

PROTECTING  
DYNAMIC DATACENTERS  
FROM THE LATEST THREATS

THIRD BRIGADE DEEP SECURITY  
PRODUCT WHITE PAPER



## Overview

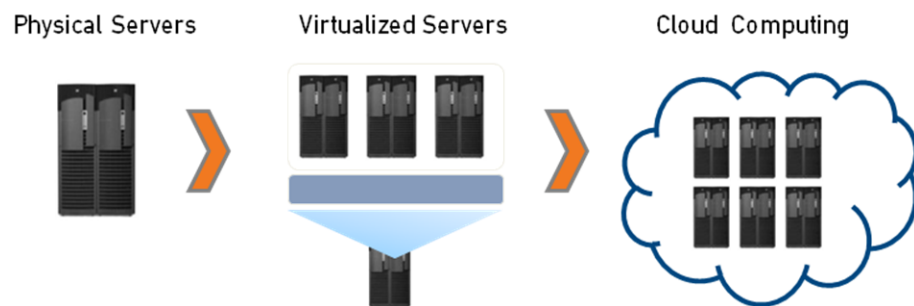
Third Brigade Deep Security is comprehensive server and application protection software that unifies security across virtual, cloud computing and traditional datacenter environments. It helps organizations to prevent data breaches and business disruptions, enable compliance with key regulations and standards including PCI, and support operational cost reductions that are necessary in the current economic climate. This product whitepaper looks at the security and compliance challenges facing dynamic datacenters and details the comprehensive, manageable protection offered through Third Brigade Deep Security. It describes product modules, functionality and architecture, as well as deployment and integration capabilities. Sample use cases and practical considerations are also included.

### TABLE OF CONTENTS

OVERVIEW .....	1
TABLE OF CONTENTS .....	1
1. THE DYNAMIC DATACENTER.....	2
2. PRODUCT OVERVIEW .....	5
3. COMPREHENSIVE, MANAGEABLE PROTECTION .....	5
4. BENEFITS .....	6
5. MODULES & FUNCTIONALITY .....	7
6. PRODUCT ARCHITECTURE .....	11
7. DEPLOYMENT AND INTEGRATION .....	16
8. THE THIRD BRIGADE DIFFERENCE .....	16
9. GET STARTED TODAY .....	17
ABOUT THIRD BRIGADE® .....	18

## 1. The Dynamic Datacenter

IT security must enable your business, not impede it. Compliance requirements are imposing security standards for data and applications on servers. Physical servers are being replaced with virtual machines to save money, be green and increase scalability. Cloud computing is evolving the traditional IT infrastructure to increase cost savings, at the same time as offering more flexibility, capacity and choice. Servers are no longer barricaded behind perimeter defenses. Like laptops before them, servers are moving outside the security perimeter and they now need a last line of defense. A server and application protection system, that delivers comprehensive security controls and that supports current and future IT environments, is now vital to your defense-in-depth security strategy.



### 1.1 Servers Are Under Pressure

According to the 2008 Data Breach Investigations Report summarizing research conducted by Verizon Business Risk Team, 59% of data breaches resulted from hacking and intrusions. TJX and Hannaford breaches brought to the forefront the potential for system compromise to have significant negative impact on the reputation and operations of any business. Organizations are continuing to struggle to balance the need to protect their resources with the need to extend access to those same resources to more business partners and customers.

The Payment Card Industry Data Security Standards (PCI DSS) recognize that traditional perimeter defenses are no longer sufficient to protect from the latest threats, and as such requires multiple layers of protection beyond appliance-based firewall and intrusion detection and prevention systems (IDS/IPS), Wireless networks, encrypted attacks, mobile resources and vulnerable web applications are contributing to the weakness of the porous perimeter that exposes enterprise servers to penetration and compromise.

Within the past five years, datacenter computing platforms, which were largely based on physical servers, have undergone a major technology change. The traditional datacenter footprint is shrinking to enable cost savings and “greener” IT through server consolidation. Nearly all organizations have some (and some organizations have all) of their datacenter workloads virtualized, enabling multi-tenant uses of what used to be single-tenant or single-purpose physical servers. Between 2007 and 2011, Gartner Group expects that the installed base of virtual machines will grow more than tenfold, and by 2012, it is expected that the majority of x86 server workloads will be running within a virtual machine.

## 1.2 Servers Are Multiplying Rapidly and In Motion

Increases in virtualization are due to the significant benefits it is offering IT organizations. Increased responsiveness to corporate demands, increased capacity and more efficient use of hardware and software licenses result in continued consolidation of server workloads.

In virtual environments, there is a loss of the strict separation that exists between network devices and servers—these are now being combined within virtualization platforms. Hosting workloads of different sensitivities, with network security appliances being blind to traffic sent between virtual machines, opens up the opportunity for attacks. Motion tools, critical for managing planned downtime, effective use of virtualization resources, and application availability, result in additional workload sharing on the same server, challenging the management of compliance history, and cause loss of security state by virtual security appliances. In addition, the inevitable “sprawl” of virtual machines makes it more likely that virtual machines, without the latest patches, can be exposed to malicious traffic. IT organizations need to closely examine methods used to protect virtual instances of enterprise servers.

“Enterprises oftentimes find themselves deploying several small physical ESX clusters in order to meet security zoning requirements. Host-based security deployed to VM guest operating systems can allow organizations to move enterprise security to the virtual infrastructure, which may allow them to realize higher consolidation densities and more efficient utilization of shared infrastructure.”

Chris Wolf  
Senior Analyst, Burton Group

### 1,3 Servers Open In The Cloud

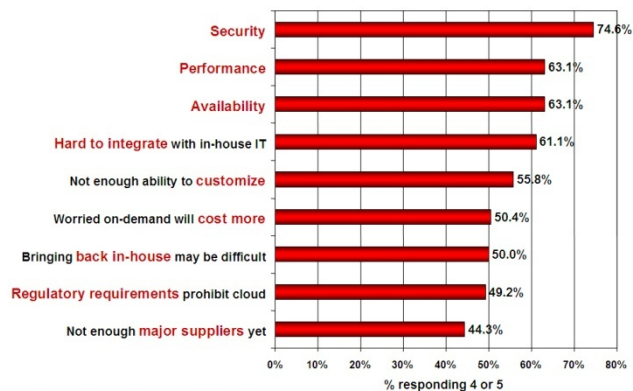
As organizations consider extending their IT environments to take advantage of cloud computing, and as the service providers building public clouds consider how to host these virtualized workloads most effectively, the security model gets challenged even further. The datacenter perimeter is providing no protection when a server is moved to public cloud resources. Administrative access to these virtualized servers is now directly over the internet. Challenges that are already faced in the datacenter such as patch management and compliance reporting become more complex. In the cloud, the only protection relevant is the lowest common denominator that the cloud computing vendor can provide on their perimeter, or what an organization is able to equip the virtual machine with to defend itself, as it is hosted on servers with server workloads from other organizations.

Cloud computing, most simply, extends an enterprise’s ability to meet the computing demands of its everyday operations. However, the area that is causing organizations to hesitate most when it comes to moving business workloads into public clouds is security. IDC recently conducted a survey of 244 IT executives/CIOs and their line-of-business (LOB) colleagues to gauge their opinions and understand their companies’ use of IT Cloud Services. Security ranked first as the greatest challenge or issue attributed to cloud computing.

“By far, the number one concern about cloud services is security. With their businesses’ information and critical IT resources outside the firewall, customers worry about their vulnerability to attack.”

Frank Gens  
Senior Vice President and  
Chief Analyst, IDC

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model  
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

## 2. Product Overview

Third Brigade Deep Security is server and application protection software that allows systems to become self-defending. It is optimized to help protect your confidential data and ensure application availability in these dynamic conditions impacting your datacenter, Deep Security provides comprehensive protection, deployed on physical servers and virtual machines, including:

- deep packet inspection enabling:
  - intrusion detection and prevention (IDS/IPS)
  - web application protection
  - application control
- stateful firewall
- file and system integrity monitoring
- log inspection

## 3. Comprehensive, Manageable Protection

Third Brigade Deep Security helps prevent data breaches and business disruptions, and enables compliance and cost reduction. This table highlights key server and application protection requirements and identifies how the different modules can be used to address them.

◆ = Essential    ◇ = Advantageous

Datacenter Requirement	Deep Security Modules					
	Deep Packet Inspection			Firewall	Integrity Monitoring	Log Inspection
	IDS / IPS	Web Application Protection	Application Control			
<b>Server Protection</b> - Protection against known and zero-day attacks - Shield vulnerabilities until patching	◆			◆	◆	◇
<b>Web Application Protection</b> - Protection against Internet attacks such as SQL Injection, Cross-Site Scripting, and brute force attacks - Meets PCI DSS Req. 6.5 - Web Application Firewall	◆	◆			◇	◆

Datacenter Requirement	Deep Security Modules					
	Deep Packet Inspection			Firewall	Integrity Monitoring	Log Inspection
	IDS / IPS	Web Application Protection	Application Control			
<b>Virtualization Security</b> <ul style="list-style-type: none"> <li>- Protection against known and zero-day attacks</li> <li>- Shield vulnerabilities until patching</li> <li>- Virtual Center integration for enhanced visibility and simplified management</li> </ul>	◆	◇		◆	◆	◇
<b>Suspicious Behavior Detection</b> <ul style="list-style-type: none"> <li>- Protection against reconnaissance scans</li> <li>- Detection of allowed protocols over inappropriate ports</li> <li>- Alert on OS and application errors that could signal an attack</li> <li>- Alert on critical operating system and application changes</li> </ul>	◇		◆	◆	◆	◆
<b>Cloud Computing Security</b> <ul style="list-style-type: none"> <li>- Use firewall policies to isolate virtual machines</li> <li>- Protection against known and zero-day attacks</li> <li>- Shield vulnerabilities until patching</li> </ul>	◆	◇		◆	◆	◆
<b>Compliance Reporting</b> <ul style="list-style-type: none"> <li>- Visibility and audit trail of all changes to critical servers</li> <li>- Inspection, correlation, and forwarding of important security events to Logging servers for remediation, reporting, and archival</li> <li>- Reports on security configurations, malicious activity detected and prevented</li> </ul>	◇	◆	◇	◇	◆	◆

## 4. Benefits

Today, datacenter server security architectures must address dynamic conditions including virtualization and consolidation, new service delivery models, or cloud computing. Third Brigade Deep Security helps to:

- Prevent data breaches and business disruptions.
- Enable compliance.
- Support operational cost reductions.

**Prevent data breaches and business disruptions by:**

- Providing a line of defense at the server itself whether physical, virtual or cloud.

- Shielding known and unknown vulnerabilities in web and enterprise applications, as well as operating systems, and blocking attacks to these systems.
- Allowing you to identify suspicious activity and behavior, and take proactive or preventive measures.

**Enable compliance by:**

- Addressing six major PCI compliance requirements—including web application security, file integrity monitoring and server log collection—along with a wide range of other compliance requirements.
- Providing detailed, auditable reports that document prevented attacks, policy compliance status, and reducing the preparation time required to support audits.

**Support operational cost reductions by:**

- Providing vulnerability protection so that secure coding efforts can be prioritized, and unscheduled patching can be implemented more cost-effectively.
- Providing the security necessary to allow organizations to fully leverage virtualization or cloud computing, and realize the cost-savings inherent in these approaches.
- Delivers comprehensive protection in a single, centrally managed software agent, thus eliminating the need for, and costs associated with, deploying multiple software clients.

## 5. Modules & Functionality

Third Brigade Deep Security is a software solution that allows you to enable one or more protection modules to deploy the right amount of protection to meet your dynamic requirements. You can create self-defending servers and virtual machines by deploying comprehensive protection, or choose to start with the Integrity Monitoring module to uncover suspicious behavior. All modular functionality is deployed to the server or virtual machine by a single Deep Security Agent which is centrally managed—unified across physical, virtual and cloud computing environments—by the Deep Security Manager software.

### 5.1 DEEP PACKET INSPECTION (DPI)

The high-performance deep packet inspection engine examines all incoming and outgoing traffic, including SSL traffic, for protocol deviations, content that signals an attack, or policy violations. It can operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities. It protects web applications from application-layer attacks including SQL injection and cross-site scripting. Detailed events provide valuable information,

*Enabling Intrusion Detection and Prevention, Web Application Protection and Application Control*

including who attacked, when they attacked and what they attempted to exploit. Administrators can be automatically notified via alerts when an incident has occurred. Deep packet inspection is used for intrusion detection and prevention, web application protection, and application control.

**Intrusion Detection and Prevention (IDS/IPS):** Shields vulnerabilities in operating systems and enterprise applications until they can be patched, to achieve timely protection against known and zero-day attacks.

- **Vulnerability rules** shield a known vulnerability—for example those disclosed on Microsoft-Tuesday—from an unlimited number of exploits. Third Brigade Deep Security includes out-of-the-box vulnerability protection for over 100 applications, including database, web, email and FTP servers. Rules that shield newly discovered vulnerabilities are automatically delivered within hours, and

#### Web Application Security

Smart rules are used to identify and block common web application attacks. A SaaS datacenter deploying Deep Security was able to shield 99% of all “High Severity” vulnerabilities that were discovered in its web applications and web servers through a customer-requested penetration test.

Third Brigade is an inaugural member of the **Microsoft Active Protections Program (MAPP)**. As part of MAPP, Third Brigade receives vulnerability information from Microsoft in advance of their monthly security bulletins. This advance notice makes it possible to anticipate emerging threats and provide mutual customers with more timely protections effectively and efficiently via Third Brigade Security Updates.

can be pushed out to thousands of servers in minutes, without a system reboot.

- **Smart rules** provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code.
- **Exploit rules** stop known attacks and malware, and are similar to traditional anti-virus signatures in that they use signatures to identify and block individual, known exploits.

**Web Application Protection:** Third Brigade Deep Security enables compliance with PCI Requirement 6.6 for the protection of web applications and the data that they process. Web application protection rules defend against SQL injections attacks, cross-site scripting attacks and other web application vulnerabilities, and shield these vulnerabilities until code fixes can be completed.

**Application Control:** Application control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules can also be used to identify malicious software accessing the network, or to reduce the vulnerability exposure of your servers.

## 5.2 FIREWALL

The Third Brigade Deep Security Firewall software module is enterprise-grade, bi-directional, and stateful. It can be used to allow communications over ports and protocols necessary for correct server operation and block all other ports and protocols reducing the risk against unauthorized access to the server.

*Decreasing the attack surface of your physical and virtual servers.*

- **Virtual machine isolation:** Allows VMs to be isolated in cloud computing or multi-tenant virtual environments, providing virtual segmentation without the need to modify virtual switch configurations.
- **Fine-grained filtering:** Firewall rules can filter traffic on: IP addresses, Mac addresses, Ports, Different policies for each network interface can be configured.
- **Coverage of all IP-based protocols:** Support for full packet capturing simplifies troubleshooting and provides valuable insight into understanding raised firewall events. (TCP, UDP, ICMP,...)
- **Reconnaissance Detection:** Detect reconnaissance activities such as port scan. Non-IP traffic such as ARP traffic can also be restricted.
- **Flexible control:** The stateful firewall is flexible, allowing complete bypass of inspection, when appropriate, in a controlled manner. It addresses ambiguous traffic characteristics that can be encountered on any network, due to normal conditions, or as part of an attack.
- **Pre-defined firewall profiles:** Group common enterprise server types (Web, LDAP, DHCP, FTP, Database, etc.) ensuring rapid, easy, consistent deployment of firewall policy, even in large, complex networks.
- **Actionable reporting:** With detailed logging, alerting, dashboards, and flexible reporting, Deep Security Firewall configuration changes (such as what policy changes have been made and who made the changes) is captured and tracked providing a detailed audit trail.

## 5.3 INTEGRITY MONITORING

The Third Brigade Deep Security Integrity Monitoring module monitors critical operating system files and critical application files (files, directories, registry keys and values, etc.), to detect suspicious behavior.

*Monitoring unauthorized, unexpected or suspicious changes.*

- **On-demand or scheduled detection:** Integrity scans can be scheduled, or performed on-demand.
- **Extensive file property checking:** File and directories can be monitored for changes to: contents, attributes (owners, permissions, size, etc), time and date stamp using out-of-the-box Integrity rules. Additions, modification or deletions of Windows registry keys and values, Access Control Lists and log files may also be monitored and alerted. This capability is applicable to the PCI DSS 10.5.5 requirement.
- **Auditable reporting:** The Integrity Monitoring module can display Integrity events within the Deep Security Manager dashboard, generate alerts, and provide auditable reports. It is also able to forward events to a SIEM via Syslog.
- **Security Profile Groupings:** Integrity Monitoring rules can be configured for groups or individual servers to simplify deployment and management of monitoring rulesets.
- **Baseline setting:** Baseline security profiles may be established and used to compare for changes to initiate alerts and determine appropriate actions.
- **Flexible, practical monitoring:** The Integrity Monitoring module offers flexibility and control to optimize the monitoring activities for your unique environment. This includes the ability to include/exclude files or wildcard filenames and include/exclude sub-directories in scan parameters. It also gives the flexibility to create custom rules for unique requirements.

## 5.4 LOG INSPECTION

The Third Brigade Deep Security Log Inspection module provides the ability to collect and analyze operating system and application logs for security events. Log Inspection rules optimize the identification of important security events buried in multiple log entries. These events are forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. The Deep Security Agent will also forward the event information to the Deep Security Manager.

*Finding and learning from important security events buried in log files.*

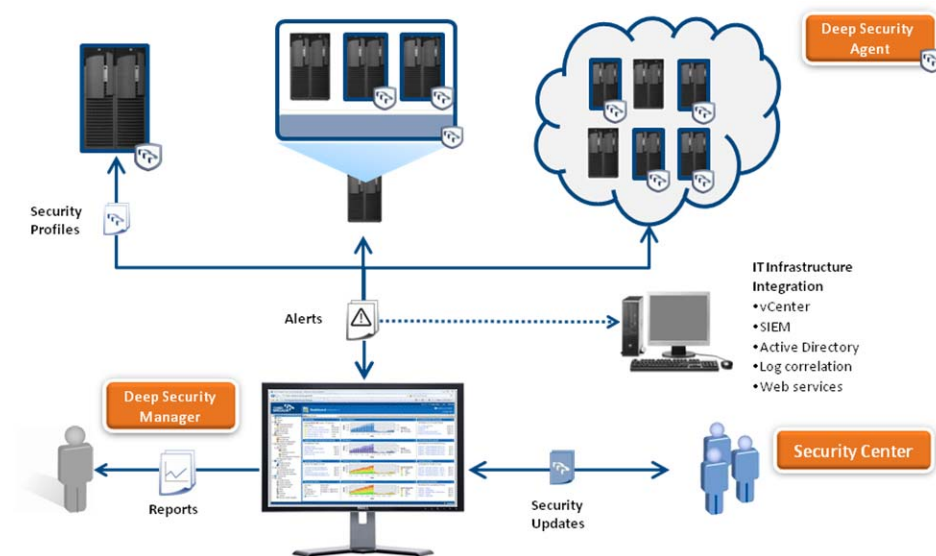
- **Suspicious behavior detection:** Log Inspection provides visibility into suspicious behavior that may be occurring on your servers.
- **Collecting events across your environment:** The Deep Security Log Inspection module is able to collect and correlate: events across Microsoft Windows, Linux and Solaris platforms; application events from Web servers, mail servers, SSHD, Samba, Microsoft

FTP, etc.; and custom applications log events.

- **Correlate different events:** Collect and correlate diverse warnings, errors and informational events including system messages (disk full, communication errors, services events, shutdown, system updates, etc.), application events (account login/logout/failures/lockout, application errors, communication errors, etc.) and administrative actions (administrative login/logout/failure/lockout, policy changes, account changes, etc.).
- **Auditable reporting for compliance:** A complete audit trail of security events can be created which assists with meeting compliance requirements such as PCI requirement 10.6.

## 6. Product Architecture

There are three components in the Third Brigade product architecture, (1) Deep Security Agent which is deployed on the server or virtual machine being protected, (2) Deep Security Manager which provides centralized policy management, distribution of security updates and monitoring through alerts and reports, and (3) Security Center, our hosted portal where our vulnerability research team develops rule updates for emerging threats and these updates are periodically pulled by the Deep Security Manager. The Deep Security product architecture is shown in the figure below.



### 6.1 How it works

The Deep Security Agent receives a security configuration, typically a Security Profile, from the

Deep Security Manager. This security configuration contains the deep packet inspection, firewall, integrity monitoring and log inspection rules which are enforced on the server. The rules to be assigned to a server can be determined simply by performing a Recommendation Scan, which scans the server for installed software and recommends the rules required to protect the server. Events are created for all rule monitoring activities, and these events are sent to the Deep Security Manager and optionally to a SIEM. All communication between Deep Security Agents and the Deep Security Manager is protected by mutually authenticated SSL.

The Deep Security Manager initiates polling of the Security Center to identify if a new Security Update is available. When a new update is available, it is retrieved by the Deep Security Manager and either manually or automatically applied to the servers which required the additional protection provided by this update. Communication between the Deep Security Manager and Security Center is also protected by mutually authenticated SSL.

Additionally, the Deep Security Manager connects to other elements of the IT infrastructure to simplify management. The Deep Security Manager can connect to VMware vCenter and also to directories such as Microsoft Active Directory to obtain server configuration and grouping information. The Deep Security Manager also has a web services API which can be used to access functionality programmatically.

The Security Center monitors both public and private sources of vulnerability information in order to protect the operating systems and applications in use by customers.

The following sections provide further information about each of the components of Deep Security.

## 6.2 Deep Security Manager

Third Brigade Deep Security provides practical, proven controls that address difficult security problems. Operational and actionable security is about providing your organization with knowledge—not just information—about a security event. In many cases, this is about providing the “who, what, when and where” so that events can be properly understood and subsequent actions, outside of what is performed by the security control itself, can be taken. The Third Brigade Deep Security Manager software addresses both security and operational requirements.

- **Centralized, web-based management system:** Create and manage security policies, and track threats and preventive actions taken in response to them, from a familiar, explorer-style UI.
- **Detailed reporting:** A wide selection of detailed reports document attempted attacks,

and provide an auditable history of security configurations and changes.

- **Recommendation scan:** Identifies applications running on servers and virtual machines and recommends which filters should be applied to these systems, ensuring the correct protection, with minimal effort.
- **Risk ranking:** Security events can be viewed based on asset value as well as vulnerability information.
- **Role-based access:** Allows multiple administrators, each with different levels of permission, to operate different aspects of the system and receive information appropriate to them.
- **Customizable dashboard:** Allows administrators to navigate and drill down to specific information, and monitor threats and preventive actions taken. Multiple, personalized views can be created and saved.
- **Scheduled tasks:** Routine tasks, such as reports, updates, backups and directory synchronization, can be scheduled for automatic completion.

### 6.3 Deep Security Agent

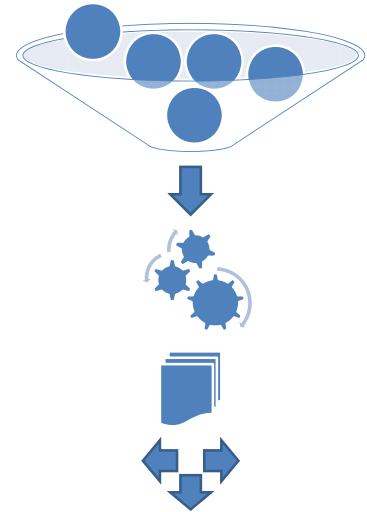
The Third Brigade Deep Security Agent is a server-based software component of the Deep Security solution. The Agent enables IDS/IPS, web application protection, application control, firewall, integrity monitoring and log inspection. It defends the server or virtual machine by monitoring incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations. When necessary, the Agent intervenes and neutralizes the threat by blocking the malicious traffic.

### 6.4 Security Center

The Security Center is an integral part of Third Brigade Deep Security. It consists of a dedicated team of security experts who help customers stay ahead of the latest threats by providing a timely and rapid response to a broad range of new vulnerabilities and threats as they are discovered, together with a customer portal for accessing security updates and information. Security Center experts apply a rigorous, six-step, rapid response process that is supported by sophisticated and automated tools.

**Six step rapid-response process:**

1. **Monitor:** Over 100 sources of public, private and government data are systematically and continuously monitored to identify and correlate new relevant threats and vulnerabilities. Third Brigade has leveraged relationships with different organizations to get early and sometimes prerelease information on vulnerabilities so that timely and accurate protection can be delivered to customers. These sources include Microsoft, Oracle and other vendor advisories, SANS, CERT, Bugtraq, VulnWatch, PacketStorm, and Securiteam.
2. **Prioritize:** The vulnerabilities are then prioritized for further analysis, based on an assessment of risk to customers along with Service Level Agreements.
3. **Analyze:** An in-depth analysis of the vulnerabilities is conducted to identify the necessary protection.
4. **Develop and Test:** Software filters that shield the vulnerabilities and rules that recommend filters are then developed and extensively tested to minimize false positives and ensure customers can deploy them quickly and smoothly.
5. **Deliver:** The new filters are delivered to customers as Security Updates. Customers receive immediate notice when a new Security update is released via an alert in Deep Security Manager. The updates can then be automatically or manually applied to the appropriate servers.
6. **Communicate:** Ongoing communication with customers is provided through Security Advisories, which provide detailed descriptions of the newly discovered security vulnerabilities.

**Proactive research further enhances protection**

In addition, the Security Center team conducts on-going research to improve overall protection mechanisms. This work is strongly influenced by results and trends uncovered during the vulnerability and threat response process. Additionally, these results impact both how new filters and rules are created, and the quality of existing protection mechanisms, which ultimately improves overall protection.

**Protecting a broad range of vulnerabilities**

The Security Center develops and delivers filters that protect commercial off-the-shelf applications, as well as custom web applications. Exploit and vulnerability filters are reactive, in

that they are used in response to the discovery of a known vulnerability. In contrast, Smart filters provide proactive protection. **Integrity Monitoring Filters** check various system components and their specific properties and alert the administrator when specific triggering conditions are met. Some components that can be monitored include system directories, files, Windows registry, user accounts, ports, and network shares. **Log Inspection Filters** parse logs from operating system and third-party applications, and alert the administrator when specific events have occurred.

## 6.5 Security Center Portal

The Security Center portal provides customers with a secure, single point of access to product-related information and support, including:

- Security Updates
- Security Advisories
- CVSS score information in vulnerabilities
- Alert summaries for Microsoft Tuesday
- Advanced search for vulnerabilities
- Full disclosure of vulnerabilities, including those not protected by Third Brigade
- Patch Information for each vulnerability
- RSS feeds
- Trouble tickets
- Software downloads
- Product documentation

The screenshot shows the Third Brigade Security Center portal. At the top left is the Third Brigade logo. The top right shows the user is signed in as 'ThirdBrigade' with links for 'User GUID' and 'Change Password'. Below the navigation bar, there's a main header area with a 'SECURITY CENTER' title and a 'Threat Level' indicator showing 'MEDIUM'. A welcome message states: 'Welcome to Third Brigade Security Center. Here you will find security updates, information on new and existing vulnerabilities, the latest Deep Security software, and access to online support.' Below this are three columns: 'LATEST SECURITY UPDATE' (June 24, 2008), 'LATEST VULNERABILITIES' (listing CVE-2008-2732, CVE-2008-1444, and CVE-2008-1412), and 'YOUR SUPPORT TICKETS' (listing tickets from June 9, 2008, to May 29, 2008).

## 7. Deployment and Integration

Deep Security is designed for rapid enterprise deployment. It leverages and integrates with existing infrastructure and investments to help achieve greater operational efficiency and support operational cost reductions.

- **VMware Integration:** Tight integration with VMware vCenter and ESX Server allows organizational and operational information from vCenter and ESX nodes to be imported into Deep Security Manager, and detailed security to be applied to an enterprise's VMware infrastructure.
- **SIEM integration:** Detailed, server-level security events are provided to Security Information and Event Management, including ArcSight, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic and other systems through multiple integration options.
- **Directory integration:** Integrates with enterprise directories, including Active Directory.
- **Configurable management communication:** The Manager or the Agent can initiate communication. This minimizes or eliminates firewall changes typically needed for centrally managed systems.
- **Software distribution:** Agent software can be easily deployed through standard software distribution mechanisms such as Microsoft SMS, Novel Zenworks, and Altiris.
- **Optimized filtering:** Advanced capabilities for dealing with streaming media such as IPTV (Internet Protocol Television) to help maximize performance.

## 8. The Third Brigade Difference

Third Brigade specializes in server and application protection that addresses the challenging operational security and compliance needs of today's dynamic datacenter. This focus ensures that we provide comprehensive protection, greater operational efficiency, superior platform support, tighter integration with existing investments, and are more responsive to customer requirements.

- **Comprehensive protection:** Third Brigade provides comprehensive protection—including stateful firewall, intrusion detection and prevention, application-layer firewalling, file and system integrity monitoring, and log inspection—in a single solution.
- **Greater operational efficiency:** The system can be deployed quickly and widely, and because it automates many key tasks including the recommendation of appropriate protection to be applied to each server, it can be managed more efficiently with minimal impact on existing IT resources.
- **Superior platform support:** Third Brigade provides full functionality across more platforms,

and supports current versions of these platforms more quickly. This enables you to continue to adopt the newest virtualization platforms and operating system releases, without sacrificing protection.

- **Tighter integration:** Third Brigade provides tighter integration with IT infrastructure, including directory and virtualization platforms, and other best-of-breed security investments such as SIEM. This ensures effective enterprise deployment, and continued vendor flexibility.

## 9. Get Started Today

To learn how Deep Security can address your datacenter security and compliance requirements, contact Third Brigade to schedule an in-depth product demo or free software trial. A detailed Product Evaluation Guide is available, including use case scenarios, to help structure your evaluation. [Request an evaluation today.](#)

### 9.1 Download Free Software

Third Brigade VM Protection is free-of-cost software that can be used to begin an evaluation of Third Brigade Deep Security. Providing a subset of the functionality of Deep Security—specifically Firewall, Intrusion Detection System (IDS), Integrity Monitoring and Log Inspection—it also includes a restricted subset of the full Deep Security protection rules. Third Brigade Deep Security enables seamless migration from [Third Brigade VM Protection](#), making VM Protection an excellent starting point for a Deep Security evaluation. [Download Third Brigade VM Protection.](#)

## About Third Brigade®

Third Brigade specializes in server and application protection for dynamic datacenters. Our advanced software and vulnerability response service allows virtual machines and physical servers to become self-defending; safe from the latest online threats. This comprehensive, proven protection helps customers prevent data breaches and business disruptions. It enables compliance, supports operational cost reductions and addresses the dynamic nature of datacenters, including virtualization and consolidation, new service delivery models, or cloud computing. Third Brigade also owns and maintains OSSEC, the Open Source Host Intrusion Detection Project actively used in 50 countries around the world. Third Brigade. That's control.

For more information, please visit [www.thirdbrigade.com](http://www.thirdbrigade.com), or contact us at:

### 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: +1.703.871.5264  
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 marks of their respective owners. © 2009 Third Brigade. All rights reserved.