KASPERSKY lab

Zuverlässige Sicherheit, speziell entwickelt für Ihre flexible Hybrid Cloud

Kaspersky Hybrid Cloud Security

www.kaspersky.de
#truecybersecurity

Zuverlässige Sicherheit speziell für Ihre Hybrid Cloud-Umgebung

Daten werden immer flexibler im Hinblick auf ihren Speicherort, da sie fortlaufend im IT-Perimeter des Unternehmens auf mobile Geräte übertragen und gleichzeitig auf virtuellen und physischen Maschinen verarbeitet werden. Und weil Public Clouds und verwaltete Infrastrukturen immer beliebter werden, fließen so viele Daten wie nie zuvor vom jeweiligen Standort ab und wieder an ihn zurück.

Der zunehmende Einsatz anpassungsfähiger Cloud-Modelle, bei denen die Ressourcen der eigenen Rechenzentren augenblicklich auf Abruf und nach Bedarf in externe Clouds erweitert werden, bietet eine ganz neue Flexibilität, Agilität und klare wirtschaftliche Vorteile. Es gibt keine Vorab-Investitionen in Infrastruktur, keine Verluste und keine Verzögerungen bei der Erfüllung der unmittelbaren Ressourcenanforderungen, und all das bei guter Verwaltbarkeit.

Public Clouds bieten einen weiteren großen Vorteil, nämlich Geschäftskontinuität. Wenn Störungen oder Schäden in Ihrem Rechenzentrum auftreten, können ausgelagerte Ressourcen dafür sorgen, dass der Betrieb bis zur Problemlösung fortgeführt werden kann. Anbieter von Public Clouds selbst haben enorm in ihre eigene Geschäftskontinuität und in Cybersicherheit investiert und sichere, robuste Umgebungen für geschäftliche Arbeitslasten geschaffen. Aber das ist noch nicht alles …

Wichtigste Sicherheitsherausforderungen beim Umstieg auf die Cloud

- Angriffe durch Malware und Ransomware auf physische, virtuelle und Cloud-basierte Umgebungen
- Datenschutzverletzungen als Ergebnis eines reaktiven und unkoordinierten Sicherheitsansatzes
- Verminderte Transparenz aufgrund einer immer komplexeren Infrastruktur
- Administrative Herausforderungen durch uneinheitliche Steuerelemente und Tools
- Verschwendung von Systemressourcen durch ressourcenintensive herkömmliche Lösungen
- Unzureichender Schutz für Daten, die in privaten Rechenzentren gespeichert sind
- Unterbrechungen der Geschäftskontinuität oder Verhinderung des Datenaustauschs durch DoS-Angriffe

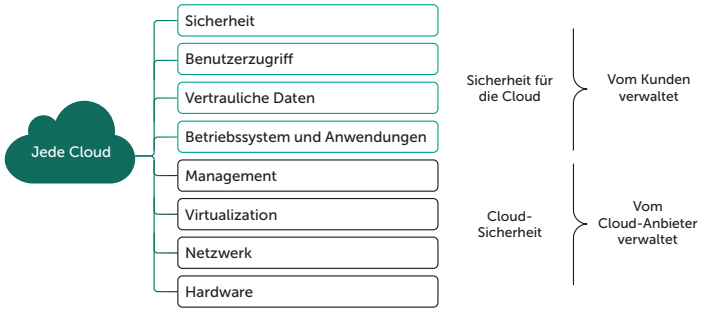
Wie sicher sind Ihre Daten in Public Clouds?

Die Antwort auf diese Frage ist nicht so einfach, wie es den Anschein haben mag.

Die heutigen Public Clouds sind überaus sicher. Es wird fortlaufend dafür gesorgt, dass Ihre Daten in der gehosteten Umgebung absolut geschützt aufbewahrt werden und dass keine Gefahr von Datenlecks innerhalb oder über die externe Cloud hinaus besteht.

Aber die Tatsache, dass Daten sicher aufbewahrt werden, bedeutet nicht unbedingt, dass sie auch wirklich geschützt sind. Datenlecks sind nur ein Aspekt der Sicherheit. Sind Daten zum Beispiel Ransomware ausgesetzt, bleiben sie zwar komplett und sicher aufbewahrt, werden allerdings möglicherweise beschädigt und somit unbrauchbar. Und alle bei der Interaktion mit Menschen beteiligten Daten, was ja schließlich die Hauptfunktion dieser Daten als Unternehmensressource ist, unterliegen den Auswirkungen menschlichen Versagens und potentiell auch menschlicher Übeltaten.

Sicherheitsmodell mit gemeinsamer Verantwortung

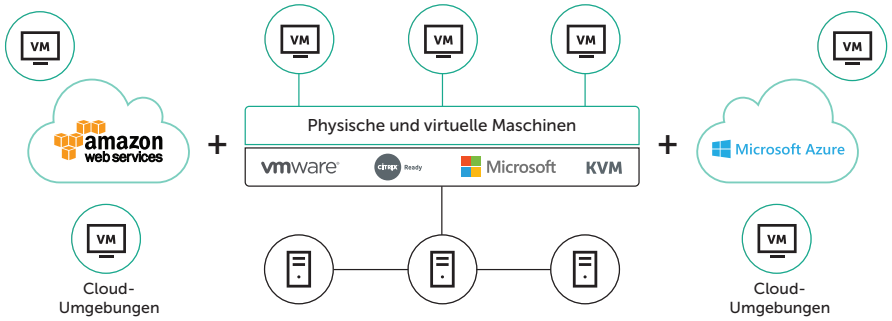


Die Anbieter gehosteter Cloud-Dienste sind für die Sicherheit der von ihnen bereitgestellten Umgebung verantwortlich, aber die Verantwortung für die interne Sicherheit Ihrer Workloads, wo immer sie sich auch befinden, liegt nach wie vor ganz und gar bei Ihnen selbst. Dies wird als „Sicherheitsmodell mit gemeinsamer Verantwortung" bezeichnet: Sie und Ihr Dienstanbieter sind für unterschiedliche Sicherheitsaspekte im Rahmen Ihrer Arbeitsbeziehung und für Ihre Datenbestände verantwortlich.

Auf die Frage: „Wie sicher sind Ihre Daten in Public Clouds?" lautet demnach die beste Antwort: „So sicher, wie an jedem anderen Ort!" Die gleichen Sicherheitserwägungen gelten überall dort, wohin Daten übermittelt werden. Sie können Daten nicht einfach dadurch schützen, dass Sie den Ort absichern, an dem sich die Daten zu einem bestimmten Zeitpunkt befinden. Da immer mehr geschäftskritische Daten häufiger und weiter über die kontrollierte Umgebung des IT-Perimeters des Unternehmens hinaus übertragen werden, ist es immer wichtiger, sich dieser Tatsache bewusst zu werden.

Schutz der Daten selbst, nicht nur der Umgebung

Jedes Datenpaket muss bei der Übertragung von innen heraus geschützt werden, wo immer es sich auch zu einem bestimmten Zeitpunkt befinden mag. Das liegt in der Verantwortung Ihres Unternehmens, und dieser Teil der Verantwortung kann auch nicht ausgelagert oder delegiert werden.



Absicherung des Workflows durch Orchestrierung

Die erste Frage lautet also: Wissen Sie genau, wo sich jedes einzelne Datenpaket jederzeit befindet und wohin es übertragen wird, und wissen Sie ebenso genau, wer jeweils mit den Daten umgeht?

Zugriffssteuerung und -überwachung sind ein fortlaufendes Sicherheitsproblem. Je größer und komplexer Ihre IT-Infrastruktur, desto mehr Lösungen sind notwendig, um die Effizienz und die Systemleistung optimal zu gestalten, und desto schwieriger ist es außerdem, alle Arbeitslasten und Programme fortlaufend im Auge zu behalten. Eine weitere Dimension bei diesem Problem besteht darin, dass die Infrastruktur von Rechenzentren heute auf externe Ressourcen erweitert wird. Es ist entscheidend, dass Sie jederzeit mit absoluter Sicherheit feststellen können, wer wie auf welche Ressourcen zugreift und sie verarbeitet.

Absicherung von Workloads im Hinblick auf besseren Schutz

Was geht vor sich? Welche Programme werden wo ausgeführt, und verhält sich jedes Programm den Erwartungen entsprechend? Schwachstellen in Programmen sind nach wie vor die primären Angriffspunkte für Sicherheitsverletzungen und Infektionen durch Cyberkriminelle. Die Systemhärtung wird durch die Bereitstellung verschiedener Technologieschichten erreicht, die entsprechende Angriffe aufhalten. Ob Verbot oder der Einschränkung bestimmter Programme, die fortlaufende Überwachung des Verhaltens jedes einzelnen Programms im Unternehmen oder das Abschirmen von Schwachstellen vor Ausnutzung: Alle diese wichtigen Maßnahmen zum Vermeiden und Erkennen von Bedrohungen sowie die erforderlichen Eingriffe liegen in Ihrer Verantwortung.

Datenschutz schafft Sicherheit für das Unternehmen

Zum Schutz Ihrer Runtime-Daten müssen Sie erkennen können, wann sie potentiellen oder tatsächlichen Angriffen ausgesetzt sind und mit welchen Mitteln diese Angriffe ausgeführt werden. Von hochentwickelten, hartnäckigen Bedrohungen (Advanced Persistent Threats, APTs), die speziell auf Ihr Unternehmen ausgerichtet sind, bis hin zu opportunistischer Ransomware, von Datendiebstahl und Finanzbetrug bis hin zu unberechenbarem menschlichem Versagen: Bedrohungen für Ihre Daten treten in vielerlei Gestalt und Umfang auf. Und weil Cyberkriminalität solch eine überaus lukrative und hoch entwickelte Branche ist, werden ständig neue Angriffsmethoden entwickelt und angewendet.

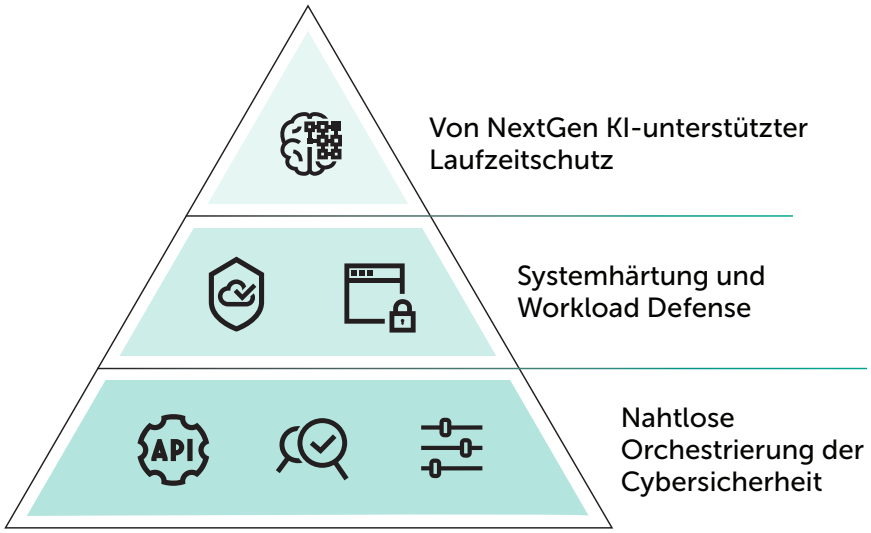
Was für Daten in der Cloud zutrifft, gilt für alle Daten: Die Effektivität des laufenden Schutzes hängt davon ab, wie gut die Threat Intelligence Ihres Sicherheitssystems ist und wie zeitnah und genau sie angewendet wird. Ihr IT-Sicherheitssystem muss in der Lage sein, eine potentielle Bedrohung zu erkennen, abzuwehren und unschädlich zu machen, bevor sie sich auf Ihre Daten und den Betrieb auswirkt. Diese Aufgabe muss dazu ohne Einschränkungen der Systemleistung erfüllt werden. Wichtiger noch: Es dürfen auch keine Fehlalarme generiert werden, die ihrerseits zu Störungen und Ressourcenverschwendung führen würden.

All dies liegt wiederum in Ihrer Verantwortung. Ihr Cloud-Dienstanbieter kann Ihre Daten nur bis zu einem gewissen Punkt schützen: Alles andere liegt bei Ihnen.

Wichtige Punkte bei der Absicherung des Hybrid Cloud-Rechenzentrums

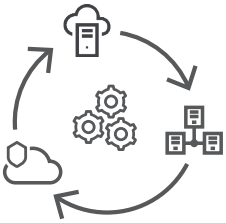
Zusammenfassend lässt sich sagen: Anbieter für externe Datenhosting-Software können zwar eine sichere und umfassend geschützte Umgebung für Ihre Workloads bereitstellen. Aber es liegt in Ihrer Verantwortung, die einzelnen Daten an allen Standorten zu überwachen, zu kontrollieren und zu schützen.

Bei Kaspersky Lab bezeichnen wir diese drei Aspekte der Sicherheitsverantwortung als Cybersicherheits-Orchestrierung, Systemhärtung und Laufzeitschutz („Runtime Protection"). Wir implementieren jede dieser Sicherheitsstufen über eine ganze Reihe von begleitenden und ineinandergreifenden Technologien, wie im Folgenden gezeigt.



Beim Festlegen einer Lösung zur Absicherung Ihrer Hybrid Cloud-Umgebung empfehlen wir Ihnen, unbedingt die folgenden Punkte in Ihre Anforderungen aufzunehmen:

Nahtlose Orchestrierung



Cloud-API – Integration mit Public Clouds (zum Beispiel Amazon AWS und Microsoft Azure) über native APIs. Damit werden Infrastruktur-Erkennung, der Einsatz automatisierter Sicherheitsagenten und eine richtlinienbasierte Verwaltung ermöglicht.

Account Management – Schutz Cloud-basierter Maschinen und erhöhte „Betriebshygiene" durch Sicherstellung, dass Sicherheitspersonal und Sicherheitsadministratoren für den Zugriff auf bestimmte Bereiche der Cybersicherheitskonsole über die entsprechenden Genehmigungen verfügen.

Rollenbasierte Zugriffssteuerung – Infrastruktur- und Sicherheitsteams können je nach den ihnen zugewiesenen betrieblichen Rollen über Zugriffs- und Steuerungsrechte unterschiedlicher Ebenen für die Cybersicherheitsschicht der Hybrid Cloud-Umgebung verfügen.

Systemhärtung

Programmkontrolle und Whitelisting – Durch Verbote bzw. Kontrollen, welche Programme wo und wann ausgeführt werden dürfen, verringert sich die Zahl der Angriffspunkte. (Ein Alleinstellungsmerkmal von Kaspersky Lab ist nach wie vor unser eigenes Whitelisting-Labor. Hier wird festgestellt, welche Programme von unseren Kunden jederzeit sicher ausgeführt werden können und in welchen Fällen möglicherweise eine „Default Deny"-Hochsicherheitsrichtlinie implementiert werden sollte.)

Schwachstellenabschirmung – Techniken wie Exploit Prevention, Vulnerability Assessment und automatisiertes Patch Management (alle diese Funktionen sind selbstverständlich in Kaspersky Security for Hybrid Clouds inbegriffen) hindern Angreifer daran, über Schwachstellen in beliebten Benutzerprogrammen in Ihre Systeme einzudringen.

Laufzeitschutz („Runtime Protection")

Anti-Ransomware – Abwehren von Ransomware, einschließlich Malware-Schutz für E-Mail und Web. Kaspersky Security for Hybrid Clouds umfasst auch ein „automatisches Rollback", mit dem eventuell beschädigte Dateien automatisch in den vorherigen unverschlüsselten Zustand zurückversetzt werden.

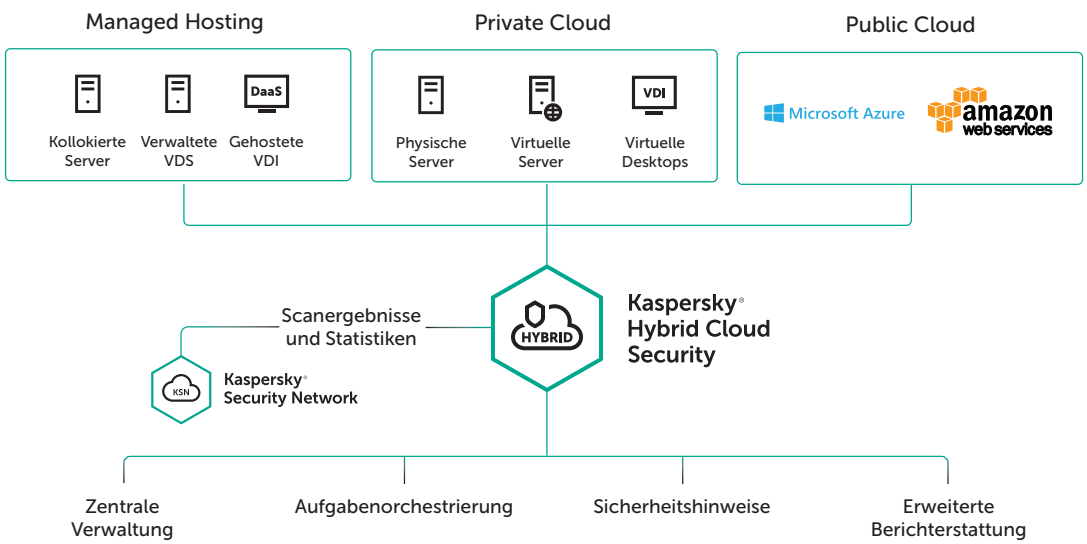
Hoch entwickelte Threat Intelligence – Zugang zu und Anwendung von hochwertiger Threat Intelligence in Echtzeit für Ihre Systeme und Datenschutzmechanismen.

Diese letztgenannte Funktion ist die wichtigste. Hierbei geht es um künstliche Intelligenz – die Fähigkeit eines Systems zur Erkennung von Software- oder Verhaltensanomalien, um Bedrohungen zu erkennen und zu identifizieren, die in der entsprechenden Form bisher noch nie aufgetreten sind. Erreicht wird dies durch eine Kombination von Techniken wie maschinellem Lernen und Verhaltensanalysen, durch unmittelbaren Rückgriff auf Cloud-basierte Informationsdatenbanken und durch Eingriffe menschlicher Experten.

Diese Fähigkeit zur Identifizierung und Abwehr bisher unbekannter Bedrohungen ist absolut grundlegend für die Datensicherheit. Ohne diese Ebene der „HuMachine® Intelligence" (wie wir sie nennen), bei der Experten und Machine Learning Hand in Hand arbeiten, wären Ihre Daten anfällig für zukünftige Angriffe, und zwar unabhängig davon, wie viele andere Sicherheitstechnologien angewendet werden. Lösungen von Kaspersky Lab sind im Hinblick auf diese Kombination aus maschineller Intelligenz konzipiert (wir implementieren bereits seit mehr als zehn Jahren lernfähige Systeme in unsere Technologien), und dank unserer langjährigen Fachkenntnisse sind wir in der Lage, heutige und zukünftige Bedrohungen zu erkennen, zu identifizieren und abzuwehren.

Cloud-Sicherheit: so elegant wie unerlässlich

Die Hybrid Cloud Security-Lösung von Kaspersky Lab bietet alle oben genannten Vorteile und mehr und stellt eine anpassungsfähige Sicherheitslandschaft für den Schutz Ihrer gesamten Hybrid Cloud vor den ausgeklügelsten Bedrohungen bereit.



Für flexible und sichere Clouds

Hybride Umgebungen sind äußerst dynamisch. Deshalb muss sich Ihre Sicherheit schnell an Weiterentwicklungen und Erweiterungen der Betriebsumgebung anpassen können.

- Verbesserte Transparenz in Ihren Cloud-Umgebungen für zuverlässigen und umfassenden Schutz
- Erkennung von und Reaktion auf hoch entwickelte Cyberbedrohungen durch Einsatz der kombinierten Leistung von Mensch und Maschine
- Schutz für alle Cloud-Umgebungen, Systeme, Netzwerke und Daten dank vielfältiger Kontrollmöglichkeiten

Ein Produkt für jede Cloud

Eine spezielle Lösung zur Bereitstellung der Next Generation-Cybersicherheit für Hybrid Cloud-Umgebungen in Unternehmen.

- Bewährte Sicherheit für physische und virtuelle Server, VDI-Speicherung und sogar Datenkanäle in Ihrer Private Cloud
- Erweiterte Sicherheitsfunktionen für Workloads in Public Clouds, einschließlich AWS und Azure
- Entspricht den Servicelevelzielen (Service Level Objectives, SLOs) von Unternehmen durch Minimierung von Cyberrisiken

Eine nahtlose Sicherheitserfahrung

Der Sicherheitsstatus Ihres Unternehmens in Bezug auf bekannte, unbekannte und neu aufkommende Bedrohungen hängt von der Transparenz und der übergreifenden Integration Ihrer IT- und Sicherheitsfunktionen ab.

- Integration zwischen den Kerntechnologien der Cloud und der zugehörigen Sicherheitsschicht über native APIs
- Automatisierte Sicherheitsbereitstellung für sichere und uneingeschränkte Cloud-Migration
- Eine nahtlose, unternehmensgerechte Orchestrierungserfahrung für jede Cloud

Dank der hochmodernen Funktionen in unserer Hybrid Cloud Security-Lösung sind die Infrastruktur- und Sicherheitsschicht vollständig integriert und kompatibel. Diese kombinierte Leistung schafft eine sichere und effiziente Umgebung, in der die nahtlose Migration von Arbeitslasten zwischen Private und Public Clouds möglich ist. Das Ergebnis ist eine permanente, flexible, transparente und verwaltbare Sicherheit – perfekt für das individuelle Hybridmodell Ihres Unternehmens.

Fazit

Extern verwaltete Cloud-basierte Hosting-Dienste bieten erhebliche geschäftliche Vorteile und sichere Umgebungen, in denen die Unternehmensdaten sicher gespeichert und verarbeitet werden können. Aber die Verantwortung für die Sicherheit ihrer Workloads verbleibt bei Ihnen. Wenn Sie jederzeit für vollständige Transparenz Ihrer Daten, Prozesse und Programme sowie eine entsprechende umfassende Kontrolle sorgen und zum Schutz Ihrer Daten die hoch entwickelte Threat Intelligence auf „HuMachine®"-Basis anwenden, gewährleisten Sie die Sicherheit sämtlicher Aspekte Ihres Hybrid Cloud-Rechenzentrums.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**
Unser einzigartiges Konzept: **https://www.kaspersky.de/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.de