

CLEAR CHOICE TEST: VIRTUALIZATION SECURITY

New tools emerge to protect VMs

Testing reveals that no one product can do it all when it comes to VM security

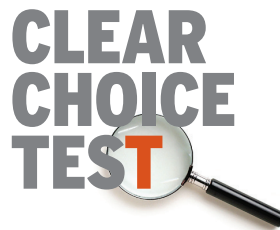
BY DAVID STROM

As enterprises move toward virtualizing more of their servers and data center infrastructure, the security technologies that are plentiful and commonplace in the physical world become few and far between.

While few direct attacks on virtual machines have been observed, it is still good security practice to protect VMs from potential vulnerabilities that exist only in the virtualized world.

For example, physical firewalls aren't designed to inspect and filter the vast amount of traffic originating from a hypervisor running 10 virtualized servers. And because VMs can start, stop and move from hypervisor to hypervisor at the click of a button, protective features have to be able to handle these movements and activities with ease. Finally, few hypervisors have the access controls that even the most basic file server has: Once someone can gain access to the hypervisor, that person can control all of the VMs that are housed there.

In response to these concerns, a number of new vendors have created virtualization security tools. And the pace of mergers and acquisitions has picked up as the established vendors try to augment their offerings and integrate products. For example, VMware purchased Blue Lane Technologies and



incorporated Blue Lane's software into its vShield product line. Juniper Networks purchased Altor Networks' Virtual Firewall and is integrating Altor into its line of firewalls and management software. And Third Brigade is now part of Trend Micro's Deep Security line.

For this test, we sent invitations to all of the major players. The five who accepted are: BeyondTrust PowerBroker Servers for Virtualization, Catbird Networks vSecurity, HyTrust Appliance, Reflex Systems Virtualization Management Center, and Third Brigade/Trend Micro Deep Security. Declining were CA for its Virtual Privilege Manager, Juniper/Altor, Fortinet FortiWeb VM (which was just announced in January) and VMware's vShield.

We found that no single product can do everything well, or even more than a few things. While it would be nice if we could buy a VM-equivalent of a unified threat management tool, none currently exists.

Since the products have different sets of

capabilities, they are not directly comparable. We developed a scorecard that indicates which vendors do a better job in various categories, but we're not naming an overall winner. In fact, a few of these vendors have teamed up to provide combined solutions. This coupled with the active mergers mentioned above means that this is a very dynamic category and you should expect further consolidations and changes.

If you are new to virtualization, these products might seem confounding as they use an entire new vocabulary, such as the word "hosts" to indicate the physical hypervisor servers that run individual VMs. And obviously, you will need some experience with vCenter and ESX to understand how to deploy and use these products.

Of the five products, Reflex's Virtual Management Center is the most comprehensive, with modules in three broad areas that we examined — auditing/compliance, firewall/intrusion detection and access controls. These modules are knit together with separate reporting and management consoles. That is a lot to handle, to be sure.

Trend has the best and most useful reports, suitable for distribution to management. Catbird has the most sophisticated network-based protection, akin to something found on a Cisco or Check Point physical device. HyTrust shines when it comes to limiting access to authorized users and roles.

NETRESULTS

Product name	Power Broker	vSecurity	HyTrust Appliance	Virtual Management Center	Deep Security
Company	BeyondTrust Software	Catbird Networks	HyTrust	Reflex Systems	Trend Micro
Price	Starts at \$1,600 per server (plus maintenance).	\$1,995/socket.	\$1,000/host.	Each protective module is \$600/socket.	\$200/VM for anti-malware, \$1,100/VM for all protective modules.
Pros	Root password protection of hosts.	Complex network protective features based on industry standard products.	Solid access controls and simple setup.	Comprehensive set of security solutions across a wide feature set.	Reports that are clear and actionable and suitable for management.
Cons	Command line interface; requires custom scripting.	User roles and reporting limited.	Reports are voluminous to the point of being overwhelming.	Reports and access controls are a weakness.	Compliance is skimpy.
Total score	3.375	3.0	3.875	4.0	4.25

BeyondTrust has its place protecting Linux VMs.

But the downsides to these products can overwhelm their benefits. Most are somewhat quirky to learn how to use and deploy. The notable exception is HyTrust with setup on the order of a network load balancing device. There are many moving parts to the other products to get their protection working properly, and all will require you to gather your experts on networking, authentication, virtualization and overall security in the same room to coordinate deployment.

We looked at four broad functional categories in our evaluation:

- **Reporting.** We looked at how easy it is to generate actionable reports and whether the product can automatically flag particular violations. If the product has compliance monitoring or remediation features, we also looked at how it performed in this arena. Reflex and BeyondTrust have separate Web-based reporting tools, the others use menus on their Web-based management tools.

We liked the reports from Trend Micro the best: They were easiest to produce and parse, and to share with management. The others (such as HyTrust or Catbird) either produced reams of pages, or were so difficult to set up that the most dedicated operator would find generating them taxing (BeyondTrust).

- **Host management.** We looked at what it takes to protect a new ESX host. Each product has a different activation process; HyTrust and Reflex are easier than the others, which require multiple configuration steps or a series of different agents to be added to each host. The goal here is to provide instant-on protection, because many times VMs can be paused and restarted, avoiding the traditional boot-up checks that physical antivirus products use.

- **Policy controls.** We looked at the granularity of the product's policies and how easy it is to add elements to existing policies or create entirely new ones. This is the bread and butter of these products, no matter what else they are designed to do. All of them delivered the goods in this area and there was little to distinguish the products.

- **User management.** We examined the granularity of user controls and how easy it is to add new users to the product, or to assign users to particular security roles. HyTrust, Reflex and Trend have the most complex and granular role settings.

All of the products are closely tied to VMware ESX and vSphere. Catbird's vSecurity can also protect Citrix Zen installations, and BeyondTrust PowerBroker can also support Xen, Solaris Zones

SCORECARD

Product	Deep Security	HyTrust Appliance	Virtual Mgmt. Center	Power Broker	vSecurity
Reporting (25%)	4.5	3.5	3	3	3
Host management (25%)	4	4	4.5	3	3
Policy Controls (25%)	4	4	4	3.5	4
User Management (25%)	4.5	4.5	4.5	4	2
Total	4.25	3.875	4.0	3.375	3.0

SCORING KEY: 5: EXCEPTIONAL; 4: VERY GOOD; 3: AVERAGE; 2: BELOW AVERAGE; 1: SUBPAR OR NOT AVAILABLE

and IBM's VM environments. None of the products currently protect Microsoft HyperV installations.

Who does what

There is no single tool that does everything. Anyone serious about VM security is going to need more than one tool. Here's a quick guide:

- **Compliance and auditing.** This includes the ability to produce reports to understand various compliance requirements, such as Payment Card Initiative standards and the ability to audit access and administrative logs to track down what someone changed and when. All five offer some of these features.

- **Intrusion detection (IDS) and firewall features.** These are the features that most people think of when they first hear about VM security. Catbird, Reflex and Trend offer modules with some of these features.

- **Access controls.** This includes being able to restrict access so users can't stop or change any VMs on any protected host machine. BeyondTrust, Reflex and HyTrust offer some of these features, and all also have the ability to tie access control roles to particular Active Directory users.

- **Antivirus/anti-malware protection.** Similar to the antivirus tools on the physical world, this provides protection against these exploits inside a VM. Trend Micro has this feature.

Where does VMware's vShield fit in?

While we didn't test vShield, it is a prerequisite for the Trend Micro product and has the beginnings of its own security interfaces that other vendors

will most certainly exploit in coming months. Reflex (and Altor/Juniper) also works with vShield, although it is not required. None of the other products we tested use vShield.

Trend Micro Deep Security

Trend Micro purchased Third Brigade and has incorporated its features into Deep Security. The product has a variety of protective modules, including agent or agentless firewall/IDS, anti-malware, and Web application protection. The antivirus scanner requires vShield Endpoint to be installed and only works on certain Windows VMs and is agentless. Trend is working to incorporate its physical and virtual protections under one roof, but isn't there with the release we tested.

As you might suspect from a consumer-focused software company, its Web management interface is very attractive and the dashboard has a lot going on. At a glance you can see your entire VM collection, whether any protective measures have been installed, and what alerts have been reported. You have to use the maps generated by VMware to see a visual picture of your network of VMs and their hosts.

And as you might suspect from a security software company, Trend's firewall and IDS features are numerous, including deep packet inspection and a collection of dozens of rules that deal with operating system integrity monitoring. For example, if anyone makes changes to the Windows "hosts" file, it can get logged as a questionable event.

Trend Micro's reporting module is clear and part of the overall Web dashboard. You have a pull-down

menu selection to create one of 18 reports in either a RTF or a PDF file. If the latter, you can click on a share button and have it e-mailed to your boss. You can easily set the date ranges and the VMs of interest by clicking on the relevant buttons.

The main drawback is the compliance feature set. Unlike HyTrust, Trend Micro doesn't categorize each guideline element by element, but scans each VM for preset rules as part of its integrity monitoring module. You can easily create your own rules or

modify the ones that are included in the program. There is no automated remediation, either.

Adding a new VM is straightforward. Because Trend hooks into the vCenter interfaces, as soon as you add the VM, it is protected. The only thing you need on the VM is the VMware vShield Endpoint Guest software.

Trend can sync with Active Directory and LDAP-enabled directories and pull its users from that. Then you can assign roles to these users. And

Trend has lots of granularity with how each role is assigned to each user, down to dozens of rights for particular activities. So you can set up users who can view things but can't delete or change any parameters. ■

Strom is the founding editor-in-chief of Network Computing magazine and has written thousands of magazine articles and two books on various IT and networking topics. His blog can be found at strominator.com and you can follow him on Twitter @dstrom. He lives in St. Louis.

FEATURESUMMARY

Product, Version	URL, Price	Agents	VM versions	Functions	Notable Features
BeyondTrust PowerBroker v6.2	Beyondtrust.com \$1,600/server	Yes	ESX/ESXi all v3. and v4.; Citrix Xen; Solaris and IBM	Compliance, access control	Root ESX password protection
Catbird vSecurity 3.5	Catbird.com \$1,995/per socket	Yes	ESX/ESXi all v3.5 and v4.; Citrix Xen	Compliance, Firewall/IDS	Deep inspection rules
HyTrust Appliance v2.1.2	Hytrust.com \$1,000/host	No	ESX/ESXi all v3.5 and v4.	Access control, compliance	Root ESX password protection
Reflex Systems v2.9	Reflexsystems.com \$1,800/per socket	Yes	ESX only, all v3.5 and v4.	Access, Compliance, Firewall/IDS	Topo map, network zones, change tracking
Trend Micro Deep Security v7.5	Trendmicro.com \$1,100/VM	Either	ESX/ESXi all v3.5 and v4; and VMsafe	Antivirus, Firewall/IDS, Compliance	Deep inspection rules, reports

www.trendmicro.com/deepsecurity