# Sophos Email

SOPHOS
Cybersecurity delivered.

## Produkt- und Lizenzierungsübersicht

| | Lizenz | Funktionsbeschreibung | Sophos Email Standard | Sophos Email Advanced |
|---|---|---|---|---|
| | Kompatible E-Mail-Service-Provider | Kompatibel mit allen E-Mail-Services, einschließlich Google Workspaces Gmail und Microsoft 365:<br>• Microsoft Exchange Online und Microsoft 365<br>• Microsoft Exchange 2003 oder höher<br>• Google Workspaces Gmail<br>Nicht nur diese Plattformen werden unterstützt – es ist lediglich eine einfache MX-Konfiguration erforderlich, um Sophos Email mit jedem beliebigen E-Mail-Dienst kompatibel zu machen, bei dem Sie die Domäne besitzen und die DNS-Einträge steuern. | ✓ | ✓ |
| | Integration von Microsoft 365 Mailflow-Regeln | Über die Sophos-Central-Konsole wird eine direkte Verbindung zwischen den Sophos-Mailflow-Regeln und Microsoft 365 hergestellt, ohne dass es zu Verzögerungen beim Schutz kommt oder MX-Einträge umgeleitet werden müssen. So werden alle E-Mails schneller verarbeitet – ohne Beeinträchtigung des leistungsstarken Schutzes.<br>Verfügbar für Kunden mit Sophos Email Advanced, die Microsoft 365 nutzen | | ✓ |
| | Active Directory Sync und Azure Active Directory Sync | Mit Microsoft Active Directory Sync (AD Sync) und Azure AD Sync können Unternehmen lokale Active Directory- und Exchange-Umgebungen einfach in die Cloud migrieren.<br>• Automatische Synchronisierung von Benutzern mit Sophos Email per AD-Synchronisierung<br>• Eine automatische Aktualisierung von AD-Daten wird vollständig unterstützt, wenn Unternehmen komplett auf eine Cloud-Infrastruktur umgestellt haben | ✓ | ✓ |
| | Manuelle Eingabe von Alias-Datensätzen | Administrator-Zugriff zum manuellen Hinzufügen von E-Mail-Adressen-Alias-Datensätzen, wenn Active Directory nicht verfügbar ist | ✓ | ✓ |
| | Self-Service-Portal für Endbenutzer | Sophos Email gibt Ihren Endbenutzern Zugriff auf die folgenden Tools:<br>• E-Mails in Quarantäne verwalten (E-Mails annehmen/ablehnen)<br>• Regeln für „Zulassen"-/„Blockieren"-Listen bearbeiten<br>• Bei Ausfällen Anzeige von Nachrichten in Notfall-Posteingang | ✓ | ✓ |
| | Richtlinien auf Domänen-, Gruppen- und Benutzer-Ebene | In Minutenschnelle lassen sich individuelle E-Mail-Sicherheitsrichtlinien für Einzelpersonen, Gruppen oder die gesamte Domäne erstellen. | ✓ | ✓ |
| | Rechenzentrumsstandorte | Erfüllen Sie Compliance-Vorschriften und verbessern Sie das Enduser-Erlebnis, indem Sie sich gezielt für eines unserer globalen Rechenzentren entscheiden:<br>• UK<br>• USA<br>• Deutschland | ✓ | ✓ |
| UNTERBRECHUNGSFREIER E-MAIL-ZUGRIFF | Spooling verhindert, dass E-Mails verloren gehen* | Bei einer Störung Ihres Microsoft- oder Google-Cloud-E-Mail-Service werden die E-Mails des Empfängers automatisch von Sophos Email in die Warteschlange verschoben und zugestellt, sobald der Service wieder verfügbar ist – mit einer Wiederholungsperiode von fünf Tagen. | ✓ | ✓ |
| | Benutzerzugriff auf 24-Stunden-Notfall-Posteingang* | Der Lesezugriff auf E-Mails in der Warteschlange wird über einen 24/7-Notfall-Posteingang innerhalb des Endbenutzer-Portals bereitgestellt. | ✓ | ✓ |
| | Administrator-Warnmeldungen* | Bei Ausfall eines Cloud-E-Mail-Service-Providers werden Benachrichtigungen versendet, falls E-Mails nicht zu einem Server/Service zugestellt werden können. | ✓ | ✓ |

| | Lizenz | Funktionsbeschreibung | Sophos Email Standard | Sophos Email Advanced |
|---|---|---|---|---|
| BEDROHUNGSSCHUTZ | Live-Updates stoppen die neuesten Bedrohungen | Mit Unterstützung der SophosLabs stellt Sophos Email Live-Updates zur Verfügung, die vor neuesten Bedrohungen schützen. | ✓ | ✓ |
| | Spam-, Virus- und Phishing-Erkennung | Filtern eingehender und ausgehender E-Mails zum Blockieren unerwünschter E-Mails:<br>• Reputation Filtering blockiert Spam zu 90 %<br>• Unsere Antispam-Engine fängt alle übrigen Bedrohungen ab – auch die neuesten Phishing-Angriffe<br>• Unsere Next-Generation-Reputation-Filtering-Technologie „Sender Genotype" eliminiert Botnet-Spam auf IP-Verbindungsebene mittels Kontrolle von Verbindungsanfragen und Ablehnen von Anfragen mit Anzeichen für Botnet-Verbindungen<br>• Sophos Delay Queue schützt vor Snow Shoe Spam | ✓ | ✓ |
| | E-Mail-Quarantäne | Mit den benutzerfreundlichen vorkonfigurierten Kontrollen von Sophos Email richten Sie Ihre Richtlinien für die Nachrichten-Quarantäne in Sekundenschnelle ein und schützen Ihr Unternehmen im Handumdrehen.<br>Im Endbenutzer-Portal können Benutzer E-Mails dann bei Bedarf selbst freigeben. E-Mail-Quarantäne-Digests bieten eine tägliche Zusammenfassung der in die Quarantäne verschobenen E-Mails mit der Option, E-Mails direkt vom Posteingang freizugeben. | ✓ | ✓ |
| | „Erlauben/ Blockieren"-Listen | Mit der Richtlinie „Zugelassene und blockierte Absender" können Administratoren Nachrichten an oder von bestimmten E-Mail-Adressen, IP-Adressen und Domänen beschränken. Es werden auch Platzhalter unterstützt, sodass Sie Top-Level-Domänen auf Länderebene blockieren können. Dank Smart-Bannern können Benutzer ihre individuellen Listen zum Erlauben bzw. Blockieren von Absendern in der E-Mail selbst aktualisieren. Die Verwaltung dieser Listen ist über das Self-Service-Portal möglich. | ✓ | ✓ |
| | Eingehende SPF-, DKIM- und DMARC-Authentifizierung | • Sender Policy Framework (SPF) erkennt IP-Adressen mit der Berechtigung, E-Mails von der Domäne aus zu verschicken.<br>• Domain Keys Identified Mail (DKIM) liefert die kryptografische Bestätigung, dass eine E-Mail tatsächlich vom Absender stammt und nicht manipuliert wurde<br>• Domain Message Authentification Reporting & Conformance (DMARC) ergreift die richtigen Maßnahmen, wenn eine E-Mail die SPF-oder DKIM-Prüfung nicht bestanden hat | ✓ | ✓ |
| | Prüfung auf Header-Anomalien | • Header Anomaly Detection erkennt, ob der angezeigte Name des Absenders mit einem Ihrer internen Benutzer übereinstimmt. | ✓ | ✓ |
| | Schutz nach der Zustellung für Microsoft 365 | Kontinuierlicher Schutz nach der Zustellung für Microsoft 365 entfernt automatisch Phishing-E-Mails mit neu infizierten URLs, sobald sich der Bedrohungsstatus ändert. | | ✓ |
| | Phishing Impersonation Protection | • Abgleich des angezeigten Namens eingehender E-Mails mit dem angezeigten Namen häufig missbrauchter Namen von Cloud-Service-Anbietern und wichtigen Personen (VIPs) im Unternehmen, um etwaige Übereinstimmungen zu ermitteln<br>• Analyse von Look-alike-Domänen, um Domänen-Namen zu erkennen, die der Unternehmens-Domäne ähneln<br>• Verdächtige Nachrichten können blockiert, in die Quarantäne verschoben, mit einer Betreffzeilen-Warnung markiert oder mit einem Banner versehen werden, der einen Direktlink zur Sperrliste auf Benutzerebene enthält | | ✓ |
| | Time-of-Click URL Protection | URL-Umschreibung zum Überprüfen der Website-Reputation von E-Mail-Links vor der Zustellung und auch wenn Sie klicken – damit werden verschleierte, verzögerte Angriffe abgewehrt | | ✓ |
| | Sophos Sandbox | Cloud-basierte Sandbox, die sowohl bekannte als auch unbekannte Malware und unerwünschte Anwendungen vor der Ausführung erkennen kann | | ✓ |
| INFORMATIONSSCHUTZ | E-Mail-Verschlüsselung (TLS, S/MIME, Push-basiert) | Nachrichtentexte und Anhänge werden automatisch auf sensible Daten gescannt. So können Sie mit wenigen Klicks Richtlinien zum Blockieren oder Verschlüsseln von Nachrichten einrichten. Alternativ können Sie Benutzern auch die Möglichkeit geben, E-Mails über unser M365-Add-in selbst zu verschlüsseln.<br>• Push-basierte Verschlüsselung schützt die gesamte E-Mail oder nur Anhänge<br>• Erzwungene TLS-Verschlüsselung verhindert das Abhören von Nachrichten bei der Übertragung<br>• Hinzufügen einer digitalen Signatur, um die Absender-Identität mit S/MIME zu überprüfen | | ✓ |
| | E-Mail-Verschlüsselung (Pull-basiert) | Mit der im Rahmen von Sophos Email Advanced optional erhältlichen vollständigen Web-Portal-Verschlüsselung können Benutzer ihre Nachrichten in einem sicheren Webportal verwalten, lesen und beantworten. | | **Add-on** |
| | Data Loss Prevention | Data-Loss-Prevention- und Content-Control-Funktionen bieten mit richtlinienbasierter E-Mail-Verschlüsselung leistungsstarken Schutz vor Datenpannen. Erstellen Sie DLP-Richtlinien mit mehreren Regeln für Gruppen und einzelne Benutzer, damit sensible Daten geschützt bleiben. Finanzdaten, vertrauliche Inhalte, Gesundheitsinformationen sowie personenbezogene Daten werden dabei in allen E-Mails und Anhängen erkannt. | | ✓ |

*Funktion nicht verfügbar mit Integration von Microsoft 365 Mailflow-Regeln.


22-02-19 LG-DE (PS)

SOPHOS