Leistungsbeschreibung rhöncloud Managed IT-Security (Add-On)

Inhaltsverzeichnis

Servicebeschreibung

Mit unserem optionalen Service »rhöncloud Managed IT-Security« bieten wir die Möglichkeit der Inanspruchnahme von erweiterten IT-Security-Leistungen für unsere bereitgestellten Cloud-Services. Durch steigende Cyberkriminalität werden zusätzliche Präventionsmaßnahmen für die Erhöhung der IT-Sicherheit unabdingbar. Unser »rhöncloud Managed IT-Security«-Paket erhöht den Schutz der durch rhöncloud bereitgestellten Cloudservices auf das bestmögliche Maximum. Durch das leistungsstarke Paket werden softwarebasierte Agenten auf den jeweiligen Cloudservices, zumeist virtuelle Serversysteme (virtuelle Maschinen), installiert und durch diverse Sicherheitsfeatures zusätzlich geschützt. Über das webbasierte Security-Dashboard haben Kunden jederzeit die Möglichkeit, aktuelle Statusmeldungen und Ereignisse der Security-Agenten in Echtzeit zu prüfen, um geeignete Gegenmaßnahmen zu ergreifen.

Voraussetzungen

Voraussetzung für die Buchung unserer »Managed IT-Security«-Pakete als Add-on ist eine vorhandene und gültige Vertragsvereinbarung unserer rhöncloud Cloudservices »rhöncloud IT-Outsourcing (https://www.rhoencloud.de/leistungsbeschreibung-rhoncloud-it-outsourcing/)« und/oder »rhöncloud cockpit (https://www.rhoencloud.de/leistungsbeschreibung-rhoencloud-cockpit/)«. Eine alleinige Buchung unserer »Managed IT-Security«-Pakete auf rhöncloud-fremden Serversystemen außerhalb unserer Rechenzentren ist nicht möglich. Zur Leistungserbringung wird auf den gewünschten virtuellen Servern (virtuellen Maschinen) ein Softwareagent installiert. Für die Installation muss der rhöncloud Zugriff auf diese virtuellen Server (virtuellen Maschinen) ermöglicht werden. Alternativ ist die Installation auch via Installationsdatei möglich, welches dem Kunden auf Anfrage zur Verfügung gestellt wird.

Einrichtungsgebühren / Setupgebühren

Bei Buchung unserer »rhöncloud Managed IT-Security«-Add-ons wird eine einmalige Setupgebühr fällig. Die jeweilige Setupgebühr ist auf dem jeweiligen Angebot oder in der zum Zeitpunkt gültigen Preisliste angegeben. Die Setupgebühr wird nach Einrichtung der »rhöncloud Managed IT-Security«-Agenten durch die rhöncloud per Basis-Lastschrift von den im Vertrag angegebenen Kontodaten eingezogen.

Vertragslaufzeit und Vertragsbeginn

Die Vertragslaufzeit sowie der Vertragsbeginn richten sich nach den genutzten Cloudservices unserer Produkte »rhöncloud IT-Outsourcing (https://www.rhoencloud.de/leistungsbeschreibung-rhoncloud-it-outsourcing/)« und »rhöncloud cockpit (https://www.rhoencloud.de/leistungsbeschreibung-rhoencloud-cockpit/)«.

	rhöncloud IT-Outsourcing	**rhöncloud cockpit**
Vertragslaufzeit	Die Vertragslaufzeit des/der Add-on(s) ist analog der Vertragslaufzeit des Hauptvertrages. Eine vorzeitige Kündigung ist ausgeschlossen.	Die Mindestvertragslaufzeit beträgt einen Monat, sofern keine separate Vereinbarung getroffen wurde.
Vertragsbezug	Das/die Add-on(s) werden als Vertragszusatz dem rhöncloud IT-Outsourcing Hauptvertrag zugeordnet.	Das/die Add-on(s) werden als eigenständiger Vertrag abgeschlossen.
Abrechnung	Das/die Add-on(s) wird/werden mit der monatlichen IT-Outsourcing-Abrechnung nach Anzahl der gebuchten Add-ons berechnet.	Das/die Add-on(s) wird/werden in einer separaten Abrechnung monatlich berechnet. Hierbei wird jeweils der gesamte Monat fakturiert.
Kündigung	Es gelten die Kündigungsfristen- und bestimmungen des Hauptvertrages.	Erfolgt keine oder eine verspätete Kündigung, so verlängert sich der Vertrag um einen weiteren Monat mit einer Kündigungsfrist von einem Monat zum Monatsende. Bei rechtzeitiger Kündigung endet der Vertrag gemäß Laufzeit zum Ende des nächsten Laufzeitmonats.

Der Vertrag kann schriftlich oder elektronisch (Textform) geschlossen werden. Im Falle des schriftlichen Vertragsschlusses kommt der Vertrag zustande durch beiderseitige Unterschrift. Im Falle der elektronischen Beauftragung durch den Kunden (beispielsweise per E-Mail) kommt der Vertrag durch unsere Auftragsbestätigung per E-Mail zustande. Der Vertrag beginnt an dem ersten Tage des Monats, in welchem wir mit der Zurverfügungstellung der vertraglichen »Patchmanagement und Monitoring«-Agenten beginnen. Die Zurverfügungstellung der vertraglichen »rhöncloud Managed IT-Security«-Add-ons wird spätestens drei Monate nach Vertragsschluss erfolgen. Fakturiert wird unabhängig des untermonatigen Startdatums der gesamte Laufzeitmonat rückwirkend zum Vertragsbeginn.

Kündigung

Nach Vertragsende werden alle technischen sowie administrativen Daten unwiederbringlich gelöscht. Als Vertragszusatz zum »rhöncloud IT-Outsourcing (https://www.rhoencloud.de/leistungsbeschreibung-rhoncloud-it-outsourcing/)«-Hauptvertrag enden das/die »Managed IT-Security«-Add-on(s) zum selben Beendigungszeitpunkt. Sind das/die »Managed IT-Security«-Add-on(s) als eigenständiges Vertragsverhältnis zu einem Cloudservice unseres Produktes »rhöncloud cockpit (https://www.rhoencloud.de/leistungsbeschreibung-rhoencloud-cockpit/)« gebucht, so richtet sich die Vertragsauflösung der unter “Kündigung” angegebenen Frist.
Für eine schnelle und eindeutige Bearbeitung wird die Kündigung des Vertrags per E-Mail an **contract-de@rhoencloud.de** empfohlen. Andere Textformen (z. B. Brief) sind ebenfalls zulässig und werden entsprechend der gesetzlichen Vorgaben anerkannt.

Kündigungen bitte per E-Mail an **contract-de@rhoencloud.de**

Vertragsgegenstand

Wir bieten mit unseren Managed–IT–Security–Paketen eine professionelle Lösung zur Früherkennung von Cyberangriffen für die gesamte Cloud–Infrastruktur im SaaS-Modell als Self-Service-Plattform an. Als Cloud–Infrastruktur werden alle virtuellen Systeme des Kunden im Rechenzentrum der rhöncloud bezeichnet. Diese Pakete können als Add-on zu den bereits bestehenden Cloud–Systemen hinzugebucht werden. Vertragsgegenstand ist die Gestattung der Nutzung der Software als SaaS–Lösung. Dies beinhaltet die Überwachung und Analyse von Hosts (Server, Clients), Endpunkten (URL, Webseiten, IP–Adresse, die über das Netzwerk (z. B. Internet) erreichbar sind) sowie IP–Adressen im internen Netzwerk, im Rahmen und Umfang des jeweils gebuchten Plans oder der bereitgestellten Softwarelizenzen.

Softwareanbieter und -bereitstellung

Wir setzten bei der Absicherung auf eine Cybersecurity–Software des deutschen Anbieters Enginsight GmbH (enginsight.com/de). Bei Nutzung der Lösung gelten die Leistungs– und Nutzungsbedingungen des Herstellers, welche über die Webseite eingesehen werden können. Die Funktionen der Software beschränken sich auf die Erfassung, Messung und Darstellung bestimmter Daten. Die Haftung für die Fehlerfreiheit der Applikationen liegt allein beim Softwarehersteller. Für

Folgeschäden aus diesem Umstand übernimmt die rhöncloud keine Haftung. Für die korrekte Bereitstellung wird die Installation eines softwarebasierten Agenten auf dem zu überwachendem System benötigt. Das Software–Management erfolgt per Fernwartung/Remotezugriff. Individuelle Erweiterungen und Anpassungen der Funktionalität der Software sind nicht Gegenstand des Leistungsumfangs und dieser Vereinbarung und müssen bei Bedarf separat vereinbart werden.

Installation Agents

Im Rahmen der Produktbereitstellung ist es notwendig, auf der entsprechenden virtuellen Maschine ein Agent bereitzustellen und zu installieren. Der Kunde kann über das Security Dashboard (https://ngs-app.security-dashboard.de/) ein Installationsskript herunterladen, welches auf dem jeweiligen Zielsystem mit administrativen Rechten ausgeführt wird. Der Security-Agent wird im Hintergrund installiert. Innerhalb weniger Minuten wird das Zielsystem im Security Dashboard (https://ngs-app.security-dashboard.de/) angezeigt.

Onboarding

Nach Buchung und Bereitstellung des Managed IT Security Add-on(s) kann der Kunde ein einstündiges Onboarding per Videomeeting in Anspruch nehmen. In diesem Onboarding wird dem Kunden das Security Dashboard (https://ngs-app.security-dashboard.de/) vorgeführt. Es können innerhalb der Zeitspanne auch gemeinsame Einstellungen getätigt werden, um die Lösung für den Kunden zu individualisieren. Der Onboarding–Termin ist mit unseren Mitarbeiterinnen und Mitarbeitern abzustimmen. Bei Überschreitung des inkludierten Zeitkontingents wird nach unseren allgemeinen Stundensätzen gemäß unserer Preisliste (https://www.rhoencloud.de/downloadcenter/) (IT-Security) nach fakturiert. Das Onboarding erfolgt auf Basis einer Beratungsdienstleistung sowie auf der Empfehlung unseres Fachpersonals. Die Inanspruchnahme des einstündigen Onboarding wird proaktiv durch den Kunden angefragt und muss während den ersten beiden Abrechnungsmonaten genutzt werden.

Zugang

Der Kunde erhält nach Buchung einen Zugang zum rhöncloud Security Dashboard (https://ngs-app.security-dashboard.de/). Der Login in unserem Security Dashboard (https://ngs-app.security-dashboard.de/) erfolgt mit einem Benutzernamen und individuellem Kennwort, welches nach

Buchung verschlüsselt übermittelt wird. Dieses Kennwort kann jederzeit selbständig im Security Dashboard (https://ngs-app.security-dashboard.de/) geändert werden.

Security Dashboard

Unser rhöncloud Security Dashboard (https://ngs-app.security-dashboard.de/) bietet eine detailreiche Ansicht von verschiedenen Möglichkeiten in Bezug auf die IT–Sicherheit der angebundenen Systeme und stellt diese u. a. in Form von aussagekräftigen Diagrammen dar. Das Security Dashboard (https://ngs-app.security-dashboard.de/) übernimmt die Aufgabe, die Analysedaten global zu aggregieren, um sie unmittelbar zugänglich zu machen. Es kann somit auf einen Blick eingesehen werden, wo etwaige Sicherheitsrisiken bestehen und wo dringlichster Handlungsbedarf besteht.

Aktive Unterstützung bei Security-Ereignissen

Stellt der Kunde Ereignisse fest, welche durch eigenes Wissen nicht kategorisiert und eingeschätzt werden können, so kann der Kunde das Team der rhöncloud zur Prüfung der Ereignisse kontaktieren. Die rhöncloud wird dem Kunden geeignete Empfehlungen aussprechen und auf Wunsch tatkräftig bei der Lösungsfindung unterstützen. Seitens der rhöncloud findet keine proaktive Prüfung der auftretenden Ereignisse statt.

Funktionsbeschreibung

IT–Monitoring

Die Cybersecurity–Software ermöglicht klassisches Verfügbarkeits–Monitoring auf allen Servern und Clients durch die Installation des Pulsar–Agents. Dazu gehört die Überwachung der CPU–, RAM–, SWAP–, Festplatten– und Netzwerk–Auslastung. In Echtzeit erhält der Anwender die betreffenden Metriken und kann sie auf etwaige Probleme untersuchen. Mit Custom Metriken lässt sich das Monitoring durch beliebige Daten erweitern, die in einem zeitlichen Verlauf darstellbar sind. Das können zum Beispiel Daten einer Datenbank, Backups oder Sensor–Daten sein. Die Datenverläufe aller Metriken (Standard–Metriken und Custom Metriken) kann das Machine–Learning–Modul analysieren und verstehen, um den erwartbaren Normalbetrieb zu prognostizieren. Bei ungewöhnlichen Verläufen kategorisiert es die Abweichung als low, medium oder high. Die autonome Überwachung der Metriken auf Anomalien ermöglicht, Alarme ohne feste Grenzwerte zu definieren.

Software
Inventur Ihrer Software mit dem Softwarenamen, der Version und der Quelle der Software.
Autostarts
Autostarts ist eine Softwareübersicht, die bei einem Systemneustart Ihres Hosts automatisch gestartet wird.

Dienste
Unter Dienste wird eine Übersicht über alle laufenden und gestoppten Dienste Ihres Servers verstanden.

Verbindungen (Ports)
Unter Verbindungen befindet sich eine Übersicht der geöffneten Ports Ihrer Server, die den Status „Listen“ besitzen.

Prozesse
Hier findet man eine Auflistung über alle auf Ihrem System laufenden Prozesse (inkl. Prozess ID), dem Prozessnamen,
etwaigen Unterprozessen und dem Benutzer des Prozesses.

Asset Monitoring
Die Installation der Softwarekomponente Watchdog im Netzwerk ermöglicht eine permanente Überwachung des Netzwerkverkehrs nach dessen Teilnehmern. Mit regelmäßigen aktiven Netzwerkscans provoziert der Watchdog darüber hinaus Netzwerkverbindungen und findet so auch IP–Adressen, die von sich aus keinen Netzwerkverkehr erzeugt haben. Automatisch versucht Enginsight die detektierten Assets zu kategorisieren. Außerdem steht es dem Nutzer offen, weitere Daten zum Asset zu Dokumentationszwecken einzupflegen (z. B. Beschreibung, Standort, Verantwortlichkeit). Via Tags lassen sich die Assets zudem gruppieren. Um die Unterscheidung zwischen offizieller und potenzieller Schatten–IT herzustellen, können Assets als begutachtet markiert werden. Um die Daten extern zu nutzen, lassen sich die Listen exportieren.

Automatische Erfassung aller Geräte im Netzwerk
Eine Übersicht über alle im Unternehmen vorhandenen Assets ist elementar. Sie bildet die Grundlage jeglicher Maßnahme zur Steigerung des Sicherheitsniveaus.

Permanente Überwachung nach neuen Geräten
Permanentes Scanning Ihres gesamtes Cloud–Netzwerk nach neuen Assets.

Visualisierung aller gefundenen Geräte
Die Assets werden nach Subnetzen gruppiert. Verfügbarkeitsüberwachung (Ping–Check) Health Checks sind auf IP–Adressen basierende Überprüfungen.
SNMP–Templates über SNMP können Sie diejenigen Geräte in das Monitoring aufnehmen, auf denen sich kein Agent installieren lässt (unter anderem Linux–basierte virtuelle Maschinen).

Risk Management

Konfigurationen
Hier erhalten Sie eine Checkliste über die Konfigurationen ihres Hosts. Falsch gesetzte Konfigurationen können ein Einfallstor für Hacker darstellen. Sie zu überprüfen und zu korrigieren, sollte daher einen zentralen Stellenwert in jeder IT–Sicherheits–Strategie einnehmen.

Systemevents
Hier besteht eine Übersicht über alle detektierten Systemevents des einzelnen Hosts. Das sind beispielsweise fehlgeschlagene bzw. erfolgreiche Login–Versuche.

Vulnerability Management

Sicherheitslücken
Unter Sicherheitslücken findet man die Ergebnisse des CVE–Scanners (Schwachstellen–Scanners). Zu jeder Sicherheitslücke erhält man den CVE–Score und die ID der Sicherheitslücke.

Patch Management

Update Manager
Im Update Manager finden man eine Auflistung anstehender Security–Updates und Security Hot–Fix für installierte Programme auf allen überwachten Systemen. Hier lassen sich mehrere Updates auf mehreren Systemen gemeinsam einspielen und ausrollen (für die korrekte Ausrollung wird seitens der rhöncloud keine Funktionsgarantie und Haftung übernommen).

Intrusion Detection

Netzwerkanomalien
Unter Netzwerkanomalien findet man die Analyseergebnisse des Netzwerkverkehrs des einzelnen Hosts.

Intrusion Prevention
(Nur im Paket Advanced und Professional enthalten)

Dynamisches Blocken
Mit Aktivierung des Intrusion Prevention System (IPS) werden mithilfe eines dynamischen

Regelwerks Hackerangriffe
blockiert. Als Grundlage dient die Analyse des Netzwerkverkehrs auf Ihren Hosts.

Autonomes Blocken
Festlegung, bei welchen Attacken der Netzwerkverkehr automatisch geblockt werden soll. Manuelles Blocken mit manuellen Regelwerken können abhängig von IP, Protokoll und Port definiert werde, ob Shield Netzwerkverkehr blockieren oder erlauben soll.

Manuelles Blocken
Mit manuellen Regelwerken können abhängig von IP, Protokoll und Port definiert werde, ob Shield Netzwerkverkehr blockieren oder erlauben soll.

Security Automation

Plugins
Hinter dem Punkt Plugins verbirgt sich ein sehr mächtiges Werkzeug. Hier können eigene Skripte erstellt werden, die sich dann auf von Ihnen ausgewählten Hosts ausführen lassen.

Machine Learning
Das Machine Learning–Modul ist in der Lage, die Datenverläufe zu analysieren, zu verstehen und den Normalbetrieb zu prognostizieren. Bei ungewöhnlichen Verläufen kategorisiert es die Abweichung als low, medium oder high und löst, wenn gewünscht, einen Alarm aus.

Alarmierungen
Standardmäßig sind folgende Alarme eingestellt:

- Verdächtiger Netzwerkverkehr
- Neue Sicherheitslücke (CVSS Score)
- Neue/Entfernte Software
- Anmeldeversuch eines nicht existierenden Nutzers
- Ein gesperrter Account wurde aktiviert
- Ein gesperrter Admin Account wurde aktiviert
- Ein Nutzer hat erhöhte Privilegien erhalten
- Fehlgeschlagener Anmeldeversuch
- Ein neuer Nutzer wurde angelegt
- Ein neuer Administrator wurde angelegt
- Host Neustart
- Neuer Autostart

Unterstützte Plattformen

Die unterstützten Plattformen entnehmen Sie bitte den Leistungs– und Nutzungsbedingungen des Herstellers, welche über die Webseite eingesehen werden können. (siehe enginsight.com/docs/technische–details/systemanforderungen).

Verfügbarkeiten

Verfügbarkeitsbereich	Verfügbarkeit	Grundlage	Maximale Ausfallzeit
Verfügbarkeit der bei rhöncloud betriebenen Management-Systeme und des Security Dashboards (Enginsight)	99,7 %	jährlich	26 Stunden, 17 Minuten
Verfügbarkeit der auf den virtuellen Maschinen installierten Agenten	Kundenseitige Verantwortlichkeit	–	Kundenseitige Verantwortlichkeit

Monitoring

Alle unsere Infrastrukturkomponenten werden durch ein proaktives 24/7-Monitoring überwacht. Das Monitoring wird durch unser Network Operation Center (NOC) betreut, administriert und analysiert.

Wartungen

Zur Sicherstellung der Funktionsbereitstellung führen wir regelmäßig Updates und Wartungen an unserer Infrastruktur sowie unseren IaaS-Services durch. Sofern hiervon die Erreichbarkeit Ihrer gebuchten Services betroffen ist, kann es unter Umständen zu nicht vermeidbaren Unterbrechungen der Funktionsbereitstellung kommen. Wartungen kündigen wir mit einer Vorlaufzeit von mindestens sieben Tagen über unser Statusportal (https://status.rhoencloud.de/) an. Über das Statusportal können Sie Ihre E-Mail-Adresse oder eine Mobilfunkrufnummer in einen automatischen Verteiler hinterlegen, sodass Sie bei angekündigten Wartungsfenstern oder aktuellen Störungsmeldungen proaktiv informiert werden. Weitere Benachrichtigungen erfolgen nicht. Sofern Sie Ihre E-Mail-Adresse und/oder Ihre Mobilfunkrufnummer im Statusportal und somit im automatischen Benachrichtigungsverteiler hinterlegen, beachten Sie bitte die Datenschutzbestimmungen des Anbieters »statuspal.io«, welche Sie hier

(https://www.statuspal.io/privacy) aufrufen können und mit welchem wir die extern betriebene Lösung anbieten. Mit der Hinterlegung stimmen Sie diesen Bestimmungen zu. Sollten Sie in unseren Vertragsunterlagen die Option gesetzt haben, dass wir Ihre Daten in den Benachrichtigungsservice unseres Statusportal aufnehmen, so sind ebenfalls die Datenschutzbestimmungen entsprechend zu beachten. Durch Setzen der Option in unseren Vertragsunterlagen stimmen Sie ebenfalls diesen Datenschutzbestimmungen (https://www.statuspal.io/privacy) zu. Es besteht jederzeit die Möglichkeit, den Benachrichtigungsservice ganz oder teilweise zu deaktivieren.

Sichere Datenlöschung

Bei Kündigung werden am Folgetag der fristgerechten Beendigung des Vertrages, Ihre Systeme vollständig gelöscht. Vorhandene Datensicherungen werden sofort, spätestens nach 14 Tage gelöscht. Alle Löschvorgänge erfolgen nach DOD 5220. 22-M. sowie gemäß den gesetzlichen Löschfristen.

Preise

Es gelten die stets aktuellen Ressourcen- und Lizenzpreise, welche über unsere Preisliste (https://rhoenbox.rhoencloud.de/index.php/s/pSLWHP75bHJMNNm) eingesehen werden können. Während der Vertragslaufzeit können sich einzelne Preise unserer Ressourcen ändern. Wir informieren Sie mindestens vier Wochen im Voraus, sofern sich Ressourcenpreise ändern. Eine Erhöhung innerhalb/unter 10 % des monatlichen Gesamtbetrages je 12 Monate seit der letzten Erhöhung berechtigen nicht zur fristlosen Kündigung des Vertragsverhältnisses. Alle angegeben Preise sind Netto-Preise, zzgl. der zum jeweiligen Zeitpunkt gültigen Umsatzsteuer.

Lizenzierung

Bei Nutzung unserer »rhöncloud Managed IT-Security«-Add-on(s) sind bereits alle Lizenzen inkludiert, die für die Bereitstellung der Managed IT-Security-Lösung anbieterseitig notwendig sind.

Hinweise zur IT-Sicherheit

Die Themen IT-Sicherheit und Cybersicherheit spielen bei der rhöncloud eine zentrale Rolle. Aus diesem Grund sind wir in diesen Bereichen mehrfach ISO-zertifiziert (https://www.rhoencloud.de/unternehmen/tuev-zertifiziert/). Durch technische und organisatorische Maßnahmen sorgen wir für einen bestmöglichen Schutz unserer Rechenzentrumssysteme. Allerdings bietet diese Art der Prävention nur eine solide Grundlage. Um ein noch höheres Sicherheitslevel zu erreichen, empfehlen wir das Treffen von weiteren Vorkehrungen zum Schutz der IT-Sicherheit Ihrer Systeme. Dazu zählen beispielsweise eigenverantwortliche Schutzmaßnahmen Ihrer virtuellen oder dedizierten Cloudsysteme, Schulungsmaßnahmen Ihrer Mitarbeiter oder auch regelmäßige Sicherheitsaudits. Wie im Bereich “Anbieterverantwortlichkeit” endet die Zuständig der rhöncloud ab der virtuellen Maschine (Virtual Machine) und Betriebssystemebene (Operating System). Der Kunde ist somit für die Absicherung seiner gebuchten Systeme verantwortlich und sichert bei Nutzung unserer Produkte zu, für eine bestmögliche und protokollierte IT-Sicherheit zu sorgen. Weitere Informationen und Hilfestellungen können bei unserem Security Operation Center (SOC) angefragt werden (✉️ E-Mail: soc@rhoencloud.de). Bei auftretenden Sicherheitsvorfällen auf Kundenseite, welche unmittelbaren Einfluss auf die Bereitstellung der Cloudservices der rhöncloud haben (in der rhöncloud gehostete Systeme), ist die Kontaktierung unseres Security Operation Center (SOC) (✉️ E-Mail: soc@rhoencloud.de) obligatorisch und umgehend vom Kunden durchzuführen.

Ansprechpartner bei Vertragsfragen / Qualitätsmanagement / Datenschutz

✉️ E-Mail: **qm@rhoencloud.de**
📞 Telefon: **06682 212003-0**

Version und letzte Änderung

Version	Änderungsdatum	Download
1.2	September 2025	Download als PDF (https://www.rhoencloud.de/wp-content/uploads/2025/09/Leistungsbeschreibung-rhoencloud-Managed-IT-Security-Add-On.pdf)
1.1	Juli 2023	Version 1.7