LIGHT AGENT ODER AGENTLESS

Leitfaden zu Kaspersky Security for Virtualization

Die zunehmende Verbreitung der Virtualisierung macht es immer wichtiger, dass Unternehmen auch geeignete Sicherheitslösungen einsetzen. Obwohl virtualisierte Umgebungen genauso anfällig für Cyberattacken sind wie physische Systeme, weisen sie doch einige besondere Merkmale auf, die im Hinblick auf Sicherheitslösungen bedacht werden müssen.

Standardlösungen, die nicht speziell für virtualisierte Umgebungen entwickelt wurden, können zwar ein bestimmtes Maß an Schutz bieten, sie bergen häufig jedoch auch Risiken wie:

1) **Exzessive Ressourcennutzung**: Verursacht durch die Replikation von Signaturdatenbanken und aktiven Anti-Malware-Engines auf der jeweiligen geschützten virtuellen Maschine (VM).
2) **„Storms“**: Simultane Datenbank-Updates und/oder Anti-Malware-Scans auf mehreren VMs führen zu einer lawinenartigen Zunahme der Ressourcennutzung, 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.
3) **„Instant-on“-Lücken**: Signaturdatenbanken auf nicht genutzten VMs können nicht aktualisiert werden, sodass die entsprechenden VMs vom Start bis zum Abschluss der Updates anfällig für Angriffe sind.
4) **Inkompatibilitäten**: Da Standardlösungen nicht für virtualisierungsspezifische Funktionen wie die Migration von VMs oder nicht persistentem Speicher geschaffen sind, kann ihre Nutzung zu Instabilität und Systemblockaden führen.

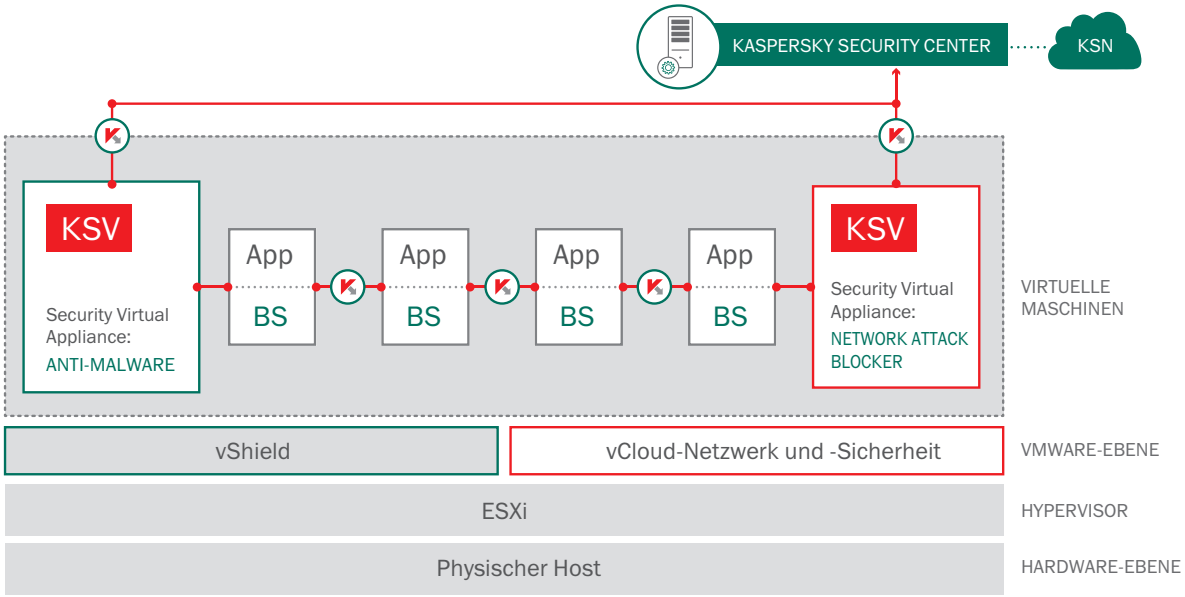
In Anerkennung der Bedeutung von Sicherheit für virtualisierte Systeme und der besonderen Merkmale der Virtualisierung entwickelte Marktführer VMware mit vShield eine spezielle Sicherheitsschicht für seine vSphere-Plattform. Diese Schicht erzeugt einen integrierten Sicherheitsbereich für alle virtualisierten Ressourcen und ermöglicht den einfachen und effizienten Zugriff durch entsprechend konzipierte Sicherheitslösungen. Ein offensichtlicher Vorteil dieses Konzepts ist, dass hiermit der „agentenlose“ Schutz virtualisierter Endpoints ermöglicht wird. Lediglich eine einzige Security Virtual Appliance (SVA) – eine spezielle, mit Anti-Malware-Scan-Engine und Signaturdatenbanken ausgestattete vrtuelle Maschine – ist erforderlich, sodass die Ressourcen einzelner VMs geschont werden, und somit der Ressourcenverbrauch erheblich reduziert wird. vShield-kompatible Sicherheitslösungen, die alle Funktionen einer VMware-Umgebung vollständig nutzen können, bieten zahlreiche Vorteile für Benutzer.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless wurde speziell für die Nutzung von vShield 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 hervorragende Erkennungsraten. Die Unterstützung des Cloud-basierten Kaspersky Security Network-Service sorgt für schnellstmögliche Reaktionszeiten. Sehr wichtig ist zudem, dass sie die Anzahl von Fehlalarmen (False-Positives) erheblich reduziert. Eine zweite SVA kann eingesetzt werden, um die Network Attack Blocker-Technologie von Kaspersky Lab in Verbindung mit der Komponente VMware vCloud Networking & Security zu nutzen.

Bei einem agentenlosen Ansatz gibt es jedoch auch Defizite.

Zunächst einmal ist VMware der einzige Anbieter, der eine zwischengeschaltete Sicherheitsschicht anbietet; bei anderen Plattformen muss die Sicherheitslösung einen anderen Weg für den Zugang zu einzelnen VMs finden. Zudem ermöglicht vShield nicht den Zugriff auf die internen Prozesse der virtuellen Maschinen, wodurch die Möglichkeit jeder Lösung, Malware auf dieser Ebene zu erkennen, deutlich abnimmt.



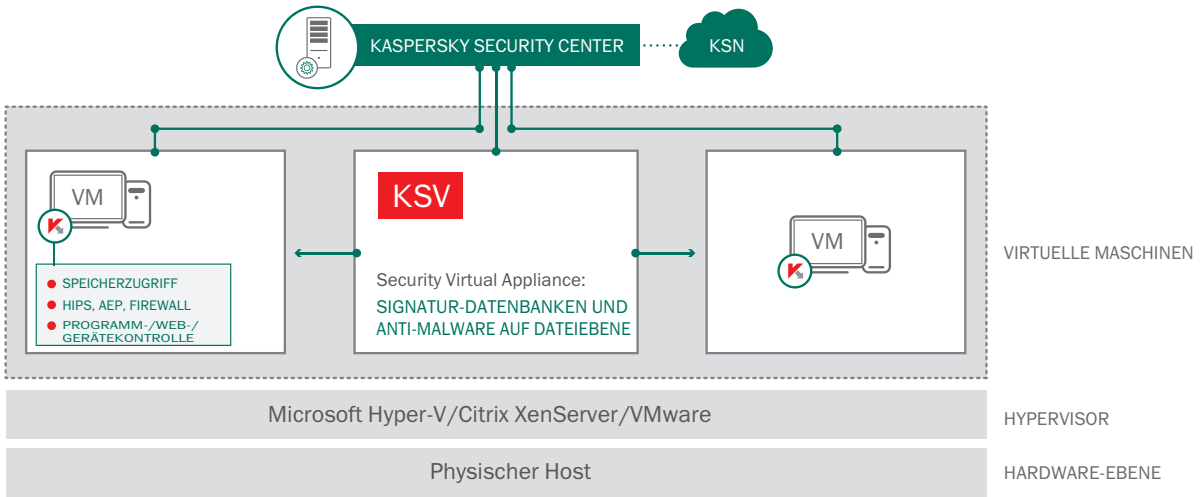
Um diese Einschränkungen zu überwinden, wurde der Ansatz gewählt, der zu schützenden VM neben der SVA ein kleines ressourcenschonendes Programm hinzuzufügen. Dieses Programm wird als „Light Agent“ bezeichnet. Dank zentraler Datei-Scan-Engine und Datenbanken weist dieses Programm eine sehr viel geringere Belastung des VM-Speichers auf als eine vollständige Agent-Lösung. Gleichzeitig ermöglicht es nicht nur den Zugriff auf das Dateisystem der virtuellen Maschine, sondern auch auf ihren Speicher und ihre internen Prozesse. Dies schafft die Grundlage für den Einsatz weiterer fortschrittlicher Sicherheitstechniken.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Kaspersky Security for Virtualization | Light Agent wurde für die drei bekanntesten Virtualisierungsplattformen entwickelt: VMware, Citrix und Microsoft Hyper-V. Der Anti-Malware-Scanner und die Signaturdatenbanken befinden sich auf einer dedizierten SVA, während die agentenlose Technologie dafür sorgt, dass Ressourcen für das Deployment zusätzlicher VMs freigesetzt und somit Konsolidierungsraten optimiert werden. Durch das Hinzufügen eines Light Agent, der auf dem jeweiligen Gastbetriebssystem läuft, wird es möglich, die fortschrittlichsten Technologien, die für physische Maschinen verfügbar sind, über **Kaspersky Endpoint Security for Business** zu nutzen. Endpoint-Kontrollen und HIPS (Host-Based Intrusion Prevention System), eine proprietäre Firewall sowie System Management-Tools können problemlos bereitgestellt werden. Es entsteht ein leistungsstarker mehrschichtiger Sicherheitsbereich, der auch komplexen Malware-Angriffen und Zero-Day-Bedrohungen gewachsen ist.

Die **Light Agent**-Lösung bietet zwar ein höheres Schutzniveau, ist aber sicherlich auch etwas „schwergewichtiger“ als ihre **agentenlose** Entsprechung. Sie erfordert daher auch ein etwas höheres Maß an Aufmerksamkeit beim Deployment neuer VMs.

Im Folgenden betrachten wir die Funktionalität beider Lösungen, Agentless und Light Agent, und die Bedrohungen, die sie abwehren sollen. Dieser Überblick hilft bei der Entscheidung, welche der beiden Lösungen für welche Gegebenheiten die geeignete ist.



BEDROHUNGEN UND FUNKTIONEN

Virtuelle Maschinen sind genauso gefährdet wie ihre physischen Pendants – vielleicht sogar noch mehr: In diesen blitzschnellen virtualisierten Netzwerken kann die Ausbreitung von Infektionen verheerende Folgen haben. Daher ist es wichtig, etwaige Sicherheitslücken in Ihrer virtualisierten Infrastruktur zu kennen und geeignete Maßnahmen gegen mögliche Bedrohungen zu ergreifen. Im Folgenden untersuchen wir potenzielle Bedrohungen für virtualisierte Systeme und die Technologien zu deren Bekämpfung.

AUSFÜHRBARE MALWARE-DATEIEN

Ob es sich um einen infizierten E-Mail-Anhang, infizierte Unterhaltungsmedien oder eine temporäre ausführbare Malware-Datei handelt – der Malware-Schutz ist unumgänglich, um diese grundlegenden Bedrohungen abzuwehren. Die Engine zur Malware-Bekämpfung ist das Herzstück der beiden **Agentless**- und **Light Agent**-Konfigurationen von **Kaspersky Security for Virtualization**, auch wenn sie mit jeweils unterschiedlichen Mitteln die Dateisysteme der geschützten VMs beeinflusst.

Eine andere Möglichkeit, Ihre virtualisierten Ressourcen vor Malware zu schützen, bietet die Programmkontrolle mit dynamischen Whitelists. Wenn nur legitime und sichere Software ausgeführt werden darf, wird Malware gestoppt, bevor sie Schaden anrichten kann. Mit Kaspersky Security for Virtualization | Light Agent kann die Programmkontrolle auf VMs aktiviert werden. Das über vShield ausgeführte Security for Virtualization | Agentless bietet keine Unterstützung für Endpoint-Kontrollen.

KÖRPERLOSE MALWARE

Eine raffinierte Form der Malware agiert sozusagen „körperlos“ – das heißt, im Dateisystem ist kein Hinweis darauf zu finden. Ausgelöst durch eine vorher gestartete EXE-Datei oder via Exploit eingebracht ist diese Malware mit traditionellem Malware-Schutz nicht zu entdecken. Hier sind erweiterte Gegenmaßnahmen erforderlich, die Prozesse im Speicher überwachen und Programme sofort blockieren können, die verdächtige oder definitiv gefährliche Aktivitäten ausführen. **Kaspersky Security for Virtualization | Light Agent** ist mit einer Reihe von Technologien ausgerüstet, die das Eindringen in den Speicher der VM verhindern. Diese beinhalten:

- Aktivitätsmonitor, der das Programmverhalten überwacht und Systemereignisse anzeigt. Unterstützt wird dieser von
- Verhaltensmuster-Signaturen, die Malware-Aktivitäten anhand von Verhaltensmuster-Merkmalen erkennen.
- Steuerung von Programmberechtigungen, die Programme daran hindert, unzulässige Änderungen (z. B. Prozessinjektionen) vorzunehmen.

Diese Werkzeuge ermöglichen der Host-basierten Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) das Verfolgen und Stoppen bösartiger Prozesse im VM-Speicher.

Kaspersky Security for Virtualization | Agentless kann hingegen aufgrund der API-Einschränkungen von vShield nur Änderungen auf Dateisystemebene verfolgen.

EXPLOITS

Die Ausnutzung von Schwachstellen, die in Systemkomponenten und häufig genutzten Programmen zu finden sind, ist weiterhin einer der effektivsten Angriffsmechanismen. Es ist zwar möglich, diesen Einbrüchen mithilfe der oben genannten Technologien entgegenzuwirken, das betroffene Programm kann jedoch auf hoher Berechtigungsebene arbeiten, sodass die Kontrolle über seine Aktivitäten begrenzt ist.

Die effektivste Methode zum Schutz vor solchen Bedrohungen ist es, Exploits grundsätzlich an der Ausnutzung von Schwachstellen zu hindern. Dies wird erreicht, indem die für Exploits charakteristischen Aktionen bei ihrer Ausführung vom automatischen Exploit-Schutz von Kaspersky Lab (AEP) erkannt werden. Die Wirksamkeit dieser Technologie wurde durch eine Reihe unabhängiger Tests bestätigt, die vom MRG Effitas-Institut durchgeführt wurden. Die Tests ergaben, dass die AEP-Technologie von Kaspersky Lab selbst bei Deaktivierung aller anderen Schutzkomponenten zu 100 % wirksam gegen Angriffe ist, bei denen Exploits eingesetzt werden. Sogar unbekannte Zero-Day-Exploits werden mithilfe dieser Technologie blockiert.

Kaspersky Security for Virtualization | Light Agent ist mit dieser erweiterten Funktion ausgestattet, was ihren Einsatz insbesondere in virtualisierten Desktop-Infrastrukturen (VDI) nützlich macht, die physische Desktops ersetzen sollen – und ein verhältnismäßig höheres Risiko an Drive-by-Infektionen beinhalten.

Kaspersky Security for Virtualization | Agentless setzt hier auf die vShield-Funktionalität, die jedoch keine mit Kaspersky AEP vergleichbaren Funktionen bietet.

ROOTKITS

Ausgeklügelte Malware ist häufig in der Lage, sich zu verbergen, und mithilfe sogenannter „Bootkits“ und „Rootkits“ die Erkennung durch traditionelle Anti-Malware zu verhindern. Das Heimtückische an diesen Tools ist, dass sie Malware so früh wie möglich laden und diese mit hohen Systemberechtigungen ausstatten, die eine Erkennung verhindern. Die Anti-Rootkit-Technologie von Kaspersky Lab kann selbst eine derart gut versteckte Malware finden und löschen. Sie arbeitet auf Speicher- und Dateisystemebene und benötigt zum Ausführen Zugriff auf RAM und Prozesse des Gastcomputers.

Kaspersky Security for Virtualization | Light Agent kann diese Technologie anbieten, da sie vollständigen Zugriff auf die Ressourcen des Gastcomputers hat.

Kaspersky Security for Virtualization | Agentless kann nur auf das Dateisystem zugreifen, sodass eine vollständige Anti-Rootkit-Funktion hier nicht realisiert wird.

NETZWERKANGRIFFE

Es gibt Bedrohungen, die Funktionen des Netzwerksystems nutzen und Angreifern wichtige Informationen über das angegriffene Netzwerk liefern, Zugang zu den Ressourcen des anvisierten Systems ermöglichen oder den reibungslosen Betrieb des Netzwerks stören. Hierzu gehören Port-Scanner, Denial-of-Service-Angriffe, Buffer-Underrun-Angriffe und weitere schädliche Aktionen. Angriffe dieser Art erfordern spezielle Gegenmaßnahmen, wie sie Network Attack Blocker von Kaspersky Lab bietet. Diese Technologie stoppt eingehende Netzwerkangriffe mithilfe von IDS (Intrusion Detection System) durch den Einsatz heuristischer Algorithmen, welche selbst die komplexesten Angriffsmuster erkennen können.

Sowohl **Kaspersky Security for Virtualization | Agentless** als auch **Kaspersky Security for Virtualization | Light Agent** weisen diese Netzwerktechnologien als Teil ihres Instrumentariums auf.

SCHÄDLICHE WEBSEITEN

Eine der häufigsten Infektionsquellen sind schädliche oder infizierte Webseiten. Virtualisierte Server sind hiervon zwar relativ selten betroffen, sie können jedoch zu einer ernsthaften Bedrohung für den VDI-Desktopersatz werden, wenn Benutzer vollen Internetzugriff erhalten. An dieser Stelle kommen die Web-Technologien von Kaspersky Lab ins Spiel. Der Phishing-Schutz verhindert, dass Benutzer auf Webseiten zugreifen, die als gefährlich gemeldet wurden. Hierfür werden Informationen aus dem **Kaspersky Security Network** bereitgestellt, 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 einen schädlichen Code erkennt. Die **Web-Kontrolle** hat zudem den Vorteil eines beschränkten Zugriffs auf nicht für die Arbeit erforderliche Webseiten (etwa Spiele oder Soziale Netzwerke).

Kaspersky Security for Virtualization | Agentless verfügt nicht über diese Host-basierten Merkmale, **Kaspersky Security for Virtualization | Light Agent** jedoch schon, sodass letztere Lösung für VDIs mit Zugriff auf das Internet besser geeignet ist.

ANGRIFFE ÜBER PERIPHERIEGERÄTE

Eine der traditionell wirksamsten Methoden der Infizierung eines IT-Netzwerks ist die Verwendung von externen Speichergeräten. Während über das Netzwerk eingeschleppte Infektionen derzeit rein zahlenmäßig die größte Bedrohung auszumachen scheinen, geht von externen Speichergeräten auch weiterhin Gefahr aus – insbesondere, wenn sie als Teil eines sorgfältig geplanten Angriffs eingesetzt werden. Erwähnenswert ist auch, dass auch andere Peripheriegeräte eine Gefahr darstellen können; ein bekanntes Beispiel hierfür ist infizierte Drucker-Firmware. Externe Speicherlaufwerke sind zudem beliebte Medien, wenn vertrauliche Daten das Firmengebäude verlassen.

Auch wenn es in der Regel für nicht autorisierte Personen nicht einfach ist, Zugriff auf die physischen Geräte zu erhalten, die als Host der virtualisierten Infrastruktur dienen, ist es dennoch möglich, und es gibt sicherlich Geschäftsszenarien, in denen allein die Möglichkeit ein zu großes Risiko darstellt. Und was den Desktop-Ersatz durch VDI betrifft, weisen selbst die einfachsten Thin Clients USB-Ports auf.

Daher ist die Kontrolle von Peripheriegeräten eine vernünftige Vorsichtsmaßnahme – die mit der **Technologie zur Gerätekontrolle von Kaspersky Lab** problemlos umgesetzt werden kann. Sie ermöglicht, dass die Nutzung bestimmter Geräte- oder Bustypen unterbunden oder beschränkt wird. Natürlich besteht auch die Möglichkeit, Ausnahmen zu konfigurieren, sodass die für berufliche Aufgaben erforderlichen Peripheriegeräte weiterhin verwendet werden können.

Die Gerätekontrolle wird wie andere Kontrolltechnologien in **Kaspersky Security for Virtualization | Light Agent** angeboten, ist in **Kaspersky Security for Virtualization | Agentless** jedoch nicht vorhanden.

DATENLECKS

Firmeninterna, die durch ein Leck im IT-Netzwerk nach außen dringen, können Unternehmen großen Schaden zufügen. Insbesondere die damit einhergehende Rufschädigung kann lange und unangenehme Konsequenzen haben. Daher ist es erforderlich, die Wege für die gemeinsame Nutzung von Informationen zu beschränken. Sowohl die **Programmkontrolle** als auch die **Gerätekontrolle** von Kaspersky Lab sind in diesem Fall nützlich. Mit der Programmkontrolle kann die Ausführung potentiell gefährlicher Programme wie Instant Messaging oder Anwendungen für Datei-Hosting und P2P-Clients verhindert werden. Die Gerätekontrolle beschränkt die Verwendung externen Speichers, der zur Ausfuhr vertraulicher Daten missbraucht werden kann.

Auch hier gilt, dass diese beiden Technologien in **Kaspersky Security for Virtualization | Light Agent** verfügbar sind, in **Kaspersky Security for Virtualization | Agentless** jedoch nicht angeboten werden.

AGENTLESS IM VERGLEICH ZU LIGHT AGENT: WAS IST BESSER?

Für einige Leser ist die Antwort wahrscheinlich völlig klar: **Kaspersky Security for Virtualization | Light Agent** ist randvoll mit hochmodernen Funktionen, die **Kaspersky Security for Virtualization | Agentless** nicht bietet – daher ist die Light Agent-Lösung vermeintlich besser. Aber in der Praxis ist die Entscheidung gar nicht so eindeutig.

Zum einen bietet **Kaspersky Security for Virtualization | Agentless** sofortigen Schutz. Virtuelle Maschinen werden also direkt von Beginn an geschützt, was von Vorteil sein kann, wenn eine Infektion bereits in Ihrem virtualisierten Netzwerk wütet (und die VM nicht über ein Image, das die **Light Agent**-Anwendung enthält, wiederhergestellt werden kann).

Andererseits geben Sie **Kaspersky Security for Virtualization | Light Agent** möglicherweise den Vorzug vor **Kaspersky Security for Virtualization | Agentless**, wenn es um Leistungsfähigkeit geht. Zur Auswahl des für Ihre virtualisierte Umgebung am besten geeigneten Schutzes ist es unumgänglich, die potentiellen Bedrohungen, den Wert der zu schützenden Daten und die erforderlichen Schutzebenen zu berücksichtigen.*

Bitte beachten Sie, dass für alle Kombinationen aus Agentless-Schutz für VMware und Light Agent-Sicherheit für jede einzelne oder alle drei Plattformen (VMware, Citrix, Microsoft Hyper-V) nur eine einzelne Lizenz für **Kaspersky Security for Virtualization** erforderlich ist. Ob VMware, Citrix oder Microsoft: Kontrolle und Schutz erfolgen komfortabel über die gemeinsame Verwaltungskonsole: das **Kaspersky Security Center**.

* Lesen Sie das Whitepaper „Kaspersky Security for Virtualization“, um mehr Einzelheiten zur Auswahl der besten Kombination aus Lösungen von Kaspersky Lab für die Sicherung Ihrer virtualisierten Infrastruktur zu erhalten.

KASPERSKY lab