Brought to you by:

ORACLE

Cloud Security

for dummies

A Wiley Brand

Detect and respond to threats

Use automation for better security

Maintain continuous compliance

Lawrence Miller

Oracle Special Edition

Table of Contents

Introduction

If one thing

cloud strategies. Today, many of these concerns have been alleviated and organizations are now aggressively moving their 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 is actually more secure than most on-premises environments.

The key is to choose the right technology — one that is designed to protect users, safeguard data, and better address regulatory compliance requirements. In this book, you will 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's 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 48 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 chap

landscape, why traditional security approaches are no
secure cloud environments in a shared responsibility
model.

Machine Learning and the Cloud Are Changing Security

Cloud adoption promises the benefit of increased flexibility, agility, and significant cost savings, so migrating more and more applications including business-critical applications to the cloud is becoming a growing priority for companies of all sizes. The *RightScale 2017 State of the Cloud Report* found that 95 percent of organizations are running applications in the cloud or experimenting with Infrastructure as a Service (IaaS), and 75 percent of enterprises run the majority of their workloads in a public or private cloud.

Although many enterprises adopt new applications on a regular basis, few have real-world experience in securely adopting or using cloud services. Migrating enterprises' business-critical applications and services to the cloud has 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.
- **Shadow IT:** Frustrated by enterprise IT's lack of flexibility and slow responsiveness, and bolstered by the simplicity and ease-of-use in Software as a Service (SaaS) applications, enterprise users have created a "shadow IT" culture — but are oblivious to security and compliance risks.
- **Manual processes:** Slow, error-prone manual IT processes are unable to keep pace with the agility and scale of the cloud.
- **Shortage of skills:** Research by Frost and Sullivan projects the shortage of IT security professionals will reach 1.5 million globally by 2020. An independent survey of 100 UK chief information officers (CIOs) commissioned by Robert Half found that cloud security was the most in demand technical skill (51 percent) and most challenging to fill (32 percent).
- **Security alert overload:** According to the Ponemon Institute, midsize companies average 16,937 alerts per week; however, only 19 percent of those alerts are reliable and only 4 percent are investigated.

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, or supported by the organization.

WARNING

According to a report by QuinStreet Enterprise, 76 percent of organizations have experienced a security incident in the past year.

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 increasingly impossible 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 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. You'll learn more about machine learning and artificial intelligence 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. Simply put, the shared responsibility model outlines the cloud service provider's responsibility to maintain a secure and continuously available service and the customer's responsibility to ensure secure use of the service. The shared responsibility demarcation line for cloud service providers and their customers depends upon the service offering: SaaS, Platform as a Service (PaaS), or IaaS, as shown in Figure 1-1.

REMEMBER

The shared responsibility model outlines the cloud service provider's responsibility to maintain a secure and continuously available service, and the customer's responsibility to ensure secure use of the service.

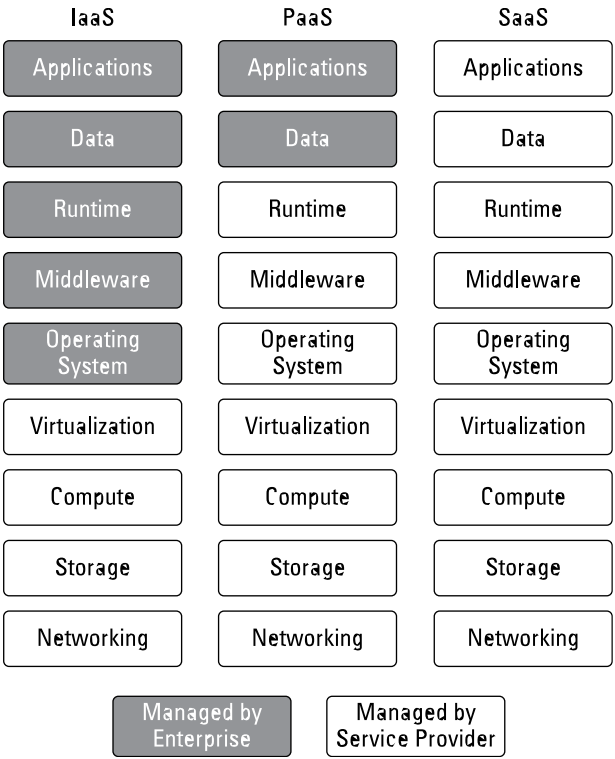

FIGURE 1-1: Shared responsibility differs depending on the cloud service model (SaaS, PaaS, or IaaS).

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 securing the entire technology stack from datacenter up to the application, whereas the customer is responsible for ensuring the SaaS application and its data is used in a secure manner by authorized users.
- In a PaaS offering, the cloud service provider is often responsible for securing the technology stack from datacenter to runtime, while the customer is responsible for the securely configuring, managing, and using the applications and data.
- The demarcation line for IaaS is typically at the operating system: The cloud provider manages the virtualization, servers, storage, networking, and datacenter, while the customer is responsible for securely configuring and maintaining software at the operating system 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 executives say their customers are willing to share personal information such as name, contact information, and demographic details with their trusted vendors.

Maintaining 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 cloud service provider. You are entrusting it with your data, as well as whatever customer data passes through your system.

REMEMBER

The Ponemon Institute's 2017 Cost of Data Breach Study calculates the average cost of a data breach is $3.62 million.

Service providers should not only stipulate capacity, availability, and performance requirements, they should 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 transparent view into how it secures its cloud environment. 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. In a survey conducted by the Independent Oracle Users Group (IOUG), 58 percent of respondents admitted that they don't know whether their cloud providers are accessing

their data, and only 38 percent said their providers will notify them of security breaches. Worse still, only one in four survey respondents said they have received assurances that their data will be deleted after the relationship with the cloud provider ends.

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 mainte- nance 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. Unfor- tunately, this is not the case in real-world deployments. And it is one of the most common reasons why enter- prises falter on their part of the shared responsibility model.

As part of the initial cloud service adoption, IT administrators define roll-out plans that include, among other things, key configuration settings for the service. These settings include user-specific security requirements such as the complexity and rotation of credentials. They also include privilege settings for users and administrators, identifying which users have access to which applications

as well as which administrators can create new users or change existing privileges. Although these settings are well defined initially, enterprises naturally drift away from them as they attempt to better support the overall business. Also, if adjustments are not restored to the original settings, those temporary changes become permanent.

Although IT administrators 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. 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. As a result, many IT administrators simply follow the "don't fix it if it's not broken" model. Some enterprises defer checks for configuration drifts to a quarterly audit exercise, but, more commonly, they simply wait to react to incidents to correct the settings. Unfortunately, both approaches lead to increased risk, which leaves the enterprise vulnerable to attacks and result in significant financial burden.

Mutual responsibility with a shared security model

Enterprises must take a new 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 lower IT spend 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 certainly lack the dedicated resources to manually audit cloud service configurations on a regular basis.

Enterprises are turning to cloud-based security automation services to fill the gaps they cannot afford to close. 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 identify compromised credentials and risky or anomalous behaviors indicative of an attack.

Cloud security automation represents a much-needed solution to address the shared responsibility model as enterprise adoption of cloud services continues to accelerate.

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. In a Coleman Parkes Research survey of more than 1,000 senior security decision-makers, more than three-quarters of respondents said that cloud providers are better able to keep security measures current and up to date than they can. Seventy-eight percent of businesses surveyed say the cloud can improve both their security and their agility.

IN THIS CHAPTER

- Introducing Oracle Cloud
- Learning 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 defense- in-depth approach to cloud security.

Oracle Cloud

Oracle Cloud redefines how you modernize, innovate, and compete in a digital world. It delivers complete and integrated cloud services that allow business users and

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

In a word — well, five words — Oracle Cloud is

- **Complete:** 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.
- **Open:** Oracle gives you more options for where and how you make your journey to the cloud. You can use existing skillsets across technology stacks, run both Oracle and non-Oracle workloads, and connect third-party apps with those from Oracle.
- **Secure:** Oracle enables your path to the cloud with layers of security throughout the stack that defend and protect every aspect of your on-premises, private, and public cloud environments. Oracle develops, integrates, deploys, and maintains software securely following Oracle Software Security Assurance.
- **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, 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-based Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) solution, but with the added advantage of retaining physical control of the cloud infrastructure.

- **Intelligent:** Oracle helps you realize the value of emerging technologies, including artificial intelligence (AI), machine learning, chatbots, and more. Oracle makes these technologies simpler to access, easier to build and extend, and more efficient to secure and manage.

Encompassing every phase of the product development life cycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products. 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 Cloud provides IaaS, PaaS, and SaaS offerings, including the following Oracle Cloud services:

- Application development
- Business analytics

- Cloud infrastructure
- Content and experience management
- Data integration
- Data management
- Enterprise integration
- Security
- Systems management

Oracle's Security Guiding Principles

Oracle Cloud security is based on four guiding principles that are independently verified by third-party auditors:

- **Secure products:** 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.
- **Securely architected:** Oracle products are architected across both hardware and software to ensure that they're securely integrated and work together seamlessly. Oracle owns the entire Oracle

Cloud stack and engineers security throughout the entire stack.

- **Securely deployed:** Oracle's goal is to ensure that deployed instances of Oracle products are secure. The open architecture of Oracle products provides customers with great flexibility on how Oracle products are deployed and used. Oracle also ensures that it is as easy as possible to use 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 maintained:** The Oracle Cloud is securely maintained, for example, eliminating/minimizing configuration drift over time to ensure patches are deployed appropriately, and more.

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

Defense-in-Depth: Securing the Cloud from Top to Bottom

Cloud services are an essential part of modern business, increasing both opportunities and risks. Oracle Cloud is

built around multiple layers of security defense throughout the technology stack, including the following:

- **Preventive controls** designed 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
- **Administrative controls** designed to address security policies, standards, practices, and procedures

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:
  - More than 4,000 cloud operations professionals
  - Developers trained on Oracle's rigorous coding standards
  - 1,700 security personnel for tactical implementations of Oracle Software Security Assurance
- **Process:** Stringent security policies and controls are employed across people, technology, and physical data centers:

- Oracle Security Oversight Committee, chaired by Safra Catz, CEO
- Oracle Software Security Assurance methodology, including secure coding standards and vulnerability handling
- Unwavering support for open standards including the system for cross-domain identity management (SCIM), open authorization (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, and bolstered by new security cloud services:

- Security cloud services for identity,

visibility, monitoring, compliance, and data protection

- Options for encryption, redaction, a

masking in production and nonproduction environments

- Privileged user controls on Oracle a

tors 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

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 cloud migration strategies and their security implications, identity as the new perimeter, and how machine learning 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 is typically characterized by one of the following cloud strategies:

- **Cloud-first:** Many organizations have fully embraced the cloud and actively pursue a "cloud-first" strategy by modernizing their 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 *RightScale 2017 State of the Cloud Report* describes these organizations as "cloud focused," representing 33 percent of small to medium businesses and large enterprises on the journey to the cloud. Cloud-first organizations benefit from rapid turn-up 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.

» **Hybrid:** Most organizations today have adopted a hybrid strategy that leverages both public cloud services (including SaaS, PaaS, and IaaS) and their existing on-premises data center infrastructure. These organizations typically have significant on-premises data center infrastructure investments that they continue to modernize and optimize, but also recognize the benefits of the cloud. RightScale describes these organizations as "cloud beginners" representing 22 percent of organizations on the journey to the cloud. These organizations have the flexibility of deploying new apps and services on-premises or in the cloud, as individual business needs dictate, but often struggle with security, risk, and compliance challenges associated with traditional and/or incompatible tools, technologies, processes, and skillsets across the different environments, as well as systems and application integration issues. According to the Crowd Research Partners *Cloud Security: 2017 Spotlight Report*, 78 percent of organizations feel traditional security solutions either don't work at all or have limited functionality in cloud environments.

» **Lift and shift:** Organizations that adopt a "lift and shift" strategy are in the process of moving on-premises applications and services to the cloud. These organizations 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. RightScale describes these organizations as "cloud explorers" representing 25 percent of organizations on the journey to the cloud. 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 re-certification.

» **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. RightScale describes these organizations as "cloud watchers," representing 14 percent of organizations on the journey to the cloud. They need to eliminate redundancies and enable cost-effective IT services while maintaining or improving their security, risk, and compliance posture.

Do not confuse a "hybrid" cloud strategy with the "hybrid cloud" model. A hybrid cloud, as defined by the U.S. National Institute of Standards and Technology (NIST), is composed of "two or more distinct cloud infrastructures (private, community, or public)."


TIP

If you're doing the math, the organizations pursuing a cloud strategy in the RightScale study add up to 94 percent of small to medium businesses and large enterprises. Another 6 percent of organizations — let's call them "cloud deniers" — don't yet have a cloud strategy, which may not bode well for them over the next three to five years!

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 or a computer in the office. 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 has 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 network environments, which support many types of information systems both on-premises and in the cloud, is much more difficult – particularly in the face of today's strict compliance regulations. Each new application and service often presents new user identities. IT professionals 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 and verify compliance with industry regulations about the safety and attestation of data. Organizations must be able to demonstrate that their system administrators have the correct privileges 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 introduce cloud apps.

As devices, apps, and user personas multiply, user identities serve as our passports to a vast new world of online services. Federated identity management (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.

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
- classification and discovery Database activity
- monitoring and blocking Consolidated
- auditing and reporting
-

Oracle provides several free online tools to help you assess your organization's data security, including the Oracle Cloud Security Risk Assessment (www.oracle.com/webfolder/s/profile/cloud-security/index.html) and, for customers, the Database Security Assessment Tool (DBSAT; www.oracle.com/technetwork/database/security/dbsat/downloads).

SECURITY IN THE AUTONOMOUS DATABASE CLOUD

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

- **Automatic encryption:** All data is au

  cally encrypted, including Transparent Data Encryption (TDE) for all application data.

- **Automatic separation of duties:** A
  control by default. Access is monitored and controlled to protect from external access, as well as unauthorized internal access with privileged user controls.

- **Automatic security patching:** Secu
  patches and updates are applied automatically.

- **Automatic auditing:** Audit by defau
  security relevant activity.

To learn more, visit www.oracle.com/database/autonomous-database/index.html.

As organizations transition to the cloud, they 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.

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. Shadow 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 has no visibility into what cloud applications users are accessing and what types of data are being shared.

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. This approach prevents employees from uploading sensitive data into unsanctioned cloud services. In a recent *Magic Quadrant for Cloud Access Security Brokers*, Gartner claims that "by 2020, 60 percent of large enterprises will use a CASB to govern cloud services, up from less than 10 percent today." When evaluating a CASB, look for the following:

- Protects your entire multicloud footprint, including IaaS (for example, Oracle Cloud), SaaS (for example, Oracle CX, ERP, HCM), and PaaS (for example, Oracle Autonomous Database)
- Provides optimal performance with no user impact
- Integrates 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, HCM, and others), 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 applies the following standard security principles:

- Least privilege
- 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 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 infra- structure changes and shrinking threat detection windows. Legacy on-premises security monitoring solutions lack the scale and reliability needed to effectively detect new threats. As a result, IT teams are unable to keep pace with the vol- ume 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 machine learning and 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, then provide probabilistic conclusions about the validity of a threat.

Specifically, regarding internal threats around user identity, machine learning uses the wealth of data it is 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 machine learning in detecting IT security threats is in its ability to learn, recognize, and make judgments without being programmed specifically for every situation or tactic that cybercriminals might use. Machine learning is not a new technology, but, previously, it was applied largely to basic data processing and optimizing system infrastructure performance. The current groundbreaking application of machine learning is

in its utilization for database automation, marketing automation/personalization, and IT security.

Such applications have become possible due to advancements in compute power, enormous storehouses 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.

Machine learning 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 those learnings to ongoing threat detection and prediction.

ORACLE IDENTITY SOC: SECURITY INTELLIGENCE WITH AUTOMATED REMEDIATION

Traditional security operations centers (SOCs) protect applications and users via static "prevent and defend" tactics. They keep bad guys out of the network, but they don't adapt contextually

to the prospect of an attacker getting into the network. They protect the corporate network, but not the applications and data residing in the cloud. That's a problem for companies with hybrid cloud strategies.

Oracle offers customers a more intelligent alternative that better prevents probable threats, helps detect threats that get through, enhances the response to those threats, and gathers intelligence to more effectively predict potential threats before they occur — all based on the context of user events, moment to moment.

Oracle Identity Security Operations Center is a cloud-based, context-aware, intelligent automation service designed to detect and respond to advanced threats and persistent attacks, as well as establish a feedback loop for adaptation and evolution with machine learning. This means it can better protect users, applications, application programming interfaces (APIs), content, and workloads.

IN THIS CHAPTER

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

Chapter 4
Achieving Continuous Regulatory Compliance

In this chapter, I cover compliance challenges, several major regulations and industry standards, and compliance solutions to implement 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 organizations, industries, employees, partners, consumers, patients, and citizens. 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 regulations. 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 the new challenges and risks that come with the cloud model, it's more critical than ever to be proactive about cybersecurity. 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 require- ments 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 adop- tion 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 so many laws, regulations, and requirements. Some regulations are focused on outcomes and best practices — and not necessarily on how to achieve them — while others are open to interpretation. This can create a complex and oftentimes subjective strategy that must be continuously examined. Additionally, regulations are dynamic and periodically updated.

Here are several important security and privacy regulations, laws, and standards:

- **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.

- **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.

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

Maintaining compliance with these regulations not only requires significant knowledge and understanding, but is also 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.

Holistic Compliance Strategy

Compliance regulations demand that you collect, ana- lyze, and store your data securely. You need to demon- strate compliance during audits and through reporting. You also need the data for eDiscovery, forensic investiga- tions, and other compliance use cases. To do this effec- tively, you need to collect comprehensive, timely, accurate, and actionable compliance data across all your IT environments. Ideally, you should be able to leverage similarities among the compliance policies to build a secure IT environment.

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

- Continuous compliance
- Multidisciplinary approach (such as legal, marketing, operations, IT, executives)
- Accountability to customers, employees, partners, and board of directors
- IT and security best practices
- Adherence to international best practice standards and concepts

There are several core technical frameworks that businesses should focus on to simplify the compliance effort.

By leveraging the similarities among regulations and policies, companies can 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 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 enable you to determine your compliance posture.
- **Securing data with data security:** Deploying encryption and key management for data, both at rest and in motion, is one of the most important

steps to securing sensitive data. This practice ensures that even if sensitive data is lost, it is useless to cybercriminals. Data masking is a great way to ensure that sensitive data is not exposed. It eases the pressure on compliance officers because you aren't storing actual sensitive data. However, these controls represent only a portion of what is required for complete security and data protection. You should also consider implementing technology for data loss prevention, anonymizing data, application layer redaction, and nonproduction data masking.

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 IT Security in the Age of Cloud

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

- **Trust and verify:** 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 roles and responsibilities, and access to independent third-party security audits and attestations.
- **Machine learning:** Rapidly evolving and increasingly advanced threats require security solutions that bring a new level of sophistication to threat prediction, prevention, detection, and response with machine learning.
- **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.
- **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 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 cloud (public, private, and hybrid) environments.
- **Visibility:** A cloud access security broker (CASB) extends visibility and control across an organization's entire IT environment, both on-premises and in the cloud.
- **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 results across your on-premises and public, private, and hybrid cloud environments.
- **Secure by default:** Security controls should be enabled by the cloud provider by default, instead of requiring the customer to remember to "turn on" security. Many customers don't have a strong understanding of different security controls and how they work together to mitigate risk and implement a complete security posture. Examples of security controls that should be enabled by default include encrypting data and preventing unauthorized users from accessing personal data. 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:** The principles of separation of duties and least privilege are security best practices that should be implemented across on-premises, public, private, and hybrid cloud environments. Doing so ensures individuals don't have excessive administrative rights and cannot access sensitive data without additional authorization. For example, in the Oracle Cloud, administrators are blocked from access to customer data by a series of technical controls. Where appropriate, break-glass procedures allow customers to authorize administrator access to the system, but ensure that administrator activity is tracked and recorded during that access.

Secure your data, users, and apps in the cloud

Security was once an inhibitor to cloud adoption, but today security has become a reason to move to the cloud for many enterprises. Partnering with a trusted cloud provider 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 access security broker (CASB) services, and more. Open the book to learn how the Oracle Cloud Platform can help your enterprise protect its apps and data against attacks and comply with mandates like the EU's General Data Protection Regulation (GDPR).

Inside...

- Mitigate shadow IT risks
- Manage security alert overload
- Address IT security skills shortages
- Use machine learning 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.

for dummies®
A Wiley Brand

ISBN: 978-1-119-49268-9
Not for resale