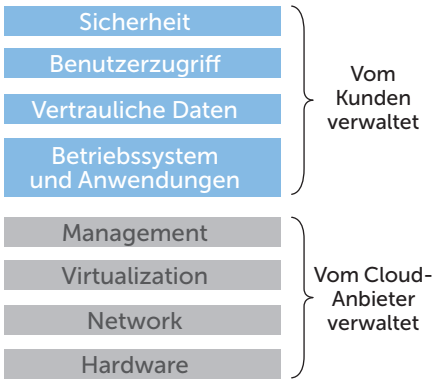
Kaspersky®
Cloud Security

Schutz Ihrer Amazon-Cloud mit Kaspersky Cloud Security

Gründe für Kaspersky Lab zum Schutz einer Hybrid-Cloud:

- **Die am häufigsten ausgezeichnete Sicherheitslösung**, optimiert für Ihre Hybrid-Cloud
- **Erhält die Systemeffizienz**, sodass Sie im Bereich der Cloud-Sicherheit volle Transparenz und und Verwaltbarkeit erhalten
- **Erweiterte Funktionalität**, darunter Kontrolle von Anwendungen und Webgeräten, sowie Schutz vor aktuellen Cyberbedrohungen und Ransomware-Angriffen
- **Zusammenarbeit** mit Ihrer Unternehmensinfrastruktur
- **Ressourcensparend** und deutliche Senkung der Betriebskosten in Ihrer Hybrid-Cloud-Umgebung

Gemeinsame Sicherheitsverantwortung in öffentlichen Cloud-Umgebungen



Stimmen Sie die Sicherheit Ihrer Hybrid-Cloud mit Amazon und Kaspersky Lab ab

Die Integration eines Hybrid-Cloud-Ansatzes für Datenverwaltung und Speicher, bei dem sich Arbeitslasten frei zwischen Ihrer eigenen virtualisierten Umgebung und mindestens einer öffentlichen Cloud bewegen, führt zu neuen Sicherheitsüberlegungen. Aber: Ganz gleich, ob sich Ihre Daten bei Ihnen vor Ort befinden oder ausgelagert sind, das Hauptziel bleibt das gleiche: Es geht um die Absicherung Ihres Unternehmens, seiner digitalen Werte, seiner geschäftlichen Kontinuität und seiner Mitarbeiter.

Der Wechsel von einer Private Cloud zu einem Hybrid Cloud-Ansatz führt ein neues Verantwortungsmodell ein. Während der Dienstanbieter die Sicherheit der Public Cloud verwaltet (Infrastruktur, Hardware, Netzwerk und Virtualisierungsebenen), bleiben Sie für die Inhalte der Cloud verantwortlich (sichere Arbeitslasten, Betriebssysteme, Daten und Anwendungen). Selbstverständlich sind Sie auch weiterhin für die Cybersicherheit der Mitarbeiter verantwortlich. Außerdem müssen Sie sicherstellen, dass Ihre Sicherheitslösung Ihre Ziele für die Cybersicherheit erfüllt.

Amazon Web Services (AWS) bietet eine zuverlässige, skalierbare und kostengünstige Public Cloud-Umgebung für Ihre geschäftlichen Arbeitslasten an. VMs und ihre mit Kaspersky Cloud Security geschützten Arbeitslasten (unabhängig von der Platzierung in der von AWS betriebenen oder privaten Infrastruktur Ihrer Hybrid Cloud) müssen einheitlichen Sicherheitsstufen und Richtlinien unterliegen. Außerdem muss für volle Transparenz und Verwaltbarkeit über eine einzige Konsole gesorgt werden.

Dieses Dokument erläutert, wie einfach es ist, Kaspersky Cloud Security in Ihre AWS-Cloud-Ressourcen zu integrieren und so erweiterte Sicherheit, umfassende VM-Transparenz und einheitliche Koordination in Ihrer gesamten Hybrid Cloud bereitzustellen.

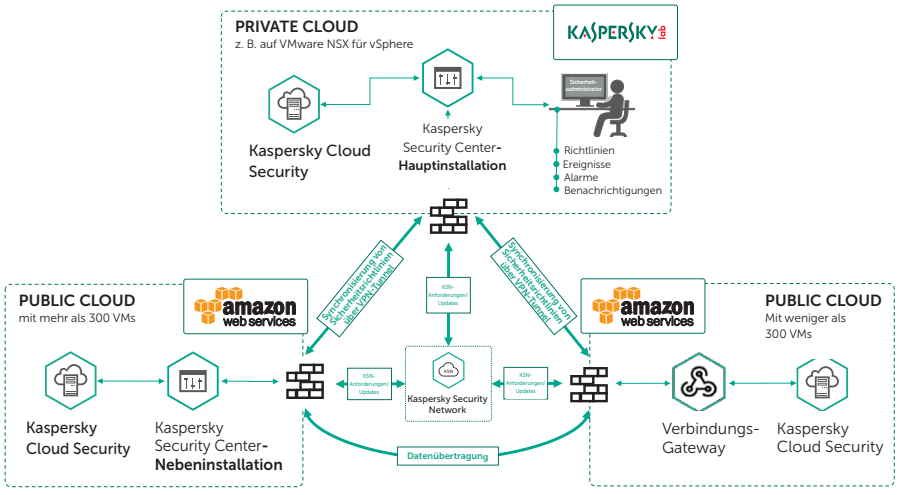


Bild 1 Hybrid-Cloud mit Amazon Web Services und Kaspersky Cloud Security

Eine allgemeine Best-Practice-Empfehlung ist, die Kommunikation zwischen den Clouds standardmäßig über das öffentliche Internet erfolgen zu lassen. Wir raten ausdrücklich zur Bereitstellung **sicherer Crypto-Kanäle** (VPN-Tunnel) zwischen Ihren Private und Public Cloud-Infrastrukturen, um für höchsten Schutz und Privatsphäre zu sorgen. Hierzu können Amazon Virtual Private Cloud Network und Amazon Virtual Private Gateway genutzt werden.

Wenn Sie noch nicht Version 10 des Kaspersky Security Center einsetzen, empfehlen wir ein Upgrade auf diese Version, da diese Implementierung von früheren Versionen ggf. nicht ausreichend unterstützt wird.

Außerdem sollten Sie sicherstellen, dass Ihre **Netzwerkinfrastruktur** korrekt konfiguriert ist, um den Datenverkehr zwischen den Infrastrukturkomponenten wie im Diagramm oben gezeigt zu verwalten. Weitere Informationen zum Einrichten der Netzwerk-Ports und der Firewall-Regeln finden Sie im Implementierungsleitfaden für das Kaspersky Security Center.

Wir bieten zwei Methoden für die Bereitstellung der Kaspersky Cloud Security-Lösung – je nach Umfang Ihrer auf der AWS-Cloud basierenden Abläufe. Beide sind sehr klar strukturiert.

Hybrid Cloud-Sicherheit: AWS-Cloud + Private Cloud

Weniger als 300 VMs in der AWS-Cloud

Die Anwendung von Kaspersky Cloud Security auf Ihre Hybrid Cloud auf dieser Aktivitätsebene in der Public Cloud umfasst die Bereitstellung eines Verbindungs-Gateways. Dieses verbindet geschützte VMs in Ihrer öffentlichen Cloud direkt mit Ihrer Kaspersky Security Center-Hauptinstallation auf Basis Ihrer normalen Private Cloud. Auf diese Weise profitieren alle VMs von Sicherheitsrichtlinien, Updates und Lizenzinformationen.

Wird ein **Verbindungs-Gateway** verwendet, werden die VMs in Ihrer öffentlichen AWS-Cloud direkt mit der Kaspersky Security Center-Hauptinstallation verbunden und können so Sicherheitsrichtlinien. Updates und Lizenzinformationen erhalten. Anti-Malware-Updates, Scan-Statistiken und Ergebnisse können bei Bedarf auch vom Cloud-basierten, globalen Dienst Kaspersky Security Network (KSN) heruntergeladen werden.

Installieren Sie einfach Kaspersky Network Agent auf einer VM in Ihrer AWS-Cloud, und geben Sie dabei die IP-Adresse der Kaspersky Security Center-Hauptinstallation in Ihrer Private Cloud an. Diese VM dient nun als „Verbindungs-Gateway", über das alle anderen VMs in Ihrer AWS-Cloud, die während der Topologiesammlung ermittelt werden, eine Verbindung zur Kaspersky Security Center-Hauptinstallation herstellen können.

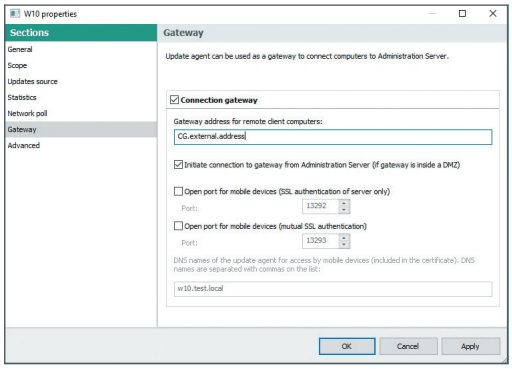


Bild 2 Verbindungs-Gateway – Konfigurationseinstellungen

300 VMs oder mehr in der AWS-Cloud

Wird eine Kaspersky Security Center-Nebeninstallation verwendet, verteilt dieser Server zentral alle Sicherheitsrichtlinien, Updates und Lizenzinformationen an geschützte VMs in Ihrer öffentlichen AWS-Cloud, nachdem alles vom Hauptserver empfangen wurde. Dies führt zu einer deutlichen Verringerung der Netzwerkauslastung zwischen den Clouds in einer größeren Implementierung.

Wenn Sie mindestens 300 VMs in Ihrer Public Cloud einsetzen, sollten Sie eine zusätzliche Kaspersky Security Center-Nebeninstallation anstatt eines Verbindungs-Gateways bereitstellen, um so für ausreichende Redundanz zu sorgen, sodass alle VMs jederzeit sicher betrieben werden können. Stellen Sie Ihre neue Kaspersky Security Center-Nebeninstallation mithilfe des einfachen Bereitstellungsassistenten auf einer VM in der AWS-Cloud bereit.

Die Sicherheit der VMs in beiden Clouds kann nun über Ihre Kaspersky Security Center-Nebeninstallation oder über das Verbindungs-Gateway verwaltet werden. Die gesamte Koordination erfolgt über die Kaspersky Security Center-Hauptinstallation in Ihrer Private Cloud.

Wenn Sie neben Ihrer Private Cloud mehrere Public Clouds nutzen, sollten Sie ein separates Verbindungs-Gateway, oder bei Bedarf eine Kaspersky Security Center-Nebeninstallation auf einer VM in jeder Public Cloud vorsehen.

Das ist auch schon alles. Nun können Sie VMs in Ihrer Private und in den Public Clouds verwalten. Nun müssen Sie nur Kaspersky Cloud Security-Agents auf den zu schützenden VMs installieren, damit unsere erweiterten Sicherheitsfunktionen und Kontrollen über Ihre vereinheitlichte Kaspersky Security Center-Koordinationskonsole in Ihrer gesamten Hybrid-Cloud eingesetzt und verwaltet werden können.

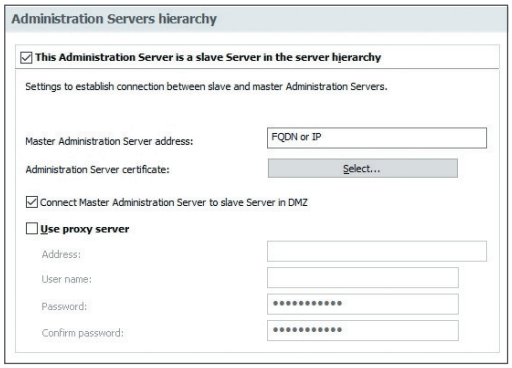


Bild 3 KSC mit Konfigurationseinstellungen für die „Nebenrolle“

Das Ergebnis:

- Das Einrichten oder Übertragen von Sicherheitsrichtlinien von Ihrer Private in Ihre Public Cloud, das Konfigurieren von Updates für Anti-Malware-Datenbanken, dass Überwachen der Sicherheit und das Erhalten von Berichten zu allen VMs kann nun zentral erfolgen.
- Ihre virtuellen Komponenten in der öffentlichen AWS-Cloud sind ebenso sicher, wie jene in Ihrer Private-Cloud-Umgebung. Gleichzeitig funktioniert Ihre Hybrid Cloud Infrastruktur weiterhin mit höchster Effizienz, ohne Auswirkungen auf die Systemleistung.
- Die Koordination Ihrer gesamten Hybrid Cloud erfolgt ebenso wie bei Ihrer Private Cloud völlig transparent.

Hybrid Cloud-Sicherheit: Nur für mehrere Public Clouds

Ein Hybrid Cloud-Ansatz kann mehrere Public Clouds (aber keine Private Cloud) umfassen und isoliert die öffentliche Infrastruktur von der übrigen IT. VMs befinden sich in AWS und in weiteren Public Clouds, darunter evtl. Microsoft Azure oder Managed Hybrid Cloud Hosting.

Auch hier kann **Kaspersky Cloud Security** eingesetzt werden, um harmonisierten Schutz, Verwaltbarkeit und Transparenz auf Unternehmensebene bereitzustellen. Auf diese Weise wird sichergestellt, dass jede einzelne VM unabhängig vom Standort der Public Cloud absolut sicher ist.

Da es in diesem Fall noch keine Kaspersky Security Center-Hauptinstallation in der Private Cloud gibt, muss im Rahmen der Bereitstellung noch ein Schritt erledigt werden. Sie müssen Ihre Kaspersky Security Center-Hauptinstallation auf einer VM in einer Public Cloud einrichten.

Anschließend wird (so wie zuvor im Abschnitt zu öffentlichen und privaten Hybrid Clouds) ein Verbindungs-Gateway oder eine Kaspersky Security Center-Nebeninstallation (bei mehr als 300 VMs) in jeder weiteren verwendeten Public Cloud eingerichtet. Schließlich wird Kaspersky Cloud Security auf jeder zu schützenden VM an den einzelnen Standorten installiert.

Sie können nun alle Ihre VMs in allen Public Clouds gemeinsam verwalten – entweder über eine Kaspersky Security Center-Nebeninstallation oder über ein Verbindungs-Gateway. Alle wesentlichen Aufgaben zur Sicherheitskoordination werden weiterhin transparent über die Kaspersky Security Center-Hauptinstallation erledigt.

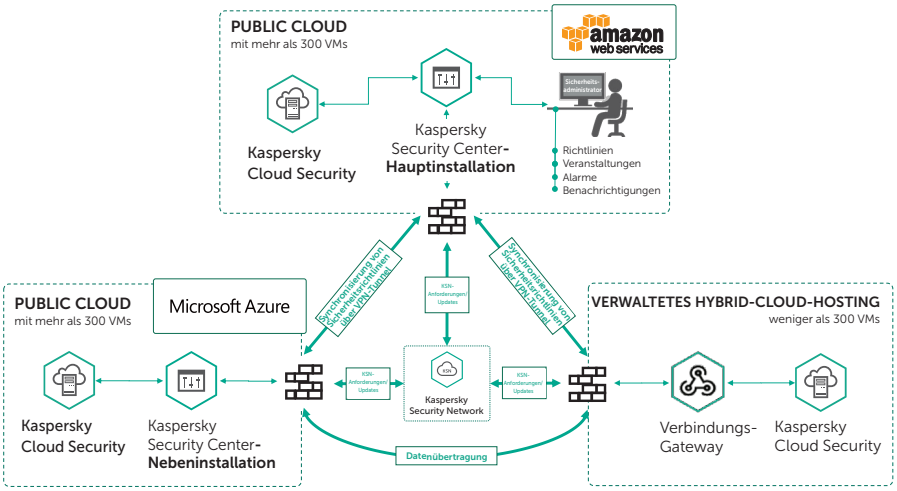
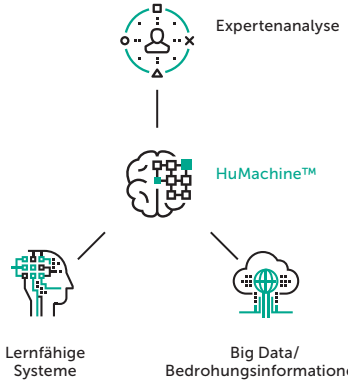


Bild 4 Hybrid-Cloud – nur mit mehreren Public Clouds

Hybrid Cloud-Sicherheit – Zusammenfassung

Die Kaspersky Cloud Security-Lösung wurde speziell entwickelt, um die technologischen Vorteile einer Hybrid Cloud zu nutzen, um Infrastrukturänderungen dynamisch zu berücksichtigen und hohe Sicherheit mit optimaler Geschwindigkeit und Ressourceneffizienz bereitzustellen. Unsere außergewöhnlichen Schutzfunktionen ermöglichen es Ihnen in Verbindung mit dem einheitlichen Security Management für alle physischen und virtuellen Endpoints (unabhängig vom Standort), Hybrid Cloud-Projekte in Ihrem eigenen Tempo zu realisieren –- problemlos, sicher und mit weniger Druck für die IT-Ressourcen.

Mehr über Kaspersky Cloud Security erfahren Sie unter
www.kaspersky.com/cloud-security



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **www.viruslist.de**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de