powerbroker® virtualization

beyondtrust
securing the perimeter within

PowerBroker® Virtualization FAQ

PowerBroker Virtualization enables organizations that move to virtualized platforms to control administrative access to the Hypervisor/VMM layer while still realizing all virtualization cost efficiencies. Features include:

- Granular delegation of administrative privileges
- Detailed and flexible reporting including keystroke logging of admin activities
- Two-click entitlement reports
- Programmable role-constrain mechanisms for segregation of duties
- Secures virtual guest and host hypervisors
- VMware ESX, Solaris Zones, AIX WPAR, and IBM z/VM
- Support for more than 30 guest operating systems

About BeyondTrust
BeyondTrust is a proven leader with more than 25 years of experience. More than half of the companies listed on the Dow Jones, eight of the 10 largest banks, seven of the 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies rely on BeyondTrust to secure their enterprise.

Can't the virtual machine vulnerability be addressed by using encrypted file systems on the virtual machines?

Yes. If the file systems of the virtual machine are encrypted, and the encryption key is not available to the user logged into the hypervisor. If both remain true, then the ability to mount and read data from the drives is removed.

What is BeyondTrust doing to support ESXi architecture?

Due to the architectural changes in ESXi, which includes the elimination of the ESX COS console, different techniques are required for supporting ESXi environments. BeyondTrust is actively working on several unannounced technologies to bring PowerBroker support for the ESXi architecture.

Doesn't disabling root access to the COS by SSH remove this vulnerability?

The virtual machine vulnerability can occur by a hypervisor user on the system console, as well as through a remote SSH session. Disabling SSH root access does improve the situation as it requires physical access to the system console, and most IT organizations have good controls in place to limit physical access to the important hosts. However, consider that the administrative users that have the skill set to exploit the virtual machine vulnerability are also the same users that typically have physcial access to the system console.

How is the ESX hypervisor layer secured by the use of PowerBroker?

The security of the ESX hypervisor environment is improved when work done in this layer is performed by non-root, but authorized users, and delegated as privileged processes and logged through the use of PowerBroker. When PowerBroker is used in the hypervisor layer, control, accountability, and traceability is maintained when the hypervisor command line interface (CLI) layer is accessed. Thus, the ESX hypervisor layer is secured by PowerBroker through careful delegation of privileged processes to non-root and authorized users.

Can a non-root, but authorized user, be prevented from executing a command with an undesirable consequence?

When PowerBroker is used to monitor the command line interface (CLI) of the ESX hypervisor layer, a non-root, but authorized user, can be granted commands appropriate for the security level of the work that needs to be performed. More privileged commands can be delegated to more privileged users thus improving and preserving the security of the ESX hypervisor layer.

Should a root-shell be granted to an authorized user in the ESX hypervisor layer?

Root-shells should not be delegated to everyone and should be carefully monitored whenever access is given to an authorized user. This should not be delegated for convenience, but delegated instead based on necessity and the requirement of the work that needs to be completed. PowerBroker provides all the required monitoring tools.

powerbroker® virtualization

beyondtrust® securing the perimeter within

PowerBroker® Virtualization FAQ continued...

Is there an operational vulnerability in the ESX hypervisor that PowerBroker secures?

When both VMware's and BeyondTrust's best practice suggestions are adhered to, and PowerBroker is used as the gatekeeper for the command line interface, the security of the ESX hypervisor layer is improved and easily maintained as PowerBroker provides the necessary control, accountability, and indelible audit trail of work done through this interface in the ESX hypervisor layer.

Is BeyondTrust a VMware partner?

Yes. BeyondTrust is an independent software vendor (ISV), and a member of VMware's TAP Program.

How is PowerBroker different from HyTrust?

PowerBroker and the HyTrust Appliance each manage the security of your virtual infrastructure, but each covers different parts of the problem. In many ways, the two solutions are more complementary than competitive. The HyTrust Appliance provides configuration management and access control for recent VMware environments and can provide controls to keep the virtual environment configured correctly. It can also provide simple access control to privileged accounts at the hypervisor level.

PowerBroker provides delegated, policy controlled privileged access to privileged accounts at both the hypervisor level (the ESX COS or the ESX/ESXi VMA) and to any Unix/Linux virtual machines. Using PowerBroker, an administrative user can be provided access to a privileged account at the hypervisor level or inside a virtual machine, and can be managed by policy to perform only the certain actions or commands that are appropriate to the functions he/she needs to accomplish.

Does the BeyondTrust solution work in heterogeneous virtual environments as virtualized data centers never seem to be homogenous(i.e., AIX, Zen, and MSFT)?

Yes. One of the strengths of BeyondTrust's PowerBroker products is the coverage we provide for a larger number of virtualization environments and virtual machines. PowerBroker provides certified support for ESX/ESXi (ESXi coming soon), Solaris Zones and Containers, AIX WPARS, z/VM Linux, IBM VIO Server and most major variants of Unix, Linux and Windows running as virtual machines. PowerBroker can also be used to manage virtualization technologies running on supported platforms, such as Xen, Oracle VM and KVM running on Linux.

Have More Questions?

Email us: info@beyondtrust.com

Call us: +1 800-234-9072
+1 818-575-4000

Fax us: +1 818-889-1894

Visit us: 2173 Salk Avenue
Carlsbad, California
USA 92008

vmware READY CERTIFIED

BeyondTrust is partners with VMware, the global leader in virtualization, who retains more than 190,000 customers worldwide.

Did You Know...

About 70% of a typical IT budget in a non-virtualized datacenter goes towards just maintaining the existing infrastructure, with little left for innovation.

beyondtrust® securing the perimeter within

www.beyondtrust.com

Corporate Headquarters
2173 Salk Avenue
Carlsbad, California 92008

Phone: +1 800-234-9072