ORACLE DATA SHEET

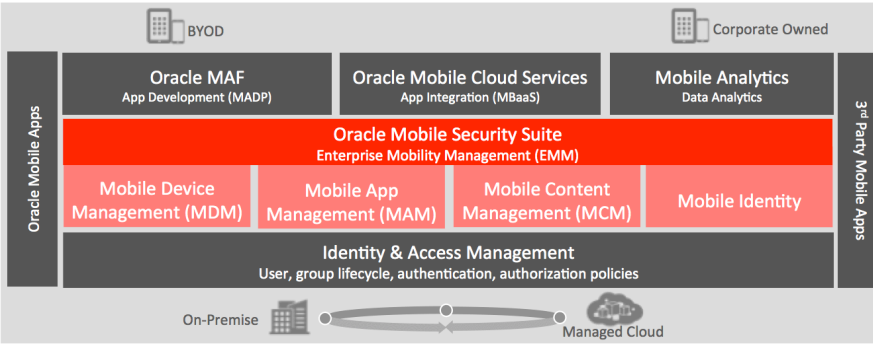
Oracle Mobile Security Suite (OMSS)

ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

With the proliferation of mobile devices there is a strong need for enterprises to secure corporate resources from these less secure access points. While encouraging BYOD (Bring Your Own Device) model, many organizations still benefit from issuing corporate owned devices for their employees, enabling personal or corporate only use. Oracle Mobile Security Suite provides a comprehensive Enterprise Mobility Management (EMM) solution that can address a mix of both BYOD and corporate owned models without compromising security, user experience or privacy. This best in class EMM solution enables organizations to easily move to a "Mobile First" strategy as part of the complete Oracle Mobile Platform, to build feature rich, cross platform, integrated apps and leverage an advanced and industry leading Oracle Identity and Access Management solution for securing corporate access.

KEY FEATURES

- Comprehensive set of device and app level security policies providing strong authentication, encryption, DLP and device controls for iOS and Android devices
- App Tunnel that eliminates need for mobile VPN and protects from rogue apps
- Hybrid Single Sign-on (SSO) with Integrated Windows Authentication (Kerberos and NTLM) and Oracle IDM (OAuth, SAML, OAM)
- Unified Self Service and Administration consoles with Oracle IDM
- Secure productivity apps included for mail, calendar, browser, file manager, doc editor
- No code change app containerization to easily secure custom and 3rd party apps



Oracle Mobile Security Suite – A platform for value added mobile services

Mobile Device Management

OMSS secures corporate owned devices by enforcing device restrictions that conform to corporate security policies and providing remote controls to manage the device. Device management includes self-service device enrollment with enterprise authentication, automated provisioning and removal of corporate profiles, settings apps and certificates. Device restriction policies ensure non-compliant devices are detected continuously and are remediated to protect corporate data. Device controls are performed over-the-air allowing remote selective or full wipe, device lock/unlock as well

ORACLE

KEY BENEFITS

- **Superior user experience:** Increase effectiveness of touch-enabled devices. Separate corporate data from personal without needing a device-level PIN or VPN. Enable single sign on between mobile apps and secure offline access to data without caching passwords on the device.
- **Regain security control:** Enforce a wide range of corporate authentication and data leakage policies. Wipe or lock only the corporate workspace when needed.
- **Accelerated mobile app deployment:** Apps adhere to security policies via zero code change wrapping. Support for multiple app development platforms like native, MAF, PhoneGap, Xamarian, Cordova and Worklight
- **Enable Mobile Transformation:** Enable business to transform via mobile by removing security objections and concerns.
- **Reduced costs:** Reduce IT costs through efficient, unified self-service and administration as part of corporate IDM infrastructure.

as reset device passcode. It also provides a data rich device and app inventory that can be used to build a wide variety of reports using BI Publisher.

Mobile Application Management

App Catalog

An intuitive app catalog that enables administrators to onboard and scope apps available to various user groups. Users can view and install available apps from the Secure Workspace and get notified of any app updates.

App Containerization

A toolset to inject security functionality for native, 3rd party or custom apps with zero code changes. These containerized apps can then be deployed in the OMSS app catalog, distributed to the Secure Workspace based on policies and configured to share content, authentication, encryption keys, policies and participate in SSO between apps without ever needing to cache the password in the device.

Mobile Content Management

Secure Workspace

The container app that ensures security by isolating personal from corporate data and apps. Provides authentication, Single Sign-on and FIPS 140-2 encryption. Offers wide variety of data leakage prevention policies to ensure data does not leave the corporate workspace.

App Tunnel

An app level SSL tunnel ONLY from the Secure Workspace, which eliminates the need for device-level VPN and risk of rogue apps. Supports role based authorization and SSO authentication via Kerberos or NTLM protocols utilizing username/password or PIN-protected, PKI certificates.

Secure Workspace Apps

A set of enterprise ready productivity apps that ensures corporate data is always protected. Embedded apps include a secure web browser to access Intranet or HTML5 apps, a file manager to access network file shares like Oracle Document Cloud Service, Oracle WebCenter Content, Windows File System or SharePoint, a document editor to enable viewing and simple editing on the go for Office files and an add-on Oracle Secure Mobile Mail Manager that is a secure native app for Email, Calendar, Contacts, Tasks and Notes. This client supports any ActiveSync mail server including Exchange, Google Apps and Lotus Notes.

Mobile Identity

OMSS leverages and extends advanced security functions provided by existing Identity and Access Management infrastructure for mobile access, enabling governance and compliance for enterprise mobile. OMSS leverages common users, roles, policies, access request, self service and delegated admin consoles; enables authentication and SSO from apps and browser; supports Kerberos, SAML 2.0, OAuth and NTLM protocols using Microsoft AD and/or Oracle IDM; supports strong authentication using PKI, context based/risk aware step up and certificate-based authentication; provides lifecycle management for device certificates provisioned during device enrollment.

ORACLE

CONTACT US

For more information about Oracle Identity Governance visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Hardware and Software, Engineered to Work Together

Oracle is committed to developing practices and products that help protect the environment