ESET® VIRTUALIZATION SECURITY

Safer computing with cloud-enabled anti-malware protection through the VMware NSX® environment

Performance, Security and the Need for Continuity

Companies that virtualize their systems seek a balance between performance and security and the need for continuity when managing their systems.

Because a virtualized environment is just as critical in a business network as any physical environment, virtual machines need the same level of antimalware protection. However, challenges include the following:

- Conventional antivirus has very high-resource consumption.
- On-demand scans and periodic updates on virtual machines often results in AV storms.
- Businesses are exposed to high risk of breach when security is sacrificed.
- Major issues with central management when running conventional antimalware on virtual machines.
- Visibility of virtual machine security status and security operations management creates unwanted overhead.

"Great protection, small system footprint and increased user productivity."

CHRIS DENT
SYSTEM ADMINISTRATOR
WASHAKIE RENEWABLE ENERGY
SOURCE: TECH VALIDATE. TVID: AEA-104-5D3

High-Performance Security that Won't Slow Down Your Virtual Machines

ESET Virtualization Security was developed to provide antimalware security for virtual machines and address the impact to virtualization ROI from AV storms. VM infrastructure is about optimizing resources and performance, and ESET's scanning engine exactly meets these requirements. It is well known for its low system demands and high speed, thus leaving more resources for other applications and processes.

ESET Virtualization Security was designed to balance performance and security.

- Superior performance – resulting from ESET's award-winning and lightweight scanning engine.
- Superior detection – resulting from our highly regarded heuristics technologies and ESET's Cloud Management Protection Systems (ESET LiveGrid® / ThreatSense Reputation Engines).

Easy Technology Adoption

While management of endpoint security in a virtual environment can be complicated, ESET Virtualization Security is convenient for businesses when integrated with NSX service.

- Ease of management – Managed by ESET Remote Administrator, which also comes as a virtual appliance. ESET Remote Administrator is a "single pane of glass" for managing all physical and virtual endpoints in the same consistent manner. A separate console is not needed to run and manage/oversee ESET in a VMware environment.
- Simplicity of licensing – ESET's Unilicense model allows businesses to easily migrate existing licenses or extend them to leverage "quantity resulting discounts." Businesses can easily transfer their existing licenses between physical and virtual endpoints.

VMWARE NSX

VMware NSX is the leading network virtualization platform that delivers the operational model of a virtual machine for the network.

ESET VIRTUALIZATION SECURITY

ESET Virtualization Security supports NSX platform. Automatic deployment of ESET Virtualization Security appliances to hosts newly connected to NSX Manager allows instant protection of newly added virtual hosts, and virtualized workloads. In addition, the solution natively supports VMware NSX automation, VMware vSphere® vMotion® and is compatible with ESET Remote Administrator 6, ESET's web-based console, allowing direct drill-down capability to virtual machines for rapid task execution and complete endpoint security management.

ABOUT ESET

ESET develops award-winning security software that now helps over 100 million users to Enjoy Safer Technology®. Its broad security product portfolio covers all popular platforms and provides businesses around the world with the perfect balance of performance and proactive protection.

USE CASES

Businesses building virtual infrastructure who care about security but want the lightest solution possible to optimize for virtualization can benefit from ESET Virtualization Security to protect their NSX endpoints on VMware vSphere 5.5+ and avoid AV storms. Contact ESET for a free trial of ESET Virtualization Security.

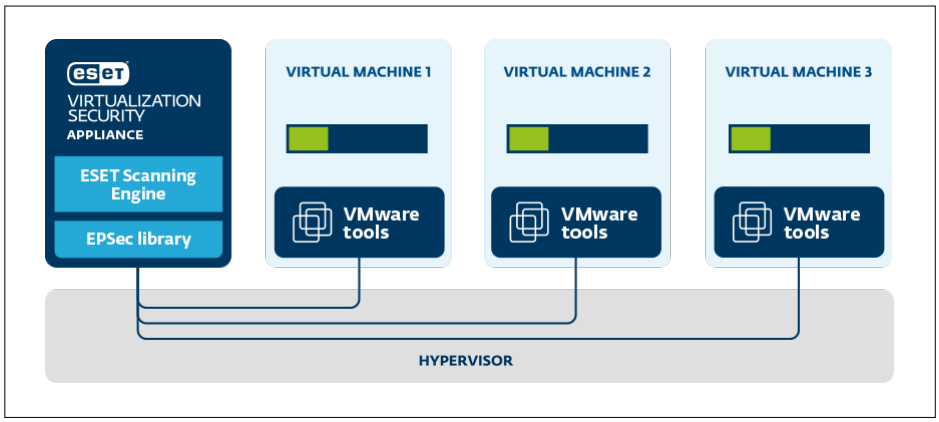
SEE OUR SOLUTIONS IN THE VMWARE SOLUTION EXCHANGE

https://solutionexchange.vmware.com/store/companies/eset-spol-s-r-o

How it Works

Once all the prerequisites are deployed, every virtual machine in the cluster is automatically protected by our award-winning ESET NOD32® scanning engine, augmented by ESET LiveGrid®. If any new VM is created or new host added to the protected cluster, automatic orchestration takes place so that all machines are immediately protected.

Thanks to VMware technology, all content on virtual machines is scanned by the separate ESET Virtualization Security Appliance to optimize resource workload and avoid AV storms. VM security is centrally managed by ESET Remote Administrator, with every VM acting as separate computer.



Prerequisites:

Deployed ESET Remote Administrator, ESET Virtual Agent Host, ESET Virtualization Security Appliance, VMware NSX Manager, VMware Guest Introspection, VMware Tools with Guest Introspection module.

Want to Learn More?

http://www.eset.com/int/business/virtualization-security/vmware/ or contact your ESET or VMware partner or sales representative for a free trial.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw48878-so-eset-nsx-US-uslet-101-final
7/17