DELL Technologies

Top 10 Best Practices for Rapidly Changing Oracle Landscapes

Get Started >

Avoid risk, seize reward with Oracle databases.

The data landscape is changing as never before. There's more data to process from more sources and more locations while businesses demand increasingly intelligent applications to deliver faster, smarter results. At the same time, cyberattacks are on the rise. Throughout this digital transformation, Oracle® remains the world's number one relational database technology, critical to the day-to-day operations of countless organizations.

But how does this evolving data landscape affect your Oracle investments, and how do you capitalize on data-driven opportunities while minimizing risk? The following best practices can help you simplify and secure your Oracle landscapes while optimizing them for applications like artificial intelligence (AI), machine learning (ML) and Internet of Things (IoT).

Click on one of these areas here to jump to that section.

Strategize >

Optimize >

Protect >

1

Establish strategies for a changing business data landscape.

Think short, medium and long term.

Whether you're running older versions of Oracle Database or planning to migrate to Oracle Converged Database 19c and above, an IT foundation that reduces total cost of ownership (TCO) and is ready to support future capabilities and operating profiles is critical for success.

Careful planning can help protect Oracle investments so that the infrastructure that underpins your application and database transformation today will support business and IT outcomes now and be ready to support emerging data-driven scenarios in the future. Taking a three-step approach to Oracle transformation is a smart strategy that lays a foundation for ongoing success.

Step-by-step strategies for success

Long term:

Enhance developer productivity to become a data-driven business.

- Accelerate DevOps, leveraging containers for building and deploying Oracle applications.
- Adopt AI using modern compute, GPUs, storage and networking to ensure high performance for data-driven workloads.
- Bridge the edge-to-core-to-cloud data gap with advanced data management.

Medium term:

Embrace an agile data strategy that connects the digital business.

- Break down data silos and integrate applications — on-premises, in the cloud, Oracle and non-Oracle — across the business.
- Streamline data ingestion and access by unifying data streams with unlimited retention.
- Secure and protect Oracle applications and data with cyber-resilient recovery paths.

Short term:

Transform IT to reduce Oracle costs and complexity.

- Consider consumption models for infrastructure, including lifecycle management.
- Free administrators from repetitive tasks with efficient, intelligent and scalable systems.
- Put the focus back on innovation, with IT designed for ease of use, reliability and lifecycle management.

2

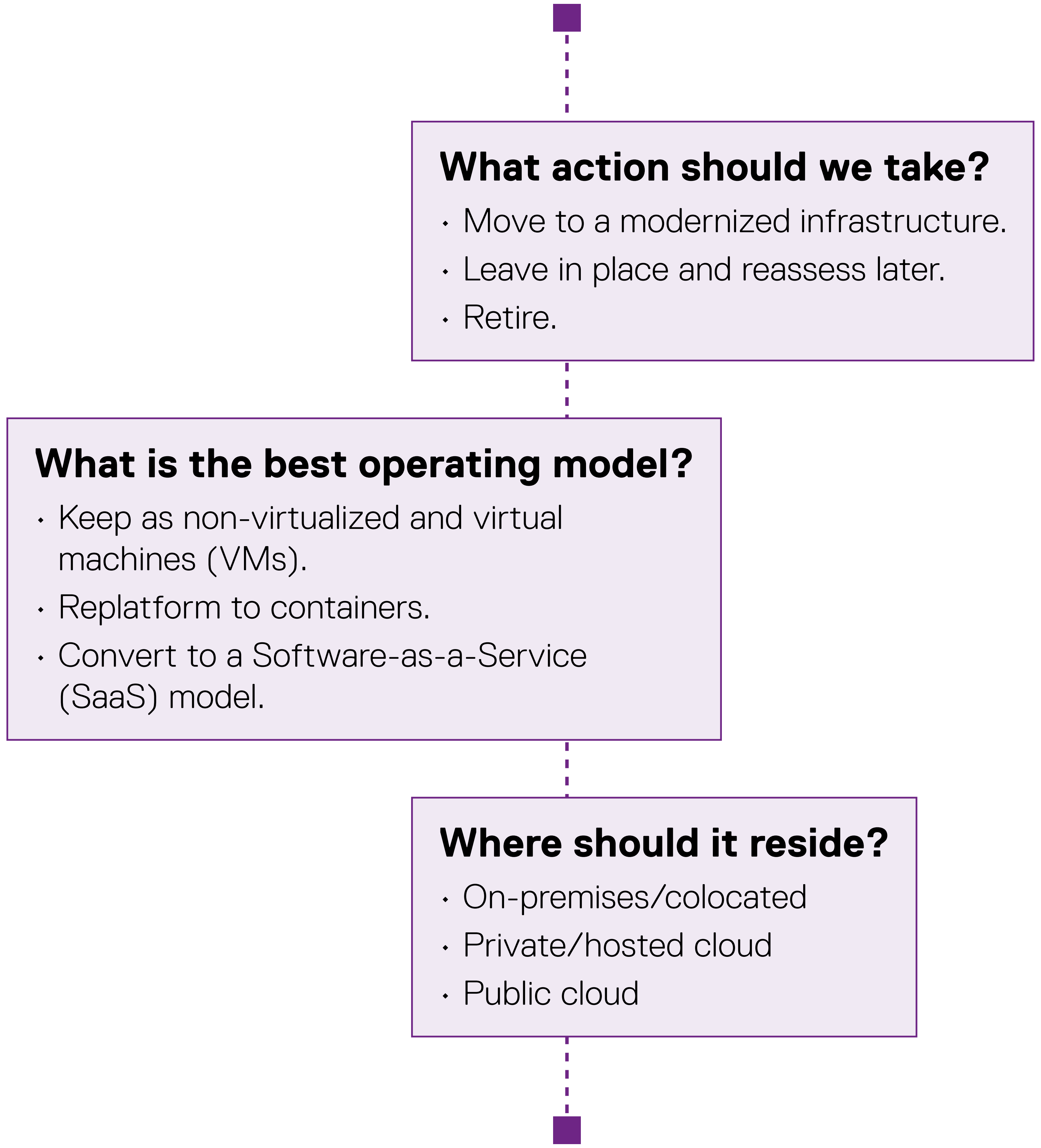
Identify your optimal infrastructure.

Consolidate for cost savings.

A typical business supports hundreds of applications backed by multiple databases, which requires more infrastructure and leads to additional costs and data center sprawl. This problem compounds as data grows. A cornerstone of digital transformation is consolidating workloads onto less — but more powerful — infrastructure to reduce costs, complexity and space requirements while increasing performance, availability and reliability.

However, when it comes to transforming and consolidating mission-critical Oracle Database landscapes, you have more choices than ever before, and a one-size-fits-all approach is seldom an ideal strategy for your digital transformation journey. Partner with a provider that can help you make infrastructure and deployment decisions on your specific use cases, performance, application and availability requirements.

Deployment decision tree



What action should we take?

- Move to a modernized infrastructure.
- Leave in place and reassess later.
- Retire.

What is the best operating model?

- Keep as non-virtualized and virtual machines (VMs).
- Replatform to containers.
- Convert to a Software-as-a-Service (SaaS) model.

Where should it reside?

- On-premises/colocated
- Private/hosted cloud
- Public cloud

Strategize

3

Build for your use cases.

Plan ahead to optimize results.
The introduction of faster, more powerful technologies has made it possible for businesses to consolidate databases with greater confidence. However, optimizing the value of your Oracle Database investments and providing adequate service levels require an environment built for your specific use cases.

Understanding the CPU, RAM, storage, networking and backup requirements of your Oracle use cases and architecting the environment to meet or exceed these requirements will improve overall Oracle performance, stability and availability.

Architecting for success use cases

Single application	Multiple workloads	Multiple workloads and databases
One or more online transaction processing (OLTP) databases	Single OLTP database with online analytical processing (OLAP) and test/dev	Multiple databases on OLTP with OLAP and test/dev
IT considerations: · Choose smaller memory/cache · Trade-off IOPS vs. throughput · Optimize for price/performance · Prioritize scalability	**IT considerations:** · Choose larger memory/cache · Balance IOPS and throughput · Architect for structured/unstructured data · Use all-flash storage	**IT considerations:** · Choose largest memory/cache · Use NVMe™ with flash · Optimize for performance at scale · Build for mixed workloads including analytics

4

Enhance efficiency with hybrid cloud.

Choose the best of both worlds.

When it comes to mission-critical legacy applications such as Oracle Database, the traditional approach of combining on-premises deployment, colocation and managed hosting is still widespread. Public cloud has become an increasingly popular choice for new, cloud-native applications. By combining the two approaches, hybrid cloud delivers the best of both worlds, enabling you to move workloads between public and private clouds, using on-premises solutions where it makes the most sense.

Hybrid cloud is a compelling option for enhancing operational efficiencies while minimizing costs and risks. New, consumption-based infrastructure models can give you integrated compute, storage and networking resources with support for both traditional and cloud-native applications. For example, Dell APEX is an as-a-Service option that can quickly deliver a mature hybrid cloud infrastructure for your Oracle databases.

Choose the right mix.

On-premises		Hybrid cloud	Multicloud
Dell cloud-enabled infrastructure	**APEX Private Cloud**	**APEX Hybrid Cloud**	**Dell storage and data protection**
Deploy preferred stack for Oracle. · VMware® vRealize® Suite and VMware vSphere® · Oracle Enterprise Manager, Database Applications and VMs · Red Hat®, SUSE® or Oracle Linux®	Deploy Oracle OS, database, application management software. · VMware vRealize Suite · Oracle Enterprise Manager and Database Applications · Red Hat, SUSE or Oracle Linux	Deploy Oracle OS, database and application. · Advanced cloud management VMware vRealize Suite and VMware vSphere · Oracle Enterprise Manager and Database Applications · Red Hat, SUSE or Oracle Linux	**Public cloud** Hybrid and in-cloud data protection Dell PowerProtect Data Manager · VMware/AWS · Google Cloud™ · AWS® · Microsoft® Azure®
Run Oracle non-virtualized and VMs. Dell Cloud-enabled infrastructure: · Compute services · Storage services · Data protection services	Run Oracle on VMware VMs. Dell hyperconverged infrastructure (HCI) with VMware: · vSphere · vSAN · HCI platform	Extend Oracle to public cloud. Dell software-defined data center (SDDC) with VMware: · Cloud Foundation™ · HCI platform	Multicloud storage and data protection Managed Service Provider: storage services and data protection services · VMware/AWS · Google Cloud · AWS · Microsoft Azure

5

Balance storage consumption/allocation.

Small discrepancies can have a big impact.
When moving to a hybrid or multicloud model for Oracle databases, the cost calculations change. Because cloud providers charge based on consumption, you need to track how much storage Oracle is consuming compared to how much you have allocated.

For example, one Dell Technologies customer allocated (and paid for) 201TB of storage for Oracle but found that they were only using 127TB. This is a common problem that can have significant cost implications for a cloud deployment model.

Determine how much storage your Oracle Database is using.

Allocated:
201TB

Consumed:
127TB

Overallocation:
58%

6

Avoid licensing issues.

Maintain compliance and reduce costs.

Oracle Database processor-based licensing depends upon physical processor counts, regardless of whether they are physical or virtual platforms. This creates complexities — particularly in virtualized environments — that make it easy for Oracle customers to unintentionally fall into costly noncompliance. At the same time, overlicensing can be an unnecessary drain on the budget.

Best practice for optimizing your Oracle spend includes performing an internal audit and setting up ongoing monitoring to identify and remediate any noncompliance and/or overlicensing issues.

Obtain a third-party license audit.

- ✓ Internal audit identifies all license exposures.
- ✓ Review of license assets ascertains any redundancies.
- ✓ Review of license sets, lifespan, models and options.
- ✓ Results shared with you, NOT with Oracle.
- ✓ Ongoing monitoring ensures continued license compliance.

7

Identify risks.

Your Oracle Database assets are under attack.

Even as technologies change and the business shifts its priorities, the one constant is the need to protect critical applications and data. Whether it's modernizing infrastructure for digital transformation, adopting or expanding hybrid cloud or enabling data-driven applications, robust cybersecurity for your Oracle Database is important.

For example, today's cybercriminals are increasingly targeting backups to make it difficult to protect against ransomware. Backup admins are a main target because they have trusted access that can give criminals free range inside your systems. Other points of vulnerability include the master server, any system mounted by the media server, file system backups, tape catalogs and cloud backups. These points of entry need to be protected against bad actors.

Protect yourself with cyber-resilient IT.

Begin with a comprehensive cyber resiliency health check from Enterprise Strategy Group (ESG) analysts.

It will help you:

- Assess current cyber-preparedness and ability to detect, respond and recover from a ransomware or other cyberattack.
- Measure exposures and vulnerabilities and gain best practices and tailored recommendations to address gaps and reduce cyber-risks.
- Receive individual actionable recommendations and peer comparison in a comprehensive appraisal of preparedness.

Take the assessment.

8

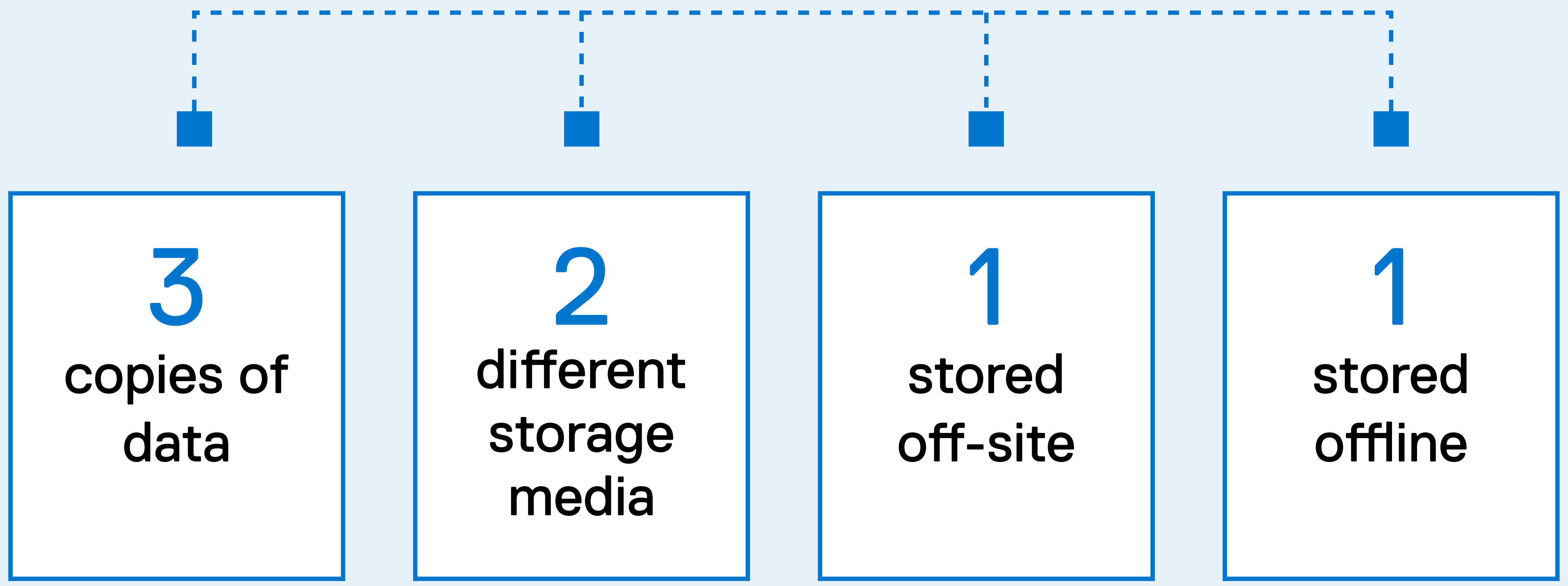
Follow the NIST Cybersecurity Framework.

Implement the 3-2-1-1 rule.

The National Institute of Standards and Technology (NIST) outlines a Cybersecurity Framework for protecting data to create a more secure organization. In order to make sure assets are adequately protected from malicious actors and code, the framework makes use of the following five steps:

1. **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.
2. **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services.
3. **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4. **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity event.
5. **Recover:** Develop, implement and maintain appropriate plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The NIST 3-2-1-1 rule



3 copies of data

2 different storage media

1 stored off-site

1 stored offline

9

Adopt a zero-trust security model.

Never trust, always verify.
With today's increasingly mobile and remote workforce, network-based security alone can't keep up. Zero-trust security is a model based on the idea that intruders are already in the network and no connection — whether internal or external — can be trusted.

The main principles of zero trust center around continuous, dynamic authentication and authorization. Under the recommended NIST Zero Trust Architecture, every connection must be continuously authenticated and authorized before access to an IT resource is granted. Essentially, never trust, always verify.

Implement a zero-trust security model.

Verify identity.
- Strong passwords
- Biometrics
- Multifactor authentication (MFA)

Verify device.
- Device health
- Managed profiles
- Users do not have admin on devices.

Verify access.
- Least-privileged access paradigm
- Network segmentations build on roles and responsibilities.

Verify service.
- Users have only the services needed for the job/role.

10

Combat emerging threats.

Stay a step ahead of cybercrime.

Cyberattacks take many different forms, and the attackers may have a variety of motivations, techniques and even platforms from which to launch their attacks. One of the most difficult types of cyberattack to defend against is one launched by an insider, whether knowingly or unknowingly. Insiders tend to have physical access, full knowledge of the infrastructure and may even have benefited from privilege creep, giving them access to more systems.

Once an attack occurs, it's important to understand that cyber-recovery can be very different from disaster recovery. Cybersecurity experts recommend logically separating infrastructure as well as maintaining offline and air-gapped copies of data.

Create a cyber-recovery strategy.

Cyber-recovery vs. disaster recovery

	Disaster recovery	Cyber-recovery
Recovery time	Close to instant	Reliable and fast
Recovery point	Continuous	One day (average)
Impact	Regional and contained	Global and spreads quickly
Topology	Connected, multiple impacted systems	Isolated, in addition to DR
Data volume	Comprehensive	Selective
Recovery strategy	Standard, such as failback	Iterative, selective recovery

Avoid risk and seize reward with Oracle database.

Whether you’re just beginning your transformation or well into your journey, operating on-premises or in the cloud, Dell Technologies is here to help you deploy, grow, optimize and secure your Oracle databases for today’s needs and tomorrow’s objectives.

We can help you determine your best strategy for running Oracle on a modern, secure IT foundation that supports traditional and emerging Oracle applications and containerized databases working with AI, ML and IoT.

Visit our website to learn more.

DELL Technologies

Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice.