INTEGRIGY

AppDefend

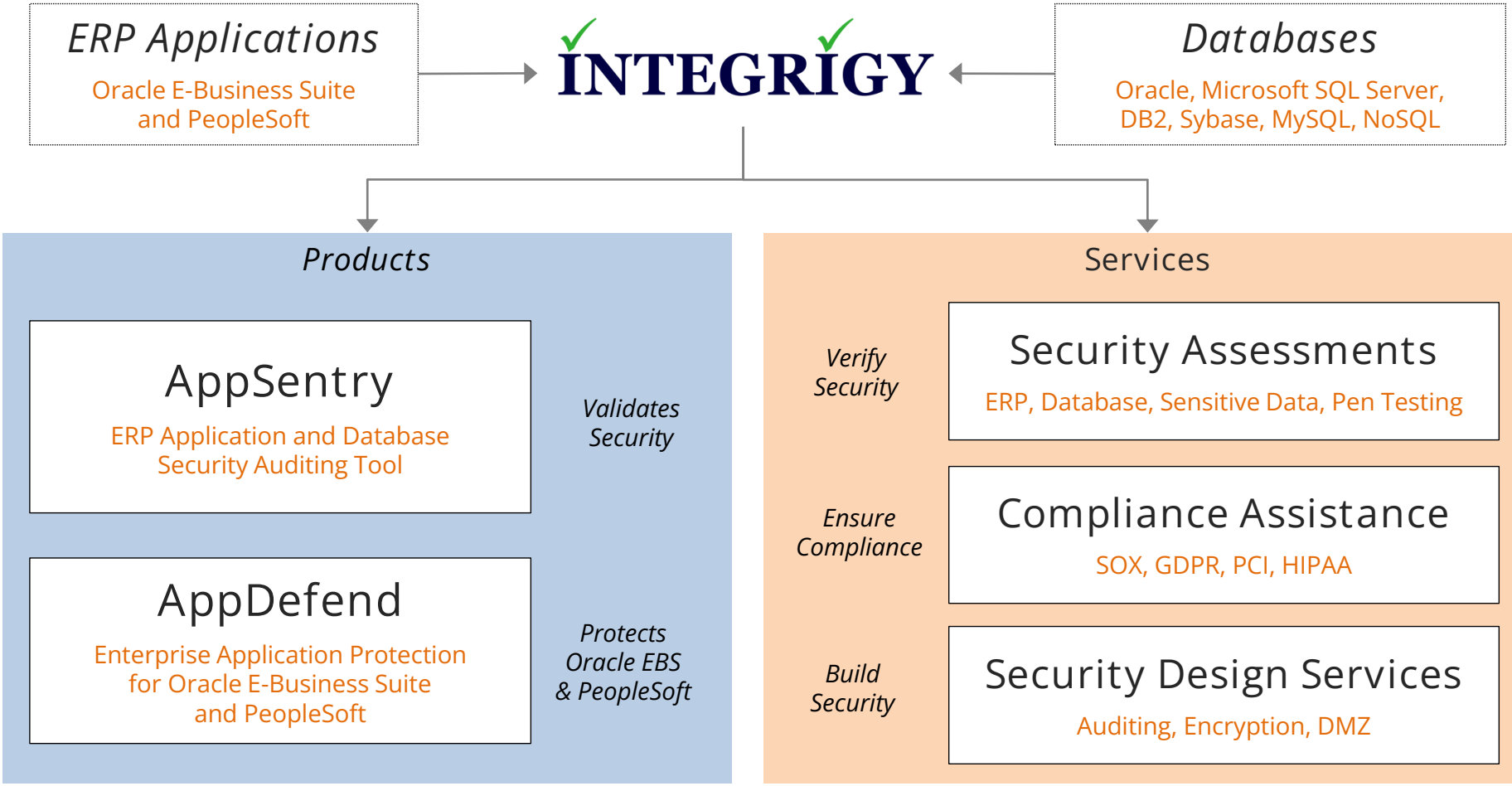
Oracle E-Business Suite

Enterprise Application Protection

October 2023

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

About Integrigy



Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

Agenda

1. AppDefend Overview
2. Application Protection and Defense
3. Application SSO and MFA
4. AppDefend Features
5. Q & A

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Integrigy's products remains at the sole discretion of Integrigy.

Integrigy's Products

AppSentry	Security scanner for databases, application servers, and ERP packages ▪ Performs advanced penetration testing and in-depth security and controls auditing ▪ Performs over 1,000+ audits and checks on Oracle products ▪ Requires no software to be installed on the target servers
AppDefend	Application firewall and protection system for ERP packages ▪ Blocks common attacks like SQL injection, session hijacking, cross site scripting, and Java deserialization ▪ Blocks access to unimplemented application modules and pages ▪ Scans all incoming web requests and outbound responses

Agenda

1. AppDefend Overview
2. Application Protection and Defense
3. Application SSO and MFA
4. AppDefend Features
5. Q & A

Integrigy AppDefend

AppDefend is an enterprise application firewall designed and optimized for the Oracle E-Business Suite.

Prevents Web Attacks

Detects and reacts to SQL Injection, XSS, and known Oracle EBS vulnerabilities with hybrid protection using WAF and RASP

Limits EBS Modules

More flexibility and capabilities than URL firewall to identify EBS modules

Protects Mobile Applications

Detects and reacts to attacks against Oracle EBS mobile applications

Protects Web Services

Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST)

SSO and two-factor (2FA/MFA)

Enables SSO and two-factor authentication for login, user, responsibility, or function

Application Logging

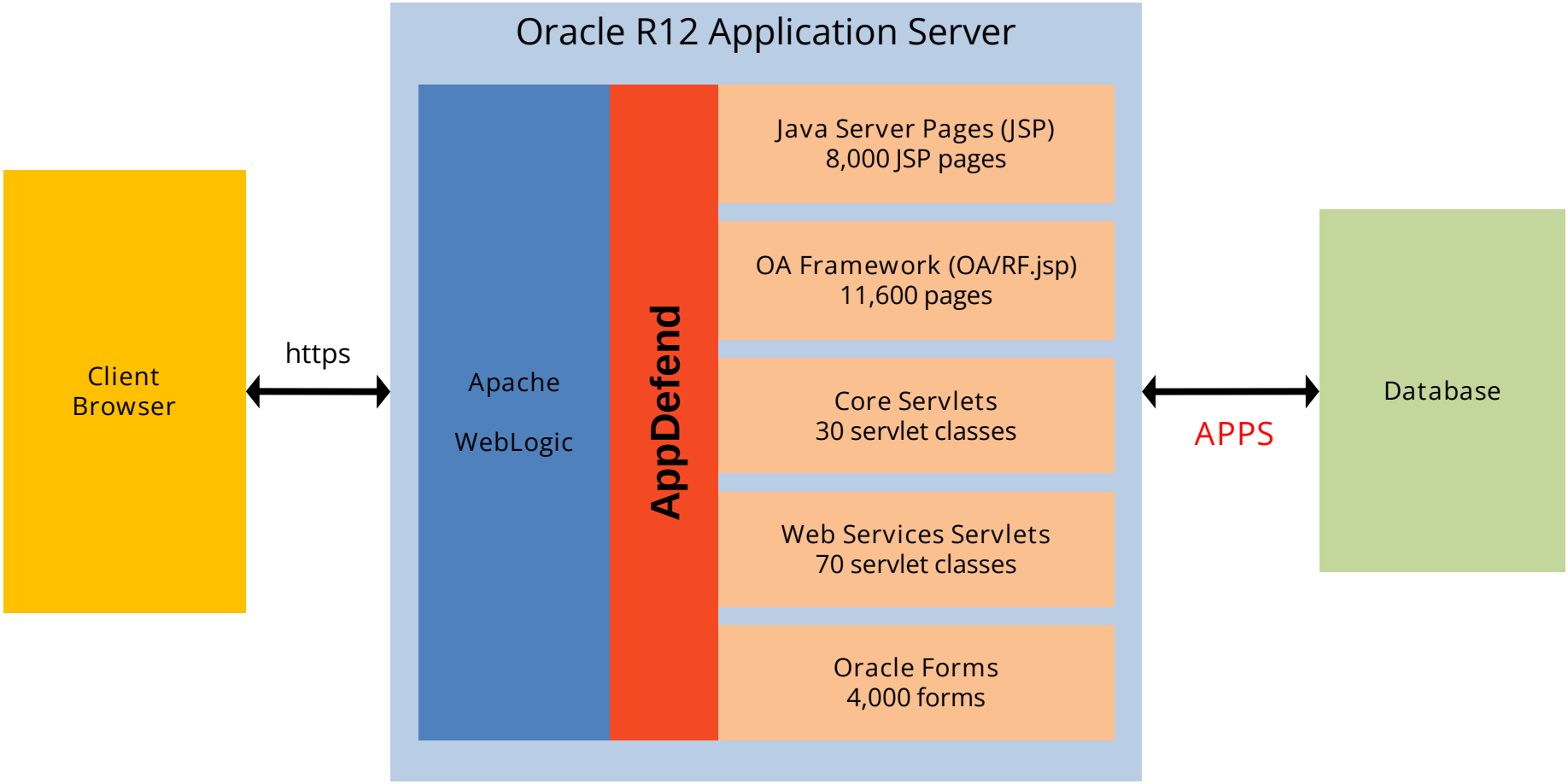
Enhanced application logging for compliance requirements like SOX, GDPR, PCI-DSS 10.2

AppDefend Oracle E-Business Suite Support

Oracle E-Business Suite	▪ 12.2.x ▪ 12.1.x ▪ 12.0.x [1] ▪ 11.5.10.x (proxy mode)
Operating Systems	Supported operating systems [2] ▪ Linux x86 (Oracle Enterprise Linux, Red Hat Enterprise Linux AS/ES, SuSe) ▪ Sun SPARC Solaris ▪ HP PA-RISC HP/UX ▪ IBM AIX

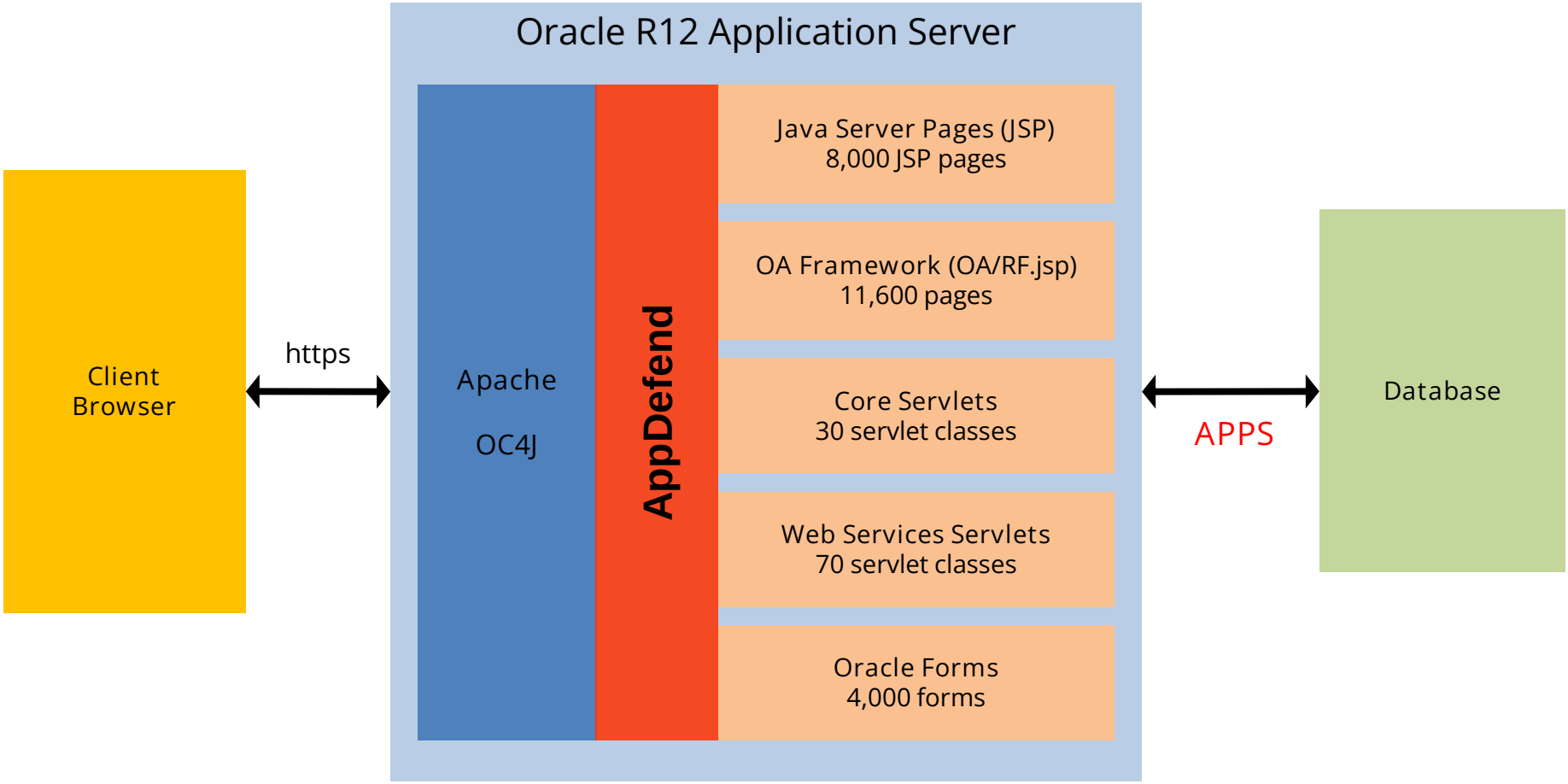
[1] For 12.0.x, application server Java version must be upgraded to JDK 1.6. [2] For 11.5.x, OS version must be supported by JDK 1.8.

AppDefend and Oracle EBS 12.2



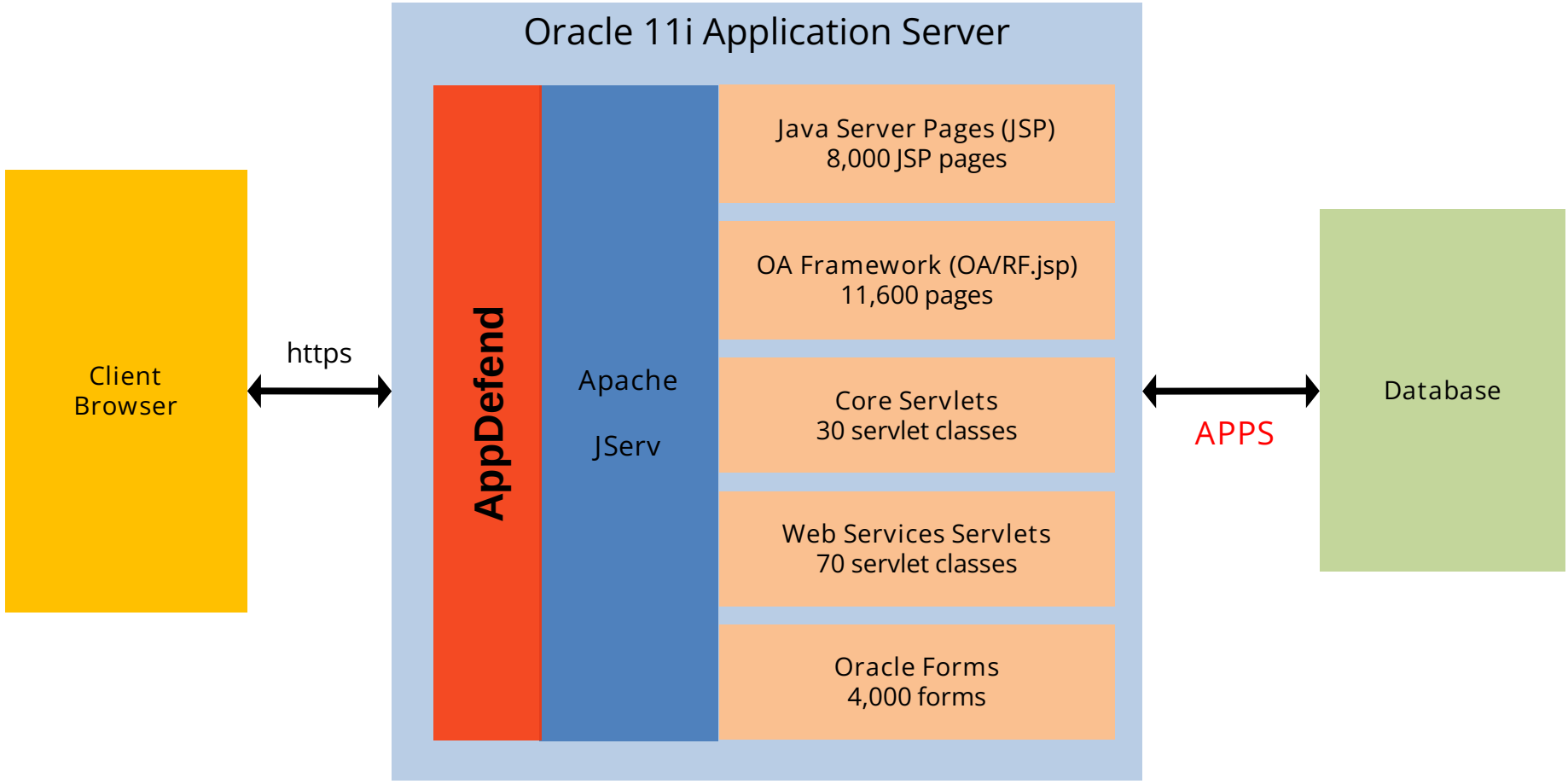
- AppDefend runs within the WebLogic Java containers as a servlet filter and Java agent that monitors all incoming requests, out-going responses, and key method calls. Being in the Java container, AppDefend can access all session state, attributes, error messages, EBS APIs, and the database.

AppDefend and Oracle EBS 12.0 & 12.1



- AppDefend runs within the Oracle E-Business Suite OC4J containers as a servlet filter and Java agent that monitors all incoming requests, out-going responses, and key method calls. Being in the OC4J container, AppDefend can access all session state, attributes, error messages, APIs, and the database.

AppDefend and Oracle EBS 11i



- AppDefend runs as a reverse proxy on the Oracle EBS application server intercepting all requests and responses. AppDefend is able to act as an SSL/TLS termination point due to the vulnerabilities in the EBS SSL libraries.

AppDefend Features

Configuration	▪ Dynamic reloading of configuration files – no restarting of the application server required ▪ Disable AppDefend dynamically and log only mode ▪ Parallel configurations to support transition to SSO and MFA ▪ Rules and configuration files use JSON notation ▪ Support for all EBS architectures like shared APPL_TOPs and DMZ servers
Logging and Alerting	▪ Flexible formatting and destinations ▪ Files with periodic or sized-based rotation, size limits ▪ Syslog with support for major logging platforms (Splunk, ArcSight, enVision, QRadar, Microsoft Sentinel, AWS CloudWatch, etc.)
Resiliency	▪ Fail open or closed upon internal errors ▪ Fail open or closed upon startup or configuration errors

AppDefend Installation and Updates

Installation	▪ One hour installation web sessions included with subscription – 15-minute install, 45-minute walk-through ▪ Download and install AppDefend binary and rules ▪ Customization AppDefend base configuration ▪ AutoConfig customization ▪ Restart oacore Java container
Updates	▪ New rules and rule updates – quarterly or as needed ▪ Download and unzip appdefend.zip ▪ AppDefend dynamically reloads rules
Upgrades	▪ New features and non-rule fixes – biannual or as needed ▪ Download and unzip appdefend.zip ▪ Restart oacore Java container

Agenda

1. AppDefend Overview
2. Application Protection and Defense
3. Application SSO and MFA
4. AppDefend Features
5. Q & A

SQL Injection Explained

Attacker modifies URL with extra SQL

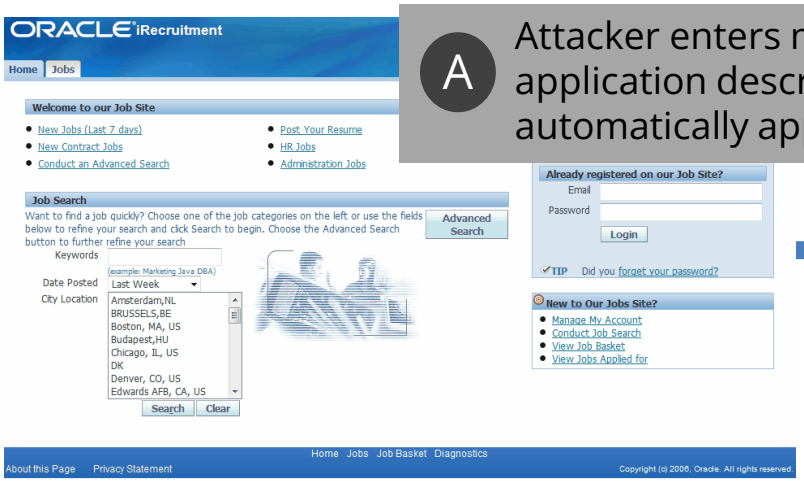
```
http://<server>/pls/VIS/fnd_gfm.dispatch?p_path=fnd_help.get/US/fnd/@search');%20fnd_user_pkg.updateUser('operations',%20'SEED',%20'welcome1
```

Oracle EBS executes appends SQL to the SQL statement being executed

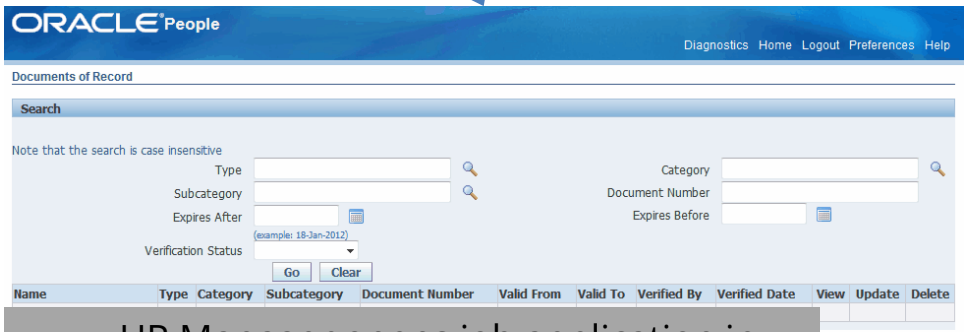
- SQL executed as APPS database account
- Example changes any application account password

This vulnerability was patched as part of Oracle Security Alert #32

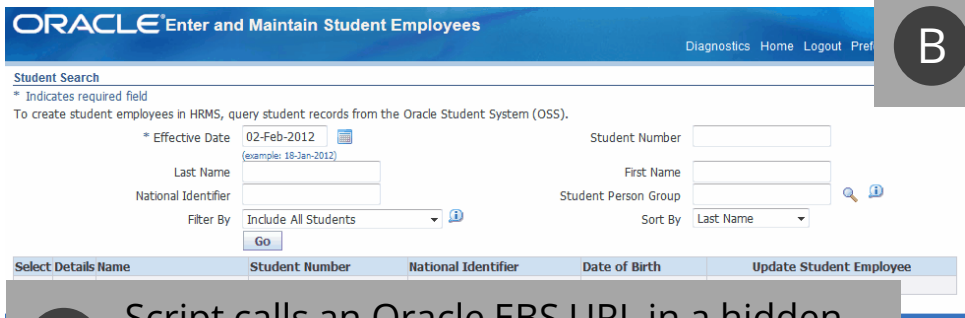
Cross Site Scripting (XSS) Illustrated



A Attacker enters malicious JavaScript into job application description field to for example automatically approve resume



B HR Manager opens job application in Oracle and script executes in browser



C Script calls an Oracle EBS URL in a hidden frame to execute some EBS functionality

Cross Site Scripting – Sample Attacks

```
<script>alert(0)</script>

<img src="x:x" onerror="alert(0)">

<iframe src="javascript:alert(0)">

<object data="javascript:alert(0)">

<isindex type=image src=1 onerror=alert(0)>

<img src=x:alert(alt) onerror=eval(src) alt=0>

with(document)alert(cookie)

eval(document.referrer.slice(10));

(É=[Å=[],µ=!Å+Å][µ[È=-~-~++Å]+({}+Å) [Ç=!!Å+µ,ª=Ç[Å]+Ç[+!Å],Å]+ª])() [µ[Å]+µ[Å+Å]+Ç[È]+ª](Å)

</a onmousemove="alert(1)">

data:text/html,<script>alert(0)</script>

%C0%BCscript%C0%BEalert(1)%C0%BC/script%C0%BE

<ScRIPT x src=//0x.lv?
```

Cross Site Scripting References

XSS Cheat Sheet

http://ha.ckers.org/xss.html

WSC Script Mapping Project

http://www.webappsec.org/projects/scriptmapping

OWASP XSS Reference

https://www.owasp.org/index.php/Cross-Site_Scripting

Oracle EBS Security Vulnerabilities

Oracle E-Business Suite security vulnerabilities
fixed between
January 2005 and April 2023

1,041

Oracle EBS Web Vulnerabilities Fixed

~150	SQL Injection in web pages
~640	Cross Site Scripting
~90	Authorization/Authentication
~60	Business Logic Issues
~7	Non-EBS Vulnerabilities

OWASP Top 10 – Oracle E-Business Suite Mapping

Ten top security risks commonly found in web applications listed by level of risk

A1: Broken Access Control	A2: Cryptographic Failures	A3: Injection	A4: Insecure Design
A5: Security Misconfiguration	A6: Vulnerable and Outdated Components	A7: Identification and Authentication Failures	A8: Software Design and Data Integrity Failures
	A9: Security Logging and Monitoring Failures	A10: Server-side Request Forgery (SSRF)	

High Risk

Medium Risk

Low Risk

http://www.owasp.org/index.php/Top_10

WASC Threat Classification

Web Application Security Consortium

Comprehensive list of threats to the security of a web site – attacks and weaknesses

Attacks

- Abuse of Functionality
- Brute Force
- Buffer Overflow
- Content Spoofing
- Credential/Session Prediction
- Cross-Site Scripting
- Cross-Site Request Forgery
- Denial of Service
- Fingerprinting
- Format String
- HTTP Response Smuggling
- HTTP Response Splitting
- HTTP Request Smuggling
- HTTP Request Splitting
- Integer Overflows
- LDAP Injection
- Mail Command Injection
- Null Byte Injection
- OS Commanding
- Path Traversal
- Predictable Resource Location
- Remote File Inclusion (RFI)
- Routing Detour
- Session Fixation
- SOAP Array Abuse
- SSI Injection
- SQL Injection
- URL Redirector Abuse
- XPath Injection
- XML Attribute Blowup
- XML External Entities
- XML Entity Expansion
- XML Injection
- XQuery Injection

Weaknesses

- Application Misconfiguration
- Directory Indexing
- Improper File System Permissions
- Improper Input Handling
- Improper Output Handling
- Information Leakage
- Insecure Indexing
- Insufficient Anti-automation
- Insufficient Authentication
- Insufficient Authorization
- Insufficient Password Recovery
- Insufficient Process Validation
- Insufficient Session Expiration
- Insufficient Transport Layer Protection
- Server Misconfiguration

http://www.webappsec.org

High Risk * Medium Risk * Low Risk * No Risk

Inherent Risks with Package Software

Structure and vulnerabilities within the application are well known and documented

- An attacker knows exactly what to expect and how the application is structured
- No probing or reconnaissance of the application is required
- Fatal attack can be one URL
- Allows for easy automated attacks

Another Layer of Security

Web Application Firewalls (WAF) are specialized firewalls designed to detect and prevent web application attacks by analyzing the HTTP web requests.

- Prevents common web application attacks
  Detects and blocks SQL injection, XSS, and known vulnerabilities in widely used web applications

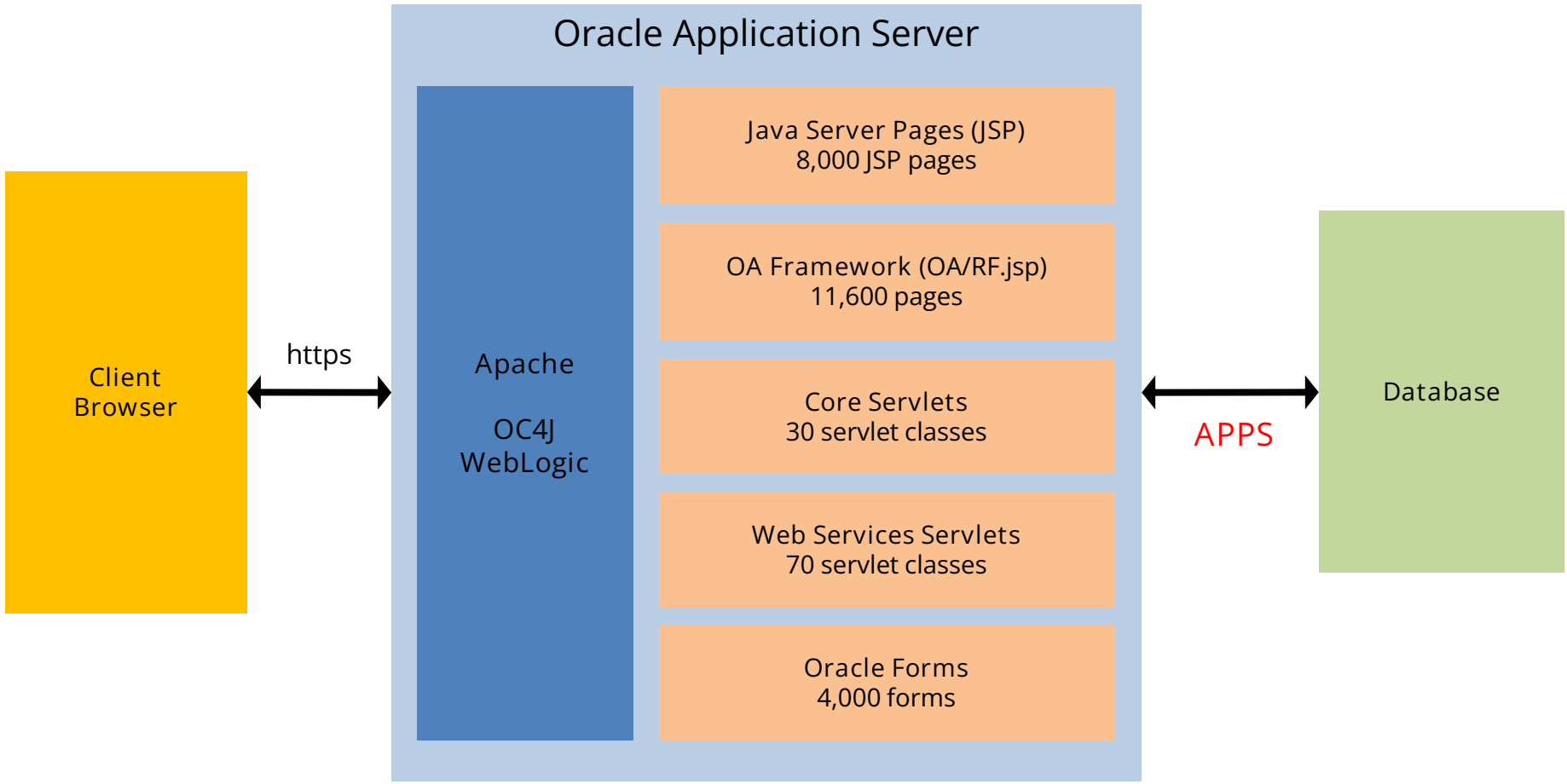
- Often implemented as an appliance
  Dedicated appliance used to protect all web applications in an organization

- May be required for compliance such as PCI-DSS
  PCI-DSS 2.0 requirement 6.6 requires use of a WAF or periodic reviews

Web Application Firewall (WAF) Shortcomings

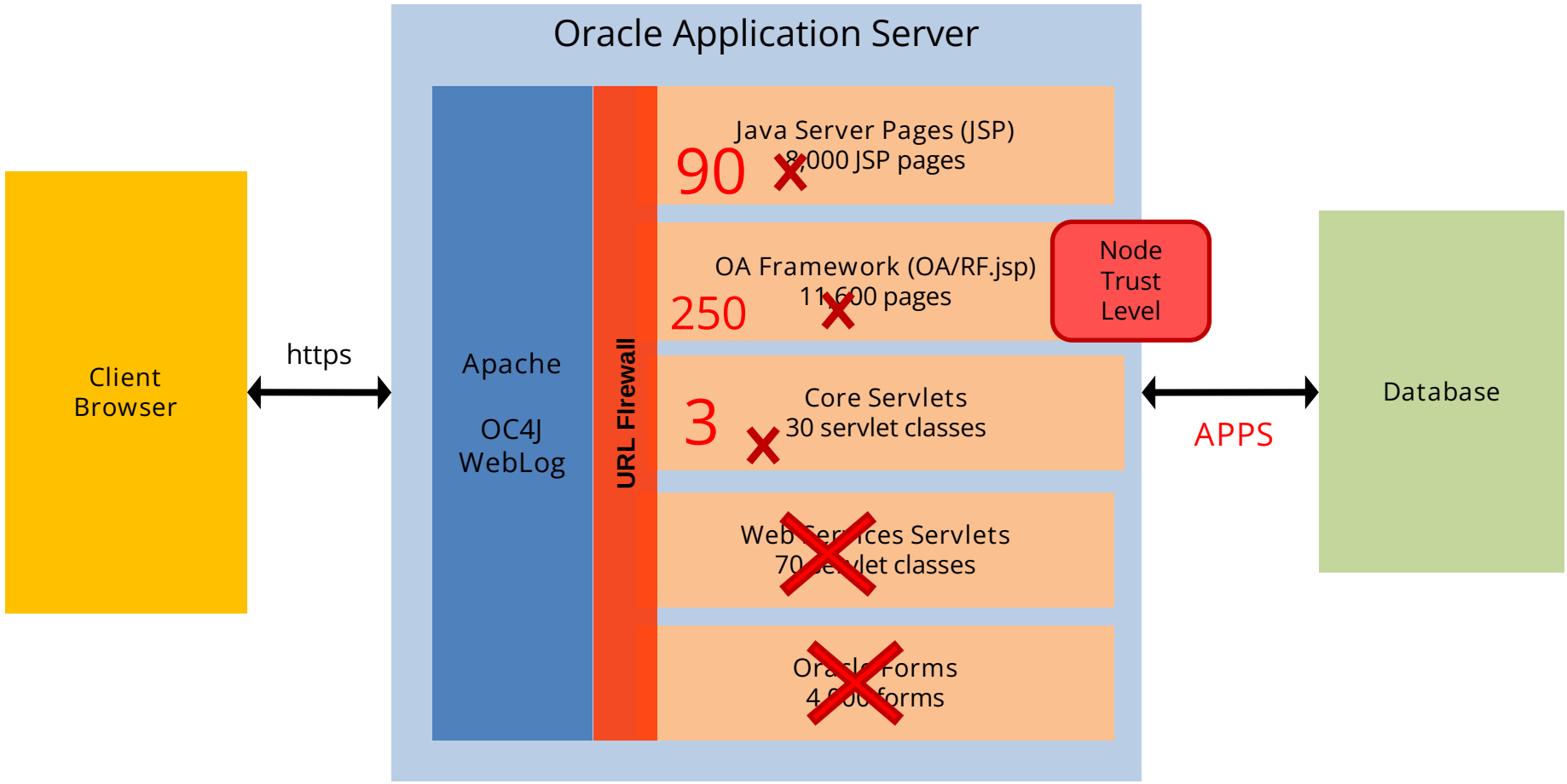
- Must be heavily customized for Oracle EBS
  - No out of the box rules for Oracle EBS – no CPU specific rules
  - Unaware for the unique web application architecture of OA Framework
  - Rules, application profiles, and learning must be developed, tuned, and tested by you
  - Oracle EBS is multiple web architectures resulting in additional tuning
- Unable to block unused Oracle EBS modules
  - Due to the complexity of the Oracle naming and design, very difficult to implement blocking of EBS modules with WAF rules
- Significant cost, effort, and skill required to deploy
  - WAFs are usually an appliance that must be deployed and the learning curve for configuring and operating an enterprise WAF is steep
- AppDefend is complementary with an enterprise WAF solution
  - AppDefend can be stand-alone or combined with an existing WAF
  - Multiple layers of defense
  - Enterprise WAF provides general protection and eliminates “noise”
  - AppDefend provides Oracle EBS specific layer of protection

Oracle EBS R12 DMZ Configuration



- All Oracle E-Business Suite environments include ALL modules (250+) and ALL web pages (20,000+) even if modules are not installed, licensed, or configured. Many security vulnerabilities exist in unused modules.

Oracle EBS R12 DMZ Configuration



- Proper DMZ configuration reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules. (See MOS Note ID 380490.1)

Oracle EBS 11i Web Components

Component	11i Version	Release Date	Non-EBS Desupport[1]
Oracle Application Server[3]	1.0.2.2.2	Dec 2001	June 2004
Apache[3]	1.3.19	Feb 2001	Feb 2010
Jserv	1.1.2	June 2000	June 2006
mod_security	1.8.4	July 2004	May 2006
OpenSSL	0.9.5a	Sept 2000	March 2004
	0.9.8zh[2]	Dec 2015	Dec 2016

1. Oracle EBS 11i web components are desupported but had support exceptions for 11i environments through January 2016. As of January 2016, all support for 11i and associated technology stack components has ended.
2. OpenSSL updated from 0.9.5a to 0.9.8zh with July 2015 Critical Patch Update for OAS 1.0.2.2.2.
3. Security vulnerabilities are patched but version is not upgraded.

AppDefend Virtual Patching

Eliminate risk and exploitation of the security bug by blocking access to the vulnerable code

- Integrigy analyzes the Oracle Critical Patch Update (CPU)
- Delivers pre-defined rules for CPU web bugs
- Rules may be at the page or field level to block known vulnerabilities

Integrigy Oracle CPU Analysis

For each quarterly Oracle CPU, Integrigy performs an analysis and updates the AppDefend rule set to include virtual patch rules for all external and internal web vulnerabilities

Sample from Integrigy CPU Analysis

CVE ID	Oracle EBS Versions	Vulnerability Information	Recommended Additional Steps and CPU Patch Testing	AppDefend External (DMZ) Rules (rule ID)	AppDefend Internal Rules (rule ID)	AppSentry Detection (check name)
CVE-2013-5890	11.5.10.2 12.0.6 12.1.1 - 12.1.3 12.2.2	*Module:* **Oracle Payroll – Public Sector Payroll** *Sub-Component:* **Payroll Exception Reporting** *Type:* **SQL Injection** *Remotely Exploitable without Authentication:* **No** *CVSS Metric:* **5.5** A SQL injection vulnerability in payroll exception report groups.	Basic testing of payroll exception report group configuration and reporting.	New request parameter rule (Rule ID 453) **Module should be blocked*	New request parameter rule (Rule ID 453)	Vulnerable file version check (oraappcpu0114)
CVE-2014-0398	11.5.10.2 12.0.6 12.1.1 - 12.1.3 12.2.2	*Module:* **Oracle Application Object Library** *Sub-Component:* **Discoverer and OBIEE Launcher** *Type:* **Information Disclosure and XSS** *Remotely Exploitable without Authentication:* **Yes** *CVSS Metric:* **5.0** Multiple information disclosure and cross-site scripting (XSS) vulnerabilities in the launcher for Discoverer and OBIEE. FND_DIAGNOSTICS has to be set to "Yes" in order to exploit most of these vulnerabilities. FND_DIAGNOSTICS should always be set to "No" at the site level for all Oracle EBS environments.	1. Ensure FND_DIAGNOSTICS is set to "No" at the site level for all environments, especially external facing implementations (i.e., iSupplier, iStore, iRecruitment, etc.). Review all applications, responsibilities, and users where FND_DIAGNOSTICS is set to "Yes". 2. Test to see if Discoverer and OBIEE launch successfully.	New request parameter rule (Rule ID 454) **Page should be blocked*	New request parameter rule (Rule ID 454)	Vulnerable file version check (oraappcpu0114)

Deep Request Inspection™

Analyze all user provided input to identify and block malicious input

- Intelligent checking of ALL parameters, user input
- Uses best practice libraries for XSS and SQL injection detection
  - OWASP AntiSamy, Java HTML Sanitizer
  - OWASP ESAPI
- Malicious input may be detected, blocked, or sanitized

Agenda

1. AppDefend Overview
2. Application Protection and Defense
3. Application SSO and MFA
4. AppDefend Features
5. Q & A

SSO Benefits for Oracle E-Business Suite

- Increase employee and IT productivity
  - Improve user experience by eliminating multiple application logins
  - Better application usability and employee satisfaction by reducing password fatigue
- Reduce IT costs
  - Fewer support calls for password resets and authentication issues
- Improve security
  - Reduce risk of password theft due to password fatigue
  - Enhance password strength with fewer passwords
  - Enables enforcement of stronger and more realistic password policies
- Improve compliance
  - Single point of user termination across applications
  - Simplify user and password management
  - Implement additional account controls like risk-based authentication

Oracle E-Business Suite User Populations – SSO and MFA

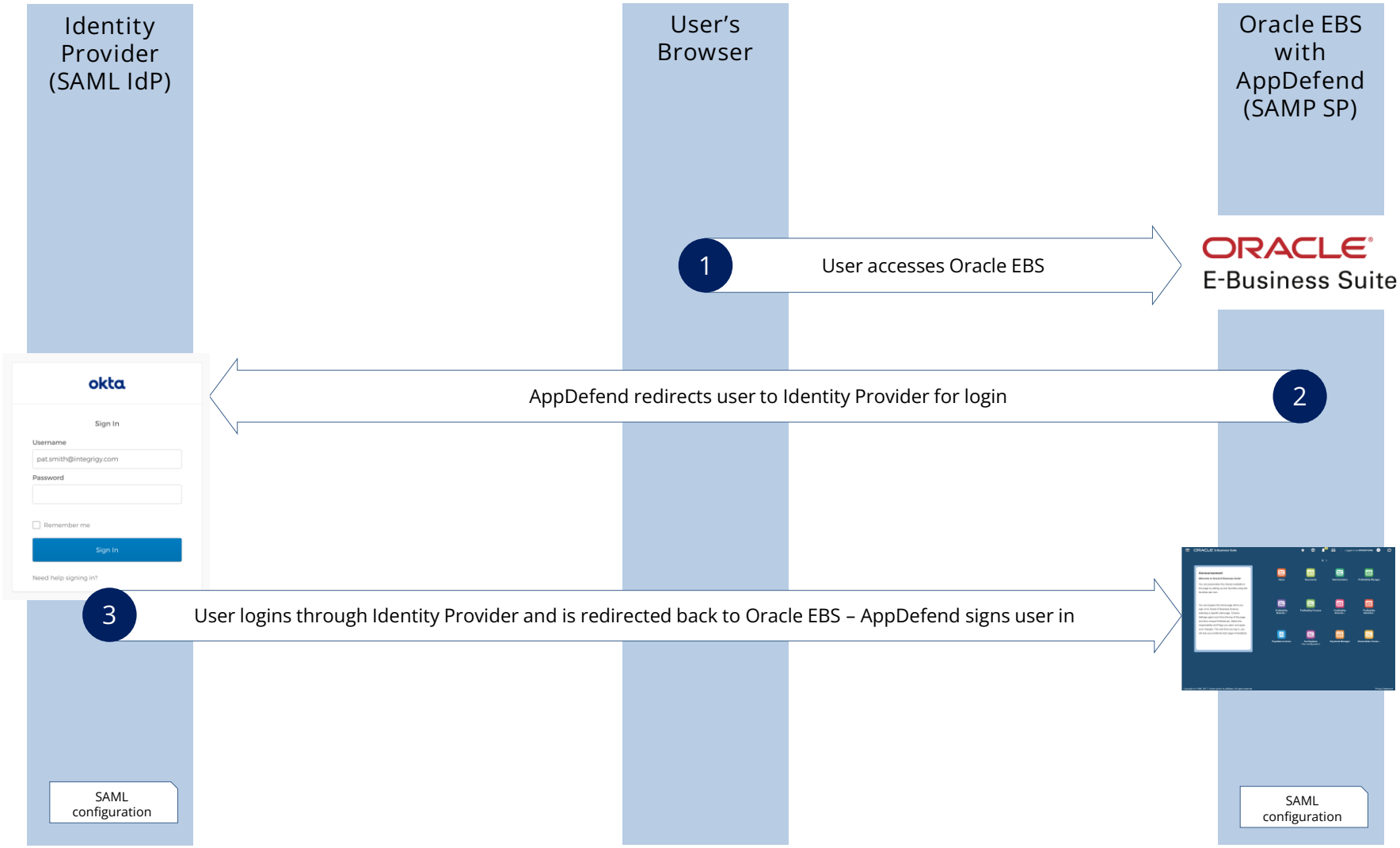
AppDefend SSO and MFA can be tailored to specific Oracle EBS user populations and configured with different SSO and MFA methods for each user population. Mix and match SSO and MFA even multiple SSO solutions for different groups of internal users.

	Typical Options for SSO/Authentication	Typical Options for MFA
Internal Users (SSO and/or MFA)	SAML (AD, Azure AD, Okta, etc.)	(1) with SAML (2) DUO, RSA, RADIUS, PKI, and SmartCard
Generic Internal Users (SYSADMIN, BATCH, JOB, ...)	SAML named user	(1) SAML named user (2) FND_USER named user (3) DUO
External Users – Suppliers (iSupplier)	FND_USER	(1) TOTP (2) SMS (3) Email (4) no MFA
External Users – Candidates/Customers (iRecruitment/iStore)	FND_USER	(1) TOTP (2) SMS (3) Email (4) no MFA

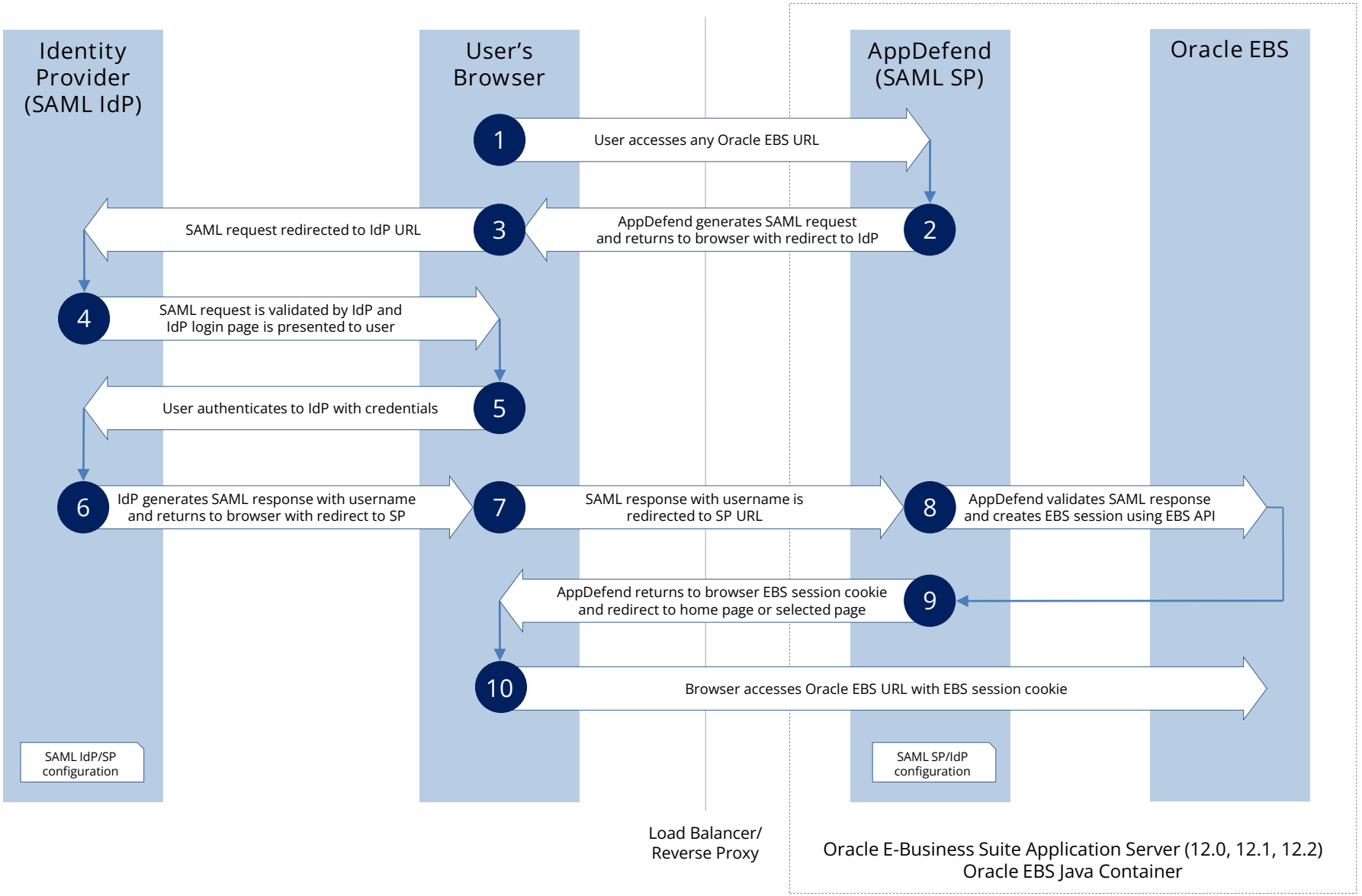
AppDefend SSO Feature (SAML)

- AppDefend adds single sign-on (SSO) for Oracle E-Business Suite
  - SAML 2.0 support for Oracle EBS as a service provider (SP)
  - No additional hardware or servers
  - No additional identity management software
- Direct integration with SAML 2.0 Identity Providers (IdP)
  - Supports any SAML 2.0 IdP such as –
    - Active Directory On-Premise (ADFS)
    - Azure AD (Microsoft Azure Active Directory)
    - Okta
    - AWS IAM Identity Center
    - Ping Identity
- Multiple Modes
  - Oracle E-Business Suite SSO Provider (system profile options)
  - AppDefend servlet filter
  - Direct SSO to Oracle E-Business Suite
  - WebADI and EBS mobile applications are fully supported
- Secure Implementation
  - Oracle EBS Session cookie set to “host” rather than “domain”

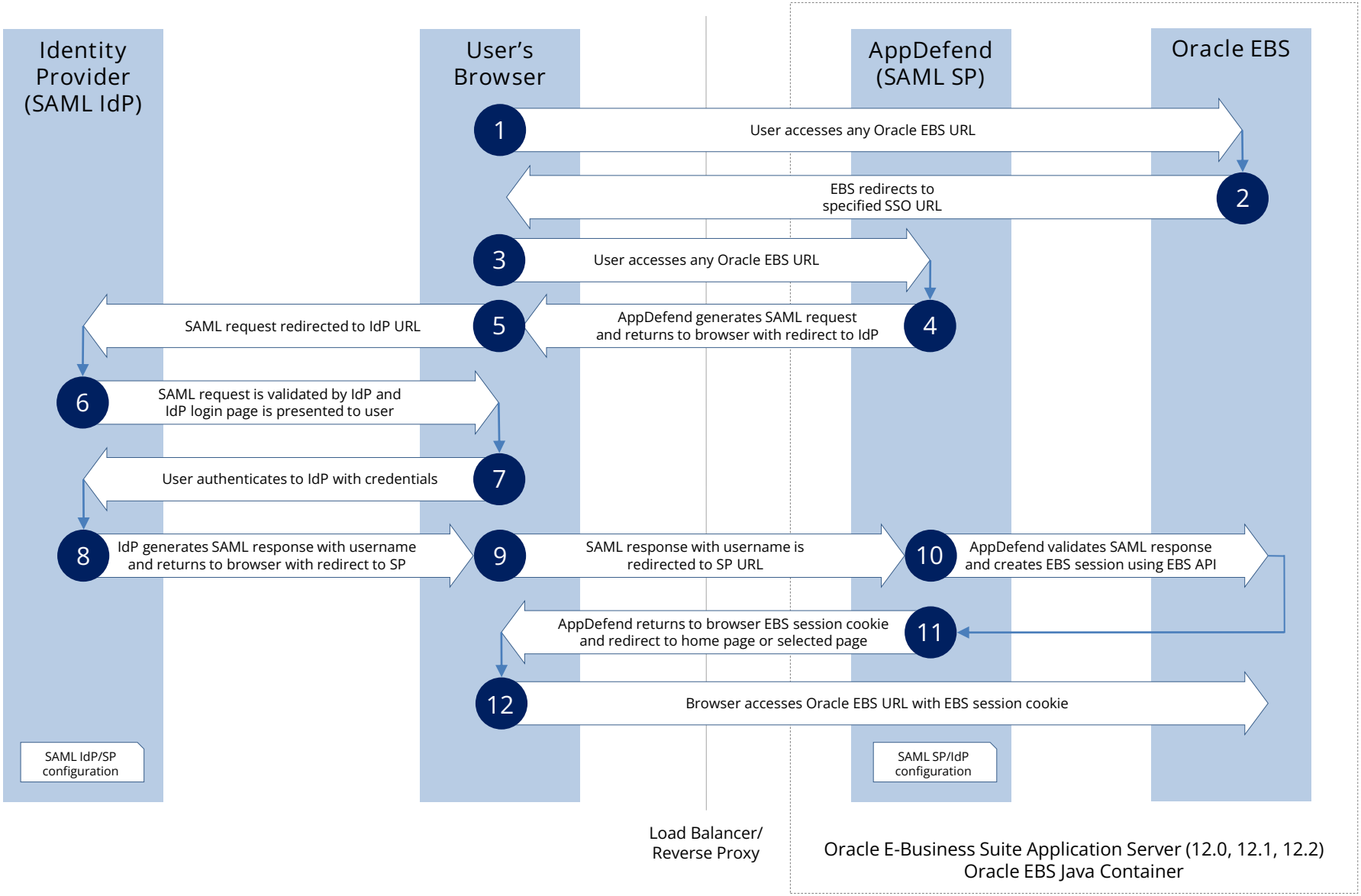
AppDefend SSO SAML Flow – High-level



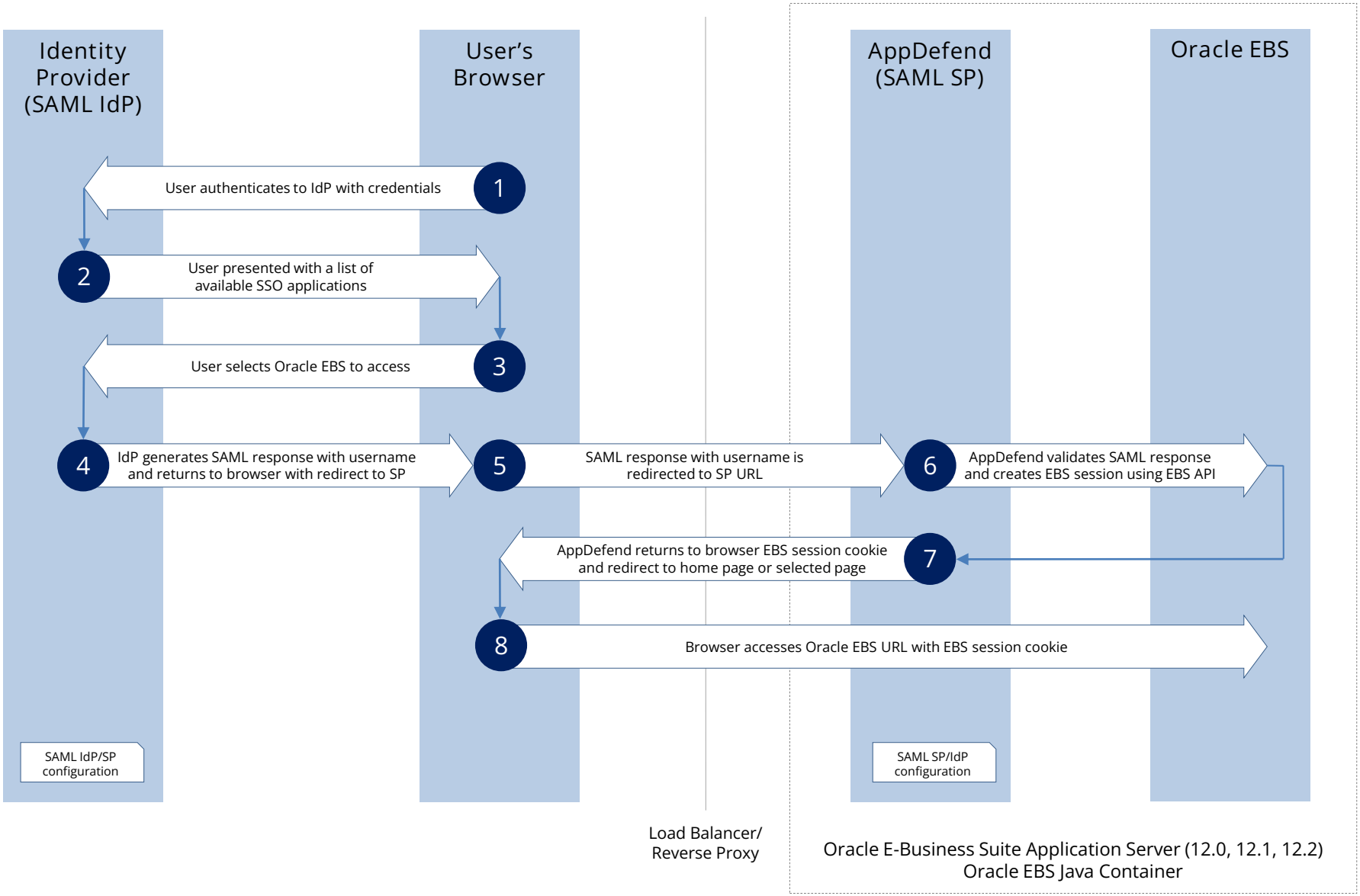
AppDefend SSO SAML Flow



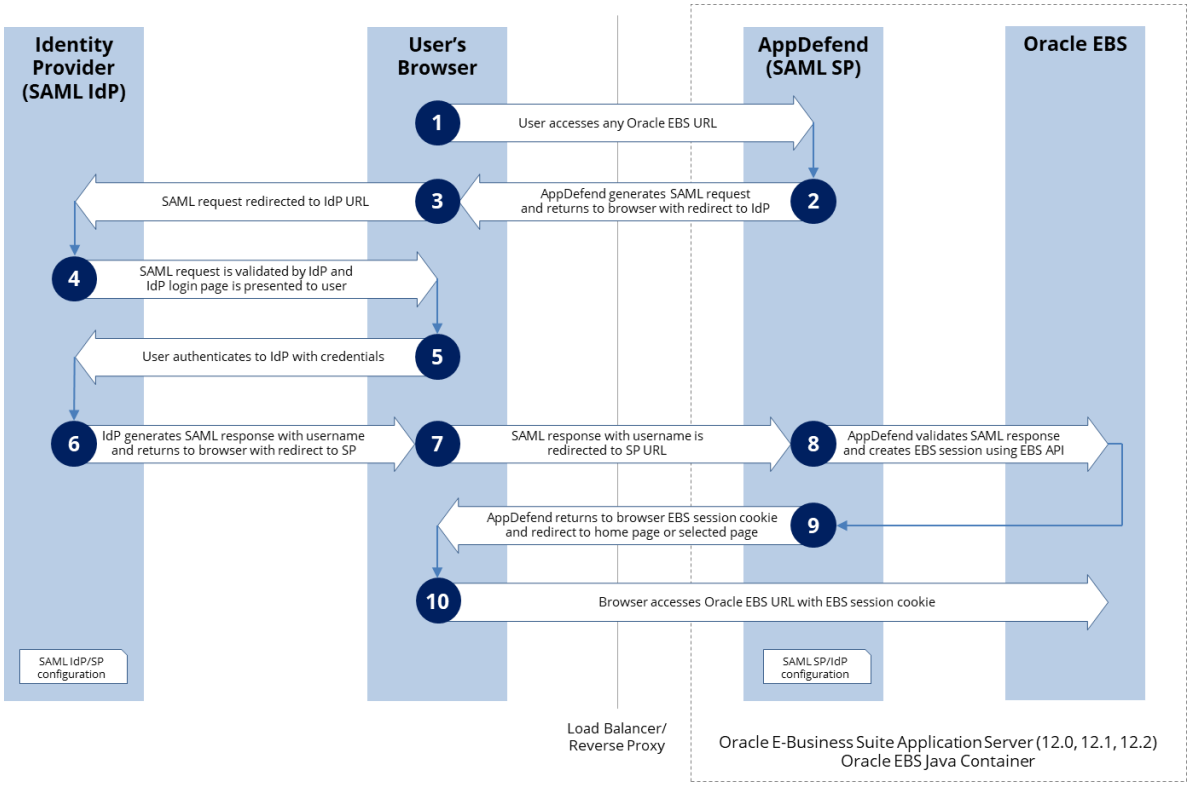
AppDefend SSO SAML Flow (EBS SSO Configuration)



AppDefend SSO SAML Flow (SSO Homepage)



AppDefend SSO SAML Security



1

- AppDefend protects access to all Oracle EBS URLs
- Must be authenticated to access any URLs except specific pages such as iStore or iSupplier registration

2

- SAML request is signed (SHA-512 if supported by IdP) and encrypted (AES-256) using IdP public key
- SAML request should be communicated using TLS 1.2 or 1.3 based on your configuration

6

- SAML response is signed (SHA-512 if supported by IdP) and encrypted (AES-256) using AppDefend public key

8

- AppDefend validates the integrity of the SAML response by decrypting using the AppDefend private key and verifying the signature against the IdP public key
- AppDefend prevents XML entity and schema attacks and by blocking entity tags and whitelisting schemas
- SAML replay attacks are prevented with a narrow expiration window, matching SAML request id for request and response as well as to JSESSIONID, and blocking already accepted assertions

9

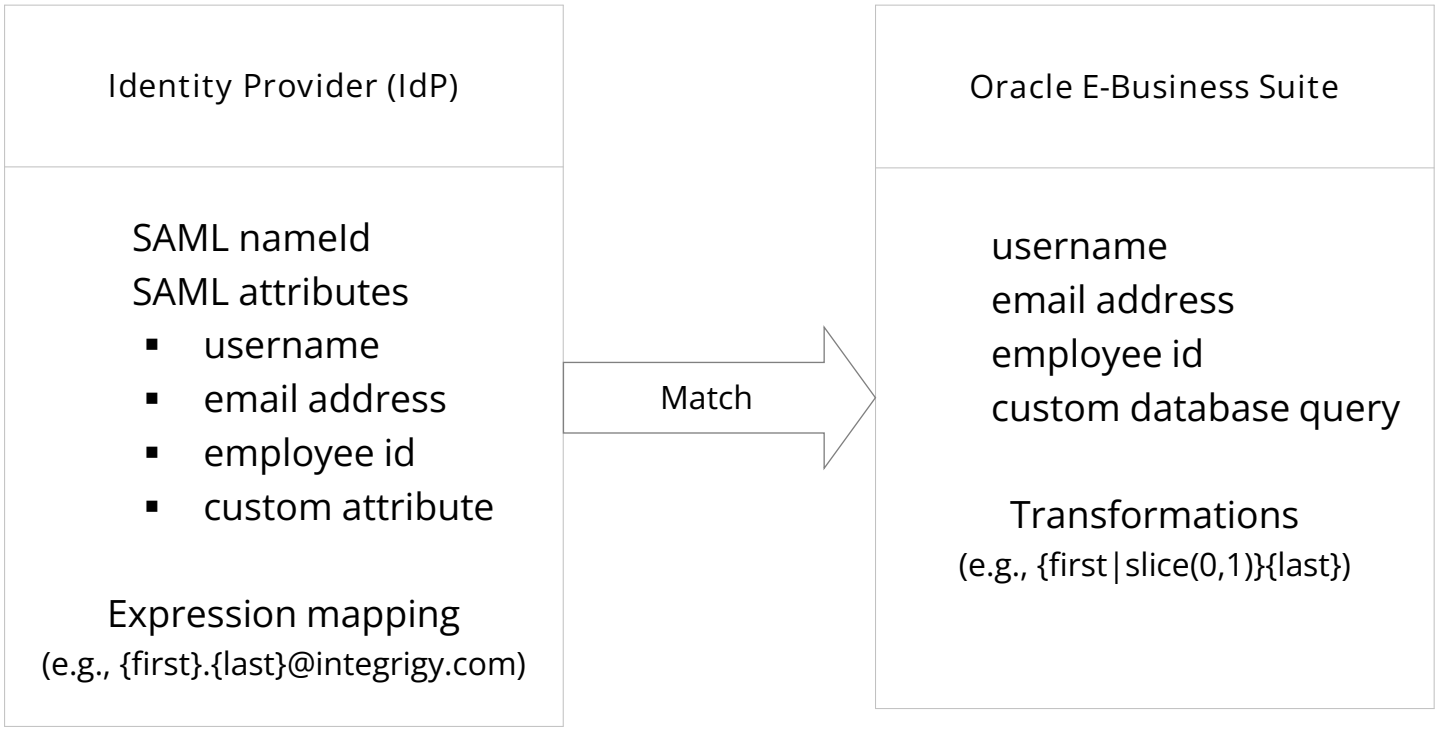
- AppDefend sets the Oracle EBS session cookie scope to host to prevent session hijacking
- All other Oracle EBS SSO solutions require session cookie scope to be set to domain which allows for potential session hijacking attacks

10

- AppDefend can maintain a mapping of EBS session cookies to IP address in order to prevent session hijacking attacks

AppDefend SSO SAML User Mapping

AppDefend can map Identity Provider user to Oracle E-Business Suite user using different attributes or values from both the Identity Provider and Oracle E-Business Suite. Multiple match rules can be defined and evaluated per login.

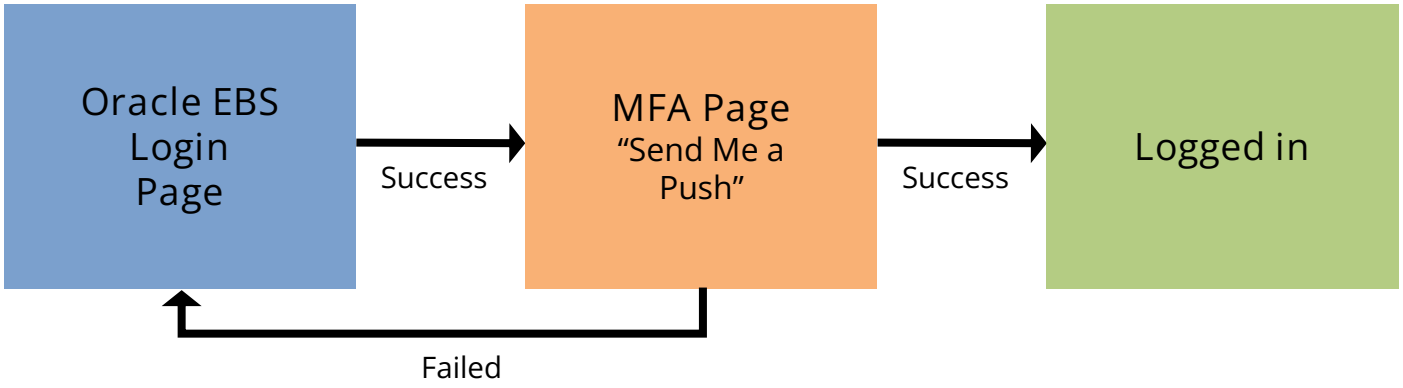


MFA Benefits

- Prevent fraud and phishing attacks
  - Two or more methods of identity verification makes account take-over harder
- Improve security
  - Enable strong authentication
  - Reduce risk of compromised passwords
- Improve compliance
  - PCI-DSS requires MFA required for access in some situations
  - GDPR, HIPAA, and other standards require strong authentication
- Contextualize authentication
  - MFA can be when specific data is accessed or actions performed like employee self-service direct deposit changes

AppDefend Adaptive Multi-Factor Authentication

AppDefend enables adaptive multi-factor authentication (MFA/2FA) for Oracle EBS using DUO Security, TOTP, SMS, email, or PKI (smartcards).



- Multi-Factor Authentication
  Enhances Oracle EBS login security by integrating with 2FA to provide secondary authentication
- Per Page, Responsibility, Function
  Require 2FA when user selects or accesses specific pages, responsibilities, or functions through menus or directly

AppDefend Two-Factor Authentication

- Application-aware
  - 2FA for login, user, responsibility, function, or page
  - Multiple 2FA authentications can be configured for different use cases and controls
- Context-aware
  - 2FA may be triggered based on session context such as time, location, device, etc.
- Single 2FA request per application session
  - 2FA authentications only when required
- Enhanced logging and audit trail for all authentications
- Supports local EBS authentication or single-signon
- No additional hardware or single point of failure

Two-Factor Authentication Use Cases

- Entire Application
  - Require 2FA when logging into Oracle EBS
- Privileged Responsibilities
  - Require 2FA when user accesses specific responsibilities like System Administrator
  - Protect highly privileged responsibilities from malicious use
- Privileged Users
  - Require 2FA when highly privileged users like SYSADMIN login
  - Preventative control for privileged, generic users accounts for SOX compliance
  - Limit access to generic user accounts by 2FA devices
  - Audit trail of named users accessing generic user accounts
- High Risk Functions or Pages
  - Require 2FA when user access specific functions or pages
  - Prevent fraud by requiring 2FA when user accesses self-service HR bank accounts

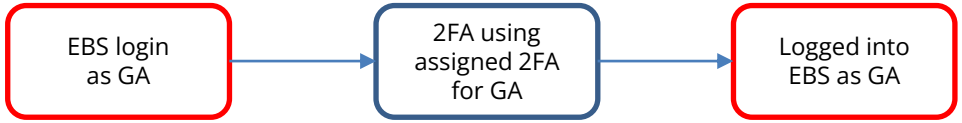
AppDefend MFA

AppDefend provides contextual multi-factor authentication for logins (SSO and non-SSO users, responsibilities, pages, and/or functions. MFA options are Duo Security, TOTP, SMS, and PKI (smartcards).

	Contextual Multi-factor Authentication			
	SSO User Login	Non-SSO User Login	Responsibility	Page/Function
AppDefend MFA (with or without SSO SAML)	✓	✓	✓	✓
AppDefend SSO SAML with IdP MFA	✓			
Legacy Oracle EBS SSO (such as OID/OAM or Oracle IDCS)	✓			

AppDefend Generic Account Protection

AppDefend MFA can be used to protect Oracle E-Business Suite privileged, generic accounts (GA), such as SYSADMIN. Multiple options to protect generic accounts and a different option may be used for each generic account.

Generic Account MFA Options	MFA Flow
1. SSO Named User profile option and/or authorized user list	
2. FND_USER Named User profile option and/or authorized user list	
3. MFA Solution such as DUO authorized in MFA solution	
4. Identity Provider (IdP) Direct authorized in IdP to access GA	

AppDefend Generic Account Protection Example Scenarios

A client with about 30 generic accounts used for various purposes configured AppDefend MFA to protect the generic accounts. Scenarios for one generic account to many named users, many generic accounts to one named user, and many generic accounts to many named users can all be easily configured and maintained. All logins including named user are monitored and logged.

Type of Generic Account	Generic Accounts	**MFA and AppDefend Configuration**
SYSADMIN	SYSADMIN	▪ Tile in IdP ▪ Assigned by IdP group ▪ Tightly controlled, limited to DBAs ▪ SYSADMIN password not known by DBAs
Job Scheduling	10 accounts, one per module, such as GL_JOB	▪ One AppDefend rule for all 10 accounts ▪ Access controlled using both an authorized user list (DBAs) and profile option set per named user (operations team)
Maintenance/Setups	12 accounts, one per module, such as GL_SETUP	▪ One AppDefend rule for all 12 accounts ▪ Access only allowed if AppDefend EBS maintenance feature is enabled ▪ Access controlled using profile option set per named user
Upgrade/Patch Test	6 accounts, such as TEST1	▪ An AppDefend rule for each of the 6 accounts ▪ Access controlled using profile option set per named user and DBA team sets prior to testing as testers will change based on the patches applied ▪ AppDefend logging enabled for these accounts to capture all activity

Agenda

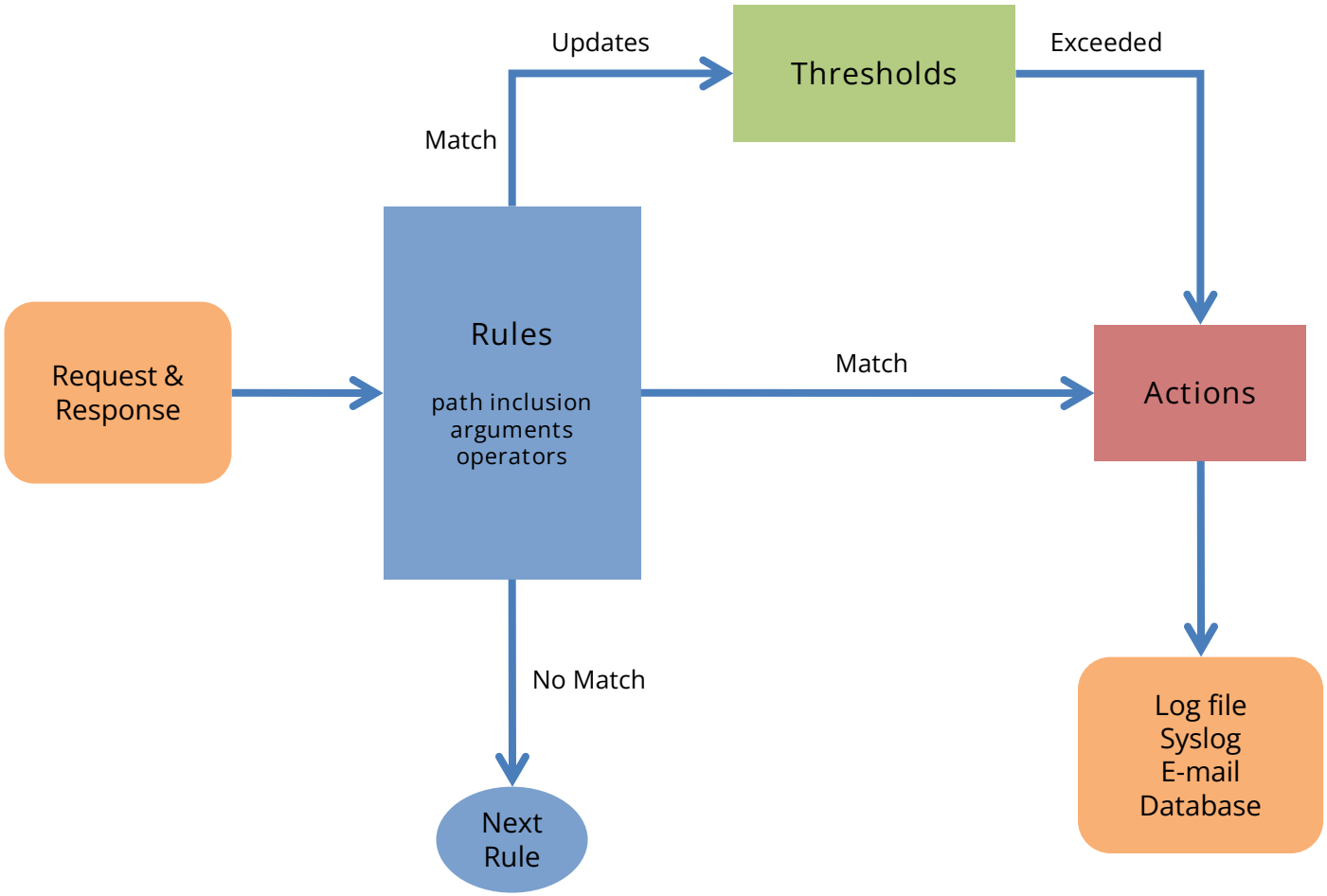
1. AppDefend Overview
2. Application Protection and Defense
3. Application SSO and MFA
4. **AppDefend Features**
5. Q & A

Application Logging and Auditing

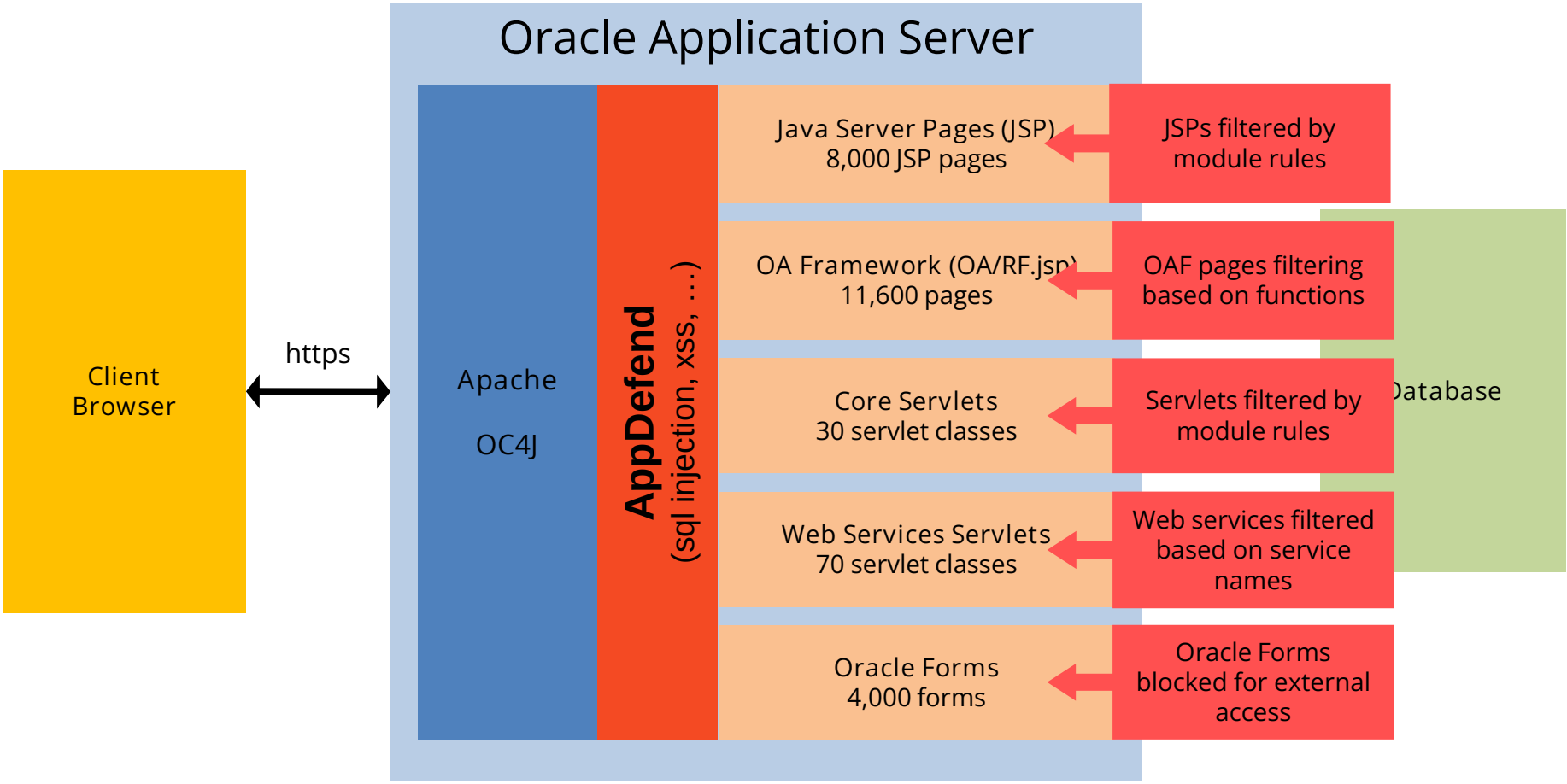
Log and audit key application and security events beyond Oracle EBS current capabilities

- Any page, action, parameter, session attribute may be logged or audited
- PCI logging includes all sessions, responsibilities, and potentially card number access through the application
- Log data can be sent to external systems such as Splunk, ElasticSearch, ArcSight, QRadar, LogRhythm, Microsoft Sentinel, AWS CloudWatch, …
- Solves gaps in Oracle EBS logging such as IP address for failed logins

AppDefend Processing



AppDefend Permit Rule



AppDefend allows access to only permitted Oracle EBS modules based on a group of white-listed modules. Individual files may be permitted also. Web page and OA Framework customizations are supported.

AppDefend Arguments

AppDefend rules and alerts may use one or more of these arguments.

- ebs.function_id
- ebs.function_id_all
- ebs.function_name
- ebs.resp_id
- ebs.resp_name
- ebs.user_id
- ebs.user_name
- ebs.user_signon_name
- request.attribute.<name>
- request.attributes.names
- request.auth_type
- request.body_length
- request.character_encoding
- request.content_length
- request.context_path
- request.cookie.<name>
- request.cookies.names
- request.file_extension
- request.file_name
- request.header.<name>
- request.headers.names
- request.is_secure
- request.line
- request.local_addr
- request.local_port
- request.method
- request.parameter.<name>
- request.parameters.combined_size
- request.parameters.get_names
- request.parameters.get_values
- request.parameters.names
- request.parameters.put_names
- request.parameters.put_values
- request.parameters.values
- request.path_info
- request.path_translated
- request.protocol
- request.query_string
- request.remote_addr
- request.remote_host
- request.remote_port
- request.remote_user
- request.scheme
- request.server_name
- request.server_port
- request.servlet_path
- request.servletcontext.<name>
- request.session_id
- request.uri
- request.url
- response.content
- response.content_length
- response.header.<name>
- response.header.names
- session.attribute.<name>
- session.attributes.names

AppDefend Operators

AppDefend rules can use any of these operators.

- beginswith
- byterange
- contains
- notcontains
- endswith
- equals
- exists
- greater
- greatereq
- ingroup
- notingroup
- inlist
- notinlist
- ipmatch
- notipmatch
- less
- lesseq
- regex
- within
- notwithin

AppDefend Actions

Log	Generates a log entry or alert to a file, syslog, e-mail
Redirect	Redirects the request to a specified full URL or relative URL for the site such as the Oracle EBS error page
Block	Block the request by returning the specified HTTP error code such as 403 Forbidden
Pause	Pause the request for the specified number of milliseconds perhaps to slow down a brute force attack
Sanitize	Sanitize one or all parameters and headers in the request to prevent XSS, HTML injection, or SQL injection
Stop	Stop the processing of all subsequent AppDefend rules. The Stop action is useful to minimize AppDefend analyzing static request such as images, etc.
DoNothing	This action will do nothing as an action

Agenda

1. AppDefend Overview
2. Application Protection and Defense
3. Application SSO and MFA
4. AppDefend Features
5. Q & A

Integrigy Contact Information

Integrigy Corporation

web – www.integrigy.com

e-mail – info@integrigy.com

blog – integrigy.com/oracle-security-blog

youtube – youtube.com/integrigy