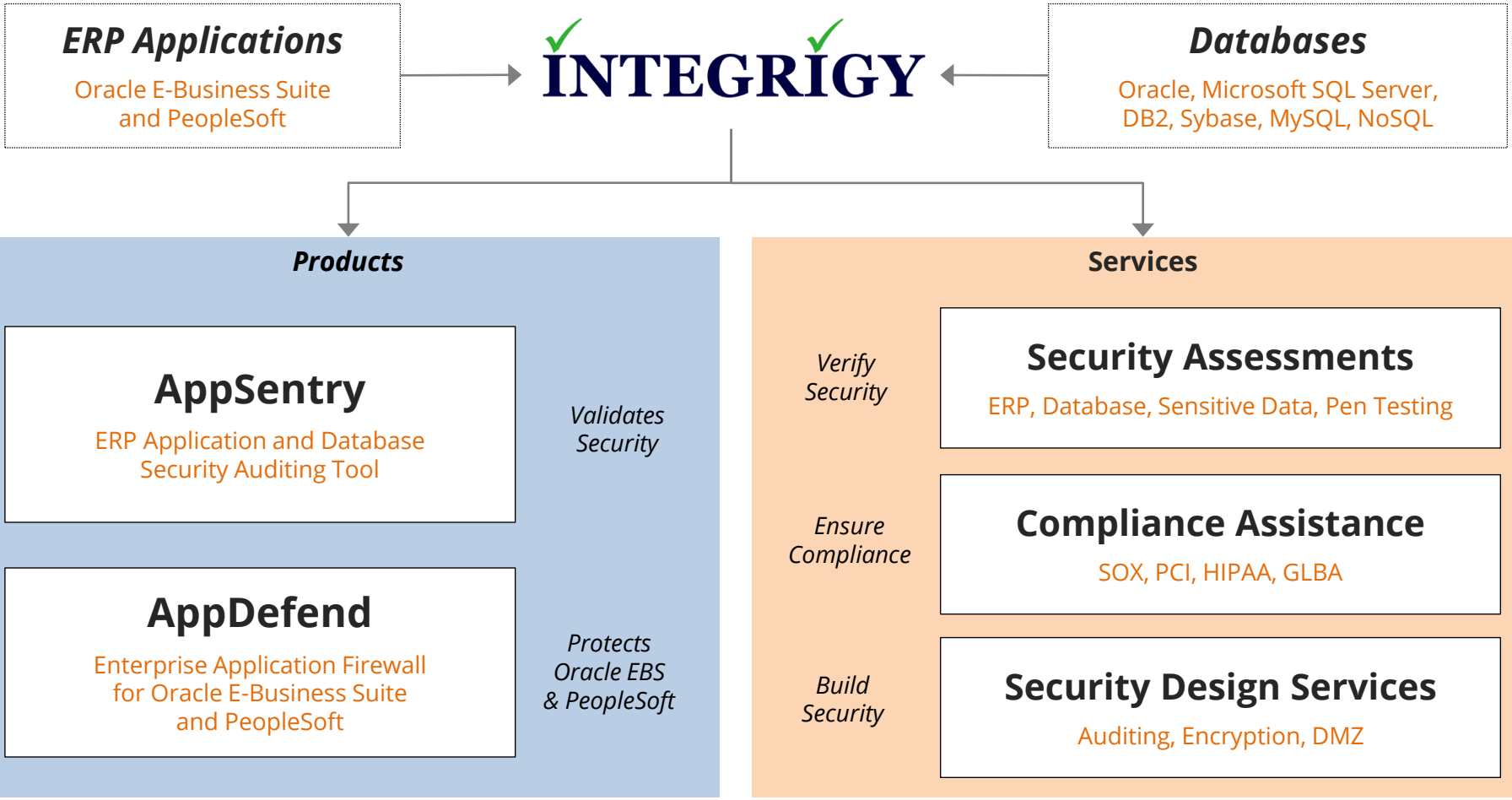

# Implementing Two-Factor Authentication (2FA) for Oracle E-Business Suite

October 15, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

# About Integrigy




## Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

# Definitions

## Multi-Factor Authentication (MFA)

Access control method in which a user is only granted access after successfully presenting two or more pieces of information or data (factors) to an authentication mechanism

## Two-Factor Authentication (2FA)

2FA is a subset of MFA where only two factors are required such as a password and a hardware token

## Factors

Pieces of information or data such as –

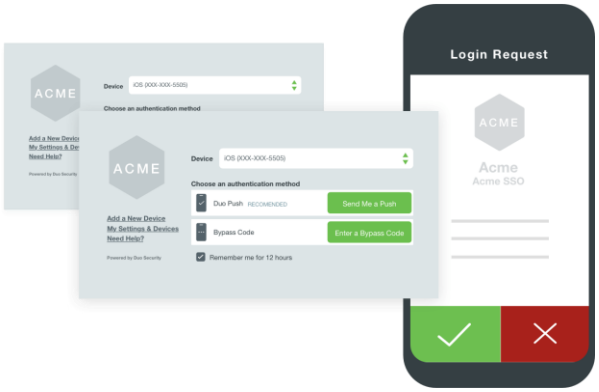
- Knowledge = something you know like a password
- Possession = something you have like a hardware token or device
- Inherence = something you are like a biometric such as a fingerprint

# Typical Factors

| | |
|---|---|
| **OTP** | ▪ One-time password or passcode |
| **TOTP** | ▪ Time-based one-time password or passcode |
| **Mobile App OTP/TOTP** | ▪ Password from mobile app |
| **Mobile App Push** | ▪ Prompt on mobile device such as phone or smart watch |
| **Mobile App Biometric** | ▪ Mobile app requires fingerprint |
| **SMS OTP/TOTP** | ▪ Password delivered via SMS |
| **Universal 2nd Factor (U2F)** | ▪ USB key with push button |
| **Hardware Token** | ▪ Passcode generated on physical token |
| **Email OTP/TOTP** | ▪ Password delivered via email |
| **Bypass Codes** | ▪ Predetermined codes to be used in case of device loss |

# Example Factors

1




2


3


4

# Popular Two-Factor Authentication Solutions

| | |
|---|---|
| **Duo Security** | ▪ Mobile app, hardware token, U2F, biometrics, SMS, phone call, … |
| **RSA SecurID** | ▪ Hardware and software tokens |
| **Okta Adaptive MFA** | ▪ Mobile app, hardware token, U2F, biometrics, SMS, phone call, … |
| **Symantec VIP** | ▪ Mobile app, hardware token, U2F |
| **Ping Identity MFA** | ▪ Mobile app, hardware token, U2F, biometrics, … |
| **Microsoft Authenticator** | ▪ Mobile-based with Azure AD integration |
| **Google Authenticator** | ▪ Mobile-based and application-level |

# Oracle E-Business Suite and Two-Factor Authentication

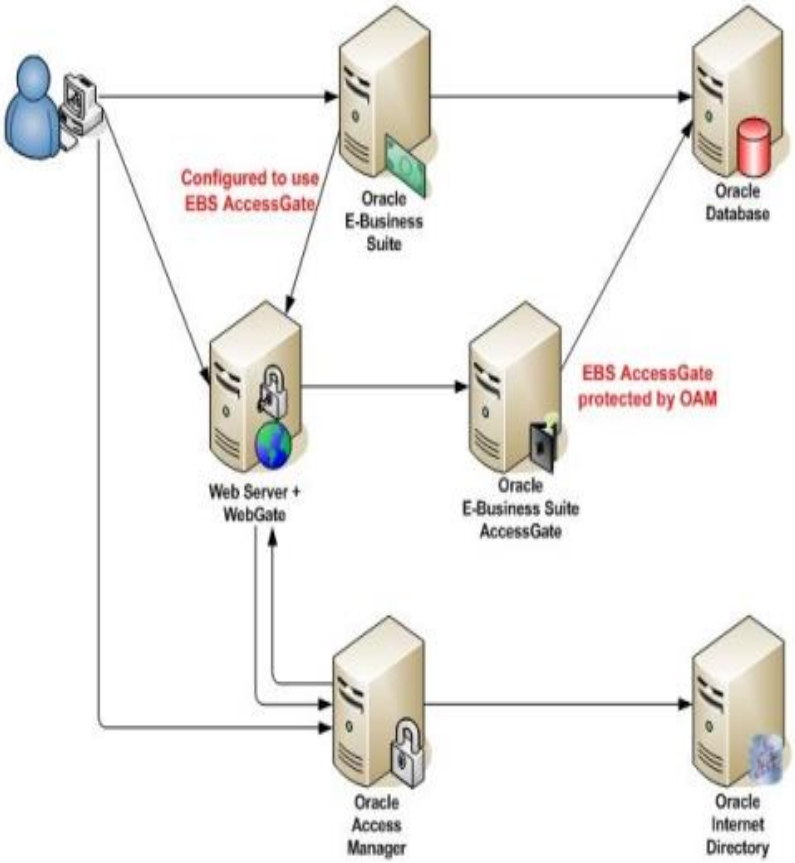
- 2FA is not supported natively by Oracle EBS

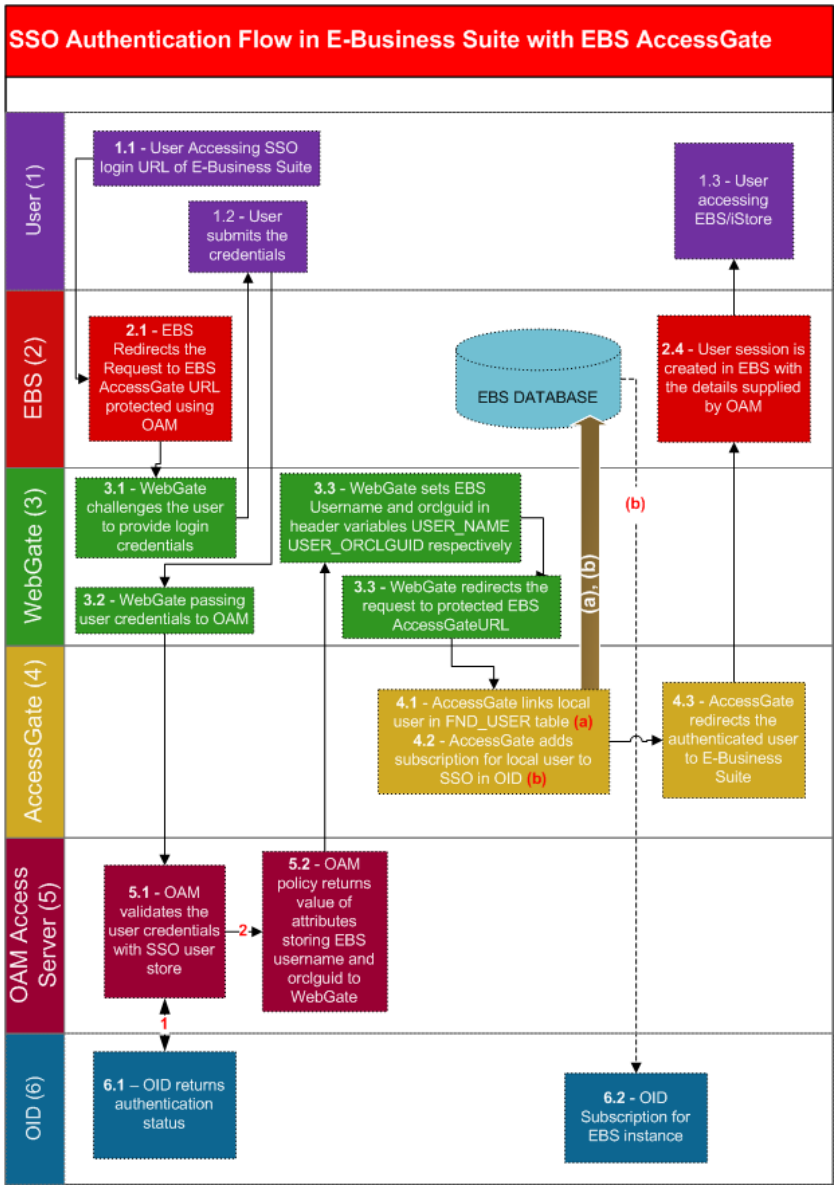
- 2FA requires implementation of an identity management solution
- Uses Oracle EBS Access Gate to integration to identity management
- Redirects from EBS login page to identity management login page

# Oracle EBS 2FA Solutions

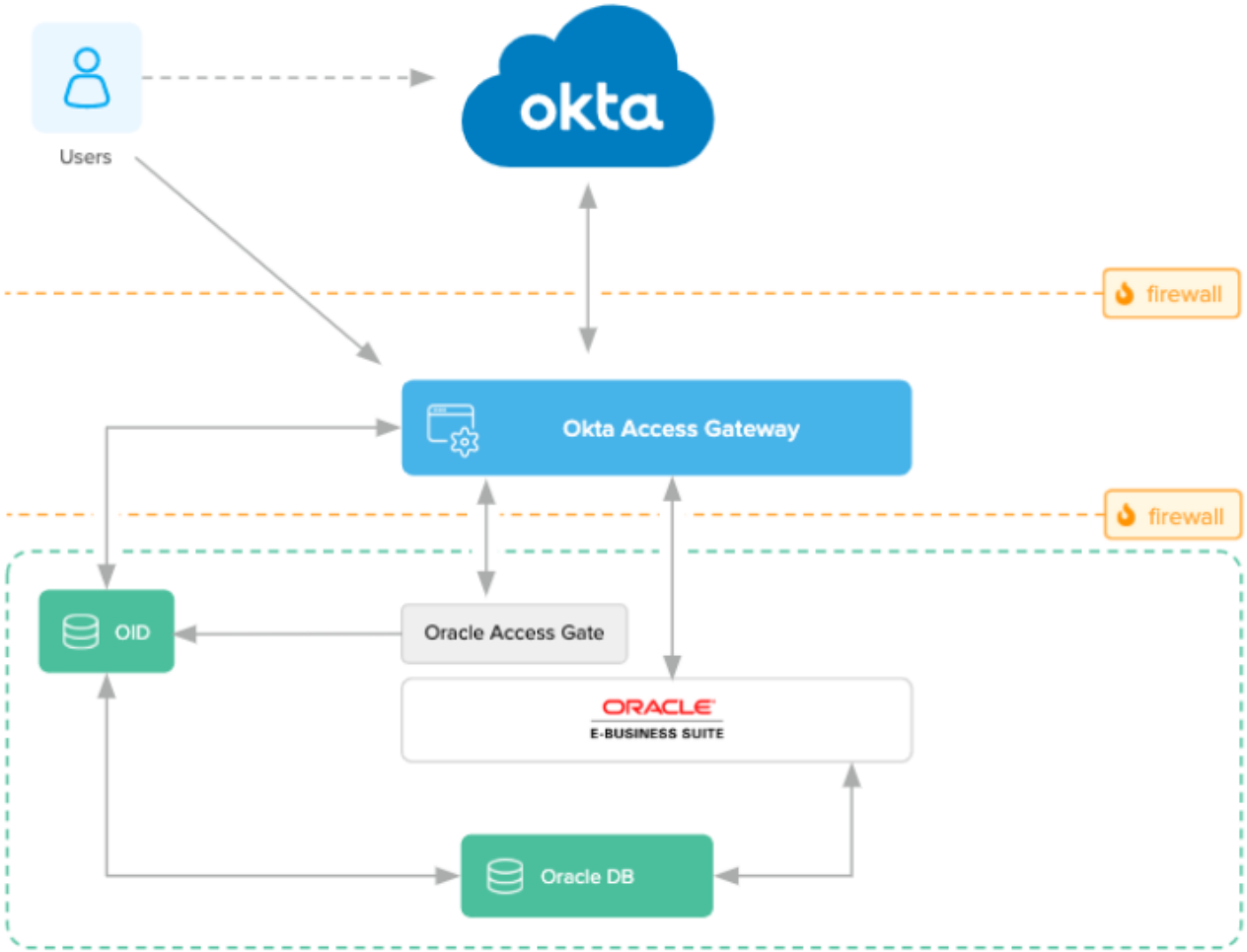
| | |
|---|---|
| **Oracle Access Manager** | ▪ Oracle SSO solution for Oracle EBS<br>▪ Requires Oracle Internet Directory or Oracle Unified Directory<br>▪ MFA using Oracle Mobile Authenticator, SMS, email, … |
| **Oracle Identity Cloud Service** | ▪ Cloud-based authentication, SSO, and MFA solution<br>▪ Integrates with Oracle EBS using EBS Asserter |
| **Okta** | ▪ Cloud-based authentication, SSO, and MFA solution |
| **SSOgen** | ▪ Integration solution between Oracle EBS and other identity management such as Active Directory, Azure AD, Siteminder, OpenID, … |
| **Integrigy AppDefend** | ▪ 2FA integration solution that protects Oracle EBS including users, responsibilities, functions, and pages |

# Oracle Access Manager for Oracle EBS



# Okta for Oracle EBS

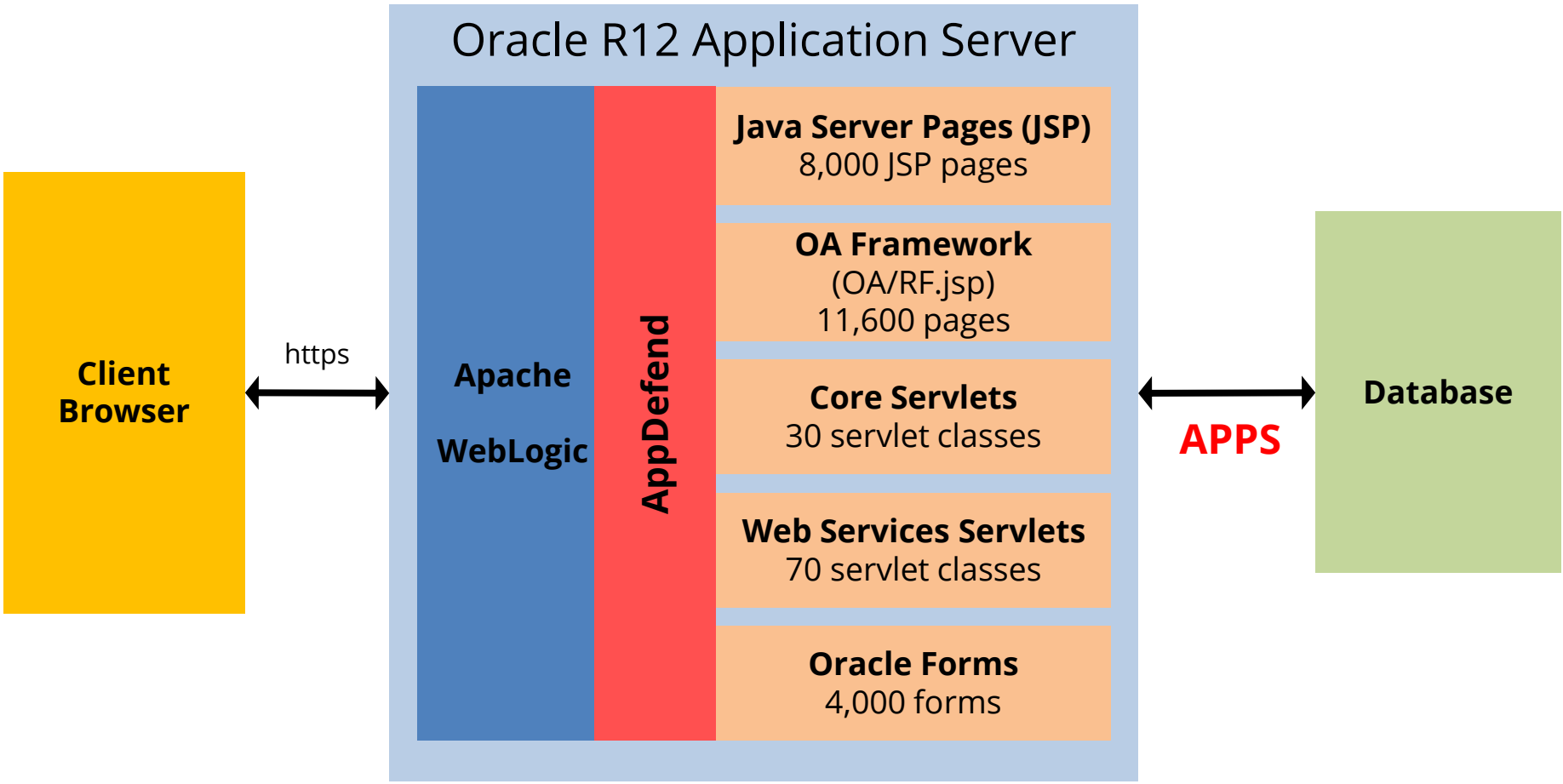


# Integrigy AppDefend

**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
- **Application Logging**
  Enhanced application logging for compliance requirements like SOX, GDPR, PCI-DSS 10.2
- **Two-factor Authentication (2FA)**
  Enables two-factor authentication for login, user, responsibility, or function
- **Limits EBS Modules**
  More flexibility and capabilities than URL firewall to identify EBS modules
- **Protects Web Services**
  Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST)
- **Protects Mobile Applications**
  Detects and reacts to attacks against Oracle EBS mobile applications

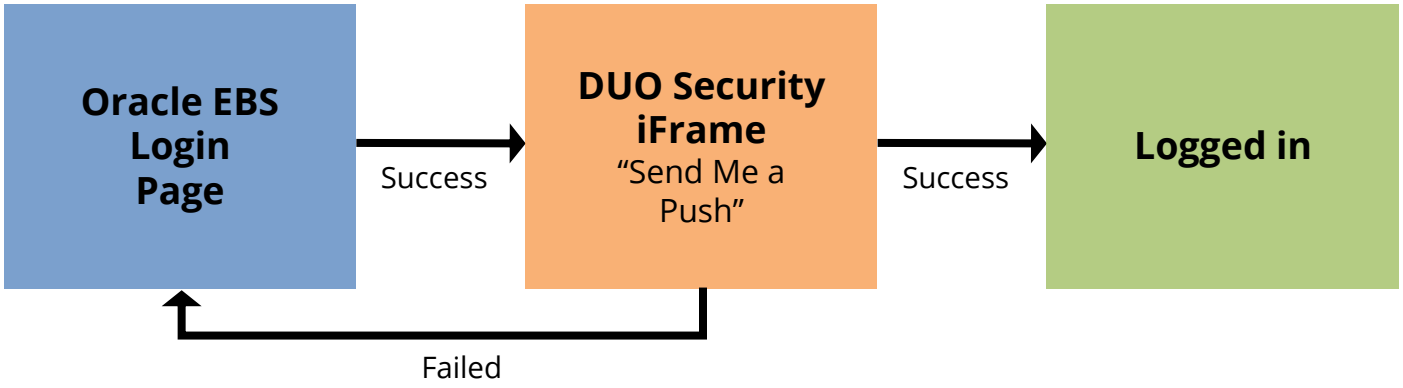
# AppDefend and Oracle EBS 12.2




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

# AppDefend Two-Factor Authentication

**AppDefend** enables two-factor authentication (2FA) for Oracle EBS popular MFA solutions such as DUO Security.




- **Two-Factor Authentication**
  Enhances Oracle EBS login security by integrating with DUO Security to provide secondary authentication
- **Per User, 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

# Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**

Copyright © 2020 Integrigy Corporation