



Protect what you value.

McAfee VirusScan Enterprise for Offline Virtual Images

Purpose-built Security for Virtual Environments

Virtualization, the latest revolution in computing, is changing the face of enterprise IT in nearly every sector worldwide. Today, it is estimated that one in every eight servers shipped is virtualized¹, and it's safe to say that there will be continued rapid growth in this direction. While the ease of deployment, operational efficiencies, and cost savings are highly desirable, virtual machines have introduced new security challenges that need to be addressed in the context of an organization's approach to security risk management (SRM).

KEY ADVANTAGES

Update security on offline virtual machines without bringing them online

- Facilitate real-time disaster recovery by ensuring offline virtual machines are secure
- Decrease risks when noncompliant, dormant virtual machines rejoin the corporate network

Lighten the load on your IT staff

- Save the time and trouble of periodically bringing offline virtual images back online for IT maintenance
- Reduce IT migration issues with a single security solution for all major virtualization environments: VMware and Microsoft
- Mitigate IT overhead with a single security solution for both production (disaster recovery) and pre-production (testing and development) virtual environments

Achieve operational efficiencies with Enterprise-class security management

- Reduce IT effort and operating costs with common security management for both physical and virtual environments

One of the key advantages of virtual machines (VM) is that enterprise applications are easier to provision and deploy compared to physical servers. In some instances, it can take as little as 15 minutes to bring up an application on a VM. But the consequence of easy deployment is VM proliferation. More and more VMs are constantly being created throughout the IT environment—even for small workloads. This proliferation of VMs has resulted in the need to periodically bring the operational VMs offline for patching, configuration, testing, and backup. Some archived VMs, in fact, may stay offline for long periods of time to meet compliance and regulatory requirements; for example, some industries are required by law to save financial applications and transactions for up to seven years.

Generally, VMs that are dormant for an extended period of time are not updated with the latest patches from Microsoft or other vendors because the task is very cumbersome, especially given the proliferation of VMs. When these archived VMs are activated again, their anti-malware security profiles are precariously out of date, and they are riddled with unpatched vulnerabilities that can potentially put an organization's entire virtual infrastructure at risk.

McAfee VirusScan Enterprise for Offline Virtual Images

McAfee® VirusScan® Enterprise (VSE) for Offline Virtual Images is the industry's first security solution that is purpose-built for offline virtual environments. It scans, cleans and updates the anti-malware security profile of dormant VMs—without having to bring them online. When offline virtual machines are finally brought back online, they are already scanned, cleaned and fully secure with updated signatures, so they no longer pose a threat to the IT environment. Because the process is automated, the IT burden of bringing VMs back online from time to time for security patches, updates, and maintenance is greatly reduced. Support for major virtualization vendors, including VMware and Microsoft is combined in a single solution, alleviating future IT migration issues. And, IT overhead is minimized because VSE for Offline Virtual Images handles both production (disaster recovery) and pre-production (testing and development) virtual environments. VSE for Offline Virtual Images can be deployed as a standalone server or as a virtual machine.

Typical Applications

When it comes to securing offline virtual machines, VSE for Offline Virtual Images covers the two key scenarios that are of greatest concern to corporate IT departments: disaster recovery and the test and development environment.

¹ IDC, 2008

SYSTEM REQUIREMENTS

Supported Operating Systems

- Microsoft Windows XP SP1 and above
 - No support for XP 64-bit
- Microsoft Windows Vista base and above
 - Includes 64-bit
- Microsoft Windows Server 2003 SP1 and above
 - Standard, Enterprise, and Datacenter editions
 - No support for Server 2003 64-bit
- Microsoft Windows Server 2008
 - Standard, Enterprise, and Datacenter Editions
 - No support for Server Cores
 - Includes 64-bit

Supported VMware Images

- Supports images using the Virtual Machine Disk Format (VMDK) and Open Virtualization Format (OVF) specification
- Microsoft Windows 2000 SP4
- Microsoft Windows XP SP1 and above
 - Includes 64-bit
- Microsoft Windows Vista base and above
 - Includes 64-bit
- Microsoft Windows 2003 SP1 and above
 - Standard, Enterprise, and Datacenter editions
 - Includes 64-bit
- Microsoft Windows Server 2008
 - Standard, Enterprise, and Datacenter editions
 - Includes 64-bit

In a typical disaster recovery, or production scenario, business applications running in virtual environments can get disrupted by hacking attempts, system failures, malicious employee intent, data corruption, or application malfunction. In the event of a disruption, backup (or archived) virtual machines at secondary sites are activated to restore the production environment. Because production applications (which can include database software, human resources applications, ecommerce, or online banking, to name a few) are vital for maintaining business continuity, it's essential that the backup VM images are updated and free of malware. VSE for Offline Virtual Images scans, cleans and updates signatures for the backup (or archived) virtual images on a periodic basis, ensuring a smooth and worry-free transition to the restored production environment. As a result, backup VMs remain secure from sophisticated malware sitting on the sidelines waiting to attack new virtual machines as soon as they are brought online.

In a test and development, or pre-production scenario, applications running on virtual machines undergo numerous revisions and many rounds of quality assurance, resulting in hundreds of VMs being created and archived on an ongoing basis. When it comes time to revert back to a working version of the workload scenario, it's critical that the virtual image is secure from the latest malware. Again, the ability of VSE for Offline Virtual Images to scan, clean and automatically update the offline VMs on demand is crucial for overburdened IT departments to administer the pre-production virtual environment.

Enterprise-class Manageability

VSE for Offline Virtual Images is administered by McAfee ePolicy Orchestrator® (ePO™), the award-winning security management console that delivers a coordinated, proactive defense against malicious threats and attacks for the enterprise. With ePO as the hub of McAfee security risk management (SRM) solutions, administrators can mitigate the risk of rogue, noncompliant systems; keep protection up to date; configure and enforce protection policies; and monitor security status 24/7 from one centralized, web-based console. Deploy ePO, and manage all of your new security solutions or extend your investment in enterprise security management by adding VSE for Offline Virtual Images to your existing ePO infrastructure. With ePO, VSE for Offline Virtual Images is easy to deploy, easy to configure, and easy to manage. As a result, ePO can be used to manage both physical and virtual security.

Features and Benefits

First purpose-built security solution of its kind for offline virtual machines

- Enterprise IT environments are rapidly adopting virtualization: as many as one out of every four workloads today is on a VM². A cost-effective, efficient security solution for VMs is a critical and often overlooked aspect to an organization's overall security posture. VSE for Offline Virtual Images is the only security solution of its kind purpose-built for offline VMs.
- McAfee, the security vendor of choice for enterprises all over the world, extends its trusted expertise in the physical environment to the virtualized environment

Reduce IT overhead to administer virtual environments

- Anti-malware security profiles of offline virtual machines are updated automatically without bringing VMs online, reducing the risk of infecting the rest of virtual environment
- When offline virtual machines are brought back online, signature files are up-to-date, so virtual machines no longer pose a risk to the virtual environment
- In testing and development environments, where there is often a proliferation of virtual machines, VSE for Virtual Offline Images keeps anti-malware protection up to date
- In disaster recovery scenarios, VSE for Virtual Offline ensures that backup virtual images are up-to-date with respect to malware signatures before they go into production
- On demand security for an unlimited number of VMs provides maximum scalability and flexibility

² The Gartner Group, June, 2008

SYSTEM REQUIREMENTS (Continued)

Supported Microsoft Virtual PC Images

- Supports images using the Microsoft Virtual Hard Disk Image Format specification
- Microsoft Windows 2000 SP4
- Microsoft Windows XP SP1 and above
 - Includes 64-bit
- Microsoft Windows 2003 SP1 and above
 - Standard, Enterprise, and DataCenter editions
 - Includes 64-bit
- Microsoft Windows Vista base and above
 - Includes 64-bit
- Microsoft Windows Server 2008
 - Standard, Enterprise, and DataCenter editions
 - Includes 64-bit

Supported ISOs

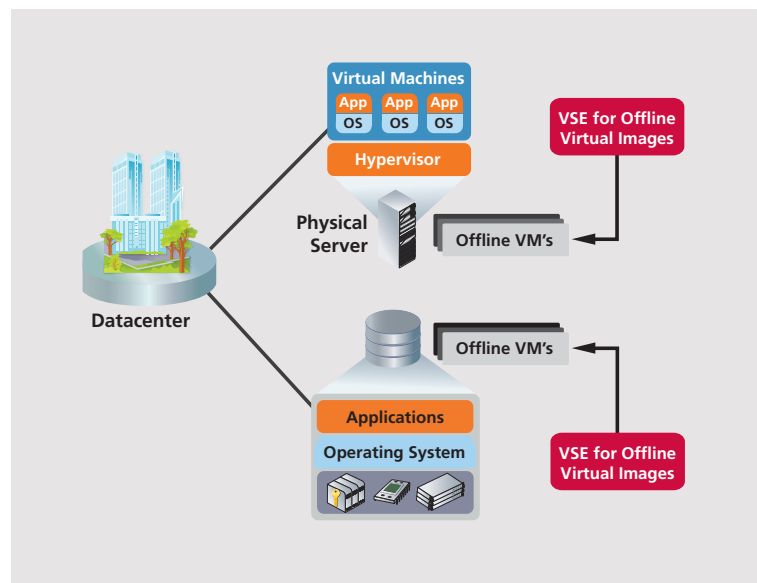
- If the OS supporting the VSE scanner recognizes the file system format of the .iso image, then it will scan it

A single solution that provides support for top virtualization vendors saves time and money and minimizes administration headaches

- There's no need to purchase multiple, difficult-to-manage point products for each type of virtual environment
- Supported vendors include:
 - VMware
 - Microsoft
- Scans ISO images

ePO simplifies, consolidates, and centralizes management for your offline virtual environments and all your McAfee products.

- Access centralized event monitoring, reports, dashboard, and workflow through a single web-based, management console
- Deploy, manage, and update agents and policies from one management platform



VirusScan Enterprise for Offline Virtual Images Deployment