KASPERSKY SECURITY FOR VIRTUALIZATION

Zuverlässiger, flexibler und effizienter Schutz für virtualisierte Server- und Desktop-Umgebungen

Datenlecks mit Beteiligung von virtualisierten Umgebungen waren durchschnittlich doppelt so kostspielig als jene ohne. Es ist also kein Wunder, dass Unternehmen sich heutzutage ernsthaft Sorgen über die Sicherheit ihrer virtualisierten Systeme machen. Eine effektive Sicherheitslösung für die wachsende virtuelle Desktop-Infrastruktur (VDI) und virtualisierte Serverumgebung zu finden und gleichzeitig die Vorteile der Virtualisierung zu bewahren, ist nicht so einfach.

Virtualisierte und physische Endpoints sind denselben Sicherheitsrisiken ausgesetzt – Cyberkriminalität macht keine Unterschiede –, weswegen Sie sich Kompromisse bei der Sicherheit nicht leisten können. Das gilt natürlich auch für die Performance. Genau hier kommt Kaspersky Security for Virtualization und seine einzigartige Architektur zum Tragen.

Kaspersky Security for Virtualization bietet einen außergewöhnlichen, mehrschichtigen und fein abgestuften Schutz für VDIs und virtuelle Serverumgebungen. Der von uns hierfür verwendete Ansatz ist einzigartig, da er die Leistungsfähigkeit Ihrer virtualisierten Infrastruktur nicht beeinträchtigt.

Wichtigste Vorteile

ERSTKLASSIGER SCHUTZ

- **Hochwertiger, mehrstufiger Schutz für alle Ihre virtuellen Maschinen (VMs) vor bekannten, unbekannten und hochentwickelten Bedrohungen.**
- Die Integration in das Cloud-basierte Kaspersky Security Network (KSN) schützt VDI und Server proaktiv vor allen aufkommenden Malware-Bedrohungen weltweit.
- Programmkontrolle (mit Integration dynamischer Whitelists) sowie Web- und Gerätekontrolle ermöglichen dem Administrator die Durchsetzung von VDI-Sicherheitsrichtlinien für Gruppen oder einzelne Maschinen, um die Sicherheit und Produktivität der Benutzer zu gewährleisten.
- Eine leistungsstarke Kombination aus Network Attack Blocker, Firewall, Host-basiertem System zur Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) und Anti-Phishing-Technologien schützt Ihre VMs vor Netzwerkangriffen.

MEHR LEISTUNG

- **Das innovative, patentierte[1] Design gewährleistet die Schonung der Systemressourcen und optimiert Konsolidierungsraten für maximale Virtualisierungsdichte.**
- Die Shared-Cache-Technologie verhindert den doppelten Scanaufwand. Dies ist insbesondere für virtuelle Desktops wichtig, auf denen eine Vielzahl von Dateien repliziert werden muss.
- AV-Update- und Scan-Storms sowie Zeitfenster für Angriffe oder „Instant-on"-Lücken werden vermieden.

vmware PARTNER TECHNOLOGY ALLIANCE | vmware READY NETWORKING AND SECURITY | CITRIX READY | VBLOCK READY

[1] US-Patent Nr. 9088618

HÖHERE EFFIZIENZ

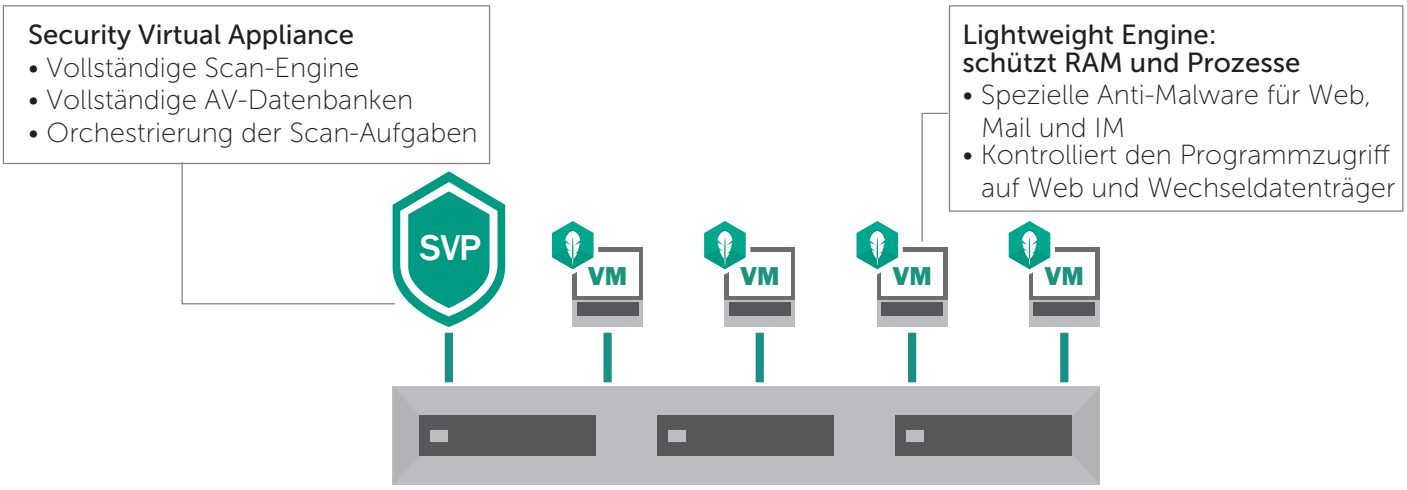
- **Für den Schutz Ihrer VMs benötigen Sie eigentlich nur eine einzige Security Virtual Appliance. Die Bereitstellung eines Light Agent auf jeder VM für umfassenderen Schutz ist so unkompliziert, dass noch nicht einmal ein Neustart erforderlich ist.**
- Eine einzige Konsole bedeutet, dass sich physische und virtuelle Maschinen sowie Mobilgeräte zusammen verwalten lassen.
- Da Bereitstellung und Verwaltung auf der vertrauten Logik für die Sicherheit physischer Maschinen beruht und die Abläufe sich somit natürlich und instinktiv anfühlen, steht einer effizienten Bedienung ohne Konfigurationsfehler eigentlich nichts mehr im Weg.

ÜBERLEGENE FLEXIBILITÄT

- **Kaspersky Security for Virtualization unterstützt die führenden Anbieter von Virtualisierungstechnologien – VMware, Citrix und Microsoft.**
- Flexible Lizenzierung – wählen Sie zwischen Lizenzierung auf Grundlage von VM-Anzahl (Desktops oder Server) oder Hardware-Ressourcen (Anzahl der Kerne).

Einzigartige Light-Agent-Technologie von Kaspersky Lab

FUNKTIONSPRINZIP UND VORTEILE



Die einzigartige Architektur von Kaspersky Security for Virtualization sorgt für einen effektiven, ressourcenschonenden Schutz von VMs ohne Verzicht auf Endpoint-Ressourcen. Deshalb können erheblich höhere Konsolidierungsraten als mit herkömmlichen Anti-Malware-Lösungen erzielt werden. Darüber hinaus können Update- und Scan-Storms sowie Zeitfenster für Angriffe oder „Instant-on"-Lücken vermieden werden.

Die Security Virtual Appliance (SVA) von Kaspersky Lab scannt alle VMs in der Host-Umgebung zentral. Die Lösung umfasst einen leistungsstarken Light Agent, der auf jeder virtuellen Maschine[2] bereitgestellt wird. Mit Bereitstellung des Lite Agent stehen dann auf jeder der VMs erweiterte Sicherheitsfunktionen zur Verfügung, darunter die Programm- Geräte- und Web-Kontrolle, Malware-Schutz für Instant Messaging, E-Mail und Web sowie hochentwickelte heuristische Verfahren.

Dadurch bietet Kaspersky Security for Virtualization eine einzigartige Kombination aus leistungsstarker, mehrstufiger Sicherheit und effizienter Performance.

Weitere Informationen zu Kaspersky Security for Virtualization erhalten Sie von Ihrem lokalen Kaspersky-Vertriebspartner oder unter www.kaspersky.de/business-security.

[2] Bei nicht-persistenten VMs steht der sofortige Schutz nach einer einmaligen Bereitstellung in der Security Virtual Appliance zur Verfügung. Bei persistenten VMs muss der Administrator den Light Agent bei der Installation manuell bereitstellen.

Kaspersky_Security_for_Virtualisation_Datasheet_August 2015-GL