IT-Sicherheit rund um die Uhr mit SOPHOS und Raab IT

Managed Detection and Response als Schutz vor der aktuellem akuten Cyberbedrohung

Christian Theilen

SOPHOS

IT-Security ist gleich

Endlos-Schleife

- Immer Endspiel
- 24/7
- Unbekante Gegner
- Viele Gegner
- Eigentore!
- Kein Schiedsrichter
- Keine Regeln (für die Gegner)

- Spiel MUSS :0 stehen: immer

Cybervorfall :1 = Spielende, Saisonende, Abstieg, Strafzahlung …

tagesschau

Sendung verpasst?

Startseite ▸ Inland ▸ Regional ▸ Baden-Württemberg ▸ Baden-Württemberg: Ellwangen: Cyberattacke auf Batteriehersteller VARTA

Baden-Württemberg

Ellwangen: Cyberattacke auf Batterieherstel-ler VARTA

Stand: 13.02.2024 18:50 Uhr

Von der Cyberattacke auf Teile der IT-Systeme bei VARTA sind laut Unternehmen fünf Standorte betroffen. Der Batteriehersteller hat die Produktion vorsorglich heruntergefahren.

Am Montag haben Cyberkriminelle IT-Systeme beim Batteriehersteller VARTA angegriffen. Wie das Unternehmen mit Sitz in Ellwangen am Dienstag mitteilte, sind fünf Standorte betroffen. Der Batteriehersteller hat die IT-Systeme und damit auch die Produktion vorsorglich und aus Sicherheitsgründen heruntergefahren und vom Internet getrennt.

SOPHOS

SOPHOS Adaptive Cybersecurity Ecosystem

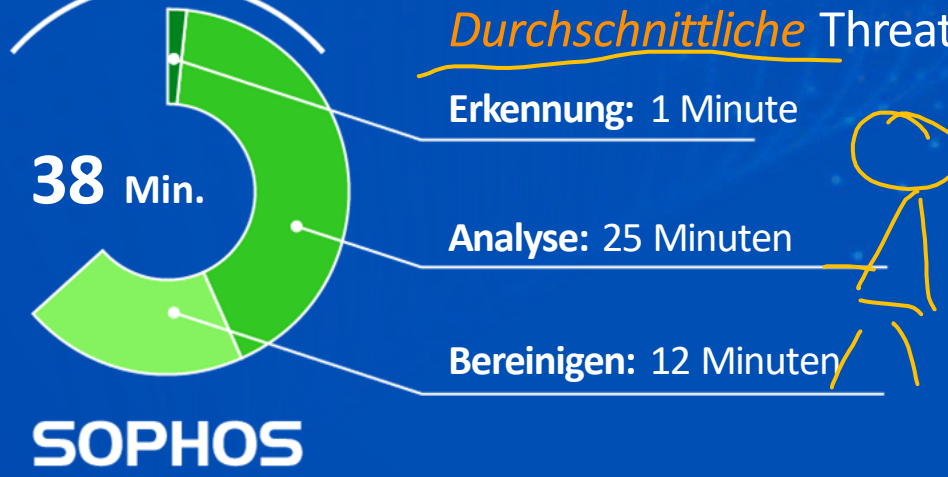
SOPHOS

Führende Erkennungs- und Reaktionszeiten

99,98%
Automatisch von Sophos blockierte Bedrohungen

Zeit bis zum Abschluss eines Vorfalls (interne SOC-Teams)

Minimum	Median	Maximum
3,7 Stunden	**16** Stunden	**30** Stunden



Durchschnittliche Threat-Reaktionszeit von Sophos MDR

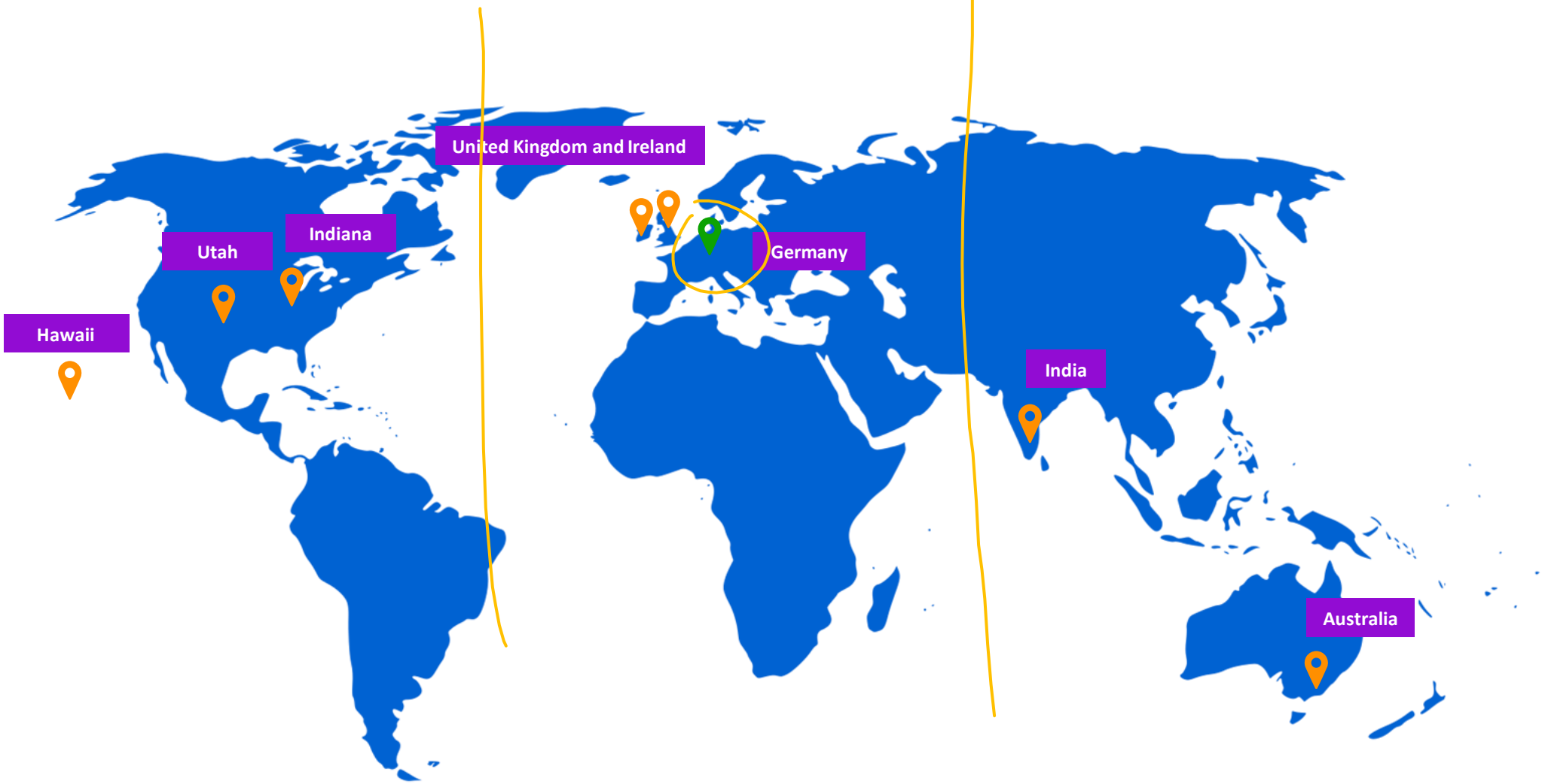
Erkennung: 1 Minute

Analyse: 25 Minuten

Bereinigen: 12 Minuten

SLA: 60 Minuten

24x7 Coverage from Six Global SOCs



SOPHOS

Sabotage

Business Case: Admin eines Kunden möchte seine Präsentation für IT-Sicherheit mit Screenshots von echten Darknet-Sites anreichern

Install TOR Browser via valid Admin-Account

Mittwoch, 27 April 2022, 21.OO Uhr

Search for hacked .de offerings

21.15 Uhr

Get called by MDR-ops

21.20 Uhr

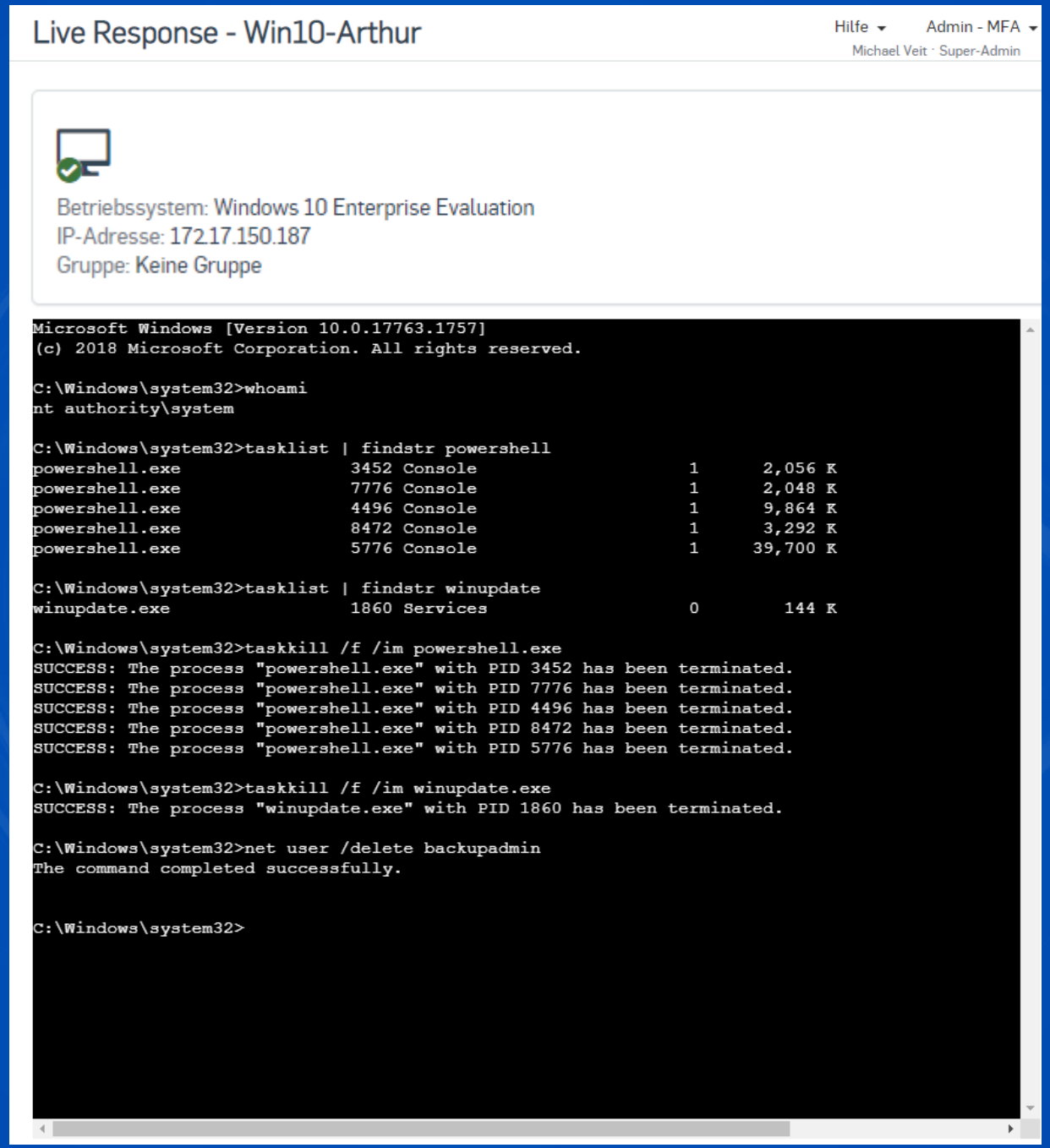
If no response MDR operator was already on device

21.22 Uhr

Close case as „false positive“

21.30 Uhr

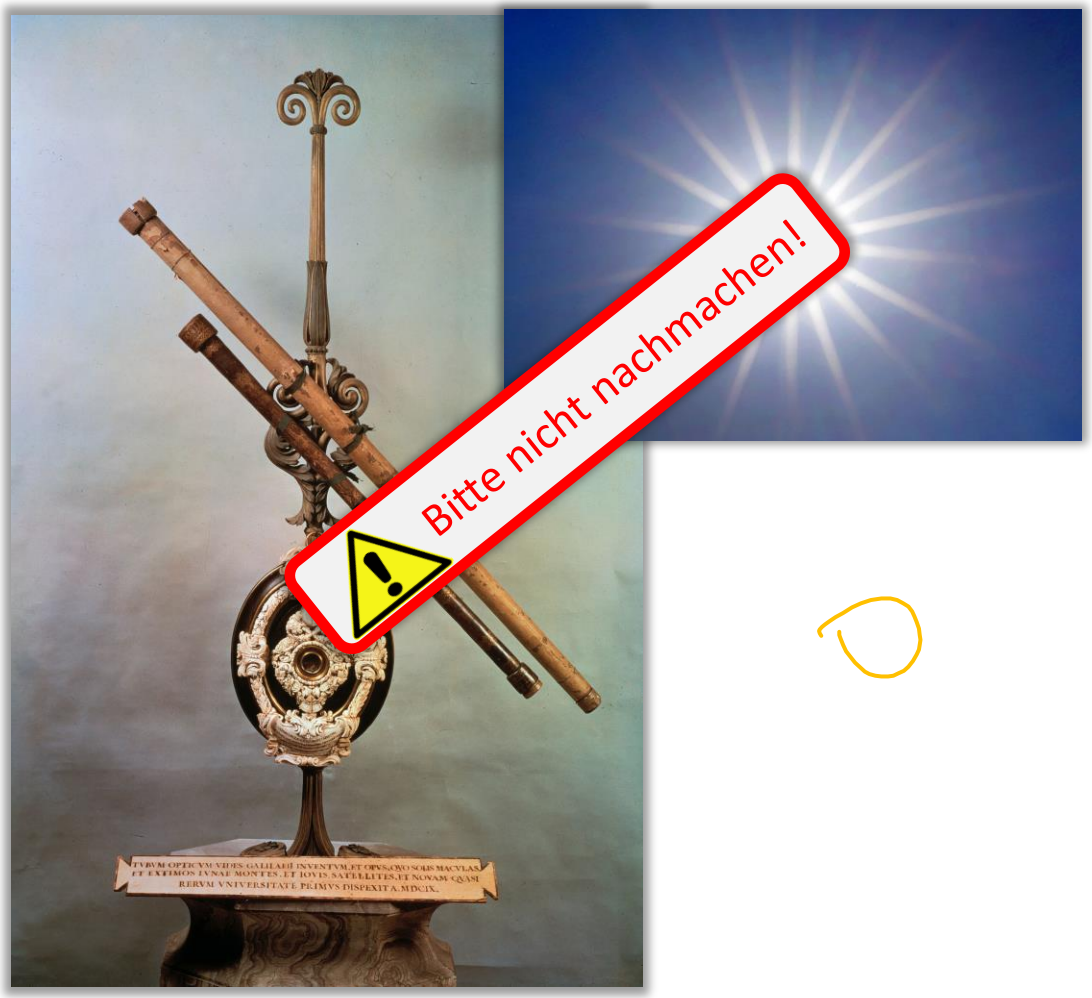
LiveResponse

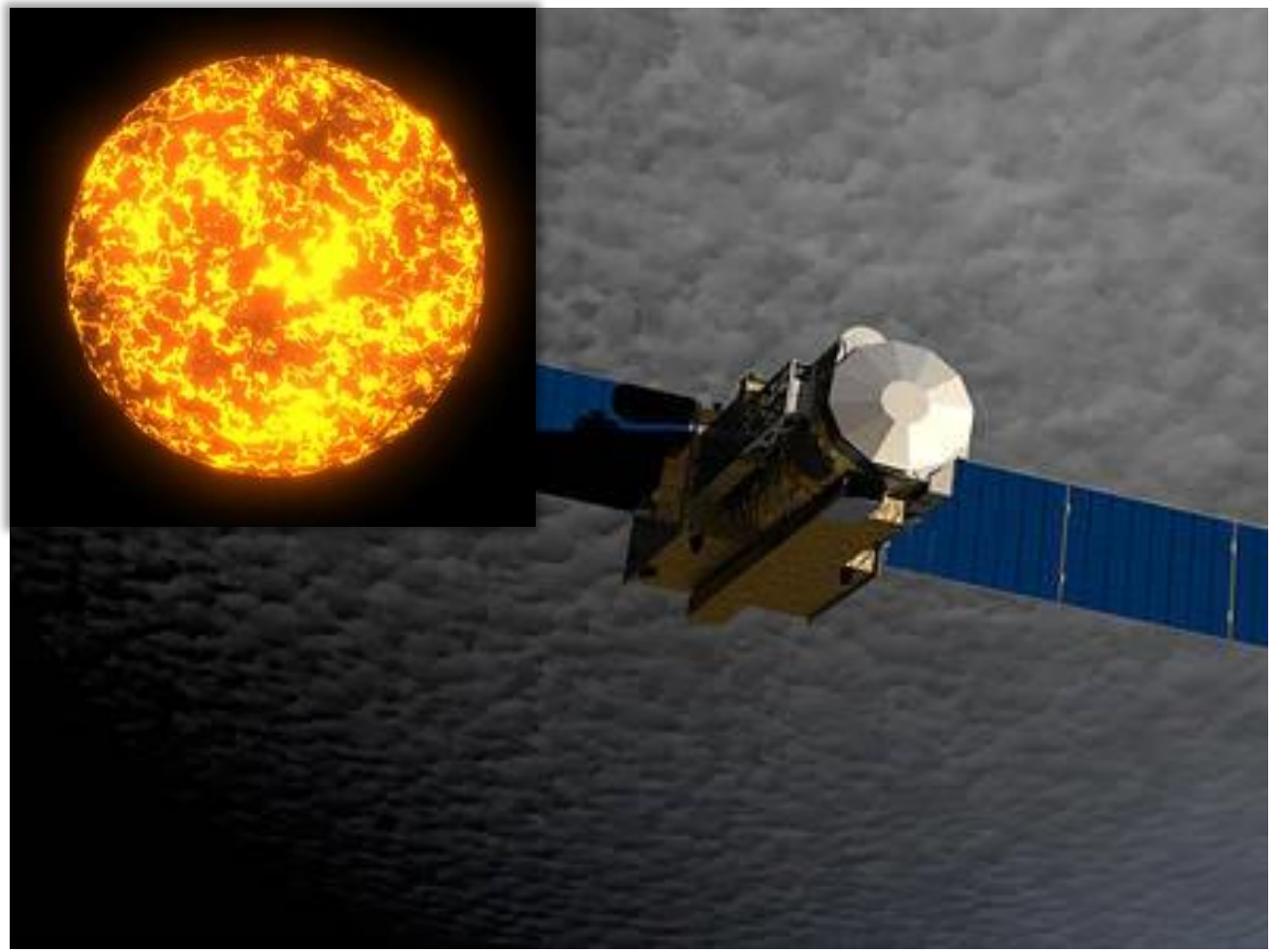


Das ist alter
“Stand derTechnik”

NEW:aktueller Stand
der Technik

Die Evolution der Sichtbarkeit





Network Detection and Response

Netzwerkteilnehmer ohne MDR-Agent (kein Win, MacOS oder Linux)

VM/hyper-v mit NDR sammelt Netzwerk-Telemetrie an Mirrorport

Cobalt Strike

Sophos DataLake wertet NDR Telemetrie aus

SOPHOS

Sophos auf einen Blick

$1.1+ billion
FY23 Billings

600,000+
Total customers

126%
Customer Renewal Rate

60,000+
Channel Partners

100+
Strategic Partners
(Technology, services, etc.)

20,000+
Sophos MDR Customers

300,000+
Sophos Endpoint Customers

40,000+
Sophos XDR Customers

250,000+
Sophos Firewall Customers

18,000+
Sophos Email Customers

The **largest provider** of Managed Detection and Response Services (MDR)

The only vendor named **Gartner Customers' Choice** for EPP, Firewall, MDR, and Mobile

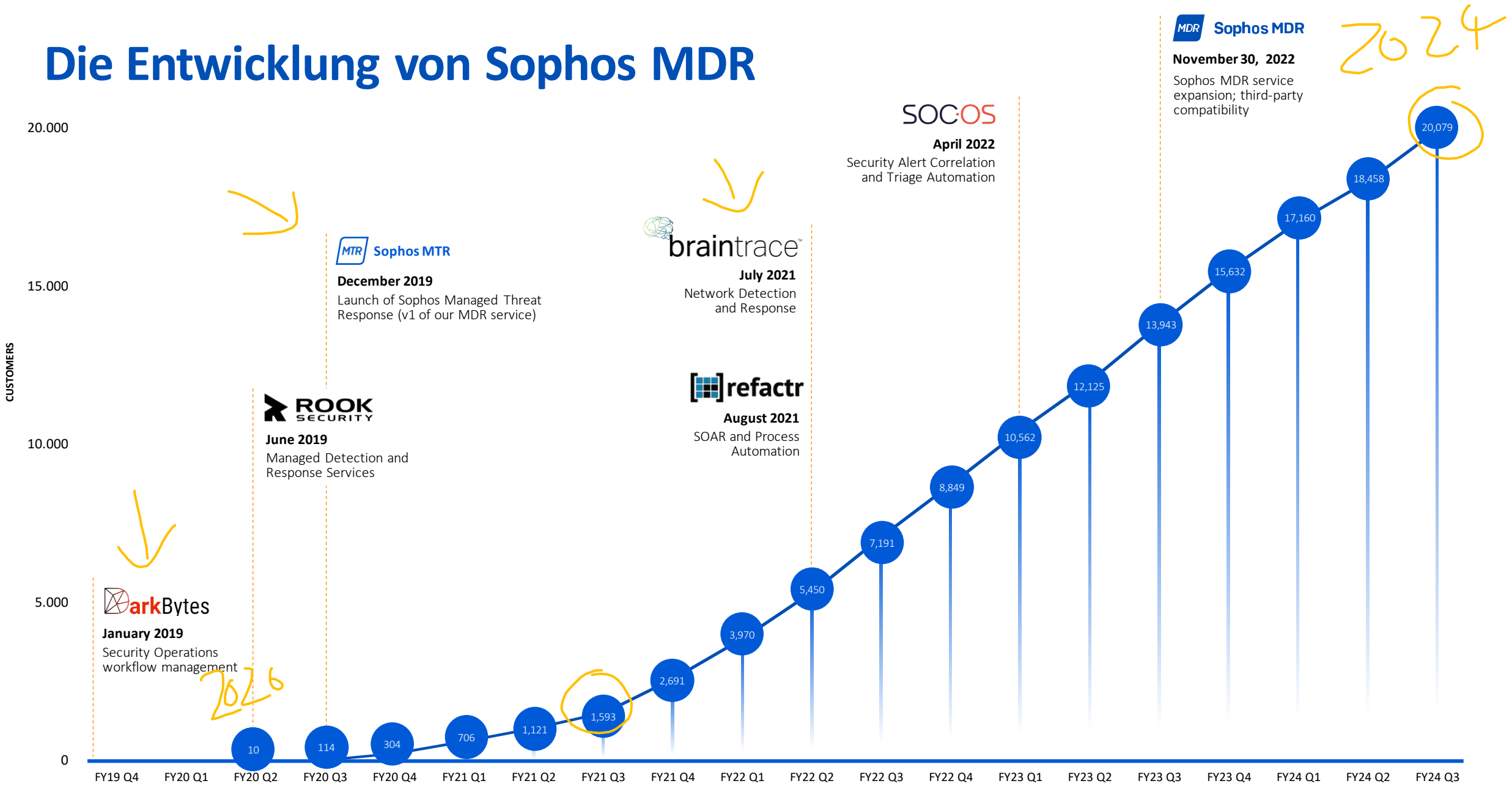
A **14-time Leader** in the Gartner Magic Quadrant for Endpoint Protection Platforms

Industry-leading **compatibility** with virtually any environment or tech stack

The most expansive portfolio of world-class products and managed security services

SOPHOS ist 27001:2022 zertifiziert

Die Entwicklung von Sophos MDR



SOPHOS

Bei 75 % der Ransomware-Angriffe konnten Hacker die Backup-Repositorys angreifen

Veeam 2023 Ransomware Trends Report

Visibility Across All Key Attack Surfaces

MDR

SOPHOS
✓ Integrations included

- Ep Endpoint
- WP Workload
- Mob Mobile
- Cld Cloud
- Fw Firewall
- Em Email
- ZT ZTNA
- NDR Network

Endpoint
✓ Included

Microsoft · CROWDSTRIKE · SentinelOne · TREND MICRO · Symantec by Broadcom (beta) · BlackBerry CYLANCE (beta)

+ Others with Sophos XDR Sensor agent

Firewall

paloalto NETWORKS · FORTINET · CHECK POINT · CISCO Meraki · SONICWALL · WatchGuard

Network

DARKTRACE · THINKST CANARY · Secutec · Skyhigh Security

Email

Microsoft 365
✓ Included

Google Workspace
✓ Included

mimecast · proofpoint.

Productivity
✓ Included

Microsoft 365

Google Workspace

NEU

Cloud

orca security · aws · Azure · Google Cloud

Identity

Microsoft
✓ Included

okta · auth0 · CISCO DUO · ManageEngine

Backup and Recovery

veeam

NEU

Sophos Endpoint and Sophos Workload Protection solutions are included with Sophos XDR and MDR. Other Sophos product integrations require a subscription to the applicable solution.

Third-party Endpoint, Microsoft, and Google Workspace integrations are included with Sophos XDR and MDR subscriptions at no additional charge. Integration Packs for other non-Sophos solutions are available as add-on subscriptions for each integration category. Licensing is based on the total number of users and servers.

Updated: January 11, 2024

Included Integrations

Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and third-party integrations.

Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm.

Microsoft Security Suite

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Microsoft Entra ID
- Microsoft Defender for Cloud Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365 IAM

Sophos Endpoint Protection

Endpoint Prevention and EDR that stop advanced threats and detect malicious behaviors—including attackers mimicking legitimate users.

Sophos Network Detection and Response

Continuously monitor activity inside your network to detect suspicious actions and lateral attacker movement.

Google Security Suite

- Google System Defined Rules
- Suspicious Activities
- Malware and Phishing
- User and Device Activity
- Alert Center
- Authentication
- Access Control
- Data Control

Sophos Cloud

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform.

Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks.

Third-Party Endpoint Protection

Compatible with...

- Microsoft
- CrowdStrike
- SentinelOne
- Symantec (Broadcom)
- Trend Micro
- BlackBerry (Cylance)

+ Other solutions with Sophos XDR Sensor agent

Includes 90 days of data retention

Add-On Integrations

Firewall

Compatible with...

- Check Point
- Cisco
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard

Identity

Compatible with...

- Auth0
- Duo
- ManageEngine
- Okta

Microsoft integration included

Cloud

Compatible with...

- Orca Security

AWS, Azure and GCP integrations available via Sophos Cloud product

Network Security

Compatible with...

- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary

Email

Compatible with...

- Mimecast
- Proofpoint

Microsoft 365 and Google Workspace integrations included

Backup and Recovery

Compatible with...

- Veeam

Add-on Integration Packs and the Data Retention Pack are available for Sophos MDR and Sophos XDR
All Integration Packs are licensed based on the total number of Sophos MDR/XDR seats (users+servers)

1-Year
Data Retention

Die Sophos Breach Protection Warranty deckt Kosten in Höhe von bis zu 1 Mio. US-Dollar für Reaktionsmaßnahmen ab.*

Ohne Aufpreis enthalten in den neuen jährlichen Subscriptions (Laufzeit-Lizenzen) von **Sophos MDR Complete**

Automatisch enthalten in **Lizenzen mit Laufzeiten von 1, 2 und 3 Jahren und MSP**, sowohl für Neu- als auch Renewal-Kunden

Umfassende Abdeckung: Endpoints, Server, Windows, macOS, keine geografischen Beschränkungen

** Im Falle von Unstimmigkeiten zwischen der englischsprachigen Version und der deutschen Übersetzung der Bedingungen der Sophos Breach Protection Warranty gelten die in englischer Sprache verfassten Bedingungen.*

Die vollständigen Bedingungen finden Sie unter www.sophos.de/legal.

SOPHOS

Sophos Breach Protection Warranty

Die Warranty erstattet Kosten in Höhe von bis zu 1 Mio. US-Dollar für Reaktionsmaßnahmen auf einen Ransomware-Vorfall in Umgebungen, die durch Sophos MDR Complete geschützt sind.

Einfaches Modell

Die Warranty ist …

- automatisch beim Kauf von „Sophos MDR Complete“-Laufzeit-Lizenzen enthalten
- in allen Ländern verfügbar, in denen Sophos tätig ist*
- nicht in Stufen unterteilt, die die Abdeckung einschränken
- ohne den Kauf zusätzlicher Lizenzen wirksam

Umfassender Schutz

Die Warranty schützt …

- Geräte mit Windows und macOS
- Endpoints und Server
- Subscription-Lizenzen 1, 2 und 3 Jahre oder MSP
- Neu- und Renewal-Kunden

Hohe Abdeckung

Die Warranty übernimmt …

- bis zu 1.000 US$ pro kompromittiertem System
- Gesamtkosten für Reaktionsmaßnahmen in Höhe von bis zu 1 Mio. US$
- bis zu 100.000 US$ Lösegeld (als Teil des Limits pro Gerät)
- diverse Ausgaben, darunter Kosten für die Anzeige des Datenschutzverstoßes, PR-, Rechts- und Compliance-Kosten

** Embargoländer ausgenommen*

Weitere Angaben und Bedingungen finden Sie unter www.sophos.de/legal.

SOPHOS

Cybersecurity delivered.