

# EASE SecureOps

## For Oracle E-Business Suite



## Layered Security Model

Organizations face an increasing need to protect their critical applications from evolving cyber threats and unauthorized access, while also managing a continuous and complex flow of available patch packages to address security vulnerabilities, performance, stability and enhanced functionality. The biggest challenge to navigate is the impact of change to operations on many tech-stack levels combined with the evaluation process associated with it. EASE SecureOps for Oracle E-Business Suite (EBS) is a comprehensive 1-2 vulnerability scanning platform and web application firewall.

Protect Oracle E-Business Suite from vulnerability exploits with EASE SecureOps, a powerful, layered vulnerability scanning platform and web application firewall, built specifically for Oracle EBS.

## Comprehensive Protection for Oracle EBS



### Vulnerability Scanning

One comprehensive tool for the full Oracle EBS stack



### Threat Protection

Internal and external—before it reaches the application



### Virtual Controls

Patching and mitigation for all modules and all versions



### Security Policies

E-Business Suite-specific, tuned to OWASP Top 10



### Service Management

Integrated for peace of mind and audit support

## Service Add-On

EASE SecureOps can be purchased as an independent managed service on your cloud of choice to bolster your Oracle EBS security posture for a flat-monthly fee and can be easily added to existing Data Intensity Total Ops Management service contracts.

## All-Inclusive

EASE SecureOps is a full-service feature-set bundled with every new Data Intensity EASE for Oracle EBS Managed Services contract. This differentiation ensures optimal security posture for your Oracle EBS deployment on your cloud of choice.

## Auditing Tool & Vulnerability Assessment Scanner

Unlike other security scanners, EASE SecureOps knows the application and database it is validating – its technology and data model. The security audits and checks are written specifically for the application or database being tested. Hackers and mischievous employees exploit security issues at different layers of the technology stack, so only a complete and comprehensive security validation will uncover all risks in a multi-tiered environment. This technology:

- Uses advanced penetration testing techniques to externally discover security risks in the operating system, web servers, application servers, databases, and the application.
- Tests for known exploits and configuration errors are performed externally to the application in an attempt to break-in.
- Uses auditing to internally pin-point security weaknesses configuration issues and can spot risks missed by traditional vulnerability testing.
- Performs more than 1,450 security audits and checks against the target. All technology components – database, web server, application server, and operating system – are analyzed as well as the application.



- Blocks access to thousands of unused web pages and servlets when deploying Oracle EBS externally in a DMZ.
- Alerts, blocks, logs, or sanitizes incoming requests or outgoing responses based on over 30 different detection points.

## EASE SecureOps for Oracle EBS Managed Services include:

- 24x7 vulnerability scanning with rapid response and resolution for discovered vulnerabilities.
- Compliance support for annual audits performed by customer designated auditors.
- Unlimited virtual patching serves as mitigating controls to protect applications when patches can't be applied.
  - Unlimited WAF policy management
  - 24x7 monitoring and management of EASE SecureOps configuration policies.
  - Quarterly reporting.
  - Management of quarterly updates aligned with Oracle patch release cycles.

## Web Application Firewall (WAF)

A runtime application self-protection system (RASP), and intrusion prevention system specifically written for Oracle EBS is included. The power of EASE SecureOps is that it blocks web attacks against Oracle EBS before they reach the application as the newest generation of intrusion prevention – direct application protection.

This technology:

- Incorporates the top ten high-risk security principles set by the Open Web Application Security Project (OWASP) for application security.
- Reduces the window of vulnerability by providing continuous protection, incorporating updated rules dynamically, and virtual patching of published security vulnerabilities in Oracle's Critical Patch Updates.

## About Data Intensity

Data Intensity is an Oracle Strategic MSP partner delivering managed services for the complex lifecycle of Oracle-powered workloads. Offering a complete portfolio under one roof, we provide full-stack, technical, and functional application managed services on any cloud.

Additionally, we maximize and future-proof our clients' Oracle investments through effective license position assessments and cloud-independent migration services. Learn more at [www.dataintensity.com](http://www.dataintensity.com).

**ORACLE** | Service Partner

Expertise in  
CSPE: Oracle Cloud Platform -  
Oracle Database to Oracle Cloud  
in North America