

Sophos-Produkte für Fertigung und Produktion SOPHOS

Mit der Industrie 4.0 wurde für produzierende Unternehmen eine neue Ära eingeläutet. Intelligente Fabriken, die mit industriellen IoT-Geräten, Robotik und moderner Analysetechnologie ausgestattet sind, revolutionieren den Fertigungsbetrieb. Die Vorteile sind zahlreich: Kosteneinsparungen, höhere Effizienz und einfachere Bedienung. Allerdings erhöhen Altsysteme, schnelle Digitalisierung, IT/OT-Konvergenz und das komplexe Lieferkettennetz die Angriffsfläche in diesem Bereich.

Sophos ermöglicht Fertigungs- und Produktions-Unternehmen mit seinen Next-Gen-Services und -Produkten, schneller auf Bedrohungen zu reagieren und ihr komplettes Sicherheitsmanagement mit einem einzigen Anbieter zu konsolidieren. Dieses Dokument bietet einen allgemeinen Überblick darüber, wie Sophos-Lösungen diese Unternehmen dabei unterstützen, ihre Cybersecurity-Anforderungen zu erfüllen und einen unterbrechungsfreien Betrieb zu gewährleisten.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Sicherung des Zugangs zu kritischen industriellen Steuerungssystemen	Sophos ZTNA	Überprüft kontinuierlich die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Anwendungen und Daten gewährt wird.
	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.
	Sophos Firewall	Unterstützt flexible Optionen zur mehrstufigen Authentifizierung, einschließlich Verzeichnisdiensten für den Zugriff auf wichtige Systembereiche.
Schutz geistigen Eigentums vor Diebstahl	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 Intercept X	Minimiert bekannte Schwachstellen und stoppt die neuesten Cybersecurity-Bedrohungen wie Ransomware, dateilose Angriffe, Exploits und Malware auf Ihren Endpoints. Die Data Loss Prevention (DLP)-Funktionen erkennen Ihre sensiblen Daten und verhindern deren Weitergabe per E-Mail, Upload und Kopie.
	Sophos Firewall	Die Sophos Firewall mit Security Heartbeat™ kann kontinuierlich wichtige Informationen zu verdächtigen Ereignissen im gesamten erweiterten IT-System austauschen. Erkennung mit automatischer und nahezu sofortiger Isolierung kompromittierter / nicht autorisierter Endpoints. So ist sichergestellt, dass diese Endpoints keine vertraulichen Daten an einen Command-and-Control-Server senden. Zudem wird die Reaktionszeit bei Sicherheitsvorfällen verkürzt.
	Sophos Mobile	Dank flexibler Compliance-Regeln lässt sich der Gerätestatus überwachen. Im Falle eines kompromittierten Geräts wird der Zugriff auf sensible Daten automatisch verweigert. Eine Vielzahl von Geräteverwaltung-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 ZTNA	Überprüft die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Ressourcen gewährt wird.
	Sophos Email	Bietet die Möglichkeit, DLP-Richtlinien mit mehreren Regeln für Benutzer zu erstellen, damit sensible Daten geschützt bleiben. Vertrauliche Inhalte werden dabei in allen E-Mails und Anhängen erkannt. Außerdem werden vertrauliche Daten nahtlos verschlüsselt, um Sicherheitsverletzungen zu verhindern.
	Sophos Managed Detection and Response (MDR)	Stoppt Datenverluste durch Angriffsaktivitäten mittels 24/7 Monitoring der Umgebung sowie Analyse und Beseitigung schädlicher Aktivitäten.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Schutz vor internen Bedrohungen	Sophos Firewall	<p>Schützt Ihre vertraulichen Daten vor versehentlicher oder vorsätzlicher Offenlegung mit vollständiger Richtlinienkontrolle über Webkategorien, Anwendungen, Wechselmedien und Mobilgeräte, die in Ihrem Netzwerk verwendet werden.</p> <p>Gibt Aufschluss darüber, wer die riskantesten Benutzer und Anwendungen sind, um sicherzustellen, dass Ihre Richtlinien durchgesetzt werden, bevor Ihre Sicherheitssysteme kompromittiert werden – mit aussagekräftigen Informationen vom Sophos User Threat Quotient (UTQ).</p> <p>Bietet branchenweit die meisten Optionen zur Benutzerauthentifizierung, einschließlich Active Directory Integration, und unsere einzigartige benutzerfreundliche „Synchronized User ID“-Lösung, mit der sich die Benutzeridentität auf sämtlichen Firewalls und Endpoints einfach und reibungslos ermitteln lässt. Dies ermöglicht einen präzise gesteuerten, differenzierten Benutzerzugriff, wodurch sowohl der Zugriff externer Angreifer als auch vorsätzlich handelnder Mitarbeiter auf sensible Systeme oder Daten unterbunden wird.</p>
	Sophos Cloud Optix	<p>Setzt verschiedene Aktionen mit Sophos AI in Beziehung zueinander, um bei Zugriffen auf Konsolen von Cloud-Anbietern ungewöhnliche Muster und Orte nahezu in Echtzeit zu erkennen. So können Sie Identitätsdiebstahl und missbräuchliche Nutzungen von Zugangsdaten einfacher feststellen. Ein praktisches IAM-Visualisierungs-Tool verschafft einen umfassenden Überblick über IAM-Beziehungen, sodass Ihre IT-Teams überprivilegierte Zugriffe sofort erkennen und adäquate IAM-Richtlinien erstellen können.</p>
Minimierung der Angriffsfläche zum Gewährleisten unterbrechungsfreier Fertigungsabläufe	Sophos Firewall	<p>Verfügt über integrierten Web-, E-Mail- und Zero-Day-Schutz zur effizienten Abwehr komplexer Malware-Bedrohungen. Angriffsversuche durch Zero-Day-Malware, APT und Ransomware werden so zuverlässig unterbunden.</p>
	Sophos XDR	<p>Berücksichtigt 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.</p>
	Sophos Managed Detection and Response (MDR)	<p>Sophos MDR erkennt und analysiert verdächtige Ereignisse in der gesamten Sicherheitsumgebung, um Bedrohungen zu identifizieren und geeignete Reaktionsmaßnahmen zu ergreifen. Daten werden u. a. aus Endpoint-, Netzwerk-, Identitäts-, und E-Mail-Quellen gesammelt und mithilfe leistungsstarker KI-Tools, Threat Intelligence und Cyberexperten korreliert, um die Auswirkungen zu ermitteln und Reaktionsmaßnahmen abzuleiten.</p>
Schutz vor Phishing-Angriffen	Sophos Email	<p>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.</p>
	Sophos Phish Threat	<p>Schult und testet Mitarbeiter durch automatische Angriffssimulationen und qualitativ hochwertige Security-Awareness-Trainings auf Phishing, Diebstahl von Zugangsdaten und Anhangsgriffe und liefert aussagekräftige Reporting-Daten.</p>
	Sophos Intercept X	<p>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.</p>

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Abwehr von komplexer Malware und Bedrohungen	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. Umfasst ein Next-Gen IPS, das über ein einheitliches, von den SophosLabs unterstütztes Signaturformat modernsten Schutz vor Hackern und Angriffen bietet.
	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 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. Endpoint-Protection-Richtlinien zur Anwendungskontrolle beschränken die Verwendung nicht autorisierter Anwendungen. Server Lockdown erlaubt nur die Ausführung vertrauenswürdiger Anwendungen auf der Positivliste und zugehöriger Dateien.
	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.
	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 Cloud Optix	Sorgt für ein kontinuierliches Monitoring der Konfigurationsstandards, um Abweichungen zu erkennen. So können Sie versehentliche oder mutwillige Manipulationen in der Ressourcenkonfiguration verhindern, erkennen und automatisch korrigieren.
	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.
Reduzierung von Risiken durch Drittanbieter	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 cloudbasierte 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.
	Sophos Intercept X Advanced with XDR	Bietet u. a. mit KI, Anti-Exploit-Technologie, Verhaltensschutz und Anti-Ransomware umfassenden Schutz vor Bedrohungen, die sich über Drittanbieter Zugriff verschaffen. Die leistungsstarken XDR-Funktionen erkennen und priorisieren verdächtige Aktivitäten automatisch. Außerdem lässt sich Ihr gesamter Endpoint- und Server-Bestand schnell auf potenzielle Bedrohungen durchsuchen.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Schutz dezentraler Fertigungsunternehmen	Sophos Secure Access Portfolio	Dieses Portfolio umfasst Sophos ZTNA für einen sicheren Anwendungszugriff, Sophos SD-RED Remote Ethernet Devices zur sicheren Erweiterung Ihres Netzwerks auf Zweigstellen und Remote-Geräte, Sophos Wireless Access Points für einfache und sichere WLANs sowie Sophos Switch für sicheren Zugriff im LAN. Alles wird über eine zentrale cloudbasierte Security-Plattform verwaltet – Sophos Central.
	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.
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.
Schutz von Altsystemen	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