

VMware Boosts Virtual Security Capabilities With Determina Buy

Neil MacDonald

We expect VMware to embed Determina's intrusion prevention technologies into ESX and extend the protection to hosted workloads. This deal raises the bar for security capabilities in hypervisors and virtualized workloads.

NEWS ANALYSIS

Event

On 13 August 2007, VMware informed Gartner that it has acquired Determina, a vendor of a host-based intrusion prevention system (HIPS) technology. There has been no public announcement of the acquisition.

Analysis

Determina brings two HIPS capabilities to VMware. First, the Determina Memory Firewall HIPS solution protects an operating system (OS) and applications against unauthorized memory and program control-flow manipulation — for example, heap and stack overflows, buffer overflows, and similar techniques used by hackers to inject malicious code into running processes (see "Best Practices for Implementing Host-Based Intrusion Prevention Systems"). Second, as a byproduct of its memory protection approach, the Determina technology can also be used to inject new (or modified) code on the fly. This ability to perform "hot patching" is the foundation of the Determina LiveShield solution — a shielding alternative built by reverse-engineering patches used to protect vulnerable systems without a reboot until a permanent patch can be applied.

We believe VMware will use both capabilities of Determina. By potentially integrating Memory Firewall into the ESX hypervisor, the hypervisor itself can provide an additional level of protection against intrusions (see "Building Blocks for Trusted, Secure Hypervisors"). We also believe the memory protection will be extended to guest OSs as well: VMware's extensive use of binary emulation for virtualization puts the ESX hypervisor in an advantageous position to exploit this style of protection. Further, by using the LiveShield capabilities, the ESX hypervisor could be used "introspectively" to shield the hypervisor and guest OSs from attacks on known vulnerabilities in situations where these have not yet been patched. Both Determina technologies are fairly OS- and application-neutral, providing VMware with an easy way to protect ESX as well as Linux- and Windows-based guest OSs.

We believe that these capabilities will be included at no cost in one or more future versions of VMware products, including the ESX hypervisor. The Determina technologies will be discontinued for stand-alone purchase, regardless of whether they would be used for VMware-based guest OSs.

We do not view this as VMware entering the "security market," and we expect VMware to continue to develop its security ecosystem. Rather, the acquisition raises the bar for the security capabilities of hypervisors and virtualized workloads (see "Security Considerations and Best Practices for Securing Virtual Machines"). The Memory Firewall and LiveShield functionality overlaps partially with network and HIPS security offerings. However, the technology should be viewed as one layer in a multilayered overall virtualization security strategy, and not as a complete intrusion prevention system (IPS) solution.

RECOMMENDATIONS

- If your organization is using Determina Memory Firewall or LiveShield technology, plan on product support being discontinued by YE08.
- If you are considering virtualization solutions from XenSource, Virtual Iron or other vendors, make security a part of the evaluation with specific queries about how the hypervisor and guests OSs are protected from intrusions.

- Request specific road map commitments from VMware as to when the Memory Firewall and LiveShield technology will be included in VMware products, whether this protection will be extended to guest OSs and which, if any, applications will be protected by the Memory FireWall and LiveShield technologies.

RECOMMENDED READING

- "Host-Based Intrusion Prevention: Myths and Realities" — Many misconceptions surround HIPS solutions, mostly due to common use of the term "HIPS" to describe a variety of solutions that deliver very different styles of protection. **By Neil MacDonald**
- "Secure Hypervisor Hype: Myths, Realities and Recommendations" — Hypervisors, like any emerging technology, will become a target for hackers, but the threats will often be overhyped. **By Neil MacDonald**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509