34 +0,15 % DAX ° 11.379,67 +0,23 % EUR/USD 1,1398 +0,66 % DOW JONES 25.386,40 -- ALLE KURSE

TECHNOLOGIE DER ZUKUNFT

Macron setzt auf Künstliche Intelligenz

AKTUALISIERT AM 27.03.2018 - 08:47

Frankreichs
für eine Schl

ABO SHOP AKADEMIE JOBS MEHR

E-PAPER AUDIO APPS ARCHIV ANMELDEN

ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur Wissen Digital Campus Arbeit Entdecken Sport ZEITmagazin Podcasts mehr Z+

Kanzlerin fordert mehr Investitionen in künstliche Intelligenz

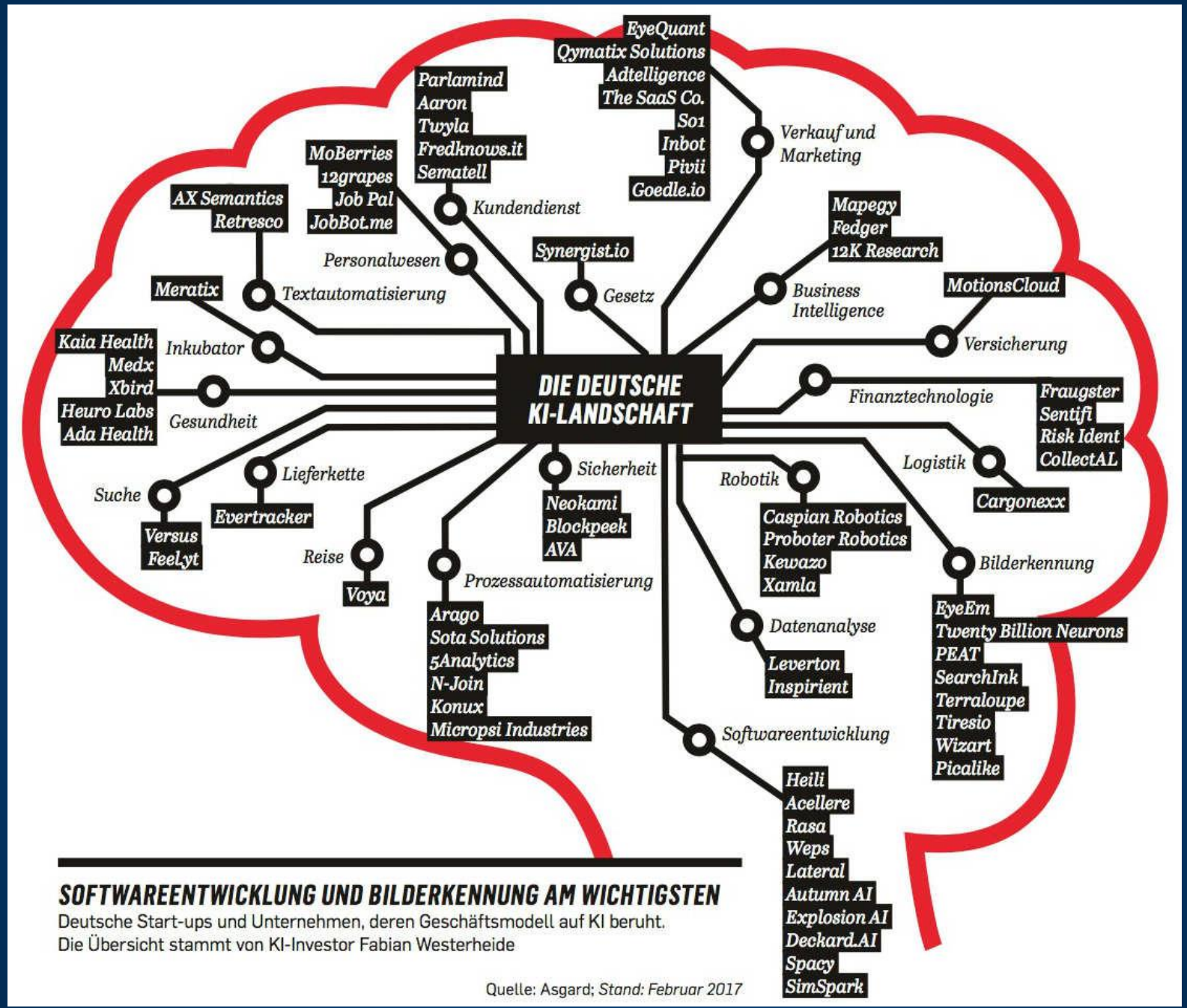
Das Kabinett trifft sich zu einer zweitägigen Digitalklausur. "Wir müssen führender Standort für künstliche Intelligenz sein", sagt Angela Merkel in einem Interview.

14. November 2018, 8:21 Uhr / Quelle: ZEIT ONLINE, KNA, dpa, jci / 116 Kommentare

SOPHOS

Deutschland Vorreiter bei Forschung

- DFKI Deutsches Forschungszentrum KI seit 1988, 900 Mitarbeiter, 4 Filialen in Deutschland, größtes KI-Forschungsinstitut weltweit
- Cyber Valley in Tübingen+Stuttgart, Initiative des Max-Plack-Instituts für Intelligente Systeme, Investoren: Porsche, Amazon, FB
- 80-100 Start-Ups mit KI in Deutschland
- Deutsche Investoren zurückhaltend, scheuen Risiken



SOFTWAREENTWICKLUNG UND BILDERKENNUNG AM WICHTIGSTEN

Deutsche Start-ups und Unternehmen, deren Geschäftsmodell auf KI beruht.
Die Übersicht stammt von KI-Investor Fabian Westerheide

Quelle: Asgard; *Stand: Februar 2017*

SEE THE

FUTURE

michael.veit@sophos.de

SOPHOS