Cloud **Essentials**

Better Security with Oracle Cloud

Technology safeguards, fewer risks, and unparalleled security motivate CIOs to embrace cloud computing.

ORACLE®

If one thing is constant in the IT world, it's change. Consider the age-old dilemma of security versus innovation. Just a few years ago, concerns about data security and privacy prevented some organizations from adopting cloud-based business models. Today, many of these concerns have been alleviated. IT leaders are migrating their applications and data to the cloud in order to benefit from security features offered by some cloud providers.

The key is to choose the right technology—one that is designed to protect users, enhance safeguarding of data, and better address requirements under privacy laws. Find out why millions of users rely on advanced and complete cloud services to transform fundamental business processes more quickly and confidently than ever before.

The Evolving Security Landscape

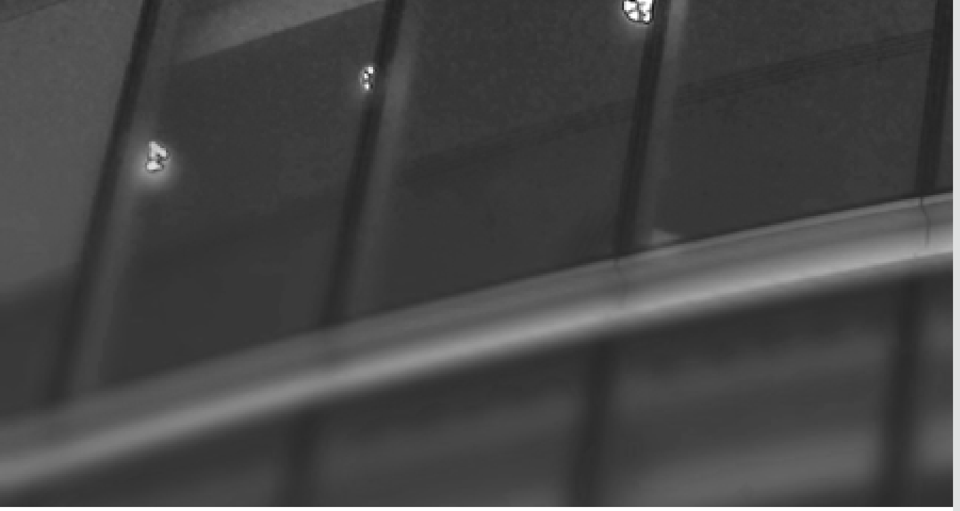
- **Sophisticated threats:** 76 percent of organizations experienced a security incident.[1]
- **Security alert overload:** Midsize companies average 16,937 alerts per week; only 19 percent are reliable and 4 percent are investigated.[2]
- **Scarcity of talent:** 66 percent of cybersecurity jobs cannot be filled by skilled candidates.[3]
- **Porous perimeter:** 91 percent of organizations have security concerns about adopting cloud; only 14 percent believe traditional security is enough.[4]

[1] QuinStreet Enterprise, "2015 Security Outlook: Meeting Today's Evolving Cyber-Threats," *baselinemag.com/security/cyber-attacks-are-more-targeted-and-sophisticated.html*.

[2] Ponemon Institute, "The Cost of Malware Containment," 2015.

[3] Leviathan Security Group, "Quantifying the Cost of Cloud Security," *blog.cybersecuritylaw.us/2016/02/15/cyber-round-up-obamas-19b-cybersecurity-plan-us-it-professional-overconfident-in-cyberattack-detection-secure-your-plant-managing-risk-posed-by-hackers-that-target-iiot*.

[4] Crowd Research Partners, "Cloud Security: 2016 Spotlight Report," *crowdresearchpartners.com/wp-content/uploads/2016/05/Cloud-Security-Report-2016.pdf*.



The Industry's Best Cloud Security Services

- Comprehensive security offerings for all cloud deployments
- Built-in controls at every layer, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS)
- Consistent security features across hybrid deployments
- Governance, visibility, and transparency into cloud services

Mitigating the Risk of Data Loss with Cloud Technology

The IT security practices of many organizations that manage their own systems may not be strong enough to resist complex threats from malware, phishing schemes, and advanced persistent threats unleashed by malicious users, cybercriminal organizations, and state actors. The perimeter-based security controls typically implemented by organizations who manage their own security—from firewalls, intrusion detection systems, and antivirus software packages—are arguably no longer sufficient to prevent these threats.

It's time to look further. It's time to look to the cloud. Thousands of organizations and millions of users obtain a better security position using a tier 1 public cloud provider than they can obtain in their own data centers. A full 78 percent of businesses surveyed say the cloud can improve both their security and their agility.[5] Consider the facts: Most of today's security budgets are used to protect the network, with less than a third used to protect data and intellectual property that resides inside the organization.[6] Network security is important, but it's not enough.

Building Oracle's Defense-in-Depth Strategy

Oracle Cloud is built around multiple layers of security and multiple levels of defense throughout the technology stack. Redundant controls provide exceptional resiliency, so if vulnerability is discovered and exploited in one layer, the unauthorized user will be confronted with another security control in the next layer.

But having some of the world's best security technology is only part of the story. Oracle aligns people, processes, *and* technology to offer an integrated defense-in-depth platform:

- **Preventive** controls designed to mitigate unauthorized access to sensitive systems and data
- **Detective** controls designed to reveal unauthorized system and data changes through auditing, monitoring, and reporting
- **Administrative** measures to address security policies, practices, and procedures

[5] Coleman Parkes Research, "A Secure Path to Digital Transformation," *oracle.com/us/solutions/cloud/cloud-security-survey-report-3103730.pdf*.

[6] CSO Market Pulse, "An Inside-Out Approach to Enterprise Security."

Finding a Cloud Partner You Can Trust

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.[7]

Maintaining customer data is a huge responsibility, especially when you consider the consequences of errors, omissions, and breaches—which can involve losing face with customers and accruing 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 plus whatever customer data passes through your system.

Service provider contracts should not only stipulate terms for capacity, availability, and performance. 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.

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, 58 percent of respondents admitted that they don’t know

[7] Economist Intelligence Unit, “The Economics of Digital Identity,” 2015.

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 contract with the cloud provider ends.[8]

Oracle Cloud customers can receive periodically published audit reports by Oracle's third-party auditors. Customers may also request a copy of the current published audit report available for a particular Oracle Cloud service.[9] Administrative access to your Oracle Cloud environment includes multiple security zones to restrict access on a need-to-know basis for all IT staff.

Logical access controls encrypt data on staff computers, while personal firewalls, two-factor authentication, and role-based accounts further protect your data and applications.

Oracle offers a variety of options to implement preventive security controls for data at rest and in transit for different cloud services, including encryption by default as part of Oracle Database Cloud Service, redaction of sensitive application-layer data, restriction of privileged-user capabilities, subsetting or masking of data in nonproduction environments, and monitoring of user activities.

Oracle's Guiding Principles

- Secure products
- Securely architected
- Securely deployed
- Securely maintained
- Independently verified

[8] Independent Oracle Users Group, "2016 IOUG Cloud Security Survey," 2016.

[9] Note: Reports may not be available for all services, or at all times.

Securing the Cloud from Top to Bottom

Cloud services have become an essential part of modern business, increasing both opportunities and risks. Oracle provides security features and options at every layer of the cloud.

Technology: Robust, layered defenses span IaaS, PaaS, and SaaS, extending security to the network, hardware, chip, operating system, storage, and application layers, bolstered by new security cloud services.

Process: Security policies and controls are maintained by people and technology at physical data centers.

People: The Oracle Cloud employs talented, industry-leading cybersecurity professionals who are trained on Oracle Software Security Assurance practices.

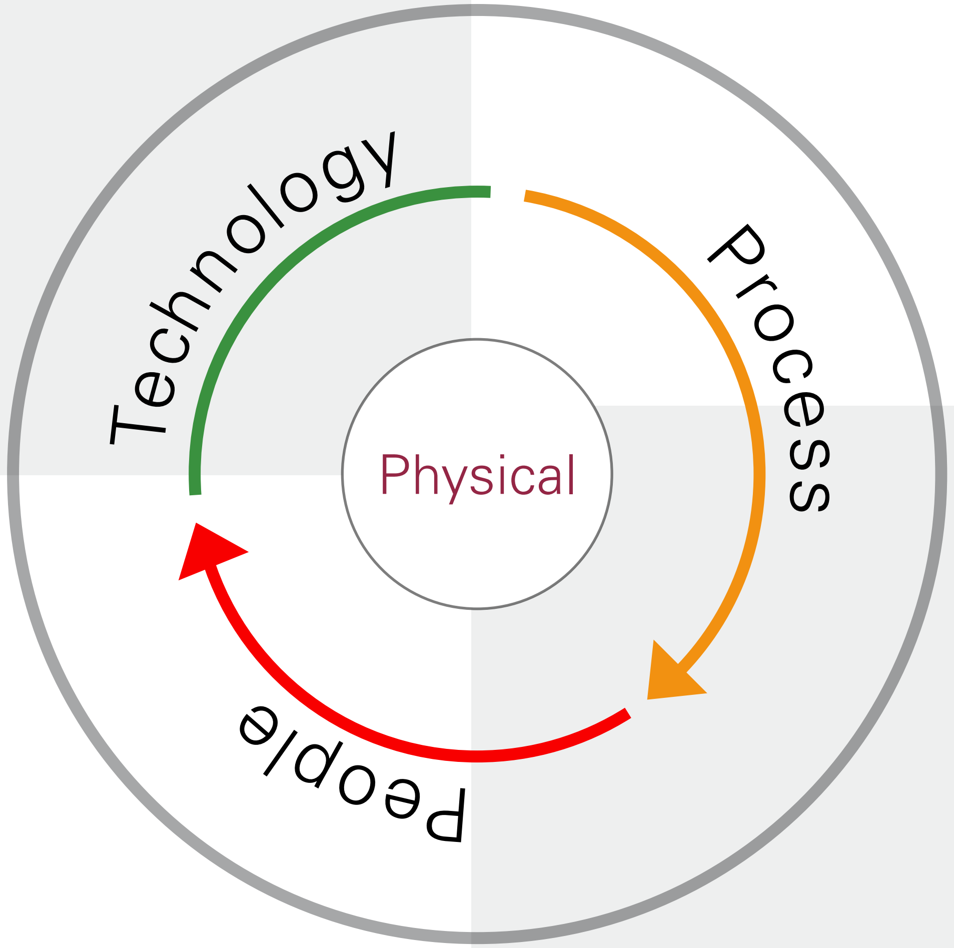
Physical: Data centers are built around multilayered physical defenses designed to allow authorized people in and keep unauthorized people out.

Technology

Push security down the stack and include layers of defense across IaaS, PaaS, and SaaS.

Process

Employ stringent security policies and controls across people, technology, and physical data centers.



Physical

Design physical access controls to secure access to data by Oracle employees and customers.

People

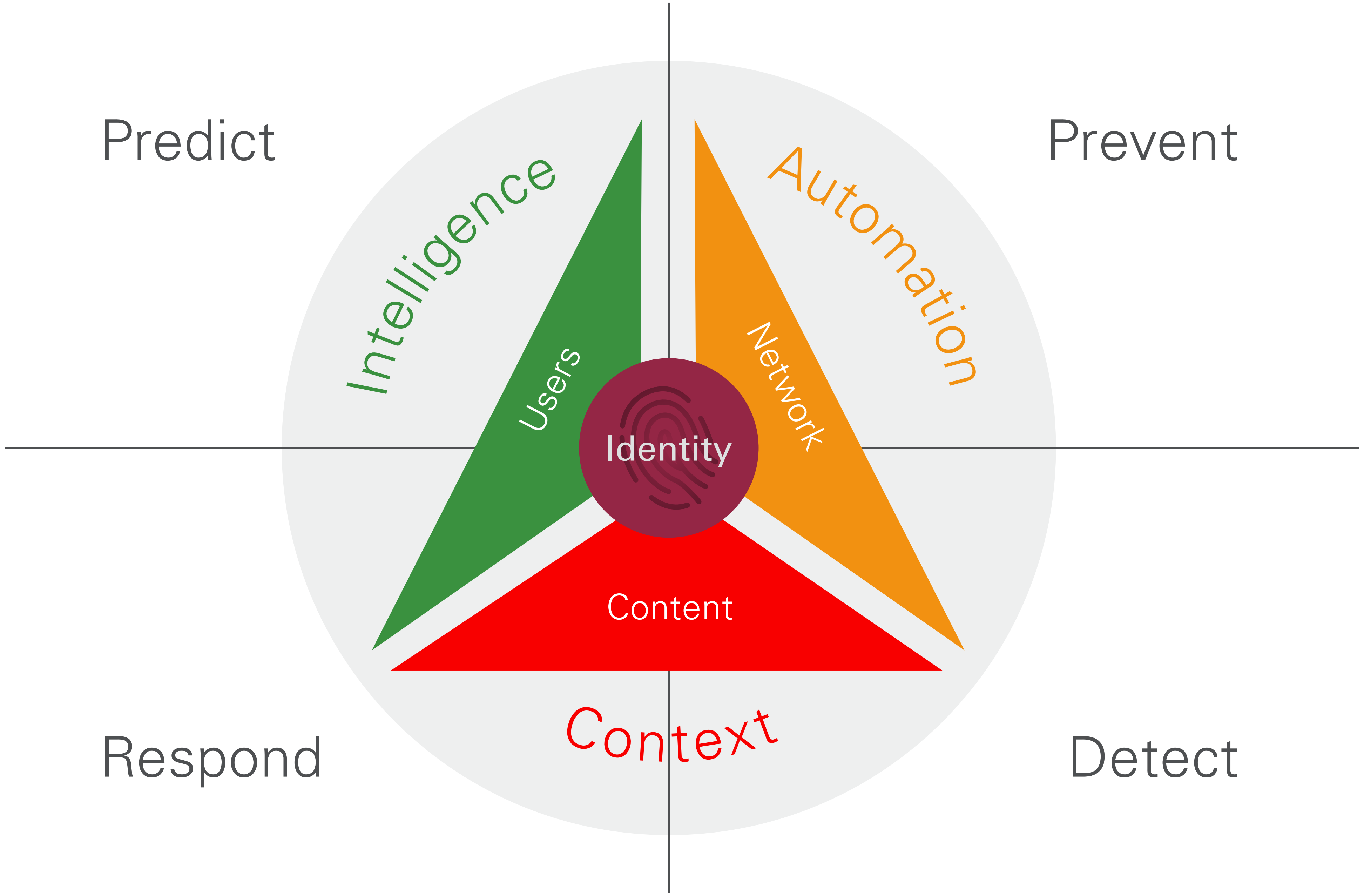
Hire highly talented cybersecurity resources and train them on Oracle Software Security Assurance methodology.

Bringing Intelligence to Security Operations Centers

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. This means it can better protect users, applications, APIs, content, and workloads.

Security Intelligence Delivered with Identity



Getting the Security—and Talent—You Need

IT security talent is in short supply. ISACA—a nonprofit, information security advocacy group—predicts there will be a global shortage of 2 million cybersecurity professionals by 2019. Every year in the US, 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cybersecurity related roles, according to cybersecurity data tool CyberSeek.[10]

When you move to Oracle Cloud, you take advantage of Oracle's large pool of security talent. By defining security assurance programs, implementing secure development practices, and driving secure standards policies, Oracle gives customers even more reasons to trust Oracle Cloud. Oracle's 19 worldwide cloud data centers are aligned with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27002 Code of Practice for information security controls. All servers include redundant subsystems (such as cooling, power, network links, and storage) and compartmentalized security zones controlled by biometric access control methods, video surveillance, and alerts for security incidents, physical breaches, and disasters.

Gaining an Edge with Cloud Security

In the Digital Age, companies depend on their information systems to connect with customers, sell products, operate equipment, maintain inventory, and carry out a wide range of other business processes. If your data is compromised, IT assets quickly become liabilities. A 2016 Ponemon Institute study found that the average cost of a data breach continues to rise each year, with each lost or stolen record that contains confidential information representing US$158 in costs or penalties.[11] In response, more and more organizations are transitioning their information systems to the cloud to achieve better security for sensitive data and critical business processes.

Security used to be an inhibitor to moving to the cloud. Now it's an enabler to get you where you need to go. Oracle helps you embrace the cloud quickly, and with confidence.

[10] Jeff Kauflin, "The Fast-Growing Job with a Huge Skills Gap: Cyber Security," Forbes, March 16, 2017.

[11] IBM Security, "2016 Ponemon Cost of Data Breach Study," *ibm.com/security/data-breach*.

Oracle Cloud Security Credentials

People

- More than 1,600 cloud operations professionals
- Developers trained on Oracle's rigorous coding standards
- 1,700 security personnel for tactical implementations of Oracle Software Security Assurance

Process

- 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), and OASIS key management interoperability protocol (KMIP)

Technology

- Security cloud services for identity, development, monitoring, compliance, and data protection
- Options for encryption, redaction, and data masking in production and nonproduction environments
- Privileged user controls on Oracle administrators and customer administrators

Physical

- Tier 3 enterprise-grade data centers
- 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 disaster recovery

In a 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.

Source: Coleman Parkes Research, "A Secure Path to Digital Transformation," 2016.

Cloud **Essentials**

Oracle Cloud Leadership

- More than 1,000 SaaS applications
- More than 17 years managing enterprise clouds
- More than 50 PaaS and SaaS cloud services
- 19 worldwide data centers
- Customers in more than 190 countries
- 98 million daily users
- 55 billion daily transactions
- More than 70,000 enterprise tenants
- US$5.5 billion spent each year on research and development
- 19 of 20 top cloud providers run on Oracle

Oracle Cloud Platform

☑ **Complete:** Best-of-breed and integrated solutions in every cloud category of data, software, platform, and infrastructure

☑ **Open:** Standard-based platform that supports all workloads, apps, languages, open source, and data types

☑ **Secured:** Automatic, always-on protection that extends throughout the entire cloud stack, all the way down to the silicon layer

☑ **Choice:** Flexible deployment options—public, private, Oracle Cloud at Customer, and hybrid cloud

☑ **Intelligent:** Artificial intelligence and machine learning in every cloud category—data, software, platform, and infrastructure

Request a security assessment from your local sales team.

Learn more at oracle.com/security or visit cloud.oracle.com/tryit to try Oracle Cloud today.

DISCLAIMER: The previous is intended to outline Oracle's general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle. Not all technologies identified are available for all cloud services.

ORACLE®