Symantec™ Endpoint Protection for VDI

Agentless anti-malware plus complete threat protection for your VDI environment

Data Sheet: Security Management

Solution Overview

VDI Basics

VDI is a form of server-based computing that utilizes server-grade hypervisor to host multiple unique and isolated client operating systems aboard a single server or group of servers in a datacenter environment. With VDI, customer admins can create a common image, store the image in one or more servers in data center, and deploy it to virtual machines on the server hypervisor (host). Virtual desktops are delivered to end user devices via the network using representative vendors and products such as Citrix (XenDesktop), Microsoft (VDI Suite), Dell (vWorkspace), and VMware (Horizon View). Users connecting to a virtual desktop can access all of the features of that specific VM without impacting other virtual desktops within the host or the host server.

VDI offers customers the following benefits:

- Rapid deployment of a common, supported desktop environment across the network delivers operational and cost savings.
- Ability to deploy different desktop images to a specific group of users based on their location or job function.
- Centrally deploy updates and changes across all virtual desktops. The next time users log-on, they will have the updated image with all of their settings maintained.
- Enhanced defense against catastrophic failure.
- Faster update speeds, and
- Ability to customize desktops for specific users or groups of user thus enhancing workplace flexibility and increasing business agility to support strategic initiatives.
- Enhance security and compliance by centralizing data and applications in the datacenter, by increasing the IT administrators' control over desktop applications and operating systems, and by enabling faster deployment of upgrades and patches. With VDI, customers can address potential data loss associated with mobile endpoints by storing data on centralized servers rather than on the device itself.

Security Considerations for Virtual Desktop Infrastructure

To deliver VDI security, three main things need to be protected—the VDI servers, the virtual desktop images, and the user profile folders. Customers looking to implement security for their VDI environments have to consider the following requirements and potential risks:

- Assess the impact of anti-malware scanning on VDI and network performance.
- Control the applications that users can download and install into their virtual desktops.
- Isolate infected or hacked "virtual machines" and protect the rest of the VDI environment.
- Address loss of visibility into every asset due to faster deployment times.
- Assess the impact of VDI into the customer's existing security and compliance protocols.
- Mitigate risks from having the host as the central point of failure.
- Segregate critical virtual desktops from the regular pool to prevent unauthorized access and exposure to malicious software.

Introducing Symantec Endpoint Protection for Virtual Desktop Infrastructure (SEP for VDI)

Symantec Endpoint Protection for Virtual Desktop Infrastructure (VDI)

Symantec Endpoint Protection for Virtual Desktop Infrastructure (SEP for VDI) enables organizations to enable operationally efficient and comprehensive solution for protecting virtual endpoints, specifically VMware Horizon View and Citrix Xen Desktop on VMware.

Standard Features:

- Agentless antimalware protection with full protection set for VMware Horizon and Citrix ZenDesktops on VMware.
- Agent-based anti-malware protection for physical endpoints and virtual desktops on HyperV and KVM.
- Full protection set includes:
  - Reputation analysis- unique Insight™ technology
  - Real-time file behavior monitoring- unique SONAR™ technology
  - Rules-based firewall and browser protection
  - Intrusion Prevention System (IPS)
  - Malware remediation tool- Power Eraser
  - Application control with system lockdown features such as whitelisting and blacklisting
  - External media control
  - Location awareness
  - Host integrity
- Designed to work with the VMware ESX platform and supports VMware vShield/vCNS and VMware NSX.

Customer Benefits

The VDI infrastructure is usually starved for resources because of the higher ratio of Guest VMs to ESX hosts. Security, therefore, needs to strike the right balance to ensure that it is able to mitigate application and network performance issues, optimize operational budgets, and meet their security and compliance standards. This optimization issue becomes more critical as the VDI environment scales out. SEP for VDI helps alleviate the tension across IT performance optimization, budget constraints, and security objectives by off-loading AV scanning to a virtual appliance and centralizing the updates of AV signatures at the hosts. SEP for VDI mitigates scan and live update storms. It also reduces the resources and performance tax associated with agent-based approaches, thus making the virtual desktops more efficient.

With this offering, customers benefit from the combination of best-of-breed, agent-based, multi-layered protection and hardening with agentless anti-malware/AV that is optimized for the VDI environment. Customers with multi-platform VDI environments are able to better optimize their VDI security operations by offering agent-based and agentless anti-malware in a single solution, combined with full protection and hardening. Customers can choose the anti-malware option that best fits their infrastructure, IT operations, and security objectives.

Customers with VMware-supported VDI environments will gain the following benefits:

- Enhance application and network performance by off-loading AV scans to a centralized process, instead of performing scans on every VM.
- Alleviate boot storms in virtual desktops.
- Mitigate scan storms during the AV scan process.
- Eliminate the need to duplicate signature content updates on every Virtual Machine and realize network, storage, and compute efficiencies.
- Eliminate definition update storms.
- Customers running both VMware NSX & VMware vShield in their data centers can leverage this product to provide agentless anti-malware protection.
- Prevent employees from plugging unauthorized USB drives into the VDI environment.
- Supports Microsoft Windows 7/8
- Full virtual endpoint threat protection offered by Symantec Endpoint Protection (SEP)

System Requirements

Symantec Data Center Security: VDI supports the following platforms:

- VMware ESXi — 5.5 Update 2/ 6.0
- VMware vCenter— 5.1/ 5.5 Update 2/ 6.0
- VMware vShield/vCNS— 5.1.4/ 5.5.4
- VMware NSX— 6.1.2/ 6.1.3/ 6.1.4

The agentless antimalware capability offered by SEP for VDI supports all versions of Citrix XenApp/ Citrix XenDesktop (on VMware) and VMware Horizon View (on VMware).

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21360010 11/15