

*mission critical applications ...  
... mission critical security*

**Application Intrusion Prevention**

# **AppDefend™ Product Overview**

The logo for Integrigy, featuring the word "INTEGRIGY" in a bold, blue, serif font. Above the letter "I" and the letter "Y" are green checkmarks.

# Integrigy Overview

- **Integrigy Corporation specializes in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. Integrigy Consulting offers security assessment services for leading databases and ERP/CRM.**
  
- **Corporate Details**
  - Founded December 2001
  - Privately Held
  - Based in Chicago, Illinois

# Integrigy Background

- **Extensive experience with Oracle**
  - Founded by former Big-6 consultants with significant experience on Oracle implementations in Fortune 500 companies
  - Founders recognized a major gap in all implementations – little or no security auditing done on projects
  - Integrigy has found more security bugs in Oracle Applications than anyone else inside or outside of Oracle
- **Both an ERP/CRM company and a security company**
  - Products developed to support and enhance an ERP/CRM implementation – Integrigy understands the issues and risks challenging large ERP/CRM implementations
  - Integrigy bridges the gap between applications, databases, and security

# Integrigy Security Alerts

Security Alert	Versions	Security Vulnerabilities
<b>Critical Patch Update July 2008</b>	Oracle 11g 11.5.8 – 12.0.x	<ul style="list-style-type: none"> <li>▪ 2 Issues in Oracle RDBMS Authentication</li> <li>▪ 2 Oracle E-Business Suite vulnerabilities</li> </ul>
<b>Critical Patch Update April 2008</b>	12.0.x 11.5.7 – 11.5.10	<ul style="list-style-type: none"> <li>▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update July 2007</b>	12.0.x 11.5.1 – 11.5.10	<ul style="list-style-type: none"> <li>▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update October 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ Default configuration issues</li> </ul>
<b>Critical Patch Update July 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> <li>▪ Information disclosure</li> </ul>
<b>Critical Patch Update April 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> <li>▪ Information disclosure</li> </ul>
<b>Critical Patch Update Jan 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #68</b>	Oracle 8i, 9i, 10g	<ul style="list-style-type: none"> <li>▪ Buffer overflows</li> <li>▪ Listener information leakage</li> </ul>
<b>Oracle Security Alert #67</b>	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> <li>▪ 10 SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #56</b>	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> <li>▪ Buffer overflow in FNDWRR.exe</li> </ul>
<b>Oracle Security Alert #55</b>	11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ Multiple vulnerabilities in AOL/J Setup Test</li> <li>▪ Obtain sensitive information (valid session)</li> </ul>
<b>Oracle Security Alert #53</b>	10.7, 11.0.x 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ No authentication in FNDFS program</li> <li>▪ Retrieve any file from O/S</li> </ul>

# Integrigy's Products

## AppDefend™

- Application firewall and intrusion prevention system for ERP packages
- Blocks common attacks like SQL injection, session hijacking, and cross site scripting
- Blocks access to unimplemented Oracle Applications modules
- Runs as an Apache modules and scans all incoming web requests

## AppSentry™

- Security scanner for databases, application servers, and ERP packages
- Performs advanced penetration testing and in-depth security and controls auditing
- Performs over 300+ audits and checks on Oracle products
- Runs on any Windows PC and requires no software to be installed on the target servers

# AppDefend

- **Application Intrusion Prevention System for ERP packages**
- **Blocks common attacks like SQL injection, session hijacking, and cross site scripting**
- **Blocks access to unimplemented Oracle Applications modules**
- **Runs as an Apache modules and scans all incoming web requests**

# AppDefend

- **Application-level intrusion prevention system for the ERP/CRM Applications**
  - Scans all incoming web requests for common web application vulnerabilities including –
    - ◆ SQL Injection
    - ◆ Cross Site Scripting
    - ◆ Session Hijacking
  - Blocks unused CGI-Bin programs and sample applications
  - Users can specify filters to block other programs or files
  
- **AppDefend for the Oracle E-Business Suite**
  - Blocks published and un-published Oracle Applications security vulnerabilities
  - **Permits access to only enabled/installed Oracle Applications Modules**
    - ◆ **Oracle Applications delivered with 12,000 accessible Java Server Pages and Java servlets, even though only a 1,000 or fewer may be used by the customer**
  - Implemented as an Apache module

# AppDefend Supported Applications

## Oracle E-Business Suite

- 11i (11.5.9 – 11.5.10 CU2)
- 12.0.x
- 12.1.x

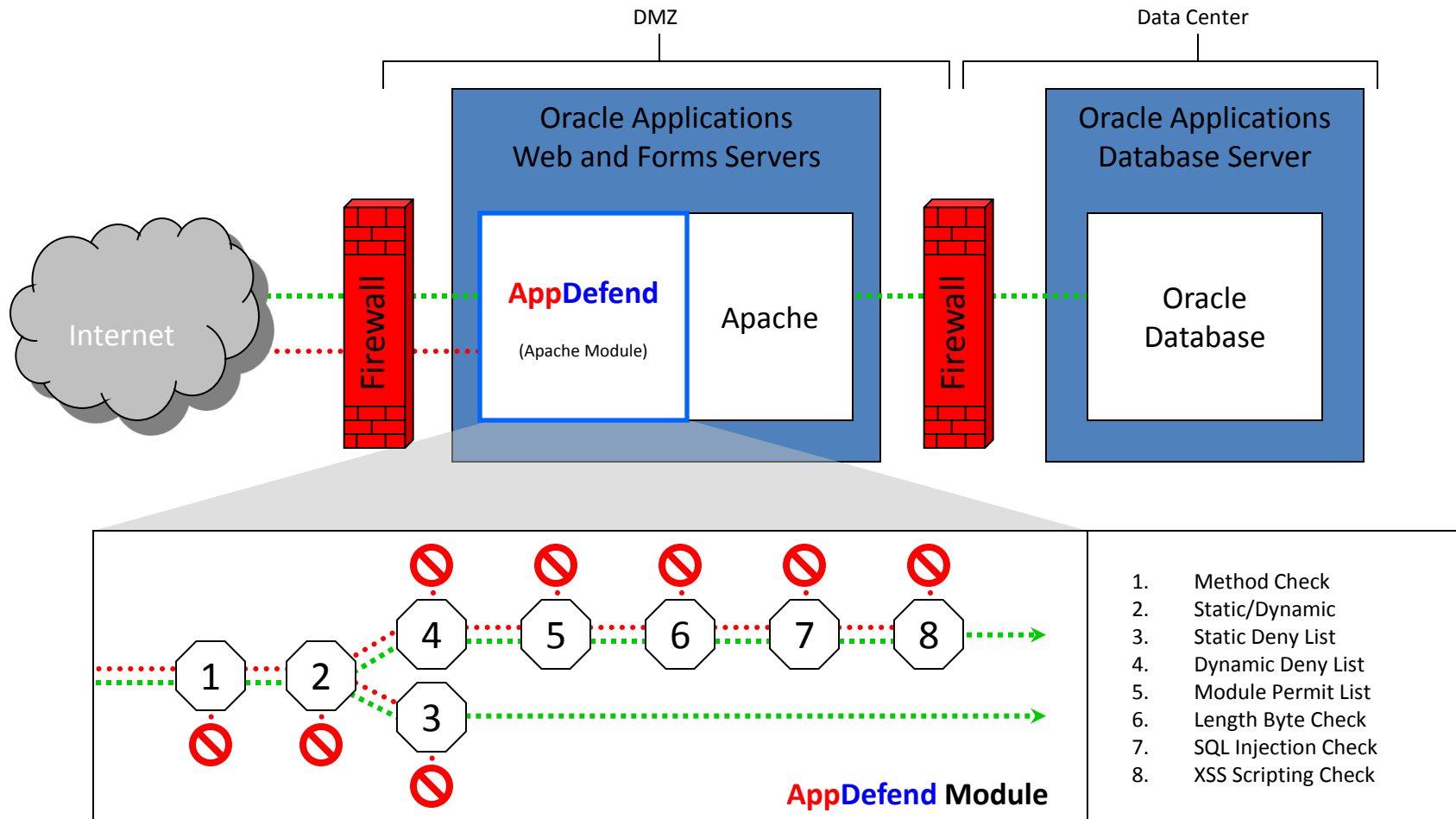
## Oracle PeopleSoft

- Under development

## Oracle Fusion Applications

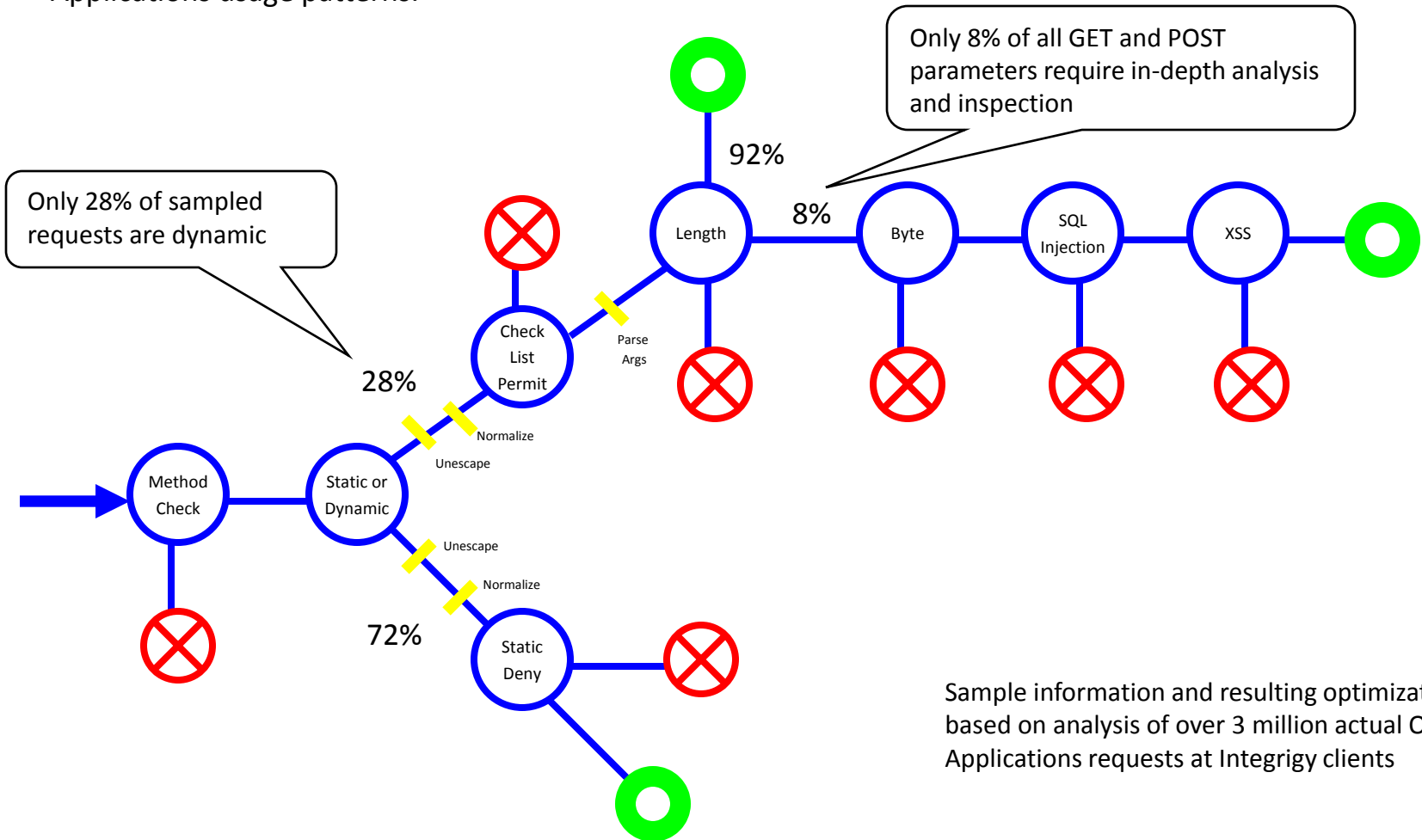
- Under development

# AppDefend™ Architecture



# AppDefend™ Processing

- Deep Request Inspection™ - highly optimized request analysis and inspection based on actual Oracle Applications usage patterns.



Sample information and resulting optimization based on analysis of over 3 million actual Oracle Applications requests at Integriqy clients

# AppDefend vs. Traditional IDS/IPS

## AppDefend

- Designed for Oracle Applications – highly specialized rules in-place with the default configuration
- Blocks unused Oracle Applications modules
- 30 minute installation and configuration
- Scans entire web request including POST
- AppDefend is distributed to each application server for resiliency and performance

## Traditional IDS/IPS

- Must be heavily customized for Oracle Applications – rules must be developed and tested
- Complex configuration required to block unused Oracle Applications modules
- Significant effort and skill required to deploy and configure
- Many IDS/IPS solutions do not scan POST data
- Potential single point of failure and a possible performance bottleneck

# AppDefend for the Oracle E-Business Suite

## ■ Oracle E-Business Suite

- 11.5.9 – 11.5.10.2, 12.0.x, 12.1.x
  - ◆ 11.5.1 and 11.5.7 not supported due to Oracle desupport
- Industry Verticals (Automotive, Clinical, Exchange)
- AutoConfig and non-AutoConfig implementations supported
- Apache 1.3.9, 1.3.12, 1.3.19, 1.3.29

## ■ Supported Operating Systems

- Sun SPARC Solaris 8, 9, 10
- HP PA-RISC HP/UX 11.0, 11.11, 11.23
- IBM AIX 4.3.2, 4.3.3, 5L, 6L
- Linux x86
  - ◆ Oracle Enterprise Linux 4, 5
  - ◆ Red Hat Enterprise Linux AS/ES 3, 4, 5
  - ◆ SuSe 8, 9, 10

# Integrigy Contact Information

**Integrigy Corporation**  
**P.O. Box 81545**  
**Chicago, Illinois 60681**  
**888/542-4802**

**Website:** [www.integrigy.com](http://www.integrigy.com)

**Sales:** [sales@integrigy.com](mailto:sales@integrigy.com)

**Development:** [development@integrigy.com](mailto:development@integrigy.com)

**Support:** [support@integrigy.com](mailto:support@integrigy.com)

**Security Alerts:** [alerts@integrigy.com](mailto:alerts@integrigy.com)

Copyright © 2011 Integrigy Corporation. All rights reserved.

