# 24/7 Schutz vor Cyberangriffen
## Ihr persönliches MDR-Service

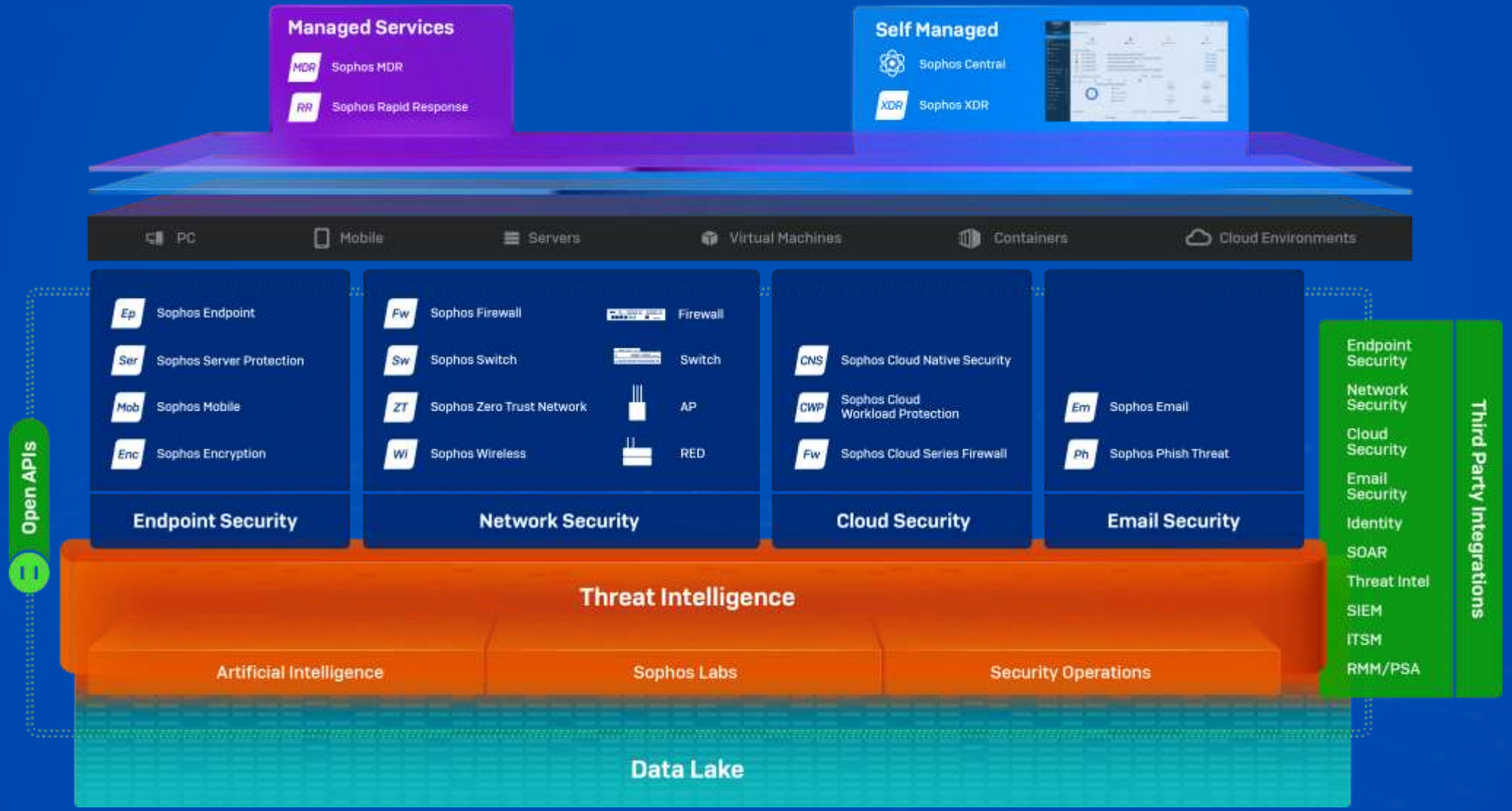
Wolfgang Lauer
Country Manager

Stefan VASIC
Enterprise Account Executive

**LSZ – Cybercrime Forum – 22. Juni 22**

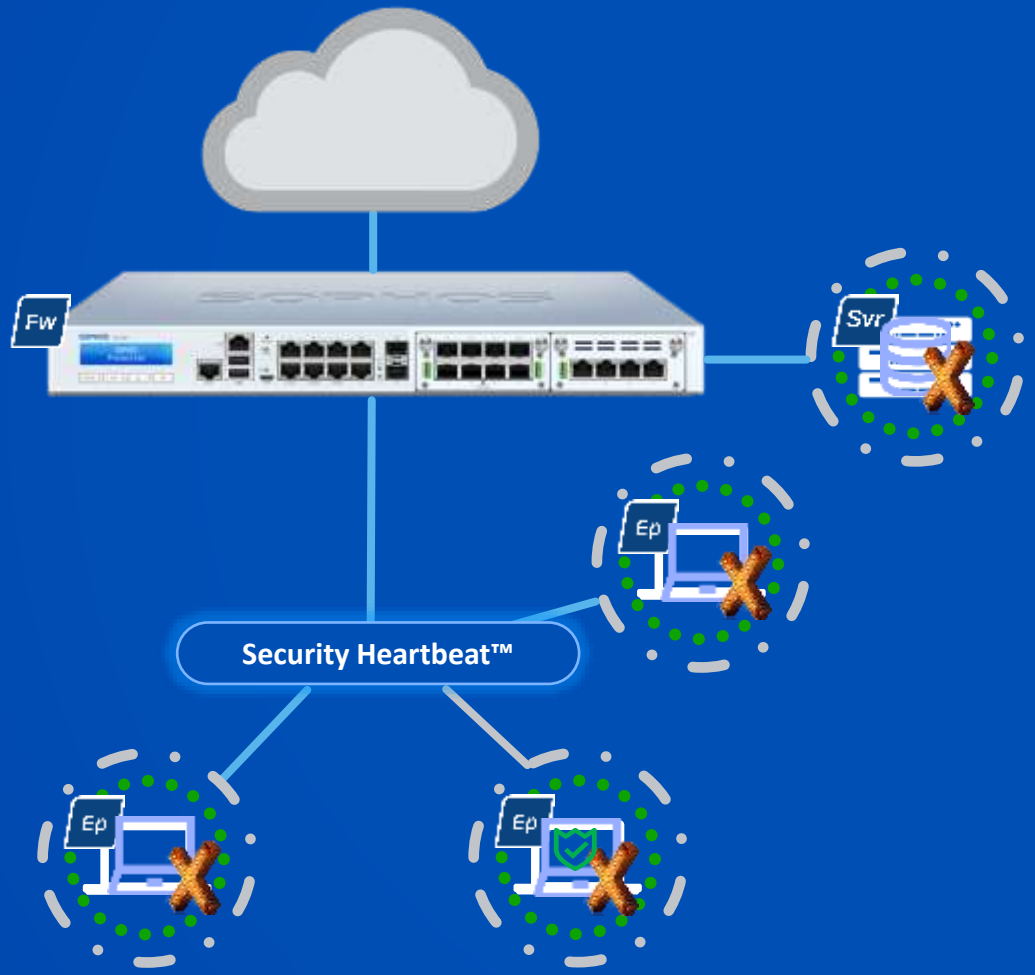
SOPHOS

# Adaptive Cybersecurity Ecosystem

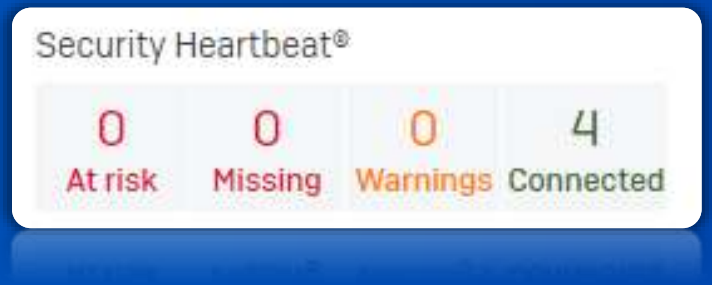



SOPHOS

# Sophos Syncronized Security

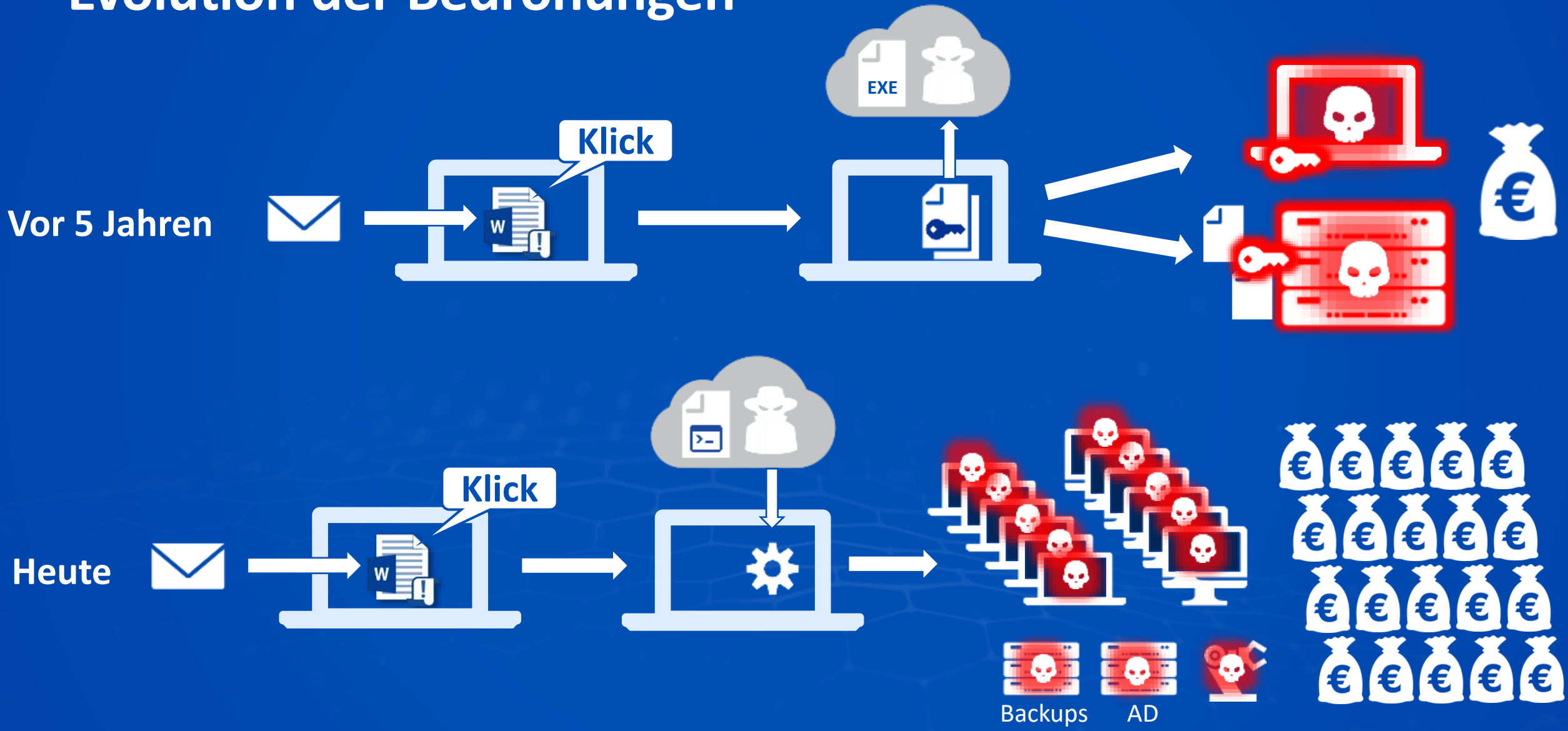



Schädlicher Prozess wird bereinigt




SOPHOS

# Evolution der Bedrohungen




SOPHOS


## Schutz

Web Control
Device Control
App Control
Firewall
Netzwerk IPS
Signaturen
Deep Learning
Heuristiken
Host IPS

## Erkennung

Exploit Prevention
Hacker-Techniken
Rechte-Ausweitung
Schutz vor Ransomware
Schutz vor Passwortdiebstahl
Botnet-Traffic-Erkennung
AMSI Speicheranalyse
KI-Bedrohungs-Suche

## Reaktion

Stoppen
Wiederherstellung
Synchronized Security
Eindämmung
Live-Sitzung
manuelle Isolation
Bereinigung
Ursachen-Analyse
Self-Isolation
Bedrohungs-Analyse
Bedrohungs-Suche

SOPHOS

# Angriffsindikatoren schnell und effizient erkennen

SOPHOS


Forensiker und Analysten onSite
Technische Expertise
Incident Response
…
7x24 SOC-Team

**SOPHOS**
**Managed Detection and Response**


# 20.000+ Kunden

SOPHOS

# Sophos MDR Advanced Funktionsumfang

- 24/7 indizienlose und indizienbasierende Bedrohungssuche Angriffserkennung
- Security Health Check
- Aktivitätsreports
- Dedizierter Ansprechpartner
- Direkter Telefon-Support
- Optimierte Telemetriedaten
- Proaktive Verbesserung des Sicherheitsstatus
- Asset-Erkennung

# Der Kunde wählt die beste Art und Weise, wie unser MTR Team mit Ihm zusammenarbeitet.


Das MTR Team benachrichtigt den Kunden über die Erkennung und stellt Details bereit, um Ihm bei der Priorisierung und Reaktion zu helfen.


Das MTR Team arbeitet mit dem Kunden oder externen Consultants eng zusammen, um auf die Erkennung optimal reagieren zu können.


Das MTR Team kümmert sich um die Eindämmungs- und Neutralisierungsmaßnahmen und informiert den Kunden über die ergriffenen Maßnahmen.

# Schnelligkeit ist wichtig – Service Level Targets

**24/7**
Team von Analysten

Durchschnittliche Zeit bis zur Erkennung
**~2 Minuten**

Durchschnittliche Zeit bis zur Erstreaktion
**~20 Minuten**

Durchschnittliche Zeit bis zur Behebung
**~60 Minuten**

Internal MDR Ops Maßnahmen

# Sophos MDR Advanced Service

## inclusive Incident Response

**Blitzschnelle Unterstützung bei aktiven Bedrohungen durch ein weltweites Expertenteam von Spezialisten**

SOPHOS

SOPHOS

Cybersecurity delivered.