SOPHOS

Security made simple.

Sophos Mobile 7

Feature-Matrix

	Bereitstellung		Geräteplattform			
	Verwaltung über Sophos Central	Installation vor Ort	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Server						
Administrationsbenutzeroberfläche						
Benutzerfreundliche Weboberfläche	✓	✓	✓	✓	✓	✓
Flexibles Dashboard mit 23 unterschiedlichen Widgets	✓	✓	✓	✓	✓	✓
Flexible Filter	✓	✓	✓	✓	✓	✓
Rollenbasierter Zugriff	✓	✓	✓	✓	✓	✓
Mandantenfähigkeit		✓	✓	✓	✓	✓
Sophos Central Partner Dashboard für Managed Service Provider	✓		✓	✓	✓	✓
Kommunikation vom Superdamin zu allen Mandanten (Administrations- und Self-Service-Portal-Oberfläche)		✓	✓	✓	✓	✓
Technische Benachrichtigungen von Sophos	✓	✓	✓	✓	✓	✓
Senden von Textnachrichten (per APNs, GCM, Baidu, WNS)	✓	✓	✓	✓	✓	✓
Individuelle Anpassung des Anmeldebildschirms		✓	✓	✓	✓	✓
Self-Service-Portal						
Registrierung neuer Geräte	✓	✓	✓	✓	✓	✓
Gerätezurücksetzung	✓	✓	✓	✓	✓	✓
Gerätesperrung	✓	✓	✓	✓	✓	
Geräteortung	✓	✓	✓	✓	✓	✓
Passwortzurücksetzung für Device, App Protection (Android), Sophos Container (iOS, Android)	✓	✓	✓	✓	✓	
Auslösen von Geräte-Check-in	✓	✓	✓	✓	✓	✓
Außerbetriebsetzung von Gerät (einschließlich Zurücksetzen von Unternehmensdaten auf iOS, Samsung, LG, Sony und Windows 10 Mobile)	✓	✓	✓	✓[5,8,9]	✓	✓
Löschen außer Betrieb gesetzter Geräte aus dem Inventar	✓	✓	✓	✓	✓	✓
Überwachung von Gerätestatus und Compliance-Informationen	✓	✓	✓	✓	✓	✓
Nutzungsrichtlinie bei Registrierung neuer Geräte anzeigen	✓	✓	✓	✓	✓	✓
Anzeige von Nachricht nach Registrierung	✓	✓	✓	✓	✓	✓
Kontrolle der Registrierung nach Art des Betriebssystems	✓	✓	✓	✓	✓	✓
Konfiguration von maximaler Gerätezahl pro Benutzer	✓	✓	✓	✓	✓	✓
Unternehmensspezifische Konfiguration von Befehlen verfügbar für Benutzer	✓	✓	✓	✓	✓	✓
Individuelle Anpassung des Anmeldebildschirms		✓	✓	✓	✓	✓
Benutzerverzeichnis und -verwaltung						
Umfassende Passwortrichtlinien	✓	✓	✓	✓	✓	✓
Benutzerseitige Passwortwiederherstellung	✓	✓	✓	✓	✓	✓
Internes Benutzerverzeichnis einschließlich Batch-Upload-Funktion	✓	✓	✓	✓	✓	✓
Integration von Microsoft ActiveDirectory	✓	✓	✓	✓	✓	✓
Integration von Novell eDirectory		✓	✓	✓	✓	✓
Integration von Lotus Notes Directory		✓	✓	✓	✓	✓
Integration von Red Hat Directory		✓	✓	✓	✓	✓
Integration von Zimbra Directory		✓	✓	✓	✓	✓
Regeln zur Durchsetzung der Geräte-Compliance						
Gruppenzuweisung oder eigentumsbasierte Compliance-Regeln	✓	✓	✓	✓	✓	✓
Analysen zu Compliance-Verstößen	✓	✓	✓	✓	✓	✓
Gerät unter Verwaltung	✓	✓	✓	✓	✓	✓
Jailbreak-/Routing-Erkennung	✓	✓	✓	✓		
Verschlüsselung erforderlich	✓	✓	✓	✓	✓	✓
Passwort erforderlich	✓	✓	✓	✓	✓	✓
Mindestens erforderliche Betriebssystemversion	✓	✓	✓	✓	✓	✓
Maximal erlaubte Betriebssystemversion	✓	✓	✓	✓	✓	✓
Letzte Synchronisierung des Geräts	✓	✓	✓	✓	✓	✓
Letzte Synchronisierung der Sophos Mobile Control App	✓	✓	✓	✓	✓	
Anwendungen auf Blacklist	✓	✓	✓	✓		
Anwendungen auf Whitelist	✓	✓	✓	✓		
Erforderliche Apps	✓	✓	✓	✓		
Installation von unbekannten Quellen (Sideloading) blockieren	✓	✓		✓		
Data-Roaming-Einstellung	✓	✓	✓	✓	✓	
USB-Debugging-Einstellung	✓	✓		✓		
Client-Version Sophos Mobile	✓	✓	✓	✓	✓	
Malware-Erkennung	✓	✓		✓[4]		✓[10]
Erkennung verdächtiger Anwendungen	✓	✓		✓[4]		

© Copyright 2017. Sophos Ltd. Alle Rechte vorbehalten.

	Verwaltung über Sophos Central	Installation vor Ort	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Regeln zur Durchsetzung der Geräte-Compliance (Fortsetzung)						
Erkennung potenziell unerwünschter Anwendungen	✓	✓		✓[4]		
Letzter Malware-Scan	✓	✓		✓[4]		✓[10]
Aktivierung von Ortung für Sophos Mobile Control App	✓	✓	✓	✓	✓	
Vorlagen für HIPAA- und PCI-Compliance-Regeln	✓	✓	✓	✓	✓	✓
Sicherheit						
Verschlüsselte Verbindung zur Web-Oberfläche	✓	✓	✓	✓	✓	✓
Verschlüsselte Kommunikation mit Geräten	✓	✓	✓	✓	✓	✓
Kontrolle des E-Mail-Zugriffs nach Compliance-Status (Exchange-Gateway, Office 365-Zugriffssteuerung)	✓	✓	✓	✓	✓	✓
2FA-Geräteauthentifizierung am Exchange-Gateway (Passwort, Zertifikat)	✓	✓	✓	✓	✓	✓
Definition von erlaubten E-Mail-Clients am Exchange-Gateway	✓	✓	✓	✓	✓	✓
Kontrolle des Netzwerkzugriffs nach Compliance (Generic NAC Interface, Sophos UTM, Cisco ISE, Check Point)		✓	✓	✓	✓	✓
USSD-Code-Schutz (z. B. *#2314#)	✓	✓		✓[4]		
SPAM-Schutz (Anruf, SMS, MMS)	✓	✓		✓[4]		
Schutz vor Schad-Websites (Web-Filterung)	✓	✓		✓[4]		
Schutz von Unternehmensanwendungen mit zusätzlicher Authentifizierung (App Protection)	✓	✓		✓[4]		
Web-Produktivitätsfilterung auf Basis von 14 Kategorien + „Zulassen"-/„Blockieren"-Listen nach IP-Adresse, DNS-Name und IP-Bereich	✓	✓		✓[4]		
Inventar						
Gerätegruppen	✓	✓	✓	✓	✓	✓
Benutzerorientierte Ansicht auf Geräten	✓	✓	✓	✓	✓	✓
Automatische Übertragung von eindeutiger Gerätekennung (IMEI, MEID, UDID) und weiteren Gerätedaten	✓	✓	✓	✓	✓	✓
Automatische Erkennung der Betriebssystemversion	✓	✓	✓	✓	✓	✓
Automatische Auflösung des Gerätemodells in einen benutzerfreundlichen Namen	✓	✓	✓	✓	✓	✓
Echten Gerätenamen als Namen im Inventar verwenden	✓	✓	✓			
Marker für firmeneigene und private Geräte	✓	✓	✓	✓	✓	✓
Kundendefinierte Geräteeigenschaften mit Vorlagenunterstützung	✓	✓	✓	✓	✓	✓
Import/Export von Geräteinformationen	✓	✓	✓	✓	✓	✓
Bereitstellung/Geräteregistrierung						
Geräteregistrierungs-Assistenten für Administratoren	✓	✓	✓	✓	✓	✓
Per E-Mail	✓	✓	✓	✓	✓	✓
Online-Registrierung über das Gerät	✓	✓	✓	✓	✓	✓
Massenbereitstellung (per E-Mail)	✓	✓	✓	✓	✓	✓
Bereitstellung von Apple Configurator		✓	✓			
Apple-DEP-Registrierung (Device Enrollment Program)	✓	✓	✓			
Administrator-Registrierung ohne installierte App (kein iTunes erforderlich)	✓	✓	✓			
Definition von Standard-Rollout-Paketen für private oder firmeneigene Geräte	✓	✓	✓	✓	✓	✓
Automatische Zuweisung von Ausgangsrichtlinien und -gruppen auf Basis der Gruppenzugehörigkeit im Benutzerverzeichnis	✓	✓	✓	✓	✓	✓
Aufgabenverwaltung						
Generieren geplanter Aufgaben	✓	✓	✓	✓	✓	✓
Aufgaben können für einzelne Geräte oder Gruppen generiert werden	✓	✓	✓	✓	✓	✓
Detaillierte Statusverfolgung für jede Aufgabe	✓	✓	✓	✓	✓	✓
Intelligente Strategien für Aufgabenwiederholung	✓	✓	✓	✓	✓	✓
Reporting						
Inventar-Export mit angewendeten Filtern	✓	✓	✓	✓	✓	✓
Export aller Tabellen im System als XLS oder CSV	✓	✓	✓	✓	✓	✓
Malware-Reports (2 verschiedene Reports)	✓	✓	✓	✓	✓	✓
Compliance-Protokolle sämtlicher Administrator-Aktivitäten	✓	✓	✓	✓	✓	✓
Reports zu Compliance-Verstößen (2 verschiedene Reports)	✓	✓	✓	✓	✓	✓
Geräte-Reports (10 verschiedene Reports)	✓	✓	✓	✓	✓	✓
Reports zu Anwendungen (6 verschiedene Reports)	✓	✓	✓	✓	✓	✓
Programmierschnittstelle (API)						
Web Service (REST) API für Geräteinformationen und Bereitstellung von Drittanbietersystemen	✓	✓	✓	✓	✓	✓
Geräte						
Funktionalität Sophos Mobile Control App						
Enterprise App Store	✓	✓	✓	✓	✓	
Anzeige von Compliance-Verstößen (einschließlich Hilfe für den Enduser zur Behebung gemeldeter Compliance-Probleme)	✓	✓	✓	✓	✓	
Anzeige von Server-Nachrichten	✓	✓	✓	✓	✓	
Anzeige von technischem Kontakt	✓	✓	✓	✓	✓	
Gerätesynchronisierung auslösen	✓	✓	✓	✓	✓	
Co-Branding der Sophos Mobile Control App		✓	✓	✓	✓	
Anzeige von Datenschutzinformationen	✓	✓	✓	✓	✓	

© Copyright 2017. Sophos Ltd. Alle Rechte vorbehalten.

	Verwaltung über Sophos Central	Installation vor Ort	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Mobile Application Management						
Installation von Anwendungen (mit oder ohne Benutzerinteraktion, einschließlich verwalteter Anwendungen unter iOS)	✓	✓	✓	✓	✓	
Deinstallation von Anwendungen (mit oder ohne Benutzerinteraktion)	✓	✓	✓	✓		
Liste aller installierten Anwendungen	✓	✓	✓	✓		
Unterstützung von Apples Programm für Volumenlizenzen (Apple Volume Purchase Program, VPP)	✓	✓	✓			
Installation von Anwendungen erlauben/verbieten	✓	✓	✓	✓	✓	
Deinstallation von Anwendungen blockieren	✓	✓		✓[5,8,9]		
Remote-Konfiguration von Unternehmensanwendungen (verwaltete Einstellungen)	✓	✓	✓[2]			
Ausführung bestimmter Anwendungen blockieren (App Blocker)	✓	✓	✓[2]	✓	✓	
Sicherheit						
Erkennung von Jailbreak (iOS)/Rooting (Android)	✓	✓	✓	✓		
Manipulationserkennung	✓	✓	✓	✓	✓	
Schutz vor Diebstahl: Remote-Zurücksetzung	✓	✓	✓	✓	✓	✓
Schutz vor Diebstahl: Remote-Sperrung	✓	✓	✓	✓	✓	
Schutz vor Diebstahl: Geräteortung	✓	✓	✓	✓	✓	
Sicherheit und Komplexität von Passwörtern durchsetzen	✓	✓	✓	✓	✓	✓
Zeit ohne Aktivität (Zeit in Minuten, bis Passwort eingegeben werden muss)	✓	✓	✓	✓	✓	✓
Maximale Anzahl von Versuchen, bis Gerät zurückgesetzt wird	✓	✓	✓	✓	✓	✓
Passwort-Mindestlänge	✓	✓	✓	✓	✓	
Anzahl der letzten Passwörter, die nicht benutzt werden dürfen	✓	✓	✓	✓	✓	✓
Passwort-Ablaufzeit	✓	✓		✓	✓	✓
Mindestlänge von Klein-/Großbuchstaben, buchstabenlosen Zeichen oder Symbolen im Passwort	✓	✓		✓	✓	
Passwortzurücksetzung (Entsperrung)/Administrator definiert neues Passwort	✓	✓	✓	✓	✓	
Activation Lock Bypass (Aktivierungssperre-Umgehung)	✓	✓	✓[2]			
Aktivierung von Speicherverschlüsselung	✓	✓	✓[3]	✓	✓	
Zugriff auf Speicherkarte kann untersagt werden	✓	✓			✓	✓
Aktivierung/Deaktivierung von Datenverschlüsselung auf Gerät	✓	✓		✓	✓	
Installation von unbekannten Quellen (Sideloading) blockieren	✓	✓		✓[5]		
WLAN blockieren	✓	✓	✓[2]	✓[5,8,9]		
Bluetooth blockieren	✓	✓		✓[5]		✓
Datenübertragung via Bluetooth blockieren	✓	✓		✓[6]	✓	✓
Datenübertragung via NFC blockieren	✓	✓		✓[6]	✓	
USB-Verbindungen blockieren	✓	✓			✓	
Kamera blockieren	✓	✓	✓	✓[5]	✓	✓
Schutz von Einstellungen gegen Modifizierung/Entfernung durch den Benutzer	✓	✓	✓			✓
Nutzung von iTunes Store/Google Play/Windows Store erlauben/verbieten	✓	✓	✓	✓[8]	✓	
Nutzung von YouTube App erlauben/verbieten	✓	✓	✓			
Nutzung von Browser erlauben/verbieten	✓	✓	✓	✓	✓	
Anstößige Inhalte erlauben/verbieten	✓	✓	✓			
Zugriff auf Kamera im Sperrbildschirm erlauben/verbieten	✓	✓		✓		
Widgets auf Sperrbildschirm erlauben/verbieten	✓	✓		✓		
Weiterleiten von E-Mails unterbinden	✓	✓	✓			
S/MIME-Durchsetzung	✓	✓	✓			
E-Mail-Nutzung durch Drittanbieter-Apps erlauben/verbieten	✓	✓	✓			
iCloud Autosync erlauben/verbieten	✓	✓	✓			
In Zwischenablage kopieren erlauben/verbieten	✓	✓		✓[5]		
Manuelle WLAN-Konfiguration erlauben/verbieten	✓	✓		✓[5]		
Senden von Absturzdaten an Apple/Google/Samsung/Microsoft (Telemetrie) erlauben/verbieten	✓	✓	✓	✓[5]	✓	✓
Zertifikate von nicht vertrauenswürdigen Quellen erlauben/verbieten	✓	✓	✓		✓	
Automatische WLAN-Verbindung erlauben/verbieten	✓	✓	✓			✓
Freigegebenen Fotostream erlauben erlauben/verbieten	✓	✓	✓			
Zugriff auf Apple Wallet/Passbook im Sperrbildschirm erlauben/verbieten	✓	✓	✓			
Nutzung des Geräts als Hotspot erlauben/verbieten	✓	✓	✓			✓
Konfiguration von Profil-Lebenszeit	✓	✓	✓			
Synchronisierung durch letzte Kontakte erlauben/verbieten	✓	✓	✓			
Siri (iOS) oder Cortana (Microsoft) erlauben/verbieten	✓	✓	✓		✓	✓
Websuche für Siri erlauben/verbieten	✓	✓	✓[2]			
Unterstützung von SCEP-Zertifikatbereitstellung	✓	✓	✓	✓	✓	
„Öffnen mit …"-Funktion zum Austausch von Daten zwischen verwalteten und nicht verwalteten Anwendungen erlauben/verbieten	✓	✓	✓			
Biometrische Lesegeräte (Touch ID) zum Entsperren des Geräts erlauben/verbieten	✓	✓	✓			
Account-Änderung erlauben/verbieten	✓	✓	✓[2]			
Änderung der Einstellungen für mobile Datenverbindungen pro App erlauben/verbieten	✓	✓	✓[2]			
Zugriff auf Control Center im Sperrbildschirm erlauben/verbieten	✓	✓	✓			
Zugriff auf Mitteilungszentrale im Sperrbildschirm erlauben/verbieten	✓	✓	✓		✓	
Zugriff auf die Heute-Ansicht im Sperrbildschirm erlauben/verbieten	✓	✓	✓			
Over-the-air PKI Updates erlauben/verbieten	✓	✓	✓			
Änderung der „Freunde suchen"-Einstellungen erlauben/verbieten	✓	✓	✓[2]			
Host Pairing erlauben/verbieten	✓	✓	✓[2]			

© Copyright 2017. Sophos Ltd. Alle Rechte vorbehalten.

	Verwaltung über Sophos Central	Installation vor Ort	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Sicherheit (Fortsetzung)						
AirDrop erlauben/verbieten	✓	✓	✓[2]			
Kioskmodus erlauben/verbieten	✓	✓	✓[2]	✓[5,8,9]		
iBooks Store erlauben/verbieten	✓	✓	✓			
Einkauf von Büchern mit erotischen Inhalten in iBooks erlauben/verbieten	✓	✓	✓			
iMessage erlauben/verbieten	✓	✓	✓			
Zurücksetzung des Geräts durch den Benutzer erlauben/verbieten	✓	✓		✓[5,8,9]	✓	
Geräteregistrierung über MDM-Verwaltung erlauben/verbieten	✓	✓		✓[5,8,9]	✓	✓
Erstellen von Screenshots durch den Benutzer erlauben/verbieten	✓	✓			✓	
Kopieren/Einfügen durch den Benutzer erlauben/verbieten	✓	✓			✓	
Zugriff auf Websites filtern (Blacklisten) oder Whitelisten von Websites mit Bookmarks	✓	✓	✓[2]			
Blockieren von Betriebssystem-Upgrade	✓	✓		✓[5]		
Gerätekonfiguration						
Microsoft-Exchange-Einstellungen für E-Mails	✓	✓	✓	✓[5,8,9]	✓	✓
IMAP- oder POP-Einstellungen für E-Mails	✓	✓	✓			
LDAP-, CardDAV- und CalDAV-Einstellungen	✓	✓	✓			
Konfiguration von Access Points	✓	✓	✓	✓		
Proxy-Einstellungen	✓	✓	✓			
WLAN-Einstellungen	✓	✓	✓	✓	✓	✓
VPN-Einstellungen	✓	✓	✓	✓[5]		
Root-Zertifikate installieren	✓	✓	✓	✓[5]	✓	✓
Client-Zertifikate installieren	✓	✓	✓	✓	✓	
VPN pro App	✓	✓	✓			
Single Sign-On (SSO) für Drittanbieter-Apps (App Protection) Unternehmens-Webseiten	✓	✓	✓	✓		
Verteilung von Bookmarks (Web Clips)	✓	✓	✓			
Automatischer Empfang von WLAN- und VPN-Einstellungen von Sophos UTM Appliances	✓	✓	✓	✓		
Verwaltete Domänen	✓	✓	✓			
Android Enterprise („Android for Work"): Konfiguration von Passwortrichtlinie	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Konfiguration von Beschränkungen	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Konfiguration von App Protection	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Konfiguration von Application Control	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Konfiguration von Anwendungsberechtigungen	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Konfiguration von Exchange	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Installation von Root-Zertifikat	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Installation von Client-Zertifikat	✓	✓		✓[11]		
Android Enterprise („Android for Work"): Installation von Client-Zertifikat via SCEP	✓	✓		✓[11]		
Samsung Knox: Container-Handling (Erstellen, Sperren, außer Betrieb setzen)	✓	✓		✓[6]		
Samsung Knox: Konfiguration von Beschränkungen	✓	✓		✓[6]		
Samsung Knox: Konfiguration von Exchange	✓	✓		✓[6]		
Samsung Knox: Verwaltung von Container-Passwort	✓	✓		✓[6]		
Samsung Knox: Daten- und Dateisynchronisierung zwischen Know Workspace und persönlichen Bereichen erlauben/verbieten	✓	✓		✓[6]		
Samsung Knox: Iris-Authentifizierung für Knox Workspace erlauben/verbieten	✓	✓		✓[6]		
Informationen zum Gerät						
Interne Speichernutzung (frei/belegt)	✓	✓	✓			
Akkustand	✓	✓	✓	✓		
IMSI (eindeutige Kennnummer) der SIM-Karte	✓	✓	✓	✓	✓	
Aktuell verwendetes Mobilfunknetzwerk	✓	✓	✓	✓		
Roaming-Modus	✓	✓	✓	✓	✓	
Betriebssystemversion	✓	✓	✓	✓	✓	✓
Liste installierter Profile	✓	✓	✓	✓	✓	✓
Liste installierter Zertifikate	✓	✓	✓		✓	✓
Auf dem Gerät erkannte Malware	✓	✓		✓[4]		✓[10]
Remote-Bildschirmfreigabe (AirPlay-Gerät erforderlich)	✓	✓	✓			
Secure Email (mit Sophos Secure Email App)						
Exchange-E-Mail	✓	✓	✓[4]	✓[4]		
Exchange-Kontakte	✓	✓	✓[4]	✓[4]		
Exchange-Kalender	✓	✓	✓[4]	✓[4]		
Räumliche, zeitliche oder WLAN-abhängige Beschränkung	✓	✓	✓[4]	✓[4]		
Kontrolle von Ausschneiden und Kopieren	✓	✓	✓[4]	✓[4]		
Anzeige von Ereignisdetails	✓	✓	✓[4]	✓[4]		
Export von Kontakten auf das Gerät	✓	✓	✓[4]	✓[4]		
Definition von Abwesenheitsnachricht in der E-Mail-Anwendung	✓	✓	✓[4]	✓[4]		
Zentrale Kalenderansicht	✓	✓	✓[4]	✓[4]		
Anti-Phishing-Schutz für Links in E-Mails	✓	✓	✓[4]	✓[4]		

© Copyright 2017. Sophos Ltd. Alle Rechte vorbehalten.

	Verwaltung über Sophos Central	Installation vor Ort	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Corporate Browser (mit Sophos Secure Workspace)						
Surf-Beschränkung auf vordefinierte Unternehmens-Domains	✓	✓	✓[4]	✓[4]		
Vorkonfigurierte Unternehmens-Bookmarks	✓	✓	✓[4]	✓[4]		
Passwort-Manager	✓	✓	✓[4]	✓[4]		
Client- oder Benutzerzertifikate zur Authentifizierung auf Unternehmens-Websites	✓	✓	✓[4]	✓[4]		
Root-Zertifikate	✓	✓	✓[4]	✓[4]		
Beschränkungen von Ausschneiden, Kopieren und Einfügen	✓	✓	✓[4]	✓[4]		
Mobile Content Management (mit Sophos Secure Workspace App)						
Veröffentlichung von Dokumenten über Sophos-Mobile-Server	✓	✓	✓[4]	✓[4]		
Räumliche, zeitliche oder WLAN-abhängige Beschränkung	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: Dropbox	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: Google Drive	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: Microsoft OneDrive – privat und geschäftlich	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: Box	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: Telekom MagentaCloud	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: Egnyte	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: OwnCloud	✓	✓	✓[4]	✓[4]		
Inhaltsspeicherung: WebDAV (z. B. Windows Server, Strato Hi-Drive usw.)	✓	✓	✓[4]	✓[4]		
Benutzerauthentifizierung	✓	✓	✓[4]	✓[4]		
FIPS 140-2-Verschlüsselung mit AES256	✓	✓	✓[4]	✓[4]		
DLP-Einstellung Offline-Ansicht zulassen	✓	✓	✓[4]	✓[4]		
DLP-Einstellung In Zwischenablage kopieren erlauben	✓	✓	✓[4]	✓[4]		
DLP-Einstellung Senden von E-Mails im verschlüsselten Format zulassen	✓	✓	✓[4]	✓[4]		
DLP-Einstellung „Öffnen mit" unverschlüsselt erlauben, einschließlich Senden unverschlüsselter E-Mails	✓	✓	✓[4]	✓[4]		
Hinzufügen von Dateien aus E-Mails oder Download auf Inhalts-App	✓	✓	✓[4]	✓[4]		
Vorhandenen Schlüssel auswählen oder neuen Benutzerschlüssel erstellen	✓	✓	✓[4]	✓[4]		
Integriert mit SafeGuard Encryption für Cloud Storage	✓	✓	✓[4]	✓[4]		
Gemeinsam mit Sophos SafeGuard genutzter Schlüsselring	✓	✓	✓[4]	✓[4]		
Sperrung des Container-Zugriffs auf nicht richtlinienkonformen Geräten	✓	✓	✓[4]	✓[4]		
Call-Home-Anfragen auf Basis von Zeit oder Anzahl der Entsperrungen	✓	✓	✓[4]	✓[4]		
Bearbeiten oder Erstellen von Word-, Excel-, PowerPoint- und Textformat-Dateien	✓	✓	✓[4]	✓[4]		
Kommentieren von PDF-Dateien	✓	✓	✓[4]	✓[4]		
Ausfüllen von PDF-Formularen	✓	✓	✓[4]	✓[4]		
Anzeige von passwortgeschützten HTML5-Dateien im SafeGuard-Format	✓	✓	✓[4]	✓[4]		
Austausch von Dokumenten als passwortgeschützte HTML5-Dateien	✓	✓	✓[4]	✓[4]		
Anti-Phishing-Schutz für Links in Dokumenten	✓	✓	✓[4]	✓[4]		
„Mit Secure Workspace anzeigen"-Zugriff auf verschlüsselte Dokumente von anderen Apps	✓	✓	✓[4]	✓[4]		
App-Entsperrung per biometrischem Lesegerät	✓	✓	✓[4]	✓[4]		
Mobile SDK (zur Einbettung in Anwendungen)						
App-Ablaufdatum	✓	✓	✓[4]	✓[4]		
In App eingebetteter EULA	✓	✓	✓[4]	✓[4]		
App-Passwort (mit SSO für alle SDK-fähigen Apps)	✓	✓	✓[4]	✓[4]		
Räumliche Beschränkung der Anwendung	✓	✓	✓[4]	✓[4]		
Zeitliche Beschränkung der Anwendung	✓	✓	✓[4]	✓[4]		
Sperrung des App-Starts auf gerooteten oder Jailbreak-Geräten	✓	✓	✓[4]	✓[4]		
WLAN für App-Nutzung obligatorisch machen	✓	✓	✓[4]	✓[4]		
Verfügbares Unternehmens-WLAN für App-Nutzung obligatorisch machen	✓	✓	✓[4]	✓[4]		
Telecom-Kostenkontrolle						
Daten bei Roaming deaktivieren	✓	✓	✓	✓[5]	✓	
Sprache bei Roaming deaktivieren	✓	✓	✓	✓[5]		
Synchronisierung bei Roaming kontrollieren	✓	✓		✓[5]		
Konfiguration von APN- oder Bertreibereinstellungen	✓	✓	✓	✓		
Netzwerk-Nutzungsregeln per App	✓	✓	✓			

(1) Gelöscht

(2) Überwachtes Gerät erforderlich

(3) Durch Einrichtung einer PIN oder eines Passworts

(4) Mobile Advanced- oder Central Mobile Advanced-Lizenz erforderlich

(5) Mit Samsung Knox Standard kompatibles Gerät erforderlich und optional Installation eines Plug-ins

(6) Samsung Knox V2.1 oder höher

(7) Gelöscht

(8) Sony-Gerät mit Eignung für MDM API erforderlich

(9) LG GATE-fähiges Gerät erforderlich

(10) Mit Windows Defender

(11) Android for Work

© Copyright 2017. Sophos Ltd. Alle Rechte vorbehalten.