SECURING YOUR VIRTUAL ENVIRONMENT

ENJOY SAFER TECHNOLOGY®

Securing your virtual environment

By Phil Herold, ESET staff writer

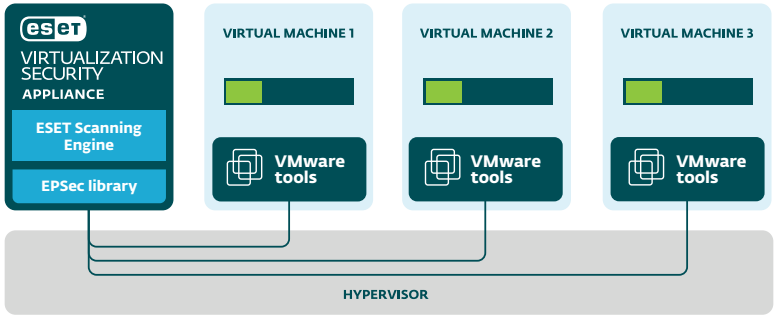
Introduction

Implementing antivirus and other endpoint security measures in virtual environments is often characterized as a trade-off between performance and security. Broadly speaking, there are two approaches:

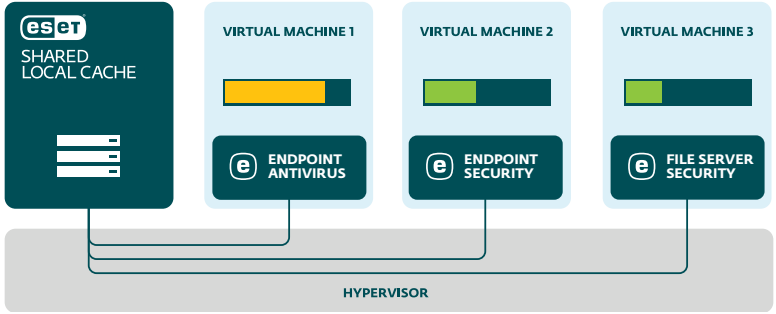
- *Agentless solutions, where the scanning engine resides within the hypervisor and is responsible for all guest VMs.*
- *Agent-based solutions, where individual scanning engines reside on each guest VM.*

Choosing the right system for your business calls for a look at each proposed solution within the particular virtual environment. There are three areas to consider: performance, security, and overall system complexity and management. Depending on the proposed solutions, the trade-offs may be more or less important—or there may be no compromises necessary at all.

AGENTLESS SOLUTION



AGENT-BASED SOLUTION



Performance

In an agentless hypervisor-based system, a single engine handles file scanning for all guest VMs on the physical host. This has performance advantages in some situations—specifically, when compared against agent-based antivirus solutions that are resource-heavy, or where each agent on each guest machine is allowed to run independent of the others without coordination.

However, it is not the case when an agent-based solution optimized for virtual environments meets these criteria:

- Has a far lighter footprint in terms of drive space, memory consumption and CPU utilization than typical endpoint antivirus
- Employs caching systems that detect when a file has already been scanned and marked as clean by another guest VM, reducing unnecessary and redundant scanning activity (and delivering a major performance boost, especially in virtual desktop infrastructure (VDI) environments
- Orchestrates scanning activity across the guests through a centralized management console, staggering the activity so all scanning doesn't occur at the same time
- Allows administrators to control when updates occur

An agent-based solution that implements these measures is far less prone to AV storms, and delivers overall performance similar to an agentless solution.

Protection

Agentless solutions are generally limited to file scanning. Agent-based solutions allow full-featured endpoint security to be implemented on each guest VM for enforcing multiple layers of protection. Such multiple layers are necessary to thwart modern malware that often evades conventional signature-based antivirus, and exploits multiple attack vectors.

A light-footprint solution with an agent on each machine delivers comprehensive protection, including:

- Security measures beyond conventional antivirus, such as host-intrusion prevention, advanced heuristics, detection of exploit behaviors in applications and network traffic, ability to scan for malware after it has been decloaked in memory and inspection of suspect websites for potential phishing scams
- Access to cloud-hosted reputation services that detect malicious files and block applications or network traffic based on blacklists of files, suspect websites and botnet command-and-control servers
- Notifications and malware warnings to end-users on virtualized desktops, to help enforce good computing practices

An agent-based solution enforces security without compromise, equivalent to what can be achieved with a full-featured solution on a physical computer.

Complexity

Agentless systems have some advantages in terms of simplicity, but at the sacrifice of granular per-machine control. That simplicity disappears completely in heterogeneous environments.

An agent-based solution with robust administration capability simplifies management. This includes:

- One common endpoint security solution in mixed hypervisor environments, for both physical and virtual endpoints, or whether servers run Windows®, Linux or Mac® OS X
- A single administration console for centrally managing all endpoints throughout the data center
- Full, multilayered protection customizable by user/role to each VM
- Templatizable agent that can be easily distributed across multiple endpoints, whether physical or virtualized

An agent-based solution with comprehensive management is in many cases simpler to maintain, while capable of being tuned to a higher and more-appropriate level of security for each VM.

Conclusion

Conventional wisdom says that agented, host-based security triggers AV storms that drag down the entire virtual environment. It goes on to say that only agentless, hypervisor-based security solutions are appropriate for virtual machines.

Unfortunately, this fear of performance degradation leaves virtual systems far more exposed to threats than necessary.

An agented solution that pays attention to details around resource consumption and management implements the full-featured endpoint security required to guard against modern malware. It takes this type of multilayered solution to defend against these increasingly sophisticated threats—the kind of protection that only an agented solution can bring to virtual environments without compromise.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®