

Do you want your business to go faster?

Third Brigade Deep Security is server and application protection software that allows systems to become self-defending, safe from the latest online threats. It provides comprehensive server security that is integral to datacenter modernization initiatives including virtualization and cloud computing.

BUSINESS VALUE

Optimized to help protect confidential data and ensure application availability in dynamic conditions, Third Brigade Deep Security helps:

Prevent data breaches and business disruptions by:

- Providing a line of defense at the server itself whether physical, virtualized or in the 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 preventive measures, before it's too late.

Enable compliance by:

- Addressing six major PCI compliance requirements—including file integrity monitoring, web application-layer firewall and network segmentation—along with a wide range of other compliance requirements.
- Providing detailed, auditable reports that document prevented attacks and policy compliance status, and better support an efficient audit process.



Support operational cost reductions by providing:

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

COMPREHENSIVE PROTECTION

Third Brigade Deep Security is a software solution that protects dynamic datacenters. Deployed on physical servers and virtual machines, Deep Security provides comprehensive, modular protection including:

- Intrusion detection and prevention (IDS/IPS)
- Web application protection
- Application control
- Firewall
- Integrity monitoring
- Log inspection

One or more protection modules are deployed to the server or virtual machine in a single Third Brigade Deep Security Agent. The Deep Security Agent is centrally managed—unified across physical and virtual environments— by the Deep Security Manager software.

Security updates to respond to the latest vulnerability threats and exploits are produced by the Third Brigade Security Center team of experts. These security updates can be delivered to the Deep Security Manager automatically, or on-demand, to achieve rapid and timely deployment to thousands of servers within minutes.

“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

COMPREHENSIVE PROTECTION

Third Brigade Deep Security provides comprehensive, modular protection—in a single solution—to address the security and compliance requirements of today's dynamic datacenter.

DEEP PACKET INSPECTION

A high-performance deep packet inspection engine examines all incoming and outgoing traffic, for protocol deviations, content that signals an attack, or policy violations. The deep packet inspection module 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®
 - Patch Tuesday—from an unlimited number of exploits.
- **Smart rules** provide zero-day protection from unknown exploits that attack an unknown vulnerability, by identifying data containing malicious code or commands.
- **Exploit rules** 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 injection 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 servers.

FIREWALL

The enterprise-grade, bi-directional, stateful firewall provides centralized management of server firewall policy, and includes pre-defined templates for common enterprise server types.

- Virtual machine zoning
- Fine-grained filtering (IP & MAC addresses, Ports)
- Coverage of all IP-based protocols (TCP, UDP, ICMP,...)
- Coverage of all frame types (IP, ARP,...)
- Prevents Denial of Service (DoS) attacks
- Design policies per network interface
- Location awareness
- Reconnaissance scan detection

INTEGRITY MONITORING

Monitors critical operating system and application files (files, directories, registry keys and values, etc.) to detect malicious and unexpected changes. Meets PCI file integrity monitoring requirements.

- On-demand or scheduled detection
- Extensive file property checking, including attributes
- Monitor specific directories
- Flexible, practical monitoring through i ncludes /excludes
- Auditable reports

LOG INSPECTION

Collects and analyzes 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.

- Suspicious behavior detection
- Collection of security-related administrative actions
- Optimized collection of security events across the datacenter
- Advanced rule creation using OSSEC rule syntax

ADDITIONAL FEATURES

- VMware® vCenter™ integration
- SIEM integration with products from LogRhythm and many others
- Active Directory integration
- Multi-node Deep Security Manager for HA and enterprise scalability
- Web Services API
- Detailed reporting
- Automated management via security rule recommendations and scheduled tasks
- Role-based administration
- Alerts and notifications
- Custom rules
- Security updates shield newly discovered vulnerabilities
- Out-of-the-box vulnerability protection for over 100 applications

PLATFORMS PROTECTED

MICROSOFT® WINDOWS®

- 2000 (32 bit)
- XP (32 & 64 bit), XP embedded
- Windows Vista (32 & 64 bit)
- Windows Server 2003 (32 & 64 bit)
- Windows Server 2008 (32 & 64 bit)

SUN® SOLARIS™

- 8, 9, 10 (64 bit Sparc)
- 10 (64 bit x86)

LINUX™

- Red Hat® Enterprise 3.0 (32 bit)
- Red Hat® Enterprise 4.0, 5.0
- (32 & 64 bit)
- SUSE® Enterprise 9, 10 (32 bit)

UNIX®*

- AIX® 5.2
 - HP-UX® 10, 11i v2
- * Integrity Monitoring & Log Inspection

VIRTUALIZATION

- VMware® ESX™ Server Guest OS
- Citrix® XenServer™ Guest VM
- Microsoft® HyperV® Guest VM
- Sun® Solaris™ 10 Partitions

SECURITY CERTIFICATIONS

- Common Criteria EAL 3+
- PCI Suitability Testing for HIPS (NSS Labs)
- ICSA Firewall
- Microsoft Application Protection Program

North America - Excelerate Systems LLC

Excelerate Systems

22914 NE 54th St
Redmond, WA 98053
Tel: +1(425) 605-8515
e-mail: info@exceleratesystems.com

Central & Eastern Europe

Elizabetes ielā 22, stāvs 3
LV-1050, Rīga, Latvija
Tel: + 371 6 766-1073
e-mail: sales@exceleratesystems.com

Latin America - Excelerate Systems S de RL de CV

Rubén Darío No. 39 - 2oPiso int 5A
Col. Bosques de Chapultepec
CP 11580, México, D.F.
Tel: + 52 (55) 5255-1329

Australia and New Zealand

Suite 111, 370 St Kilda Rd
Melbourne
VIC 3000
Australia