Oracle Cloud Applications with Security-First Design

Security Breaches Happen, But Are You Aware of Their Implications?

It's an issue that faces all companies, so if you haven't been thinking about it, perhaps you should be. Data breaches are more common than you may realize. According to Gartner, worldwide spending on cybersecurity is going to reach $170.4 billion in 2022. (Gartner).[1]

With online initiatives kicking in for everything from health records to consumer spending habits, the amount of data that businesses must manage and maintain has grown astronomically—IDC states that, today. more than 5 billion consumers interact with data every day — by 2025, that number will be 6 billion, or 75% of the world's population.[2] Securing all this data and making sure it's protected at every level of business is no longer just an IT responsibility. According to the Identity Theft Resource Center, there were 80 breaches exposing close to a million records in early 2020 alone — and these are just the ones they know about.[3]

The job of keeping business data safe has spread across the organization to become an enterprise wide concern. The critical question now —the one that's being asked, not only by IT but also by line-of-business (LOB) managers—is: "Whether it's on-premises or in the cloud, how do I keep sensitive data secure?" Your cloud provider should be able to help answer these questions.

When it comes to security, not all cloud providers are created equal. If you find a cloud provider that is committed to data security—a provider with a security-first design—then improved security can be a reason for you to move to the cloud.

> "We have invested in Oracle's security cloud services to enhance our ability to detect and respond not only to potential threats but also data leakage and to better meet our regulatory requirements."
>
> **CSO, Large Global Bank**

1 https://cybersecurityventures.com/cybersecurity-market-report/.

2 https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html

3 https://www.idtheftcenter.org/wp-content/uploads/2020/05/April-2020-Category-Summary.pdf

World-Class Security Controls

Helping customers meet their regulatory compliance needs is important to Oracle. Many of Oracle's cloud solutions have industry-standard third-party audit reports available in formats such as:

- SSAE 18: SOC 1 and SOC 2

Also, many of Oracle's cloud solutions adhere to the requirements or guidance of well-recognized industry standards. Examples of these standards include:

- International Organization for Standardization (ISO) 27001, 27002, 27017, 27018
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Risk and Authorization Management Program (FedRAMP)
- UK GOV Cloud — HMG Cloud Security Principles, Cyber Essentials Plus

Oracle is committed to providing assurance about its cloud services in industry recognized frameworks.[4]

4 Availability of different standards and reporting formats varies by service. The relevant contracts between you and Oracle determine the scope of services provided and the related security terms.

Why Should You Care About Cloud Security?

As SaaS cloud applications become decentralized from IT, the responsibility for securing data can get overlooked.

It's not just proprietary information or company secrets that are at risk; it's also the data that is used daily to transact business.

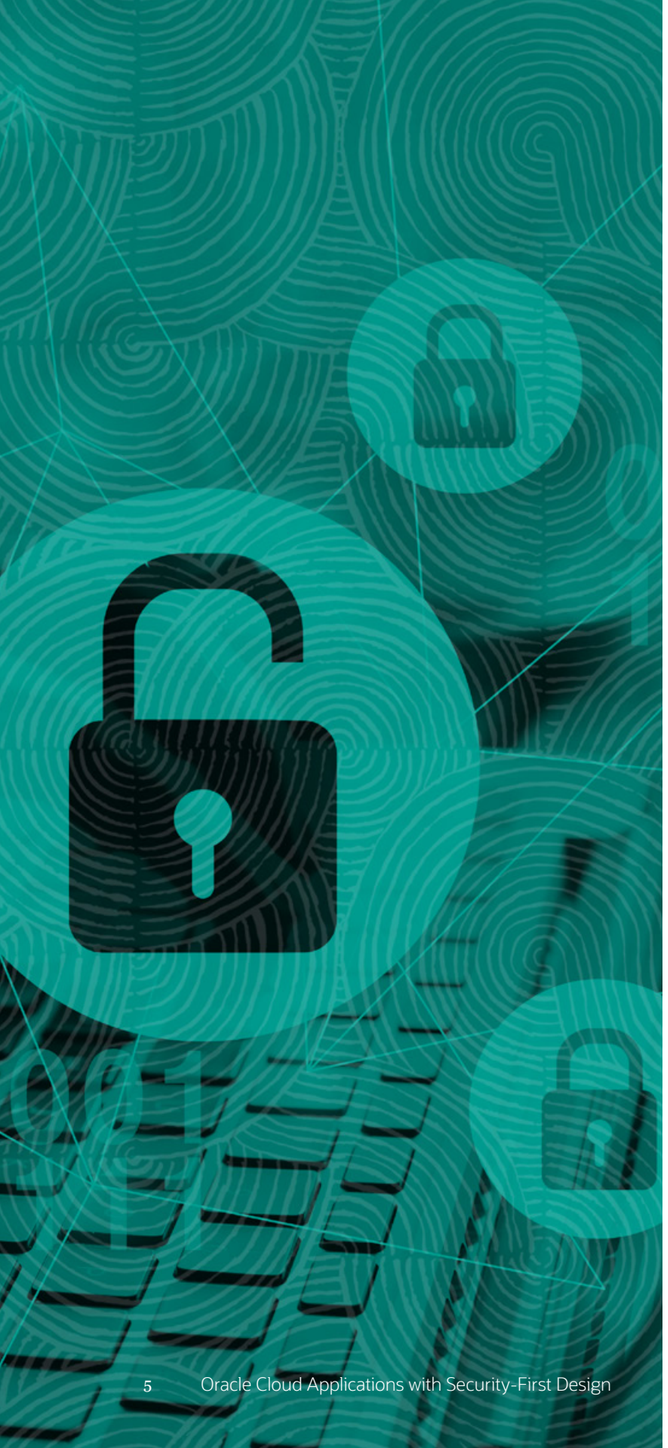
Employee / Consumer Data

Social security numbers, addresses, phone numbers, and other personal information (PI) must always be kept confidential.

Many countries have regulatory requirements concerning the privacy of data. Protecting data not only secures one of your most valuable assets but also helps mitigate the risk of identity theft (and other potentially unwanted occurrences) that can happen when data gets into the wrong hands.

Human Resources Process

Onboarding and offboarding employees and the administration of benefits mean that HR collects a lot of data about employees. For example, when onboarding employees, there can be interview notes, reference letters, and other confidential information. Likewise, employee healthcare choices and benefits, in addition to any data that reveals specific diagnoses or treatments, must remain absolutely confidential.



Financial Reporting Systems

Keeping financial information—including sensitive employee and customer data confidential is a top priority, not just for CFOs but for all business leaders. Data security risk can be reduced within financial systems using scope controls, advanced role analysis, segregation of duties, and data privacy tools for audit and evaluations across business units.

Compensation and Payroll

Compensation and payroll data can be extremely sensitive information. A data leak can result in employee morale issues as well as potential HR issues. In addition, because many employees use direct deposit for their paychecks, private bank account information is also often stored.

Customer Order and Contract Information

In addition to maintaining the integrity of your customers' data, you also want to keep information about your customer accounts confidential.

Information about account plans and strategies—especially information on mobile devices—can easily fall into the wrong hands if security is missing or inadequate.

Industry-Specific Requirements

Some organizations have to adhere to certain regulations and restrictions by industry such as HIPAA and FISMA. It is important to consider necessary regulations when choosing a cloud provider.[4]

Hosting of Data by Region

As part of a cloud services agreement, your cloud provider, should specify where your data is located within a data center region. For those with specific data location requirements, support may be offered by your cloud provider.

And, should your business require it, your cloud provider must be able to provide regional storage for backup and recovery data. Cloud providers should not migrate the hosting of data outside of the customer's specified region.

Global Access Controls

Employees should not have access to other employees' sensitive information, so it is vital that your cloud provider offer unified global access controls across your business.

Following least privilege practices and denied by default settings, the right users will have the right level of access to the right systems and data.

Roles and Territory Visibility

Sales representatives need access to the data (including customers, leads, and opportunities) and functionality that enable them do their jobs, but there's no reason to give them access to territory definitions. Sales managers need visibility into each representative's account to gauge activity across the team, and sales operations has its own access.

Unified security controls provide role-based access that allows teams to do their work while limiting access to sensitive data.

4 Applicability of different standards and reporting formats varies by service. The relevant contracts between you and Oracle determine the scope of services provided and the related security terms.

What Should You Look for in a Cloud Provider?

Protect your valuable data and mitigate the risk of data breaches. And when it comes to security, look for a provider that offers:

- Cloud Provider Viability
- Secure Data Isolation Architecture
- Global Unified Access Controls
- Compliance and GDPR Controls
- Global Cloud Operations
- Advanced Data Security

These key considerations can help you choose a secure cloud provider. The next pages will describe how each consideration can benefit your organization.

Security-First Design

Oracle Cloud Applications suite was developed with a focus on security-first and designed with a secure isolation architecture. It protects data from unwanted access and is built-in at multiple layers of the stack.

Security-first design improves data protection, scalability and performance.

Cloud Provider Viability

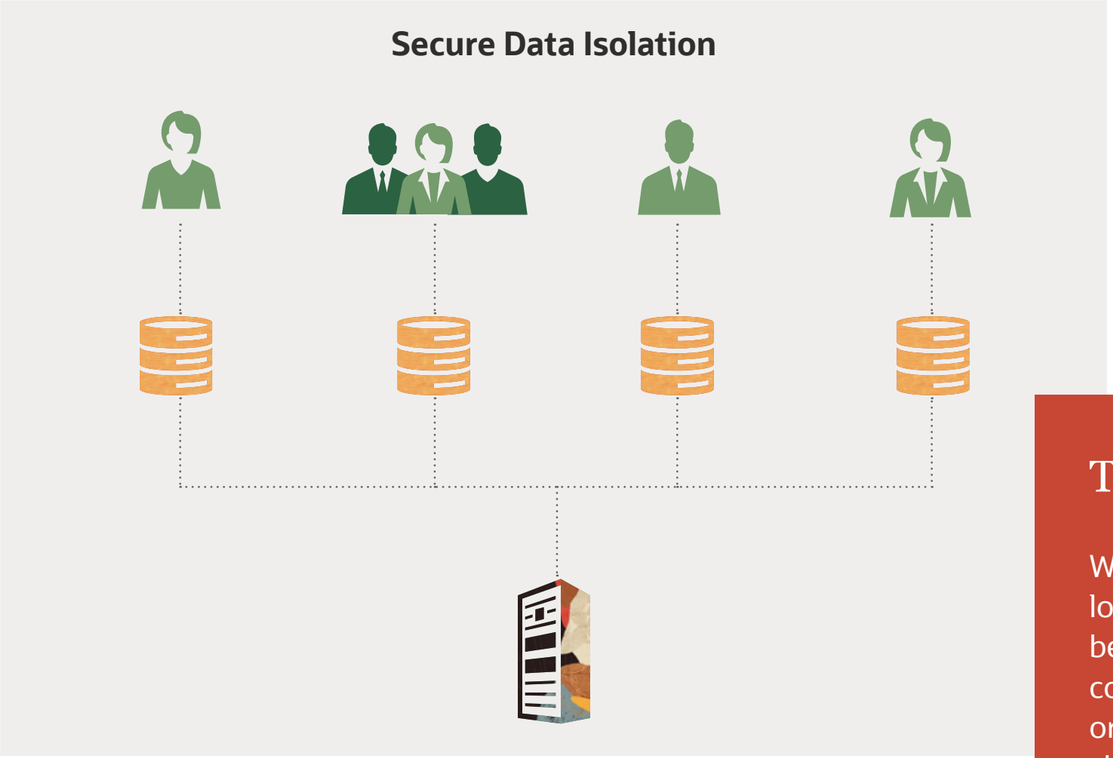
Is your cloud provider viable? Will they be around tomorrow? Making a decision about your cloud applications is very important for your business, so investigate whether your provider has a long and proven track record of securing clouds. Examine your provider's financials and ability to invest in secure innovations. You'll want your cloud provider to be one that can serve you well in the long term.

Secure Data Isolation Architecture

Oracle Cloud enables you to leverage shared resources (such as hardware) across the cloud, where it makes sense, to keep costs low. However, with Oracle's security-first design and secure data isolation architecture, Oracle isolates data to reduce risk and enables high-performance scalability.

Choose a provider that does not commingle your data with other customers' data—one that uses secure data isolation.

Shared Resources Where It Makes Sense, Isolated Where It Doesn't



With Oracle Cloud, customers have their own database instance in the cloud, including their own virtual network and isolated storage. Because of this architecture, there is no concern about noisy neighbors.

Take the Long View

When it comes to data security, it pays to take a long-term view. Where will your security needs be in five years? Can the security solution you're considering grow with you and adjust to new or changing requirements? You don't want to choose cloud providers again. Choose a cloud provider that can secure your data and innovate for you for the long term.

Global Unified Access Controls

Issues can arise if unauthorized users have access to business-critical data. The ideal cloud provider enables you to manage access controls globally.

For example:

- When users join your company, you have complete control in determining the correct level of access, and revoking that access when it is no longer appropriate.
- Only users you have approved have access to relevant data—both across clouds and on premises—with enterprise wide centralized identity management and federated single sign-on (SSO).
- Role-based access controls (RBAC) are put into place to allow for segregation of duties (SOD) to help prevent unauthorized access to confidential information.
- Users see only data that's related to their job specific duties. Administrators configure job roles that map to job functions and data privileges.

Compliance and GDPR Controls

To help you meet your compliance needs under GDPR and other privacy laws, a modern cloud provider should have many global data center regions and software solutions that help to manage compliance such as, risk management software.

Global Cloud Operations

Oracle's global network operation centers are staffed with Oracle badged cloud security experts that proactively monitor cloud security. Cloud operations should have a 24/7 "follow the sun" model to better support customers.

Your cloud provider should have state-of-the-art physical data center protection, logical data security, and data privacy protection policies already in place. In addition, the right cloud provider enables proactive security engagement and monitoring as well as leading-edge disaster recovery.

Advanced Security Options

A world-class cloud provider offers advanced security options in the cloud when your business requires additional security measures. Some of the advanced data security services to look for:

- Oracle Transparent Data Encryption to prevent unauthorized use of sensitive data.[6]
- Oracle Breakglass with Database Vault to provide additional controls over data and administrator access to prevent unauthorized use, views or sharing of employee information. Oracle customers hold the "keys" and must grant access to the cloud provider should they need to access the cloud environment.[6]
- Oracle Cloud Access Security Broker (CASB) Cloud Service can give you additional protection by automating SaaS security monitoring. It combines threat detection across cloud applications and cloud providers.
- Oracle Identity Cloud Service (IDCS) provides secure and adaptive authentication and access controls including: SSO, and user provisioning for on-premises and SaaS applications and hybrid identity management capabilities.
- The ability to extend Identity Management solutions to cloud applications for hybrid cloud models.[6]

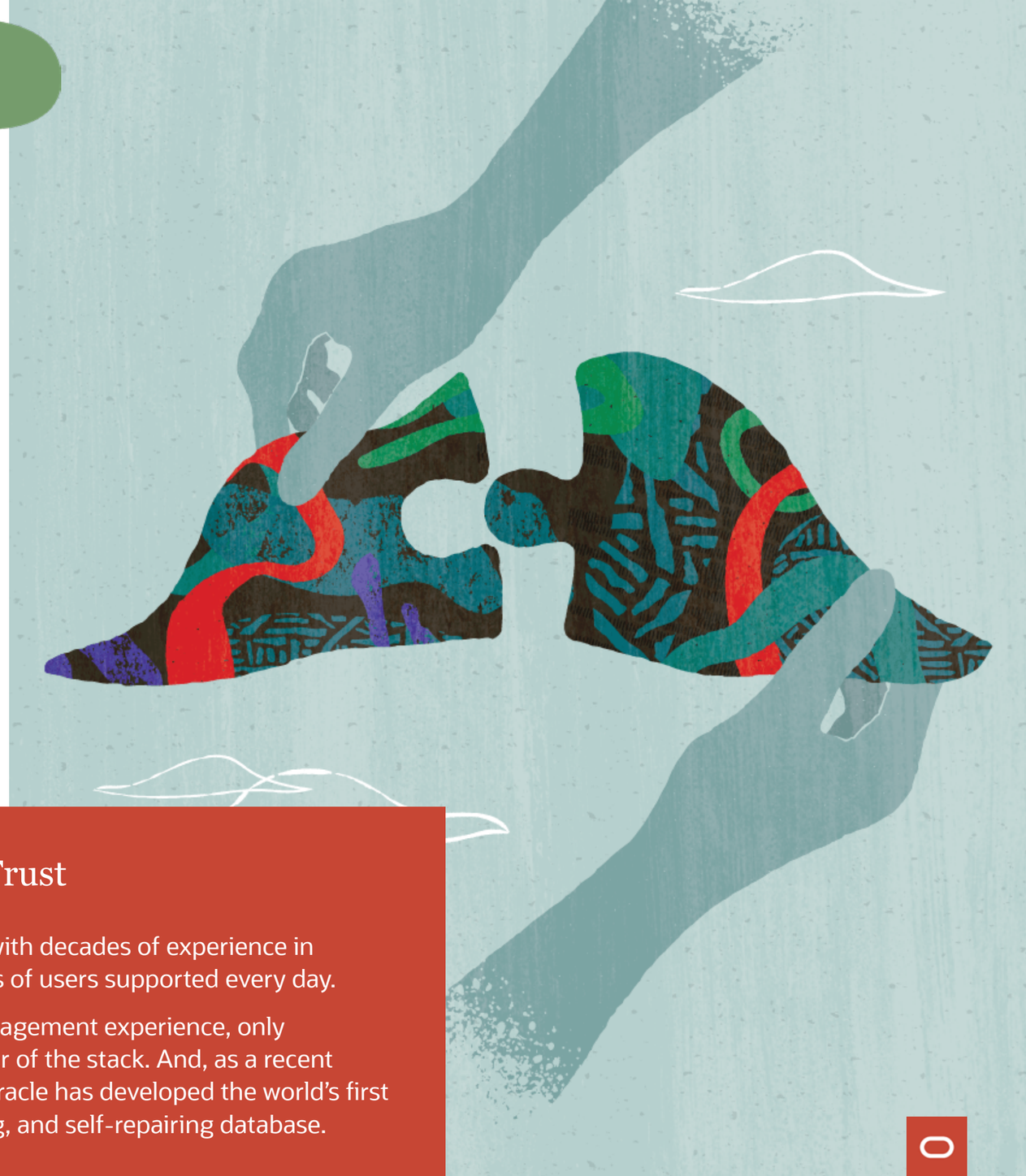
6 Available for select cloud offerings

Oracle Cloud Applications with Security-First Design

Oracle continually invests in every layer of cloud security-first as part of its overall design across global data center regions and now we are building in autonomous capabilities that reduce risk, reduce errors, enable better compliance and auditing, and increase productivity.

Oracle Cloud does just that with:

- **Cloud provider viability.** Oracle's experience says it all: more than 40 years in secure data management, decades of running enterprise clouds, and millions of users supported every day.
- **Secure data isolation architecture.** Shared resources where it makes sense, isolated where it doesn't. Each customer has their own isolated database for secure and reliable performance.
- **Global unified access controls.** Across the enterprise, only approved users have access to data in cloud and on-premises systems. Centralized identity management with federated SSO and RBAC prevents unauthorized access.
- **Global cloud operations.** Oracle operates enterprise-grade cloud data centers with highly redundant infrastructure and high availability.
- **Compliance, GDPR & Risk Management.** A modern cloud provider should have many global data center regions and software solutions help with current compliance, GDPR and data residency requirements.
- **Advanced security options.** Oracle offers advanced security options when your business has additional security needs: Oracle Transparent Data Encryption[6], Oracle Break Glass, Oracle CASB and Oracle Identity Cloud Service[6] including identity management solutions for hybrid models.



A Cloud Partner You Can Trust

Oracle has a complete cloud strategy with decades of experience in running enterprise clouds with millions of users supported every day.

With over 40 years of secure data management experience, only Oracle designs in security at every layer of the stack. And, as a recent demonstration of that commitment, Oracle has developed the world's first autonomous self-driving, self-securing, and self-repairing database.

6 Available for select cloud offerings

Oracle: A Cloud Partner You Can Trust

Oracle is a trusted, strategic business innovation and transformation partner with a commitment to continuously invest and develop secure cloud innovations for you. Oracle Cloud Applications suite was developed with a focus on security-first. An isolated design improves data protection, scalability and performance. As part of a global ecosystem, the suite can connect securely to multi-clouds and other systems.

Oracle Invests and Innovates

Oracle recognizes that not all customers' needs are the same. Some have global requirements and some have local data security requirements in other countries. Others have regulatory compliance requirements that are specific to their industry.

As our customers' needs grow, Oracle continues to invest and innovate to offer secure data management offerings at the level that your business requires.

How It Works

When you subscribe to an Oracle Cloud service, service level and security standards are presented in the cloud service contract.

Tens of millions of Oracle subscribers use Oracle Cloud every day. Based upon their input, Oracle continues to develop autonomous capabilities that are self-repairing to deliver state-of-the-art secure innovations that reduce risk, reduce manual errors, help to improve compliance and auditing, and increase productivity.

When your business has additional security needs, Oracle has advanced data security options and will continue to innovate for future needs.

Contact Us

To learn more, call +1.800.ORACLE1 to speak to an Oracle representative or visit oracle.com/applications

Outside North America, find the phone number for your local Oracle office at oracle.com/corporate/contact/global.html

Connect with Us