Leistungsbeschreibung & zusätzliche Bedingungen Appvisory Secure App Check /Plus.

1 Allgemeines

Die Telekom Deutschland GmbH (im Folgenden Telekom genannt; www.telekom.de) bietet mit dem Produkt Appvisory Secure App Check/Appvisory Secure Check Plus (die beiden Produktvarianten im Folgenden gemeinsam auch „Produkt“ genannt) dem Kunden eine Dienstleistung mit der er mobile Endgeräte schützt und sensible Unternehmensdaten sichert, indem Apps auf Schwachstellen, Malware und Risken vollautomatisiert in Echtzeit analysiert werden. Der Kunde erhält ein zentrales Admin-Dashboard, das alle Prüfberichte beinhaltet.

Appvisory Secure App Check ist spezialisiert auf die Analyse von Apps und sorgt mit seinem Mobile Application Management dafür, dass schadhafte Apps schon im Vorfeld erkannt und damit gar nicht erst auf das Endgerät und damit ins Firmennetz gelassen werden. So wird das Risiko schadhafter Verbindungen, Datenverluste und DSGVO Verstöße, die durch die Nutzung öffentlicher und interner Apps zwangsläufig entstehen, verringert.

Für die Nutzung von Appvisory Secure App Check hat der Kunde die nachfolgend technischen Voraussetzungen sicherzustellen:

- Internet-Zugang
- aktueller Internet-Browser
- mobile Endgeräte wie Mobiltelefone, Laptops, Tablets
- Registrierung der Endgeräte
- Mobile Device Management (MDM)

Das Produkt bietet mit „Appvisory MDM Connect“ eine automatische Anbindung an eine vom Kunden genutzte MDM Software (Mobile Device Management) via API. Darüber hinaus besteht alternativ die Möglichkeit der Verwendung einer integrierten MDM Variante mit reduziertem Funktionsumfang.

2 Leistungen von Telekom

Die Telekom erbringt im Rahmen der technischen und betrieblichen Möglichkeiten folgende Leistungen:

2.1 Appvisory Secure App Check

Der Basisschutz umfasst die grundlegende Datensicherheitsprüfung von Apps auf Basis der NUCLEUS Engine® Prüftechnologie und beinhaltet folgende Leistungen:

2.1.1 Administrator Konsole
- Service und Hosting in und aus Deutschland
- Administrator-Zugang zur Verwaltungskonsole per Web-Login

2.1.2 APPVIRORY Dashboard
- Darstellung prozentuale Verteilung der Testergebnisse pro Prüftechnologie, auf Basis der aktiven Sicherheitskonfiguration
- Überblick der favorisierten Apps
- Dashboard zur Anzeige der aktiven/inaktiven an einMDM angeschlossene Geräte und Übersicht der Top 10 App-Installationen mit Sicherheitsverstößen (MDM abhängig)

2.1.3 App-Group-Management
- Frei konfigurierbare App-Portfolios auf Grundbasis zur Erstellung von Blacklists, Withelists, individuelle Applisten und Basis der durch APPVISORY geprüften Apps

2.1.4 APP-Risk-Management
- Sicherheitseinstufung der Top_Apps aus den beauftragten offiziellen App Stores auf Basis der DSGVO-konformen Standard-Sicherheitskonfiguration
- Intuitiv verständliche Sicherheitsprüfung von Apps durch ein standardisiertes Bewertungsverfahren
- Risikoeinstufung „kritisch“: Apps sind im Unternehmenseinsatz nicht empfohlen (Blacklist)
- Risikoeinstufung „unkritisch“: Apps sind für den Einsatz im Unternehmen zugelassen (Withelist)
- Veränderungen des Sicherheitsstatus einer App wird im App-Katalog hervorgehoben

2.1.5 Security-Settings-Manager
- Individuell konfigurierbare Sicherheitskonfigurationen für Mobile-Application-Management gemäß unternehmenseigener Sicherheitsrichtlinien und Compliance Anforderungen
- Auswahl verschiedener Sicherheitsrichtlinien auf Basis von unterschiedlicher Regularien (z.B. CWE, DSGVO, FFIEC, FISMA (Low), FISMA (medium), Google CAQ, HIPAA, NIAP, OWASP, PCI)

2.1.6 Sicherheitshistorie
- Sicherheitshistorie der letzten App-Updates im Portfolio der im Portfolio enthaltenen App-Tests

2.1.7 AppScan Sicherheitsprüfungen
- Vollautomatisierte und hoch skalierbare Prüftechnologie zur Risikoeinstufung von mobilen Applikationen
- Prüfung der App-Berechtigungen
- Prüfung potentieller Datenzugriffe
- Prüfungen der potentiellen Zielserver inkl. Serverstandorte
- Prüfung der Verwendung von Transportverschlüsselung und Qualität der Verschlüsselung
- Prüfung der implementierten Drittanbieter-Bibliotheken und Android
- Prüfung auf Sicherheitslücken und bekannte Schwachstellen je nach Betriebssystem

2.1.7.1 Abwehrbare Angriffsszenarien

Übersicht über die verarbeitbaren Daten und die möglichen Zugriffe in Echtzeit.
- Problematische Berechtigungskombinationen z.B. Mikrofon- und Internetzugriff
- Unerwünschte Datenverarbeitungen & Übertragungen z.B. Adressbuch
- Nicht freigegebene integrierte Drittanbieter & Verbindungen z.B. Dropbox
- Identifikation von Geräten mit problematischen App-Installationen

2.1.8 AppScan App-Katalog
- Umfangreicher App-Katalog fortlaufend geprüfter Apps mit mehr als 50.000 business-relevanten Top-Apps
- verfügbare Betriebssysteme: iOS, Android

2.1.9 AppScan Aufwuchsflatrate
- Kostenlose Prüfung aller Apps (bis 15€ netto pro App) im AppScan Prüfverfahren
- Apps ab 15€ netto werden zu Selbstkostenpreis geprüft

2.1.10 Black- & Withelisting
- Vollautomatisierte oder manuelle Zusammenstellung von Applisten auf der Basis der Risikoeinstufung nach aktivierter Sicherheitskonfiguration zur Erstellung einer Basis-Whitelist /Blacklist
- Automatische Synchronisation bei veränderter Risikoeinstufung von Apps aufgrund von Update-Tests

2.1.11 Notifikation Service
- Automatische E-Mail-Benachrichtigung über Veränderungen im App-Katalog und den Gruppenlisten
- individuelle Konfiguration des Benachrichtigungsmodus bzgl. gewünschten Zeitintervallen

2.1.12 Exportfunktionen
- Export von einzelnen Prüfergebnissen und Applisten als CSV, JSON, und PDF zum Einsatz im Unternehmen (z.B. für Intranet-Anbindung)

2.2 Appvisory Secure App Check Plus
Appvisory Secure App Check Plus enthält alle Funktionen von Appvisory App Check und folgende weitere Funktionen:

2.2.1 AppScan+ Sicherheitsprüfungen
Automatisierte statische- und dynamische Analyse während der Ausführung der Apps:
- Überprüfung auf bekannte Schwachstellen und unerwünschte Datenverarbeitungen
- Kommunikation
- Netzwerkverkehrsanalyse
- Datensicherung
  - lokale Datenspeicherung (Orte, Zugriffsrechte)
  - Logs
  - Verwendung von iOS-Keychain
- Verwendete Transportverschlüsselung
  - Verwendete Verfahren und Schlüsselstärken
- Codequalität
- Verhalten während der Runtime
  - Verwendetes Framework
  - Verwendete Berechtigungen
  - Eingebundene Drittanbieter
- abwehrbare Angriffsszenarien
  - Schnelle Übersicht über die zu verarbeitenden Daten, Zugriffe, aufgebaute Serververbindungen und mögliche Schwachstellen
  - Problematische Berechtigungskombinationen z.B. Mikrofon und Internetzugriff
  - Unerwünschte Datenverarbeitung & Übertragungen z.B. Adressbuch
  - Berechtigungsanalyse statische Analyse möglicher genutzter Berechtigungen
  - Codeseitige Schwachstellen z.B. externe Code-Ausführungen, Schwächung der Crypto etc.
  - Compliance-Verstöße

2.3. Appvisory MDM Connect (Schnittstelle)
- Appvisory MDM Connect ermöglicht die Anbindung an eine MDM-Software des Kunden via API (u.a. Ivanti / MobileIron, VMware Workspace ONE, Microsoft Intune) an APPVISORY® (Hinweis: der Funktionsumfang ist abhängig vom MDM-Hersteller ggf. weitere Anbindungen via Service oder .csv import/export sind grundsätzlich möglich).
- Portfolio-Check: Abgleich des im MDM angelegten App-Portfolios mit der APPVISORY® Datenbank
- Abgleich der Inventare der im MDM verwalteten Endgeräte mit der APPVISORY® Datenbank
- Übertragung eines App-Portfolios in die MDM Whitelist / Blacklist, optionale automatische Synchronisation
- Vollautomatisierte Übertragung eines App-Portfolios in den MDM Enterprise App Store, optionale automatische Synchronisation
- Freigabe von Applikationen für im MDM hinterlegte Nutzer
- Eskalation per Push-Benachrichtigung an mobile Endgeräte bei Verstoß gegen die unternehmenseigenen Compliance-Richtlinien

(Genauer Funktionsumfang und weitere Eskalationsstufen je nach MDM-Unterstützung und Konfiguration.)

2.4 Zugang
Der Zugang des Administrators zur Administration und Nutzung der Produkte erfolgt über das Internet.
Voraussetzung für jeden Zugang zur Administration ist die Authentifizierung mittels einer Zugangskennung, bestehend aus Benutzername und Passwort.
Die Zugangskennung bekommt der Administrator des Kunden durch die Telekom mit der Bereitstellung der Leistungen zugesandt.
Auf weitere zusätzliche Angaben zur sicheren ersten Authentifizierung wird der Kunde auf Informationsseiten im Internet hingewiesen.
Die Passwörter können jederzeit von den Administratoren geändert werden; das erste Passwort ist unverzüglich zu ändern.

2.5 Support und Störungsannahme
Die Telekom nimmt unter einer besonderen Servicerufnummer täglich von 0.00 Uhr bis 24.00 Uhr Störungen an und beantwortet allgemeine Fragen zum Betrieb von Appvisory Secure App Check.
Die Telekom stellt dem Kunden weitere Supportleistungen zur Verfügung. Alle Angaben zu diesen Supportleistungen wie u. a. die Servicezeiten und Kontaktdaten können im Internet unter https://cloud.telekom.de/de/hilfe-faq/ abgerufen werden.
Der Support steht nur den Kunden, dem Administrator bzw. dessen Stellvertretern zur Verfügung; die weiteren Nutzer sind nicht supportberechtigt.

2.6 Betriebsfähige Bereitstellung
Die betriebsfähige Bereitstellung der Leistungen der Telekom gilt ab der Registrierung auf der Plattform von APPVISORY mit der Zustellung der für den Zugang erforderlichen Zugangsdaten als erfolgt.

2.7 Betreiben der Server- und System-Komponenten
Alle Server- und Systemkomponenten, die zum Betreiben von Appvisory Secure App Check notwendig sind, werden in einem technisch und organisatorisch abgesicherten, hoch performanten Rechnerverbund innerhalb Deutschlands betrieben, der durch ein Firewall-System vor Angriffen und unberechtigten Zugriffen aus dem Internet geschützt ist. Die Leistungen zum Betrieb stehen mit einer mittleren Verfügbarkeit von 99,0 % im Jahresdurchschnitt zur Verfügung. Die Internet-Anbindung des Rechnerverbundes erfolgt über das Internet Backbone der Telekom mit einer dem Stand der Technik entsprechenden Übertragungsgeschwindigkeit und ist redundant ausgelegt.
Für Betrieb und System-Management gelten folgende Leistungsmerkmale:
- Betriebszeit täglich von 0.00 bis 24.00 Uhr
- Automatische Erkennung von Störungen innerhalb des Rechnerverbundes

2.8 Wartungsfenster
Zu Wartungszwecken – insbesondere für Änderungen und Aktualisierungen der Server-Konfiguration – können die Leistungen von der Plattform außer Betrieb genommen werden (Wartungsfenster). Die Telekom wird den Administrator rechtzeitig vor Inanspruchnahme eines Wartungsfensters Informieren. Die Zeiten der Wartungsfenster fließen nicht in die Berechnung einer Verfügbarkeit ein.

3 Vertragslaufzeit und Kündigung
Das Produkt wird mit einer Mindestvertragslaufzeit von 24 Monaten überlassen und kann zum Ablauf mit einer Frist von sechs (6) Wochen zum Monatsende gekündigt werden. Die Vertragslaufzeit beginnt mit dem Tag der betriebsfähigen Bereitstellung. Wird nicht fristgerecht zum Ablauf der Mindestvertragslaufzeit gekündigt, so verlängert sich die Vertragslaufzeit jeweils um zwölf Monate. Die Kündigungsfrist beträgt in einem solchen Fall weiterhin sechs (6) Wochen zum Monatsende.

4 Besondere Hinweise zum Datenschutz
Appvisory Secure App Check erfordert zwingend die Erhebung von Endgerätekennungen. Hierbei handelt es sich um die IMEI (International Mobile Equipment Identity) und weiteren eindeutigen Kennungen (Device hash). Die Erhebung aller weiteren persönlichen Daten kann vom Kunden in der Console aktiviert bzw. deaktiviert werden. In Betrieben oder Behörden müssen die Mitbestimmungsrechte bei der Nutzung des Produktes sowie die gültigen gesetzlichen Regeln angewendet werden.

5 Preise

Die angegebenen Preise sind Preise ohne Umsatzsteuer (USt); die USt wird in der gesetzlich vorgeschriebenen Höhe zusätzlich berechnet. In der Rechnung werden für die Abrechnung der in Anspruch genommenen Leistungen die Preise ohne USt angegeben. Diese Preise ohne USt werden aufsummiert und sind Grundlage für die Berechnung des Umsatzsteuerbetrages.
Die Lizenzpreise werden auf Basis des aktuellen Lizenzjahres berechnet, wenn innerhalb eines Jahres in eine höhere (Upgrade)oder niedrigere (Downgrade) Staffelung wechselt wird, wird diese Leistungsänderung im darauffolgenden Lizenzjahr berechnet. Ein Downgrade ist erstmals nach 2 Jahren und ein Upgrade auch während der Mindestvertragslaufzeit möglich.

	Preise in EUR ohne USt
Überlassung Appvisory Secure App Check und Appvisory Secure App Check Plus Mindestens werden immer 10 Lizenzen pro Monat berechnet. Je administrierten Mobilfunkgeräte wird eine Lizenz berechnet. Die Anzahl der im jeweiligen Monat abgerechneten Lizenzen ergibt sich aus der Anzahl, der innerhalb des Monats administrierten und neu aufgenommen Mobilfunkgeräte unabhängig von der Dauer der Nutzung in dem Monat. Mobilfunkgeräte, die vom Kunden aus dem Mobile Device Management herausgenommen werden, werden erst ab dem darauffolgenden Monat nicht mehr berechnet.	
Appvisory Secure App Check	
Appvisory Secure App Check S (10 bis 100 Lizenzen)	3,19
Appvisory Secure App Check M (101 bis 500 Lizenzen)	2,97
Appvisory Secure App Check L (501 bis 2.500 Lizenzen)	2,39
Appvisory Secure App Check XL (ab 2501 Lizenzen)	1,28
Appvisory Secure App Check P (öffentlicher Dienst)	1,98
Appvisory Secure App Check Plus	
Appvisory Secure App Check Plus S (10 bis 100 Lizenzen)	4,49
Appvisory Secure App Check Plus M (101 bis 500 Lizenzen)	4,18
Appvisory Secure App Check Plus L (501 bis 2.500 Lizenzen)	3,37
Appvisory Secure App Check Plus XL (ab 2.501 Lizenzen)	1,80
Appvisory Secure App Check Plus P (öffentlicher Dienst)	2,78
Zusatzleistungen optional	
Onboarding initial, 1,5 Stunden	349,00
Consulting Manntage, 8 Stunden	1600,00
Consulting pro Stunde	235,00