Managed Detection and Response

Erkennung und Abwehr von Cyberangriffen im Fullservice

Markus GRÖLLER
Senior Sales Engineer

Kategorien der Threat Akteure

Skript Kiddies

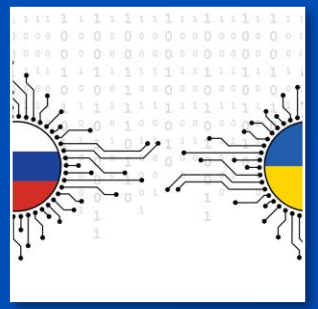
Insider

organisatorisches Verbrechen

Wettbewerber

Hacktivist

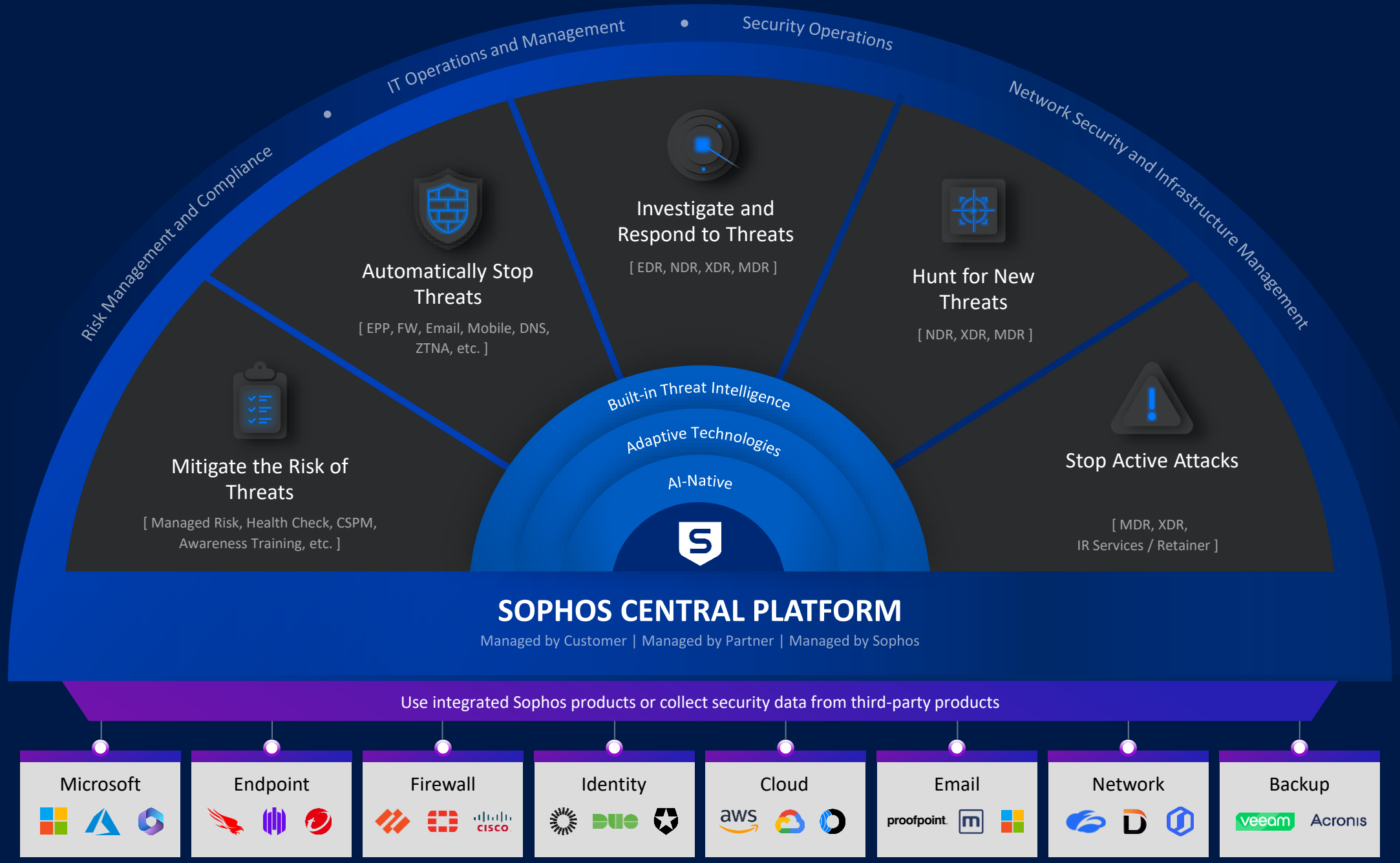
nationale Staaten (APTs)



Wieso werden Organisationen gehackt?

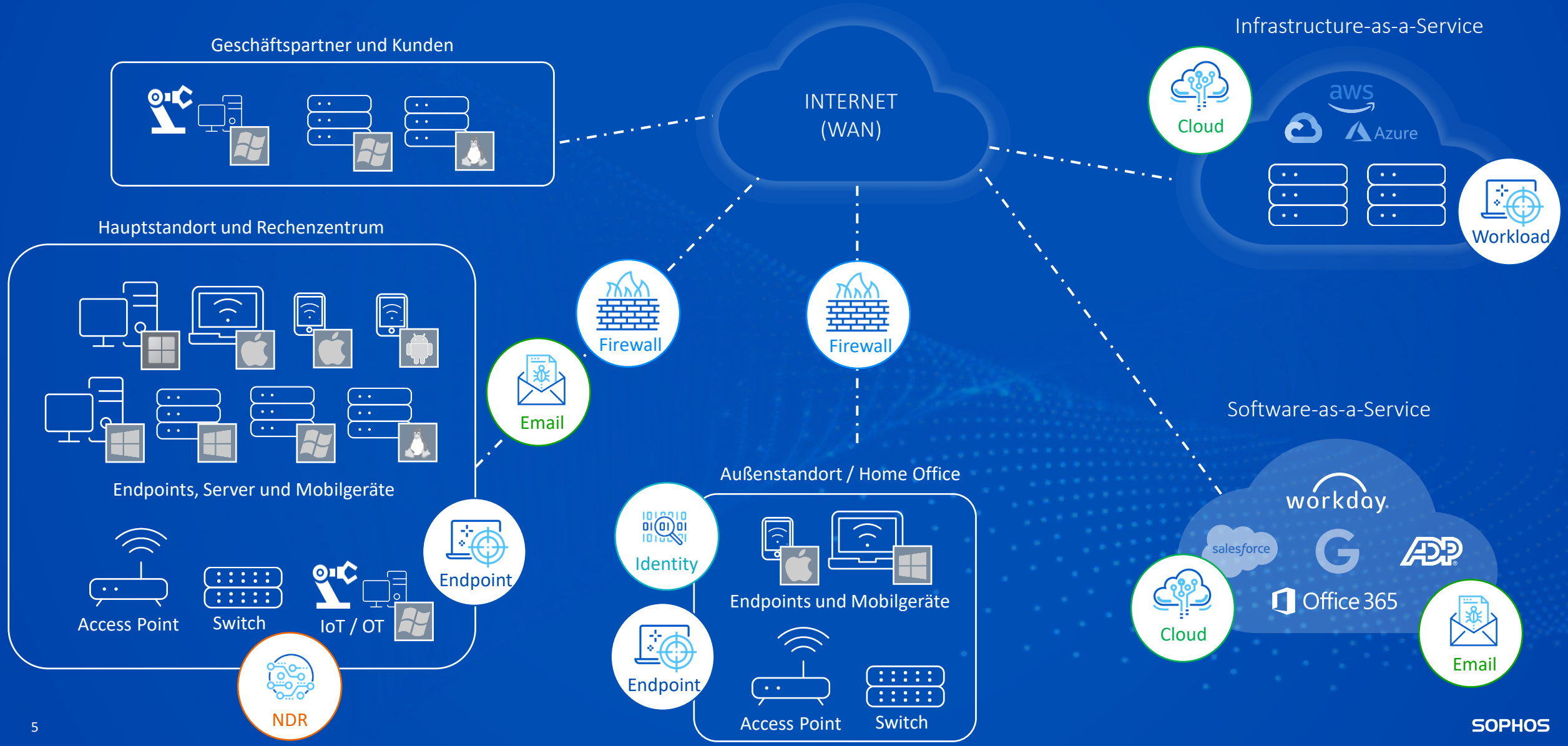
Flughafen Leipzig im Mai 2024

Mainstream Support Ende 2011
Extended Support Ende 2016


IT Operations and Management
Security Operations
Risk Management and Compliance
Network Security and Infrastructure Management
Automatically Stop Threats
[EPP, FW, Email, Mobile, DNS, ZTNA, etc.]
Investigate and Respond to Threats
[EDR, NDR, XDR, MDR]
Hunt for New Threats
[NDR, XDR, MDR]
Mitigate the Risk of Threats
[Managed Risk, Health Check, CSPM, Awareness Training, etc.]
Stop Active Attacks
[MDR, XDR, IR Services / Retainer]
Built-in Threat Intelligence
Adaptive Technologies
AI-Native
SOPHOS CENTRAL PLATFORM
Managed by Customer | Managed by Partner | Managed by Sophos
Use integrated Sophos products or collect security data from third-party products
Microsoft
Endpoint
Firewall
Identity
Cloud
Email
Network
Backup
proofpoint
veeam
Acronis

SOPHOS

IT-Sicherheitskonzepte von heute



SOPHOS

Warum benötigt man nochmal Telemetriedaten?

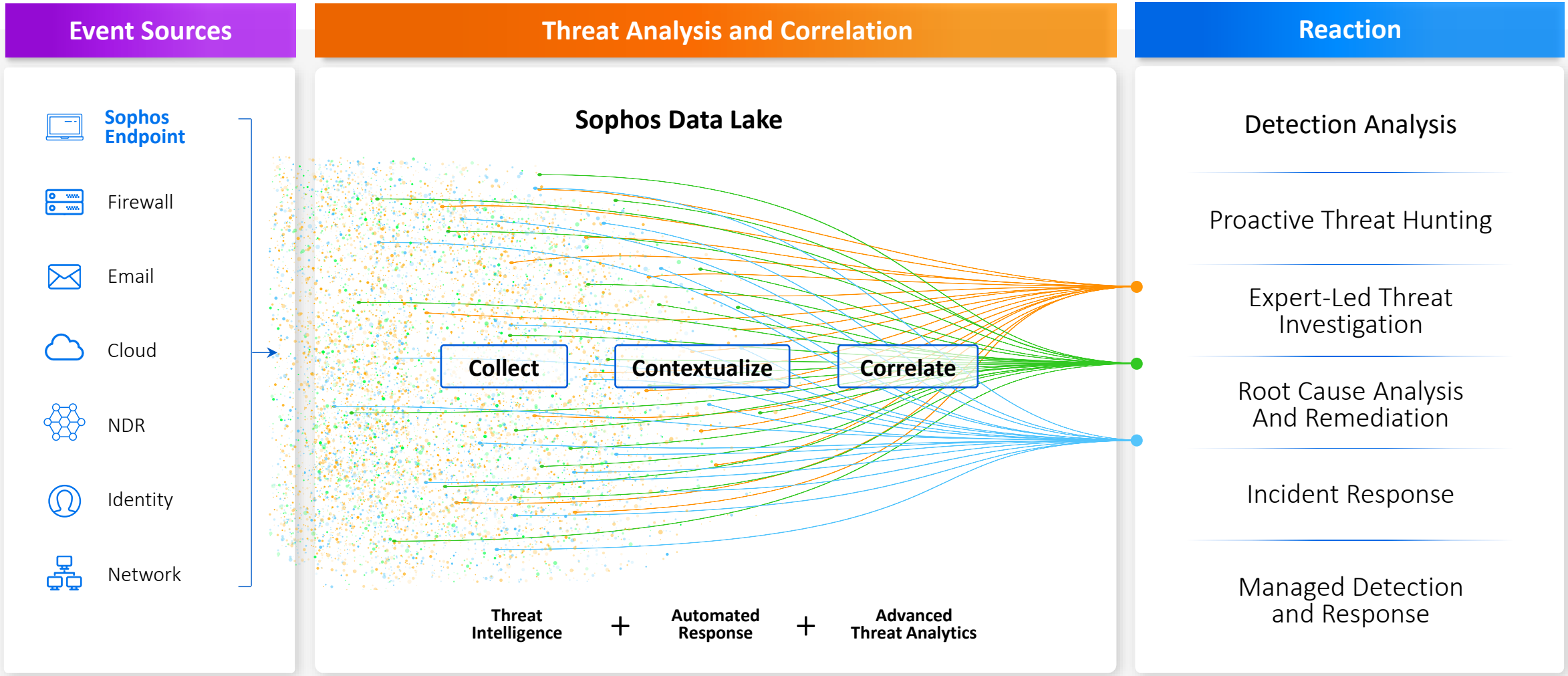
… und das ist nur der Heimgebrauch

SOPHOS

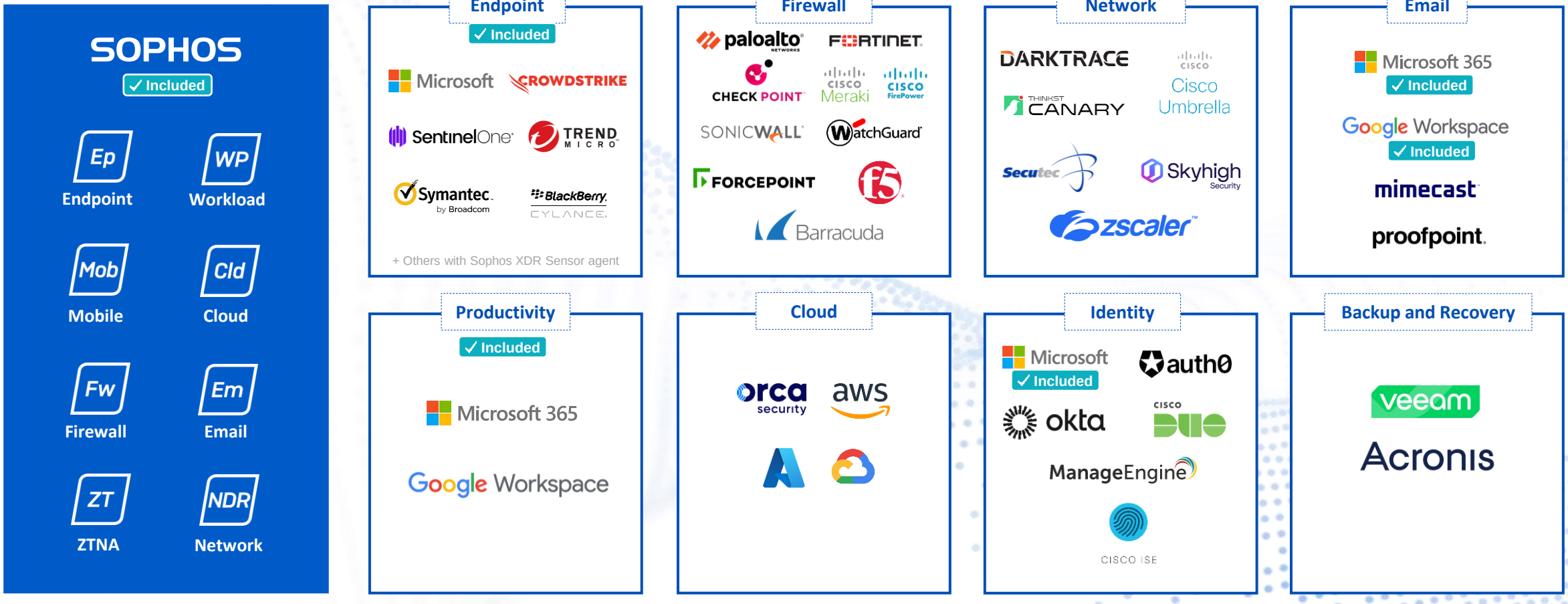
Telemetriesammlung bei den Spezialisten

SOPHOS

Sophos Data Lake



Plattform und Herstellerübergreifende Visibilität



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.

3.4 Millionen

Der weltweite Mangel an Cybersicherheits Praktiker, die derzeit gesucht werden

(ISC)², 2022 Cybersecurity Workforce Study

71%

der Sicherheitsteams haben mit zu vielen Warnungen ihrer Tools zu kämpfen

Sophos, The State of Cybersecurity 2023

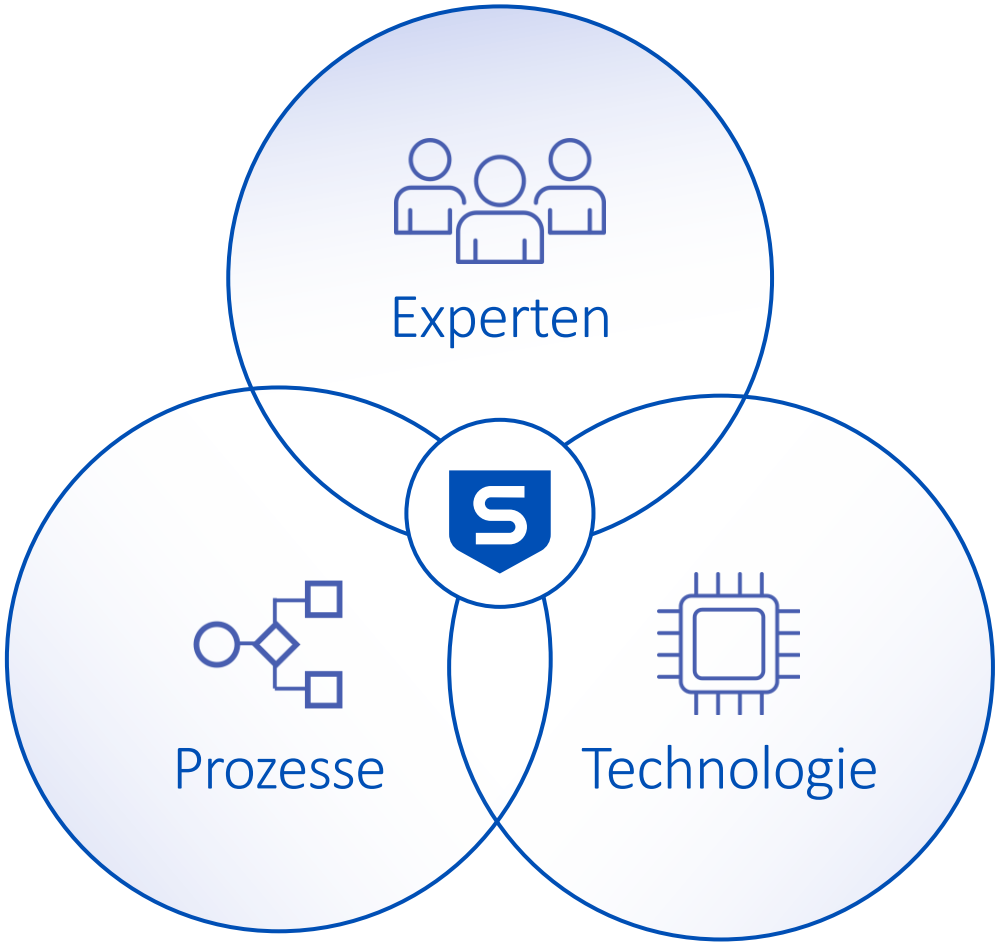
16 Stunden

Durchschnittliche Reaktionszeit auf Bedrohungen für Organisationen mit dedizierten Sicherheitsteams

Gartner, Cybersecurity Business Value Benchmark database

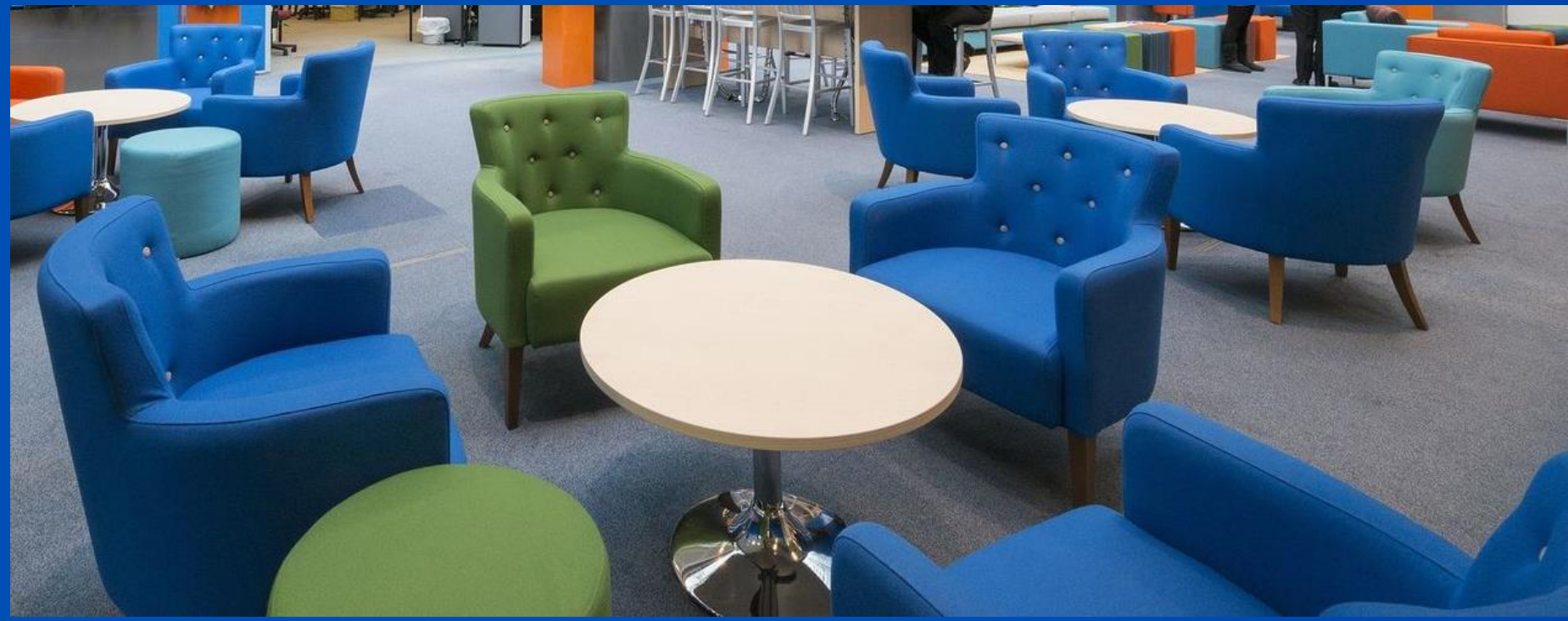
Managed SOC per Definition

SOPHOS MDR - Cybersecurity as a Service



- Proaktive Bedrohungssuche
- 24/7 Erkennung und Reaktion durch Analysten
- Vollständige Ursachenanalyse + Incident Response
- Mehr als 23.000 MDR Kunden
- Telemetrie von mehr als 600.000 Unternehmenskunden
- All-inclusive Service – keine versteckten Kosten
- Bestmögliches Ergebnis für Ihre IT-Sicherheit

Ihr nächster Schritt …



14:20 – 15:10 Round Table 4

SOPHOS