Kaspersky® Hybrid Cloud Security

Zuverlässiger Schutz und nahtlose Orchestrierung für Ihre Hybrid Cloud

Wichtigste Herausforderungen beim Umstieg in die Cloud:

- Steigende Infrastrukturkomplexität führt zu geringerer Transparenz
- Ein mehrstufiger Ansatz, der Schlüssel für zuverlässigen Schutz, ist selten in einem einzigen Produkt zu finden
- Herkömmliche speicherintensive Sicherheitslösungen belasten Systemressourcen
- Ein Siloansatz und uneinheitliche Steuerelemente bedeuten zusätzliche Herausforderungen für Verwaltung und Sicherheit
- Malware und Ransomware zielen auf virtuelle und physische Endpoints ab
- Wenn versäumt wird, angemessene Cybersicherheitsmaßnahmen für den Schutz personenbezogener Daten zu ergreifen, können rechtliche Problemen entstehen.

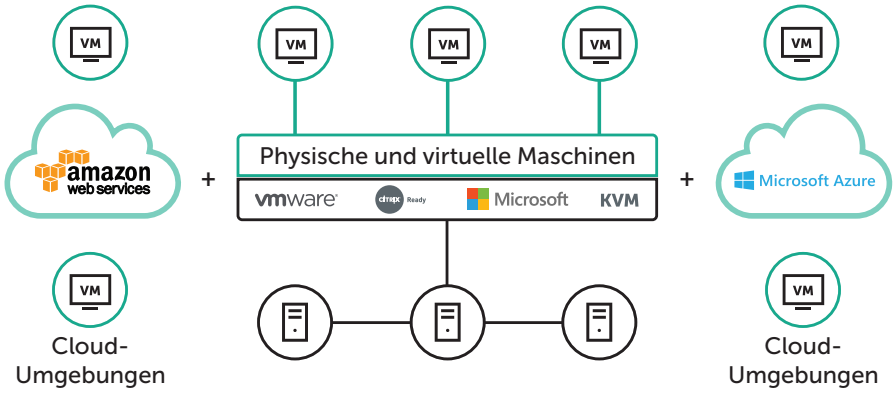
Warum Kaspersky Hybrid Cloud Security?

- Für physische, virtuelle und Cloud-Umgebungen entwickelt
- Integrierte mehrstufige Sicherheit für alle Arten von Workloads
- Nahtloser, automatisierter und flexibler Schutz für AWS und Azure Public Clouds
- Umfasst ein vollständiges Set an Sicherheitstools, um der gemeinsamen Verantwortung gerecht zu werden
- Nahtlose Orchestrierung der Sicherheit über die gesamte Hybrid Cloud hinweg
- Umfassend getesteter, sichererer Schutz, nachgewiesen[1] durch vielfache Auszeichnungen und unabhängige Tests
- Basiert auf von Kunden anerkannten und vertrauenswürdigen Technologien, unter anderem in Form des „Platinum Customer Award" von Gartner Peer Insights.

1 Die angeführten Untersuchungen beziehen sich auf eine Reihe von Produkten von Kaspersky Lab, die die gleichen Schutztechnologien wie Kaspersky Hybrid Cloud Security bieten.

Virtualisierung ist heute ein entscheidender Ansatz für Unternehmen, die flexibel und effizient sein wollen. Cloud Computing ist dabei der nächste logische Schritt. So müssen Unternehmen keine komplexen Infrastrukturen mehr unterstützen und können bis dato unerreichbare Effizienz erzielen. Die Cloud birgt jedoch auch Risiken – einige sind neu, andere gleichen denen aus physischen Umgebungen.

Kaspersky Hybrid Cloud Security bietet in allen Phasen und Szenarien der Umsetzung Ihrer Cloud-Infrastruktur einheitliche Sicherheit. Die Lösung eignet sich für die Cloud-Migration und für native Cloud-Szenarien und schützt Ihre physischen und virtuellen Workloads, ganz gleich, ob sie vor Ort, in einem Rechenzentrum oder in einer Public Cloud ausgeführt werden. Da die Programme im Hinblick auf Virtualisierung und Serverbetrieb entwickelt wurden, erhalten Sie ohne Einschränkung der Systemleistung einen überaus ausgewogenen Schutz vor hoch entwickelten aktuellen und künftigen Bedrohungen.



Hauptvorteile

Ermöglicht einen sicheren Umstieg in die Cloud – ohne Kompromisse beim Sicherheitsniveau

- Patentierte Technologien und unsere vielfach ausgezeichnete Cybersicherheits-Engine sorgen für den Schutz aller Workloads, ob physisch, virtuell oder in der Cloud.
- Mehrstufiger Echtzeitschutz auf der Grundlage maschinellen Lernens sichert Ihre Daten, Prozesse und Programme gegen neu entstehende Bedrohungen ab.
- Durch einen ganzheitlichen Ansatz bei der Datensicherheit werden Risiken durch Reputationsverlust und rechtliche Probleme im Zusammenhang mit Datenschutzvorschriften reduziert.

Ansatz von Kaspersky HuMachine™

Unterstützt durch die nahtlose Kombination von Big Data Threat Intelligence, Funktionen lernfähiger Systeme und menschlicher Expertise bietet Kaspersky HuMachine™ zahlreiche Vorteile und einen effizienteren Schutz. Durch die Kombination aller Elemente wird jede einzelne Komponente zu einem noch effizienteren und effektiveren Ganzen optimiert.

Sorgt dafür, dass Sie das Beste aus Ihren Ressourcen und Investitionen herausholen

- Agentenloser und agentenbasierter „Light"-Schutz sichert virtuelle Ressourcen in normalen und softwarebasierten Netzwerken, ohne die Leistung zu beeinträchtigen.
- Dank der Integration in die native Sicherheit von Public und Managed Clouds können Programme, Betriebssysteme, Datenströme und Benutzer-Workspaces unter minimaler Beanspruchung abgesichert werden.
- Die Verwaltung physischer und virtueller Ressourcen mithilfe einer Ansicht spart bei Einführung und Wartung Personalstunden ein.

Bietet Transparenz und Kontrolle unabhängig von der Konfiguration Ihrer hybriden Infrastruktur

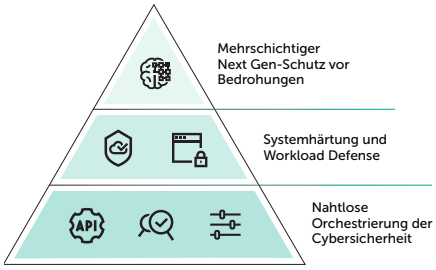
- Verwaltung und Sicherheitsorchestrierung funktionieren nahtlos über mehrere Clouds hinweg.
- Vollständige Transparenz und Kontrolle sowie ein ganzheitlicher Schutz vor hoch entwickelten Bedrohungen für Workloads an beliebigen Orten.
- Einfachere Bereitstellung von Sicherheitsservices und richtlinienbasierter Betrieb über Ihre gesamte Hybrid Cloud hinweg.

Funktionen

Mehrstufiger Schutz vor Bedrohungen dank HuMachine

Next Generation-Malware-Schutz von Kaspersky umfasst mehrere proaktive Sicherheitsschichten, die eine breite Palette von Cyberangriffen auf unternehmenskritische Arbeitslasten abwehren können.

- **Globale Threat Intelligence** bietet Echtzeitdaten zum Status der sich ändernden Bedrohungslandschaft und sorgt somit für kontinuierlichen Schutz.
- **Lernfähige Systeme:** Die weltweite Big Data Threat Intelligence wird durch die kombinierte Leistung maschineller Algorithmen und menschlicher Expertise verarbeitet, was zu hohen Erkennungsraten mit minimalen Fehlalarmen führt.
- **Schutz vor Web- und E-Mail-Bedrohungen** ermöglicht die sichere Ausführung virtueller und Remote-Desktops mit Schutz vor E-Mail- und webbasierten Bedrohungen.
- **Überwachung der Dateiintegrität** trägt dazu bei, die Integrität von kritischen Systemkomponenten und anderen wichtigen Dateien zu gewährleisten.
- **Protokollüberprüfung** untersucht interne Protokolldateien im Hinblick auf optimale Betriebshygiene.
- **Verhaltensanalyse** überwacht Programme und Prozesse und schützt vor hoch entwickelten Bedrohungen, einschließlich körperloser oder Skript-basierter Malware.
- Die **Remediation Engine** sorgt ggf. für das Rollback aller schädlichen Aktivitäten innerhalb von Cloud-Umgebungen.
- **Exploit-Schutz** bietet wirksamen Schutz vor neuen Angriffen und sorgt dabei für weitreichende Kompatibilität mit geschützten Programmen – unter minimalen Auswirkungen auf die Leistung.
- **Anti-Ransomware-Funktionen** schützen virtuelle Workloads vor allen Versuchen, Lösegeld für geschäftskritische Daten zu erpressen, indem betroffene Dateien per Rollback in den Zustand vor der Verschlüsselung zurückversetzt und die von außen angesetzte Verschlüsselung abgewehrt werden.
- **Schutz vor Bedrohungen im Netzwerk** erkennt und verhindert netzwerkbasierte Eingriffe in Cloud-Ressourcen.



Einheitliche Sicherheit für alle Cloud-Umgebungen

Public Clouds
- Amazon Web Services (AWS)
- Microsoft Azure

Private Rechenzentren:
- VMware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM
- Proxmox

VDI-Umgebungen
- VMware Horizon
- Citrix XenDesktop

Physische Server
- Windows
- Linux

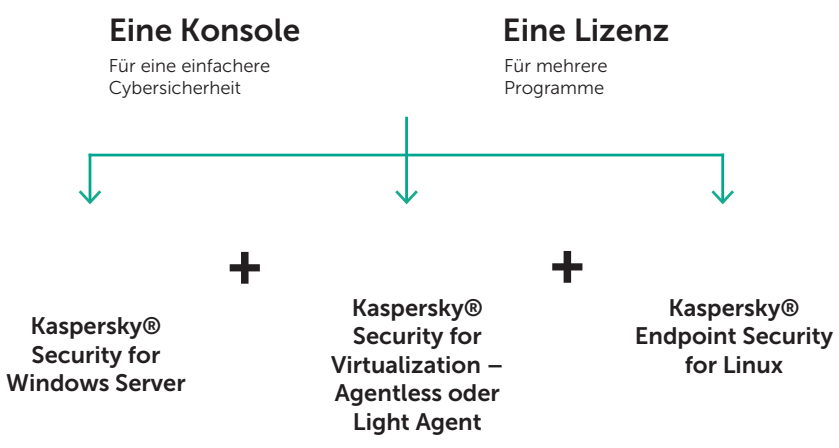
Systemabsicherung sorgt für erhöhte Stabilität

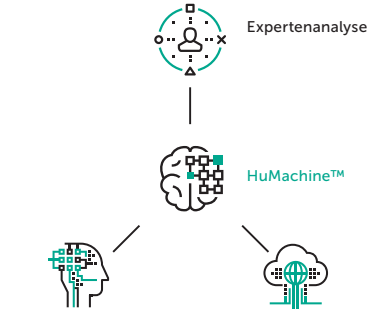
- **Programmkontrolle** ermöglicht die Verankerung all Ihrer Hybrid Cloud-Umgebungen im Modus „Default Deny" für eine optimale Systemabsicherung. Auf diese Weise können Sie die Palette der ausgeführten Programme auf rechtmäßige und vertrauenswürdige Programme beschränken.
- **Gerätekontrolle** legt fest, welche virtuellen Geräte auf einzelne Cloud-Umgebungen zugreifen dürfen.
- **Webkontrolle** regelt die Verwendung von Webressourcen durch virtuelle und Remote-Desktops, um Risiken zu minimieren und die Produktivität zu fördern.
- **Hostbasierte Angriffsüberwachung (Host Intrusion Prevention System, HIPS)** weist gestarteten Programmen Vertrauenskategorien zu und schränkt auf diese Weise den Zugriff auf kritische Ressourcen sowie die Möglichkeiten dieser Programme ein.

Übergreifende Transparenz

- **Unified Security Management** über das Kaspersky Security Center ermöglicht die Sicherheitsverwaltung mithilfe einer Ansicht über die gesamte Infrastruktur mit Endpoints und Servern hinweg – im Büro, im Rechenzentrum und in der Cloud.
- **Cloud-API:** Nahtlose Integration mit öffentlichen AWS- und Azure-Umgebungen ermöglicht das Erkennen der Infrastruktur, die automatisierte Bereitstellung von Agenten und die richtlinienbasierte Verwaltung sowie eine einfachere Bestands- und Sicherheitsbereitstellung.
- **Flexible Verwaltungsoptionen** bieten Flexibilität durch Mehrmandantenfähigkeit, genehmigungsorientiertes Account Management und rollenbasierte Zugriffssteuerung, während die Vorteile der einheitlichen Orchestrierung über einen einzelnen Server erhalten bleiben.
- **SIEM-Integration:** In Infrastrukturen mit ausgereifterer IT kann „Security Information and Management Systems" über das gesamte hybride IT-Netzwerk hinweg als einheitliches Fenster für unterschiedliche Aspekte der Cybersicherheit eines Unternehmens eingesetzt werden.

Kaspersky Hybrid Cloud Security bietet mehrere vielfach ausgezeichnete und branchenweit anerkannte Sicherheitstechnologien, mit denen Sie für eine einfachere Unterstützung und Transformation Ihrer IT-Umgebung sorgen. Die Lösung ermöglicht eine sichere Migration von physischen zu virtuellen Umgebungen und in die Cloud. Hohe Sichtbarkeit und Transparenz führen zu einer einwandfreien Sicherheitsorchestrierung.





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