

VIRTUALIZATION SECURITY:

A Coordinated Approach for
Intrusion Detection and Prevention

WHITE PAPER



Overview

Virtualization environments share many of the same security challenges faced by physical server environments. This paper explores the challenges of protecting, and the opportunities for improving the security of, virtualized environments. It outlines a Coordinated Approach for Intrusion Detection and Prevention which can be deployed today, and that is architected to take advantage of additional capabilities which virtualization vendors are adding to their platforms.

TABLE OF CONTENTS

1. Introduction.....	1
2. Virtualization Security Challenges	2
3. Current Virtualization Security Approaches	4
4. Security Watchdog VM.....	6
5. Third Brigade Coordinated Security Approach.....	8
6. Conclusion	14
About Third Brigade®	15

1. Introduction

Virtualization allows organizations to achieve significant savings in their data centers through reduced energy and hardware costs. Green IT and consolidation of hardware resources was the initial driver for virtualization deployments; however, the benefits achieved by virtualization are fundamentally affecting how mission-critical applications are being designed, deployed and managed. Virtualization is also causing organizations to consider which security mechanisms can best meet the security requirements of both physical and virtual servers.

This paper explores the challenges of protecting, and the opportunities for improving the security of, virtualized environments. It outlines a Coordinated Approach for Intrusion Detection and Prevention which can be deployed today, and that is architected to take advantage of additional capabilities which virtualization vendors are adding to their platforms—such as through the recently announced VMware® VMsafe™ APIs¹. This approach provides the necessary level of security for mission-critical applications in virtualized environments.

¹ <http://www.vmware.com/overview/security/vmsafe.html>

2. Virtualization Security Challenges

Virtualized environments use the same operating systems, enterprise and web applications as physical environments. The ability for malware to remotely exploit vulnerabilities in these systems and applications is the primary threat to virtualized environments [Figure 1, a]. There are also vulnerabilities which can be exploited in the service console and hypervisor [Figure 1, b & c].

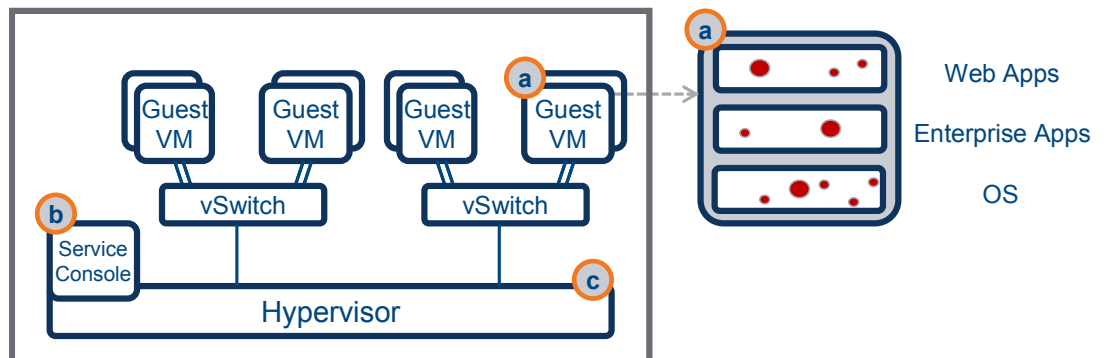


Figure 1 – Virtualization Vulnerabilities

Virtualization vendors continue to work to simplify the service console, as seen with VMware ESXi², and as such reduce its potential attack surface. Most hypervisor vulnerabilities will not be remotely exploitable, since the hypervisor does not have services which terminate remote protocols. Hypervisor vulnerabilities will typically be exploited from malware which compromises a virtual machine (VM). One of the best methods to protect against attacks to hypervisor vulnerabilities is to prevent malware from getting installed in the virtual environment in the first place.

The dynamic nature of virtualized environments presents new challenges for intrusion detection/prevention systems (IDS/IPS). Because virtual machines can quickly be reverted to previous instances, and easily moved between physical servers, it is difficult to achieve and maintain consistent security.

² <http://www.vmware.com/vmworldnews/esx.html>

When deciding on an approach to virtualization security, organizations should be guided by the same security principles that have evolved to protect their physical environments. One of these principles is “defense-in-depth”, which is a fundamental security requirement for organizations that recognize the “de-perimeterization” that has emerged in their information technology deployments. Defense-in-depth is supported by industry best practice, and organizations such as the Jericho Forum³ include it as part of their security recommendations. For example, the first fundamental of the Jericho Forum commandments is:

1. The scope and level of protection should be specific and appropriate to the asset at risk
 - Business demands that security enables business agility and is cost effective
 - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
 - In general, it’s easier to protect an asset the closer protection is provided

Virtualization has made the challenge of de-perimeterization even more apparent. The inability of appliance-based security to deal with attacks between virtual machines on the same server highlights the need for mechanisms to be deployed directly on the server to protect these environments. A requirement has emerged for an approach to virtualization security that allows protection to occur as close as possible to the asset itself.

³ <http://www.jerichoforum.org/>

3. Current Virtualization Security Approaches

There are two approaches currently being taken with security software to protect virtual machines. One approach is to apply a virtual security appliance within the virtualized environment. These virtual security appliances monitor the traffic flow between a virtual switch (vSwitch) and one or more guest VMs [Figure 2].

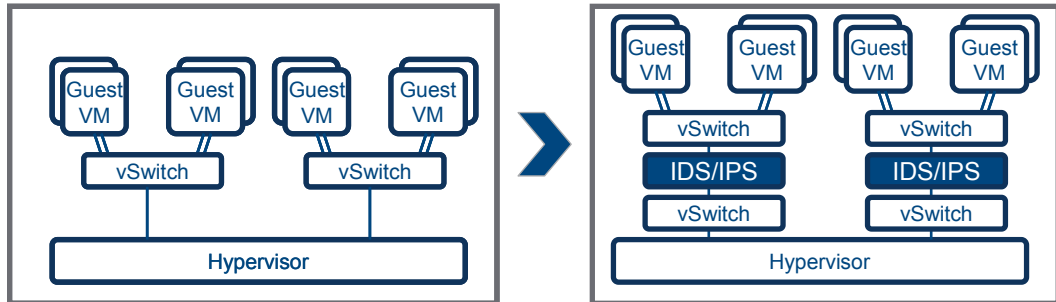


Figure 2: Virtual security appliance approach to IDS/IPS

Although these virtual security appliance solutions provide IDS/IPS protection for attacks which are coming from the network, they have significant limitations:

- **Inter-VM traffic:** The virtual security appliance must be placed in front of a virtual switch and therefore cannot prevent attacks between virtual machines on the same virtual switch.
- **Mobility:** When a virtual machine is moved from one server to another, using controls like VMware® Storage Vmotion™, the security context is lost. Clustering of the virtual security appliances must be configured for all potential destinations to which a virtual machine could be moved. This will have a corresponding negative impact on performance.
- **Non-transparent:** The virtual network architecture must be altered to deploy virtual security appliances. This will have adverse administrative and performance impacts on the existing system.
- **Performance bottleneck.** All traffic sent between virtual machines and the network must be processed by the virtual security appliance. This centralized processing can be a performance bottleneck.

In contrast, the same IDS/IPS functionality can be deployed on each virtual machine [Figure 3]. This VM-centric approach does not have the same inter-VM traffic, mobility and non-transparent limitations of the virtual security appliance approach. Although the VM-centric approach also has a performance impact on the system, it is distributed across the virtual machines.

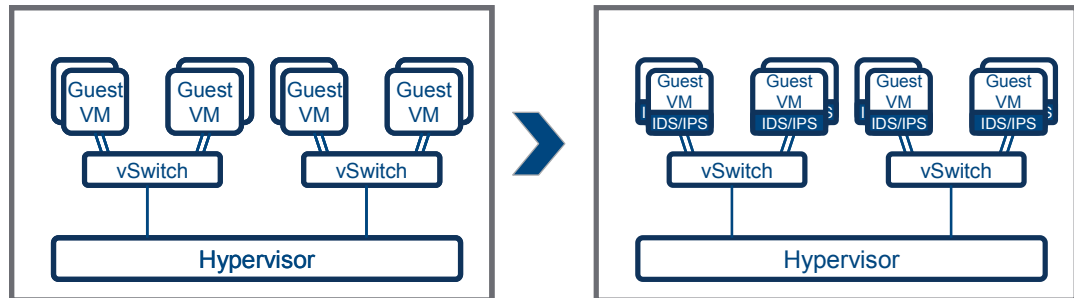


Figure 3: VM-centric IDS/IPS

In the VM-centric approach, there still exists the challenge of deploying an IDS/IPS security agent on each virtual machine. Use of mechanisms such as templates⁴ eases the ability to deploy a common security agent across each virtual machine. However, the dynamic nature of virtualized environments can still result in virtual machines being introduced to the production environment without a security agent in place.

⁴ Working with Templates:
<http://www.vmware.com/support/vc13/doc/c13templateintro.html>.

4. Security Watchdog VM

The VMware VMsafe program allows dedicated security VMs to be deployed that will have privileged access to hypervisor APIs. This allows the creation of a unique security control, a security watchdog VM⁵, as a new means of implementing security controls within a virtual environment [Figure 4]. Through the use of introspection APIs, security watchdog functions can access privileged state information about each virtual machine, including the memory, state and network traffic. Therefore, for IDS/IPS filtering, the inter-VM and non-transparent limitations of the virtual security appliance approach are removed, since all network traffic within the server can be seen without any change to virtual network configuration. There will still be mobility and performance impacts which need to be considered when performing IDS/IPS filtering in security watchdog VMs.

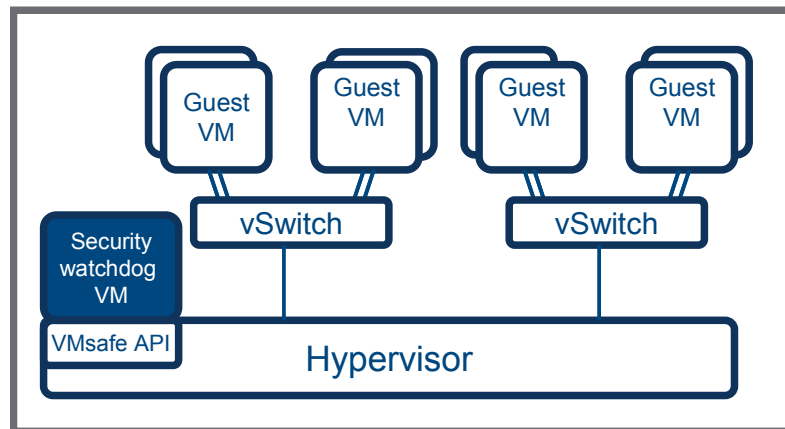


Figure 4: Security Watchdog VM

As indicated by the list of vendors that have joined the VMware VMsafe program, a range of security functions including antivirus, encryption, firewall, IDS/IPS and system integrity all have the potential to be applied in security watchdog VMs. It can be expected that virtual security appliances will be redeveloped to use these

⁵ Source: Gartner, "Radically Transforming Security and Management in a Virtualized World: Concepts", Neil MacDonald, March 14, 2008

APIs. VM-centric agent technologies will also be altered to execute in security watchdog VMs.

However, there will still be a requirement for flexibility to deploy some functionality within a security watchdog VM and some using VM-centric agents, because:

- Certain security functionality can only be achieved by VM-centric agents (for example, dealing with encrypted traffic or accessing certain real-time state information).
- Performance tradeoffs exist between implementing via security watchdog VM or via VM-centric agent.
- The introspection APIs will be developed in stages and starting with a VM-centric approach delivers security during the transition as security watchdog VM functionality emerges.

As a result, a coordinated approach is needed: one that provides the benefits of both a VM-centric approach and takes advantage of introspection APIs to provide intelligent choices that eliminate bottlenecks, redundant controls and cost effectively reduce security risk.

5. Third Brigade Coordinated Security Approach

Third Brigade's coordinated approach to protecting virtualized environments consists of a VM-centric agent that can be deployed on individual virtual machines, as well as a security watchdog VM deployed to protect multiple virtual machines. This architecture ensures that critical assets (virtual machines) can be protected by deploying software on the asset itself, whereas non critical assets are protected by the security watchdog VM [Figure 5].

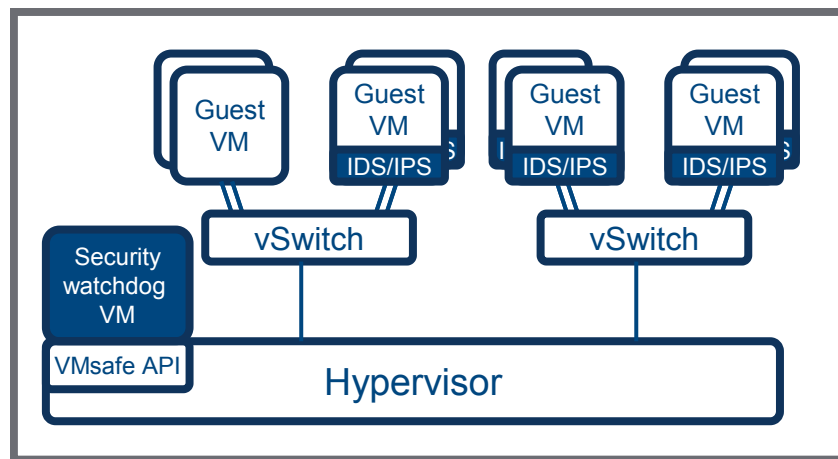


Figure 5: Coordinated IDS/IPS Approach

Five aspects of the coordinated approach are outlined below:

- Intrusion Detection and Prevention Processing
- Virtualization Management Integration
- Enterprise Management
- Comprehensive IDS/IPS functionality
- Multiple virtualization architectures
- Software Licensing Models

Intrusion Detection and Prevention Coordination

Figure 6 outlines the coordination which exists between the security watchdog VM and the VM-centric agent. The coordination sequence is as follows:

1. When a virtual machine is started, the security watchdog VM is notified.
2. If the security watchdog VM detects that a security agent is deployed on the guest VM (or should have been deployed), then it ensures that the correct software version and security configuration has been deployed and updates the configuration as necessary.
3. The guest VM is now up to date with its protection mechanisms and the guest VM is allowed to communicate on the network, with traffic being sent directly from hypervisor to virtual machine.

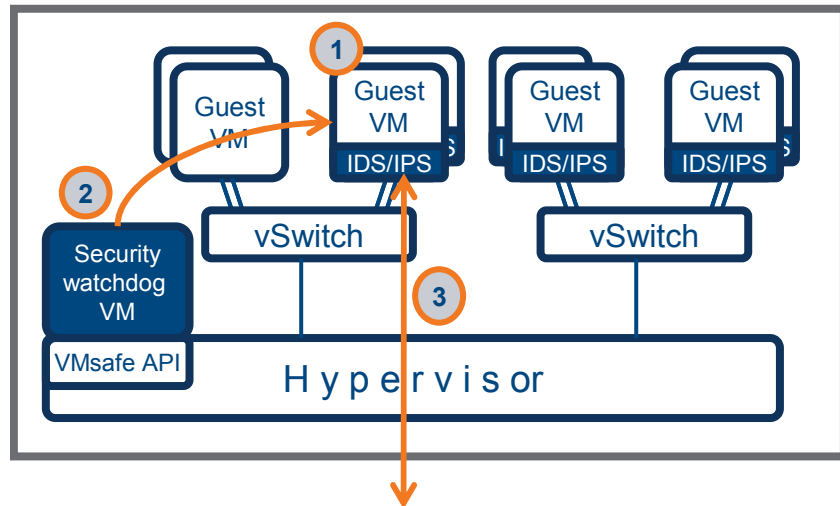


Figure 6: Guest VM has security

As described earlier, not all virtual machines will necessarily have a security agent installed. Figure 7 outlines the coordination which exists when a guest VM is deployed that does not require an agent:

1. When a guest VM is started, the security watchdog VM is notified.
2. The guest VM does not require an agent, the security watchdog VM scans the guest configuration and applies appropriate IDS/IPS filtering within the security watchdog VM.

3. Data flows through the security watchdog VM via VMsafe APIs and IDS/IPS filtering is applied.

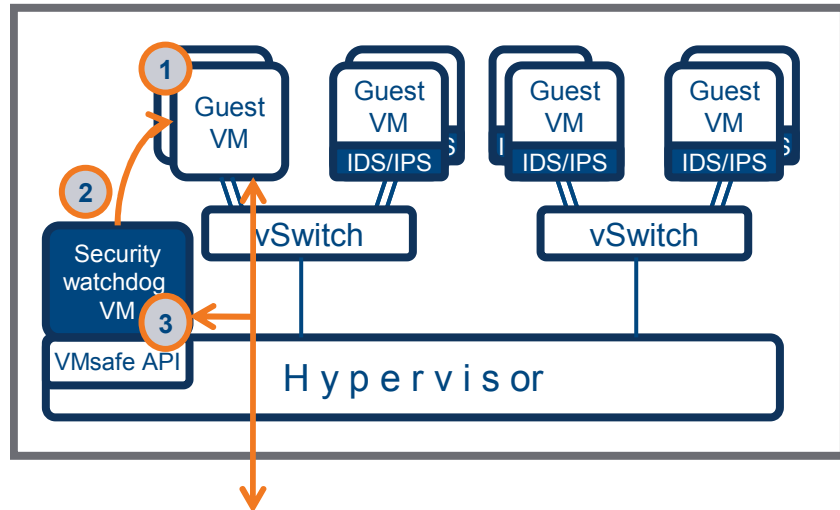


Figure 7: Guest VM without agent

The advantage of this architecture is that traffic destined for virtual machines which have an IDS/IPS security agent deployed will not incur any significant delay, since traffic is being routed directly from hypervisor to the guest VM. Traffic for the remaining virtual machines which do not have an agent can be processed by the security watchdog VM, and the impact that this central processing has can be minimized.

Virtualization Management Integration

Virtualization platforms typically have a method of managing the deployment of physical hosts and virtual machines from a centralized management system (for example, VMware® VirtualCenter™). The security management of the IDS/IPS system connects to the virtualization management platform to obtain the configuration of hosts and virtual machines [Figure 8]. The layout of systems can then be displayed within the IDS/IPS security manager in a similar structure to allow physical host and virtual machines to be managed easily and effectively [Figure 9].

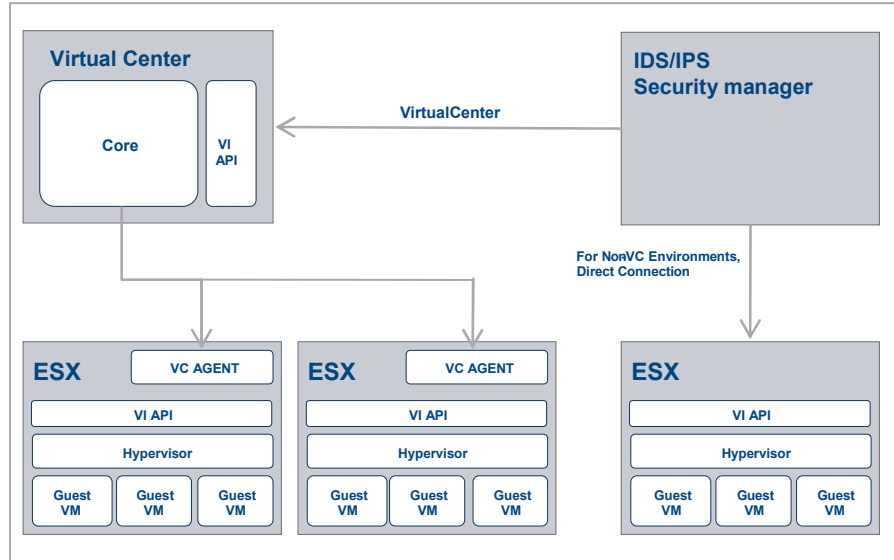


Figure 8 Virtualization Management Integration

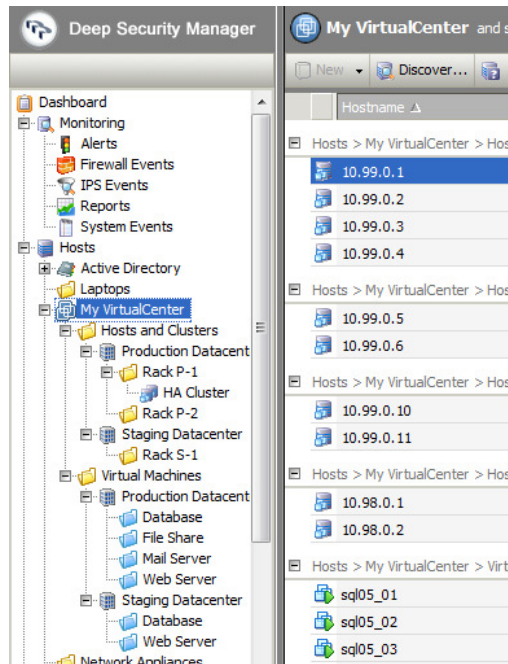


Figure 9 Hosts and Virtual Machines

Enterprise Management

Any enterprise-class IDS/IPS system has centralized security management which defines and distributes policy to the IDS/IPS enforcement components and collects events for the actions the enforcement components have taken (i.e. attacks detected or prevented). In addition to the virtualization management integration described above, some key elements for centralized security management of the distributed IDS/IPS system include:

- Management scalability. The management component itself should be able to be virtualized into multiple virtual machines to allow scalable deployments and high availability of the management infrastructure.
- Integration points such as syslog and web services so IDS/IPS can be integrated into other enterprise security elements such as Security Information and Event Management (SIEM) systems.
- Supporting security capabilities such as role-based access control, audit history of administrator actions.
- Third-party evaluations such as Common Criteria⁶ assist in ensuring a specific set of security properties has been achieved.

Complete IDS/IPS Functionality

Although this paper has focused on network traffic analysis because it is the method common to both virtual security appliances and VM-centric agents, the NIST Guide to Intrusion Detection and Prevention Systems⁷ defines host-based intrusion detection and prevention as:

- Code Analysis
- Network Traffic Analysis (deep packet inspection and application protocol inspection)
- Network Traffic Filtering (firewall)
- Filesystem Monitoring

⁶ Common Criteria for Information Technology Security Evaluation, www.commoncriteriaportal.org

⁷ NIST Guide to Intrusion Detection and Prevention Systems, <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

- Log Analysis
- Network Configuration Monitoring

Each of these areas of functionality also require coordination between VM-centric agents and security watchdog VMs to ensure consistent security is achieved.

Multiple Virtualization Platforms

Although VMware is the market leader in virtualization, Microsoft® Windows® Server Virtualization, Citrix® XenServer™, and many other vendors are developing virtualization platforms. Although the depth of functionality which a security watchdog VM will be able to accomplish on each of these platforms will vary, the coordination approach for IDS/IPS is one which can be applied to each of the virtualization platforms.

Software Licensing Models

An area that is getting increasing attention with the transition to virtualized environments is software licensing. In the same way that virtualization has revolutionized hardware utilization within the enterprise; it is also having a significant impact on software utilization. Organizations expect licensing that increases software utilization, by offering appropriate choices while not inflating software costs.

Flexible licensing options are required that fit well in both physical and virtual environments and are “future proof” as customers adopt the coordinated approach to IDS/IPS. This includes the ability to license IDS/IPS agents per virtual machine, as well as the ability to license IDS/IPS functionality for an unlimited number of virtual machines on a physical server. License management mechanisms should ensure that organizations can track license use in a dynamic virtualized environment without adding complexity.

6. Conclusion

Virtualization environments share many of the same security challenges faced by physical server environments. The investment organizations have made in multi-processor, multi-core architectures and virtualization software can also be leveraged to provide the security mechanisms required to protect them. Virtualization deployments can be protected today and enhanced as introspection capabilities emerge in the virtualization platforms. A coordinated approach with security software that can be deployed today as a VM-centric agent and later combined with a security watchdog VM when introspection APIs are available, ensures a baseline of security for all virtual machines without introducing bottlenecks or redundant controls. This approach will enable organizations to expand their virtualization deployments to cover all of their mission critical systems.

About Third Brigade®

Third Brigade (www.thirdbrigade.com) best-of-breed host intrusion defense systems protect critical data and applications, including those on virtual machines, from attacks that bypass or penetrate network defenses, and target vulnerabilities in operating systems, and enterprise and web applications. With a high performance deep packet inspection engine, Third Brigade Deep Security detects and prevents known and zero-day attacks, and provides a virtual patch for Microsoft® Windows®, Solaris™, Linux, and other Unix® hosts on physical and virtualized systems. It helps ensure regulatory compliance with PCI and other standards, and prevents costly business disruptions. Unlike others, Third Brigade provides broader, faster and simpler protection. Third Brigade. That's control.

For more information, or to schedule your personalized demo, please visit www.thirdbrigade.com. Contact us today to discuss your virtualization security.

Corporate Headquarters

40 Hines Road
Suite 200
Ottawa, Ontario, Canada
K2K 2M5
Toll free: +1.866.684.7332
Local: +1.613.599.4505
Fax: +1.613.599.8191

United States Headquarters

11710 Plaza America Drive
Suite 2000
Reston, Virginia, USA
20190
Toll free: +1.866.684.7332
Local: +1.703.903.4479
Fax: +1.613.599.8191

European Headquarters

Fetcham Park House
Lower Road, Fetcham,
Surrey, KT22 9HD
United Kingdom
Tel: +44 1372 371210
Fax: +44 1372 371211

"Third Brigade", "Deep Security Solutions", and the Third Brigade logo are trademarks of Third Brigade, Inc. and may be registered in certain jurisdictions. All other company and product names are trademarks or registered trademarks of their respective owners. © 2008 Third Brigade. All rights reserved.