Oracle SaaS Cloud Platform Architecture

WHITE PAPER / MAY 20, 2018

ORACLE

DISCLAIMER

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 Oracle's products remains at the sole discretion of Oracle.

Table of Contents

INTRODUCTION

The Oracle Software as a Service (SaaS) Cloud Applications are a complete suite of capabilities spanning Enterprise Resource Planning, Human Capital Management, Customer Experience and Supply Chain Management. They have been designed and built from the ground up using the latest technologies and are deployed in state-of-the-art data centers around the globe.

This white paper describes the Oracle SaaS Cloud Platform Architecture and how it is deployed.

TECHNOLOGY FOUNDATION

The Oracle SaaS Applications are based on a Service Oriented Architecture and use a common data model. They are built on Oracle Fusion Middleware and the Oracle Database using industry-standard languages, including Java, XML, HTML, SQL and BPEL.

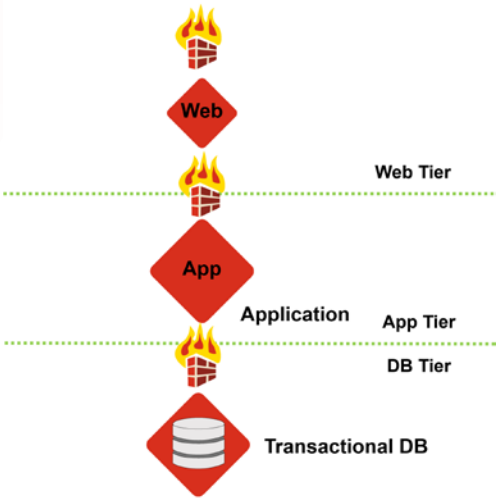


Figure 1. High Level Architecture

There are three tiers in the Oracle Application Cloud. The first is the Web Tier, where transactions are received, authentication takes place, and the load across all instances is balanced and routed. The next is the Application Tier containing the applications processes and policies as well as the middleware that enables customers to manage business processes, integrations, reports, and generally run the applications and middleware. And finally, the Data Tier which provides support for the database container that the customer uses to store their data.

Oracle is unique in the marketplace in that the entire deployment stack from hardware through to the applications is owned, developed and managed by Oracle.

POWERED BY ORACLE FUSION MIDDLEWARE

Oracle Fusion Middleware is the engine behind the Applications.

Fusion Middleware Components

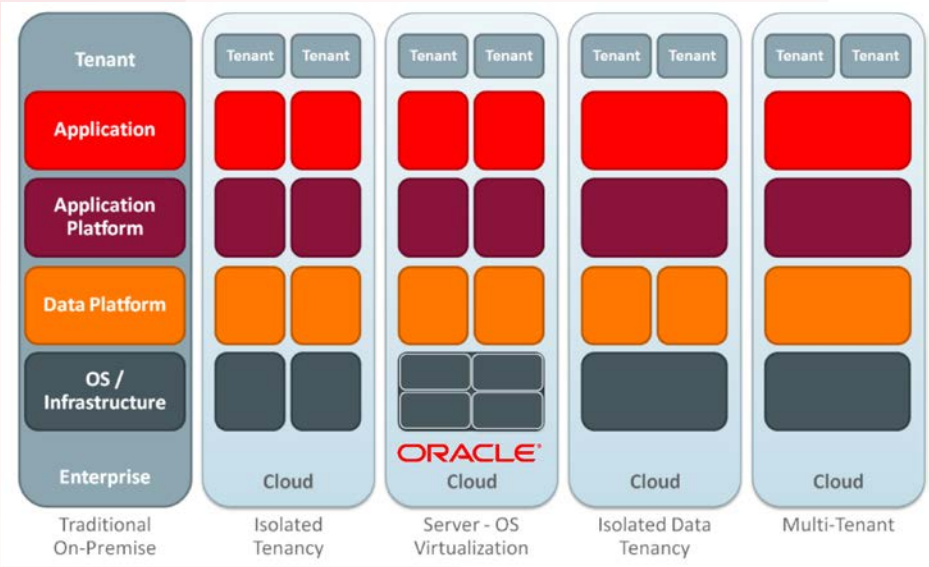
COMPONENT	DESCRIPTION
Oracle WebLogic Server	Oracle WebLogic Server provides the scalable, enterprise-ready application server based on Java Enterprise Edition (Java EE) that forms the core of the deployment architecture.
Oracle SOA Suite	Oracle SOA Suite Provides a complete set of service infrastructure components for designing, deploying, and managing SOA composite applications.
Oracle WebCenter Portal and Content	Oracle WebCenter Portal Provides design-time and runtime tools for configuring pages and displaying content. Oracle WebCenter Content enables file and document management.
Oracle Business Intelligence	Oracle Business Intelligence provides a full range of business intelligence capabilities that enable you to analyze, present, report, and deliver organizational data. This includes both BI Answers for detailed analysis and BI Publisher which provides report publishing.
Oracle Enterprise Manager	Oracle Enterprise Manager provides built-in applications management, integrated application to disk management, integrated systems management
Oracle Identity Management	Oracle Identity Management provides the authentication and authorization framework for the applications.

No Single Points of Failure: Architected for High Availability and scalability.

These building blocks are combined in the Application tier to create a redundant architecture with no single point of failure. The enterprise deployment of Oracle Fusion Middleware makes use of multiple clustered managed servers to provide the infrastructure of the applications. This architecture also allows the applications to scale across all tiers.

VIRTUALIZED ISOLATED TENANCY

The tradition model of SaaS deployment makes use of a multi-tenant architecture where multiple customers share the same database and binaries. Isolation is effectively provided through data striping. While this represents obvious cost savings for the SaaS vendor, this model provides few tangible engineering benefits for the end customer. The diagram below shows the major variants found for cloud tenancy; from the traditional on-premise deployment through to legacy multi-tenant and Oracle's own virtualized isolated tenancy.



Customer data is always isolated.

Figure 2. Cloud Tenancy Comparison

Oracle has deliberately broken with tradition and offers a virtualized isolated tenancy deployment where customers each have their own:

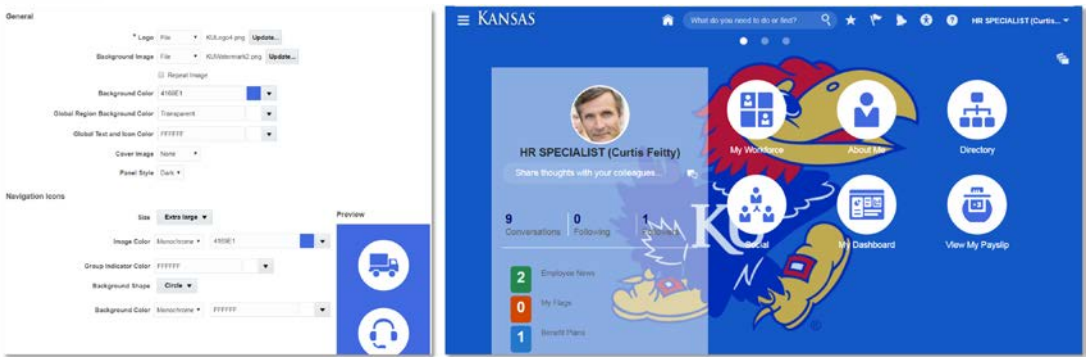
- database
- virtualized middle tier

There is no co-mingling of data between customers.

This provides a number of benefits including the ability to provide private encryption keys, deeper configuration capabilities and minimization of the “noisy neighbor” effect found in conventional multi-tenant architectures.

CONFIGURATION AND TAILORING

Changes that can only be made through invasive customizations in other systems are configurations in the Oracle SaaS Applications. Deep configuration is supported through the capabilities of the underlying Oracle Fusion Middleware platform.



Configured, not “Coded”

Figure 3. Branding: Left - configuration screen; Right – branded page

Users are able to personalize or tailor their UI experience by selecting which springboard icons and infolets they want to appear. They can build their own dashboards (display reports/analytics, iFrames, videos, hyperlinks, etc.). Users can of course also set favorites for transactions or pages they access most frequently.

Administrators, on the other hand, are able to create and modify springboard icons and infolets. With the additional privileges they are assigned, administrators can manage themes, including logo, background, color scheme, and search and replace for text lingo. Administrators are also able to add user-defined fields to the various pages of the application. These are called “flexfields” and allow the applications to be configured to capture additional information.

Responsive UI

In addition, administrators are able to manage page and field properties (including adding content to pages) and can make these configurations much more dynamic using expression language. They are then able to manage custom help topics based on these changes.

Infolets are used to provide an aggregate view of important information and analytics on intuitive tiles that call immediate attention to the end user; directly on their homepage.

End User Configuration Options:

- Show/hide springboard icons
- Show/hide infolets (Report “Blocks” that appear on pages)
- Build/modify dashboards
- Set favorites
- Setup user preferences

Administrator Configuration Options:

- Create/modify springboard icons
- Create/modify infolets
- Manage themes
- Add user-defined fields
- Configure page/field properties
- Manage custom help

Configurability also extends to reporting.

Oracle cloud also empowers end users to build their own ad-hoc analytics without IT intervention. The Applications provide a wizard-driven report builder which uses business-friendly terminology and allows end users the ability to quickly and easily build reports and share them across the enterprise.

End-Users are able to drag and drop columns onto their reports and select the tables and chart to be inserted. Using the wizard, prompts and sections can be added, followed by sorting, filtering and conditional formatting of the report. WYSIWIG preview provides visibility throughout the entire process.

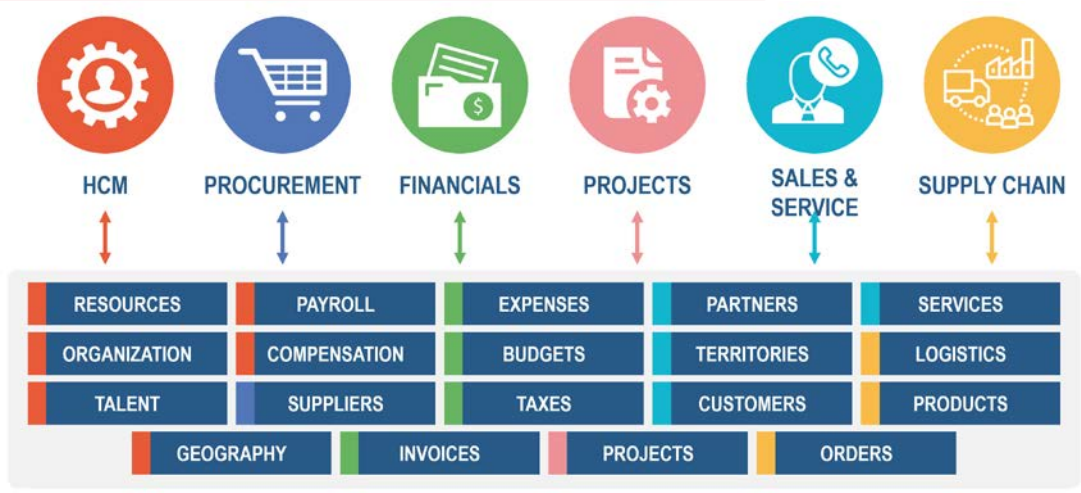
Built-in Reporting

Security is baked into the reporting tool meaning users will still only be able to see the data and functional areas that their role in the application permits.

UNIFIED DATA MODEL

Integration is arguably the most significant source of complexity and risk within enterprise architectures. Deploying your enterprise cloud solutions within a global single instance reduces the need to build and maintain integrations across the enterprise.

Oracle's modern cloud comes with delivered processes based on best practices and a shared data model that aligns business objects between your mission-critical business applications.



Global Single Instance Deployment: internally integrated applications reduce complexity, risk and cost.

Figure 4. Unified Data model

Internal integration is done through the use of shared data structures and internal web services.

INTEGRATION

Business organizations typically have a recurring need for the streamlined management of inbound and outbound data in areas such as initial data conversion, master data creation and maintenance, regular transaction processing, and fiduciary compliance. Oracle SaaS Cloud Applications offer a comprehensive collection of built-in tools and feature sets to meet these requirements. Integration scenarios generally involve system-to-system integration flows between distinct on-premise systems, third-party or legacy systems, and Cloud systems. These can be broken down into inbound and outbound data flows.

Inbound:

- Spreadsheet Loads
- Inbound REST and SOAP Web Services
- Excel Integration
- Bulk Data Loads
- Data Loader (Human Capital Management)

Outbound:

- Extracts
- XML, CSV, Excel Report formats

- Outbound REST and SOAP Web Services
- ATOM Feeds for Human Capital Management
- Events for Supply Chain

DEPLOYMENT

Data Centers

The facilities that house the Oracle SaaS Cloud Applications are built and managed by leading co-location vendors; all of which meet Oracle's strict criteria for service and infrastructure. All facilities meet the following criteria:

Construction, Power, and Cooling:

- Concrete, stone, and/or steel construction
- Redundant utility feeds
- Redundant UPS
- Redundant standby power
- Excess power capacity
- Cooling capacity that matches or exceeds power capacity
- Redundant ISPs

Leading Co-Lo providers such as Equinix

Physical Security:

- 24x7 human guards
- Secure ingress/egress always includes multiple levels of physical technology, including:
  - Man traps
  - Biometric scanners
  - Proximity card readers and identification badges
  - Audible alarms when security is breached
  - Access limited by defined access lists
  - Physical access logging
  - Cage space secured by physical key or hand scanner
  - Compulsory visitor escort
  - Closed circuit TVs and recorders

Disaster Recovery

Oracle maintains a Cloud DR Plan designed to protect customer productivity and Oracle's commitment to customer support in the event that all, or part, of its hosting operation is rendered "unusable". If a

disaster is declared, each primary site can be recovered at a disaster recovery data center. The RTO is 12 hours from the disaster declaration, and RPO is 1 hour, excluding any data loads that may be underway.

Oracle Cloud Services maintains a redundant and resilient infrastructure designed to maintain high levels of availability and to recover services in the event of a significant disaster or disruption. Oracle designs its cloud services using principles of redundancy and fault-tolerance.

Oracle Cloud Services provide an infrastructure that incorporates a comprehensive data backup strategy. The Oracle Cloud includes redundant capabilities such as power sources, cooling systems, telecommunications services, networking, application domains, data storage, physical and virtual servers, and databases.

DR is included

To support DR, Oracle has two separate data centers that function as primary and secondary sites. Customer's production standby (secondary site) environment will reside in a data center separate from Customer's primary site. Oracle will commence the disaster recovery plan under this policy upon its declaration of a disaster and will target to recover the production data and use reasonable efforts to re-establish the production environment at the secondary site. For a major regional jurisdictional area (e.g., the United States or the European Union), Oracle operates both a production and secondary site within that region. Customer data is replicated in physically separate facilities in order to restore services in the event of a disaster at a primary site. Backups are for Oracle's sole use in the event of a disaster.

Global Nerve Centers

Our state-of-the-art operation centers (GNCs) follow the sun 24 hours a day every day. We have three GNCs which are located in the United States (Montana), United Kingdom, and a third GNC in India (Bangalore). GNCs are staffed 24x7x365 and are connected to all production pods worldwide, providing up-to-the-minute visibility into components of the environment. Our GNCs are responsible for monitoring and ensuring stability of the pods and customer sites, managing customer events, and handling proactive communications with customers.

Detection and prevention capabilities are marked by a dedicated 24x7x365 team of database and systems administrators at each GNC, and hand-offs between GNCs are both written and verbal at the end of every shift. Multiple individuals on the Operations Team have U.S. government clearance to support government sites.

Networking

In addition to the highly available horizontal scale deployment architecture, the applications have been designed and coded to run efficiently in the Cloud.

The applications leverage modern Cloud coding practices such as Partial Page Rendering where sub-sections of a page can be refreshed in response to user actions rather than re-rendering the entire page. Additional features such as No Blind Searches, Chunking of Search Results, and Chunked Report Results help to optimize network bandwidth requirements.

The result of 500 concurrent users at 1.70 Mbit/sec is a good approximation and can be used by implementation and IT teams to estimate their network bandwidth requirements. The numbers are linear with increased or decreased user load.

Oracle Cloud Services can leverage Akamai CDN (Content Delivery Network) as a way to optimize the delivery of static and dynamic content. In particular, Akamai servers deliver several types of content: static and dynamic content over HTTP and HTTPS, as well as streaming audio and video over major streaming protocols.

Akamai deploys their CDN servers across the globe and will automatically route HTTP and HTTPS requests to the server location closest to the users' network location, minimizing the network latency for delivering the content.

SECURITY

Defense in Depth

Oracle's approach to securing our applications and their deployment follows a Defense in Depth Strategy. This strategy builds upon our unique capabilities such as full stack ownership as well as the adoption and development of industry and internal best practices, standards and certifications. The diagram below summarizes the measures taken at each layer of the deployment.

Defense in Depth spans physical plant, procedures and software.

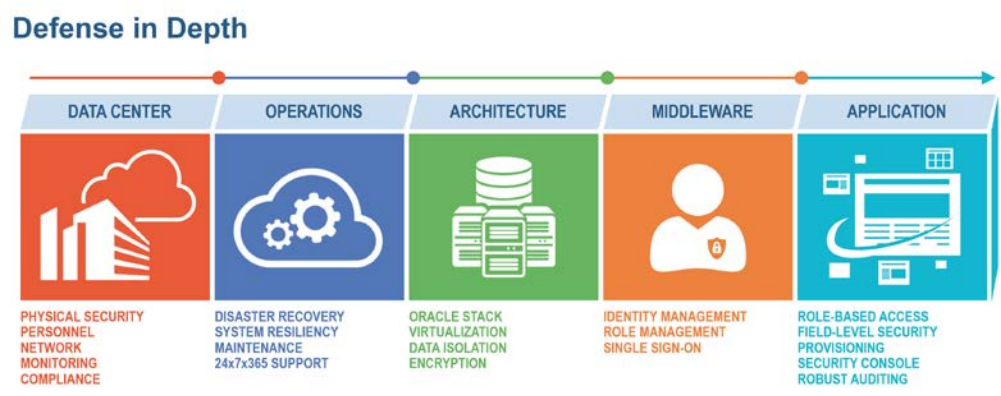


Figure 5. Defense in Depth

Comprehensive Security

Physical Security

As described above, data centers must meet stringent security and infrastructure requirements.

Full-time 24/7 local operations and security staff are tasked with ensuring that only authorized individuals have access to the data center. Data center access doors, including shipping and parking areas, are monitored and video recorded. Data center access is secured by access cards, biometric devices (e.g. hand scanners), man-traps, portals, or a combination thereof. Design of exterior walls, doors and windows are taken into careful consideration in order to protect from natural hazards including lightening and wind.

Server and network equipment is physically secured within locked cages/suites separate from other data center tenants. The listing of employees and cages are updated frequently so that access is limited to authorized personnel. Each data center provides centralized security operations and monitoring on a 24/7 basis, including prompt response to actual or suspected physical security incidents. In addition to administering and monitoring access to the data center, the operations and security teams monitor and enforce other security policies and environmental sensors and alarms. Security and environmental systems are supported by redundant power, uninterruptible power supply (UPS) devices, and stand-by generators.

Environmental Controls

Each data center facility has redundant generators and UPS systems. Load is handled by the battery backup until the generators take over the load. Structured cabling runs within overhead cable trays.

Cages are built on either concrete slab or raised floor. Power is installed overhead.

Logical Security

The Oracle Service Cloud Platform requires management authorization for employee access to any critical applications and systems, and additional approval levels are required for all Cloud Services access. Access is granted on an as-needed and on-going basis according to a user's role and business need, like Cloud Operations, Customer Care, and Engineering. Logical and physical access is required to be promptly revoked from employees who have resigned or are terminated. The Oracle SaaS Cloud Platform audits system and network activities, including access, or attempted access, to customer data. This includes monitoring and auditing of systems for unauthorized or inappropriate access to customer data by Oracle employees.

When deploying new systems into a POD, hosts are first imaged from known secure OS images, and before being integrated into the pod, the new systems are hardened further using hardening guidelines based on CIS, NIST and DISA standards, according to Oracle policies.

Oracle employs software VPN, two-factor authentication, and encrypted protocols like SFTP and TLS for systems administrators accessing the environments. Host administration is performed via either encrypted SSH or TLS using bastion hosts, and multi-factor authentication is required for access to all systems. Oracle retains security logs for at least one year.

Auditing of the environments includes daily and quarterly infrastructure and application scans, quarterly patching and version reviews, quarterly formal access reviews that include justifying privileged access, and ethical hacking reviews both before and after GA release of new software versions. Third-party application security tests are performed for every new release, and advanced event correlation and vulnerability detection is done using a SIEM solution.

Monitoring

Oracle uses an extensive monitoring framework to provide a 360-degree view across our cloud services. It not only provides visibility of the Oracle Cloud infrastructure itself, but also provides monitoring of external elements.

The framework we use covers everything from the network layer all the way up through the application and database layers. It uses different tools to monitor everything from the availability and performance of the infrastructure all the way through to the user experience.

All the data collected is stored in our SIEM: from the network to the logs generated, are analyzed to ensure that the security of the platform is not compromised. Dedicated security monitoring software is used to analyze and correlate security incidents and raise the relevant alerts when suspicious activity occurs. Oracle Cloud Operations is able to have a precise indication of where issues arise: from the end-user, application and infrastructure perspectives.

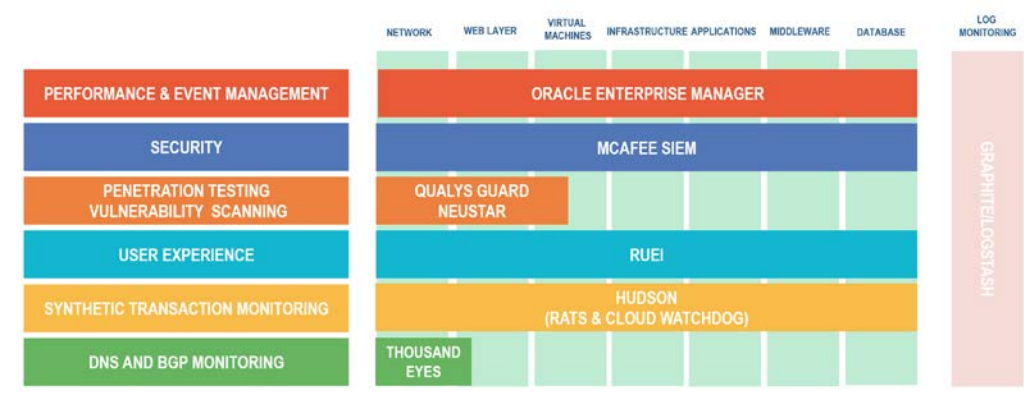


Figure 6. Monitoring Framework

The key tools that make up our monitoring framework are summarized in the table below.

Cloud Monitoring

TOOL	DESCRIPTION
Oracle Enterprise Manager	Enterprise Manager is used specifically to monitor the Web Servers, Virtual Machines, Physical Hosts, and databases.
McAfee SIEM (Security Information & Event Management)	SIEM software provides real-time analysis of security alerts generated by network hardware and applications and are used to log security data and generate reports for compliance purposes. The tool analyzes incoming data for suspicious or malicious activity and generates dashboards, reports, and alarms.
Qualys Guard	QualysGuard, a product suite from Qualys, includes solutions to discover and scan IT infrastructure and applications for security vulnerabilities and malware.
Neustar	SiteProtect Service from Neustar, is designed to recognize malicious traffic signatures and alerts when certain thresholds are breached. This includes DDOS protection
RUEI (Real User Experience Insight)	RUEI provides passive non-intrusive monitoring capability built using state-of-the-art Network Protocol Analysis technology. RUEI provides visibility into areas of the application that may be having performance issues. (non-invasive)
Hudson + RATS	Oracle uses Read-Only Automated Test Suite (RATS) . Synthetic transaction monitoring is a form of active web application performance monitoring that involves deploying behavioral scripts in a web browser to simulate the path a real end-user takes through a website. Hudson provides job execution
Thousand Eyes	Oracle leverages Thousand Eyes to monitor DNS and BGP, which will detect issues so that the relevant parties can be notified as to minimize service interruptions.
Logstash and Graphite	Oracle uses a combination of Graphite and Logstash to collect, analyze and store logging data.

COMPLIANCE

Oracle Cloud Services operate under Policies which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a set of controls are selected.

The Information Security Management System Family of Standards are a comprehensive reference for information security management, data protection and risk management for organizations of all types and sizes.

The internal controls of selected Oracle Cloud Services are subject to periodic testing by independent third-party audit organizations. Such audits may be based on the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization ("SSAE 16"), the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization ("ISAE 3402"), or such other third-party auditing standard or procedure applicable to the specific Oracle Cloud Service. Audit reports of Oracle Cloud Services are periodically published by Oracle's third-party auditors. Reports may not be available for all services or at all times. Customer may request to receive a copy of the current published audit report available for a particular Oracle Cloud Service.

PLATFORM AS A SERVICE: PAAS

By tailoring your SaaS Cloud, you can receive the following benefits:

- Improve the user experience at no extra cost
- Increase user satisfaction and usage
- Protect all your changes across software updates

As previously discussed, some of the ways your business users can tailor your cloud applications include:

- Branding - Configure and display your logos on the screen
- Place data fields and validate
- Change built-in approval processes
- Tailor dashboard reporting based upon your role or group with role-based access
- And add UI changes & apply to all devices

Tailor with SaaS, Enrich with PaaS

There will be areas where a company's business requirements are unique and their processes represent differentiation from those of other competitors. These require specialized functionality which is generally not available within any commercial application suite.

This is where the extensibility framework provided by Oracle Platform as a Service (PaaS) comes to the fore. The Oracle Cloud Platform helps customers build new applications, extend existing ones, and easily move existing on-premises workloads to the cloud with no application changes. The services are designed to maximize end user experience and productivity; enable developers to manage and analyze data, rapidly develop, test and deploy applications; enable architects to quickly integrate across on-premises and cloud applications; and enable business users to drive rich business insights and enterprise collaboration.

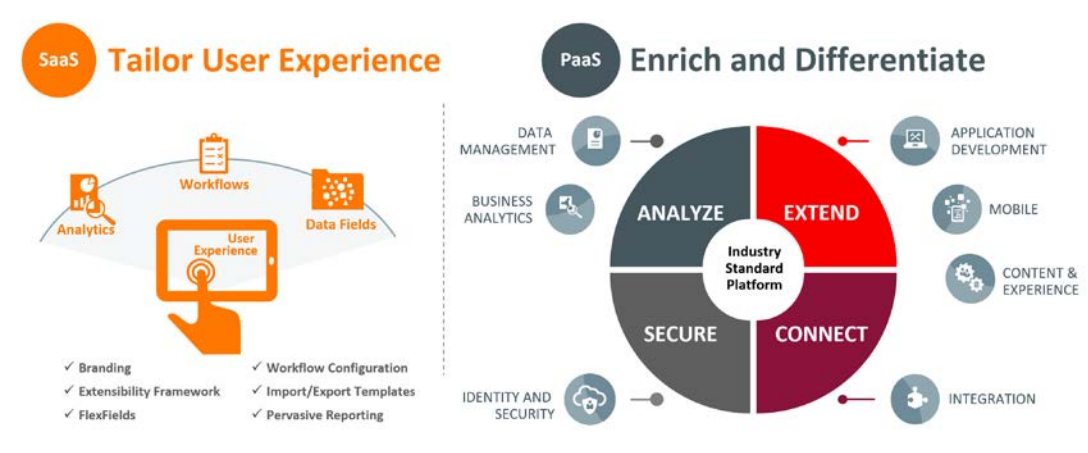


Figure 7. Oracle PaaS is designed to enrich SaaS

With the Oracle PaaS, customers and partners are able to take advantage of the industry-leading Oracle middleware and database software that thousands of global organizations already use to run their own businesses, all delivered via cloud. The extensive level of automation that has been engineered into the Oracle Cloud, results in faster time-to-value, greater innovation, and lower cost for customers.

CONCLUSION

The Oracle SaaS Applications are built on a modern technology framework that provides flexibility and scalability. They are deployed in world class facilities and meet the highest standards of security.

ORACLE CORPORATION

Worldwide Headquarters
500 Oracle Parkway, Redwood Shores, CA 94065 USA

Worldwide Inquiries
TELE + 1.833.386.META (6382) + 1.800.ORACLE1
FAX + 1.650.506.7200
oracle.com

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com/oracle  facebook.com/oracle  twitter.com/oracle

Integrated Cloud Applications & Platform Services

White Paper Title
January 2017
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]

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