360 Virtualization Security Management System

New Security Threats Faced by Virtualization

While offering significant increase in the efficiency and effectiveness for complex computing scenarios, virtualization does not only inherit almost all of the risks faced by traditional physical servers, but also faces new security challenges, including special risks posed by dynamic virtual machines, and the impact of security software, such as virus scanners, on single physical host resources in multiple virtual machines.

Virtualized Network Fueling Rapid Spread of Malware

In virtualized data centers, virtualized 2-layer network structures are created among virtual machines. Such east-west traffic is a complete blind spot for traditional solutions such as firewalls, IPS or antivirus gateways, so a grey zone of security management is formed among virtual machines. Even if one or a few virtual machines are controlled by an attacker, the malware can spread wildly throughout the whole data center.

Attack Window Period

Extensive adoption of virtualization technology empowers enterprise IT services with higher flexible and better load balance. Nevertheless, the dynamic adjustment of resources by turning on or off virtual machines creates gaps for threat protection. When one of the inactive virtual machines, without in-time update of malware signature database or OS and application patches for some time, is automatically started by business needs to join the server group, a window period is potentially provided for attacks.

Computing Resource Utilization

If traditional security methods--installing anti-virus software on each virtual machine and scanning for malware--are used, the effectiveness might be close to that of physical server protection, but the resource consumption is problematic. The consumption by anti-malware agents for a physical server hosting tens of virtual machines is considerable, especially when all agents are scanning or updating in the same period, the stress on computing resources and back-end storing IOPS will rise sharply, which might, for severer cases, cause one or more physical hosts to crash.

Management Complexity

In a virtualized environment, it is easy to create, modify, copy and migrate virtual machines. The automatic settings, reconfiguration, migration among different hosts, and even the flexible migration of virtual servers make it extremely difficult for administrators to track, maintain and enforce consistent security policies. Therefore, corresponding measures are necessary to protect such dynamic data centers.

360 Virtualization Security Features

VMware provides the Guest Introspection (formerly EPSEC) API library to build dedicated *Service Virtual Machines (SVMs)* that provide VMware NSX customers with end point protection solutions. VMware NSX is the network virtualization platform for the Software-Defined Data Center (SDDC). NSX embeds networking and security functionality that is typically handled in software on the hypervisor instead of requiring specialized hardware.

360 Virtualization Security Management System is one of the NSX Partner programs for end point protection. Thanks to the API library by VMware, our solution enables hypervisor introspection by offloading from each virtual machine the virus scanning and other endpoint security activities onto a Service VM with our patented security engine. The Service VM runs scanning upon policies enforced by the 360 Management Controller, gets notified of potential security violations and acts to remediate the affected files. Further details are shown as below:

Virtual Pool Management

- vCenter creation to the Management Controller
- vCenter deletion from the Management Controller
- Automatic service insertion
- Manual deployment/deletion of SVMs in NSX
- Manual service deletion in NSX

VM Management

- Automatic synchronization of VM data from vCenter
- VM security status display and monitoring

Anti-Malware

- Real-time scan
- Full scan
- Quick scan
- On-Demand scan
- Scheduled scan

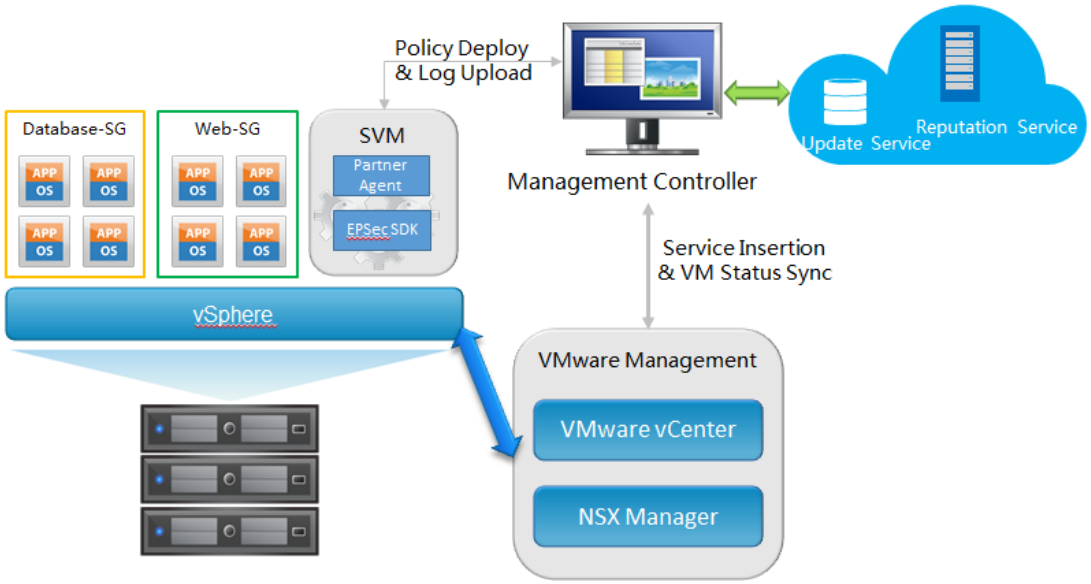
Policy Configuration

- Enabling/Disabling real-time scan
- Scheduled scan configuration
- File scan white list
- Scan-only configuration

Log & Report

- Anti-malware events display on Dashboard
- Log analysis for anti-malware events
- Report for anti-malware events

System Architecture



Management Controller

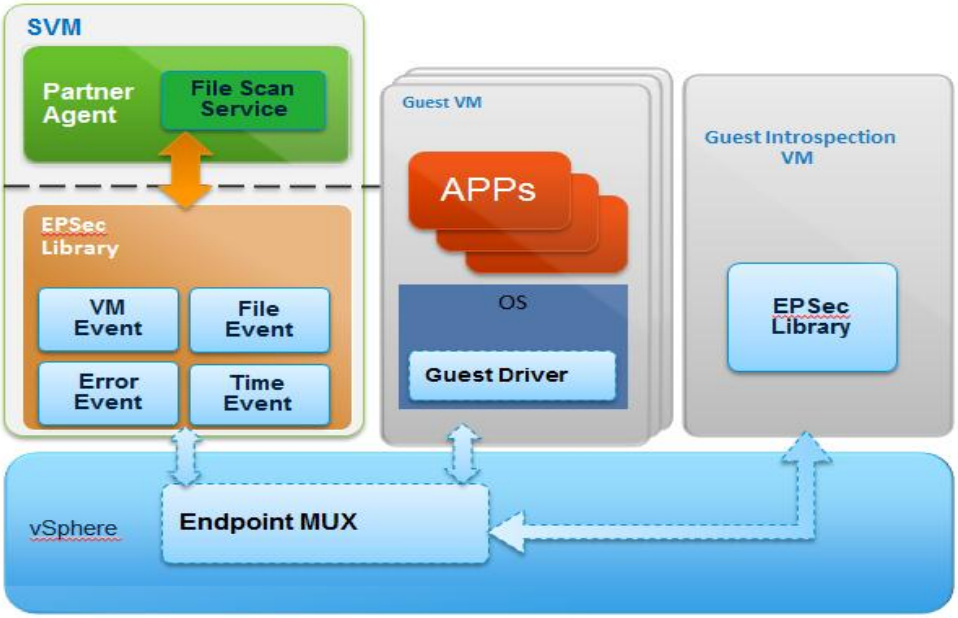
- Communicate with the NSX Manager and vCenter from the management plane
- Sync VMs' status from vCenter
- Manage and monitor SVMs centrally
- Configure and deploy security policies to SVMs
- Receive security event logs from the SVMs
- Receive security pattern updates from the Update Service
- Query proxy for File Reputation Service

SVM

- Deployed as service VM on each host
- Receive security policies from the Management Controller
- Real-time monitoring and anti-malware against virtual machines' file systems on same host with the NSX Guest Introspection SDK
- Upload security event logs to the Management Controller

Partner Agent

- Running as a service in SVMs
- Integrate with EPSec SDK for On-Access Scan(OAS)& On-Demand Scan(ODS)
- Get policies from the Management Controller for scan configuration and actions
- Quarantine infected files in SVMs and recover from SVMs
- Send scan status and security event logs to the Management Controller



Compatibility List

Virtualization Platform	Version
VMware	vSphere ESXi 5.5
	vSphere ESXi 6.0
	vSphere ESXi 6.5
	NSX 6.2.4
	NSX 6.3.0
	VC 6.0
	VC 6.5

Operation System List

- Windows XP、Vista 7、8、8.1、10（32 /64 bits）
- Windows Server 2003（32 /64 bits）
- Windows Server 2008（32 /64 bits）、2008 R2、2012、2012 R2、2012 Server Core （64 bits）、2016（64 bits） 2016 Server Core（64 bits）
- Red Hat® Enterprise 5、6、7（32 /64 bits）
- SUSE® Enterprise 10、11、12（32 /64 bits）
- CentOS 5、6、7（32 /64 bits）
- Ubuntu 12、14、16（64 bits）
- Oracle Linux 5、6、7（32 /64 bits）
- CloudLinux 5、6、7（32 /64 bits）
- Amazon Linux（32 /64 bits）
- Debian 6、7（64 bits）
- Red Flag Linux
- NeoKylin Linux
- Kylin Linux
- Deepin Linux