ORACLE

ORACLE
CLOUD APPLICATIONS

A Secure Cloud for the Digital World

You hear about security breaches all the time, but are you aware of all the implications?

It's an issue that faces all companies, so if you haven't been thinking about it, you should be. Data breaches are more common than you may realize—not all of them make the headline news. According to the Identity Theft Resource Center, there have been over 139 data breaches and over 4,294,000 records exposed in one year alone. These numbers are astonishing and they show that data breaches are an ongoing concern.[1]

With online initiatives in progress for everything from health records to consumer spending habits, the amount of data that businesses must manage and maintain has grown astronomically—the most recent numbers estimate that our digital universe will grow to 44 trillion gigabytes by 2020. Securing data and protecting it at every level of the business is no longer just an IT responsibility. For example, a recent data breach at a well known credit agency compromised sensitive information—including social security and driver's license numbers of 15 million customers.[2]

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 provide the right answers.

You shouldn't trust your data to just anyone. And when it comes to security, not all cloud providers are created equal. But if you find a cloud provider that truly understands data protection—a provider that "does cloud right"—then security can actually be an important reason for you to move to the cloud.

"In a scenario where we use Oracle ERP Cloud, it makes a lot of sense for us to be able to say, here's Oracle who's a lot better at cloud security than we are. And we think the risks in the cloud are significantly smaller."

Head of Finance, a global gaming company, with ~50 million visitors monthly

1 (http://www.idtheftcenter.org/2016databreaches.html)

2 (http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2015/7/)

World Class Security and Compliance.

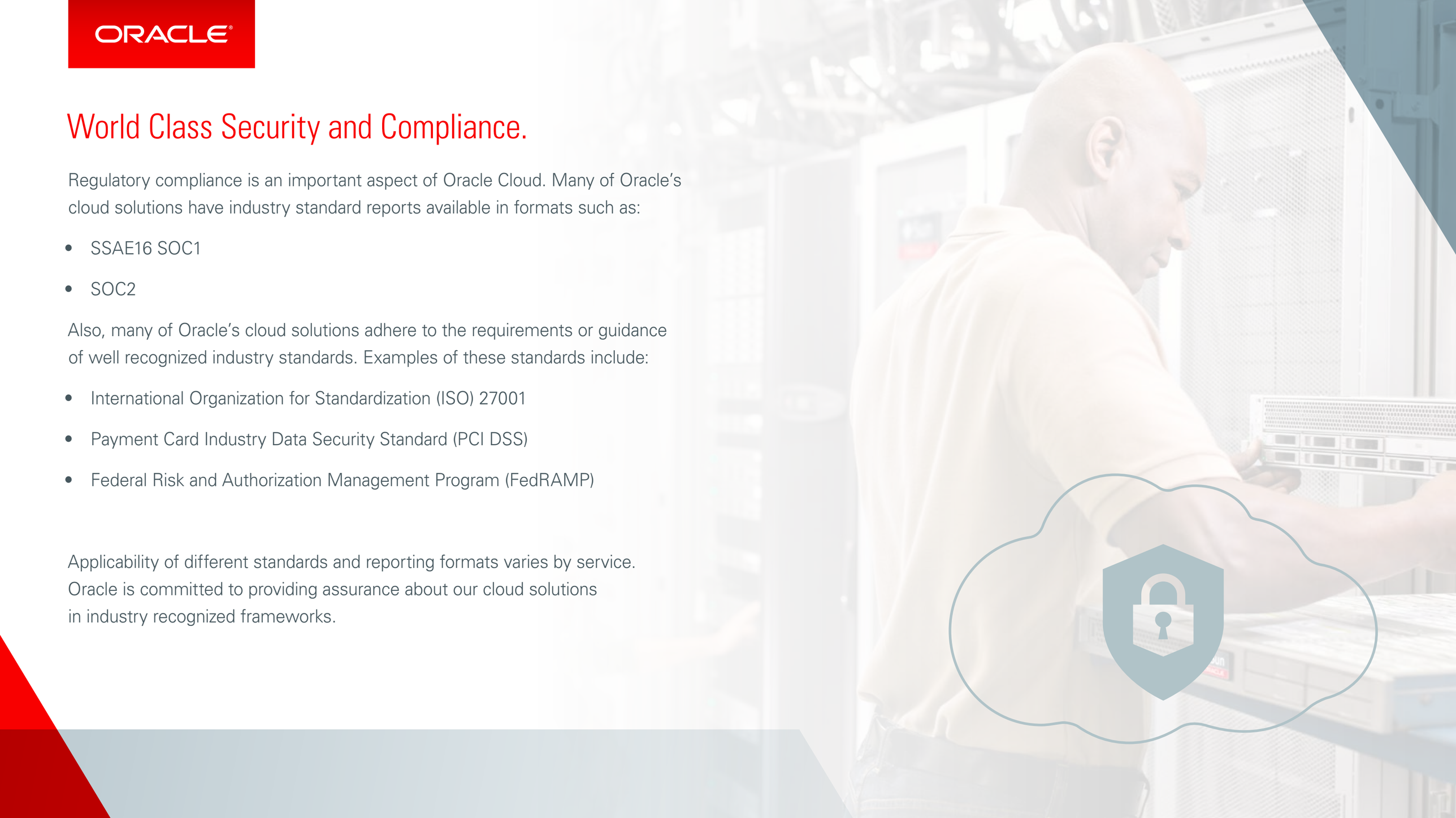
Regulatory compliance is an important aspect of Oracle Cloud. Many of Oracle's cloud solutions have industry standard reports available in formats such as:

- SSAE16 SOC1
- SOC2

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
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Risk and Authorization Management Program (FedRAMP)

Applicability of different standards and reporting formats varies by service. Oracle is committed to providing assurance about our cloud solutions in industry recognized frameworks.



ORACLE

Why Should You Care About Cloud Security?

As software as a service (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.

Private Employee/Consumer Data

Social security numbers, addresses, phone numbers, and other personally identifiable information (PII) must always be kept confidential.

Many countries have regulatory requirements concerning the privacy of employee data and penalties for data breaches. Protecting employee data not only secures your most valuable asset, but also averts the risk of identity theft (and other potentially disastrous occurrences) that can happen when Personally Identifiable Information (PII) gets into the wrong hands.

Financial Reporting Systems

A data breach of company financials could affect company performance and have serious repercussions for the organization, including bad publicity, negative analyst reports, and declining stock prices. Keeping financial information—including sensitive employee and customer data—confidential should be a top priority not just for CFOs but for all LOB leaders.

Human Resources Data

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.

Compensation and Payroll

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

HIPAA and FISMA are just two of the many industry-specific regulations that must be enforced to avoid potentially heavy fines and legal issues—not to mention the bad publicity that can accompany data breaches.

Localized Data Residency and Compliance

Because of the increasing number of countries that specify where data can and cannot be stored, cloud providers must be in compliance with industry and country data standards. And, should your business require it, your cloud provider must be able to provide regional storage for backup and recovery data.

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. This way, approved users have the right level of access to relevant 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.

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

ORACLE

What Should You Look For in a Cloud Provider?

Protect your valuable data and avoid cloud 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
- Local data residency and compliance
- Data center 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.

Share Resources or Keep Them Isolated?

Privacy and processing performance are critical to your business. If your cloud provider makes you choose between the two and doesn't offer secure data isolation, find another provider.

Cloud Provider Viability

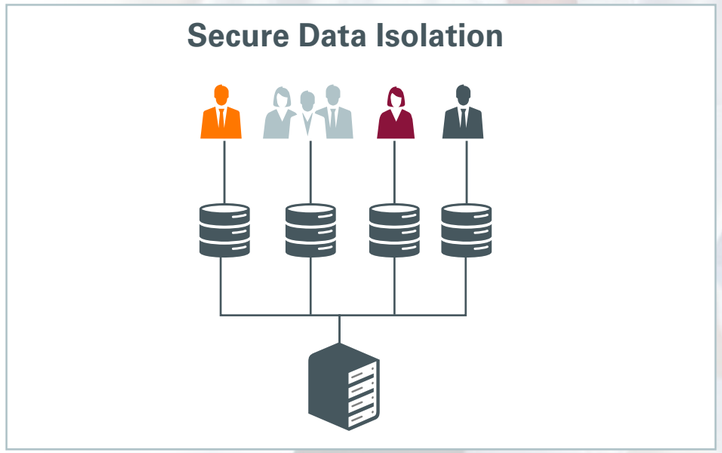
Is your cloud provider viable? Will they be around tomorrow? Making a decision about your cloud applications is very important for your business, so investigate whether your provider has a long and proven track record of security in the cloud. Examine your provider's financials and ability to invest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

Secure Data Isolation Architecture

Oracle Cloud enables you to leverage shared resources across the cloud, e.g. (hardware etc.), where it makes sense, to keep costs low. However, with Oracle's secure data isolation architecture, Oracle isolates data to reduce risk and enable high performance scalability.

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

Share resources when it makes sense; keep resources isolated when it doesn't.



With Oracle Cloud, each customer has its own database instance in the cloud, each customer can select a best time to upgrade and know that "noisy neighbors" won't affect reporting or processing performance.

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 the 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

Damage can be done if unauthorized users have access to business critical data. The ideal cloud provider enables access controls globally.

For example:

- When users join your company, they'll have correct level of access; when they leave, their access to all relevant systems and data is revoked globally and consistently.
- Only approved users have access to relevant data—both across clouds and on-premises—with 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 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.

Local Data Residency and Compliance

A modern cloud provider should have multiple 24/7 global data centers that meet local data residency requirements while still adhering to industry-specific compliance requirements.

Data Center Operations

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 Data Security

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
- Oracle Database Vault with additional controls over data and administrator access to prevent unauthorized use,views or sharing of employee information
- The ability to extend Identity Management solutions to cloud applications for hybrid cloud models*

* Coming soon as a service.

Oracle Cloud: Complete. Data-Driven. Personalized. Connected. Secure.

Modern business leaders create real value by providing their employees with complete, data-driven, personalized, connected and secure cloud solutions—solutions that enable your employees focus on the big picture for your business. The modern business requires a new cloud approach that can bring solutions not just to the IT department but also to employees throughout the enterprise.

Oracle Cloud does just that with:

- **Cloud provider viability.** Oracle's experience says it all: more than 40 years in secure data management, more than 15 years in running enterprise clouds, and more than 70 million users supported every day
- **Secure data isolation architecture.** Shared resources where it makes sense, isolated where it doesn't. Each customer has their own physically isolated database for secure and reliable performance without limits
- **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 prevent unauthorized access
- **Local data residency and compliance.** When your data must be stored in a particular location, one of Oracle's many global data centers is available with Oracle badged cloud security experts that pro-actively monitor the security of your data. Oracle also provides best in class industry based compliance.
- **Data center operations.** Oracle operates enterprise-grade cloud data centers with highly redundant infrastructures and high availability
- **Advanced data security.** Oracle offers advanced security options when your business requires additional security needs: Oracle Transparent Data Encryption, Oracle Database Vault, Oracle Identity Management solutions to cloud applications for hybrid cloud models*

A Cloud Provider You Can Trust

Oracle has a complete cloud strategy with more than 15 years of experience in running enterprise clouds with over 70 million users supported every day.

With more than 40 years in secure data management and the broadest portfolio of cloud services in the industry, Oracle has demonstrated its commitment to its customers and to future innovations.

* Coming soon as a service.

A Modern Cloud for the Modern Global Enterprise

In today's digital age, modern businesses need more than just a cloud—they need a modern cloud to power innovation and drive change. Oracle provides complete, data- driven, personalized, connected, and secure cloud applications that let you take your business to the next level and stay ahead of the competition.

- **Complete.** One cloud for your entire business with best in class applications that you can consume incrementally and grow with no matter the size of your business.
- **Data-Driven.** Unified, actionable information you can trust with embedded intelligence so you unlock the value of data every level.
- **Personalized.** SaaS applications are configurable per user and can be enriched for your unique business.
- **Connected.** Connect any part of the business, connect any person anywhere with embedded social and mobile and connect any "thing" as in IoT.
- **Secure.** Designed to be secure at every layer of the stack with reliable performance without limits.

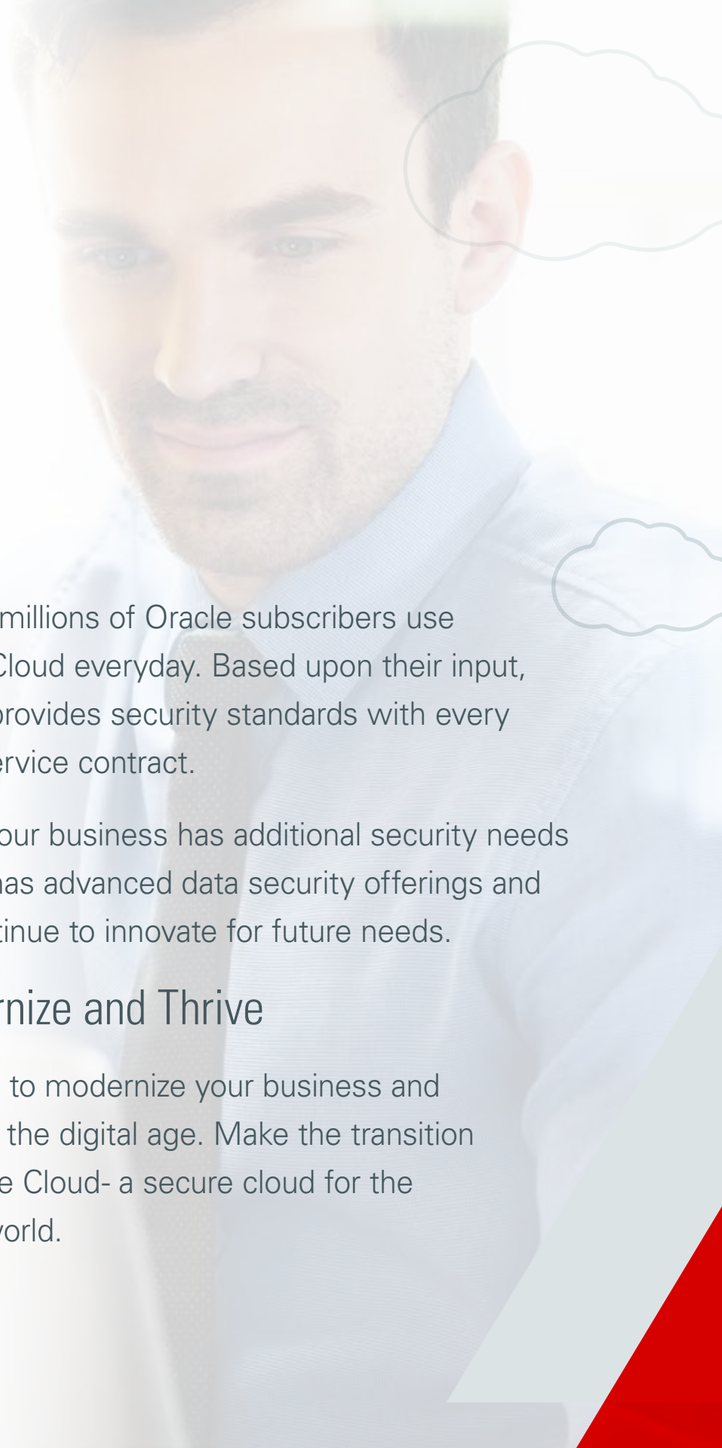
Oracle Invests and Innovates

Oracle recognizes that not all customers' needs are the same. Some have global requirements and some have local data residency requirements in other countries. Others have regulatory compliance or reporting 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 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 everyday. Based upon their input, Oracle provides security standards with every cloud service contract.

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

Modernize and Thrive

It's time to modernize your business and thrive in the digital age. Make the transition to Oracle Cloud- a secure cloud for the digital world.

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