Bitdefender®

Virtuelle Infrastrukturen ohne Leistungseinbußen absichern

Inhalt

Einführung

Trotz aller Vorteile, die die Virtualisierung mit sich bringt, entstehen auch neue Probleme, wenn Sicherheitslösungen die Leistungsfähigkeit von Systemen beeinträchtigen. Damit stellt sich die Frage, ob Virtualisierungssicherheit nicht in Wirklichkeit kontraproduktiv ist. Und mehr noch: Machen die aktuell erhältlichen Sicherheitslösungen nicht im Vergleich zu physischen Server-Umgebungen viele Virtualisierungsvorteile wieder zunichte, indem Sie Performance-Engpässe und eine Reihe zusätzlicher Probleme in virtualisierten Umgebungen hervorrufen?

In diesem Dokument werden einige Herausforderungen besprochen, die mit Virtualisierung einhergehen. Ferner werden die Erbnisse diverser von Bitdefender durchgeführten Leistungstests präseniert. Und schließlich wird die Hypervisor-unabhängige Lösung Security for Virtualized Environments (SVE) vorgestellt.

Tücken der Virtualisierungssicherheit

Agentenbasierte Malware-Schutz-Lösungen, die auf virtuellen Maschinen installiert sind, werden früher oder später veraltet sein, da virtuelle Maschinen oft länger ausgeschaltet sind. Soviel ist bekannt. Wenn eine virtuelle Maschine neu gestartet wird, muss die Sicherheitslösung zunächst die neuesten Viren- und Engine-Signaturen und Software-Updates herunterladen. Dieser Update-Prozess allein kann schon 5 bis 12 Sekunden in Anspruch nehmen und öffnet damit Angriffen Tür und Tor.

Eine Alternative zu herkömlichen Malware-Schutz-Lösungen sind Sicherheitslösungen, die über eine Integration mit VMware Endpoint Security verfügen und so agentenlose Sicherheit bieten. Durch den agentenlosen Ansatz werden definitiv Sicherheitsprobleme durch Startverzögerung und veralteten Virenschutz vermieden. Dieser Ansatz hat jedoch auch seine Tücken:

VMware ist derzeit der einzige Anbieter agentenloser Sicherheit über die Integration mit vShield Endpoint. Für Unternehmen, die Hypervisoren von Xen oder Hyper-V einsetzen, gibt es einfach keine agentenlose Sicherheitslösung. Zusätzlich ist die agentenlose Lösung auf Windows-Umgebungen beschränkt. Linux-basierte Umgebungen und solche ohne VMware sind weiterhin auf herkömmliche agentenbasierte Lösungen angewiesen.

Auch wenn man die Lösungen agentenlos nennt, so stimmt das doch nicht gänzlich. Auf jeder virtuellen Maschine, die geschützt werden soll, muss weiterhin der Treiber für vShield Endpoint installiert werden.

Die agentenlose Lösung hat auch ihre Einschränkungen. So können nur Dateien gescannt werden. Für Speicher- und Registry-Scans, Verhaltensüberwachung sowie Anwendungs- und Gerätesteuerung müssen weiterhin herkömmliche agentenbasierte Lösungen eingesetzt werden.

Die unten stehende Abbildung veranschaulicht Bitdefenders agentenlose Sicherheit über die Integration mit VMware vShield Endpoint. Aber auch für Unternehmen, die Virtualisierungs-Software anderer Hersteller einsetzen, hat Bitdefender eine Lösung.

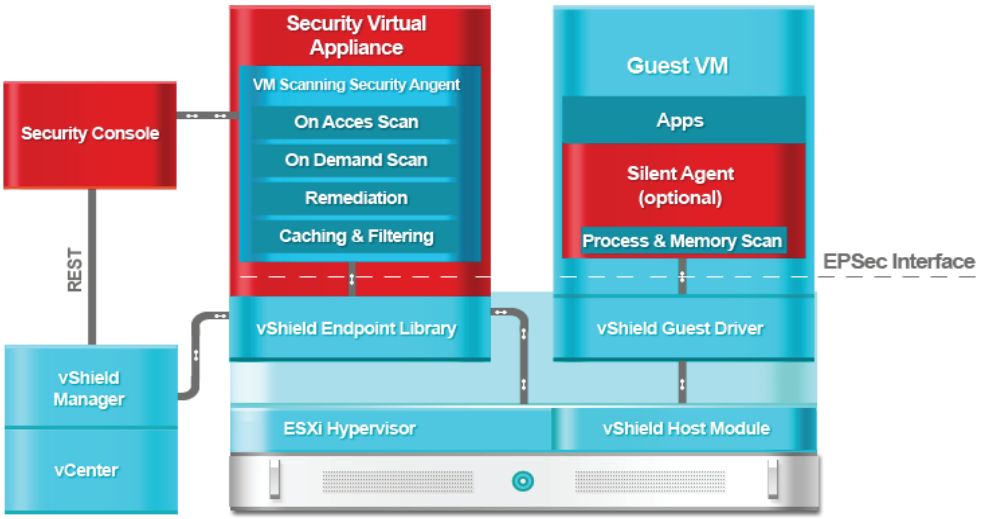


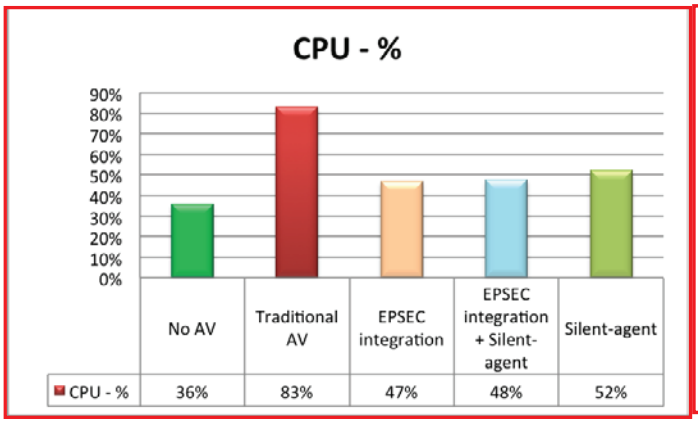
Abbildung 1: Security for Virtualized Environments – Integration mit VMware EPSEC

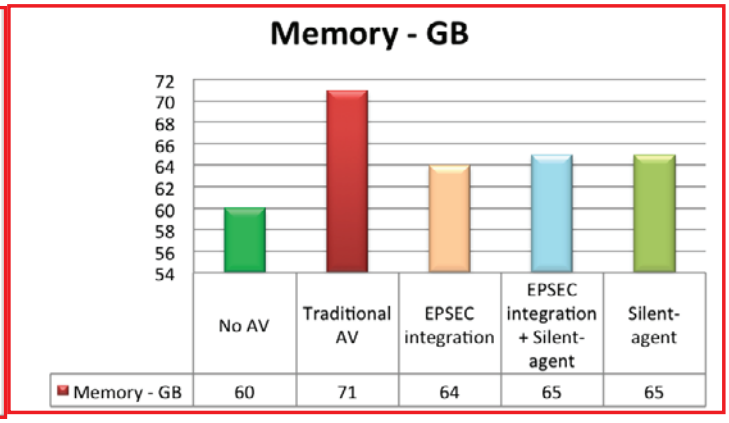
Szenario der Konsolidierungsraten

Eins der Hauptargumente für Virtualisierung ist das Sparpotenzial durch erhöhten Konsolidierungsraten bei virtuellen Maschinen - so viele virtuelle Maschinen auf demselben Host wie möglich. Sicherheitslösugen sollten speziell auf virtuelle Umgebungen ausgelegt sein und eine möglichst geringe Auswirkung auf die Leistung haben, um maximale Konsolidierungsraten zu ermöglichen.

Die Hardware-Anforderungen für virtuelle Umgebungen können sehr unterschiedlich sein; sie hängen stark von den Anwendungen ab, die in der Umgebung laufen sollen. Die Leistung der Prozessoren, des Arbeitsspeichers, des Netzwerks und des Speicherplatzes hängen von der Art der virtuellen Maschinen ab, die in der Umgebung laufen sollen. So können z. B. mit virtuellen Maschinen, auf denen Web-Anwendungen laufen, höhere Konsolidierungsraten erzielt werden, als mit solchen, auf denen Datenbankanwendungen laufen. Je nach Anwendung empfiehlt es sich in jedem Fall, mindestens 20 % der Systemressourcen für Leistungsspitzen zu reservieren.

Die Auswirkung der Sicherheit auf die Leistung der Umgebung sollte auch beachtet werden. Die folgenden Leistungstestergebnisse veranschaulichen dies. Nähere Informationen zu den Testumgebungen finden Sie im Anhang.





Mit traditionellem Malware-Schutz wurden im Test Konsolidierungsraten von 45 virtuellen Maschinen pro Host-Server erreicht. Laut dem VMware-Rechner für Kosten pro Anwendung1 würden die durchschnittlichen Kosten pro virtueller Maschine in der Beispielkonfiguration $1358.19 betragen. Für die folgenden Konfigurationen werden CPU- und RAM-Auslastung angezeigt:

- SVE in einer agentenlosen Konfiguration und Integration mit VMware vShield Endpoint Security (EPSEC)
- SVE in einer agentenlosen Konfiguration und Integration mit VMware vShield Endpoint Security (EPSEC) + SVE Silent Agent
- Nur SVE Silent Agent

Die Testergebnisse sprechen für sich: herkömmlicher agentenbasierter Malware-Schutz verbraucht ca. 36 Prozentpunkte mehr CPU-Ressourcen (83 % statt 47 %) und 7 Prozentpunkte mehr Arbeitsspeicher (71 % statt 64 %) als die mit vShield integrierte SVE-Lösung. Die Leistungseinbußen durch traditionellen Malware-Schutz würden die Anschaffung zusätzlicher Hardware erforderlich machen, was höhere Kosten pro VM bedeuten würde, noch bevor die Lizenzgebühren für die Malware-Schutz-Lösung überhaupt eingerechnet wurden.

Auf der Grundlage der Testergebnisse lässt sich schätzen, dass Kunden mit SVE mindestens 20 % mehr virtuelle Maschinen auf jedem Host laufen lassen können als mit herkömmlichem Malware-Schutz, und das in jeder beliebigen virtuellen Umgebung.

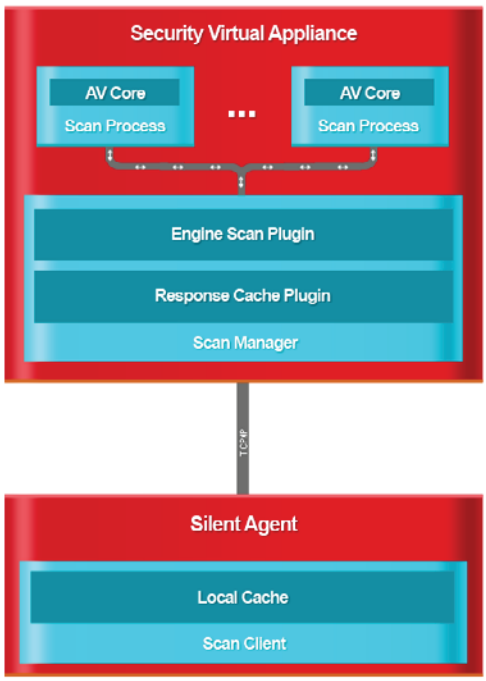


Abbildung 2: Überblick über die Scan-Architektur

[1] VMware-Rechner für Kosten pro Anwendung

Optimale Sicherheit für virtuelle Umgebungen

Security for Virtualized Environments (SVE) von Bitdefender sichert jede beliebige virtuelle Umgebung und verschafft Kunden höhere Konsolidierungsraten auf jedem Host-Server als herkömmliche Sicherheitslösungen. Das spart Kosten bei der Hardware, Lagerung und Kühlung, was die Investition in Virtualisierung noch rentabler macht. Bitdefender erreicht diese Kostenvorteile durch zum Patent angemeldete Technolgoien und Optimierungsmechanismen, von denen einige im Folgenden näher beschrieben werden.

Zentrale Scans für jede beliebige virtuelle Umgebung

SVE ist eine Hybrid-Sicherheitslösung, die speziell auf die heterogenen und dynamischen Rechenzentren unserer Zeit ausgelegt ist. Anders als herkömmliche Sicherheitslösungen zentralisiert Bitdefender Scan-Funktionen, indem ein Großteil der Malware-Schutz-Funktionen auf eine dedizierte virtuelle Hochsicherheits-Appliance ausgelagert wird: die Security Virtual Appliance (SVA). Durch diesen Ansatz werden sowohl Scans bei Zugriff als auch bei Bedarf effektiver. Außerdem werden kritische Systemressourcen auf den Host-Servern dedupliziert. Prozess- und Speicher-Scans werden durch den Silent Agent zur Verfügung gestellt, einem kleinen Programm, das auf den Gastmaschinen installiert wird.

Der Silent Agent ist mit dem Windows-Security-Center integriert und informiert den Benutzer über den Sicherheitsstatus und die aufgetretenen Ereignisse auf der VM. In VMware-Umgebungen wird der Silent Agent nur für Speicher-Scans eingesetzt, da Bedarf- und Zugriffs-Scans über den vShield-Endpoint-Treiber laufen. Bei anderen Plattformen und Betriebssystemen sorgt der Silent Agent für die Durchsetzung von Sicherheitsrichtlinien und lagert Malware-Schutz-Funktionen über das TCP/IP-Protokoll auf die SVA aus.

Bedarf-Scans in der Umgebung werden sequenziell ausgeführt (eine VM nach der anderen). Mit nur einem Treiber und Dienst, der auf jeder virtuellen Maschine installiert werden muss, ist die Ressourcennutzung äußerst gering und die Auswirkungen auf den Host-Server minimal. Im Durchschnitt werden in mit vShield integrierten Umgebungen 15 MB Festplattenspeicher und 20 MB Arbeitsspeicher benötigt.

Höhere Leistung durch Caching-Mechanismen

Bitdefenders Security for Virtualized Environments setzt einen zum Patent angemeldeten Caching-Mechanismus ein, bei dem bekannte Systemdateien und Anwendungen auf eine Whitelist gesetzt werden. Dadurch wird die Scan-Leistung von virtuellen Maschinen deutlich gesteigert und die Sicherheit immer auf dem neuesten Stand gehalten. Dabei setzt die Lösung einen Cache auf zwei Ebenen ein, wovon einer ein selbstlernender Cache ist und in die SVA integriert ist. Der Silent Agent verwendet einen lokalen Cache, der abhängig von den Variablen seiner Umgebung vorgefüllt ist. So kann er die Scans auslagern, die nötig sind, und Objekte ausschließen, die als sicher bekannt sind.

Fazit

Virtualisierungssicherheit darf die Leistungsfähigkeit von virtuellen Rechenzentren nicht einschränken und so die eigentlichen Vorteile von Virtualisierung zunichtemachen. Security for Virtualized Environments (SVE) von Bitdefender löst dieses Problem durch seinen einzigartigen Ansatz an den Schutz virtueller Maschinen in jeder beliebigen virtuellen Umgebung. Durch die Architektur von Bitdefenders Security for Virtualized Environments werden Scan-Funktionen von den geschützten Systemen isoliert, womit viele der oben erwähnten Sicherheitsprobleme in virtuellen Umgebungen umgangen werden. Zusätzlich steigert die Bitdefender-Lösung die Sicherheit durch den Einsatz zum Patent angemeldeter Caching-Mechanismen. Das Ergebnis sind höhere Konsolidierungsraten in virtuellen Rechenzentren, wodurch schließlich Kosten gesenkt werden können, ohne an der Sicherheit sparen zu müssen.

Anhang

Die Leistungstest wurden auf den folgenden Hardware-Konfigurationen und Virtualisierungsplattformen durchgeführt:

Hardware-Spezifikationen	1x HP ProLiant BL460c G7
	2 * Xeon 6 CORE + HT @ 2.53 GHZ (Intel Xeon E5649)
	144 GB RAM
	1.2 TB PCI-E SSD iSCSI Speicherplatz(10 GBit)
VDI-Infrastruktur	20x Windows XP SP3 (32-Bit), 1xCPU, 1 GB RAM
	20x Windows 7 (64-Bit), 1xCPU, 2 GB RAM
	5x Windows 2k8 R2, 1xCPU, 6 GB RAM
Virtualisierungsplattformen	Citrix XenServer 6.0 + XenCenter 6.0
	Citrix XenDesktop 5.5
	VMware ESXi 5.0 + vSphere 5.0

Bitdefender ist ein Anbieter von Sicherheitstechnologien, dessen Lösungen über ein innovatives Netzwerk aus Value-Added-Kooperationen, Vertriebspartnern und Wiederverkäufern in über 100 Ländern verfügbar sind. Seit 2001 hat Bitdefender immer wieder mit preisgekrönter Sicherheitstechnologie für Unternehmen und Privatanwender überzeugen können und ist einer der führenden Anbieter von Sicherheitslösungen für Virtualisierungs- und Cloud-Technologien. Bitdefender hat seine preisgekrönten Technologien mit den passenden Vertriebskooperationen und Partnerschaften kombiniert und seine globale Marktposition durch die strategische Zusammenarbeit mit den weltweit führenden Virtualisierungs- und Cloud-Technologieanbietern gestärkt.

BD-Business-May.20.2015-TI#: 70593