Unternehmensinformation

Server-Sicherheit von McAfee

Sichere Server-Workloads mit geringen Leistungseinbußen und integrierter effizienter Verwaltung

TM

Wie würden Sie sich entscheiden, wenn Sie zwischen der Absicherung aller Server – physisch oder virtuell – in Ihrem Rechenzentrum oder der Optimierung ihrer Leistung wählen müssten? Würden Sie auf die Sicherheit und damit auf Hochverfügbarkeit für Ihre IT-Dienste, die Absicherung Ihrer Daten und eine Auszeichnung bei Ihrer nächsten Compliance-Prüfung setzen? Oder würden Sie sich für Leistung entscheiden und eine bessere Rendite für Ihre Hard- und Software-Investitionen erzielen, ganz zu schweigen vom begeisterten Finanzvorstand? Sicherheit oder Leistung – was ist wichtiger? Und was wäre, wenn Sie jetzt beides haben könnten?

Entscheidung zwischen Sicherheit und Leistung

Tatsächlich zwang die rasant zunehmende Virtualisierung der Rechenzentrumsumgebungen viele CIOs zu genau dieser Entscheidung. Konventionelle Sicherheitskontrollen für physische Server verursachen auf virtualisierten Systemen hohen Rechenaufwand, während eigenständige Lösungen ohne zentrale Verwaltungsoberfläche hohen Verwaltungsaufwand nach sich ziehen. Deshalb deaktivieren zahlreiche IT-Verantwortliche einfach sämtliche Endgeräte-Sicherheits-Tools und verlassen sich ausschließlich auf Peripherieschutzmaßnahmen.

Komplexe Anforderungen an moderne Server-Sicherheit

Geschäftskritische Server ohne integrierte Sicherheit bitten förmlich um eine Katastrophe, aber der Grund dafür ist schlicht, dass die meisten verfügbaren Sicherheitstechnologien für den Schutz dedizierter physischer Systeme entwickelt wurden. Sie können nicht an Virtualisierung angepasst werden und erfüllen nicht die Anforderungen an moderne gemischte Rechenzentrumsumgebungen. Aus diesem Grund sind dringend Server-Sicherheitslösungen notwendig, die folgende Anforderungen erfüllen:

- Unterstützung für die individuellen und unterschiedlichen Sicherheitsanforderungen aller Kernaufgaben des Rechenzentrums, einschließlich Datenbank, Web, Anwendungen, E-Mails, Zusammenarbeit und Speicher-Server. In einem aktuellen Artikel des SANS Institute[1] wird darauf hingewiesen, dass umfassender Server-Schutz die Bereitstellung „verschiedener Technologien erfordert, um Server sicher bereitzustellen, Schwachstellen langfristig zu verwalten, den Zugriff auf Informationen zu kontrollieren, Bedrohungen gleich nach ihrem Auftreten zu erkennen und die Netzwerksicherheitsabläufe zu verbessern."

Hauptvorteile

Optimierung der Sicherheitsmaßnahmen. Minimierung von Leistungseinbußen. McAfee Server Security Suite Essentials und McAfee Server Security Suite Advanced machen Schluss mit den Kompromissen zwischen Server-Sicherheit und Leistung in modernen virtualisierten Rechenzentren.

Jede Suite kombiniert Blacklists mit der Unterstützung von Virtualisierungstechnologien, um umfassenden Schutz für wichtige Aufgaben auf physischen und virtuellen Servern bei einer CPU-Gesamtlast von höchstens 5 % zu bieten. McAfee Server Security Suite Advanced bietet mit Whitelists sowie Änderungskontrollen zusätzlichen Schutz.

Alle Suites können über die Software McAfee ePO zentral verwaltet werden.

Zu den verfügbaren Suites gehören:

- McAfee Server Security Suite Essentials
- McAfee Server Security Suite Advanced
- McAfee Security Suite for VDI
- McAfee Data Center Security Suite for Databases

intel Security

- Kein Ringen mit geschäftlichen Diensten um CPU-Ressourcen. Herkömmliche Sicherheitslösungen sind übermäßig abhängig von signaturbasierten Blacklist-Technologien, die das gesamte Systemabbild permanent scannen müssen, um Bedrohungen zu erkennen. Dadurch benötigen sie meist einen erheblichen Teil der Rechenleistung.
- Gewährleistung eines optimierten Supports für alle wichtigen Virtualisierungsumgebungen.
- Steuerung sämtlicher Sicherheitskontrollen in der gesamten Server-Umgebung – physisch sowie virtuell – über eine zentrale Konsole.

McAfee-Suites für Server-Sicherheit

Zur Erfüllung der oben genannten Kriterien und Gewährleistung der Sicherheit in modernen hoch virtualisierten Rechenzentren bietet McAfee eine Reihe von Server-Sicherheits-Suites an, die auf die speziellen Anforderungen von Microsoft Windows- und Linux-Servern zugeschnitten sind.

McAfee Server Security Suite Advanced garantiert dank Whitelist-Technologien (wie Anwendungskontrolle) und signaturbasierten Blacklist-Technologien (wie Virenschutz sowie hostbasiertem Eindringungsschutz) bestmögliche Server-Sicherheit. Diese integrierte Steuerungs-Suite schützt unmittelbar zuvor gescannte Systeme vor Malware-Infektionen, indem ausschließlich zugelassene Anwendungen ausgeführt werden dürfen. Dadurch werden die Scan-Häufigkeit erheblich verringert und die Rechenlast auf ein Minimum verringert, was für Unternehmen eine erhebliche Verbesserung bedeutet. Diese einmalige Kombination aus White- und Blacklists sowie Unterstützung für virtualisierte Umgebungen ermöglicht die bislang unerreichte Optimierung der Vorgänge im Rechenzentrum. Dadurch wird die maximale Sicherheit physischer und virtueller Server bei minimaler Beeinträchtigung der Server-Leistung gewährleistet. Sämtliche Komponenten aller Suites sind eng in die Verwaltungsplattform McAfee® ePolicy Orchestrator® (McAfee ePO™) integriert und ermöglichen dadurch effiziente zentrale Risikoanalyse, Sicherheitsverwaltung sowie Behebung von Zwischenfällen.

McAfee Data Center Security Suite for Databases verbindet globale Datenbankerkennung sowie Schwachstellenbewertung mit unterbrechungsfreier Echtzeit-Aktivitätsüberwachung auf allen Bedrohungsvektoren. Folgende Kontrollkomponenten werden eingesetzt:

- McAfee Database Activity Monitoring
- McAfee Vulnerability Manager for Databases

McAfee Server Security Suite Essentials bietet umfassende Blacklist-Funktionen sowie optimierte Virtualisierungsunterstützung für Server aller Typen. McAfee Server Security Suite Advanced bietet zusätzlich noch Whitelists sowie Schutz durch Änderungskontrollen.

McAfee Security Suite for VDI bietet umfassenden Schutz für virtuelle Desktops, ohne dass dabei die Leistung oder Benutzerfreundlichkeit beeinträchtigt werden. Folgende Kontrollkomponenten werden eingesetzt:

- McAfee Application Control for Desktops
- McAfee VirusScan® Enterprise
- McAfee VirusScan Enterprise for Linux
- McAfee MOVE AntiVirus for Virtual Desktops (VDI)
- McAfee ePO

Folgende weitere Sicherheitslösungen stehen zur Verfügung:

- McAfee Security for Microsoft SharePoint
- McAfee Security for Email Servers
- McAfee VirusScan Enterprise for Storage

McAfee-Lösungen zum Schutz von Rechenzentren

	McAfee Server Security Suite Essentials	McAfee Server Security Suite Advanced	McAfee Security Suite for VDI	McAfee Data Center Security Suite for Databases
McAfee VirusScan Enterprise	■	■	■	
McAfee VirusScan Enterprise for Linux (Desktop)			■	
McAfee VirusScan Enterprise for Linux (Server)	■	■		
McAfee VirusScan Command Line	■	■		
McAfee Application Control for Servers		■		
McAfee Application Control for Desktops			■	
McAfee MOVE AntiVirus for Virtual Desktops (VDI)			■	
McAfee MOVE AntiVirus for Virtual Servers	■	■		
McAfee MOVE Scheduler	■	■		
McAfee Data Center Connector for VMware vSphere	■	■		
McAfee Data Center Connector for Amazon AWS	■	■		
McAfee Data Center Connector for OpenStack	■	■		
McAfee Data Center Connector for Microsoft Azure	■	■		
McAfee Host Intrusion Prevention	■	■		
McAfee Deep Defender for Servers	■	■		
McAfee Change Control		■		
McAfee Agentless Firewall		■		
McAfee ePO (Software)	■	■	■	
McAfee File and Removable Media Protection			■	
McAfee Database Activity Monitoring				■
McAfee Vulnerability Manager for Databases				■
Lizenzformat	Pro Betriebs-systeminstanz (d. h. pro virtueller Maschine)	Pro Betriebs-systeminstanz (d. h. pro virtueller Maschine)	Pro virtueller Maschine	Datenbank-instanz

Branchenweit umfassendste Paket an Server-Sicherheitstechnologien

Nur McAfee bietet ein so umfassendes Paket an Sicherheitslösungen an, da ausschließlich McAfee über eine umfassende Palette von Technologien zur Absicherung physischer und virtueller Server sowie zur zentralen Verwaltung komplexer Sicherheitslösungen in gemischten Umgebungen verfügt. Diese Suites nutzen den vollen Umfang der McAfee-Palette an Sicherheitstechnologien:

- **McAfee VirusScan Enterprise** kombiniert Viren- und Spyware-Schutz sowie Firewall- und Eindringungsschutztechnologien, um böswillige Software zu stoppen und zu entfernen. Darüber hinaus werden mit dieser Lösung neue Sicherheitsrisiken abgedeckt und die Kosten für die Reaktion auf Sicherheitsverletzungen reduziert, wobei die Auswirkungen auf die Systemleistung geringer sind als bei jeder anderen Lösung der Branche.
- **McAfee VirusScan Enterprise for Linux** bietet überlegenen, dauerhaften Schutz vor der wachsenden Anzahl an Viren, Würmern sowie böswilligem Code, die auf Linux-Systeme abzielen. McAfee VirusScan Enterprise for Linux ist für moderne, äußerst flexible Unternehmen ausgelegt. Die Lösung lässt sich leicht skalieren, aktualisiert sich automatisch und kann zentral von einer einzigen Konsole, der Plattform McAfee ePO, verwaltet werden.
- **McAfee Application Control** blockiert effektiv nicht autorisierte Anwendungen sowie Code auf Servern, Desktop-Rechnern von Unternehmen und Geräten mit festen Funktionen. Die zentral verwaltete Whitelist-Lösung nutzt dazu ein dynamisches Vertrauensmodell sowie innovative Sicherheitsfunktionen, die hochentwickelte, hartnäckige Bedrohungen vereiteln, ohne Signaturaktualisierungen oder zeitintensive Listenverwaltung zu erfordern.
- **McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus** optimiert den McAfee-Virenschutz für virtuelle Desktops und Server ohne Beeinträchtigung der Leistung oder Sicherheit, damit Sie operative Erträge erzielen und die Sicherheits-maßnahmen effektiver verwalten können. McAfee MOVE AntiVirus schützt Ihre virtuelle Umgebung einschließlich der virtuellen Maschinen in der Cloud.
- **Die McAfee Data Center Connector-Module** ermöglichen einen vollständigen Überblick über Ihre virtuellen Maschinen. Sie erkennen nicht nur physische Server, sondern auch Hypervisoren und virtuelle Maschinen in den Umgebungen von VMware vSphere, Amazon Web Services, OpenStack und Microsoft Azure. Wenn Sie feststellen, dass virtuelle Maschinen in Ihrer öffentlichen Cloud bereitgestellt werden, können Sie festlegen, welche von ihnen mithilfe entsprechender Sicherheitsrichtlinien geschützt werden sollen.
- **McAfee Host Intrusion Prevention for Server** schützt präventiv vor bekannten und neuen Zero-Day-Angriffen. Es stärkt die Sicherheit und ermöglicht durch die Reduzierung der Häufigkeit und Dringlichkeit von Patch-Installationen zudem Kostensenkungen. McAfee Host Intrusion Prevention integriert sich in die Plattform McAfee ePO für zentrale Berichterstellung und Verwaltung, die präzise, skalierbar sowie benutzerfreundlich ist und sich mit anderen Produkten von McAfee sowie Drittanbietern kombinieren lässt.
- **McAfee Deep Defender for Servers** bietet Hardware-unterstützten Endgeräteschutz der nächsten Generation auf Basis der McAfee DeepSAFE™-Technologie, der über das Betriebssystem hinaus geht und hochentwickelte sowie verborgene Angriffe erkennt, blockiert und abwehrt. McAfee Deep Defender, das erste Produkt auf Basis der in Zusammenarbeit mit Intel entwickelten McAfee DeepSAFE-Technologie, revolutioniert den Schutzansatz der Sicherheitsbranche.
- **McAfee Change Control** verhindert Änderungen in Server-Umgebungen, die zu Sicherheitsverletzungen, Datenkompromittierungen und Systemausfällen führen können. McAfee Change Control erleichtert erheblich die Einhaltung von Compliance-Anforderungen.

- **McAfee Agentless Firewall** stellt eine Übersicht aller isolierten virtuellen Netzwerke bereit. Die Lösung ermöglicht die Kontrolle und Isolierung virtueller Maschinen und Daten durch Integration in die VMware vCNS App-Firewall.
- **McAfee File and Removable Media Protection** bietet Sicherheit durch Verschlüsselung ruhender Daten auf internen und Wechselmedien, damit Benutzer USB-Medien verschlüsseln und Informationen sicher übertragen können.
- **McAfee Database Activity Monitoring** findet automatisch Datenbanken in Ihrem Netzwerk. Die Lösung schützt sie mit vorkonfigurierten Schutzmaßnahmen und unterstützt Sie bei der Entwicklung individueller Sicherheitsrichtlinien für Ihre Umgebung. Ihre Daten werden effektiv vor allen Bedrohungen geschützt, indem die Aktivitäten lokal auf jedem Datenbank-Server überwacht werden und böswilliges Verhalten selbst bei virtuellen Umgebungen oder Cloud Computing in Echtzeit angezeigt oder beendet wird.
- **McAfee Vulnerability Manager for Databases** liefert schnelle, genaue und vollständige Einblicke in die Schwachstellen aller Ressourcen in Ihrem Netzwerk. Dadurch bleiben Sie auch den neuesten Bedrohungen einen Schritt voraus und können Ihre Problembehebungsmaßnahmen über eine zentrale und korrelierte Übersicht Ihrer Schwachstellen priorisieren.
- **Die Software McAfee ePO** bietet eine zentrale Verwaltungsoberfläche für physische und virtuelle Server, einschließlich der Server in der privaten und öffentlichen Cloud. Die Verwaltung Ihrer gesamten Endgeräte-Infrastruktur über eine zentrale Konsole hat den Vorteil niedrigerer Gesamtbetriebskosten. Sämtliche Komponenten der Suite sind eng in die Verwaltungsplattform McAfee ePO integriert und ermöglichen dadurch effiziente zentrale Risikoanalyse, Sicherheitsverwaltung sowie Behebung von Zwischenfällen.

Erfolgreiche Server-Sicherheitslösungen

Die McAfee-Suites für Server-Sicherheit sind die branchenweit umfassendsten Lösungen zur Absicherung geschäftskritischer Dienste in modernen gemischten physischen und virtuellen Umgebungen. Sie kombinieren Server-Sicherheitstechnologien zur Entlastung der CPU, bieten umfassende Sicherheitskontroll-Sets für alle wesentlichen Aufgaben, unterstützen alle größeren virtualisierten Umgebungen und zentralisieren die Sicherheitsverwaltung durch eine einzelne Verwaltungskonsole. Weitere Informationen erhalten Sie unter **www.mcafee.com/de/products/data-center-security/index.aspx**.

1. **www.sans.org/reading_room/analysts_program**

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com