Kaspersky® Hybrid Cloud Security

Schutz Ihrer Microsoft Azure Cloud-Infrastruktur

Public und Managed Clouds sind mittlerweile fester Bestandteil der IT-Landschaft von Unternehmen. Neu ist das zunehmende Bewusstsein, dass Public Clouds wie Microsoft Azure so weit gereift sind, dass sie auch mit geschäftskritischen Arbeitslasten umgehen können.

Diese Möglichkeiten werden sich auf die Sicherheitsbelange in Unternehmen und die Gestaltung ihrer IT-Strategien auswirken. Wie wird sich Ihre IT-Infrastruktur in den nächsten drei bis fünf Jahren entwickeln und erweitern? Wie können die Möglichkeiten von Public und Managed Clouds am besten genutzt werden, während gleichzeitig dafür gesorgt ist, dass die entsprechende Hybrid-Infrastruktur weiterhin zuverlässig und vor allem sicher ist?

Vorfälle im Bereich der Cybersicherheit sind nach wie vor ein großes Problem, und immer mehr Großunternehmen müssen Konsequenzen im Bereich Finanzen, bei der Reputation und gelegentlich sogar in rechtlicher Hinsicht ausbaden. Die Sicherheitsfunktionen in Unternehmen müssen agil und intelligent genug sein, um gegen aktuelle und künftige Bedrohungen anzukämpfen. Darüber hinaus sind Skalierbarkeit und Flexibilität erforderlich, um sie in Public Cloud- und Private Cloud-Infrastrukturen mit der hybriden Cloud-Umgebung weiterzuentwickeln und entsprechend anzupassen.

51 %

der Unternehmen geben zu, dass die Komplexität der IT-Infrastruktur ihre Fähigkeit, eine angemessene Sicherheitsstufe aufrechtzuerhalten, direkt beeinflusst

Bis zu

80 %

der Datenverluste in hybriden Clouds sind auf veraltete oder reaktive Cybersicherheitslösungen zurückzuführen

Private und Public Clouds – Ihre Hybridumgebung

Die Absicherung Ihrer Private Cloud ist relativ unkompliziert. Ein softwarezentriertes Rechenzentrum anhand von Virtualisierung zu entwickeln, ist eine vergleichsweise bewährte Praxis. Kaspersky Lab hat daher eine spezialisierte Software mit überaus geringer Belastung auf einer virtuellen Maschine bereitgestellt (oder, im Fall von VMware, ganz ohne feststellbare Belastung), um optimale Effizienz zu gewährleisten und die durch Virtualisierungstechnologie ermöglichten Ressourceneinsparungen und die Flexibilität zu bewahren.

Aber beim Übergang von der Private Cloud in die Public Cloud und vor allem, wenn beide unter einen Hut gebracht werden sollen, haben sich neue Problemfelder ergeben. Wo fängt eigentlich Ihre Sicherheitsverantwortung an, und wo hört sie auf? Und wie orchestrieren und schützen Sie Arbeitslasten, wenn diese zwischen lokalen und externen Speicherorten übertragen werden?

Erst Bescheid wissen, dann loslegen

Flexible Cloud-Umgebungen bergen vielfache Risiken, unabhängig von der Größe, der im privaten, softwarezentrierten Rechenzentrum verwendeten Virtualisierungsplattformen oder der zur Ausführung geschäftskritischer Programme auserkorenen Cloud-Plattform. Anbieter von Cloud-Diensten wie Microsoft Azure tun eine Menge, um sicherzustellen, dass Public Clouds auch weiterhin eine sichere Anlaufstelle für den Umstieg in Clouds beliebiger Größenordnungen sind. Azure bietet eine Reihe überaus wirksamer nativer Cloud-Sicherheitstools für die Einrichtung umfassender, unternehmensgerechter Umgebungen. Dennoch bleiben Risiken bestehen.

Bei Kaspersky Lab verzeichnen wir eine Reihe ernsthafter Bedrohungen (und nicht nur in Sachen Cybersicherheit), die sich u. U. negativ auf Ihre Strategien zur Einführung der Cloud auswirken und Ihre digitale Transformation verlangsamen.

Datenschutzverletzungen und Datenlecks

Unsere Empfehlung zur Vermeidung von Datenschutzverletzungen ist es, für alle Arbeitslasten in Ihrer Hybrid Cloud-Umgebung eine verlässliche Cyberabwehr aufrechtzuerhalten. Die Sichtbarkeit und Transparenz von IT- und Sicherheitsschichten ist hier ebenfalls von entscheidender Bedeutung, denn so wird sichergestellt, dass Sie alle zu schützenden Arbeitslasten im Blick behalten. So können Sie auch automatisierte Cybersicherheitsfunktionen überall in Ihrer sich laufend ändernden flexiblen Cloud-Umgebung bereitstellen.

Die Sichtbarkeit der Infrastruktur stellt in den flexiblen digitalen Umgebungen von heute ein Problem dar. Möglicherweise ist Ihre Cybersicherheit selbst mittlerweile weniger transparent. Das bedeutet, dass Sie Risiken nicht immer direkt und unmittelbar feststellen können. Und selbst wenn Sie ein Risiko erkennen, könnte es bereits zu spät sein. Durch diesen fragmentierten Sicherheitsansatz werden hybride Unternehmens-Clouds zu einem beliebten Ansatzpunkt für Cyberkriminelle, nicht zuletzt, weil in der Regel dieselben Tools wie für Angriffe auf herkömmliche und Cloud-Infrastrukturen eingesetzt werden können. Eine ernsthafte Datenschutzverletzung kann zur Offenlegung vertraulicher Daten von Kunden oder Geschäftspartnern, von geistigem Eigentum und Betriebsgeheimnissen führen, was alles schwerwiegende Folgen hat.

Datenverlust oder Nicht-Integrität

Der effizienteste Weg zur Aufrechterhaltung von Datenintegrität ist die Implementierung von Cybersicherheitstools, die leistungsfähige Funktionen für den Laufzeitschutz bieten, einschließlich Verhaltensanalyse auf der Basis von lernfähigen Systemen. Damit wird die Erkennung äußerst hoch entwickelter, aber bisher noch nicht aufgedeckter Bedrohungen sowie von ausgeklügelter Ransomware möglich.

Datenschutzverletzungen werden zwar nach wie vor generell durch schädliche Aktivitäten verursacht, aber es gibt auch zahlreiche Szenarien, in denen Daten auch aufgrund unabsichtlicher Handlungen der Endbenutzer unzugänglich oder beschädigt werden. In den meisten Unternehmen gibt es Strategien für die Wiederherstellung von Daten, um gegebenenfalls die Mindestwiederherstellungsdauer (RTO) und den nächstmöglichen Wiederherstellungspunkt (RPO) zu gewährleisten. Eine Datensicherung oder -replikation bedeutet aber nicht unbedingt, dass Sie bei der späteren Datenwiederherstellung vor unliebsamen Überraschungen geschützt sind. Die Statistiken verzeichnen immer mehr erfolgreiche und überaus schädliche Ransomware-Angriffe auf Unternehmen aller Art, was aufzeigt, dass die Aufrechterhaltung der Datenintegrität keine leichte Aufgabe ist. Alter und Aufbewahrungsort der Daten spielen dabei keine Rolle (physisch, virtuell oder in Cloud-Umgebungen): Für die Risiken von Datenverlust oder Nicht-Integrität sind Sie immer selbst verantwortlich.

Unerwünschte oder anfällige Programme

Die erfolgreichsten Cyberabwehrstrategien basieren auf einer Kombination aus Application Startup Control (Whitelisting, „Default Deny“) und Funktionen für den Exploit-Schutz.

Endbenutzer im Unternehmen installieren aus verschiedenen Gründen Systeme und Programme aller Art und nutzen sie. Nicht immer können Sie kontrollieren, was auf den Geräten von Endbenutzern oder sogar auf geschäftskritischen Servern installiert ist. Je größer die Unternehmensumgebung, desto schwieriger ist es, alles unter Kontrolle zu behalten. Selbst geschäftskritische Programme, mit denen Sie völlig vertraut sind, sind unter Umständen nicht vollständig gefeit gegen Zero-Day-Schwachstellen und -Exploits, benötigen aber die unmittelbare Absicherung gegen potentielle Cyberrisiken.

Ressourcenhungrige Sicherheit

Sie müssen sich bewusst sein, dass Sie sich selbst ein klares Bild von allen Aspekten Ihrer Hybrid Cloud und der zugehörigen Bestandteile machen müssen. Ebenso sind Sie für die Implementierung von Cybersicherheitsfunktionen verantwortlich, mit denen eine möglichst effiziente Kombination aus Schutz und Ressourceneffizienz gewährleistet wird.

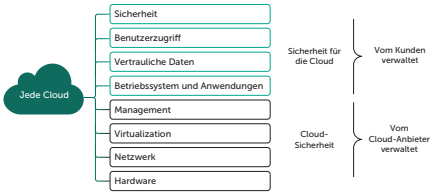
Die meisten Hybrid Clouds werden in einer Kombination aus softwarezentrierten privaten Rechenzentren und flexiblen Public Cloud-Diensten betrieben. Beide Umgebungen benötigen Schutz, wobei Technologien mit unterschiedlichen Integrationsmöglichkeiten miteinander kombiniert werden müssen. Der altbewährte Ansatz nach dem Motto „Virenschutz überall“ für Sicherheit der Hybrid Cloud, bedeutet einen hochgradig ineffizienten Einsatz Ihrer Cloud-Ressourcen. Die Effektivität geschäftskritischer Systeme wird beeinträchtigt, und die Rendite Ihrer digitalen Transformation reduziert sich erheblich.

Sicherheit und Fehlausrichtung der Infrastruktur

Die Arbeit mit Public Cloud-APIs und -Erweiterungen ermöglicht eine zuverlässige Verbindung zwischen IT- und Sicherheitsschicht, damit beide Schichten zusammenarbeiten und die Möglichkeiten der jeweils anderen unterstützen können. Weiterhin lässt sich dadurch die Bereitstellung von Sicherheitsfunktionen unabhängig vom Umfang Ihrer Hybrid Cloud-Umgebung vereinfachen.

Die Einführung der Hybrid Cloud fördert eine neue Dynamik und eine effektive Bestandsführung, bedeutet aber auch die fortlaufende Bereitstellung von Cybersicherheit für Hunderte neu eingerichteter Cloud-Arbeitslasten gleichzeitig, was sich am Ende zu einem Albtraum in Sachen IT-Sicherheit entwickeln kann. Als Sicherheitsprofi sind Sie mit einer eingeschränkten oder verzögerten Sichtbarkeit der von Ihren IT-Kollegen eingerichteten Cloud-Maschinen konfrontiert. Daher sind diese Maschinen bis zur nächsten Überprüfung des Unternehmensnetzwerks anfällig. Automatisierte, allgemein von den IT-Mitarbeitern einsetzbare Tools für Verwaltungsaufgaben wie Netzwerksegmentierung, Isolierung und Neukonfiguration der Topologie sind sehr nützlich, um schnell auf neu entstehende Cyberbedrohungen zu reagieren und eine angemessene Sorgfaltspflicht aufrechtzuerhalten. Wenn Ihre IT- und Sicherheitsschichten nicht ineinandergreifen, können die Sicherheitsteams nur das schützen, was sie sehen können. Die IT-Mitarbeiter können sie dann nicht bei der Wahrung eines wirklich sicheren und anpassungsfähigen Ökosystems in der gesamten Hybrid Cloud unterstützen.

Gemeinsame Verantwortung in Public Clouds



Public Clouds verfügen über ihre eigene integrierte Sicherheit. Aber das Modell der „Shared Responsibility" gibt vor, dass Sie trotzdem für die Sicherheit Ihrer Arbeitslasten, Programme und Daten in Public Clouds verantwortlich sind. Und wenn diese Arbeitslasten geschäftskritisch sind, ist es umso wichtiger, dieser Verantwortung gerecht zu werden. Microsoft Azure ist ein führender Public Cloud-Dienst, der eine hoch entwickelte Cloud-Umgebung mit herausragender Zuverlässigkeit und Skalierbarkeit bietet.

Allerdings erfordert das Modell der gemeinsamen Verantwortung zusätzliche Funktionen, die eine flexible Cybersicherheitsschicht über Ihre gesamte Cloud-Umgebung (Public und Private) hinweg ermöglichen und auch die Daten in Ihrer Azure-Umgebung vollständig schützen. Sie müssen sich der Risiken vollständig bewusst sein und wissen, wie entsprechende Risiken über Ihr gesamtes Cloud-Ökosystem hinweg zu beseitigen sind, einschließlich der Public Cloud-Präsenz.

Cybersicherheitserweiterungen zum Schutz der Azure-Cloud

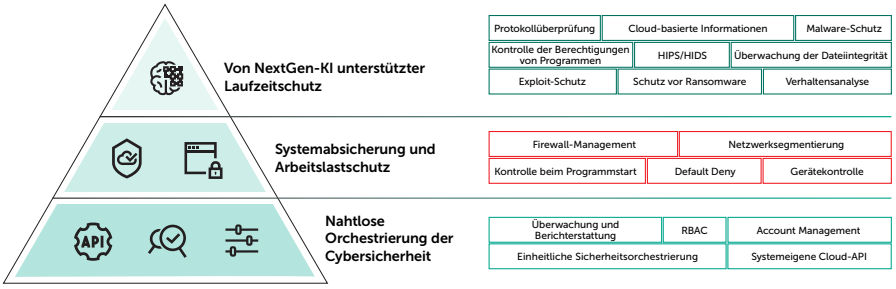
Kaspersky Lab möchte nicht nur einfach Next Generation-Schutz mit KI-Unterstützung auf Ihre Cloud-Umgebungen anwenden, sondern mit den Microsoft Azure-Erweiterungen arbeiten, um eine direkte und reibungslose Überwachung und Bereitstellung der Sicherheit zu ermöglichen. Diese einfache und unkomplizierte Verwaltung bedeutet, dass Arbeitslasten im Rahmen Ihrer Azure-Infrastruktur in Sekundenschnelle geschützt werden können, wodurch Ihre Cloud-Ressourcen und die Benutzer abgesichert werden.

Zunächst bringen wir unsere innovativen „Next Generation"-Funktionen ein, die auf unserer umfassend getesteten und in der Branche vielfach ausgezeichneten[1], weithin anerkannten[2] Protection Engine beruht. Next Generation-Cybersicherheit bedeutet, dass Menschen und Maschinen gemeinsam eine adaptive Cloud-Sicherheitsumgebung erschaffen. So können Sie und Ihre integrierte Cloud-basierte Sicherheit selbst ausgeklügelte Cyberbedrohungen erkennen und darauf reagieren.

Echter Next Generation-Schutz

Zusätzlich zu den nativen Cloud-Tools von Azure bieten wir vorausschauende, KI-gestützte Systeme und Laufzeitschutz, darunter die folgenden:

- **Unsere vielfach ausgezeichnete Anti-Malware-Engine** stellt automatischen Echtzeitschutz auf Dateiebene für jede Cloud-Umgebung bereit, sowohl beim Zugriff als auch auf Abruf.
- **Cloud-basierte Aufklärung** identifiziert im Handumdrehen neue Bedrohungen und stellt automatische Updates bereit.
- **Verhaltenserkennung** bei der Überwachung von Programmen und Prozessen schützt vor hoch entwickelten Bedrohungen und sogar vor körperloser Malware. In Cloud-Umgebungen vorgenommene schädliche Aktivitäten werden bei Bedarf per Rollback zurückgeführt.
- **Exploit-Schutz** sorgt für die Kontrolle von Systemablaufprozessen und Programmverhalten und unterstützt auf diese Weise die Abwehr hoch entwickelter Bedrohungen, einschließlich Ransomware.
- **Anti-Ransomware** schützt Cloud-Umgebungen und die zugehörigen freigegebenen Netzwerke vor Angriffen und stellt per Rollback gegebenenfalls betroffene Dateien im Zustand vor der Verschlüsselung wieder her.
- **HIPS/HIDS** dient der Aufdeckung netzwerkbasierter Eingriffe in Cloud-Ressourcen.
- **Programmkontrolle** ermöglicht es Ihnen, alle Hybrid Cloud-Umgebungen für eine optimale Systemabsicherung im Modus „Default Deny" zu verankern und zu bestimmen, welche Programme wo ausgeführt werden und auf was sie zugreifen dürfen.
- **Gerätekontrolle** legt fest, welche virtuellen Geräte auf einzelne Cloud-Umgebungen zugreifen dürfen, während Webkontrolle vor Cyberbedrohungen im Internet schützt.
- **Netzwerksegmentierung** sorgt für Transparenz und automatisierten Schutz von Netzwerken mit Hybrid Cloud-Infrastruktur.
- **Schwachstellenabschirmung** hindert hoch entwickelte Malware und Zero-Day-Bedrohungen daran, ungepatchte Schwachstellen auszunutzen.
- **E-Mail-Sicherheit** einschließlich Anti-Spam schützt den E-Mail-Verkehr in Cloud-Umgebungen.
- **Websicherheit** einschließlich Anti-Phishing schützt vor Bedrohungen durch potentiell gefährliche Webseiten und Skripte.
- **Überwachung der Dateiintegrität** schützt kritische und Systemdateien, während bei der Protokollüberprüfung interne Protokolldateien im Hinblick auf die Betriebshygiene untersucht werden.



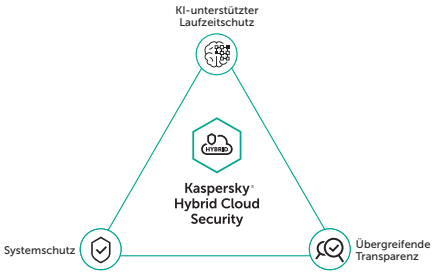
Alle diese Möglichkeiten zum Schutz der physischen und der virtuellen Serverumgebung sowie der Ressourcen in der Azure-Cloud werden in einem einzigen Produkt von Kaspersky Lab bereitgestellt – mit übergreifender Verwaltung über eine einheitliche Sicherheitskonsole.

1 https://www.kaspersky.de/top3

2 Gartner Peer Insights Customer Choice Awards für Endpoint Protection-Plattformen

Warum Kaspersky Hybrid Cloud Security?

- Für physische, virtuelle und Cloud-Umgebungen entwickelt
- Mehrstufiger integrierter Schutz für alle privaten Rechenzentren
- Nahtloser, automatisierter und flexibler Schutz für Azure-Public Clouds
- Umfasst ein vollständiges Set an Sicherheitstools, um der gemeinsamen Verantwortung gerecht zu werden
- Orchestrierung einer unternehmensgerechten Sicherheit über Ihre gesamte Hybrid Cloud hinweg



Integrierter Schutz, Sichtbarkeit und Orchestrierung

Umfassende Sicherheit

Dank diesen qualitativ herausragenden und umfangreichen Funktionen zur mehrstufigen Sicherheit Ihrer Private und Public Cloud können Sie sich darauf verlassen, dass alle Ihre Arbeitslasten an allen Speicherorten in einem umfassenden -Hybrid Cloud-Ökosystem angesiedelt sind.

Für die Cloud optimierte Bereitstellung

Die Cybersicherheitsfunktionen sind über Azure-Erweiterungen verfügbar, sodass sie direkt in Ihrer Cloud-Umgebung bereitgestellt werden und Ihre „always on" – Geschäftsanwendungen durchgehend schützen können.

Richtlinienkonformität

Dank unserem Ansatz einer integrierten Sicherheitslösung können Sie darauf vertrauen, dass die Sicherheit aller Inhalte in Ihrer Azure-Cloud Ihre Unternehmensstandards erfüllt und Ihre Ressourcen und Benutzer jederzeit sicher sind.

Einheitliche Orchestrierung

Cybersicherheit wird dank der Integration in das Azure Security Center zu einem selbstverständlichen Teil Ihrer Cloud.

Vereinfachte Sicherheitsbereitstellung

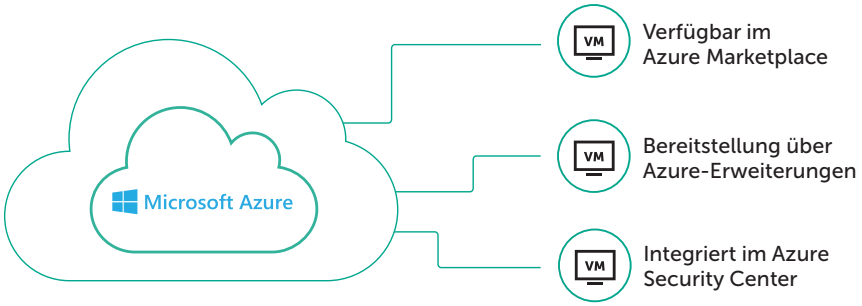
Sie können mehrstufigen Schutz für Azure-Cloud-Umgebungen direkt vom Azure MarketPlace aus bereitstellen.

Flexible Lizenzierung

Mehrere Lizenzierungs- und Preisoptionen, darunter BYOL (Bring-Your-Own-License) und PPU (Pay-Per-Use). So können Sie Ihre Investitionen in IT und die digitale Transformation optimal nutzen und bei Ihrem Cloud-Migrationsprojekt eine hohe Rendite erzielen.

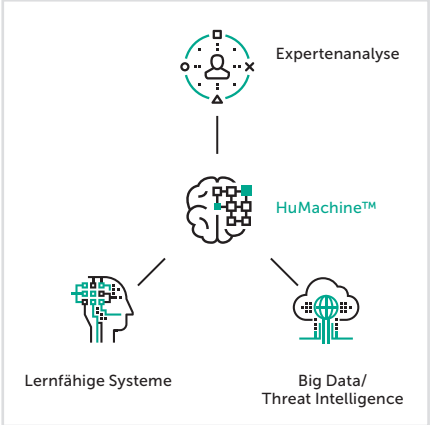
Cloud-Sicherheit, die einfach funktioniert

Das Gesamtergebnis ist eine perfekt orchestrierte und adaptive Cybersicherheits-Infrastruktur mit genau den richtigen Funktionen für Ihre Hybrid Cloud-Umgebung, die für Ressourceneffizienz und eine nahtlose Orchestrierung sorgen.



Die Zukunft der Unternehmens-IT absichern

Microsoft Azure verändert die Unternehmens-IT. Kaspersky Lab sorgt aktuell und in der Zukunft für die Sicherheit, Transparenz und Verwaltbarkeit aller Ihrer Arbeitslasten in der Azure-Cloud-Infrastruktur sowie in der Private Cloud-Umgebung.



Kaspersky Lab
Cybersicherheit für Unternehmen: **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