

## Intel vPro a Step Forward for Security Software Appliances

Neil MacDonald, Amrit T. Williams

The use of virtualization to isolate security software functionality is becoming increasingly important. Intel's new vPro virtualization will take time to reach the market, but will accelerate this trend.

## NEWS ANALYSIS

---

### Event

On 24 April 2006, Intel introduced the vPro platform for maintaining and managing desktop PCs. vPro, which includes an Intel Core microprocessor, the Q965 chipset, the Intel Pro/1000 controller, and integrated graphics and network interface cards, will be available in 3Q06.

### Analysis

Systems that carry Intel's vPro brand will offer important new integrated capabilities (see "Intel vPro Adds Value Through Remote Management for Desktop PCs"). These capabilities include security virtualization, which enables security software to run as a software appliance — a single virtual-machine partition, isolated from the operating system (OS) and applications. Partitioned security functionality (for example, host-based intrusion prevention systems and patch management tools) cannot be altered or deactivated by end users or malicious code. Intel's "ecosystem" partners will deliver additional functionality that makes use of this increasingly important capability.

Security virtualization is not new. Lenovo's security appliance, for example, exploits Intel Virtualization Technology-enabled systems, and products such as VMware isolate virtual machines using software-based enforcement by the virtual-machine manager, which can itself be a target for attack. vPro's hardware-enforced virtualization reduces this threat, but areas of vulnerability remain: A thin hypervisor layer governs virtual-machine creation and management, and the security partition itself runs an OS. These will be targets for attack and may need to be patched. vPro also presents other challenges:

- Virtualization is limited to a single partition and application, but many security and management products would be useful as appliances. (Gartner believes this limitation is intended to appease Microsoft, which plans its own future hypervisor.)
- vPro-branded systems will initially be unavailable for mobile notebook computers.
- Migrating installed PCs, and developing a healthy vendor ecosystem, will take time.
- The technologies behind vPro are proprietary to Intel.

### Recommendations

- Consider the benefits of isolating security functionality using virtualization, but do not necessarily wait for vPro. Enterprises that need this functionality can find products on the market now that use existing hardware
- Use virtualization products that exploit Intel Virtualization Technology or AMD Pacifica technology for hardware-enabled enforcement and virtual-machine management
- If possible, pursue a hypervisor or virtualization strategy that supports both Intel and AMD processors (as Xen does and Microsoft's future hypervisor will).
- If you plan to use vPro to deliver a security appliance and plan to use another hypervisor (for example, Microsoft or Xen), make certain the appliance and the hypervisor can coexist and test thoroughly for compatibility issues before deployment.

**Analytical Sources:** Neil MacDonald and Amrit Williams, Gartner Research

## Recommended Reading and Related Research

- "Understanding the Nine Protection Styles of Host-Based Intrusion Prevention" — Many technology providers are entering the market with host-based intrusion prevention systems using markedly different protection approaches. The best of these offerings will use multiple protection techniques. **By Neil MacDonald**
- "Hypervisor Plug-Ins Create New System Opportunities" — Today's virtual-machine monitors will generate computer code called "hypervisors," which will offer a secure and managed environment. **By Martin Reynolds**

(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