Virtualization Security mit Kapersky Hybrid Cloud Security - ein Leitfaden zu den Funktionen

# Light Agent oder Agentless?

kaspersky

# Zusammenfassung

Virtualisierung wird weiterhin weitgehend in der gesamten Unternehmenswelt eingesetzt. Aus gutem Grund. Signifikante Einsparungen von Ressourcen sind möglich durch den Einsatz virtueller Maschinen (VM), wenn und wo immer sie gebraucht werden. Einen 'herkömmlichen' Sicherheitsansatz mit einem vollen Sicherheitsagenten auf jeder Maschine für virtualisierte Umgebungen einzusetzen, ist ressourcenintensiv und kann den ROI ernsthaft beeinträchtigen. Damit werden die Vorteile der Virtualisierung wieder ausgehebelt.

Die Antwort liegt in der Verringerung der Rechner- und Speicherbelastung des Agenten auf dem virtuellen Gerät. Kaspersky Hybrid Cloud Security erreicht das durch zwei verschiedene Ansätze – Agentless und Light Agent.

Dleser Leitfaden erklärt wie jeder dieser Ansätze funktioniert und erläutert die Merkmale und Vorteile jedes Ansatzes.

# Sichern von virtualisierten Umgebungen - die Herausforderung

Virtualisierte Umgebungen stellen einzigartige Herausforderungen dar, die berücksichtigt werden müssen, wenn verschiedene Sicherheitslösungen bewertet werden.

Die immer stärkere Verbreitung der Virtualisierung macht den Bedarf an geeigneten Sicherheitslösungen offensichtlich. Obwohl virtualisierte Umgebungen genauso anfällig für Cyberangriffe sind wie physische Systeme, bergen sie doch einige Herausforderungen, die bei der Bewertung verschiedener Sicherheitslösungen berücksichtigt werden müssen.

Unternehmen können dieselbe Sicherheitssoftware zum Schutz von physischen und virtuellen Maschinen einsetzen. Standardlösungen, die nicht speziell für virtualisierte Umgebungen entwickelt wurden, können zwar ein bestimmtes Maß an Schutz bieten, sie bergen jedoch häufig auch Risiken wie die folgenden:

- **Exzessive Ressourcennutzung:** Verursacht durch die Replikation von Signaturdatenbanken und aktiven Anti-Malware-Engines auf der jeweiligen geschützten virtuellen Maschine (VM).
- **„Storms“:** Simultane Datenbank-Updates und/oder Anti-Malware-Scans auf mehreren VMs führen zu einer lawinenartigen Zunahme der Ressourcenauslastung, die drastische Leistungseinbußen bis hin zum Denial of Service (DoS) verursachen können. Versuche, dieses Problem durch die Planung solcher Prozesse zu umgehen, führen zu „Vulnerability-Zeitfenstern“ – Zeitphasen, in denen auf einen späteren Zeitpunkt verlegte Malware-Scans die VM für Angriffe anfällig machen.
- **Instant-on-Lücken:** Signaturdatenbanken können nicht auf inaktiven VMs aktualisiert werden. Alsovom Start der Maschine bis zum Abschluss des Update-Vorgangs ist die VM für Angriffe anfällig.
- **Imkompatibilitäten:** Da Standardlösungen nicht für virtualisierungsspezifische Funktionen wie die Migration von VMs oder nicht persistentem Speicher geschaffen sind, kann ihre Nutzung zu Instabilität und sogar Systemabstürzen führen.

# Herausforderungen meistern - zwei Ansätze

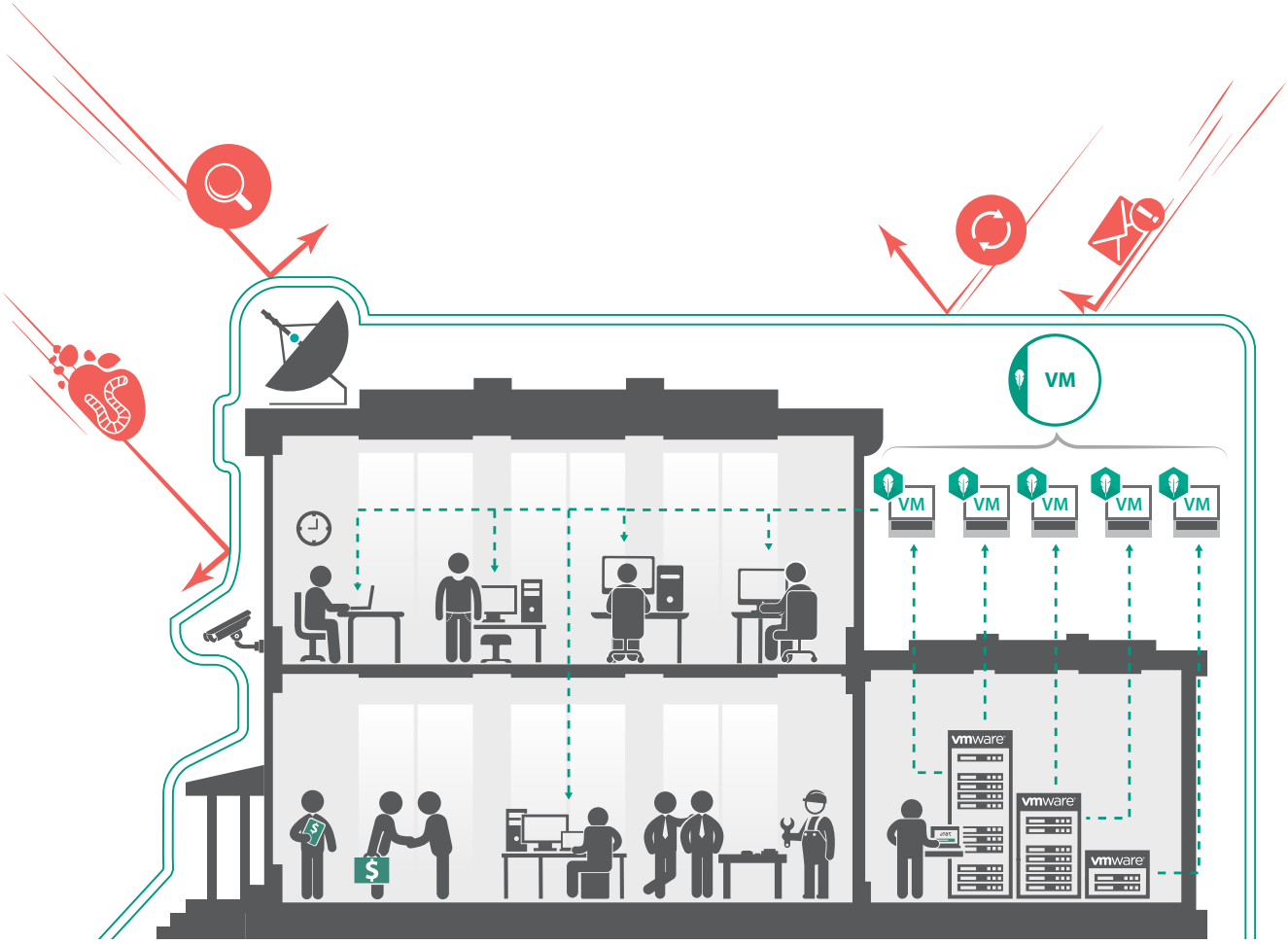
Die Light Agent-Lösung von Kapersky deckt eine große Anzahl von Plattformen ab, unter anderen:

- **Microsoft Hyper-V**
- **Citrix Hypervisor**
- **Citrix Virtual Apps und Desktops,**
- **KVM**
- **VMware vSphere**
- **VMware NSX**
- **VMware Horizon**

Marktführer VMware entwickelte mit der vShield-Endpoint-Technologie einen speziellen Verteidigungs-Layer für seine vSphere-Virtualisierungsplattform. Dieser zusätzliche Layer schafft einen integrierten sicheren Raum für Drittanbieterlösungen, die nativ über VMware-APIs, wie z. B. vShield Endpoint und NSX Guest Introspection, integriert werden können und alle virtualisierten Assets umfassen. So erhalten entsprechende Sicherheitslösungen einfachen und effizienten Zugriff auf die entsprechenden Ressourcen.

Es ist nur eine Security Virtual Machine (SVM) – eine spezielle, mit Anti-Malware-Scan-Engine und Signaturdatenbanken ausgestattete virtualisierte Maschine – pro Host erforderlich, sodass die Ressourcen einzelner VMs geschont werden und die Ressourcenauslastung erheblich reduziert wird. Der größte Vorteil dieses Ansatzes für Unternehmen ist die naht- und reibungslose Integration in die VMware-Umgebung.

Eine Alternative stellen Lösungen dar, die von APIs bzw. Virtualisierungsplattformen unabhängig agieren und einen ressourcenschonenden Agenten nutzen, der für das Betriebssystem der jeweiligen VM optimiert ist. Da sich Scan-Engine und Datenbanken auch bei diesem Ansatz zentral auf der SVM befinden, beansprucht die Light-Agent-Technologie die Systemressourcen deutlich weniger als traditionelle Lösungen mit Full Agents. Die Lösung ist eingebettet zwischen agentenlosen und herkömmlichen vollen Agentenlösungen in Bezug auf Ressourcenverbrauch, aber sie ist nicht gebunden, oder noch wichtiger, begrenzt durch VMWare-Technologien, und kann auf anderen populären Plattformen eingesetzt werden.




**Sie entscheiden.**
Kaspersky Hybrid Cloud Security umfasst sowohl Agentless als auch Light Agent-Anwendungen - Sie entscheiden, welche Sie wo einsetzen wollen.

# Die Lösung - Bereitstellung von beiden on Premise und in der Cloud

Kapersky Hybrid Security bietet mit nur einer Konsole und einer einzigen Ansicht einheitlichen Schutz und Kontrolle für den gesamten virtualisierten Bestand einer Organisation, sowohl on Premise als auch in öffentlichen Clouds.

Wir schützen den ROI unserer Kunden und ihre Ressourcen und Arbeitslasten durch die Minimierung der Belastung auf jeder VM.

Kaspersky Hybrid Cloud Security erreicht dies auf zwei verschiedene Weisen, wobei beide als Teil der Lösung angeboten werden:

- Unsere agentenlose Lösung bietet erhebliche Leistungsvorteile, zusammen mit vereinfachtem Einsatz, durch Nutzung der Sicherheitsarchitektur, die von VMWare-Umgebungen angeboten werden.

- Unsere Light Agent-Architektur bietet umfangreichen mehrschichtigen Schutz für virtuelle Umgebungen mit einer viel geringeren Ressourcenbelastung als herkömmliche Sicherheitsagenten, und sie ist kompatibel mit allen wesentlichen Virtualisierungsplattformen.

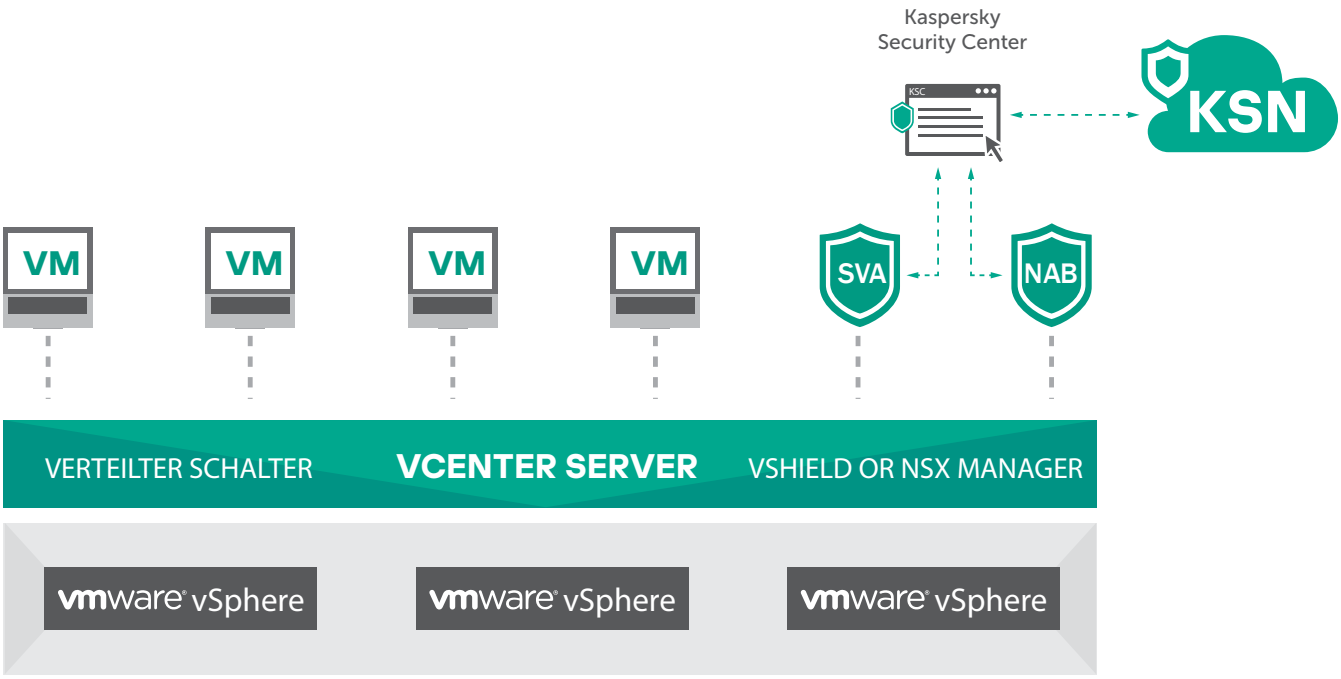
# KASPERSKY SECURITY FOR VIRTUALIZATION AGENTLESS

Kaspersky Security for Virtualization Agentless wurde speziell für die Nutzung von vShield Endpoint und der damit einhergehenden Vorteile entwickelt. Die direkt einsetzbare Security Virtual Appliance (SVA) wird von der vielfach ausgezeichneten Anti-Malware-Engine von Kaspersky Lab unterstützt und bietet eine hervorragende Erkennungsrate und Performance.

Die Unterstützung des cloud-gestützten Kaspersky Security Network-Service (KSN) gewährleistet schnellstmögliche Reaktionszeiten und was am Wichtigsten ist, die Erkennung neuer Malware im weniger als 0,02 Sekunden. Die ermöglicht Kapersky Hybrid Cloud Security Ihre virtualisierte Umgebung gegen sogar die neusten Bedrohungen zu schützen.

VMware NSX-Umgebungen können die Vorteile der Integration zwischen Kaspersky Security for Virtualization Agentless und VMware NSX Guest Introspection optimal nutzen. So lässt sich Ihre Infrastruktur skalieren, während Ihre Sicherheitslösung nahtlos über alle Topologie- und Infrastrukturänderungen informiert ist.

## KASPERSKY SECURITY FOR VIRTUALIZATION AGENTLESS




Für einen fortgeschrittenen Netzwerkschutz kann eine zweite SVA genutzt werden, um die Funktionalität des Kapersky Network Attack Blockers zu liefern. Das erfolgt eng integriert in die vCloud Networking & Security-Komponente von VMWare.

# Zwei wichtige Überlegungen

Es gibt einige Nachteile beim agentenlosen Ansatz.

Erstens ist VMWare vSphere die einzige Virtualisierungsplattform, die eine Zwischenschicht -vShield-Endpunkt bietet. Bei anderen Virtualisierungsplattformen muss die Sicherheitslösung eine Art von Agenten innerhalb des Gastbetriebssystems der jeweiligen VMs installiert werden, um Dateiscans auf Geräteebene durchführen zu können.

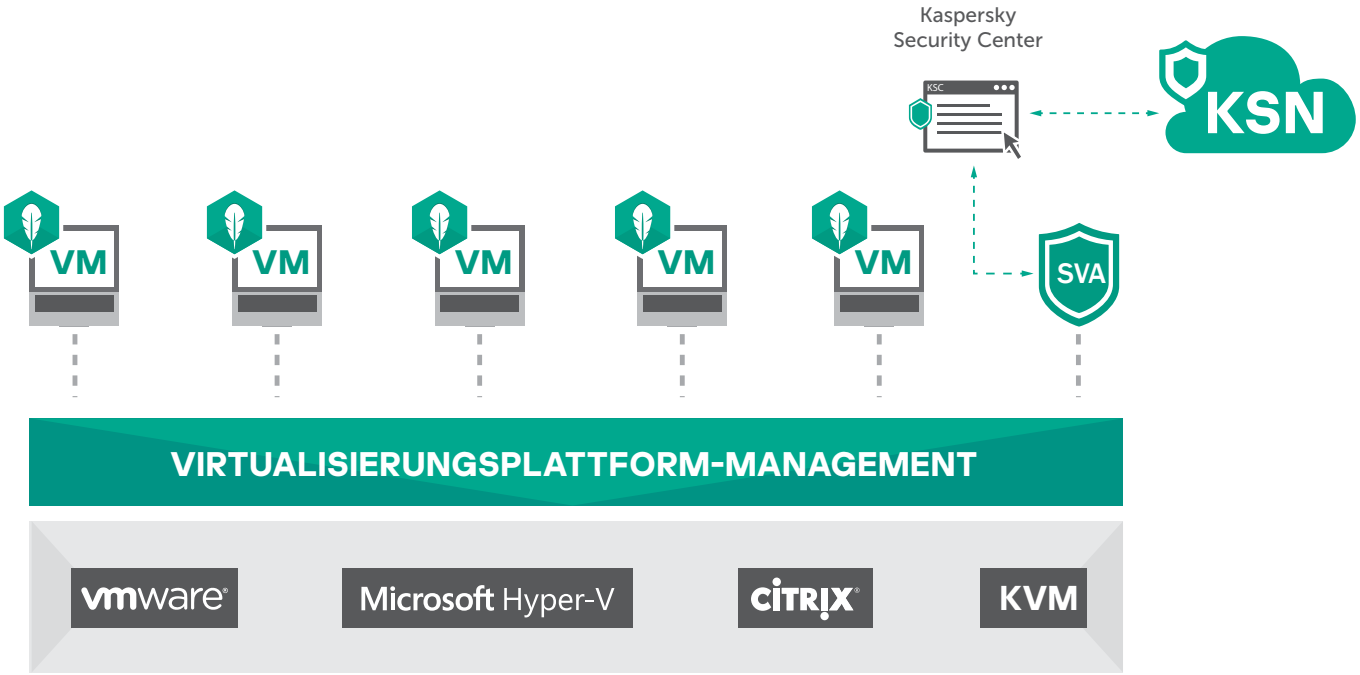
Zweitens bieten native Technologien wie vShield Endpoint und NSX Guest Introspection aufgrund des VMware-Designs keinen Zugriff auf die internen Prozesse, Programme und den Web-Datenverkehr der VM sowie auf virtualisierte Geräte. Deshalb ist der Schutz der Infrastruktur auf Scans der Dateiebene beschränkt, was die Fähigkeit der Lösung, tief gehenden Schutz vor fortschrittlicher Malware auf individueller VM-Ebene zu bieten, deutlich einschränkt.

# KASPERSKY SECURITY FOR VIRTUALIZATION LIGHT AGENT

Der Ansatz mit Light Agent umgeht all diese Einschränkungen. Weil sich Scan-Engine und Datenbanken auch bei diesem Ansatz zentral auf der SVA befinden, beansprucht diese Anwendung die Systemressourcen deutlich weniger als traditionelle Lösungen mit Full Agents. Der auf den VMs installierten Light Agent bietet Zugriff auf den Arbeitsspeicher, die Programme und die internen Prozesse des der individuellen VM sowie auf Web-Datenverkehr und virtualisierte Geräte. Mithilfe dieses Zugriffs können fortschrittliche Sicherheitstechnologien direkt auf VM-Ebene installiert werden. So werden Effizienz und Performance der Virtualisierungsplattform geschont.

Kapersky Security für Virtualization Light Agent wurde speziell für virtualisierteUmgebungen entwickelt und unterstützt die beliebtesten Plattformen: Citrix Hypervisor, Citrix Virtual Apps und Desktops, Microsoft Hyper-V, VMWare vShield, NSX, Horizon, KVM und andere.

## KASPERSKY SECURITY FOR VIRTUALIZATION LIGHT AGENT




Kaspersky Security für Virtualization Light Agent bietet ein leistungsstarkes mehrschichtiges Verteidigungsperimeter, das fähig ist, ausgeklügelte Malware und sogar die allerneuesten Bedrohungen zu eliminieren. Nutzer profitieren von Technologien wie HIPS (Host-Based Intrusion Prevention System), einer persönlichen Firewall.Automatic Exploit Prevention und einer vollständigen Reihe von Endpunktkontrollen. Die Architektur der Lösung reduziert die Angriffsfläche deutlich und spart wertvolle Rechenressourcen.

Mit dem Light-Agent-Ansatz können Sie Ihre virtualisierte Umgebung, einschließlich virtuelle Server und VDI, ohne wesentlichen Einfluss auf die Performance des Hypervisor sichern. So schützen Sie Ihre Systeme und vertraulichen Unternehmensdaten vollständig, bewahren aber gleichzeitig die Maschinendichte und Qualität der Benutzererfahrung.

# Die schützenden Technologien von Kapersky vs. die Bedrohungen Ihrer virtualisierten Infrastruktur

VMs sind genauso gefährdet wie ihre physischen Pendants – vielleicht sogar noch mehr. In diesen blitzschnellen virtualisierten Netzwerken kann die Ausbreitung von Infektionen verheerende Folgen haben. Deshalb ist es wichtig, etwaige Sicherheitslücken in Ihrer virtualisierten Infrastruktur zu erkennen und eine effiziente Sicherheitslösung einzusetzen, die speziell vor fortschrittlichen Bedrohungen schützt. Im Folgenden untersuchen wir die Technologien, die eingesetzt werden, um potentiellen Bedrohungen von virtualisierten Systemen entgegen zu wirken.

## Programmkontrolle und Whitelisting

Wenn nur vertrauenswürdige Software auf einer VM ausgeführt werden darf, hat ausführbare Malware keine Chance. So halten Application Control und Dynamic Whitelisting Malware davon ab, Ihren virtualisierten Assets Schaden zuzufügen. Kaspersky Security for Virtualization Light Agent ermöglicht Endpoint-Kontrollen, einschließlich Application Control, die auf den einzelnen VMs aktiviert werden.

## Exploit Prevention

Unabhängige vom MRG Effitas-Institut durchgeführte Tests ergaben, dass die AEP-Technologie von Kaspersky selbst bei Deaktivierung aller anderen Schutzkomponenten zu 100 % wirksam gegen Angriffe ist, bei denen Exploits eingesetzt werden.

Die Ausnutzung von Schwachstellen, die in Systemkomponenten und häufig genutzten Programmen zu finden sind, ist jedoch weiterhin eine äußerst effektive Angriffsmethode. Es ist zwar möglich, diesen Angriffen entgegenzuwirken, wenn das betroffene Programm jedoch auf hoher Berechtigungsebene arbeitet, ist die Kontrolle über seine Aktivitäten beschränkt.

Die effektivste Methode, solche Bedrohungen abzuwehren, ist es, die Ausnutzung von Schwachstellen zu verhindern. Um der Gefahr ungepatchter Schwachstellen schnell Einhalt zu gebieten, bietet Kaspersky Security für Virtualization Light Agent eine Technologie, die wir Automatic Exploit Prevention (AEP) nennen. AEP überwacht speziell die am häufigsten angegriffenen Programme in kritischen Umgebungen wie VDI – darunter Adobe Reader, Internet Explorer, Microsoft Office und Java – und bietet dadurch eine zusätzliche Ebene der Sicherheitsüberwachung und des Schutzes vor unbekannten Bedrohungen.

Die Effizienz dieser Technologie wurde in unabhängigen Tests des MRG Effitas Institute bestätigt, in denen die AEP-Technologie von Kaspersky selbst bei Deaktivierung aller anderen Schutzkomponenten zu 100 % wirksam gegen Angriffe ist, bei denen Exploits eingesetzt werden (weitere Informationen hierzu finden Sie in Real World Enterprise Security Exploit Prevention, MRG Effitas, März 2015). Sogar unbekannte Zero-Day-Exploits werden mithilfe dieser Technologie blockiert.

## Vulnerability Assessment und Patch Management

Kaspersky Vulnerability & Patch Management stellt umfassende Informationen zu den Endpoints und Programmen bereit, die in Ihrem Netzwerk sind. Die Lösung erfasst Daten zu Softwareversionen und prüft, ob Updates erforderlich sind und Patches für Schwachstellen installiert werden müssen. Die erkannten Schwachstellen können automatisch priorisiert werden, sodass die wichtigsten Patches zuerst installiert und die wichtigsten Updates bevorzugt bereitgestellt werden. Sie erhalten einen vollständigen Überblick über Ihre Komponenten, die damit verbundenen Risiken und die Tools, um diese Risiken zu mindern.

## Systems Integrity Assurance

Diese Funktionen arbeiten neben der Programmkontrolle und den Exploit Prevention-Technologien, und können verwendet werden, um VMs auf Statusänderungen und Konfigurationsänderungen zu überwachen. Sie sind außerdem häufig aus Gründen der Compliance erforderlich.

Zu den Technologien rund um System Integrity Assurance gehören File Integrity Monitoring (FIM), Registry Integrity Monitoring und Baseline Management für virtualisierte Windows-Server.

# Netzwerksicherheit

Netzwerkbasierte Cyberbedrohungen können es dem Angreifer ermöglichen, wichtige Informationen über das Netzwerk abzurufen, Zugang zu den Ressourcen des angegriffenen Systems zu erhalten und so wichtige Prozesse zu stören und den reibungslosen Betrieb zu unterbrechen. Diese Bedrohungen beinhalten schädliche Aktionen wie Portscans, DoS-Attacken (Denial of Service) und Buffer-Underruns. Unsere beiden agentenlosen und Light Agent-Lösungen verfügen über native Netzwerk-Schutztechnologien. Kaspersky Security für Virtualization Light Agent erweitert den Netzwerkschutz um ein integriertes HIPS (Host-based Intrusion Prevention System) und zusätzliche Kaspersky-eigene Technologien zur Abwehr externer und interner Netzwerkangriffe – einschließlich Bedrohungen, die sich in nicht transparentem virtualisierten Datenverkehr verbergen.

Auch Kaspersky Security für Virtualization Agentless geht dieses Problem an, indem über die VMware-Integration unser Network Attack Blocker bereitgestellt wird. Hierbei handelt es sich um eine dedizierte virtuelle Appliance, die den Netzwerkdatenverkehr nach Anzeichen typischer Angriffsaktivitäten durchsucht.

# Behavioral Protection

Kaspersky Security für Virtualization Light Agent ist mit einer Reihe von Technologien ausgerüstet, die einen feindlichen Einfall in den Arbeitsspeicher der VM verhindern. Dazu zählen:

- System Watcher, der das Programmverhalten überwacht und Systemereignisse verfolgt.
- Behavioral Protection-Signaturen erkennen Malware-Aktivitäten anhand von Verhaltensmuster-Merkmalen.
- Privilege Control hindert Programme daran, unzulässige Änderungen, wie beispielsweise Prozessinjektionen vorzunehmen.

Diese Werkzeuge ermöglichen dem HIPS (Host-based Intrusion Prevention System) das Verfolgen und Stoppen schädlicher Prozesse im VM-Speicher.

# Schutz vor dateiloser Malware

Dateilose Malware ist Malware, die nicht direkt auf einer Festplatte gespeichert wird. Diese Art von Malware hat sich im Jahr 2017 weiter verbreitet wegen der sich erhöhenden Komplexität seiner Entdeckung und Ausmerzung. Obwohl solche Technologien sich auf zielgerichtete Angriffe beschränkten, vermehren sie sich heute mehr und mehr in der aktuellen Bedrohungslandschaft, und Kapersky registriert neue Familien von Trojaner-Klickern oder sogar Adware mit dateilosen Komponenten.

Hier sind erweiterte Techniken erforderlich, die Prozesse im Speicher überwachen und Programme sofort blockieren können, wenn diese verdächtige oder gefährliche Aktivitäten ausführen.

# Schutz vor schädlichen Websites

Eine der häufigsten Infektionsquellen sind schädliche oder infizierte Webseiten. Zwar wirken sich diese selten auf virtualisierte Server aus, jedoch stellen sie ein ernsthaftes Risiko für VDIs dar – eine Tatsache, die von vielen Unternehmensbenutzern gerne ignoriert wird. An dieser Stelle kommen die Web-Schutztechnologien von Kaspersky ins Spiel.

Anti-Phishing verhindert, dass Benutzer auf Webseiten zugreifen, die als gefährlich gemeldet wurden. Dafür werden Informationen aus dem Kaspersky Security Network (KSN) genutzt, die mithilfe von Millionen freiwilliger Teilnehmer des KSN überall auf der Welt kontinuierlich aktualisiert werden. Auch bisher nicht erkannte Phishing-Webseiten werden dank einer heuristischen Engine blockiert, die den Quelltext der geladenen Seite analysiert und dabei Hinweise auf schädlichen Code erkennt.

Mit der Web-Kontrolle können Sie die Internetnutzung steuern: Sie können den Zugang zu sozialen Netzwerken, Musik, Videos, externen E-Mail-Tools und anderen Webseiten mit unangemessenen oder gemäß Unternehmensrichtlinie ungeeigneten Inhalten blockieren. Darüber hinaus können Sie für unterschiedliche Benutzerrollen verschiedene Kontrollen festlegen und zwischen der vollständigen Blockierung und der Blockierung zu bestimmten Zeiten wählen.

# Ausführbare Programme zum Blocken von Malware

Ob es sich um einen heimtückischen E-Mail-Anhang, infizierte Unterhaltungsmedien oder ein temporär ausführbares Malware-Programm handelt – der Malware-Schutz ist unumgänglich, um diesen grundlegenden Bedrohungen Herr zu werden.

Den Kern von Kaspersky Security for Virtualization | Agentless und Light Agent bildet unsere leistungsstarke Anti-Malware-Engine, jedoch werden verschiedene Methoden eingesetzt, um auf die Dateiebene der geschützten VM zuzugreifen.

# Anti-Rootkit und Remediation-Technologien

Rootkit ist ein bösartiges Programm, das verschiedene Technologien anwendet, um schädlichen Code und Aktivitäten zu verbergen, und agiert aktiv gegen Antivirus-Technologien. Die Anti-Rootkit-Technologie als Teil des mehrschichtigen Schutzes der nächsten Generation von Kapersky entdeckt aktive Infektionen durch diese Rootkit-Programme und entfernt diese Art von Infektion aus den Systemen.

Kaspersky Security für Virtualization ermöglicht Ihnen den besten Ansatz für jeden Teil Ihrer virtualisierten Umgebung - Agentless, Light Agent oder eine Kombination aus beidem - mit einer Lizenz.

# Agentless oder Light Agent: Was ist besser?

Die Antwort hängt davon ab, welche Virtualisierungsplattform oder Plattformen Sie nutzen, von Ihrer spezifischen Infrastruktur und Ihren Sicherheitszielen.  Egal welcher Hypervisor verwendet wird, um Ihre virtualisierte Umgebung zu bilden. Sie können Ihre virtuellen Server und VDI mit Kapersky Security für Virtualization Light Agent schützen. Aber Sie können auch Kapersky Security für Virtualization Agentless für unkritische VMWare-basierte Server in Betracht ziehen.

Das Lizenzmodell von Kaspersky Security ermöglicht es Ihnen, den am besten geeigneten Ansatz für jeden Teil Ihrer virtualisierten Umgebung auszuwählen - Agentless, Light Agent oder eine Kombination von beiden - mit einer Lizenz. Sogar noch besser - flexible Lizensierung ermöglicht es auch, herkömmliche Endpoint Agents einzusetzen, was einen Weg bietet, stufenweise von der physikalischen Infrastruktur zum virtuellen Server oder Desktopinfrastruktur zu migrieren. So können Sie schrittweise migrieren, müssen aber nicht mit verschiedenen Paketen von Lizenzen für den jeweils physikalischen und virtuellen Einsatz jonglieren.

Welche Kombination von Virtualisierungsplattformen, und welchen Ansatz Sie auch immer nutzen, alle unsere virtuellen und physischen Maschinen, wie auch die Public Cloud Workloads, können einfach und zentral über eine einzelne vereinheitlichte Verwaltungsschnittstelle - das Kapersky Security Center - verwaltet werden.  Darüber hinaus ermöglicht die Nutzung von Kaspersky Security Network, unseres Cloud-basierten Sicherheitsservice, die sofortige Erkennung neuester Bedrohungen.

Kaspersky Hybrid Cloud Security:
kaspersky.com/hybrid
Cyber Threats News: de.securelist.com
IT Security News: kaspersky.de/blog/b2b
Cybersicherheit für SMB: kaspersky.de/business
Cybersicherheit für Großunternehmen:
kaspersky.de/enterprise

**www.kaspersky.de**



Bewährt. Unabhängig. Transparent. Wir wollen ein sicheres Umfeld schaffen, in dem Technologie unser Leben verbessert. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven.
Transparent.
Independent.