SEE THE FUTURE

Live Demo

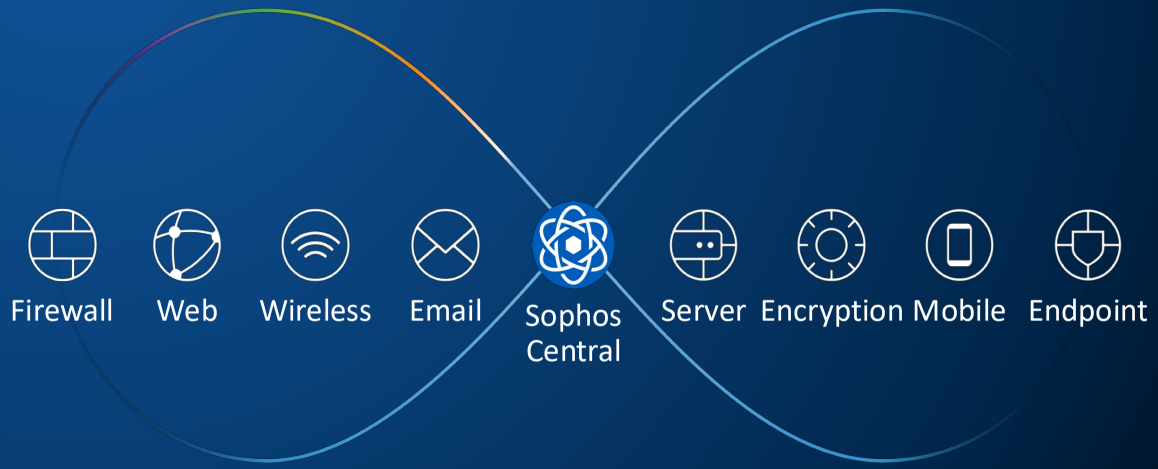
Wie Zero-Days und Ransomware Unternehmen heute bedrohen

Michael Veit
Technology Evangelist

SOPHOS

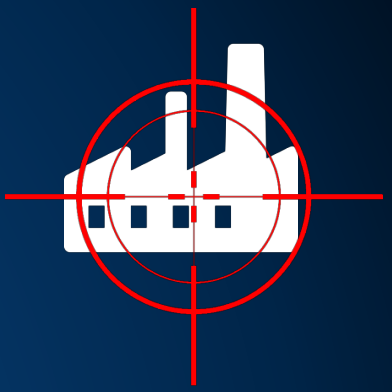
Sophos im Überblick

- 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

Unternehmen im Visier



Ransomware

54% der Unternehmen in 2017 von Ransomware betroffen

Ransomware

26% der Malware in 2017

Advanced Threats

83% sagen, dass moderne Angriffe schwer zu stoppen sind

Advanced Threats

1% nutzen Passwortdiebstahl / Rechteausweitung

Exploits

Die meisten Unternehmen haben keinen Exploit-Schutz

Exploits

20% der Malware nutzt Exploits

SOPHOS

Quelle: The State of Endpoint Security Today Survey, Jan 2018

Source: SophosLabs

Unbekannte Bedrohungen sind immer schwerer zu erkennen

400,000

SophosLabs sehen täglich
400,000 bisher unbekannte
Malware-Samples

75% der Malware-Samples
sehen wir nur in einem
einzigen Unternehmen

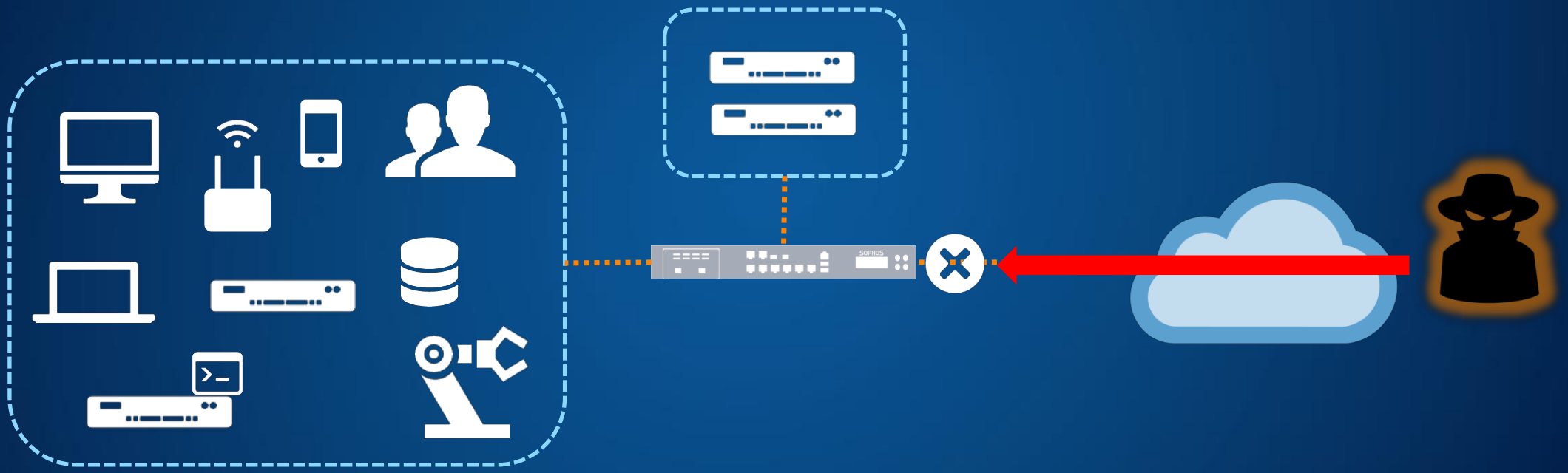
SOPHOS

Quelle: SophosLabs

Neue Sicherheitskonzepte sind notwendig

SOPHOS

Es war einmal… Netzwerk vs. Endpoint Sicherheit

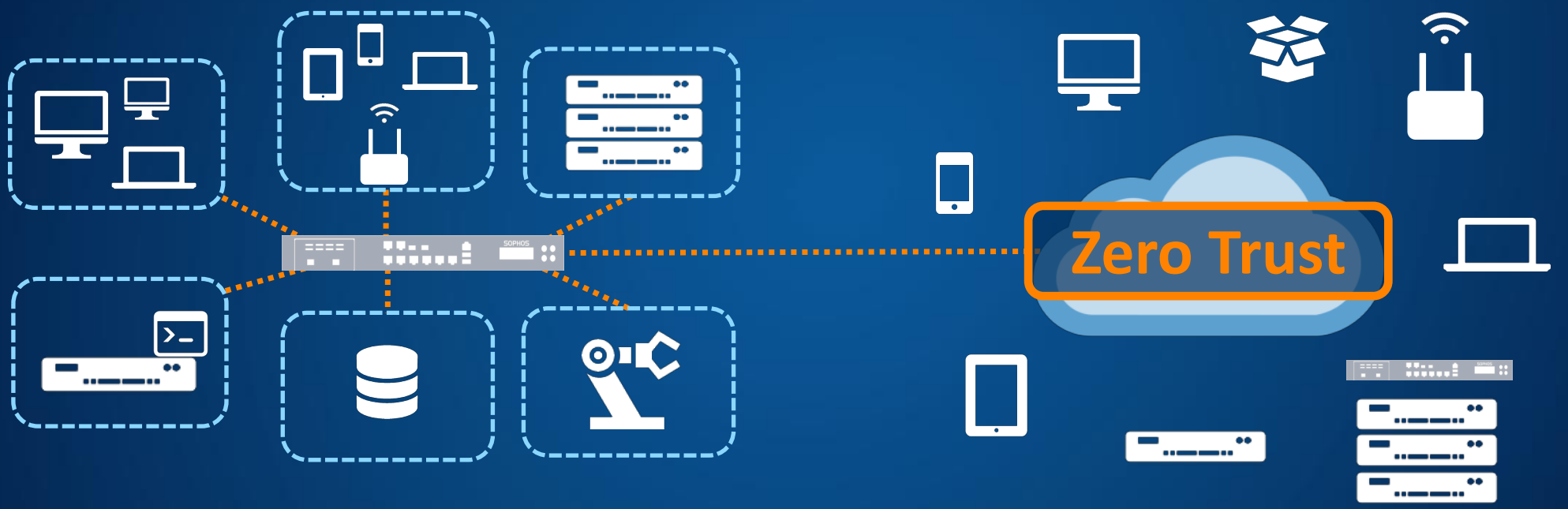


Es war einmal… Netzwerk vs. Endpoint Sicherheit

Konsequenz 1:
Segmentierung
und
ZeroTrust

SOPHOS

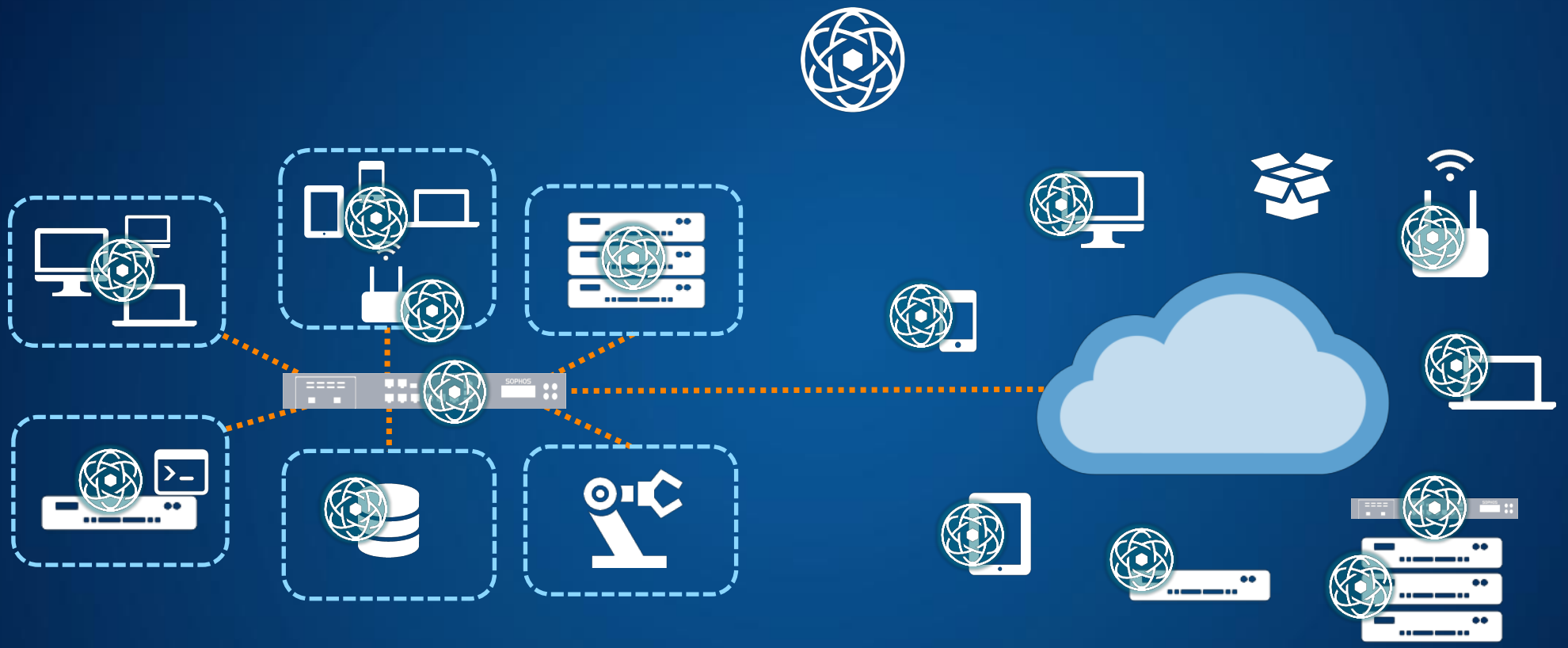
Heute: Netzwerksegmentierung und Zero-Trust



Konsequenz 2:
Zentrales Management
aller Geräte

SOPHOS

Zentrales Management aller Geräte

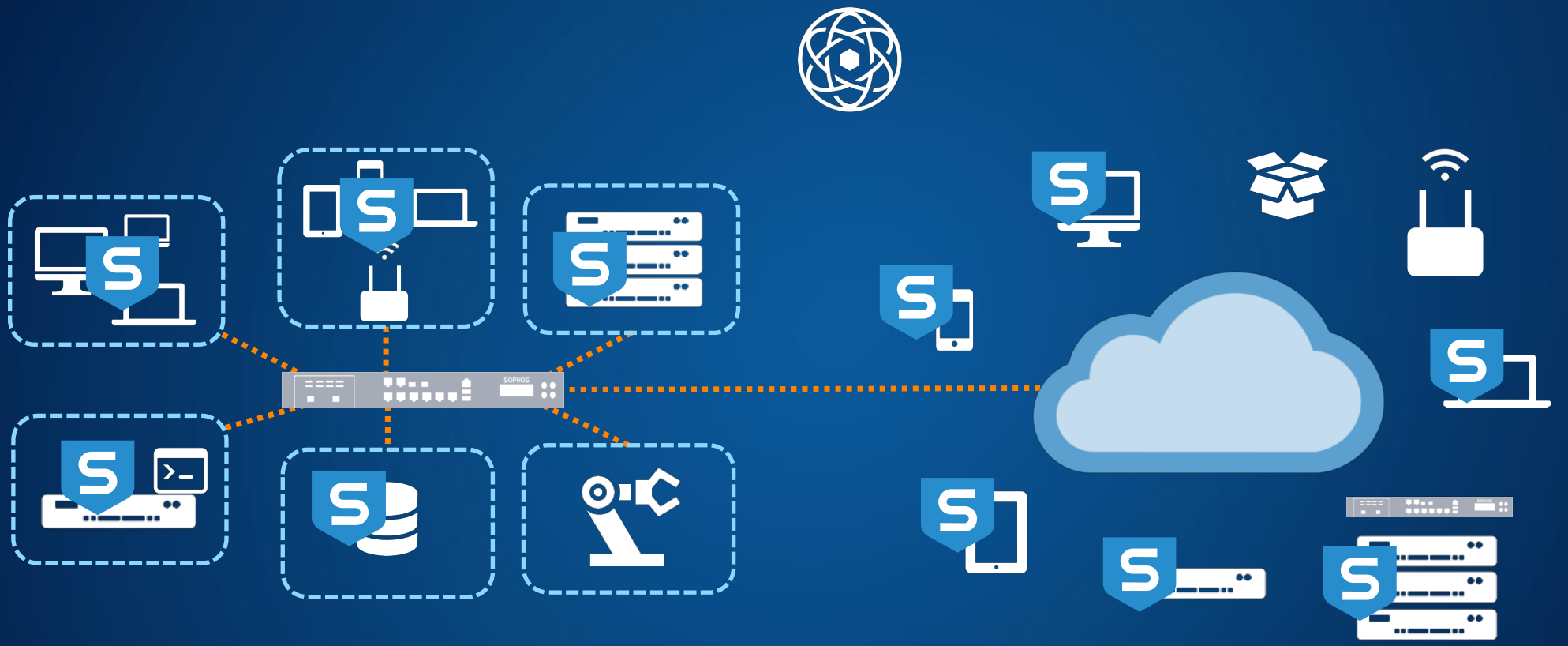


SOPHOS

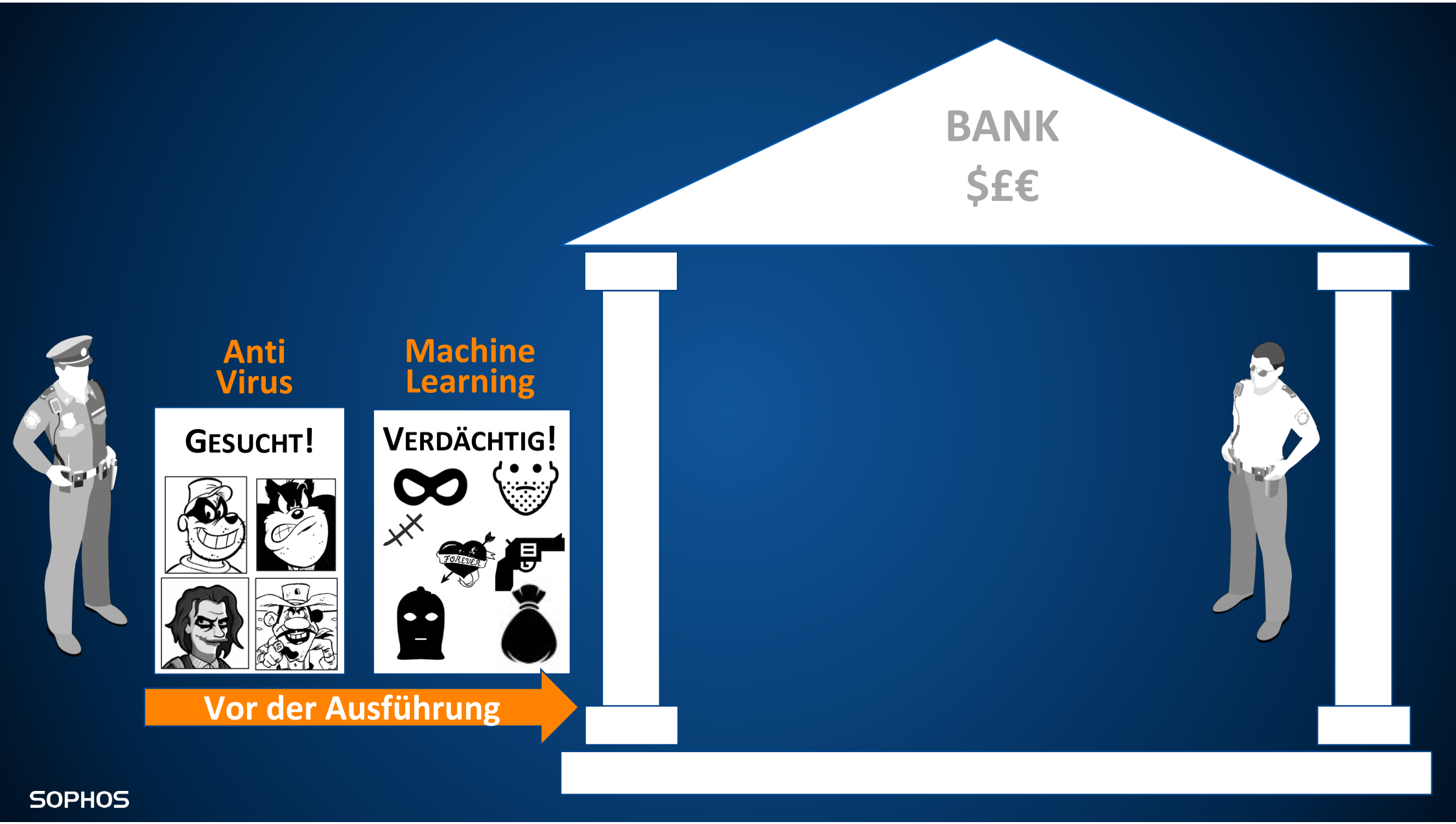
Konsequenz 3:
Geräte müssen sich
selbst schützen

SOPHOS

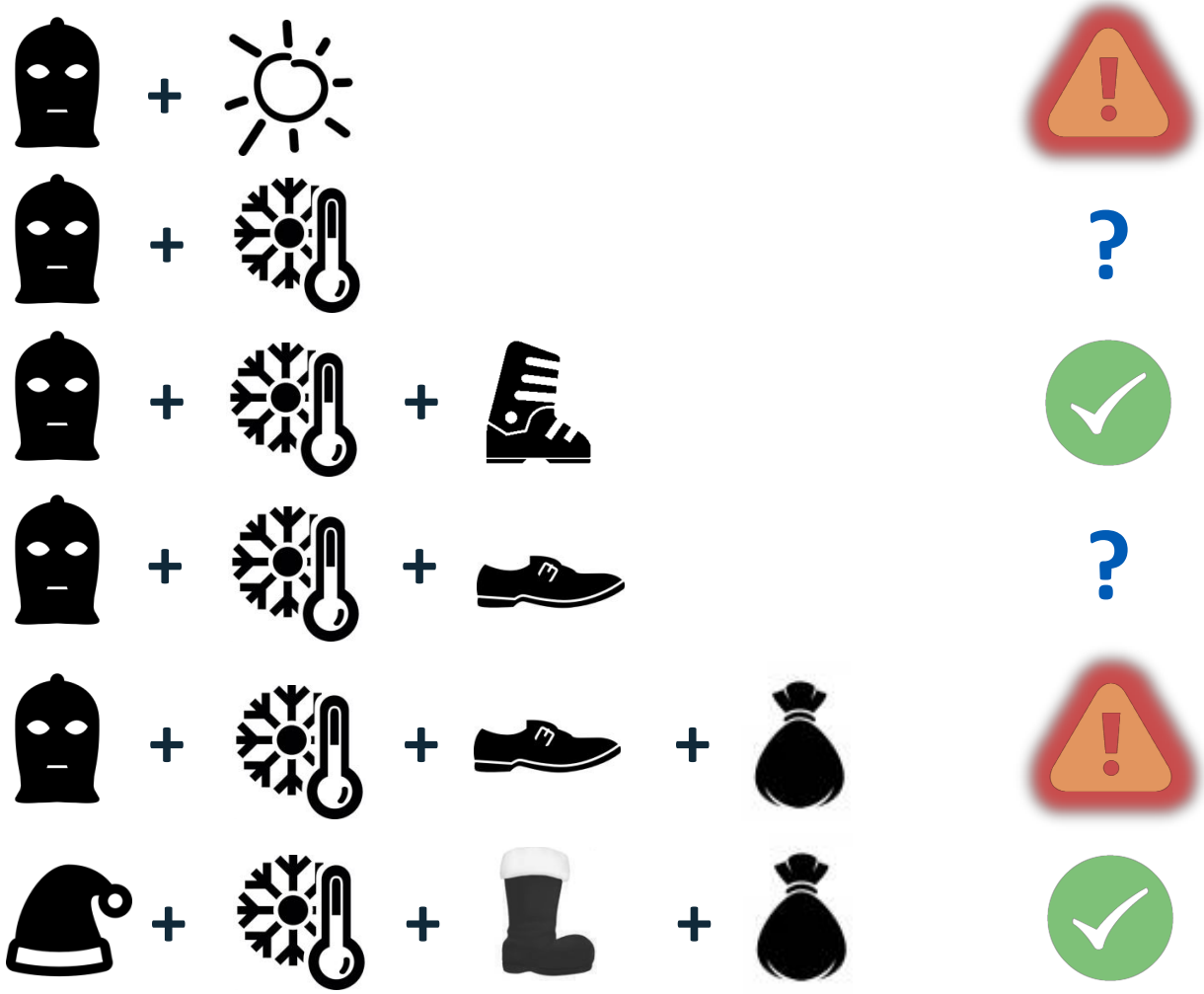
Geräte müssen sich selbst schützen



SOPHOS


BANK
$£€
Anti Virus
Machine Learning
GESUCHT!
VERDÄCHTIG!
FOREVER
Vor der Ausführung
SOPHOS

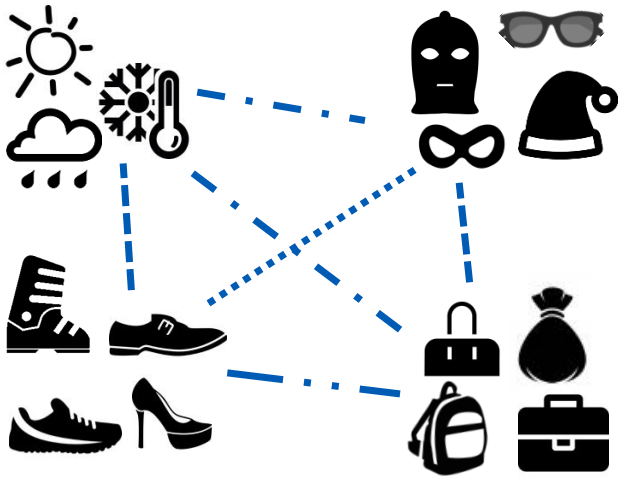
Machine Learning



Konventionelles Machine Learning

Menschlicher Analyst identifiziert Merkmale und definiert deren Beziehungen

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



SOPHOS Deep Learning

Neuronales Netz lernt selbstständig Merkmale und deren Beziehungen

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

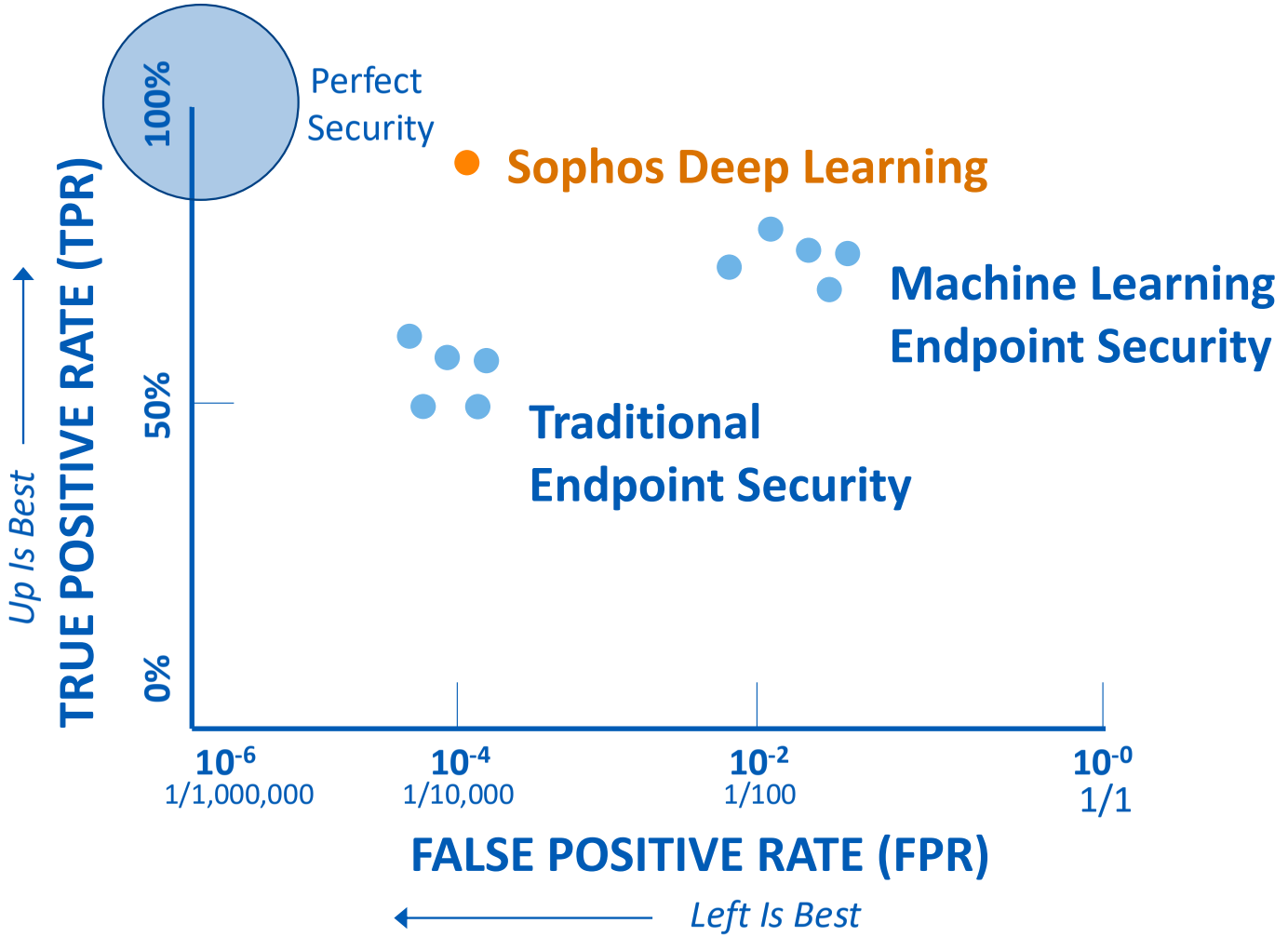
SOPHOS Deep Learning

- Erkennt bekannte und unbekannte Bedrohungen ohne Signaturen
- Extrem schnell – Erkennung in < 20ms
- Funktioniert auch offline
- Sofort einsatzfähig, kein Training beim Kunden notwendig
- Sehr zuverlässig – geringste False Positive Rate
- Profitiert von 30 Jahren Erfahrung und 100e Millionen von Samples
- Bewährt – überzeugt in unabhängigen Tests!

"One of the ***best performance scores*** we have ever seen in our tests"
Maik Morgenstern, CTO, AV-TEST

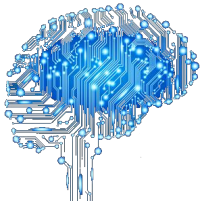
VIRUS TOTAL NSS LABS AV TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS

Sophos – beste Erkennung bei weniger False Positives



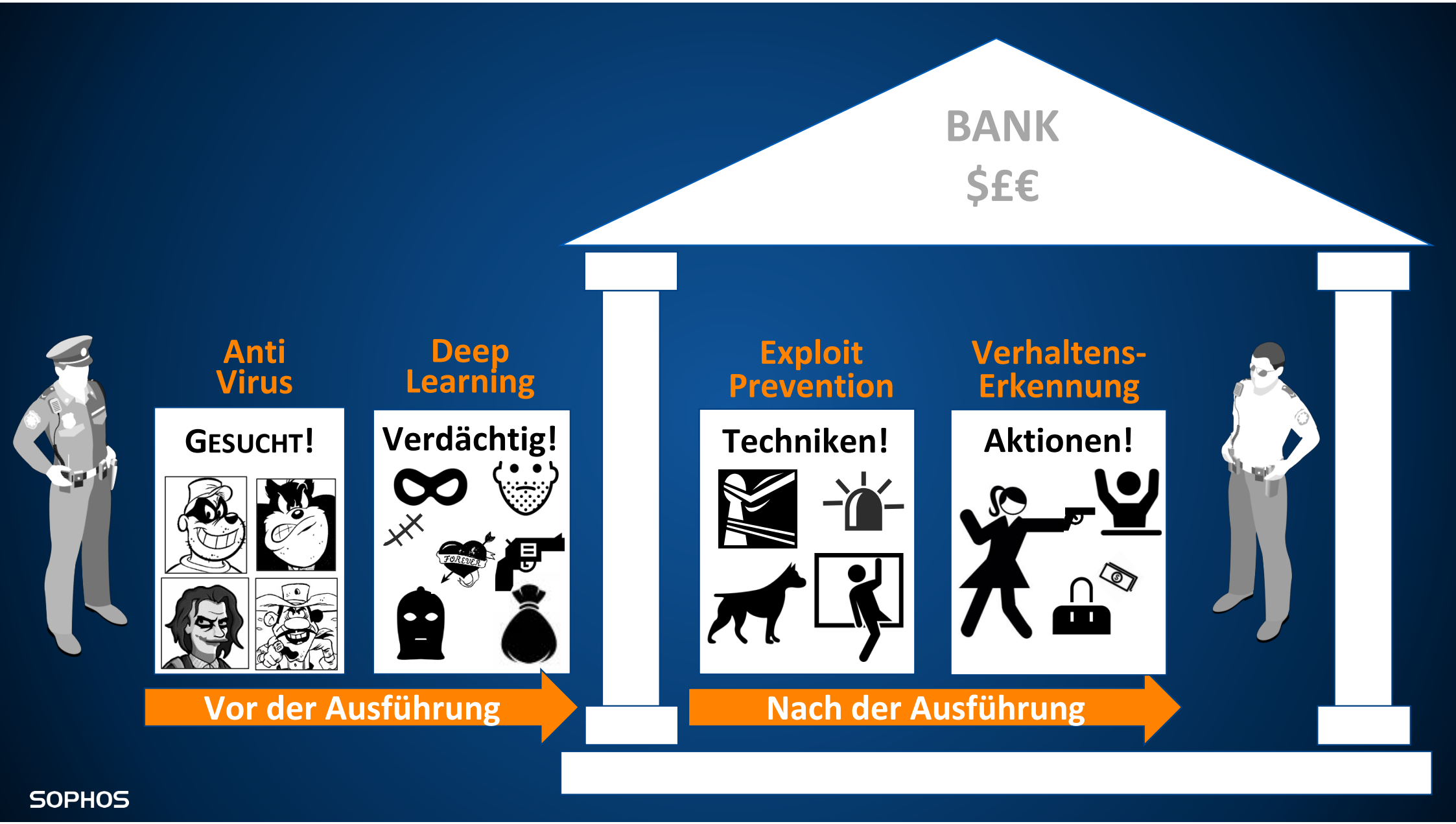
Source: SophosLabs analysis of malware found in the wild

Machine Learning / Deep Learning



- Sehr effektiv, um Programmdateien vor der Ausführung zu untersuchen
- Ca. 50% aller Malware kommt aktuell als Programmdatei
- Schützt nicht vor Infektionen per Exploit und speicherbasierter Malware
- Ist ein Element des Schutzes in der Infektionskette

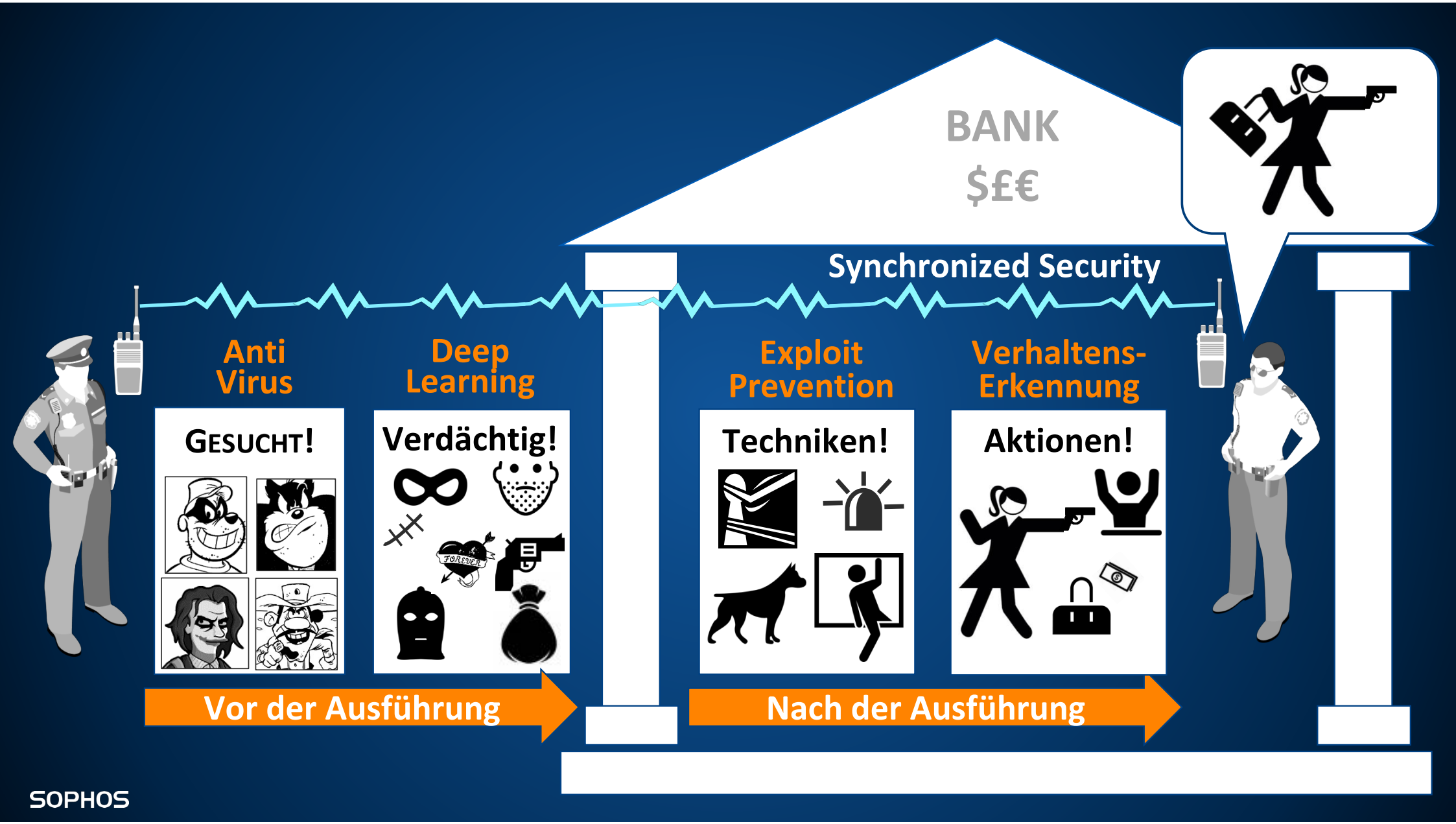
Malware	
Programmdateien	Dokumente, Mediendateien, Skripte, Java, Webseiten, rein speicherbasierte Angriffe
50%	50%

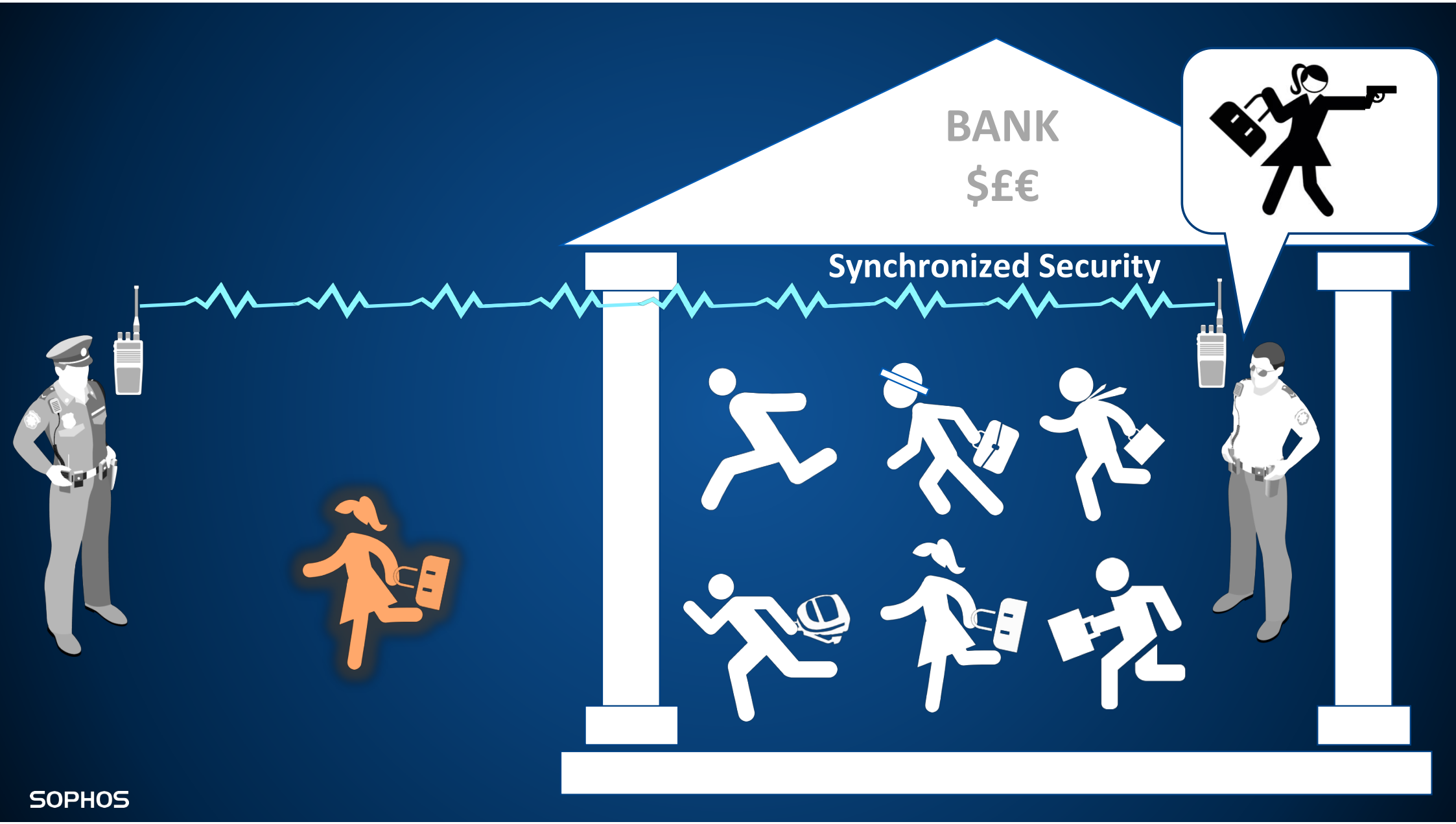

BANK
$£€
Anti Virus
GESUCHT!
Deep Learning
Verdächtig!
Exploit Prevention
Techniken!
Verhaltens-Erkennung
Aktionen!
Vor der Ausführung
Nach der Ausführung
SOPHOS

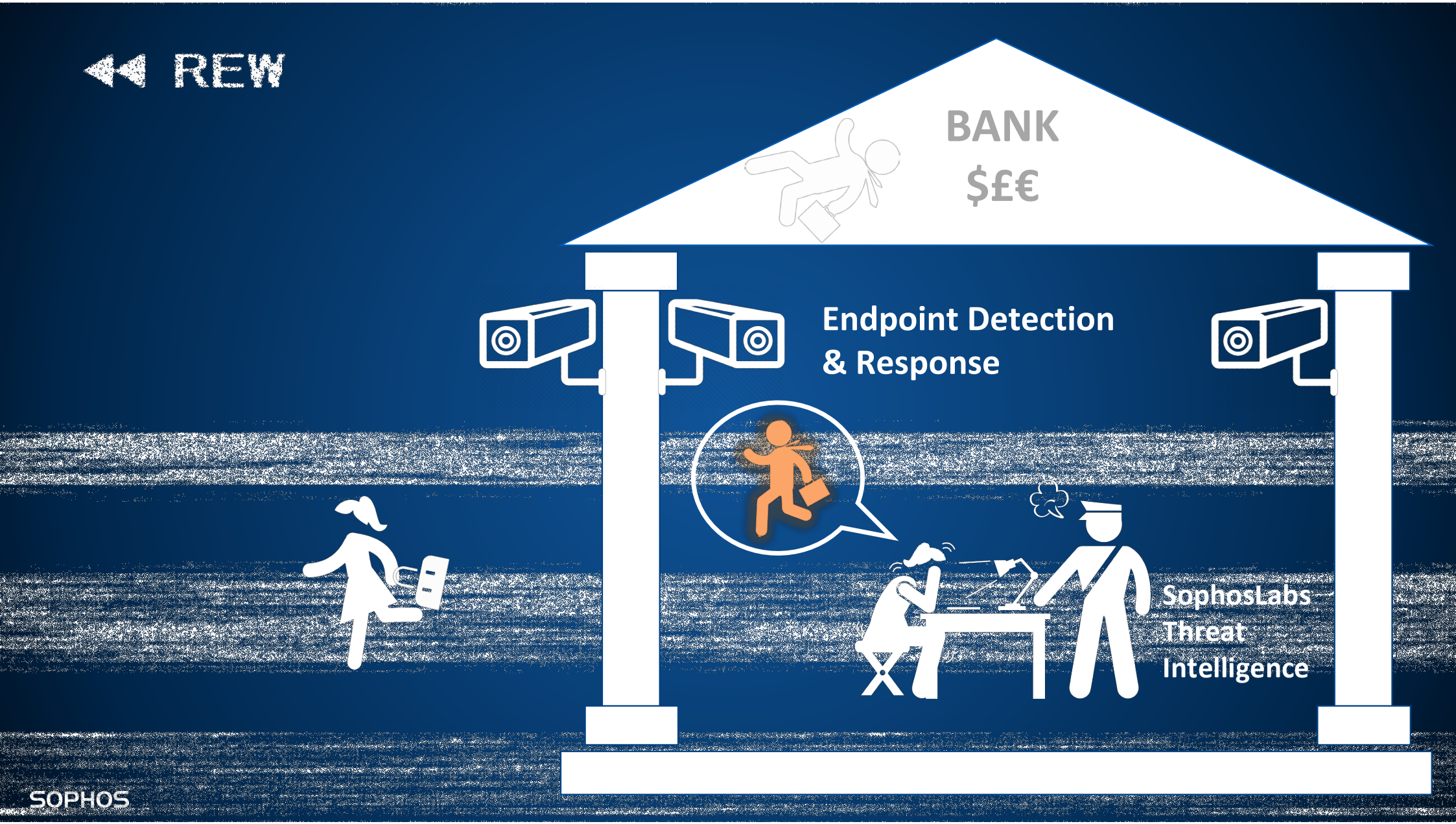
Konsequenz 4: Komponenten agieren als System

Synchronized Security

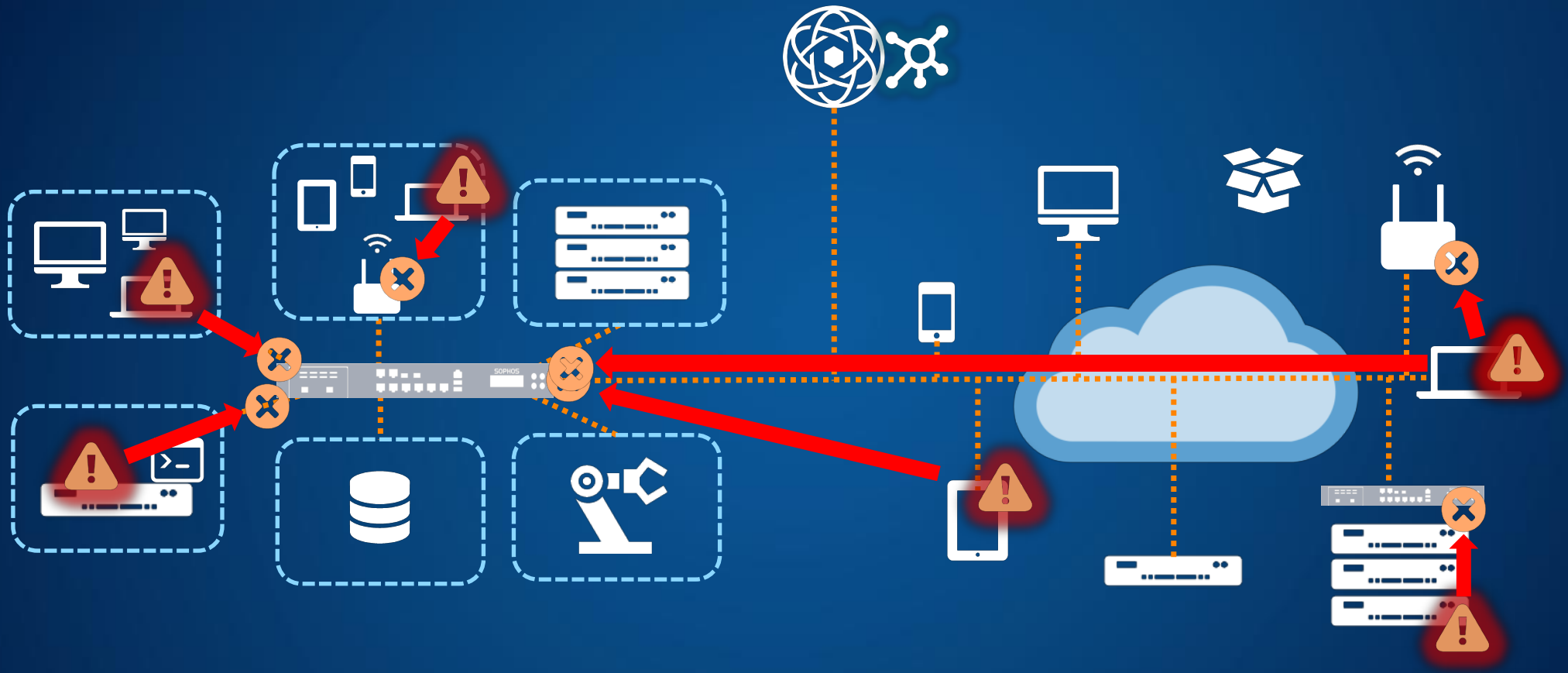
SOPHOS


BANK
$£€
Synchronized Security
Anti Virus
Deep Learning
Exploit Prevention
Verhaltens-Erkennung
GESUCHT!
Verdächtig!
Techniken!
Aktionen!
Vor der Ausführung
Nach der Ausführung
SOPHOS


BANK
$£€
Synchronized Security
SOPHOS

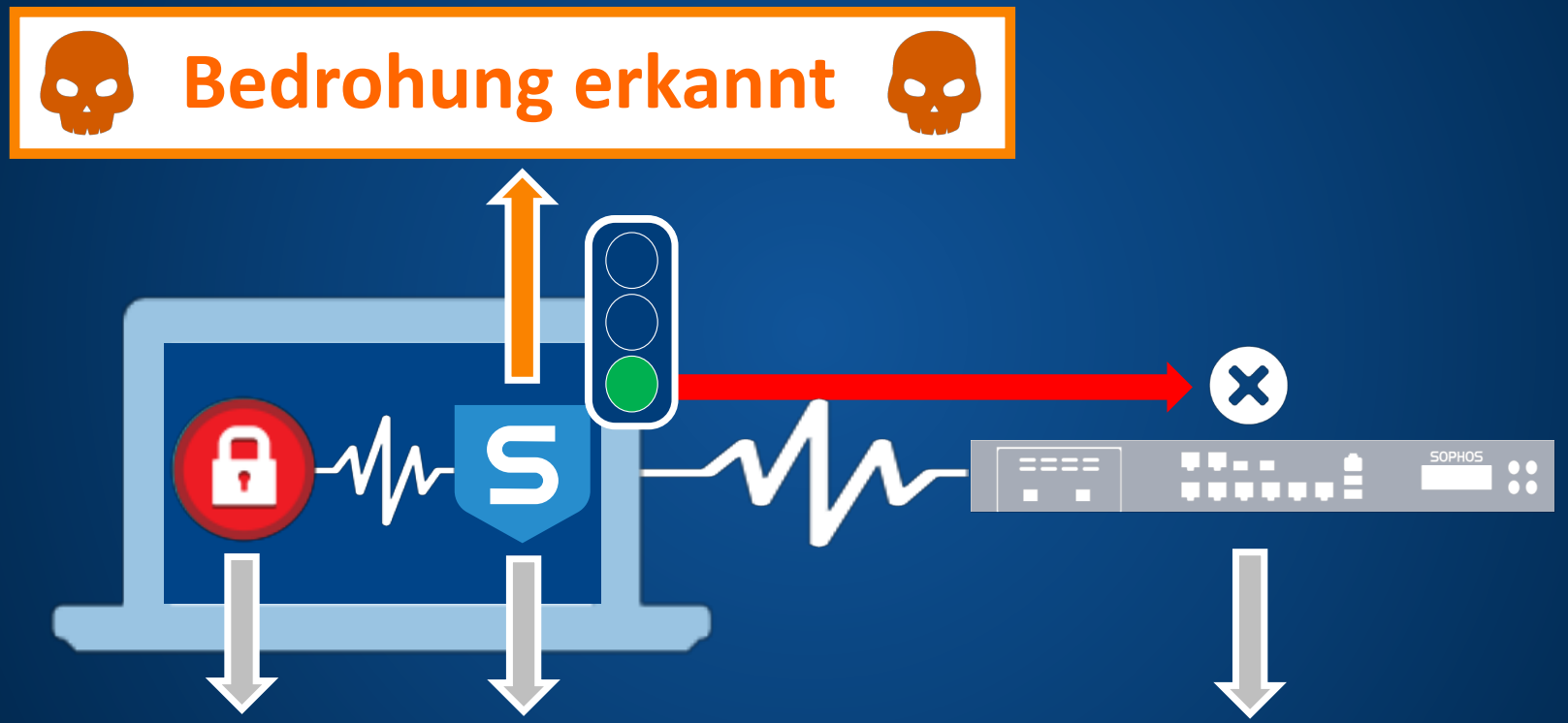

REW
BANK
$£€
Endpoint Detection
& Response
SophosLabs
Threat
Intelligence
SOPHOS

Komponenten agieren als System

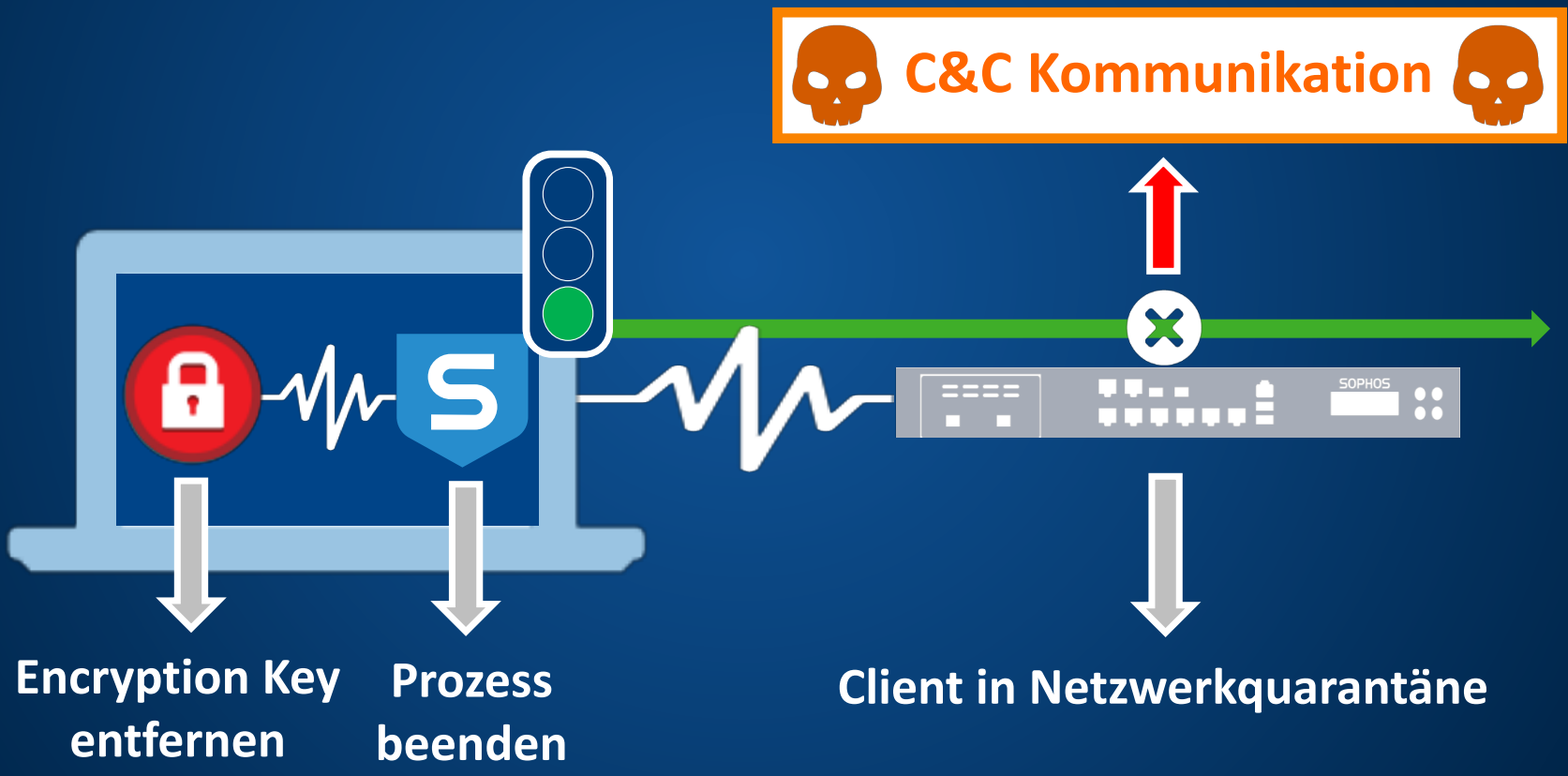


SOPHOS

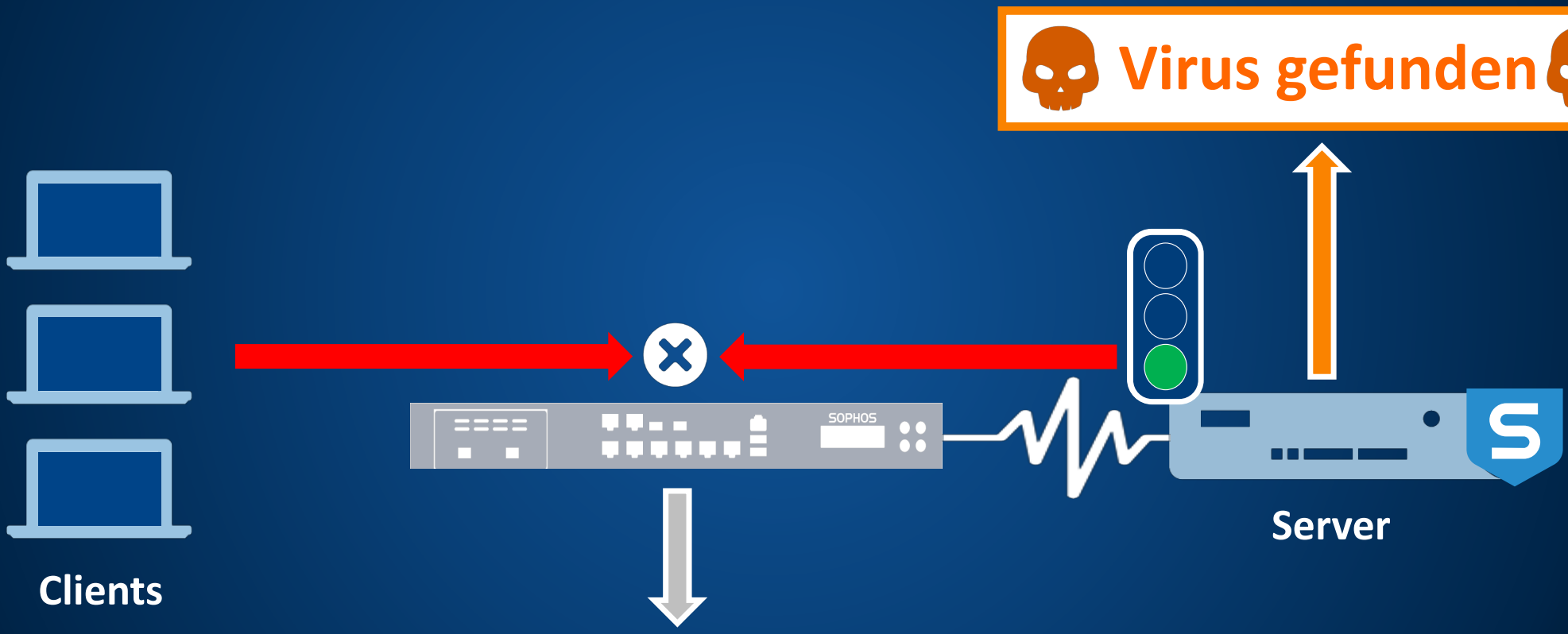
Security Heartbeat – Automatische Netzwerkquarantäne



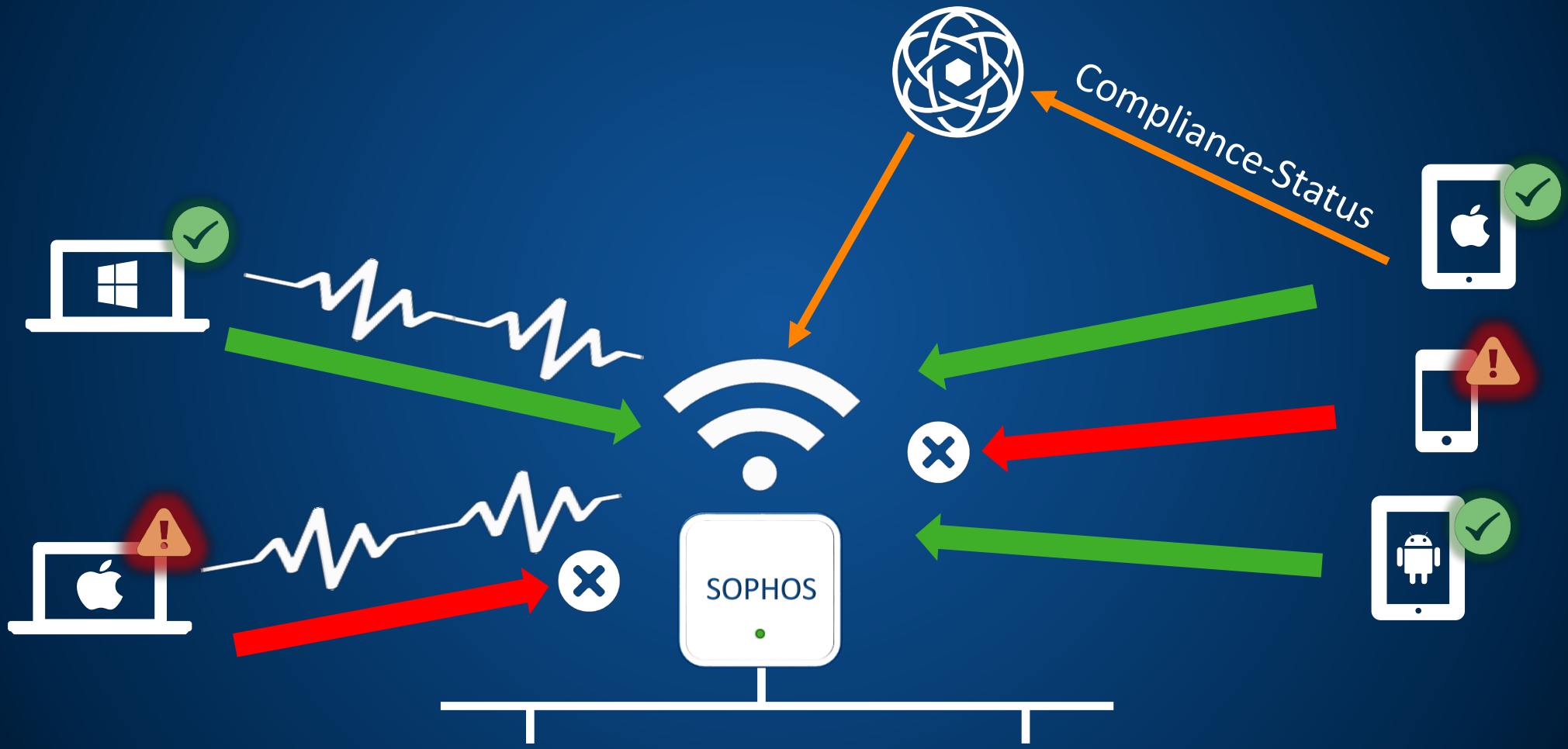
Security Heartbeat – Botnet C&C-Verkehr erkannt



Security Heartbeat – Server Heartbeat



Security Heartbeat – WLAN Access Point Enforcement



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

SOPHOS

SOPHOS INTERCEPT X Advanced

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

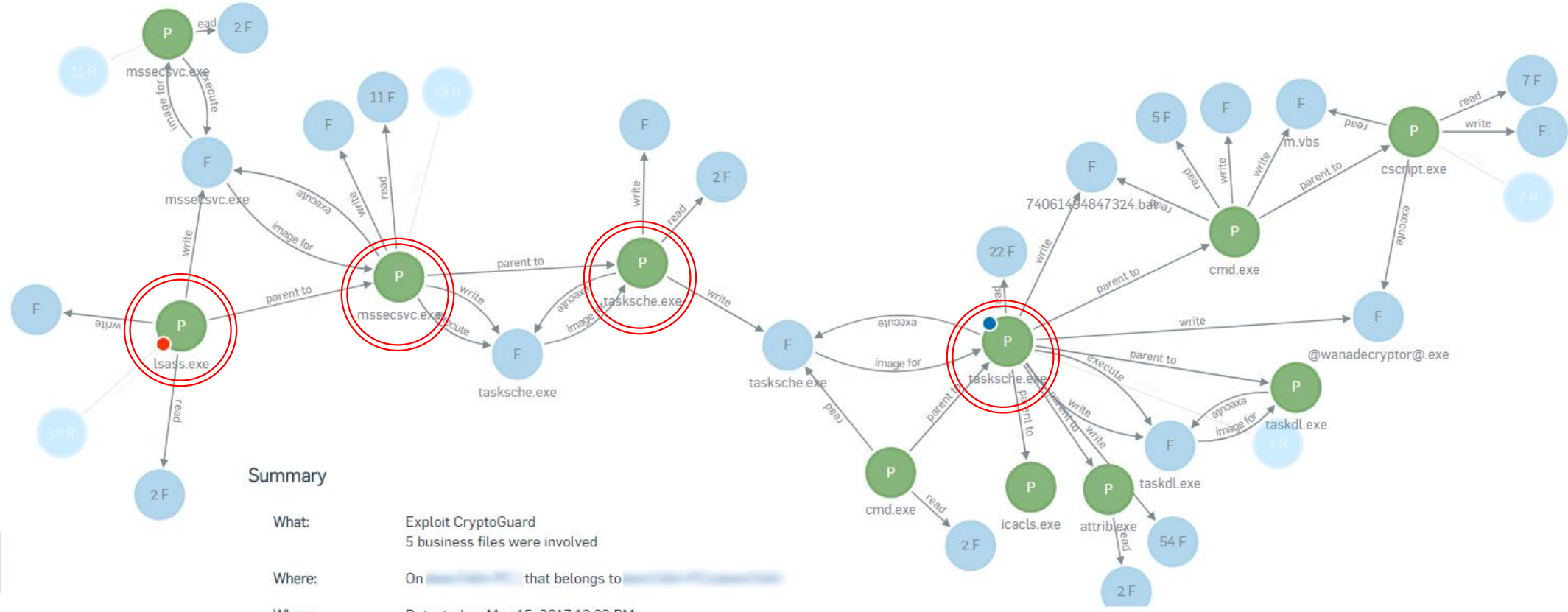
- Logging & Reporting
- Alarmierung
- Zentrales Management
- Ursachen-Analyse

Demo

https://vimeo.com/253967041/6bf44dc5ff

SOPHOS

Ursachenanalyse, Bsp. WannaCry



Synchronized Security – Teamplay statt Best-of-Breed

SOPHOS

“**No other company** is close to delivering this type of communication between endpoint and network security products.”

Chris Christianson, Vice President of Security Programs, **IDC**

Warum hat Sophos die beste Lösung am Markt?

- Sophos deckt die komplette Infektionskette
- Effektivste und umfangreichste Schutztechnologien am Markt!
- Ursachenanalyse von Infektions- und Verbreitungswegen
- Gesamte Unternehmenssicherheit in einer Oberfläche
- Mit Synchronized Security agieren Sophos Lösungen als System und reagieren bei Bedrohungen automatisch

SEE THE FUTURE

SOPHOS

Fragen?

michael.veit@sophos.de


SEE THE
FUTURE
SOPHOS