HYPERTECTION

The new era of Hypervisor Antivirus Protection has come!

No agents
No performance problems
No capacity problems
No malware

Protect your virtual environment!

www.hypertection.com
info@hypertection.com

DESCRIPTION

Hypertection is agentless solution that resides in the virtual environment at the hypervisor level and performs virtual machine inspection and antivirus scanning.

Hypertection obtains access to the file system of each virtual machine and provides the malware detection engine with the required data.

All analysis is performed outside the virtual machine. Both online and offline virtual machines can be scanned.

FEATURES HIGHLIGHTS

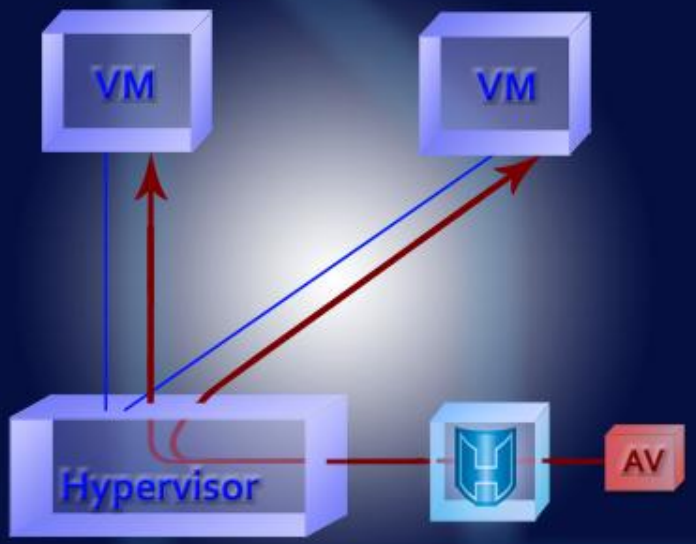
- Online and offline virtual machine scanning
- Reliable and high-performance malware detection
- All popular hypervisors supported (constantly growing compatibility list)
- Scheduled scanning option
- Comprehensive reporting

LOOKING FOR BEST TCO?

Hypertection is licensed on the per-CPU base with the unlimited number of VMs.

It also doesn't reduce the effective capacity of the host as it does not use VM resources.

ARCHITECTURE



System includes two main components:

- Hypervisor Antivirus
- Antivirus Engine

Hypervisor Antivirus obtains virtual machine file system data and transmits it to the Antivirus Engine. Engine performs analysis for malware and provides user with the results.

Each virtual machine even doesn't get notified that it has been scanned.

PURE AGENTLESS

You should not make any compromise. Hypertection is true agentless solution. There is no antivirus system agents that permanently or temporary reside on a virtual machine, there are not any specific components of the virtualization platform to support this antivirus solution on an end-point.

Hypertection really resides only on the host and performs scanning using only host means.

BENEFITS

Solution is easily manageable as it doesn't include agents. It also allows to get round the necessity of system self-protection: malware exists in virtual machine context while Hypertection resides outside it.

Other benefits are:

- Obtained data cannot be violated by malware as it is obtained beyond the virtual machine context.
- No virtual machine resources are used as all scanning and analysis are performed in antivirus engine.
- Any just created virtual machine can be automatically included to the scan list.
- Scanning cannot be avoided from the virtual machine side, so the hypervisor administrator is the only one who manages the process.

VIRTUALIZATION ERA HAS COME

Virtualization market is actively growing. It supposes constantly increasing number of both virtualization servers and virtual machines. Thus while IDC estimates the number of VMs in 2010 in about 10 mil, it predicts that in 2013 there will be about 15 mil and in 2014 - about 18.7 mil of VMs.

At the same time, there is a trend of increasing the number of VMs per host. It is estimated that their density per 1 physical host will increase almost twice till 2014.

The mentioned trends will surely affect the agent-based solutions in terms of both costs and performance influence. When you deploy more VMs it's worth considering the solutions, whose price will not depend on the end-point number.

The increase of VM density will ask any system a question about its scalability - as the load of each host will permanently grow.

Under such conditions, the most effective solutions will be the agentless ones.

WHY DON'T YOU USE...

... antivirus solution installed on each VM?

- Costly licensing
- Inefficient IT resource usage
- AV Storms
- 9 AM Problem
- Complicated Security Management.

... agent-based antivirus solution with hypervisor-based management?

- Agent on each VM is the object to protect from 0-day attacks
- VM's resource are used for scanning
- Only on-line VMs can be scanned
- Limited system scalability.

... virtualization platform adapted solution (like for VMware vShield)?

- Virtualization platform provides its «agents» for each VM
- Such agents commonly do not have the self-protection mechanism as antivirus agents do.

... the scheme with the dedicated Security VM?

- It uses several times more resources than in typical physical PC scenario.