ESET® VIRTUALIZATION SECURITY FOR vSHIELD ENDPOINT

Safer computing with cloud-enabled anti-malware protection through vShield Endpoint

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.

ESET DELIVERS IN VIRTUAL ENVIRONMENT

"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. ESET Virtualization Security provides agentless scanning of virtual machines utilizing VMware vShield Endpoint™ technology. Offloading the antimalware scanning to a central, secure virtual appliance on the host ensures both security and performance.

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 (LiveGrid® / Threat-Sense 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 vShield Endpoint.

- 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.

"ESET Virtualization Security has helped our company by reducing the individual virus scanning workload on our 9 Host (100vm) vSphere Cluster."

CRAIG LARGE
SENIOR IT CONSULTANT
MANDATA TRANSPORT MANAGEMENT SOFTWARE, LTD.

VMWARE vSPHERE

VMware vSphere®, the industry-leading virtualization platform, empowers users to virtualize any application with confidence, redefines availability and simplifies the virtual data center. The result is a highly available, resilient, on-demand infrastructure that is the ideal foundation of any cloud environment. This can drive down data center cost, increase system and application uptime, and drastically simplify the way IT runs the data center.

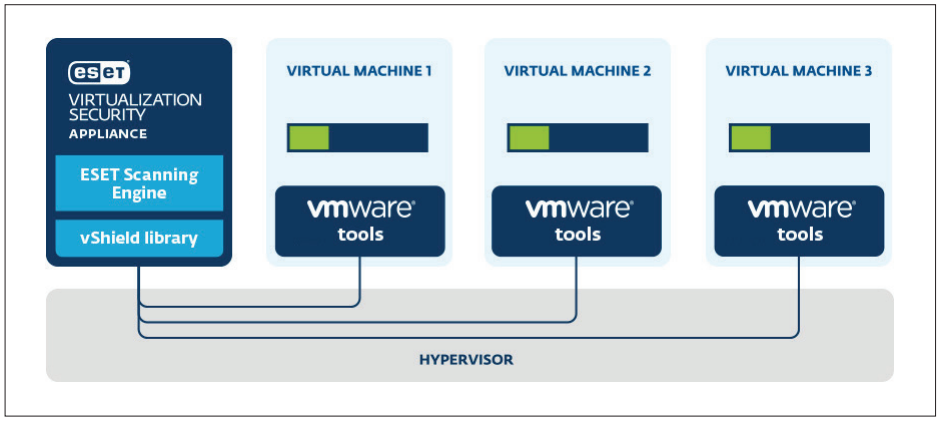
ESET VIRTUALIZATION SECURITY

ESET Virtualization Security for VMware vShield™ is a single ESET appliance that protects all virtual machines running on hypervisor while keeping their speed and performance intact. In addition, the solution natively supports VMware vSphere vMotion® and vCenter™, 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.

vmware READY NETWORKING AND SECURITY

How it Works

ESET's solution includes an ESET Virtualization Security Appliance (EVSA), which offloads scanning, plus ESET Remote Administrator (ERA), the management interface, and ESET Virtual Agent Host (EVAH), the component for virtualizing ERA agents on each protected virtual machine. With VMware vShield Endpoint installed on the host, and VMware tools on each of the virtual machines, users will deploy ESET Remote Administrator management server, and then deploy the ESET Virtualization Security appliance on the host, which integrates vShield manager with ESET's NOD32® scanning engine. With vShield, a dedicated on-hypervisor network is available for rapid file exchange to offload AV scanning from virtual machines to the ESET appliance. All virtual machines with installed VMware tools are protected with on-access real-time scanning, which is assisted by ESET's Cloud Management Protection System. Admins can also initiate on-demand scans from ESET Remote Administrator.



Want to Learn More?

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

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 vShield endpoints on 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

solutionexchange.vmware.com/store/products/eset-virtualization-security

vmware® | eset

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com