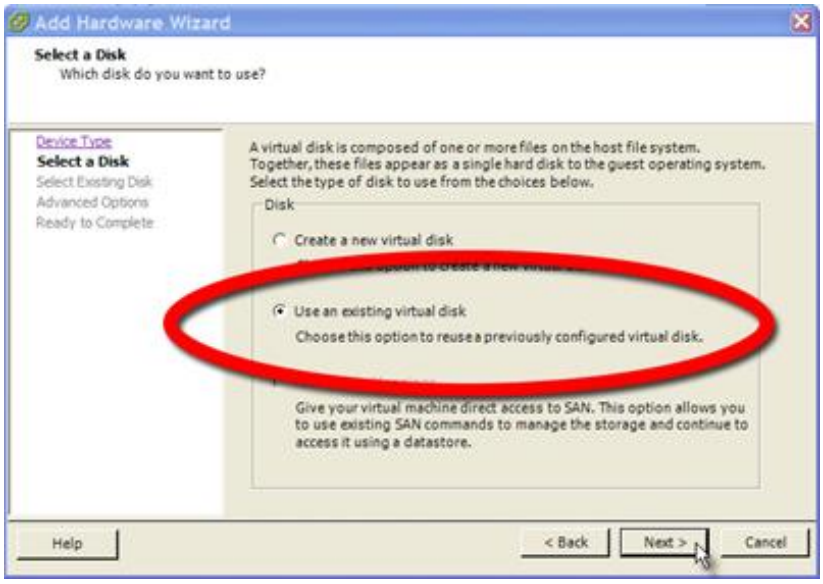
Full Disk Encryption for Virtual Machines

Virtualization technology is dramatically transforming the IT landscape and changing the way people and organizations use technology and resources. Virtualization solutions essentially allow users to transform hardware into software — thus reducing overall IT costs while increasing the efficiency, utilization, and flexibility of their existing computer hardware. Basically, organizations can now more easily and rapidly deploy infrastructure and resources.

With data center power consumption and costs growing exponentially, enterprises are increasingly turning to virtualized infrastructures as a way to maximize their operational efficiencies while minimizing their administrative costs. However, these added efficiencies create a number of new potential security issues due to the centralized and virtualized nature of the "server" technology.

Virtualization: A cost-effective way to essentially add a hard drive



Virtualized machines simply exist as files on a storage area network (SAN).

Because of this, it is extremely easy to attach any virtual machine to another as a "disk" — much like physically attaching an additional hard disk drive to a PC in order to gain access to its data.

In a virtual environment, anyone with the right privileges can easily mount an existing virtual machine without attracting attention. A SAN administrator simply has to connect to the virtual machine to gain access to the data by clicking a few buttons.

SAN administrators are granted high levels of access to these machines in order to administer, deploy, provision, and manage the resources on both a virtual and physical level. Many enterprises maintain multiple SANs with different administrators in order to control the level of access to critical data. Nevertheless, even this precaution cannot completely prevent unauthorized access:

- SAN Administrators can replicate data from a SAN when they have limited access to a SAN where they have more privileges.
- Administrators can mount a virtual machine to multiple hosts and gain access to data in the virtual machine they wish to breach.
- SAN Administrators can simply copy a virtual machine to a USB drive and take the data offsite.

How does AlertBoot protect and secure machines on a virtual infrastructure?

If your enterprise's virtual machines are encrypted with AlertBoot full disk encryption, the SAN administrator can attempt to access them but, without the proper AlertBoot privileges, these virtual machines will appear as unformatted disks. Any attempt to gain access to the data this way would be futile.

Furthermore, this encryption persists no matter where the virtual machine image resides. AlertBoot disk encryption employs *USER* security policies, which persist for the user regardless of the machine. This means

- Replicating data to a SAN where an administrator has more privileges will never work because the encryption policy is enforced for the user. Thus, the machine appears as an unformatted disk.
- Mounting an unauthorized virtual machine to an administrator's host is pointless. Again, because of the persistent user security policy, the machine appears as an unformatted disk.
- Copying the virtual machine data to a USB drive is useless because that virtual machine image is encrypted and utterly unusable.

Virtualization offers a multitude of cost benefits and IT efficiencies for enterprises but, as we've seen, they also create a multitude of unique security issues as well. Attempts to plug these security holes by limiting virtual machine access and SAN administrator privileges ultimately dilute the efficiencies and benefits that are gained by this technology. Additionally, these limitations can sacrifice the high availability and uptime capabilities of the virtualization technology.

Using AlertBoot disk encryption to encrypt the virtual machines as if they were actual, physical servers allows enterprises to reap all the cost-saving advantages of virtualization without compromising the overall security of an organization's critical data.