Sophos-Produkte für den Einzelhandel

Einzelhändler speichern und verarbeiten eine Vielzahl sensibler Kundendaten und Zahlungsinformationen. Einzelhandelsunternehmen jeder Größe stehen daher im Fokus von Cybersecurity-Angreifern, die mittels Phishing, Credential Stuffing, Ransomware-, DDoS- und Supply-Chain-Angriffen versuchen, Zugang zu Systemen sowie wertvollen Kreditkartendaten und Zahlungsinformationen zu erlangen. Solche Angriffe können bei Nichteinhaltung gesetzlicher und branchenspezifischer Auflagen wie der DSGVO und dem PCI DSS nicht nur hohe Geldstrafen, sondern auch empfindliche Daten-, Finanz- und Reputationsverluste nach sich ziehen.

Dieses Dokument bietet einen allgemeinen Überblick darüber, wie Sophos-Lösungen Einzelhandelsunternehmen dabei unterstützen, ihre individuellen Cybersecurity-Anforderungen zu erfüllen sowie die Einhaltung gesetzlicher Vorschriften und branchenüblicher Verfahren zu vereinfachen.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Schutz gespeicherter vertraulicher Informationen wie Kreditkartendaten und private Kundendaten	Sophos Firewall	Unterstützt flexible Optionen zur mehrstufigen Authentifizierung, einschließlich Verzeichnisdiensten für den Zugriff auf wichtige Systembereiche. Die Sophos Firewall mit Security Heartbeat™ ermöglicht es, wichtige Informationen zu verdächtigen Ereignissen im gesamten IT-System kontinuierlich auszutauschen. 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 Firewall Sophos Intercept X Sophos Intercept X for Server	Die Data Loss Prevention(DLP)-Funktionen der Sophos-Produkte erkennen Ihre sensible Daten und verhindern deren Weitergabe per E-Mail, Upload und Kopie.
	Sophos Managed Detection and Response (MDR)	Stoppt Datenverluste durch Angriffsaktivitäten mittels 24/7 Monitoring der Umgebung sowie Analyse und Beseitigung schädlicher Aktivitäten.
	Sophos Intercept X Sophos Intercept X for Server	Minimieren bekannte Schwachstellen und stoppen 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 Central Device Encryption	Zahllose Notebooks gehen täglich verloren oder werden gestohlen. Daher ist eine Festplatten-Verschlüsselung als erste Verteidigungslinie gegen Verlust oder Diebstahl von Geräten so entscheidend. Schützt Geräte und Daten mit leistungsstarker Festplatten-Verschlüsselung für Windows und macOS. Überprüft den Verschlüsselungs-Status des Geräts und weist die Compliance nach.
	Sophos ZTNA	Überprüft die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Ressourcen gewährt wird.
	Sophos Email	Verhindert Datenverluste durch die Möglichkeit, DLP-Richtlinien mit mehreren Regeln für Gruppen und einzelne Benutzer zu erstellen, damit sensible Daten geschützt bleiben. Vertrauliche Inhalte werden dabei in allen E-Mails und Anhängen erkannt.
	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

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Schutz vertraulicher Daten während der Übertragung	Sophos Email	Verschlüsselt Nachrichten und fügt digitale Signaturen hinzu, um die Absenderidentität mit S/MIME zu überprüfen, und bietet darüber hinaus auch anpassbare Verschlüsselungsoptionen, u. a. TLS-Verschlüsselung, Verschlüsselung von Anhängen und Nachrichten (PDF und Office) oder vollständige Web-Portal-Verschlüsselung (Add-on).
	Sophos Firewall	Ermöglicht eine Zwei-Faktor-Authentifizierung für VPN-Verbindungen, mit RADIUS/TACACS-Integration.
	Sophos Wireless	Stellt dynamisch verschlüsselte WLAN-Verbindungen zum Schutz Ihrer Daten während der Übertragung in Netzwerken und auf Hotspots her, die von Sophos verwaltet werden.
Schutz verteilter Einzelhandelsumgebungen	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.
Minimierung des Risikos von Supply-Chain-Angriffen	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 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.
Sicherheit für drahtlose Netzwerke	Sophos Wireless	Schützt die wachsende Anzahl von Mobilgeräten im Einzelhandel und bietet mehr Transparenz über den Integritätsstatus Ihrer WLAN-Netzwerke und Clients, die sich mit dem Netzwerk verbinden. Auf einen Blick sehen Sie hier potenzielle Bedrohungen wie etwa Rogue APs, und Clients mit Compliance- oder Konnektivitätsproblemen lassen sich dank modernster Diagnosefunktionen einfach und schnell ermitteln. So können Probleme schnell und einfach erkannt und behoben werden. 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. Rogue AP Detection klassifiziert benachbarte WLANs, um Bedrohungen zu erkennen und Unternehmen vor Infiltrierungsversuchen zu schützen.
Verhindern von BEC-Betrug (Business Email Compromise)	Sophos Email	Blockiert Business-Email-Compromise-Angriffe und Versuche, falsche Identitäten vorzutäuschen. Verwendet dazu „Natural Language Processing (NLP)", eine Sonderform des Machine Learning. Für zusätzlichen Schutz enthält Sophos Email auch einen Setup-Assistenten, der mit AD Sync integriert ist. So werden automatisch die Personen innerhalb eines Unternehmens ermittelt, deren Identitäten für Angriffe missbraucht werden könnten. Alle eingehenden E-Mails werden auf Namensänderungen überprüft, die mit diesen Benutzern in Verbindung stehen. So wird der Schutz vor Phishing-Betrügern nochmals verstärkt.
Schutz vor Phishing-Scams	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.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Schutz vor Angriffen auf POS-Systeme	Sophos Intercept X Sophos Intercept X for Server	Exploit Prevention-Funktionen verhindern, dass Hacker Schwachstellen in Anwendungen und Betriebssystemen ausnutzen. Sophos Server Workload Protection scannt Ihr System automatisch auf bekannte erwünschte Anwendungen und setzt nur diese auf die Positivliste. Die Ausführung nicht autorisierter Anwendungen auf dem System wird blockiert.
	Sophos Cloud Optix	Überwacht Ihre Multi-Cloud-Umgebungen kontinuierlich, um unzulässige Aktivitäten, Schwachstellen und Fehlkonfigurationen zu erkennen, und zeigt detaillierte Schritte zur Bereinigung, um Ihre Cloud-POS-Systeme noch besser zu schützen.
	Sophos XDR	Bietet durch Berücksichtigung umfangreicher Netzwerk-, E-Mail-, Cloud- und mobilen Datenquellen maximale Transparenz über Ihre Cybersecurity Posture und hilft Ihnen, Systeme und Geräte mit fehlenden Patches oder veralteter Software zu ermitteln.
	Sophos Managed Detection and Response (MDR)	Überwacht kontinuierlich Signale aus Ihrer gesamten Sicherheitsumgebung, damit Sie potenzielle Cybersecurity-Ereignisse schnell und genau erkennen können. Erkennt, analysiert und korreliert ungewöhnliche Verhaltensweisen und die Verwendung von Code, um schädliche Aktivitäten zu identifizieren und den Vorfall schnell zu beheben.
Schutz vor internen Bedrohungen	Sophos Firewall	Schützt Ihre vertraulichen Daten vor versehentlicher oder vorsätzlicher Offenlegung mit vollständiger Richtlinienkontrolle über Webkategorien, Anwendungen, Wechselmedien und Mobilgeräte, die in Ihrem Netzwerk verwendet werden. 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). 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.
	Sophos Cloud Optix	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.
Abwehr von komplexer Malware und Bedrohungen	Sophos Firewall	Umfasst ein Next-Gen IPS, das über ein einheitliches, von den SophosLabs unterstütztes Signaturformat modernsten Schutz vor Hackern und Angriffen bietet. Erkennt dank der branchenführenden Machine-Learning-Technologie von Sophos (unterstützt von SophosLabs Intelix) neueste Ransomware und unbekannte Bedrohungen, bevor sie in Ihr Netzwerk gelangen. Die Synchronized-Security-Funktion Lateral Movement Protection verhindert, dass Bedrohungen oder Hacker auf andere System übergreifen, Daten stehlen oder Informationen zurück an den Host melden.
	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.
	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 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.
	Sophos Cloud Optix	Sorgt für ein kontinuierliches Monitoring der Konfigurationsstandards, um Abweichungen zu erkennen. So können Sie versehentliche oder mutwillige Änderungen in der Ressourcenkonfiguration verhindern, erkennen und automatisch korrigieren.

ANFORDERUNG	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
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.
Einhaltung von Richtlinien und Vorschriften	Sophos Central	Bietet flexible Reporting-Tools, die eine Visualisierung der Netzwerkaktivität und der Sicherheit über einen längeren Zeitraum ermöglichen. Neben einer Reihe von integrierten Compliance-Reports sind auch einfache Tools zum Erstellen eigener benutzerdefinierter Reports enthalten.
	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 auditfähigen Reports für Standards wie FFIEC, DSGVO, HIPAA, PCI DSS und SOC2.

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

2023-04-27 RC-DE (PS)

SOPHOS