

# VirtSec

## Protecting Virtual Infrastructures

Blue Lane Technologies Inc.  
10450 Bubb Road  
Cupertino, CA 95014

## Why you should read this white paper

The broad range of substantial benefits and opportunities that virtualization provides has resulted in it being rapidly propelled into the enterprise mainstream with the dominant platform from VMware now being leveraged by more than 20,000 corporations, including 99 Fortune 100 companies. Despite such widespread adoption, virtualization can still be regarded as an emerging technology – especially when it comes to security. While best practices for securing physical infrastructures are both well established and well documented, there is much less material available relating to the securing of a virtual infrastructure. Organizations sometimes assume that the security practices and policies they apply to the physical infrastructure can simply be carried over to the virtual infrastructure, and to some extent they can: virtual security (VirtSec) and physical security considerations are really not all that different. But nor are they identical and virtualization does introduce a number of complications.

This white paper will examine the challenges associated with securing a virtualized infrastructure and explain how Blue Lane Technologies' VirtualShield™ can help an organization overcome those challenges.

## What is virtualization?

While the majority of people will no doubt already be familiar with virtualization, a brief explanation will benefit those who are not. Virtualization is a technology that splits a computer into multiple execution environments enabling multiple heterogeneous operating systems to be run concurrently. To achieve this, a hypervisor such as VMware ESX Server is installed onto the bare metal of the server to enable the creation of multiple self-contained virtual machines. According to VMware, a virtual machine is “like a physical server, only instead of being a box of electronics, it is a set of software files. Each virtual machine represents a complete system – with processors, memory, networking, storage and BIOS – so that operating systems and software applications run in virtual machines, just like in a physical server, without any modification.” Resources are allocated to each virtual machine by the hypervisor ensuring that servers are optimally utilized without creating resource contention between virtual machines.

The benefits of virtualization are both manifold and substantial:

- The workloads from multiple under-utilized servers can be consolidated to a single server resulting in increased utilization rates and enabling both a reduction in the installed server base and in future spending.
- Reducing the installed server base reduces rack space, energy and cooling requirements and costs while streamlining management tasks such as backup and provisioning.
- Virtual machines can be easily backed up, moved between physical servers or kept on hot standby and so can both increase agility and simplify disaster recovery planning.
- Virtual machines run in complete isolation and so provide a completely sandboxed environment for testing and development.

This list is far from exhaustive. Virtualization also enables enterprises to reduce their carbon footprint, extend the life of legacy applications, enhance both application availability and business continuity, reduce licensing costs as well as delivering a broad range of other benefits.

There can, however, be no gain without pain. Virtualization results in an infrastructure that is so radically different from its physical predecessor that it will be necessary for organizations to rethink parts of their existing security strategy.

## The challenges of VirtSec

Security considerations in virtual and physical environments are not entirely dissimilar. A virtual machine is nothing more than a software version of a physical system, and so it makes sense that many of the rules which apply in the physical world are equally applicable in the virtual world. That said, virtualization does introduce some additional complications.

While hyperjacking - attacking the hypervisor in order to obtain complete control over the entire virtual system - has received a not inconsiderable amount of publicity, the fact is that vendors have put much effort into securing their already leanly coded hypervisors and they have yet to be exploited in the wild- and possibly may never be exploited. Similarly, talk about rogue virtual machines and virtual machine hopping is entirely speculative: neither is happening today and neither may ever happen.

The *real* VirtSec challenge at this point in time lies with securing the operating systems that are run in virtual machines.

Virtual machines are both highly mobile and ephemeral: they can be speedily created, speedily put to rest and moved from location to location just as easily and as quickly as any other collection of files. This is both a blessing and a curse. On one hand, it can inject real agility into the infrastructure; on the other hand, it can make tasks, such as patching, extremely difficult. Managing physical servers can be challenging, but managing virtual servers can be akin to herding cats.

In a virtual environment, base builds - images of preconfigured operating systems - are created, stored and used to provision virtual servers. But, as new security vulnerabilities are discovered, both the base images and the virtual servers provisioned using those base images need to be patched. Resultantly, administrators must either patch the base builds and then re-provision virtual servers or apply patches directly to each virtual server. This may not seem too different from the position in a non-virtualized environment - physical servers need to be patched too, of course - but what makes matters more complex in the virtual world is the mobility of virtual servers. Given the speed with which virtual servers can be created and the ease with which they can be moved, discovering which servers exist at a particular point in time and their patching levels can be a daunting prospect.

VMware's ESX Server does have some in-built functionality to make patching an easier and speedier process. The Update Manager, introduced in version 3.5, can discover and scan all online, offline or suspended virtual machines within the virtual environment, compare the results against a pre-defined update baseline and perform automated remediation. However, as not all machines *should* be updated - development and legacy application requirements will invariably necessitate that a number of machines running older or unpatched operating systems be retained - the process is nonetheless complex and room for human error exists. Furthermore, the Update Manager can only patch a machine once it has gathered the latest patch data from VMware, Microsoft and other vendors. This means that there is a delay between the discovery of a vulnerability, the release of the patch, the Update Manager checking for the availability and the patch being applied to machines - and that delay represents a window during which virtual machines remain vulnerable. Additionally, the Update Manager's automatic remediation capabilities are limited to Windows Virtual Machines and all other operating systems will need to be manually patched. And of course with the high rate of change in a virtual environment even regular patching can leave extended vulnerability windows. That puts even more importance on properly protecting VMs in the network.

Complicating matters further is the fact that many security products have shortcomings when deployed in a virtual environment. For example, signature-based products, such as intrusion prevention systems (IPSs), that are hosted within a virtual machine will not be updated while a machine is offline or suspended and, consequently, the machine will be vulnerable for a period when next brought online. While IPS vendors have added some vulnerability coverage to their capabilities, they are not comprehensive enough to defend most data center operating systems and applications. Similarly, the majority of network-based IPSs are limited by the fact that they are unable to monitor inter-virtual machine traffic – it is not a job that they were designed to do – and lack host-specificity. This is crucially important. In the physical world, IPSs can mitigate risk between the time that a vulnerability is discovered and the time that it is patched; in the virtual world, however, such limitations simply increase the risk factors during the period in which machines remain unpatched. Additionally, the risks escalate even further when outdated operating systems or applications are run for development purposes or to support legacy applications.

The upshot of all this is that while virtualization certainly has the potential to increase the robustness and security of an infrastructure, it can end up having exactly the opposite effect unless the issues previously discussed are properly mitigated.

### The Blue Lane solution: VirtualShield

VirtualShield was designed to enhance the security of virtual servers on the VMware Virtual Infrastructure 3.0 platform.

VirtualShield is a plug-in to the ESX Server hypervisor that analyzes both externally and internally sourced traffic crossing virtual switches and removes potentially malicious content before it reaches the virtual servers.

To enable VirtualShield to identify and correct potentially malicious content:-

- Software vulnerabilities and patches are analyzed by Blue Lane and updates automatically pushed to VirtualShield that enable it to shield VMs from exploits targeting those vulnerabilities, directly within the network stream. This is an extremely speedy process with updates being pushed out before or soon after patches are released.
- Vulnerabilities listed by sources such as Bugtraq are examined and VirtualShield is updated to protect unpatched vulnerabilities. This too is a speedy process with VirtualShield being updated within a very short period of the announcement of a vulnerability. Once a vendor patch is released, VirtualShield can be updated in order to ensure that it duplicates the functionality of that patch.

Unlike IDSs that rely on attack-specific signatures, VirtualShield is vulnerability-specific and so produces a minimal number of false-positives and is invulnerable to attack variants and leading evasion techniques, including layer 2 evasions, SQL injection, cross-site scripting and polymorphic bot attacks. Additionally, VirtualShield is able to secure all network traffic – including inter-virtual machine traffic – and so is able to provide a more complete protection than an IDS without causing disruption.

By pre-emptively addressing vulnerabilities, VirtualShield secures virtual servers at the earliest possible time – often even in advance of a vendor patch being released – enabling organizations to secure their VMs quickly while setting their own patching schedule, rather than being forced to adhere to a schedule that is determined by vendors or taking unnecessary availability risks by patching too quickly.

VirtualShield's key features and benefits include:-

- Continual automatic discovery of virtual servers to both minimize administration and ensure that virtual servers are immediately protected, even when relocated by VMotion and regardless of online/offline state.
- Instantaneous protection for a comprehensive range of operating systems, servers and applications including Windows Server 2003, Windows 2000, Windows NT, FreeBSD, Red Hat, Microsoft SQL Server 2000 and 2003, Microsoft Exchange Server 5.0, 5.5 and 2003, Solaris 7, 8, 9 and 10 and more.
- Protects VMs regardless of their physical location, state or level of patching.
- Corrects data midstream to ensure that servers are not disrupted.
- Protects older operating systems, even when those operating systems are no longer supported by the vendor.
- Provides quick protection without requiring servers to be rebooted.
- Vulnerability-specific detection ensures immunity to variant attacks.
- Integration with VMware Virtual Center to enable easy management of virtual machines.

## Conclusion

The *real* challenges of VirtSec can sometimes be obscured by the publicity given to subjects such as the susceptibility of the hypervisor to attack and the possible emergence of virtualization-specific malware. While such matters are by no means unimportant and may eventually become real word problems with which organizations must deal, they are currently little more than hypothetical talking points.

The *real* VirtSec challenge of today is securing virtual machines against traditional threats and exploits that can affect any public-facing server – physical or virtual. In the virtual world where machines can be created, moved from online to offline and vice versa or VMotioned from one location to another in a matter of moments, securing servers can be far from easy – especially as many security solutions have limitations when deployed in a virtual environment.

VirtualShield remedies this problem and enables an organization to reap the maximum benefits of virtualization with a minimum of risk.

## About Blue Lane Technologies

Headquartered in Cupertino, CA., Blue Lane Technologies provides solutions that secure virtual and physical data centers with zero footprint, zero downtime and zero tuning. Since January 2007 Blue Lane has won Best of Interop in security as well as InfoWorld's Technology of the Year, also in security. In 2007 Blue Lane also won a Best of VMworld Finalist award in data protection. Blue Lane has won numerous other awards, including the AO 100 Top Private Company Award for 2006 and 2007.

Blue Lane Technologies is privately held. It has alliances with Microsoft, VMware, Oracle, Red Hat and Qualys. Customers include Davidson Hotels, WesCorp, The Metropolitan Transportation Authority, Wyeth, service providers Ornis and Artful and some of the world's top consumer, healthcare, financial, government and technology organizations.

To find out more about Blue Lane and its products, please visit [www.bluelane.com](http://www.bluelane.com).

## About the authors

Brett Callow and Rhonda Turner are technical consultants providing services to a number of leading international technology companies and have been extensively involved in the planning and development of various industry-standard IT certification examinations. Brett has been awarded Microsoft's Most Valuable Professional (MVP) designation for the last 4 years. MVPs are exceptional technical community leaders from around the world who are awarded for voluntarily sharing their high quality, real world expertise in offline and online technical communities by Microsoft. To contact the authors, e-mail [brett@mvp.org](mailto:brett@mvp.org).