Securing Your Users, Data, and Apps in the Cloud

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

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. 31 »

» 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

compliance32 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited. ance recertification. the pandemic took hold.

challenges associated with a lift-and-shift strategy

typically include potential downtime, incompatibil

ity issues requiring software modifications or new

development, secure data migration, and compli-

» 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

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 33 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

at home. Ideally, your information systems should rec

ognize 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 34 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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 35 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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, 36 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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

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 37 SECURITY IN THE

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) 38 -

(continued)

• **Automatic auditing:** Database activity mon

itoring 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 organi

zational security and compliance requirements. IT may

have no visibility into what cloud applications users are accessing and what types of data are being shared. 39

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 40 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

governance is in place is clear. When evaluating a CASB and CSPMs, look for solutions that Oracle Autonomous Database). through a simple deployment.

» Protect your entire multicloud footprint, including IaaS (for example, Oracle Cloud), SaaS (for example, Oracle CX, ERP, and HCM), and PaaS (for example,

» Provide optimal performance with no user impact.

» Integrate with your existing security investments

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. 41 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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 "snatchand-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 42 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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 43

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. 44 -

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 inte

grated 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 45 -

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. 47 These materials are

Exploring Oracle Cloud Security

ın 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 20 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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

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

» 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. 21 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited. **» 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 intelli-gence (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.

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.22 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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 23 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited. **» Securely architect.** Oracle products are archi-when deploying databases.

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:

tected 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 configurations24 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited. **» 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.

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 25 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited. **» Detective controls** designed to reveal unauthor-ized 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 Learn more about Oracle Cloud Infrastruc-ture 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 26 These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited. physical

data centers: **» Technology:** Robust, layered defenses push by new security cloud services: in mind protection environments

» Process: Stringent security policies and controls are employed across people, technology, and

- 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 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
- Secure cloud architecture designed with high customer isolation and automated protections
- Security cloud services for identity, application visibility, monitoring, compliance, and data
- Options for encryption, redaction, and data masking in production and nonproduction

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

capacity components zones redundant power

» 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
- Multiple physical layers of defense, including access controls and monitoring
- Access cards, biometrics, man traps, and secure
- Surveillance and alerts for physical entry and

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.