Sophos-Produkte für das Gesundheitswesen

Cybersicherheit ist für das Gesundheitswesen von großer Bedeutung, denn Cyberangriffe bedrohen nicht nur die IT-Sicherheit in diesem Bereich und die Verfügbarkeit von Gesundheitsdaten, sondern auch die Gesundheit und Sicherheit der Patienten. Gesundheitseinrichtungen sind ein einladendes Ziel für finanziell motivierte Bedrohungsakteure, die Patientendaten für kriminelle Zwecke wie Versicherungsbetrug nutzen und im Darkweb zum Kauf anbieten.
Dieses Dokument bietet einen allgemeinen Überblick darüber, wie Sophos-Lösungen Gesundheitseinrichtungen dabei unterstützen, ihre Cybersecurity-Anforderungen zu erfüllen und eine unterbrechungsfreie Patientenversorgung zu gewährleisten.

Problem	Sophos-Lösung	Funktionen und Vorteile
Wahrung der Vertraulichkeit elektronisch geschützter Gesundheitsdaten	Sophos Firewall	Unterstützt flexible Optionen zur mehrstufigen Authentifizierung, einschließlich Verzeichnisdiensten für den Zugriff auf wichtige Systembereiche.
	Sophos Central Device Encryption	Schützt Geräte und Daten mit leistungsstarker Festplatten-Verschlüsselung für Windows und macOS. Überprüft den Verschlüsselungs-Status des Geräts und weist die Compliance nach.
	Sophos Switch	Ermöglicht Network Access Control, mit der Sie Benutzer über LDAP, MAC-Adresse oder andere Authentifizierungsmethoden authentifizieren können, bevor Sie Zugriff zu einem Netzwerk gewähren. Dadurch wird verhindert, dass unbefugte Benutzer und Geräte Zugriff auf Ihr LAN erhalten.
	Sophos Managed Detection and Response (MDR)	Stoppt Datenverluste durch Angriffsaktivitäten mittels 24/7 Monitoring der Umgebung sowie Analyse und Beseitigung schädlicher Aktivitäten.
	Sophos Email	Genaue Kontrolle der Richtlinien zur Verhinderung von Datenschutzverletzungen, einschließlich Richtlinien mit mehreren Regeln für Gruppen und einzelne Benutzer mit nahtloser Integration der Verschlüsselung. Erstellen benutzerdefinierter CCLs mithilfe von Sophos Content Control Lists bzw. Anpassung integrierter Vorlagen für spezielle CCLs. Wählen Sie die für Sie relevanten Richtlinien, einschließlich Blockieren, Anhang entfernen, Quarantäne sowie „Protokollieren und fortfahren"-Modus.
	Sophos Mobile	Eine Vielzahl von Gerätemanagement-Funktionen sorgen dafür, dass sensible E-Mails und -Dokumente auf Mobilgeräten sicher bleiben – selbst auf Privatgeräten. Flexible Compliance-Regeln überwachen den Gerätestatus und kennzeichnen etwaige Abweichungen von den gewünschten Einstellungen.
	Sophos ZTNA	Überprüft kontinuierlich die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Anwendungen und Daten gewährt wird.
	Sophos Wireless	Erstellt dynamisch verschlüsselte WLAN-Verbindungen zum Schutz Ihrer Daten während der Übertragung in über Sophos Central verwalteten Netzwerken und Hotspots.
	Sophos Cloud Optix	Befolgen Sie das Least-Privilege-Prinzip in Public-Cloud-Umgebungen mit der „Cloud Security Posture Management"-Lösung „Sophos Cloud Optix". Der SaaS-basierte Service setzt verschiedene Aktionen mit KI von Sophos in Beziehung zueinander, um bei Zugriffen auf Konsolen von Cloud-Anbietern ungewöhnliche Muster und Orte nahezu in Echtzeit zu erkennen. So lassen sich Identitätsdiebstahl und missbräuchliche Nutzungen von Zugangsdaten einfacher feststellen. Beinhaltet ein IAM-Visualisierungs-Tool, das einen umfassenden Überblick über IAM-Beziehungen verschafft. Damit lassen sich überprivilegierte Zugriffe schnell erkennen und adäquate IAM-Richtlinien erstellen.

SOPHOS

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Schutz vor Malware	Sophos Firewall	Erkennt bereits – dank der branchenführenden Machine-Learning-Technologie von Sophos (unterstützt von SophosLabs Intelix) – neueste Ransomware und unbekannte Bedrohungen, bevor sie in Ihr Netzwerk gelangen. Bietet modernsten Schutz vor aktueller Drive-by- und gezielter Web-Malware, Filterung von URLs/ schädlichen Websites, Filterung von Webanwendungen und cloudbasierte Filterung für Offsite-Schutz.
	Sophos Sandboxing	Ergänzt die Sophos Web- und E-Mail-Sicherheitsprodukte und die Sophos Firewall und analysiert und blockiert Executables und Dokumente mit ausführbarem Inhalt, bevor die Datei auf das Gerät des Benutzers gelangt.
	Sophos Intercept X for Mobile	Erkennt schädliche und potenziell unerwünschte Anwendungen auf Android-Geräten mithilfe der Deep-Learning-Technologie aus Sophos Intercept X und Bedrohungsdaten aus den SophosLabs. Durch die Integration mit Microsoft Intune können Admins Richtlinien für eingeschränkten Zugriff festlegen und so den Zugriff auf Apps und Daten beschränken, wenn eine Bedrohung erkannt wird.
	Sophos Intercept X Sophos Intercept X for Server	Eine Kombination aus HIPS-Technologie, Deep Learning, Anti-Exploit, Active Adversary Protection und Malicious Traffic Detection erkennt proaktiv schädliches Verhalten auf dem Host. Exploit-Schutz-Funktionen verhindern, dass Schwachstellen in Anwendungen und Betriebssystemen von Angreifern ausgenutzt werden. Richtlinien zur Anwendungskontrolle beschränken die Verwendung nicht autorisierter Anwendungen.
	Sophos Intercept X for Server	Verhindert mittels Server Protection, dass nicht autorisierte Anwendungen ausgeführt werden, indem Ihr System automatisch auf bekannte erwünschte Anwendungen gescannt wird und nur diese Anwendungen auf die Positivliste gesetzt werden.
	Sophos Cloud Optix	Überwacht kontinuierlich die Konfigurationsstandards, um Abweichungen zu erkennen. So können Sie versehentliche oder mutwillige Manipulationen in der Ressourcenkonfiguration verhindern, erkennen und automatisch korrigieren.
	Sophos Managed Detection and Response (MDR)	Überwacht kontinuierlich Signale aus der gesamten Sicherheitsumgebung (u. a. von Netzwerk-, E-Mail-, Mobile-, Identity-, Endpoint- und weiteren Technologien), um potenzielle Cybersecurity-Vorfälle schnell und präzise zu erkennen. Ungewöhnliche Verhaltensweisen und die Verwendung von Code werden erkannt, analysiert und korreliert, um schädliche Aktivitäten zu identifizieren und den Vorfall schnell zu beheben.
Sicherer Remote-Zugriff	Sophos Firewall	Ermöglicht eine Zwei-Faktor-Authentifizierung für VPN-Verbindungen, mit RADIUS/TACACS-Integration. Dank Sophos SD-RED können Sie einen sicheren Ethernet-Tunnel aufbauen und so Ihr sicheres Netzwerk ganz einfach auf einen Remote-Standort ausweiten.
	Sophos ZTNA	Überprüft kontinuierlich die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Anwendungen und Daten gewährt wird.
	Sophos Mobile	Eine Vielzahl von Gerätemanagement-Funktionen sorgen dafür, dass sensible E-Mails und -Dokumente auf Mobilgeräten sicher bleiben – selbst auf Privatgeräten. Flexible Compliance-Regeln überwachen den Gerätestatus und kennzeichnen etwaige Abweichungen von den gewünschten Einstellungen.
	Sophos Wireless	Überwacht den Integritätsstatus von Geräten, die eine Verbindung zum WLAN herstellen, und ergreift bei Bedarf entsprechende Maßnahmen. Der WLAN-Zugriff von unsicheren und nicht konformen Endpoints und Mobilgeräten wird automatisch beschränkt, sodass sich eine Infektion nicht lateral ausbreiten kann.
	Sophos Cloud Optix	Befolgen Sie das Least-Privilege-Prinzip in Public-Cloud-Umgebungen mit der „Cloud Security Posture Management"-Lösung „Sophos Cloud Optix". Der SaaS-basierte Service setzt verschiedene Aktionen mit KI von Sophos in Beziehung zueinander, um bei Zugriffen auf Konsolen von Cloud-Anbietern ungewöhnliche Muster und Orte nahezu in Echtzeit zu erkennen. So lassen sich Identitätsdiebstahl und missbräuchliche Nutzungen von Zugangsdaten einfacher feststellen. Beinhaltet ein IAM-Visualisierungs-Tool, das einen umfassenden Überblick über IAM-Beziehungen verschafft. Damit lassen sich überprivilegierte Zugriffe schnell erkennen und adäquate IAM-Richtlinien erstellen.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Sicherheit für vernetzte medizinische Geräte	Sophos Firewall	Unternehmenskritische medizinische Geräte im Netzwerk bleiben geschützt, sodass sich Angreifer nicht durch Ihre Server und Anwendungen bewegen können. Flexible und leistungsstarke Segmentierungsoptionen über Zonen und VLANs ermöglichen Ihnen, Vertrauensebenen in Ihrem Netzwerk zu separieren und den Schutz gegen laterale Bewegungen zwischen verschiedenen Netzwerksegmenten zu erhöhen.
	Sophos Switch	Ermöglicht Network Access Control, mit der Sie Benutzer über LDAP, MAC-Adresse oder andere Methoden authentifizieren können, bevor Sie Zugriff zu einem Netzwerk gewähren. Dadurch wird verhindert, dass unbefugte Benutzer und Geräte Zugriff auf Ihr LAN erhalten.
	Sophos Mobile	Eine Vielzahl von Gerätemanagement-Funktionen, Container und eine marktführende Verschlüsselung sorgen dafür, dass sensible Geschäfts-E-Mails und -Dokumente auf mobilen Geräten sicher bleiben – selbst auf Privatgeräten. Führende Antivirus und Ransomware Protection schützt Ihre Benutzer und Geräte vor schädlichen Inhalten und Anwendungen.
	Sophos Wireless	Überwacht den Integritätsstatus von Geräten, die eine Verbindung zum WLAN herstellen, und ergreift bei Bedarf entsprechende Maßnahmen. Der WLAN-Zugriff von unsicheren und nicht konformen Endpoints und Mobilgeräten wird automatisch beschränkt, sodass sich eine Infektion nicht lateral ausbreiten kann.
	Synchronized Security in Sophos-Produkten	Ermöglicht durch den Austausch von Telemetrie- und Statusdaten ein koordiniertes Erkennen, Isolieren und Beseitigen von Malware auf Servern, Endpoints und Firewalls. So können auch komplexe Angriffe gestoppt werden.
Gewährleistung der Wireless-Sicherheit	Sophos Wireless	Sicherheit für die wachsende Anzahl an mobilen Geräten im Gesundheitswesen und mehr Transparenz über den Integritätsstatus Ihrer WLAN-Netzwerke. Der WLAN-Zugriff von unsicheren und nicht konformen Endpoints und Mobilgeräten wird automatisch beschränkt, sodass sich eine Infektion nicht lateral ausbreiten kann. Trennen Sie den WLAN-Zugang von Gastbenutzern vom Zugang Ihrer Mitarbeiter mit Tagespasswörtern oder zeitbasierten Vouchern. Unsere APX-Modelle sind für den Einsatz im Gesundheitswesen zertifiziert, d. h. der Betrieb medizinischer Geräte wird nicht gestört.
Reduzierung von Lieferketten-Risiken	Sophos Intercept X with XDR	Bietet u. a. mit KI, Anti-Exploit-Technologie, Verhaltensschutz und Anti-Ransomware umfassenden Schutz vor Bedrohungen, die sich über Drittanbieter Zugriff verschaffen. Außerdem können Sie mit der leistungsstarken XDR-Funktionalität verdächtige Aktivitäten automatisch erkennen, Bedrohungsindikatoren priorisieren und Ihren gesamten Endpoint- und Server-Bestand schnell und einfach auf potenzielle Bedrohungen durchsuchen.
	Sophos Managed Detection and Response (MDR)	Bietet Threat Hunting durch ein Experten-Team und Bereinigung als Fully-Managed-Service. Sophos-Experten arbeiten rund um die Uhr daran, für Sie proaktiv potenzielle Bedrohungen und Sicherheitsvorfälle in der Lieferkette aufzuspüren, zu analysieren und Reaktionsmaßnahmen zu ergreifen.
	Sophos ZTNA	Schützt durch gezielte Zugriffssteuerung vor Angriffen auf die Lieferkette, die auf den Zugriff von Drittanbietern auf Ihre Systeme angewiesen sind. Diese Cloud-basierte Lösung überprüft die Benutzeridentität sowie den Gerätestatus und die Compliance, bevor Zugriff auf Ressourcen gewährt wird. Anfragen von vertrauenswürdigen Partnern werden unabhängig vom Standort authentifiziert.
Schutz für Ressourcen in der Cloud	Sophos Cloud Native Security	Bietet kompletten Multi-Cloud-Schutz für Umgebungen, Workloads und Identitäten. Die Lösung schützt Ihre Cloud-Infrastruktur und -Daten mit flexibler Host- und Container-Workload-Sicherheit für Windows und Linux. Unsere mehrschichtigen Technologien, einschließlich cloudnativer Verhaltens- und Exploit-Laufzeiterkennungen (Runtime Detections), schützen vor Ransomware und anderen modernen Angriffsstrategien. Zudem erkennen sie Bedrohungen wie Container-Escape, Kernel-Exploits und Versuche, die Berechtigungsstufe zu erhöhen.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Proaktive Sicherheit	Synchronized Security in Sophos-Produkten	Ermöglicht durch den Austausch von Telemetrie- und Statusdaten ein koordiniertes Erkennen, Isolieren und Beseitigen von Malware auf Servern, Endpoints und Firewalls. So können auch komplexe Angriffe gestoppt werden.
	Sophos Managed Detection and Response (MDR)	Sophos MDR erkennt und analysiert verdächtige Ereignisse in der gesamten Sicherheitsumgebung, um Bedrohungen zu erkennen und geeignete Reaktionsmaßnahmen zu ergreifen. Daten werden u. a. von Endpoint-, Netzwerk-, Identitäts-, und E-Mail-Quellen gesammelt und dann mithilfe leistungsstarker KI-Tools, Threat Intelligence und Cyberexperten korreliert, um die Auswirkungen und Reaktionsmaßnahmen zu identifizieren.
	Sophos XDR	Geht über die Endpoint-Ebene hinaus und berücksichtigt auch zahlreiche Netzwerk-, E-Mail- und andere Datenquellen. So erhalten Sie ein noch umfassenderes Bild Ihrer Cybersicherheit und haben die Möglichkeit, bei Bedarf jederzeit Detailinformationen abzurufen. Da Daten von jedem Produkt in den Sophos Data Lake einfließen, können Sie schnell geschäftskritische Fragen beantworten, Ereignisse aus verschiedenen Datenquellen korrelieren und noch besser gezielte Maßnahmen ergreifen.
	Sophos Cloud Optix	Mit Sophos Cloud Optix, der „Cloud Security Posture Management"-Lösung von Sophos, können IT-Teams die Security Posture im Unternehmen proaktiv verbessern und unsichere Konfigurationen sowie Schwachstellen erkennen. Cloud Optix richtet Ihre Umgebung automatisch an Best Practices im Bereich Compliance und Sicherheit aus und liefert so maximale Transparenz zur lückenlosen Überwachung und Aufrechterhaltung Ihrer Security Posture.
Phishing-Schutz	Sophos Email	Scannt alle eingehenden Nachrichten in Echtzeit – mittels SPF-, DKIM- und DMARC-Authentifizierungsmethoden sowie Prüfung auf Anomalien im E-Mail-Header – auf wichtige Phishing-Hinweise wie Brand-Spoofing und Versuche, falsche Identitäten vorzutäuschen. So können Phishing-E-Mails bereits erkannt und blockiert werden, bevor sie den Empfänger erreichen.
	Sophos Phish Threat	Schult und testet Mitarbeiter durch automatische Angriffssimulationen und qualitativ hochwertige Security-Awareness-Trainings auf Phishing, Diebstahl von Zugangsdaten und Anhangsangriffe und liefert aussagekräftige Reporting-Daten.
	Sophos Intercept X	Bietet umfassenden Schutz für alle Ihre Endpoints – Windows, Mac, Linux und virtuelle Maschinen – mit mehrschichtigen Schutztechnologien, die Ihre Abwehrmaßnahmen optimieren, einschließlich Credential Theft Protection, Exploit-Schutz, Anti-Ransomware und Manipulationsschutz.
Einhalten geltender Vorschriften	Sophos Cloud Optix	Eliminiert Compliance-Lücken, da Sie den Compliance-Status von AWS-, Azure- und Google-Cloud-Umgebungen in einer zentralen Ansicht verfolgen können. Sorgt für ein kontinuierliches Monitoring der Compliance, mit benutzerdefinierten oder fertig nutzbaren Vorlagen und audit-fähigen Reports für Standards wie FFIEC, DSGVO, HIPAA, PCI DSS und SOC2.
Schutz älterer Systeme	Sophos Firewall Sophos SD-RED	Indem ein SD-RED vor das gefährdete Gerät geschaltet wird, kann es den gesamten Datenverkehr zur Überprüfung an eine schützende Sophos Firewall leiten. Wenn Ihre Netzwerktopologie sehr flach ist, müssen Sie vermutlich kleinere Änderungen an den IP-Adressschemata und der möglichen Switch-Topologie vornehmen. Unsere technischen Experten erörtern gerne Ihre Anforderungen und beraten Sie, wie Sie dies konkret umsetzen können.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2023-04-17 CC (PS)

SOPHOS