ORACLE®
Autonomous
Database Cloud

Oracle Autonomous Database

White Paper Series: The Industry s First **Self Securing** Database

DECEMBER 9, 2019

ORACLE®

DISCLAIMER

This document focuses on the Self-Securing attributes of the Oracle Autonomous Database. Autonomous Database is a service offering based on Oracle Database (version 19c and later), which runs in the Oracle Cloud. Self-Securing, combined with Self-Driving and Self-Repairing attributes, comprise the 3 key categories of autonomous capabilities within the Oracle Autonomous Database.

The initial sections of the paper are appropriate for business-level audiences. The details that follow may be more useful for DBAs and IT managers who are unfamiliar with the more recent Self-Securing capabilities of Oracle Autonomous. This document is part of a series of Oracle Autonomous Database white papers. Details on the Self-Driving and Self-Repairing capabilities of Oracle Autonomous Database are provided in separate Oracle white papers within this series.

The **"Introduction"** and "**What is an Autonomous Database?"** sections of this document are intentionally common to all of the Oracle Autonomous Database white papers in this series.

.

TABLE OF CONTENTS

INTRODUCTION

Relational databases have made tremendous improvements in performance, availability and security over the past couple of decades. They can run up to 100x faster; can be configured for zero data loss; and have hardened security capabilities that can protect against malicious internal and external threats. These attributes have been enhanced by cloud databases and infrastructure services that deliver elastic scalability and provisioning for real-time agility and growth.

Database workloads that were deemed too large or "mission critical" to run outside corporate data centers just a few years ago now run in public clouds. In addition, capabilities such as database resource deployment, monitoring and management can also be automated, leading to greater operational efficiencies and cost savings. So what's missing? The degree of manual intervention required to manage today's cloud databases and all of the above attributes inhibits true Database as a Service – as a utility, or driver-less offering if you will. As a result, enterprises are unable to realize the full operational and financial benefits of the cloud.

WHAT IS AN AUTONOMOUS DATABASE?

There is an understandable element of confusion that arises when talking about "automatic" versus "autonomous" capabilities. A process for database backup, failover or resizing that can be accomplished *automatically* is still not *autonomous* if a database administrator has to respond to an alert, make decisions and click a few buttons (or type a few commands) in order to initiate the automated activity.

A more dramatic example is when an alert related to a component outage or performance degradation appears automatically on a management console, but doesn't provide sufficient information to diagnose the problem, determine its root cause or offer a definitive recommendation for resolution. The automation literally stops with the alert. What happens next and how long it takes until resolution is unclear.

By contrast an autonomous database combines the dynamic agility of the cloud with the intelligent responsiveness of applied, adaptive machine learning. The design goal is to minimize or eliminate human labor – and associated human error – and ensure data safety and optimal performance.

Businesses will find that autonomous capabilities can further help IT staff improve efficiencies by enabling them to focus on higher value activities in lieu of mundane, time-consuming tasks. This is significant considering that up to 75% of IT budgets are spent on manual database management. [iii] An autonomous database can help organizations transform IT operations into a modern cloud model that lowers operating expenses, eliminates costly downtime, and ultimately enables them to innovate more while using fewer resources.

Oracle Autonomous Database is designed to deliver the above benefits across 3 primary categories, all accomplished with minimal to zero human intervention.
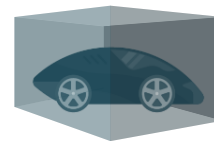
- **Self-driving:** The Autonomous Database automates database and infrastructure provisioning, management, monitoring, backup, recovery and tuning.

"Many of our customers operate 24/7 and Oracle's Autonomous Transaction Process (ATP) provides zero downtime. ATP patches, maintains, and tunes itself, providing a more secure environment, allowing us to focus our resources on developing innovative solutions for our customers."

Mark Carleton
Director
MESTEC

- **Self-securing:** The Autonomous Database is more secure than a manually operated database because it automatically protects itself from internal and external vulnerabilities and attacks. The Oracle Cloud provides continuous threat detection, while the Autonomous Database automatically applies all security patches online, provides "always on", end-to-end encryption, and leverages Oracle Data Safe to secure users and data. This preventative approach is critical because 85% of security breaches today occur after a CVE (Common Vulnerability and Exposure) alert has been issued. [iv]

- **Self-repairing:** The Autonomous Database provides preventative protection against all unplanned and planned downtime – and rapid, automatic recovery from outages without downtime. A key Oracle differentiator is the Autonomous Health Framework, which takes availability and performance management to the next level of AI-based autonomy by integrating multiple areas of diagnostics and enabling analysis and action to be taken at runtime to minimize or eliminate operational disruption.
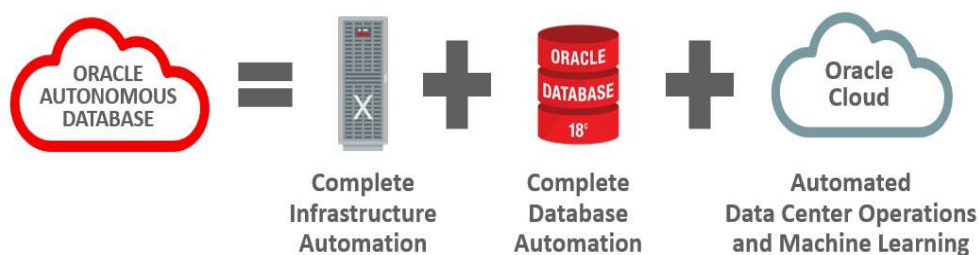
What is the Autonomous Database Cloud?

Figure 1: Autonomous Database Components in the Oracle Cloud

UNDERSTANDING THE NEED FOR A SELF-SCURING DATABASE

Organizations of all sizes are becoming well-versed in the risks associated with data theft, misuse of data, and inappropriate access to data. The growing cost of post-breach fines and litigation, combined with regulatory penalties for failure to adequately protect data, make securing sensitive data a top priority for most organizations.

While the importance of securing data continues to grow, the resources available to work on securing the data are simultaneously becoming scarcer. Security administrator jobs typically go unfilled for between six to nine months. The global cybersecurity workforce shortage is estimated to be 3 million worldwide, with nearly 60% survey respondents indicating that their organizations are at moderate or extreme risk of cybersecurity attacks due to this shortage[vi].

85% of security breaches today occur after a CVE (common vulnerability and exposure) alert has been issued. 77% of organizations noted that delays in vulnerability patching are caused by not having enough resources to keep up with the sheer volume of patches.[vii] Unfortunately, attackers work to leverage security vulnerabilities as soon as they become known – thus creating a security "patch gap" that has resulted in some of the most spectacular data breaches of the past few years.

It's about much more than just patching though; good security hygiene for sensitive data requires properly configuring the system (including patching), encrypting the data within the system, controlling access to that data, and monitoring the data for anomalies and risky users. The answer is to automate as much of the routine security work as possible – and Oracle Autonomous Database, in conjunction with Oracle Data Safe, is the first solution to address all of these key security needs.

ORACLE'S LEADERSHIP IN SELF- SECURING CAPABILITIES

Oracle has been a leader in database security for over 40 years. The Autonomous Database's Self-Securing features are the culmination of decades of both development effort and experience running critical workloads for some of the most demanding customers on the planet.

The Autonomous Database takes care of some of the most common and time consuming security requirements, including: encryption (both at rest and in motion), separation of duties, collection of audit data, patching, upgrades, and reducing the opportunity for human error. Integration with Oracle Data Safe adds additional security capabilities including security assessment, user assessment, activity auditing, data discover and data masking.

Oracle has addressed these security issues on-premises for decades using database technologies like Oracle Advanced Security, Oracle Database Vault, and Oracle Real Application Clusters[viii]. Properly applied, these security capabilities are part of the Oracle Maximum Security Architecture (MSA). The MSA is a comprehensive set of security controls that can be configured to address almost any security requirement – from enforcement of trusted path access to fine-grained access control. The MSA portfolio is also available in the Oracle Cloud and has been enhanced with automation and default deployment templates in the Autonomous Database. No other vendor offers the comprehensive autonomous self-securing database capabilities that Oracle does – on-premises or in the cloud.

WHY IS A SELF-SECURING DATABASE IMPORTANT?

A self-securing database is more trustworthy than a manually secured database. Automating basic security requirements like encryption and patching not only removes the element of human error, it eliminates the dangers that are inherent to competing IT priorities and an industry-wide tendency to procrastinate when it comes to applying security controls to databases. In Verizon's 2019 Data Breach Investigation Report (DBIR), Verizon realized that many breaches are "a result of poor security hygiene and lack of attention to detail." [ix] We can extend that to note that security controls that aren't applied during initial system rollout or replatforming are often never applied at all. It's much more efficient to build security into a system than it is to bolt it on afterwards.

Analysis of over 400 on-premises database security risk assessments conducted globally by Oracle experts reveals that a surprising number of production databases lack basic security hygiene like encryption, auditing, and up-to-date patch levels. In many cases, the root causes of this security gap are lack of time and skills to do the work, and organizational inertia against change. The Autonomous Database solves both problems. It establishes a baseline security posture, including controls that reduce risk and improve compliance to meet data privacy requirements and security regulations. In addition, Oracle Data Safe can alert you in real-time to risky users and misconfigurations and monitor database activity to help you quickly discover suspicious attempts to access data. Data Safe notifies you of sensitive data in your system, including exactly where it resides, even allowing you to mask that data when appropriate.

Shifting responsibility for these routine security tasks to the database service frees up scarce security resources to concentrate on more high-value efforts like enabling digital transformation, mitigating application vulnerabilities, and remediating access anomalies.

By replacing manual security tasks with extensive automation, Oracle Autonomous Database reduces security administration costs by up to 55%. Studies also show that 85% of security breaches today occur after a CVE (common vulnerability and exposure) alert has been issued. Automated patching can significantly reduce this security risk.

APPLICABLE ENVIRONMENTS FOR SELF- SECURING (AUTONOMOUS) DATABASES

Oracle Autonomous Database is an Oracle Cloud offering running Oracle Database. While many security capabilities of Oracle Database are available both on-premises and in the cloud, a number of autonomous elements are unique to the Oracle Cloud. Examples include autonomous patching, encryption by default, and the enforced separation of duties inherent in the Autonomous Database model.

Although Oracle Autonomous Database is a cloud-only offering, it is available as a serverless or dedicated cloud infrastructure. With an Autonomous Database Dedicated Cloud Infrastructure deployment, customers can avoid noisy neighbors and secure workload isolation with a fully isolated cloud in the public cloud. In addition, enterprises that must keep data behind corporate firewalls to meet data sovereignty or control requirements will soon be able to run the Autonomous Database on-premises. Oracle Exadata Cloud at Customer, an Oracle Public Cloud offering, can be deployed on-premises, and delivers all of the capabilities of Autonomous Database from within the enterprise's data center.

The Autonomous Database can be deployed in a hybrid cloud or all-cloud model; for example, when multiple databases are deployed for production and test environments or as primary and standby systems in a disaster recovery scenario.

There are no workload restrictions associated with the Autonomous Database or its self-securing capabilities. This includes transaction processing, mixed workloads that involve transaction and batch processing and reporting, as well as analytic workloads associated with data warehouses and data lakes.

WHAT CAN A SELF-SECURING CLOUD DATABASE DO?

The self-securing capabilities we've discussed so far are integral to Oracle Autonomous Database. They provide a baseline security posture that is already superior to most on-premises environments and are extensible enough to meet the most stringent security requirements with ease. Most of the Oracle Maximum Security Architecture (MSA) technologies are de-facto industry-standards for protecting and monitoring Oracle Database environments. The self-securing capabilities include:

- **Encryption for data in motion** – Each Autonomous Database service is automatically configured to use industry-standard TLS 1.2 to encrypt data in transit between the database service and clients or applications. Required client certificates and networking information are automatically packaged for the service consumer when the service is provisioned.

- **Encryption for data at rest** – Data in the Autonomous Database is automatically encrypted using Oracle Transparent Data Encryption – first available with Oracle 10g in 2004. Transparent Data Encryption has been continuously enhanced and improved since its introduction. Automated encryption for data at rest and in motion are available only with Oracle Cloud.

- **Automated separation of duties** – The Autonomous Database completely eliminates direct access to the database node and local file system. Further isolation between the service administrators and service consumers is provided through Oracle Database Vault, first available in Oracle Database 9i. This separation of duties – a key Oracle Cloud differentiator – not only reduces the risk of administrator malfeasance, it also eliminates the ability of the service administrators to view or modify data stored in the Autonomous Database. As with Transparent Data Encryption, Database Vault has been continuously enhanced and improved - with some new features added explicitly to support the Autonomous Database.

- **Database auditing configured by default, customizable to meet your needs** – Autonomous Database comes preconfigured using Oracle Unified Audit. This feature includes automated auditing for privileged user activity and logon failures and optional pre-configured policies for the Center for Internet Security audit benchmarks, account management, and much more.

- **Effectively protect the customer data and users** – With Data Safe, customers with Autonomous Database can identify sensitive data and mask it for use in partner or development environments. With the cloud service available to Autonomous Database customers, it can alert customers on risky users and system configurations and monitors database activity to let them quickly discover suspicious attempts to access data

- **Reduced opportunity for human error** – Human error plays a significant role in many data breaches and is one of the most difficult threat vectors to eliminate. The Autonomous Database minimizes the chances of human error by automating a significant portion of database administration. Opportunities for human error are further reduced by restricting the range of commands that an Autonomous Database service consumer is allowed to run.

- **Automated patching, upgrades, and maintenance** – One of the most significant advantages of the Autonomous Database is its ability to automatically apply security patches and upgrade them without downtime. Much of this capability builds on well tested, mature Oracle Database technologies like Real Application Clusters (for rolling online RAC patches) and cloud service process automation. The latter draws from experience accumulated over decades – starting with Oracle's On-Demand hosting service, progressing through Oracle Managed Cloud Services and further evolving in the Oracle Cloud.

Together, these capabilities within the Autonomous Database provide a security framework that covers the core security requirements for most organizations out of the box, freeing up operations and security teams to elevate enterprise security posture to the next level.

CONCLUSION

No databases that run on-premises or in cloud environments today are 100% autonomous – but that is the goal toward which the industry is headed. To further the evolution of cloud databases toward this true utility model, Oracle introduced the Autonomous Database, running on Oracle Database (version 18c and later) in the Oracle Cloud. Autonomous Database minimizes or eliminates human labor using self-driving, self-securing and self-repairing functionality. The self-securing capabilities of the Autonomous Database leverage both the Oracle Maximum Security Architecture (MSA), Oracle Data Safe, and Oracle operations best practices. Oracle MSA combines advanced technologies, best practices and autonomous functions to proactively protect against common attack vectors, and free up scarce security resources to focus on higher-value activity. Self-securing capabilities include encryption, access control, automated patching, auditing, and the ability to secure data and users. This collection of self-securing capabilities offered by the Oracle Autonomous Database is unmatched by any other cloud (or on-premises) database in the industry.

i The "Introduction" is intended to be common for each of the three Oracle Autonomous Database White Papers that focus on Self-Driving, Self-Securing and Self-Repairing attributes.

Ii The "What is an Autonomous Database" section is intended to be common for each of the three Oracle Autonomous Database White Papers that focus on Self-Driving, Self-Securing and Self-Repairing attributes.

Iii IDC Perspective, "Oracle's Autonomous Database: AI-Based Automation for Database Management and Operations", Feb. 2018 iv Verizon - 2018 Data Breach Investigation Report

v Cybersecurity Ventures 2018 - https://cybersecurityventures.com/jobs/

vi (ISC)2 Cybersecurity Workforce Study, 2018

vii Ponemon Costs and Consequence of Gaps in Vulnerability Response, 2018

viii 0Patch. "Security Patching is Hard" 2017

viii Oracle RAC is also an integral part of Oracle Maximum Availability Architecture (Oracle MAA)

ix Verizon Data Breach Investigation Report 2019

ORACLE CORPORATION

Worldwide Headquarters
500 Oracle Parkway, Redwood Shores, CA 94065 USA

Worldwide Inquiries
TELE   + 1.650.506.7000 + 1.800.ORACLE1
FAX   + 1.650.506.7200
oracle.com

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

B blogs.oracle.com/oracle   f facebook.com/oracle   🐦 twitter.com/oracle

Integrated Cloud Applications & Platform Services

ORACLE®

Oracle is committed to developing practices and products that help protect the environment