

**SOPHOS**

# Sophos-Lösungen für das Gesundheitswesen

Entscheidungsvorlage für IT-Leiter und Geschäftsführer



## Einleitung

Um eine schnellere, qualitativ hochwertige Versorgung zu gewährleisten, setzen Gesundheitsdienstleister immer mehr auf moderne Technologien, wie etwa vernetzte medizinische Geräte, Telemedizin, Remote-Überwachung von Patienten sowie medizinische Apps (z. B. PACS für die medizinische Bildgebung). Darüber hinaus finden neue IT-Trends Einzug in das Gesundheitswesen: Die Cloud, Machine Learning, künstliche Intelligenz und Mobility-Lösungen sorgen für eine bessere Patientenversorgung und einfacheren Zugriff auf Patientendaten. Dieser Trend ist auch Cyberkriminellen nicht entgangen: Anhand zunehmend raffinierter Angriffsmethoden versuchen diese immer häufiger, sich Zugriff auf sensible Patienten- und Gesundheitsdaten zu verschaffen, wie aktuelle Berichte in Medien eindrücklich zeigen.

**Mit unseren preisgekrönten Lösungen für das Gesundheitswesen gewährleisten Sie eine modernste, verlässliche Patientenversorgung, schützen Patientendaten und medizinische Geräte und sorgen darüber hinaus für DSGVO-Compliance. Und wenn Sie sich für unseren Rundum-Service entscheiden, kümmert sich unser Expertenteam um Ihre gesamte IT-Sicherheit – und zwar rund um die Uhr.**



## Anwendungsfälle

### Schutz für Netzwerke

Unsere Lösungen sorgen dafür, dass Ihr Netzwerk sicher und mit regulatorischen Auflagen konform ist. So gewährleisten Sie sicheren Internet-Zugriff für Mitarbeiter, Patienten und Besucher.

### Schutz für medizinische Geräte und Mobilgeräte

Sie erhalten umfassende Sicherheit für alle Geräte, sodass eine moderne, verlässliche Versorgung gewährleistet ist.

### Komplett-Schutz als Service

Unsere Experten kümmern sich rund um die Uhr um Ihre IT-Sicherheit.

### Schutz von Patientendaten: DSGVO-Compliance

Wir unterstützen Sie bei der Einhaltung aller Vorgaben und sorgen für die Sicherheit aller Gesundheitsdaten.

### Schutz für Rechenzentren

Wir schützen Ihre lokalen, cloudbasierten und hybriden Server-Umgebungen.

### Schutz für Workloads in der Public Cloud

Sie erhalten Transparenz über Assets und Netzwerkverkehr in AWS, Azure und Google Cloud sowie Funktionen zum automatischen Erkennen von Sicherheits- und Compliance-Risiken.

### Absicherung von entfernten Kliniken

Mit unseren Lösungen weiten Sie Ihr sicheres Netzwerk einfach und kostengünstig auf andere Standorte aus.

### Security-Awareness-Trainings

Sophos Phish Threat schult und testet Ihre Mitarbeiter durch praxisnahe Security-Awareness-Trainings.

## Unsere Lösungen

### Sophos XG Firewall

Unsere starke Next-Gen Firewall für den Schutz Ihrer Netzwerke.

### Sophos Intercept X with EDR

Unsere einzigartige Endpoint Protection mit EDR mit dem branchenweit besten Schutz gegen Hackerangriffe und alle Arten von Cyberbedrohungen.

### Sophos Managed Threat Response (MTR)

Unser 24/7 MDR Service: Managed Detection and Response mit Threat Hunting durch ein Expertenteam.

### plus: Komplettes Security-Portfolio

[www.sophos.de/products](http://www.sophos.de/products)

### plus: Security-Awareness-Trainings für Mitarbeiter

[www.sophos.de/phish-threat](http://www.sophos.de/phish-threat)



## Schutz für Netzwerke

Die Sicherheit Ihrer Netzwerke muss lückenlos gewährleistet sein – für die medizinische Versorgung sowie für Ihre Mitarbeiter, Patienten und Besucher. Leistungsstarke Next-Gen-Schutztechnologien wie Deep Learning und branchenführende Intrusion Prevention bieten Ihnen den besten Schutz vor Ransomware, Cryptomining, Bots, Würmern, Hacks, Sicherheitsverletzungen und Advanced Persistent Threats (APTs).

Mit intelligenten Firewall-Richtlinien und Reports erhalten Sie volle Kontrolle über Anwendungen, Websurfen, Bandbreitenkontingente und weitere Netzwerkressourcen. Synchronized App Control identifiziert alle Anwendungen und priorisiert bzw. blockiert sie nach Bedarf. Unsere Technologien sorgen dafür, dass personenbezogene Daten sicher sind: benutzerbasiertes Monitoring von Keyword-Inhalten und Downloads, Web Keyword Monitoring, Datei-Download-Filter, Data Loss Prevention für E-Mails.

In Kombination mit unserem branchenführenden Endpoint-Schutz Intercept X profitieren Sie zudem von Exploit Prevention und CryptoGuard Protection zur Abwehr von Ransomware. So sichern Sie sich den besten Schutz vor komplexen Bedrohungen und müssen bei Vorfällen nicht selbst tätig werden, da die Reaktion automatisch erfolgt.

**Mit der Sophos XG Firewall erhalten Sie alle wichtigen Kontrollfunktionen für Netzwerk, Benutzer und Anwendungen und sorgen dafür, dass Ihr Netzwerk sicher und mit regulatorischen Auflagen konform bleibt.**

## Schutz für medizinische Geräte

Lebenserhaltende Systeme wie Magnetresonanztomographen, Infusionspumpen, Patientenmonitore und sonstige medizinische Geräte dürfen Hacker-Angriffen unter keinen Umständen schutzlos ausgeliefert werden. Daten medizinischer Geräte werden von verschiedenen Geräten gemeinsam genutzt und sind daher leicht verfügbar. Jedoch wird der Zugriff auf hochsensible Patientendaten dabei oft nicht ausreichend kontrolliert und geschützt.

Branchenführendes Deep Learning in Kombination mit Bedrohungsdaten aus den SophosLabs setzt bei der Bedrohungsabwehr komplett neue Standards.

Synchronized Security bündelt Ihre Abwehrmaßnahmen durch den Echtzeit-Austausch von Sicherheitsdaten zwischen Ihren Endpoints und Ihrer Firewall. Dabei werden infizierte Systeme automatisch isoliert und Malware wird sofort entfernt. Zudem erhalten Sie maximale Transparenz über Anwendungen im Netzwerk.

**Unsere Lösungen bieten hocheffektiven Schutz durch eine extrem leistungsstarke Malware-Erkennung, Ransomware-Abwehr, Exploit-Schutz sowie Endpoint Detection and Response (EDR).**

## Schutz für Mobilgeräte

Mobilgeräte kommen auch im Gesundheitswesen immer mehr zum Einsatz. In der Regel wurden verbraucherorientierte Geräte jedoch nicht für die Sicherung sensibler Patientendaten konzipiert. Trotzdem werden vertrauliche Patientendaten immer häufiger auf Mobilgeräten gespeichert, verarbeitet und übertragen. Werden Patientendaten gestohlen, veröffentlicht oder modifiziert, drohen Gesundheitsdienstleistern empfindliche Strafen und behördliche Maßnahmen.

Mit den sicheren, AES-256-verschlüsselten Containern von Sophos Mobile bleiben sensible Patientendaten auf Mobilgeräten geschützt und von privaten Daten getrennt. Die komfortable Konfiguration für den E-Mail- und Datenzugriff spart Ihnen Zeit und Ihre Benutzer werden mit Anti-Phishing-Technologie vor schädlichen Links in Dokumenten und sonstigen Inhalten geschützt. Sie können den Zugriff auf Container sogar je nach Uhrzeit, WLAN-Netzwerk oder Standort beschränken.

**Sophos Intercept X for Mobile schützt vor schädlichen Apps, Ransomware, Spam, potenziell unerwünschten Anwendungen (PUA) sowie neuen Apps für Android-Geräte. Die Software überwacht den Gerätestatus kontinuierlich und informiert Sie, falls ein Gerät kompromittiert werden sollte. In diesem Fall können Maßnahmen eingeleitet werden oder der Zugriff wird automatisch blockiert.**

Mit unseren Lösungen erhalten Sie zuverlässigen Schutz für alle denkbaren Einsatzszenarien. Wenn Sie sich für unseren MDR-Service entscheiden, kümmern sich unsere Experten 24/7 um Ihre IT-Sicherheit. So können Sie sich auf die Versorgung Ihrer Patienten konzentrieren, ohne sich Sorgen um Hackerangriffe machen zu müssen.

## Komplett-Schutz als Service

Krankenhäuser sind in der letzten Zeit verstärkt Opfer von Cyberangriffen geworden. Die Berichte in den Medien dazu zeigen eindrücklich: Ein Cyberangriff kann verheerende Folgen haben auf den Krankenhausbetrieb und auf die Versorgung der Patienten. Viele kritische Systeme sind hier im Einsatz und können bei einem Cyberangriff vollständig ausfallen: Medizinische Geräte, Systeme zur Diagnose, Behandlung und Monitoring von Patienten, Planungsdatenbanken, Paging-Systeme, Gebäudekontroll-Systeme, Informations- und Verwaltungssysteme des Krankenhauses, etc.

Krankenhäuser und medizinische Einrichtungen benötigen deshalb eine gute Sicherheitsstrategie. Nur mit einer solchen Strategie ist es möglich, Cyberangriffe zu verhindern oder im Ernstfall schnell und wirksam zu reagieren.

Tritt der Ernstfall ein und ein Cyberangriff findet statt, zählt jede Sekunde, um Schaden abzuwenden: Alle betroffenen Systeme müssen schnell gefunden und isoliert werden, damit sich die Bedrohung nicht ausbreiten kann. Dazu müssen sofort gezielte Maßnahmen eingeleitet werden, um die Angreifer zu stoppen.

**Mit Sophos MTR erhalten Sie ein Expertenteam, das 24/7 für Sie nach Bedrohungen Ausschau hält und bei Bedarf sofort gezielte Maßnahmen ergreift, um selbst hochkomplexe Bedrohungen unschädlich zu machen.**



## Schutz von Patientendaten: DSGVO-Compliance

Die DSGVO verlangt, dass Gesundheitsdienstleister, die vertrauliche Patientendaten verarbeiten, mit Hilfe von Sicherheitsmaßnahmen Compliance sicherstellen. Wir bieten effektive Tools zur Erfüllung von Sicherheitsauflagen im Rahmen Ihrer DSGVO-Compliance-Maßnahmen.

So können wir Ihre DSGVO-Compliance-Maßnahmen unterstützen:

- Kontrolle der Systemintegrität: Hochkarätige Funktionen zur Abwehr vor Bedrohungen, wie Anti-Exploit und Anti-Ransomware, in Kombination mit Deep Learning und den einzigartigen Synchronized-Security-Funktionen von Sophos sorgen für branchenweit führenden Schutz
- Access Control: Die Benutzeridentität bildet die Grundlage für alle Firewall-Richtlinien und Reports
- Audit-Kontrolle: Anhand detaillierter Protokolle und umfassendem Reporting lassen sich verdächtige Aktivitäten auf Systemen ermitteln, auf denen unter Umständen vertrauliche Patientendaten gespeichert oder verarbeitet werden
- Sichere Übertragung: Die SPX Encryption wandelt E-Mail-Inhalte und -Anhänge dynamisch in ein sicheres, verschlüsseltes PDF um und stellt so Compliance sicher. SafeGuard Encryption verschlüsselt Daten auf Macs, Windows-Computern und Mobilgeräten. Daten bleiben auch bei der Übertragung im Netzwerk verschlüsselt.

## Schutz für Rechenzentren

Rechenzentren spielen im Gesundheitswesen eine wichtige Rolle. Moderne digitale Technologien wie Röntgenapparate und MRT-Geräte generieren große Mengen an hochauflösenden bildgebenden und diagnostischen Daten. Herzfrequenz-Messgeräte, Schrittzähler und sonstige tragbare Geräte senden Daten in Echtzeit an medizinisches Fachpersonal, damit Patienten schnell und korrekt versorgt werden. Dabei werden wiederum wichtige Gesundheitsdaten generiert, die alle verlässlich in Rechenzentren gespeichert werden müssen.

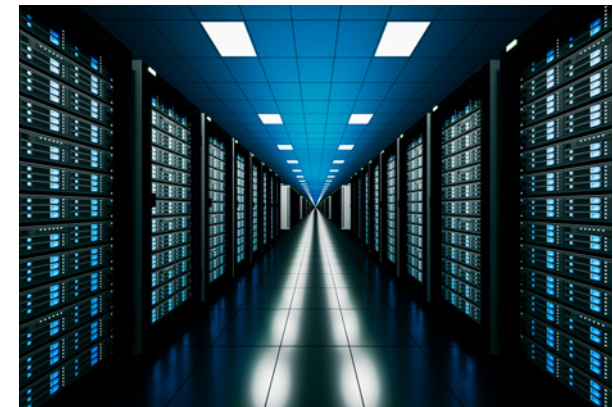
In Einklang mit regulatorischen Auflagen wie der DSGVO müssen Gesundheitsdienstleister einen sicheren Zugriff auf elektronische Patientendaten gewährleisten. In Rechenzentren sind stringente Kontrollen zum Schutz von Daten sowie die Sicherstellung der Verfügbarkeit von Informationen für befugte Benutzer unerlässlich.

Sophos Intercept X for Server schützt Ihre lokalen, cloudbasierten und hybriden Server-Umgebungen. Blockieren Sie komplexe Bedrohungen, stoppen Sie Ransomware und schützen Sie Ihr Netzwerk vor gefährlichen Exploit-Techniken. So haben Hacker keine Chance.

Intercept X for Server und die Sophos XG Firewall arbeiten aktiv zusammen. Dadurch können Sie kompromittierte Server isolieren und so verhindern, dass Bedrohungen sich lateral ausbreiten. Bedrohungen werden automatisch bereinigt. Sie erhalten lückenlose Transparenz über alle

Anwendungen, die auf Ihren Servern ausgeführt werden, und verhindern so, dass unbekannte Apps nach außen kommunizieren.

**Endpoint Detection and Response (EDR) liefert Ihnen maximale Transparenz über alle Server. So können Sie evasive Bedrohungen finden, kontrollieren, welche Anwendungen ausgeführt werden, und automatisch auf Sicherheitsvorfälle reagieren.**



## Schutz für Workloads in der Public Cloud

Wie andere Unternehmen verlagern auch Gesundheitsdienstleister ihre Workloads zunehmend in die Public Cloud. So senken sie ihre Kosten und gewinnen gleichzeitig an Flexibilität. Tagtäglich arbeiten Gesundheitsdienstleister mit vertraulichen Kunden- und Patientendaten, die geschützt werden müssen. Und da das Gesundheitswesen darüber hinaus stark reglementiert ist, gelten strenge Compliance-Anforderungen (z. B. DSGVO).

Hier hilft unsere Cloud-Lösung: Leistungsstarke künstliche Intelligenz erkennt verdächtiges Verhalten und riskante Anmeldeaktivitäten schnell – mit intelligenten Warnmeldungen und optional der automatischen Bereinigung von Risiken. Dank hochkarätiger Compliance-Funktionen wird zudem die Konformität mit der DSGVO, HIPAA, PCI und sonstigen Standards gewährleistet.

**Durch die leistungsstarke Kombination von KI und Automatisierung vereinfacht Sophos Cloud Optix Compliance, Governance und die Überwachung der Sicherheit in der Public Cloud. Ihre Assets in Umgebungen von Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) werden automatisch erkannt. So können Sie innerhalb weniger Minuten auf Sicherheitsrisiken reagieren und diese bereinigen.**

## Absicherung von entfernten Kliniken

Das Gesundheitswesen überbrückt räumliche Distanzen: Telemedizin und Fern-Monitoring finden immer mehr Zuspruch. Dank dieser innovativen Trends können Mediziner ihre Patienten weltweit unterbrechungslos behandeln. Dazu bedarf es jedoch der Zusammenarbeit und Kommunikation mit Kollegen an entfernten Standorten in aller Welt.

**Mit Sophos SD-RED (SD-WAN Remote Ethernet Devices) können Sie Ihr sicheres Netzwerk einfach und kostengünstig auf andere Standorte ausweiten. Am Remote-Standort ist dabei kein technisches Fachwissen erforderlich.**

Geben Sie einfach die ID Ihres RED-Geräts in Ihre XG Firewall ein und schicken Sie das Gerät an den betreffenden Standort. Sobald das Gerät angeschlossen und mit dem Internet verbunden ist, stellt unser Bereitstellungsservice automatisch eine Verbindung zu Ihrer Firewall her und baut einen sicheren Ethernet-Tunnel auf.

Darüber hinaus ermöglicht die Sophos XG Firewall eine Zwei-Faktor-Authentifizierung für VPN-Verbindungen, mit RADIUS/TACACS-Integration. Sophos SafeGuard Encryption sorgt durch Verschlüsselung für sicheren Zugriff auf Patientendaten: Benutzer werden für den Zugriff auf bestimmte Geräte, Dateien und/oder Ordner mit benutzer- oder gruppenspezifischen Schlüsseln authentifiziert.

Die Daten bleiben auch dann verschlüsselt, wenn sie im Netzwerk übertragen werden. Die SPX-Verschlüsselung in Sophos Email und der XG Firewall wandelt E-Mail-Inhalte und -Anhänge dynamisch in ein sicheres, verschlüsseltes PDF um und stellt Compliance sicher. Sophos Secure Email und Sophos Secure Workspace in Sophos Mobile speichern Daten sicher auf mobilen Geräten mit AES-256-Verschlüsselung. Der Zugriff auf die Inhalte in den Apps kann basierend auf Gerätestatus, Compliance-Regeln, Zeit, WLAN-Netzwerk oder Standard eingeschränkt werden.

## Awareness-Trainings für Mitarbeiter

Phishing ist ein lukratives Geschäft. Phishing-Angriffe haben in den letzten Jahren dramatisch zugenommen. Ein solides Awareness-Programm darf deshalb in keiner fundierten Sicherheitsstrategie fehlen.

**Sophos Phish Threat schult und testet Ihre Mitarbeiter durch automatische Angriffssimulationen, qualitativ hochwertige Security-Awareness-Trainings und aussagekräftige Reporting-Daten.**

Wir haben mehr als 30 Security-Awareness-Trainingsmodule im Angebot, die sowohl Sicherheits- als auch Compliance-Themen abdecken. Sophos Phish Threat „verpackt“ Tests und Trainings in einfachen, benutzerfreundlichen Kampagnen. Diese bieten automatische, sofort einsatzbare Trainings für Ihre Mitarbeiter, je nach Bedarf.

## Profitieren Sie jetzt mit Sophos optimal vom Krankenhauszukunftsgesetz (KHZG)

Cybersicherheit ist die notwendige Bedingung für die fortschreitende Digitalisierung in den Kliniken. Ein zentrales Ziel des KHZG ist deshalb die Verbesserung der IT- bzw. Cybersicherheit in Krankenhäusern, die nicht zu den kritischen Infrastrukturen gehören, sowie in Hochschulkliniken.

Vorhaben zur Verbesserung der IT- bzw. Cybersicherheit sind gemäß KHZG förderfähig, wenn sie eines oder mehrere der folgenden Ziele verfolgen:

- Prävention von IT-Sicherheits-Vorfällen
- Detektion von IT-Sicherheits-Vorfällen
- Mitigation von IT-Sicherheits-Vorfällen
- Steigerung und Aufrechterhaltung der Awareness für IT-Sicherheit

Mit Sophos-Lösungen erfüllen Sie alle diese Anforderungen:

Ziel	Sophos-Lösungen
Prävention	Abwehr von externen Angriffen und Bedrohungen mit der <b>XG Firewall</b> .
Detektion	Erkennen bisher unbekannter Bedrohungen mit <b>Intercept X with EDR und MTR</b> .
Mitigation	Eindämmen der Bedrohung bei einem Angriff mit <b>Synchronized Security</b> .
Awareness	Sensibilisierung der Mitarbeiter mit <b>Phish Threat</b> .

Darüber hinaus unterstützen wir Sie umfassend bei der Umsetzung Ihrer Vorhaben. Unser dediziertes Healthcare Team berät Sie und vermittelt Sie an einen unserer spezialisierten Vertriebspartner. Wir arbeiten mit einem Netzwerk von Vertriebspartnern zusammen, die sich gezielt auf den Bereich Gesundheitswesen spezialisiert haben, sodass Sie in den besten Experten-Händen sind. Alle wichtigen Schritte und Ansprechpartner sowie weiterführende Informationen finden Sie auf der nächsten Seite.



## Die nächsten Schritte:

1. Kontaktieren Sie unser Sophos Healthcare Team. Unsere Experten sind für Sie da und beraten Sie.  
E-Mail: [gesundheitswesen@sophos.de](mailto:gesundheitswesen@sophos.de)  
Tel.Nr: 0611-5858-0
2. Wir empfehlen Ihnen einen unserer spezialisierten Vertriebspartner und stellen wenn gewünscht auch gerne den Kontakt her.
3. Ihr Vertriebspartner unterstützt und begleitet Sie bei der Umsetzung Ihres Vorhabens. Bei Fragen stehen selbstverständlich auch wir Ihnen weiterhin jederzeit zur Verfügung.

## Weiterführende Informationen

Sophos-Webseite für das Gesundheitswesen zum Krankenhauszukunftsgesetz:

[www.sophos.de/khzzg](http://www.sophos.de/khzzg)

Genauere Beschreibung des Bundesgesundheitsministeriums zum Krankenhauszukunftsgesetz:

<https://www.bundesgesundheitsministerium.de/krankenzukunftsgesetz.html>

Sophos Healthcare Team Deutschland  
E-Mail: [gesundheitswesen@sophos.de](mailto:gesundheitswesen@sophos.de)  
Tel.: 0611-5858-0

© Copyright 2020. Sophos Ltd. Alle Rechte vorbehalten.  
Eingetragen in England und Wales, Nr. 2098520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB  
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Firmennamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

09.04.2020 WP-DE (NP)