KHZG-Erfahrungsberichte

Martin Weiß
Senior Sales Engineer Public

SOPHOS

Krankenhauszukunftsgesetz (KHZG/KHZF)

- Fördertatbestand 10 – IT Sicherheit

Verbesserung der IT- bzw. Cybersicherheit
in Krankenhäuser (Non-Kritis) & Hochschulkliniken

(§ 19 KHSFV Absatz 1 Satz 1 Nr. 10 KHSFV)

Krankenhauszukunftsgesetz (KHZG/KHZF)

- Förderfähige Vorhaben zur Verbesserung der IT- bzw. Cybersicherheit – Fördertatbestand 10

Prävention vor Informationssicherheits-Vorfällen

- Systeme zur Zonierung von Netzwerken
- Next Generation Firewalls
- MicroVirtualisierung/Sandbox-Systeme
- Schnittstellen-Kontrolle
- Intrusion Prevention Systeme
- VPN-Systeme
- verschlüsselte Datenübertragung
- Network Access Control
- verschlüsselte mobile Datenträger
- sichere Authentisierungssysteme
- Softwareversionsmanagement
- Datenschleusen
- Datendioden
- ISMS
- Schwachstellenscanner

Krankenhauszukunftsgesetz (KHZG/KHZF)

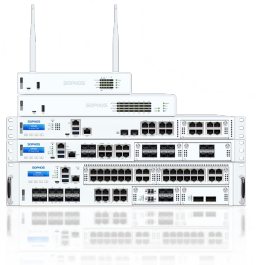
- Förderfähige Vorhaben zur Verbesserung der IT- bzw. Cybersicherheit – Fördertatbestand 10

Detektion von Informationssicherheits-Vorfällen

- Security Operation Center
- Intrusion Detection Systeme
- lokaler Schadsoftwareschutz mit zentraler Steuerung
- Schadsoftwareschutz in Mailsystemen bzw. bei Mailtransport
- Security Information Event Management Systeme
- Log Management Systeme

Krankenhauszukunftsgesetz (KHZG/KHZF)

- Maßnahmen müssen Stand der Technik entsprechen
- Schutz von Netzwerken, Zonierung, VPN, IDS/IPS, ZTNA
- Interoperabilität muss gewährleistet sein
- Systeme zur Detektion von Informationssicherheits-Vorfällen (u. a. SOC & MDR) werden explizit gefördert
- Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen

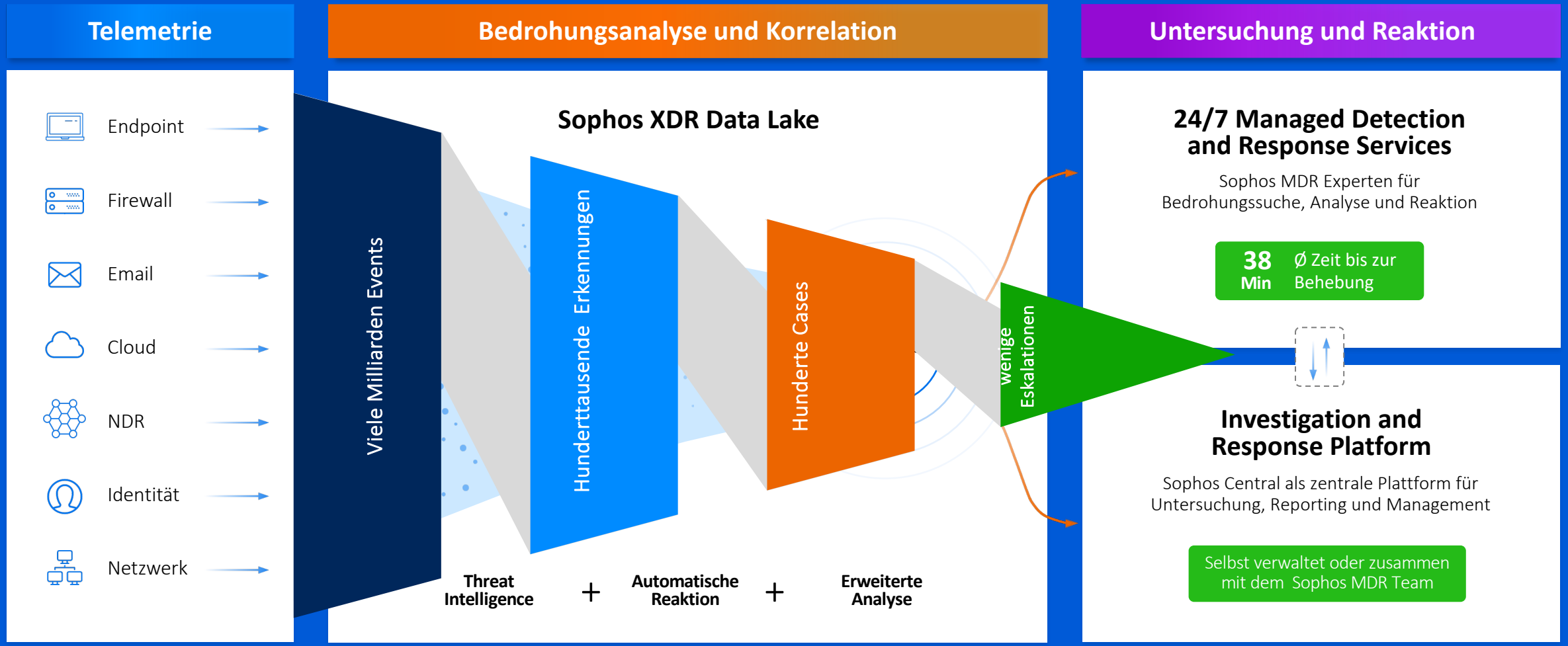


Optimale Sicherheit für Ihre Organisation

Digitale Brandmeldeanlage

SOPHOS

Erkennung und Reaktion: Gemeinsam oder durch Sophos



SOPHOS

Führende Erkennungs- und Reaktionszeiten

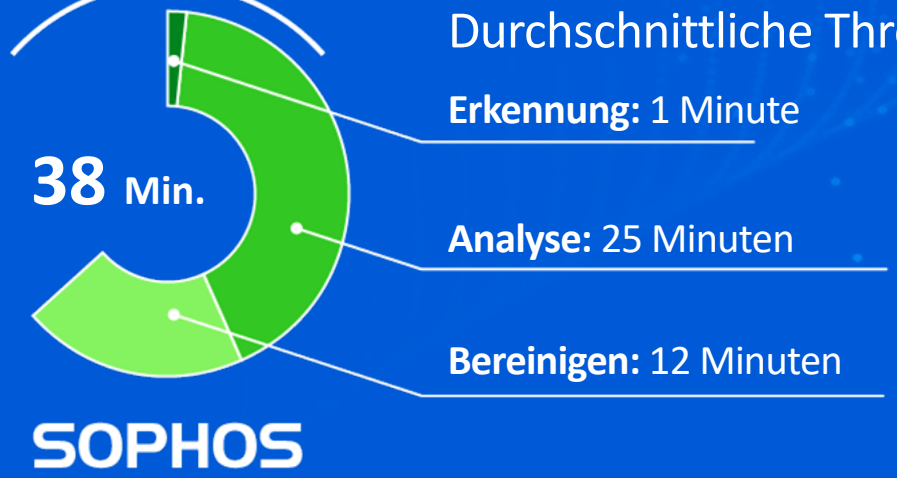
99,98%
Automatisch von Sophos blockierte Bedrohungen

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

3,7 Stunden

16 Stunden

30 Stunden



Durchschnittliche Threat-Reaktionszeit von Sophos MDR

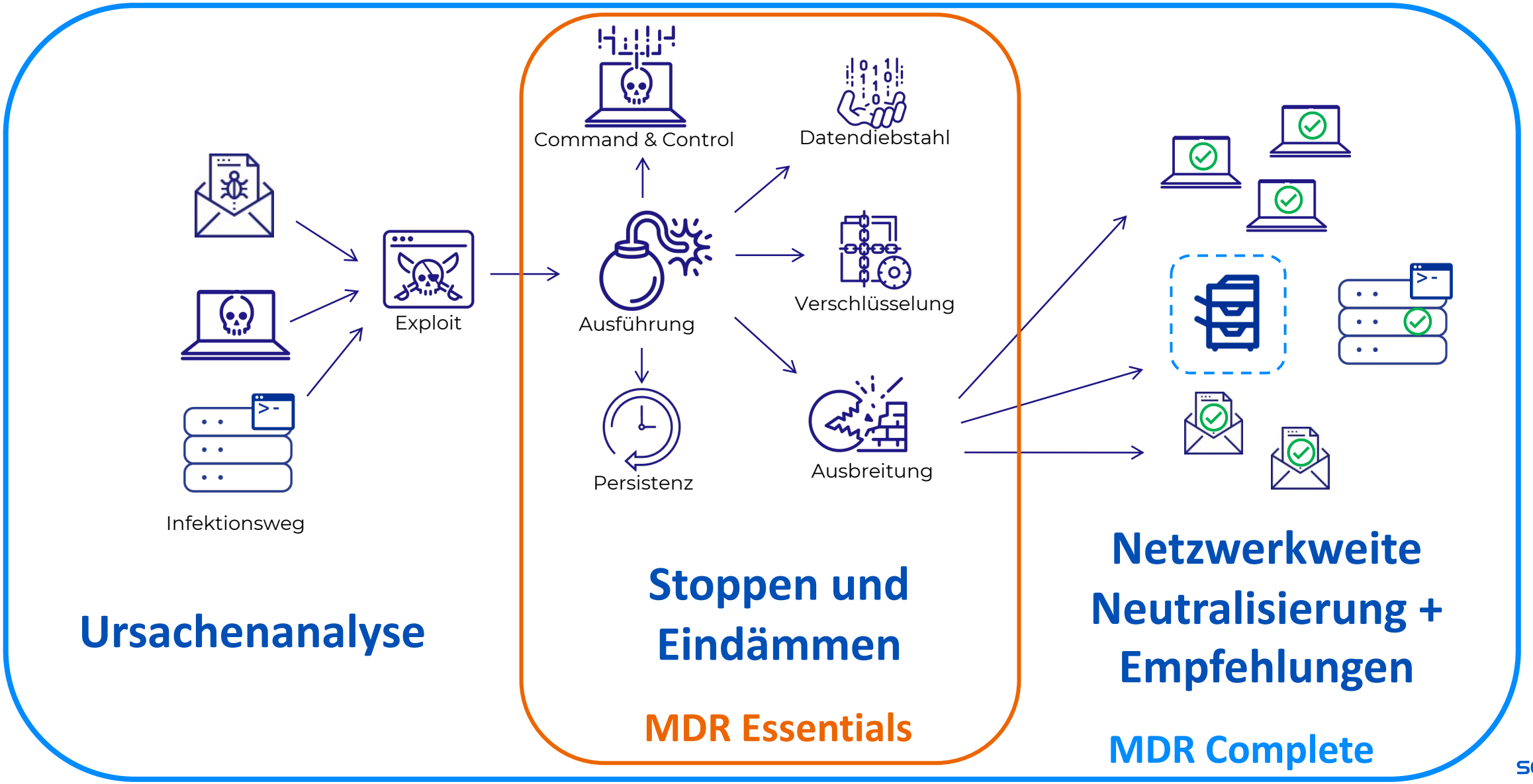
Erkennung: 1 Minute

Analyse: 25 Minuten

Bereinigen: 12 Minuten

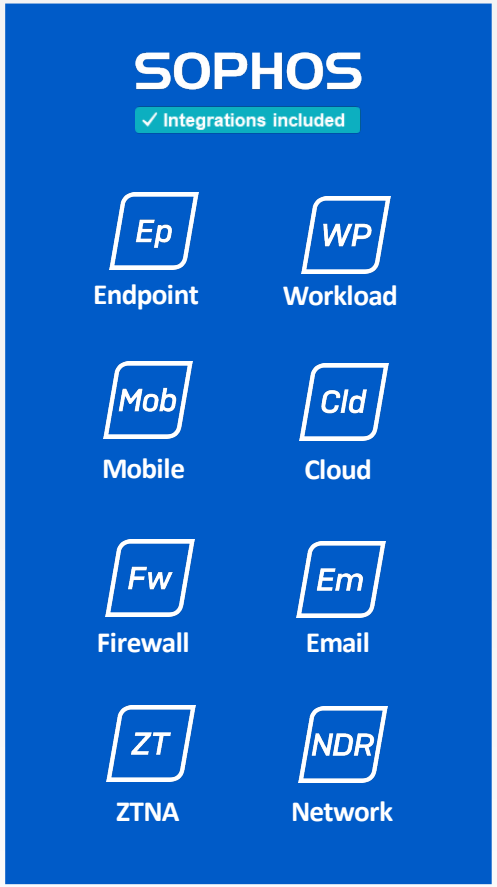
SOPHOS

Stoppen + Eindämmen vs. volles Incident Response



SOPHOS

SOPHOS MDR: Offen und flexibel



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

Cloud

orca security · aws · Azure · Google Cloud

Identity

Microsoft ✓ Included · okta · auth0 · CISCO DUO · ManageEngine

Backup and Recovery

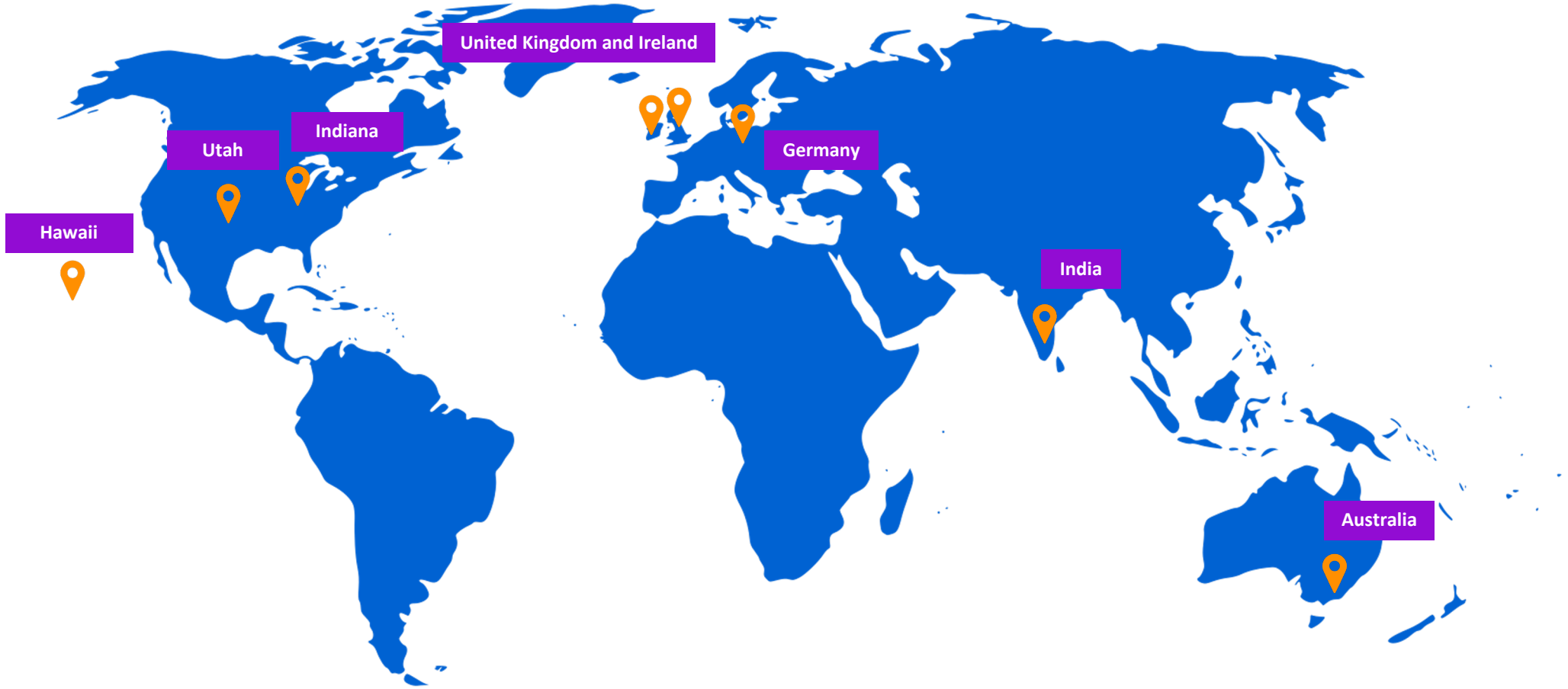
veeam

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

24x7-Abdeckung durch sieben globale SOCs



SOPHOS

MDR Interaktion

- Reports
  - Wöchentlich
  - Monatlich
- Bei dringenden Fällen direkte Kontaktaufnahme
- Cases werden automatisch im MDR Dashboard erzeugt
- MDR Team unternimmt regelmäßige Threat Hunts
- Empfehlungen zur Verbesserung der Sicherheit

Kundenszenario
Westpfalz-Klinikum

SOPHOS

Westpfalz-Klinikum

- Rollout-Phase: kritische Prüfung der Systemressourcen der Server vorab
- Dashboard ermöglicht unmittelbares Erkennen von Auffälligkeiten „täglicher Blick“ ins Dashboard
- Alle Bereiche im Team „Infrastruktur“ nutzen das Dashboard, gegenseitiger Hinweis bei Auffälligkeiten
- „Zahlen, Daten, Fakten“ (Bezug letzte 90 Tage):
  - 353 unerwünschte Applikationen erkannt, 163 blockiert, 135 bereinigt, 23 keine Bereinigung notwendig
  - 100 Malware-Erkennungen
- Aktiver Eingriff durch Sophos MDR nicht notwendig
- Wunsch/Anforderung: regelmäßiger Managementbericht (mind. pro Quartal) als Nachweisdokument für Audits

Die nächsten Schritte

Entscheidungsvorlage für IT-Leiter und Geschäftsführer

Jetzt downloaden

Podcast

Cybersecurity für kritische Infrastrukturen – was KRITIS-Unternehmen aus gesetzlicher Sicht beachten müssen mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB.

Zum Podcast

IT-Sicherheitsgesetz und Kritis

Das neue IT-Sicherheitsgesetz 2.0 betrifft nicht nur KRITIS-Betreiber in Deutschland, sondern auch deren Lieferanten in anderen Ländern. Weitere Informationen erhalten Sie auf unserer Webseite.

sophos.de/it-sicherheitsgesetz

Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

gesundheitswesen@sophos.de

SOPHOS