Brought to you by:

ORACLE

Cloud Security

for dummies®

A Wiley Brand

Detect threats with a security-first design

Use automation for better security

Address continuous compliance

Lawrence Miller

Oracle
3rd Special Edition

About Oracle

Oracle, a global provider of enterprise cloud computing, is empowering businesses of all sizes on their journey of digital transformation. Oracle Cloud provides leading-edge capabilities in Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Cloud Security

Cloud Security

Oracle 3rd Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Cloud Security For Dummies®, Oracle 3rd Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

ISBN 978-1-119-81108-4 (pbk); ISBN 978-1-119-81109-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: William Hull

Production Editor: Tamilmani Varadharaj

Special Help: Maywun Wong, Fred Kost, Greg Jensen, Sean Cahill, Taylor Lewis, WaiSau Sit, Eric Maurice, Nancy Kramer, Julie Miller, Nader Mikhail

Table of Contents

Introduction 1
Foolish Assumptions 2
Icons Used in This Book 2
Beyond the Book 3
CHAPTER 1: Looking at the Current State of Cloud Security 5
Machine Learning and the Cloud Are Changing Security 6
Traditional Security Approaches Are Not Enough 9
Making Sense of the Shared Responsibility Model 10
Trust and verify 13
The "set it and forget it" myth 14
The new model for cloud security 16
CHAPTER 2: Exploring Oracle Cloud Security 19
Oracle Cloud Services 19
Oracle's Security Guiding Principles 23
Oracle Cloud Infrastructure: Defense-in-Depth 24
CHAPTER 3: Securing Your Users, Data, and Apps in the Cloud 29
Multiple Journeys to the Cloud 30
Identity Is the New Perimeter 32
Data Is Your Organization's Most Important Asset 35

Cloud Visibility and Consistent Data Protection 38
Securing apps 40
Security Monitoring and Analytics 41
Threat Detection and Prevention 42
CHAPTER 4: Addressing Regulatory Compliance 47
Recognizing the Compliance Mandate 48
Addressing Regulations and Standards 49
Comprehensive Compliance Strategy 51
CHAPTER 5: Ten Requirements for Better Cloud Security 55

Introduction

Change is a constant in information technology. In 2019, the FBI's Internet Crime Complaint Center (IC3) (www.fbi.gov/news/stories/2019-internet-crime-report-released-021120) saw both the highest number of complaints and the highest dollar losses reported since the center was established in May 2000, recording more than $3.5 billion in losses to individual and business victims. Just a few years ago, concerns about security and privacy prevented some organizations from adopting cloud strategies. Today, many of these concerns have been alleviated and organizations are now aggressively moving their infrastructure, devices, applications, and data to the cloud to leverage the robust security offered by some cloud providers. In fact, there is growing consensus that the cloud can actually be more secure than many on-premises environments.

The key is to choose the right technology — one that is designed to protect users, safeguard data, and help better address certain regulatory compliance requirements. In this book, you learn why enterprises rely on advanced and complete cloud services to transform fundamental business processes more quickly and confidently than ever before.

Foolish Assumptions

It has been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless! Mainly, I assume you're a chief information security officer (CISO), chief security officer (CSO), chief compliance officer (CCO), or security manager for a large enterprise that is evaluating security and compliance capabilities in the cloud to support your organization's rapidly evolving cloud strategy.

Icons Used in This Book

Throughout this book, I occasionally use icons to call out important information. Here's what to expect:

The Remember icon points out information you should commit to memory — along with anniversaries and birthdays!

The Tip icon points out helpful suggestions and useful nuggets of information.

The Warning icon points out practical advice to help you avoid potentially costly and frustrating mistakes.

Beyond the Book

There's only so much I can cover in 64 short pages, so if you find yourself at the end of this book thinking, "Gosh, this is an amazing book! Where can I learn more?," just go to `www.oracle.com/security`.

IN THIS CHAPTER

- Learning about security trends
- Recognizing the limitations of traditional security approaches
- Understanding shared responsibility in the cloud

Chapter 1

Looking at the Current State of Cloud Security

In this chapter, you learn about the modern threat landscape, why traditional security approaches alone are no longer sufficient to protect the enterprise, and how cloud service providers (CSPs) and enterprises work together to secure cloud environments in a shared responsibility model.

Machine Learning and the Cloud Are Changing Security

Cloud adoption promises the benefit of increased flexibility and agility and significant cost savings, so migrating business-critical applications to the cloud is a growing priority for companies of all sizes. The Oracle and KPMG *Cloud Threat Report 2020* (`www.oracle.com/security/cloud-threat-report`) found that "76 percent of businesses are now leveraging infrastructure as a service (IaaS), up from 65 percent in 2019." The report further indicates that 29 percent of business-critical applications are being consumed as software as a service (SaaS) today and will grow to 38 percent over the next two years based on trending from 2018 to 2020.

Although many enterprises adopt new applications on a regular basis, not all organizations have real-world experience in securely adopting or using cloud services. Migrating enterprises' business-critical applications and services to the cloud can have a much larger ramification than any single software upgrade. Often, cloud adoption is part of a companywide initiative that represents a new paradigm for doing business.

Here are some of the modern cybersecurity challenges in the rapidly and ever-evolving threat landscape:

- **Advanced threats:** Attackers target enterprise users with adaptive malware, ransomware,

vulnerability exploits, and increasingly sophisticated email phishing campaigns.

- **Porous perimeter:** The ubiquity of the cloud and mobile devices means employees are increasingly accessing enterprise applications and data from beyond the traditional network perimeter, including working from home due to the pandemic.
- **Unsanctioned IT:** Frustrated by enterprise IT's lack of flexibility and slow responsiveness, and bolstered by the simplicity and ease-of-use in SaaS applications, enterprise users have created an unsanctioned IT culture — that may also include valid services that run in non-approved configurations.
- **Configuration Management/DevSecOps:** Some organizations are struggling with managing the secure configurations of business-related cloud services (that is, insecure containers/buckets) due to human error, misconfigurations, vulnerabilities, patch management, identity and access management challenges, and more. These challenges are further complicated by adoption of on-premises DevSecOps strategies that have more limited capabilities in the cloud.
- **Shortage of skills:** According to the International Information System Security Certification Consortium, or (ISC)^2, 2020 Cybersecurity Workforce Study, the global cybersecurity

workforce shortage is estimated to be 3.1 million worldwide.

- **Cloud experience gaps:** According to the Oracle and KPMG *Cloud Threat Report 2020,* 92 percent of organizations feel they have a readiness gap as they shift to cloud, leading to three-quarters having experienced data loss from a CSP. Addressing the gap starts with understanding the shared responsibility security model for the cloud.

REMEMBER

Shadow IT is a term used to describe applications and IT services — particularly cloud-based apps and services — that are provisioned and used by end users but are not explicitly approved, authorized, managed, supported, or otherwise sanctioned by the IT organization. For example, an organization's legal department may use a highly restricted and preconfigured version of Dropbox that allows them to access company files. However, other departments may not have these same controls in place and simply assume they can use Dropbox "out of the box" to share files.

WARNING

According to the Oracle and KPMG *Cloud Threat Report 2020*, 75 percent of executives reported that they have experienced data loss from a compromised cloud provider

configuration and 40 percent of organizations experienced a cyber business fraud attack in the last 12 to 24 months.

Traditional Security Approaches Are Not Enough

In the face of these threats, traditional security approaches are no longer sufficient to protect the enterprise — whether on-premises or in the cloud. Traditional security tools such as perimeter-based firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) add complexity to the enterprise environment and require a depth and breadth of skills and experience that is more and more difficult to find, maintain, and retain among IT security staff.

WARNING

Threats are moving at machine speed, while traditional enterprise security analyzes and reacts at human speed.

Machine learning (ML) and artificial intelligence (AI) are changing threat management in terms of cost, complexity, and resources for legacy security approaches, and bringing a new level of sophistication to cybersecurity threat prediction, prevention, detection, and response. Furthermore, the Oracle and KPMG *Cloud Threat Report 2020* indicates that 84 percent of respondents feel that AI is more effective at threat "hunting" than humans. You

can learn more about ML and AI in modern IT security in Chapter 3.

Making Sense of the Shared Responsibility Model

The shared responsibility model is arguably one of the least understood security concepts in the cloud. In fact, only 10 percent of chief information security officers (CISOs) fully understand their role in securing SaaS versus the CSP. Simply put, managing security in the cloud is largely derived from the shared responsibility of the cloud customer and the cloud provider who are expected to perform certain security and functional tasks. The nature and extent to which security tasks are performed by the customer and provider varies by types of cloud services: SaaS, platform as a service (PaaS), or IaaS, as shown in Figure 1-1.

REMEMBER

The shared responsibility model outlines the CSP's area(s) of responsibility in regards to maintaining security and availability of the service, the customer's responsibility to ensure secure use of the service, and where both share a specific responsibility.

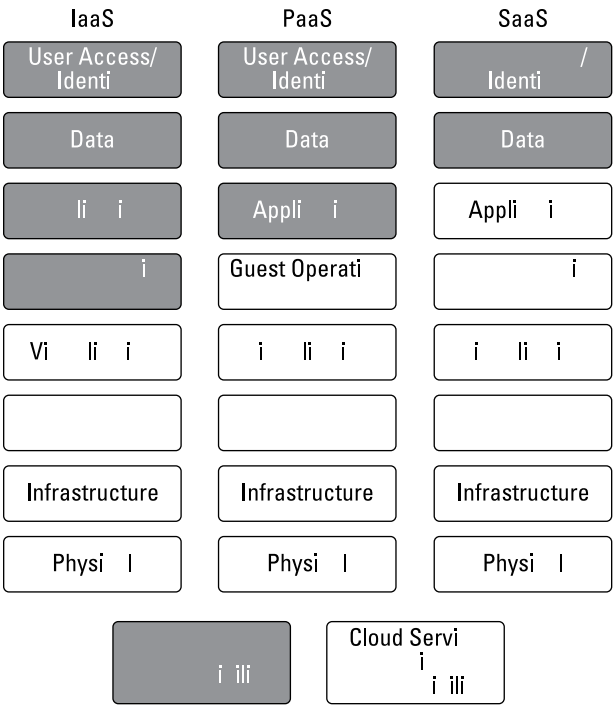

FIGURE 1-1: Shared responsibility differs depending on the cloud service model (SaaS, PaaS, or IaaS).

A key difference between SaaS, PaaS, and IaaS is the level of control (and responsibility) that the enterprise has in the cloud stack:

- In a SaaS offering, the cloud provider is typically responsible for providing security for the entire technology stack from the data center up to the application, whereas the customer is responsible for ensuring that the SaaS application (including configurations) and its data are used in a secure manner by authorized users.
- In a PaaS offering, the CSP is often responsible for security for the technology stack from data center to the guest operating system (OS), while the customer is responsible for securely configuring, managing, and using the applications, data, and user access.
- The demarcation line for IaaS is typically at the OS. The cloud provider manages the virtualization, servers, storage, networking, and data center, while the customer is responsible for securely configuring and maintaining software at the OS layer and above, including middleware, runtime environments, data, and application software.

Trust and verify

Trust is paramount in choosing a cloud partner — not just for your own data, but also for the data owned by your end customers. According to a report from the Economist Intelligence Unit, 92 percent of customers say they "want control over what information is gathered, and a similar share wants to be informed at the point of sale of the data collection capabilities of devices."

Maintaining end-customer data is a huge responsibility, especially when you consider the consequences of errors, omissions, and breaches — which can involve losing customers and incurring millions of dollars in fines. Keep that in mind whenever you decide to do business with a CSP. You're entrusting it with your data, as well as whatever customer data passes through your system.

REMEMBER

According to Juniper Research (`www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches`), the cost of data breaches will rise from $3 trillion per year in 2019 to more than $5 trillion per year in 2024, an average annual growth of 11 percent. Service providers should not only stipulate capacity, availability, and performance requirements, but also provide peace of mind. More and more, that peace of mind stems from unwavering confidence in the security of your applications and data. Verifying the security

capabilities of your cloud vendor includes having a clear view into the shared responsibility security model. You should have a clear understanding of roles and responsibilities for system access, as well as access to security audit reports from a trusted third party.

WARNING

Unfortunately, most customers have only a vague understanding of what their cloud providers do or don't do to protect their data.

The "set it and forget it" myth

In preparation for cloud application adoption, many enterprises plan their IT resources assuming that the bulk of their efforts and resources will be needed during the initial onboarding process. Many companies believe that when the various service settings are configured according to sound guidelines, the ongoing maintenance will require significantly fewer resources. After all, the IT staff should gain experience and familiarity with the cloud service as part of the initial setup. Unfortunately, this is not the case in real-world deployments. And it's one of the most common reasons enterprises falter on their part of the shared responsibility model.

As part of the initial cloud service adoption, plans and standards are leveraged that define rollout plans, which include key configuration settings for the service. These settings include user-specific security requirements, such as the complexity and rotation of credentials. Each

service and application will have unique requirements around privileged accounts used for managing the service. They also include privilege settings for users and administrators and identifying which users have access to which applications, as well as which administrators can create new users or change existing privileges. Although these settings may have been well defined initially, enterprises naturally drift away from them as they attempt to better support the overall business, which must be corrected. Also, if adjustments are not restored to the original configuration and user entitlement settings, those temporary changes become permanent. Because these configuration and user entitlements fall on the customers' side of the shared responsibility model, CSPs cannot and will not remediate drift introduced by the subscriber, though some have begun to provide tools to alert on known risky misconfigurations that need attention.

Although cloud service owners can and should check for configuration drift on a regular basis, such efforts are rarely practiced with any vigor due to the amount of resources needed. For example, chasing down the reason why a configuration was changed six months ago by an administrator who is no longer with the company can be very time consuming and may not even be possible anymore. Unfortunately, simply reverting the configuration without thorough investigation is not an option. As many IT administrators can attest, such an action usually results in a late-night phone call from an angry executive who just realized critical data needed for a board meeting the next day cannot be accessed.

The new model for cloud security

Enterprises must take a new security-first approach to ensure secure use of cloud services and fulfill their obligations under the shared responsibility model. The traditional approach of relying solely on firewalls, proxies, and other solutions to secure the perimeter of the enterprise network doesn't apply any longer. Focusing only on the initial configuration of the service — and expecting the same level of security as the configuration drifts and changes — has also proven to be unrealistic. Unfortunately, even when enterprises recognize the limitations of these approaches, the solution may not seem readily evident.

The IT budget is always under scrutiny, especially as enterprises adopt cloud services. In fact, the promise of a shifted IT spend toward operational expenditures (OpEx) is a commonly expected benefit of adopting cloud services. Given these conditions, enterprises often lack the resources to fulfill their part of the shared responsibility model. They may also lack the dedicated resources to manually audit cloud service configurations on a regular basis.

Instead, enterprises are turning to cloud-based security automation services to help fill the gaps. These solutions are tightly coupled with business-critical services to alert enterprises of critical configuration changes. In some cases, the configurations can even be reverted back automatically. With user behavior analytics, these solutions can also help identify compromised credentials and risky or anomalous behaviors indicative of an attack.

TIP

Cloud security automation represents a much-needed component in addressing the shared responsibility model as enterprise adoption of cloud services continues to accelerate. Although customers are, indeed, responsible for risk vectors like misconfigurations and overprivileged users, CSPs are increasingly offering solutions to mitigate those risks and simplify the journey to the cloud.

SECURITY: NOW A REASON TO MOVE TO THE CLOUD

Security concerns have historically been a top inhibitor to enterprise cloud adoption. However, that perception (and reality) is changing. The 2019 research report, *Security in the Age of AI* (`www.oracle.com/a/ocom/docs/data-security-report.pdf`), found that more than six in ten C-suite executives and policy-maker respondents cite security as the top benefit of cloud technology. According to the Oracle and KPMG *Cloud Threat Report 2020,* three-quarters of organizations say they feel the cloud can provide a more secure environment for their business-critical data than their own data center can.

IN THIS CHAPTER

- Introducing Oracle cloud services
- Identifying Oracle's guiding security principles
- Peeling back the layers of Oracle cloud security

Chapter 2
Exploring Oracle Cloud Security

In this chapter, I fill you in on the Oracle Cloud, Oracle's guiding security principles, and Oracle's security-first approach to cloud security.

Oracle Cloud Services

Oracle cloud services redefine how you modernize, innovate, and compete in a digital world. They deliver complete and integrated cloud services that allow business

users and developers to cost-effectively build, deploy, and manage workloads seamlessly.

Oracle wants every organization to take advantage of the cloud's agility, flexibility, and scalability without compromising its own data or its customers' data. That's why Oracle bakes security into its cloud solutions at the architectural level, ensuring full-stack protection and a platform that's secure by design.

Oracle cloud services provide the following:

- **Complete solutions:** Businesses need complete technology solutions that reduce complexity. They want cloud layers that are fully integrated and integrated with on-premises platforms to deliver a seamless experience.
- **Options:** Oracle gives you many options for where and how you make your journey to the cloud. You can use existing skill sets across technology stacks, run both Oracle and non-Oracle workloads, and connect third-party apps with those from Oracle.
- **Security:** Oracle enables your path to the cloud with layers of security throughout the stack that can help defend and protect every aspect of your on-premises, private, and public cloud environments. Oracle develops, integrates, deploys, and maintains software following Oracle Software Security Assurance (OSSA) processes.

- **Choice:** Options are important on your path to the cloud. With Oracle, you can deploy and manage apps on your private cloud or move them to the public cloud. You can also adopt a hybrid IT model, where certain IT resources run in Oracle cloud services, while others remain on-premises. You can even get the best of both worlds, extending Oracle Cloud into your own data center in order to get the benefits of a cloud but with the added advantage of retaining physical control of the infrastructure.
- **Intelligence:** Oracle helps you realize the value of emerging technologies, including artificial intelligence (AI), machine learning (ML), blockchain, and more. Oracle makes these technologies simpler to access, easier to build and extend, and more efficient to secure and manage.
- **Performance:** Oracle leverages bare-metal instances so each tenant gets predictable high performance and low latency. Oracle offers leading scalability, availability, integrated governance, control, and reliability.

REMEMBER

Encompassing every phase of the product development life cycle, OSSA is Oracle's methodology for building security into the design, build, testing, and maintenance of its products and services. Oracle's goal is to ensure that Oracle's products are helping customers meet their security requirements while providing for the most cost-effective ownership experience.

Oracle provides infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) cloud offerings, including the following Oracle cloud services:

- Analytics
- Application development
- Blockchain
- Chatbot
- Cloud infrastructure
- Content and experience management
- Data integration
- Data management
- Enterprise integration
- Enterprise resource planning
- Human capital management
- IoT applications
- Marketing, sales, and service
- Mobility
- Security
- Supply chain management
- Systems management

Oracle's Security Guiding Principles

Oracle Security protects against major points of vulnerability with a zero trust approach, starting with a cloud architecture that is secure by design. Oracle security extends to a layered approach to provide protection for infrastructure, users, devices, applications, and data.

Oracle cloud security is based on security-first design principles:

- **Securely architect.** Oracle products are architected across both hardware and software to be securely integrated and work together seamlessly. Oracle owns the entire Oracle cloud stack and engineers security throughout the entire stack.
- **Securely deploy.** The open architecture of Oracle products provides customers with great flexibility on how Oracle products are deployed and used. Oracle also assists you in using Oracle products securely, regardless of the technical choices that were made during their initial deployment. For example, Oracle uses standard configurations when deploying databases.

- **Securely maintain.** This means, for example, reducing configuration drift so that patches are deployed appropriately and automatically, while providing monitoring and alerts for database security risks that fall on the customer side of the shared responsibility model.


TIP

Oracle cloud customers can opt to receive periodically published audit reports by Oracle's third-party auditors.

Oracle Cloud Infrastructure: Defense-in-Depth

Cloud services are an essential part of modern business, increasing both opportunities and risks. Oracle Cloud Infrastructure is designed using security-first architecture. The public cloud delivers high customer isolation and automated protections with data resiliency, sovereignty, and cloud security at the core of its innovation and operations. Oracle cloud services are created with multiple layers of security defense throughout the next-generation cloud infrastructure technology stack, including:

- **Preventive controls** designed with a security-first architecture to block unauthorized access to sensitive systems and data

- **Detective controls** designed to reveal unauthorized system and data access and changes through auditing, monitoring, and reporting
- **Automated controls** designed to prevent, detect, and respond to security updates — both regular updates and critical ones
- **Administrative controls** designed to address security policies, standards, practices, and procedures

TIP

Learn more about Oracle Cloud Infrastructure at `www.oracle.com/cloud`.

Oracle aligns people, processes, and technology to secure its physical data centers and offers an integrated defense-in-depth cloud platform:

- **People:** The Oracle cloud employs highly talented, cybersecurity professionals who are trained on OSSA practices:
  - Ten thousand customer support and service specialists, speaking 29 languages
  - Developers trained on Oracle's rigorous coding standards
  - Thirty-eight thousand developers and engineers

- **Process:** Stringent security policies and controls are employed across people, technology, and physical data centers:
  - OSSA methodology, including secure coding standards and vulnerability handling
  - Unwavering support for open standards including the System for Cross-domain Identity Management (SCIM), OAuth, OASIS Key Management Interoperability Protocol (KMIP), and more
- **Technology:** Robust, layered defenses push security down the stack and include layers of defense across IaaS, PaaS, and SaaS, extending security to the network, hardware, chip, operating system, storage, and application layers, bolstered by new security cloud services:
  - Secure cloud architecture designed with high customer isolation and automated protections in mind
  - Security cloud services for identity, application visibility, monitoring, compliance, and data protection
  - Options for encryption, redaction, and data masking in production and nonproduction environments

- ML, AI, and contextual awareness technologies within the cloud security portfolio
- Privileged user access controls on Oracle administrators and customer administrators

» **Physical:** Data centers are built around multilayered physical defenses designed to allow authorized people in and keep unauthorized people out:

- Tier 3 enterprise-grade data centers with redundant power, networking, and critical capacity components
- Multiple physical layers of defense, including access controls and monitoring
- Access cards, biometrics, man traps, and secure zones
- Surveillance and alerts for physical entry and redundant power

Effective cloud security does not only involve a technology decision. Ultimately, it comes down to the cloud platform itself. Does the cloud platform provide a comprehensive approach to security with layers of protection and preventive capabilities? See how Oracle Cloud Infrastructure security offers a security-first approach at `www.oracle.com/security/cloud-security`.

IN THIS CHAPTER

- Mapping different paths to the cloud
- Recognizing identity as the new perimeter
- Keeping your data secure
- Having cloud visibility
- Leveraging machine learning in cloud security

Chapter 3

Securing Your Users, Data, and Apps in the Cloud

In this chapter, you learn about different cloud adoption strategies and their security implications, identity management (IDM) challenges, how to protect your data in the cloud, why you need complete visibility in the

cloud, and how machine learning (ML) is transforming everything from security monitoring and analytics to threat detection and prevention in the cloud.

Multiple Journeys to the Cloud

The journey to the cloud is different for every organization, but it's typically characterized by one of the following strategies:

- **Cloud-first:** Embrace the cloud and actively pursue a "cloud-first" strategy by modernizing existing business applications in the cloud with software as a service (SaaS) applications, developing new "cloud-native" applications leveraging platform as a service (PaaS), and migrating existing app workloads to the cloud using infrastructure as a service (IaaS) rather than upgrading costly legacy on-premises infrastructure. The *ESG 2020 Technology Spending Intentions Study* found that "47 percent of organizations define themselves as having a mature cloud-first program, while 33 percent do not." Cloud-first organizations benefit from rapid deployment of new apps and services, but they often face obstacles with security, risk, and compliance as they scale their businesses and the associated IT support infrastructure.

- **Both public cloud and on-premises:** Adopt a strategy that leverages both public cloud services (including SaaS, PaaS, and IaaS) and existing on-premises data center infrastructure. Organizations that choose this path typically have significant on-premises data center infrastructure investments that they continue to modernize and optimize, but also recognize the benefits of the cloud. They have the flexibility of deploying new apps and services on-premises or in the cloud, as individual business needs dictate, but they often struggle with security, risk, and compliance challenges associated with traditional and/or incompatible tools, technologies, processes, and skill sets across the different environments, as well as systems and application integration issues. According to the Oracle and KPMG *Cloud Threat Report 2020,* only 25 percent of organizations feel they can provide greater security controls within their own data center than a cloud service provider can offer.

- **Lift and shift:** Implement a "lift-and-shift" strategy to move on-premises applications and services to the cloud. Organizations opting for this path often use the cloud as a migration platform and leverage other cloud services, such as PaaS and IaaS, to get there. A lift-and-shift strategy acknowledges the value of the cloud and provides a steady migration path in that direction. Security, risk, and compliance

challenges associated with a lift-and-shift strategy typically include potential downtime, incompatibility issues requiring software modifications or new development, secure data migration, and compliance recertification.

- **On-premises:** Organizations that have their entire IT infrastructure on-premises are often looking for ways to transition key services out of the data center but are still developing their cloud strategies and evaluating different cloud options. They need to eliminate redundancies and enable cost-effective IT services while maintaining or improving their security, risk, and compliance posture. The business effects of COVID-19 in 2020 have accelerated organizational journeys to the cloud. Omdia's 2020–2021 *ICT Enterprise Insights* survey (`https://omdia.tech.informa.com/OM012798/ICT-Spend--Sourcing--ICT-Enterprise-Insights-2021`) found that almost one-third of organizations class the adoption of cloud services as "significantly more important" than before the pandemic took hold.

Identity Is the New Perimeter

Today's users expect a consistent login experience, whether they access your network from a mobile phone on the train, from a desktop in the office, or from a laptop

at home. Ideally, your information systems should recognize people in the same way and support a universal set of access controls, permissions, and password security constraints across all devices and locations.

However, as enterprise computing services become more diverse and many aspects of the IT infrastructure move to the cloud, authorizing people to use enterprise information systems becomes progressively more challenging. How do you handle identity administration, authentication, trust management, access control, directory services, and governance for a disconnected workforce that uses a mix of cloud and on-premises applications?

Historically, user authentication and authorization have been handled by directories associated with specific business applications and computer platforms — often taking the form of simple lists of users and their access privileges. This worked fine for homogeneous computing systems that were protected by a firewall. But controlling access within today's mixed environments, which support many types of information systems both on-premises and in the cloud, is much more complex. Each new application and service often presents new user identities. IT professionals may find themselves re-creating these identities again and again. These repetitive processes create identity silos that spring up with each new deployment, making it difficult to audit usage. Organizations must be able to demonstrate that their system administrators have the correct entitlements for each

application, and their users are correctly authorized to access those applications. This is a recurring challenge in the on-premises world that gets even more challenging as organizations move to hybrid environments by introducing cloud services.

As devices, apps, and user personas multiply, user identities serve as our passports to a vast new world of online services. Federated IDM systems allow external users to securely access internal applications across organizational boundaries. Many organizations use digital identities not only to authorize employees, but also to build trust with customers and partners. In some cases, these services are set up to support credentials from third-party social networks as well. They use federated identities to accept existing credentials from these networks, as well as to socially enable other applications using social network credentials. This unified approach allows people to use their Facebook or LinkedIn credentials to establish an identity on other apps and information systems — an efficient strategy when you're creating an extended social network of customer and partner advocates, but one that does include a degree of increased risk because the industry has seen several examples of credential compromises.

Centralized Identity as a Service (IDaaS) simplifies access to enterprise information resources and enables administrators to easily audit which users can access which

resources at which times. They can maintain constant control and conduct complete entitlement reviews to catch situations where people no longer need access, with outbound credentials for hosted applications in the cloud and inbound credentials from third parties. This mature cloud service streamlines the process of accepting trusted identities and granting access to all types of applications. It's a proven, centralized approach that dramatically expands your ability to leverage the identity platform for all your user authorization needs.

Data Is Your Organization's Most Important Asset

Modern cybercriminals target databases — both on-premises and in the cloud — because that's where your organization's most valuable asset (data) is located.

Sensitive data — such as customer information, financial data, protected health information (PHI), personally identifiable information (PII), and intellectual property (IP) to name a few — is arguably the most important asset for practically any organization today.

Protecting your organization's data — both on-premises and in the cloud — requires an effective defense-in-depth data protection strategy that includes preventive,

detective, and administrative security controls such as the following:

- Transparent data encryption
- Encryption key management
- Data masking
- Privileged user and multifactor access control
- Data discovery and classification
- Database activity monitoring and blocking
- Consolidated auditing and reporting
- Configuration management


TIP

Oracle provides several free online tools to help you assess your organization's data security, including the Oracle Cloud Security Risk Assessment and, for customers, the Database Security Assessment Tool (`www.oracle.com/database/technologies/security/dbsat.html`).

As organizations transition to the cloud, they can gain security by design and default with Oracle Database Cloud Service, automatically encrypting data in transit and at rest. And with Oracle Autonomous Database Cloud, the database automatically applies patches and security updates while running — eliminating downtime and human error and providing increased protection against

emerging threats. With Oracle Data Safe, customers now enjoy the added benefit of active monitoring and alerting for risks resulting from sensitive data in databases and users accessing that data.

SECURITY IN THE AUTONOMOUS DATABASE CLOUD

Oracle Autonomous Database provides security by default in the following areas:

- **Automatic encryption:** All data is automatically encrypted, at rest and in motion, including Transparent Data Encryption (TDE) for all application data.
- **Automatic separation of duties:** Access is monitored and controlled to protect from external access, as well as to defend against unauthorized internal access with privileged user controls.
- **Automatic security patching:** Database security patches and updates are applied automatically, with zero downtime.

(continued)

(continued)

- **Automatic auditing:** Database activity monitoring is automatically enabled, as well as alerts for anomalous behavior.
- **Risk management:** Oracle Data Safe extends security by monitoring for undue risk from configurations, users, sensitive data types and database activity.

Learn more about Oracle Autonomous Database at `www.oracle.com/autonomous-database`.

Cloud Visibility and Consistent Data Protection

Lines of business can move faster when accessing cloud applications to address immediate requirements; unfortunately, IT and InfoSec are often left out of the loop. *Unsanctioned IT* (when software, hardware, and other assets are procured and used without IT authorization or knowledge) often fails to incorporate appropriate organizational security and compliance requirements. IT may have no visibility into what cloud applications users are accessing and what types of data are being shared.

At the same time, misconfigured cloud services, cloud resources, and insecure configurations present two distinct attack surfaces when operating in an IaaS cloud environment. As reported by *SC Magazine* (www.scmagazine.com/featured/cloud-misconfigurations-contributed-to-more-than-200-breaches), "Misconfigured storage services in 93 percent of cloud deployments have contributed to more than 200 breaches over the past two years, exposing more than 30 billion records." Cloud security administrators have a difficult time balancing security in the cloud and maintaining business continuity due to lack of visibility into tenancies that span multiple regions with thousands of different cloud resources, cloud security and privacy knowledge gaps, and limited native support for cloud security orchestration and automation.

Cloud access security brokers (CASBs) provide much needed visibility into cloud services that employees are using and set consistent security policies and governance across sanctioned cloud services. Cloud security posture management (CSPM) services detect cloud infrastructure misconfigured resources and insecure activity across tenants and help provide security administrators with the visibility to triage and resolve cloud security issues.

These approaches can help prevent employees from uploading sensitive data into unsanctioned cloud services. In a recent *Magic Quadrant for Cloud Access Security Brokers*, Gartner recognized that cloud adoption shows no signs of slowing, with SaaS spending up to double that of IaaS. The need to govern cloud use and demonstrate that

governance is in place is clear. When evaluating a CASB and CSPMs, look for solutions that

- Protect your entire multicloud footprint, including IaaS (for example, Oracle Cloud), SaaS (for example, Oracle CX, ERP, and HCM), and PaaS (for example, Oracle Autonomous Database).
- Provide optimal performance with no user impact.
- Integrate with your existing security investments through a simple deployment.

Securing apps

Personnel, technology, and operations are secured with multiple layers of defense across the life cycle of the data in motion, while at rest, and when accessed or used. In Oracle Fusion Applications (for example, CRM, ERP, SCM, and HCM), authentication and password security, encryption, and logging and auditing are mechanisms of redundant defense that enforce protection. A comprehensive defense-in-depth approach to protecting private and sensitive data includes securing sensitive data at rest or stored in database files and their backups, as well as in transit.

Oracle Fusion Applications apply the following standard security principles:

- Least-privilege access
- Containment and no write-down
- Transparency
- Assured revocation
- Defense in depth

Adherence to these principles enhances Oracle Applications Cloud security.

Security Monitoring and Analytics

Modern technology trends, including consumerization, containerization, cloud, mobile, and Internet of Things (IoT), have exponentially increased the attack surface in enterprise IT environments. Additionally, the "snatch-and-grab" attacks of yesterday have been replaced by advanced, multistage attacks that can evade detection by traditional signature-based tools. Meanwhile, DevOps and related continuous integration (CI) and continuous delivery (CD) initiatives have introduced the perfect

storm of faster infrastructure changes and shrinking threat detection windows. Legacy on-premises security monitoring solutions often lack the scale and reliability needed to effectively detect new threats. As a result, IT teams may struggle to keep pace with the volume and sophistication of modern security threats.

Threat Detection and Prevention

Legacy intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) match discrete patterns and signatures in data to known threats. Next-generation IDSs/IPSs leverage ML, employ models that process massive amounts of data and identify patterns that a static set of patterns and signatures in legacy IDSs/IPSs might miss, and then provide probabilistic conclusions about the validity of a threat. The CASBs and CSPMs of today act as the modern equivalents of an IPS/IDS to detect and prevent suspicious behaviors.

Specifically, regarding internal threats around user identity, ML can use the wealth of data it's processing to define a baseline for typical user behavior in relation to one's role in the company and historical activity, which serves as a "norm" against which deviations can be measured. If a user exhibits behavior outside of those well-established expectations, that behavior can be

flagged as an anomaly. This is often called user and entity behavior analytics (UEBA). The power of ML in detecting IT security threats is in its capability to learn, recognize, and make judgments without being programmed specifically for every situation or tactic that cybercriminals may use.

ML is not a new technology, but in the past it was applied largely to basic data processing and optimizing system infrastructure performance. The current groundbreaking application of ML is in its utilization for database automation, marketing automation/personalization, and IT security.

Such applications have become possible due to advancements in compute power, the greater availability of data, and the realization of artificial neural networks that can be "trained" or "learn" how to identify and classify patterns and then make determinations or predictions in relation to the task at hand.

ML brings a new level of sophistication to cybersecurity threat prediction, prevention, detection, and response. In the evolution of IT security, enterprises require intelligent systems that provide visibility into potential threats, send alerts only when necessary, and learn from threat patterns and apply what they've learned to ongoing threat detection and prediction.

ORACLE SECURITY

Oracle has been building security into its solutions and protecting its customers' sensitive data for decades. Oracle has had a long-time focus on security, and this focus is highly important as it pursues a cloud with a security-first approach that automates and integrates security across its cloud services and applications.

Oracle helps protect customers' sensitive data and eases the security burden for their infrastructure and applications with security focused on the following:

- **Secure by design:** Security built in and integrated for infrastructure, applications, and databases with an expanded security portfolio
- **Data defense:** Long-standing focus on data protection and securing the paths to access sensitive data
- **Automation:** Simplifying security and enabling rapid defenses with always-on encryption and self-securing, automated responses

Security is not about a silver-bullet strategy. Oracle pursues a layered security approach, one that begins with securing the core data repositories, followed by layered controls within the application ecosystem to detect and prevent fraud and risks, and leveraging a hardened cloud infrastructure designed to identify and respond to threats, protecting all known paths to the data. Attackers are adept at finding an opening or vulnerability and then using that vulnerability to move across resources within an enterprise. Oracle is focused on not only protecting against that first attack, but also preventing the further progress of an attacker in the attacker's attempts to steal data. Oracle pursues a layered approach across the cloud that spans data, applications, users, and infrastructure.

Learn more about Oracle Security at `www.oracle.com/security`.

IN THIS CHAPTER

- Understanding compliance challenges
- Looking at common regulations and standards
- Managing compliance in the cloud

Chapter 4
Addressing Regulatory Compliance

In this chapter, I cover some compliance challenges, several major regulations and industry standards, and potential approaches to compliance in the cloud.

Recognizing the Compliance Mandate

Many aspects of today's IT environment must adhere to laws and regulations that safeguard sensitive data on behalf of employees, partners, consumers, and patients. Most executives know that data breaches can occur when criminals gain illicit access to IT resources and data, but perhaps less understood is the fact that violations can arise from improper configuration and IT process errors as well. In other words, you don't need to be a victim of a cyberattack for your information systems to be on the wrong side of compliance requirements. It could just be your own oversight or error that puts you out of compliance.

Unfortunately, many companies delay investing in risk management tools until after a compliance violation or data breach has occurred. Because of new challenges and risks that come with the cloud model, being proactive about cybersecurity is more critical than ever. Being unaware of violations won't excuse you from the consequences.

WARNING

You don't need to be a victim of a cyberattack for your information systems to be on the wrong side of compliance regulations. It could just be your own internal oversight or error that leads to fines and penalties.

Organizations require comprehensive, timely, accurate, and actionable compliance data across all environments ranging from production to development and testing. These requirements have never been more important in today's highly virtualized environments where a system life cycle may last anywhere from hours to years. Furthermore, the rapid adoption of hybrid cloud-based services has created additional attack vectors, challenging IT's ability to provide both timely and comprehensive enterprise compliance attestation.

Addressing Regulations and Standards

Regulatory compliance is complicated because there are many laws, regulations, and requirements. This can create a complex and oftentimes subjective strategy that must be continuously examined. Additionally, regulations are dynamic and periodically updated.

There are several important security and privacy regulations, laws, and standards, such as the following:

- **European Union (EU) General Data Protection Regulation (GDPR):** Strengthens and unifies data protection for all EU citizens and addresses the export of personal data outside the EU and data handling

- **U.S. Health Insurance Portability and Accountability Act (HIPAA):** Designed to protect patient confidentiality and data privacy
- **U.S. Sarbanes–Oxley Act (SOX):** Enacted to prevent fraudulent practices and accounting errors in public corporations
- **U.S. Federal Information Security Management Act (FISMA):** Requires federal agencies to conduct annual reviews of information security programs
- **Payment Card Industry Data Security Standard (PCI DSS):** Safeguards the security of credit, debit, and cash card transactions
- **California Consumer Privacy Act (CCPA):** Enacted to protect the personal information that businesses collect

There are also numerous local and international standards and regulations that apply to various industries, fields, and specialized trades.

Maintaining compliance with regulations not only requires significant knowledge and understanding, but can also be expensive and resource intensive. Organizations must identify compliance requirements that are defined by local regulatory entities and international laws and regulations, as well as internal compliance requirements outlined in contracts, business strategies, and company policies.

Internal requirements and service-level agreements (SLAs) may not follow the same regulations as legislated mandates, but businesses can't overlook the overall governance required for internal audits and compliance.

Comprehensive Compliance Strategy

Many compliance regulations demand that you collect, analyze, and store your data securely. You may need to demonstrate compliance during audits and through reporting. You may also need the data for eDiscovery, forensic investigations, and other compliance use cases. To do this effectively, you need to collect comprehensive, timely, accurate, and actionable compliance data across all your IT environments.

Compliance with regulations often should be approached systematically, not one by one, because they often have the following requirements in common:

- Continuous compliance
- A multidisciplinary approach (such as legal, marketing, operations, IT, executives)
- Accountability to customers, employees, partners, and the board of directors

- IT and security best practices

  ce to international best-practice standards and concepts

In order to simplify the compliance effort, businesses should focus on several core technical frameworks. By leveraging similarities among regulations and policies, companies may achieve an integrated approach to enterprise-wide governance, risk management, and compliance. Core compliance technologies include

- **Securing users with identity and access management:** Identity management systems associate specific rights and restrictions with each user's established identity. They govern how employees, contractors, vendors, partners, customers, and other stakeholders use IT resources. To comply with strict regulations, you need to implement access and identity management technology for both application users and IT personnel, including system administrators.
- **Securing apps with application security:** You may need to ensure that the use and administration of your core business applications complies with pertinent regulations governing the privacy of consumers, patients, and citizens. For many organizations, that means evaluating operating

systems, application servers, and databases to establish a compliance score, and then associating that score with relevant benchmarks, rules, and resource evaluations. These evaluations help you to determine your compliance posture.

- **Securing data with data security:** This often includes deploying encryption and key management for data, both at rest and in motion. In addition, data masking is a good way to reduce unnecessary visibility of sensitive data. But these controls represent only a portion of what may be required for data protection — you should also consider implementing technologies like data redaction, data subsetting, key management, privileged user access controls, auditing, and monitoring.

Learn more about managing risk and compliance while reducing fraud with cloud security at `www.oracle.com/cloud/cloud-infrastructure-compliance`.

IN THIS CHAPTER

- Holding your cloud provider accountable
- Gaining an advantage with machine learning and automation
- Layering your defenses
- Managing identities
- Ensuring scalability and visibility
- Maintaining continuous compliance
- Turning on security by default and following security best practices

Chapter 5

Ten Requirements for Better Cloud Security

In this chapter, I describe ten key requirements for cloud security in the modern cloud era.

- **Shared responsibility and trust with a security-first design:** Trust is paramount in choosing a cloud partner to uphold its end of the shared security model (see Chapter 1). You should have a clear understanding of mutual roles and responsibilities and access to independent third-party security audits and attestations while jointly establishing a security-first approach to cloud deployments.
- **Machine learning (ML):** Rapidly evolving and increasingly advanced threats require security solutions that bring a new level of sophistication to threat prediction, prevention, detection, and response with ML.
- **Automation:** Threats are moving at machine speed while traditional enterprise security analyzes and reacts at human speed. Modern security in the cloud and hybrid environments must automate threat detection and response to reduce the risk of human error and unexpected downtime.
- **Defense-in-depth:** Multiple layers of security through the entire technology stack must include preventive, detective, and administrative controls for the right people, processes, and technology to help secure the cloud provider's physical data centers.
- **Identity management:** As mobile devices, apps, and user personas become more ubiquitous, identity has become the new perimeter. Controlling

access and privileges in the cloud (public, private, and hybrid) and on-premises based on secure credentials is critical.

- **Scalability:** Modern security solutions must be able to massively scale and seamlessly interoperate across multiple on-premises and public, private, and hybrid cloud environments.
- **Visibility:** Cloud access security broker (CASB) and cloud security posture management (CSPM) tools extend visibility and control across an organization's entire IT environment.
- **Continuous compliance:** Regulatory compliance is not optional, and compliance and security are not the same thing. You can experience compliance violations without a security breach (for example, due to configuration drift and configuration errors). Look for a cloud management solution that provides comprehensive, timely, and actionable compliance-related data across your on-premises and public, private, and hybrid cloud environments.
- **Security by default:** Security controls should be enabled by the cloud provider by default, instead of requiring the customer to remember to "turn on" security. Not everyone has a strong understanding of different security controls and how they work together to mitigate risk, prevent business fraud, and implement a complete security posture. For example, data encryption should be turned on by

default. Consistent data protection controls and policies need to be enforced on-premises, as well as in public, private, and hybrid clouds.

- **Separation of duties and least privilege access:** The principles of separation of duties and least privilege access are security best practices that should be implemented across on-premises, public, private, and hybrid cloud environments. Doing so helps ensure that individuals don't have excessive administrative rights and can't access sensitive data without additional authorization.

REMEMBER

These ten key requirements for effective cloud security make use of a layered approach that operates on prevention and people. Keep these in mind when considering the next platform for your cloud and its security.

TIP

Learn how Oracle Cloud Security brings a security-first approach at `www.oracle.com/security/cloud-security`.

ORACLE CUSTOMERS SHARE THEIR SECURITY EXPERIENCES

"What I like about Cloud Guard is because it is continuously running and available to a wider group of people, it provides a continuous improvement process in our security posture. It's also included with OCI, which is a really good value."

—Tom Morgan, Threat Intelligence Lead, Cyber Security Group, Darling Ingredients

"With Oracle Cloud Guard on Oracle Cloud Infrastructure, we were able to quickly analyse each alert and assess the associated security risks. Oracle Cloud security allowed us to quickly obtain a key security certification by one of our biggest customers and frees up valuable time to focus on more customer innovations."

—Alexandre Gillet-Markowska - Cloud Security Officer, Discngine

"As part of Oracle Cloud Infrastructure, we found Oracle Cloud Guard to be very powerful to help us discover complex security issues. As a managed service provider, Oracle Cloud Guard helped ALEF anticipate the right security posture for upcoming compliance regulations for our customers and implement them quickly using existing tools and APIs."

—Pietro Lascari, Delivery Manager for ALEF

"Security is a big concern to our customers, because we do have PII information. Oracle does a great job in the security area for us. We really feel like, especially as we move into the cloud, that transparent data encryption gives us the ability to control that encryption process. We have the keys to our data ."

—Keith Wilcox, VP of Database Administration at Epsilon

"Oracle Cloud Guard is an excellent product to automatically identify and resolve security misconfigurations and unused resources on Oracle Cloud Infrastructure. As a result, we have been able to improve our Oracle Cloud governance and security with minimal effort."

—Davide Benedetto, Head Cloud Team, Siram Veolia

"One of the key benefits of moving to the Oracle Database Cloud Service was transparent data encryption– we could ensure our customers that, right out of the gate, their data was secure, and the risk of compromise was minimum."

—Paul Vanhout, CEO and Founder, Pragmatyxs

"It solidifies the conversations I have with my clients about how Oracle builds OCI with security in mind first; Oracle Cloud Guard is a great example of how Oracle continues that heritage."

—Chris Pasternak, Managing Director, Accenture

Secure your data, users, and apps in the cloud

Security has moved from being an inhibitor to cloud adoption to being a reason to move to the cloud for many enterprises. Partnering with a trusted cloud provider with a security-first design architecture can bolster an enterprise's security and compliance posture with the latest defense-in-depth security designs, cloud security experts, machine learning, identity management, cloud security posture management (CSPM) services, and more. Open the book to learn how Oracle Cloud security can help your enterprise protect its apps and data against attacks and comply with industry and government regulations.

Inside…

- Protect your organization's sensitive data
- Help make sense of the shared security model
- Address IT security skills shortages
- Adopt automation in threat detection

ORACLE

Lawrence Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 130 other *For Dummies* books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-81108-4
Not For Resale

Also available as an e-book

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.