Securing SaaS at Scale

Protecting Mission-Critical Business Applications in the Cloud

Cloud **Essentials**

ORACLE Cloud

SaaS Usage Is Growing—Along with Security Problems

When it comes to the cloud, everyone wants in on the action. Whether it's a new ERP system, a mobile CRM module, an online time-and-attendance app, or some other business and productivity service, the demand for software-as-a-service (SaaS) applications is on the rise. Market demands are pushing line-of-business (LOB) owners to deploy new cloud-based functionality at an increasing pace, without the constraints associated with legacy on-premises applications.

All cloud-based systems pose unique security risks and challenges, but ERP applications are particularly vulnerable, given the sensitive nature of their data and functions. According to the Cloud Security Alliance (CSA) ERP Security Working Group, it is vital to understand and evaluate all the risk factors involved with ERP migration, provisioning, and consumption of cloud services.[1] Many SaaS-based ERP apps have only nominal controls governing who can access application services—and there are various other security factors to consider as well.

This guide explains how cloud security architects and IT managers can standardize on SaaS-based ERP applications in a safe and productive fashion, mitigating risks with cost-effective, consistent security controls that protect users, applications, and data. It addresses major concerns summarized by the CSA ERP Security Working Group, and it offers solutions for safe and secure usage of business applications in the cloud, based on Oracle Cloud Access Security Broker (CASB) Cloud Service, Oracle Identity Cloud Service, and related technologies in the Oracle Cloud Security portfolio.

[1]ERP Security Working Group, "State of Enterprise Resource Planning Security in the Cloud," Cloud Security Alliance (CSA), 2018.

Sizing Up the Problem

Securing cloud-based software environments and protecting the associated data has become progressively more challenging with the rise of external cyberthreats, internal fraud, and an onslaught of new, increasingly complex regulatory requirements. As IT professionals seek to scale SaaS apps and integrate them with on-premises applications and databases, the threat landscape expands accordingly. While LOB managers welcome the relative ease of maintaining a cloud-based ERP system, they can't overlook IT policies governing the security and integrity of application data, not to mention privacy constraints prescribed by government and industry regulations.

> "When it comes to today's pressing cybersecurity challenges, the most frequently mentioned concern is difficulty detecting and responding to security incidents in a cloud environment."
>
> **Oracle and KPMG Cloud Threat Report 2018**

According to the recent Oracle and KPMG Cloud Threat Report, 97 percent of organizations surveyed have policies in place that require the IT or security team to approve and review cloud services. Yet 82 percent of the respondents believe these policies are being violated as employees introduce cloud services without going through the proper channels.[2]

As organizations add more SaaS apps and simultaneously scale out their users, data, and devices, it becomes progressively more difficult to maintain the appropriate security layers required to protect these hybrid, multicloud-enabled enterprises. Today's mobile workforce has dramatically shifted the concept of a network perimeter, and boundaries are no longer defined by a corporate intranet or surrounded by a firewall. While perimeter security, firewalls, and intrusion detection systems remain important, these legacy solutions are not designed to effectively support the cloud threat landscape. In fact, 84 percent of IT pros interviewed for a recent cloud security report said that traditional security solutions either don't work at all in cloud environments, or have only limited functionality.[3]

[2] "Oracle and KPMG Cloud Threat Report 2018: Keeping Pace at Scale—The Impact of the Cloud-Enabled Workplace on Cybersecurity Strategies," study sponsored by Oracle and KPMG, 2018.
[3] Crowd Research Partners, "2018 Cloud Security Report," 2018.

You're Responsible for Security and Compliance

Most SaaS vendor agreements stipulate a shared responsibility model. The vendor guarantees to provide a secure and continuously available application service, while the customer secures access to that service by its employees. In some cases, the customer is also responsible for securing the data in the SaaS apps. In a SaaS shared responsibility model, customers own the identity and access management (IAM) policies for SaaS apps as well as the customer data within those apps. While a cloud provider is responsible for the security of its global infrastructure, each customer must implement security measures according to its own corporate risk policies.

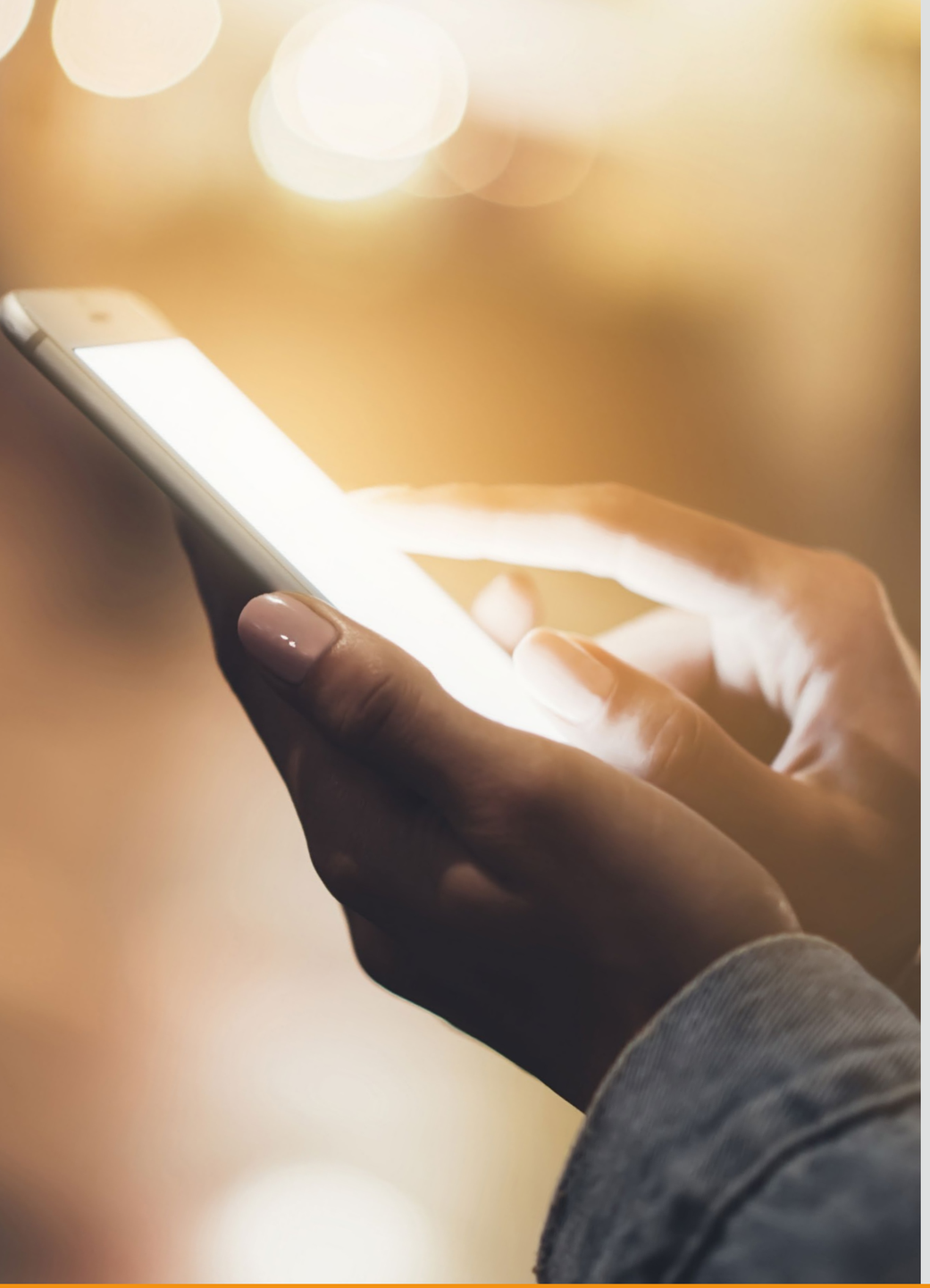
IT organizations may only acknowledge a few dozen SaaS applications that have been officially sanctioned by the enterprise. In reality, most large organizations contend with hundreds or even thousands of cloud services, due, in part, to rogue or unauthorized use of apps that can be easily downloaded to computers and mobile devices—a phenomenon known as shadow IT.

All these factors contribute to the difficulty of mitigating cloud security risk in a cohesive way and complying with government and industry regulations. For example, organizations that collect personal data must be able to prove that they uphold privacy and security principles. With the advent of new European Union General Data Protection Regulations (GDPR), many business leaders recognize that organizations must account for, and successfully protect, EU citizens' personal data.

These regulations are dynamic and regularly updated. The onus is on the organization to comply, and the fines can be severe: as high as €20 million for GDPR mishaps and in excess of US$1.5 million per Health Insurance Portability and Accountability Act (HIPAA) violation.

> "97 percent of organizations surveyed have policies in place that require the approval and review of cloud services by the IT or security team. However, 82 percent of respondents believe these policies are being violated as employees bring on cloud services without going through the proper channels."

Oracle and KPMG Cloud Threat Report 2018



Manage User Identities Across All Enterprise Resources

Historically, user authentication and authorization was handled by directories associated with specific business applications and computer platforms, or by individual user IDs. This worked fine for on-premises information systems protected by a firewall. But controlling access within today's multicloud environments is much more difficult. Hackers may hijack legitimate credentials to gain access to your SaaS apps. Once they gain access, they can misappropriate funds, steal data, take control of enterprise systems, and disrupt operations. These data breaches and attacks are more likely to occur when companies have inadequate IAM systems.

Most organizations depend on a mix of cloud and on-premises applications, and each has its own method of identifying users and provisioning access to IT resources. As the CSA ERP Working Group suggests, you must continually monitor user activity to detect malicious and anomalous behavior. The day-to-day functioning of large organizations requires employees of various trust levels and roles to have access to business-critical applications, as well as to the highly sensitive data that resides in them.[4] To do this safely, you need adaptive, multifactor authentication for both users and administrators—at a minimum, for privileged users—along with dynamic, risk-based policy controls that identify unusual login patterns, such as when a known user enters an application through an unknown device, network, or other unusual context.

IAM policies for ERP systems and other business applications should include the automatic provisioning and deprovisioning of users. When employees join the company, their authorizations are automatically provisioned. When they leave the company, their entitlements are automatically revoked, keeping company data safe.

[4] ERP Security Working Group, "State of ERP Security in the Cloud," CSA, 2018.

Other essential risk-based policies should be in place to detect suspicious user activity within cloud applications, such as requests from nonreputable IP addresses and network domains.

Oracle Identity Cloud Service

This synchronizes user identities from on-premises sources such as Oracle Directory Services, Microsoft Active Directory, and other LDAP directories, extending on-premises identities to the cloud with appropriate access controls. It simplifies login procedures by federating access to multiple applications via single sign-on, while also automating account management, provisioning, and auditing of user activities. As new cloud applications come online, you can use Oracle Identity Cloud Service to securely provision the users of those applications based on their on-premises identities.

Benefits of Identity as a Service

- Rationalizes user access to diverse platforms and devices
- Securely authorizes a broad base of users—on both sides of the firewall
- Eliminates identity silos with centralized management
- Scales up and down to meet business demands in a cost-effective way

"48 percent of security professionals said they rely on multifactor authentication to lock down sensitive data and mission-critical assets."

Oracle and KPMG Cloud Threat Report 2018

Monitor Users and Activity with a Cloud Access Security Broker

Network security used to be a matter of monitoring access to on-premises data sources accessible via enterprise applications behind a firewall. Today's users can upload sensitive company data to cloud data centers anywhere in the world, and from any location. They may also connect their personal devices to the corporate Wi-Fi network to access cloud-based social networks, despite company policies that prohibit such behavior. These routine activities are not only risky, but also extremely difficult to monitor.

As the CSA ERP Security Working Group points out, security professionals need to actively monitor what users are doing at any point in time in order to detect malicious and anomalous user behavior. This is important because the day-to-day functioning of large organizations requires employees of various trust levels and roles to access ERP solutions and other business-critical applications, and the highly sensitive data that resides within them.

The starting point for implementing comprehensive SaaS security is a CASB that can enforce security policies and extend user entitlements to the cloud. It builds a baseline of normal, white-listed activities, and then sends alerts when a system or user defies accepted usage patterns.

Oracle CASB Cloud Service meets SaaS security requirements by allowing you to configure standard security settings that are inherited by each cloud application—as well as for infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) deployments.

Once these fundamental values are established, Oracle CASB Cloud monitors your cloud service settings and alerts you to any changes. It prevents configuration drift by enabling you to restore approved settings at any time, eliminating tedious investigations and making it easier

to prepare for compliance audits.
You can use Oracle CASB Cloud to monitor on-premises apps in your data center as well as cloud apps connected to them. This holistic visibility enables you to quickly identify threats across multiple cloud services and take remedial action to address the source of each problem. Predictive analytics and automated operations prevent future incidents by using machine learning technology to identify what constitutes normal behavior and what does not—so your security systems get smarter over time.

In a SaaS environment, Oracle CASB Cloud can monitor changes to security policies in critical business apps, such as the creation of or changes to role settings, which may impact the access privileges for sensitive information. A CASB can also monitor suspicious or malicious activity, such as detecting user or admin sessions from suspicious IP addresses or geo-locations. Oracle CASB Cloud uses machine learning to automatically detect risks when accounts are compromised, such as users logging in from unexpected locations and unrecognized devices.

Benefits of CASB

- Provides visibility into user activity and shadow IT
- Protects against external and insider threats
- Secures data from exfiltration
- Enforces consistent policies and compliance

"We chose Oracle CASB Cloud Service and Oracle Advanced Security to minimize risk exposure and gain transparency, high visibility, and control. This allowed us to stay a step ahead of threats while enforcing our cloud environment security configurations and EU GDPR compliance with minimum performance impact."

Dimosthenis Nikolopoulos, IT Operations and Program Management Director, WIND Hellas

Automate Incident Response

Manually monitoring users, data, and encryption policies across hybrid and multicloud information systems is an immense task. Large organizations receive thousands of security alerts per week, and most of these organizations don't have the time or personnel available to review the bulk of their security event data.

In addition, APIs contain IP addresses that can be accessed from outside trusted organizational boundaries. You need adequate controls to monitor API usage and detect unusual activities.

As more and more mission-critical applications move to the cloud, organizations must employ consistent activity monitoring controls that automatically predict, prevent, detect, and respond to these threats—and keep sensitive information secure. Cyberattacks aren't all you need to worry about—you must also look out for internal mistakes and negligence from IT administrators, which can compromise compliance regulations. Discerning between friend and foe involves making sense of alerts across a huge variety of systems, applications, and datasets—everything from system and application logs, user session activity, use of sensitive resources, and changes to security configurations.

To automate ERP security, some customers store their ERP data in Oracle Autonomous Database, which uses machine learning technology to automatically detect and fix problems without human intervention—a capability known as adaptive response. Bolstered by machine learning algorithms, this intelligent database defines baselines for normal and expected user behavior, providing a standard for measuring deviations.

Put Security Patching on Autopilot to Alleviate Vulnerabilities

SaaS apps shift the responsibility for applying software patches and updates to the cloud provider. It is the provider's job to ensure that your ERP instance is free from vulnerabilities.

Hugely damaging security lapses can occur if patches are not applied in a timely manner, but how do you know whether or not your cloud provider is actually performing important security updates?

Oracle has the answer with Oracle Autonomous Database, which detects available patches and automatically applies them to avoid errors or human omissions.

> Oracle Autonomous Database uses machine learning technology to minimize labor, eliminate human error, and automate incident response.

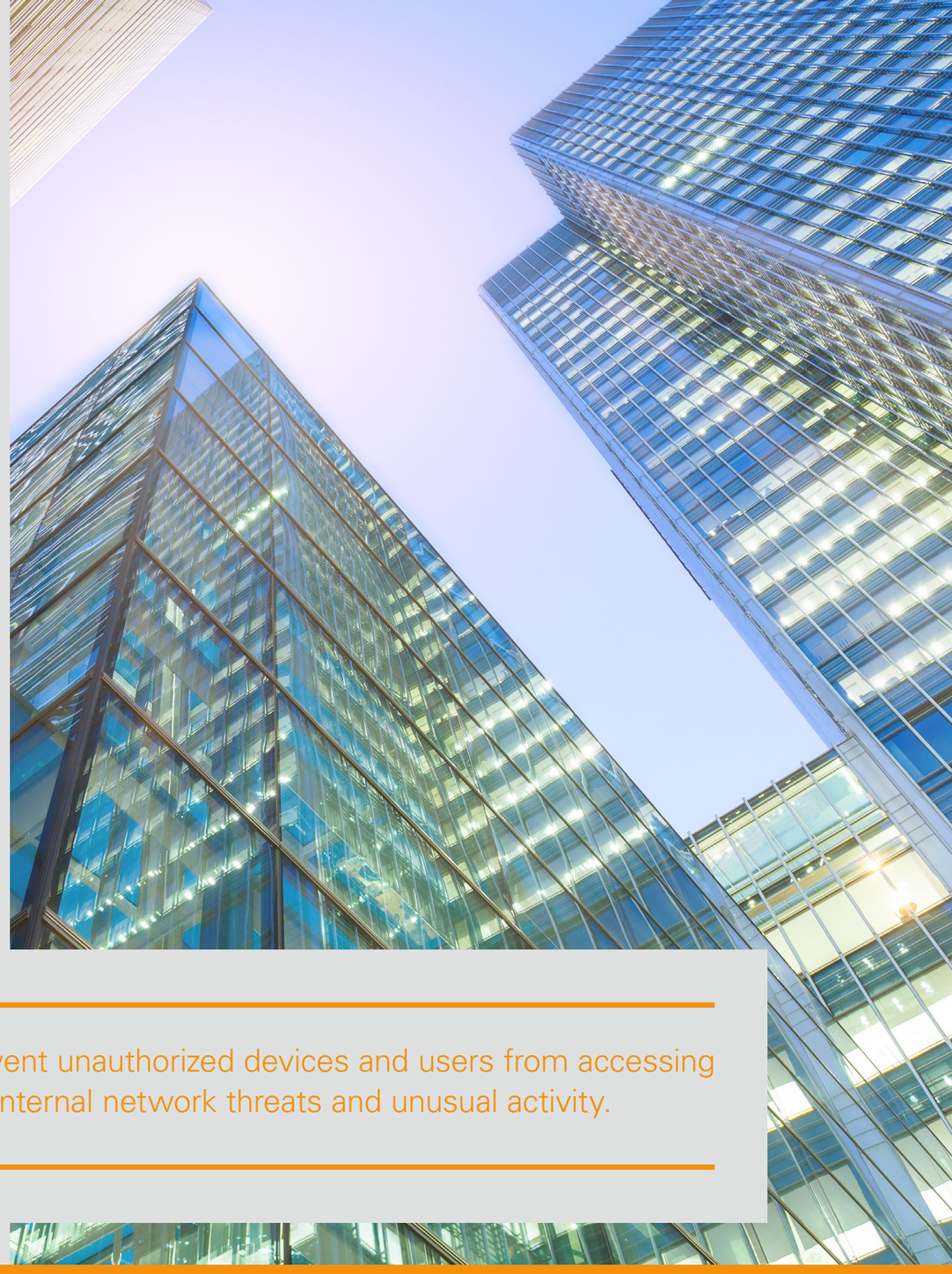
Security updates are applied automatically without downtime, and data is encrypted automatically—leaving nothing to chance. Additionally, Oracle autonomously secures the databases by providing automatic, transparent encryption of data at rest and in transit to prevent external database access.

Oracle automates the protection from potentially malicious internal users by implementing strong user controls that prevent administrators from seeing user data. This means Oracle employees cannot see customer data and customers have complete control over access to it.

Address Data Residency and Regulatory Requirements

For some industries, such as financial services and healthcare, data residency requirements necessitate maintaining data within certain domiciles to comply with government regulations. In addition, organizations must collect, analyze, and store data in a way that adheres to privacy regulations such as HIPAA for healthcare organizations and the Payment Card Industry Data Security Standard (PCI DSS) dictates for retailers. Companies in these industries need to show compliance during audits and through reporting, as well as ensure that certain types of data remain in designated domiciles.
That means imposing controls on cloud usage to enforce compliance with these and other industry regulations, and being able to detect when cloud service usage and configurations are at risk of falling out of compliance. Inadvertent technology misconfigurations and lack of security controls can lead to security vulnerabilities that result in compliance violations and potential data breaches. Staying proactive and vigilant is critical.

Oracle Configuration and Compliance Cloud Service simplifies compliance for both on-premises and cloud resources by automating the configuration, scanning, assessment, scoring, and reporting of your compliance posture, so you can focus on remediation rather than enforcement. It automatically monitors security configurations and helps you evaluate corporate policies for compliance readiness. Compliance officers receive enterprisewide assessment snapshots, while IT administrators receive compliance violation work lists, so they can prioritize the remediation of severe violations that affect their compliance scores. In addition, Oracle has cloud data centers throughout the world, enabling customers to observe data residency requirements, and fulfill regulatory requirements.



Threat protection software must not only prevent unauthorized devices and users from accessing corporate cloud services, but also be alert to internal network threats and unusual activity.

Secure Oracle and Third-Party Clouds

Oracle's cloud security portfolio protects your entire technology footprint—not only SaaS applications, but also IaaS and PaaS services. It includes out-of-the-box rules for Oracle Cloud as well as for third-party services such as Amazon Web Services and Microsoft Azure. By establishing baselines of typical behavior, Oracle's cloud security products use automated technology to recognize unusual activities, such as when a user changes permissions, privileges, or configuration settings. Rather than manually investigating incidents separately in each application, and at each layer of the stack, your security operations center (SOC) can obtain a complete view of a multicloud environment, including all users and devices, through a single pane of glass.

This comprehensive security portfolio, anchored by Oracle CASB Cloud Service and Oracle Identity Cloud Service, interacts with other Oracle security technologies to enable an identity SOC approach. Governed by automated technology, this addresses and remediates threats with little or no human interaction.

- Secure the entire cloud stack including IaaS, PaaS, and SaaS.
- Identify risky users and compromised credentials.
- Auto-respond to incidents.
- Identify anomalous behavior within cloud and on-premises apps.
- Eliminate configuration drift with custom alerts and remediation.

Oracle brings together the best security technology, people, processes, and policies, and gives you visibility into an integrated portfolio of security apps through a single pane of glass. This advanced security portfolio enables you to standardize on cloud-based ERP applications in a safe and productive fashion. You can mitigate risks with cost-effective, consistent security controls that protect users, applications, and data.

For more information, please visit:

iPaper: Mitigate the Top Nine Cloud Threats with a CASB
iPaper: Managing Identities Across Hybrid Clouds
Brief: Better Security with Oracle Cloud

Oracle Identity Security Operations Center: Security Services

Modern SaaS-Delivered Artificial Intelligence and Automation Platform

Protect your business-critical cloud services by combining visibility, threat detection, compliance management, and automated incident response into a single platform.

Your Automated Future

Artificial intelligence (AI) technology is fundamentally altering enterprise computing by changing how organizations receive, manage, and secure business data. By 2020, Oracle predicts that 90 percent of all applications and services will incorporate AI at some level—and that more than half of all enterprise data will be managed autonomously.

Intelligence at Every Layer

Oracle's complete, integrated cloud platform includes intelligent solutions that span the SaaS, PaaS, and IaaS layers. For example, Oracle embeds intelligence into all of its apps. Oracle also extends intelligence into the platform, making it available for any developer to build upon. The goal is to make cloud technologies simpler to access, easier to create, and more efficient to secure, manage, and run—so you can achieve real business outcomes.

Bring Your Own License

Oracle recently introduced two new programs to make it easier to buy and consume cloud services, helping you get more value from your hardware and software investments.

- **Oracle Universal Credit Pricing** enables you to access current and future Oracle Cloud Platform and Oracle Cloud Infrastructure services under a single umbrella contract.
- **Oracle's Bring Your Own License** program enables you to apply your on-premises software licenses to equivalent Oracle services in the cloud.

These popular programs alleviate cloud adoption challenges by simplifying the way your organization purchases and consumes cloud services.

Cloud **Essentials**

Learn more about cloud security for SaaS, and how to manage identities across the hybrid cloud. Try Oracle Cloud today. Go to cloud.oracle.com/try it