



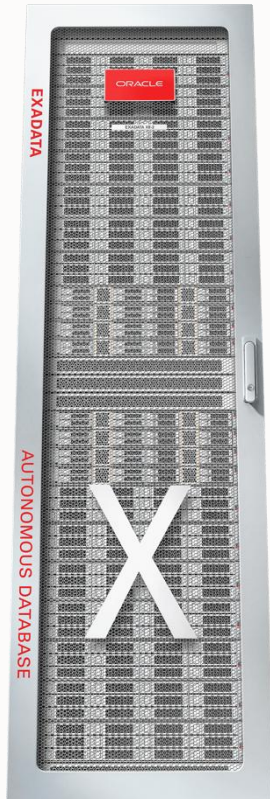
ORACLE

Oracle Exadata Database Machine

Maximum Security Architecture to Protect your Data

Exadata Maximum Security Architecture (MSA) Vision

Extreme Performance, Availability, and Security



Database Aware System Software

Unique algorithms vastly improve OLTP, Analytics, Consolidation

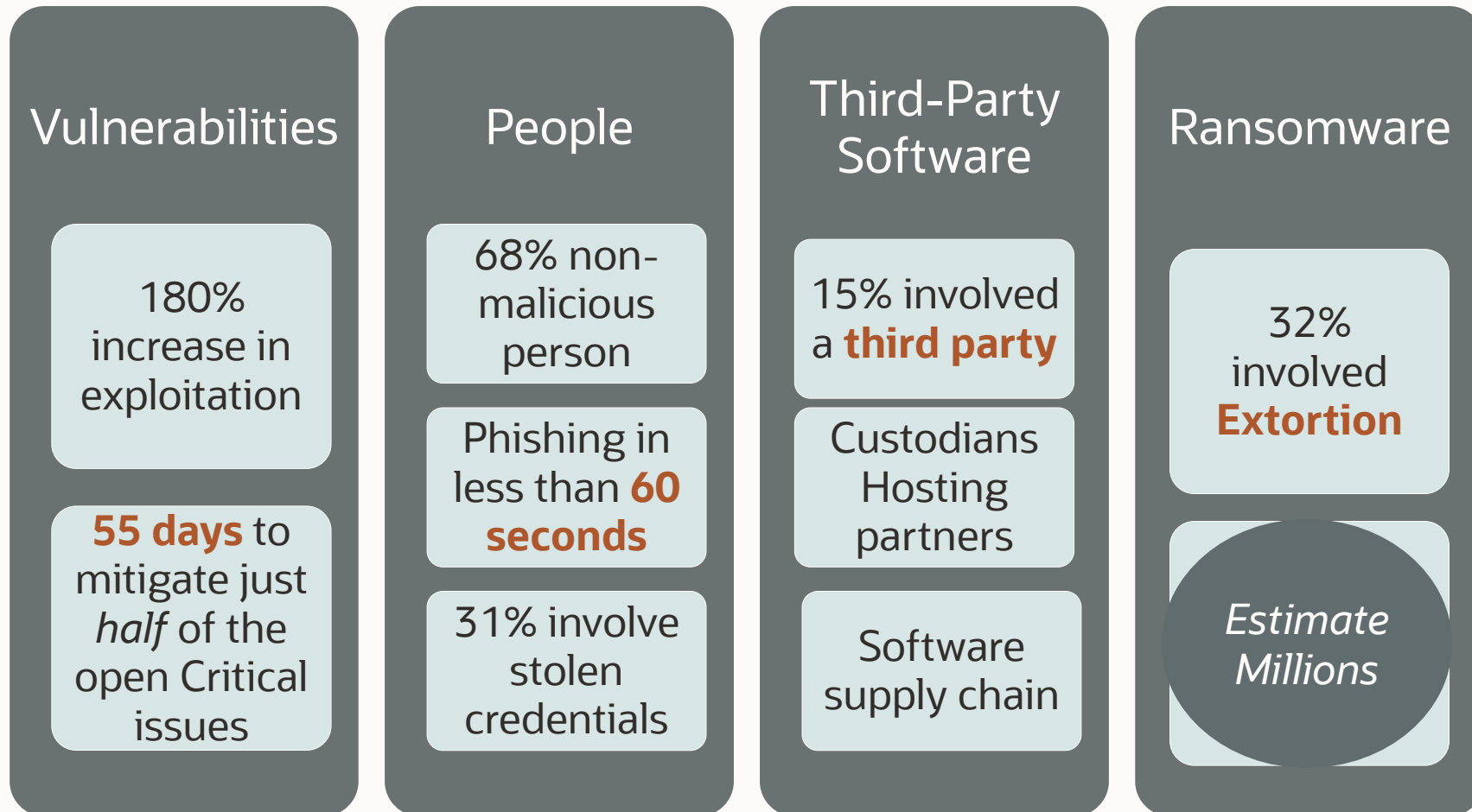
Highly Available Architecture

Oracle MAA Best Practices Built-In

End-to-End Security

Security-optimized, Security-focused, Security-hardened

Verizon 2024 Data Breach Investigations Report



Oracle Corporate Security Policies

Oracle's security practices are multidimensional, encompassing how the company develops and manages enterprise systems, and cloud and on-premises products and services.

Aligned with the following standards

- ISO/IEC 27002:2013
- ISO/IEC 27001:2013
- NIST

References

- <https://www.oracle.com/corporate/security-practices/>

Exadata Security Value-Add Overview

- ✓ Smaller Kernel/Package Footprint
- ✓ Principle of Least Privilege
- ✓ Storage Server Firewall
- ✓ System Calls Restrictions
- ✓ Centralized User Authentication
- ✓ File Integrity Monitoring
- ✓ System Hardening
- ✓ Multi-Tenant Isolation
- ✓ Boot Device Protection
- ✓ Fast Crypto Erase
- ✓ Security Enabled Linux
- ✓ Memory Protection Keys
- ✓ Storage Server SSH Lockdown



“The Oracle Autonomous Database, which completely automates provisioning, management, tuning, and upgrade processes of database instances without any downtime, not just **substantially increases security and compliance of sensitive data stored in Oracle Databases** but makes a compelling argument for moving this data to the Oracle Cloud.”

KuppingerCole Analysts

Smaller Installation Footprint

Exadata uses a minimal Linux kernel with removed dependencies that reduce size.

- Fewer device drivers
- Smaller footprint
- Improved upgrade time

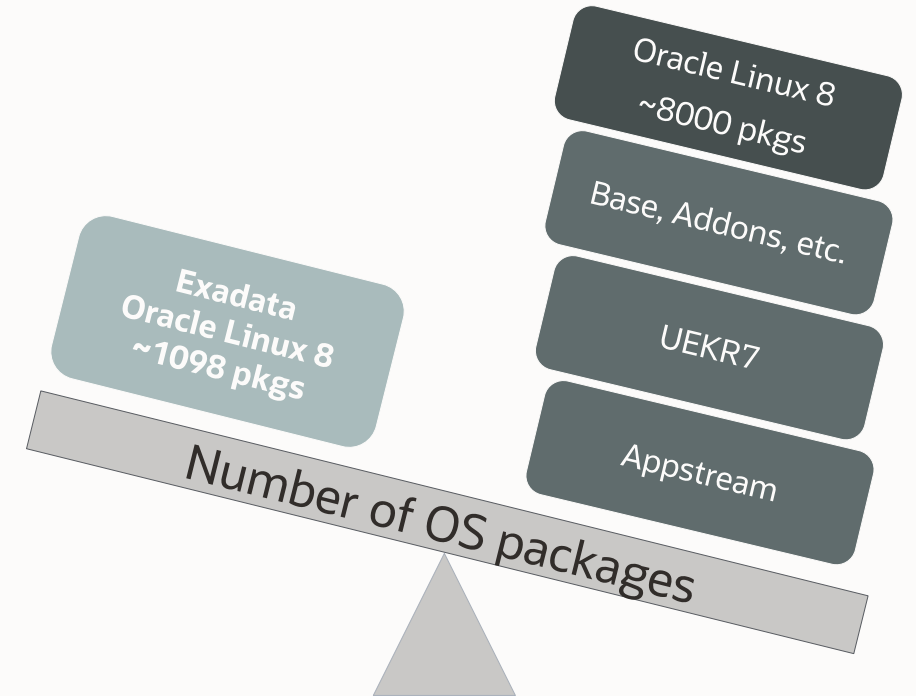
Full Enterprise Oracle Linux 8 UEK7 kernel

- kernel-uek-5.15.<>.el8uek
- Guest kernel size **161MB**

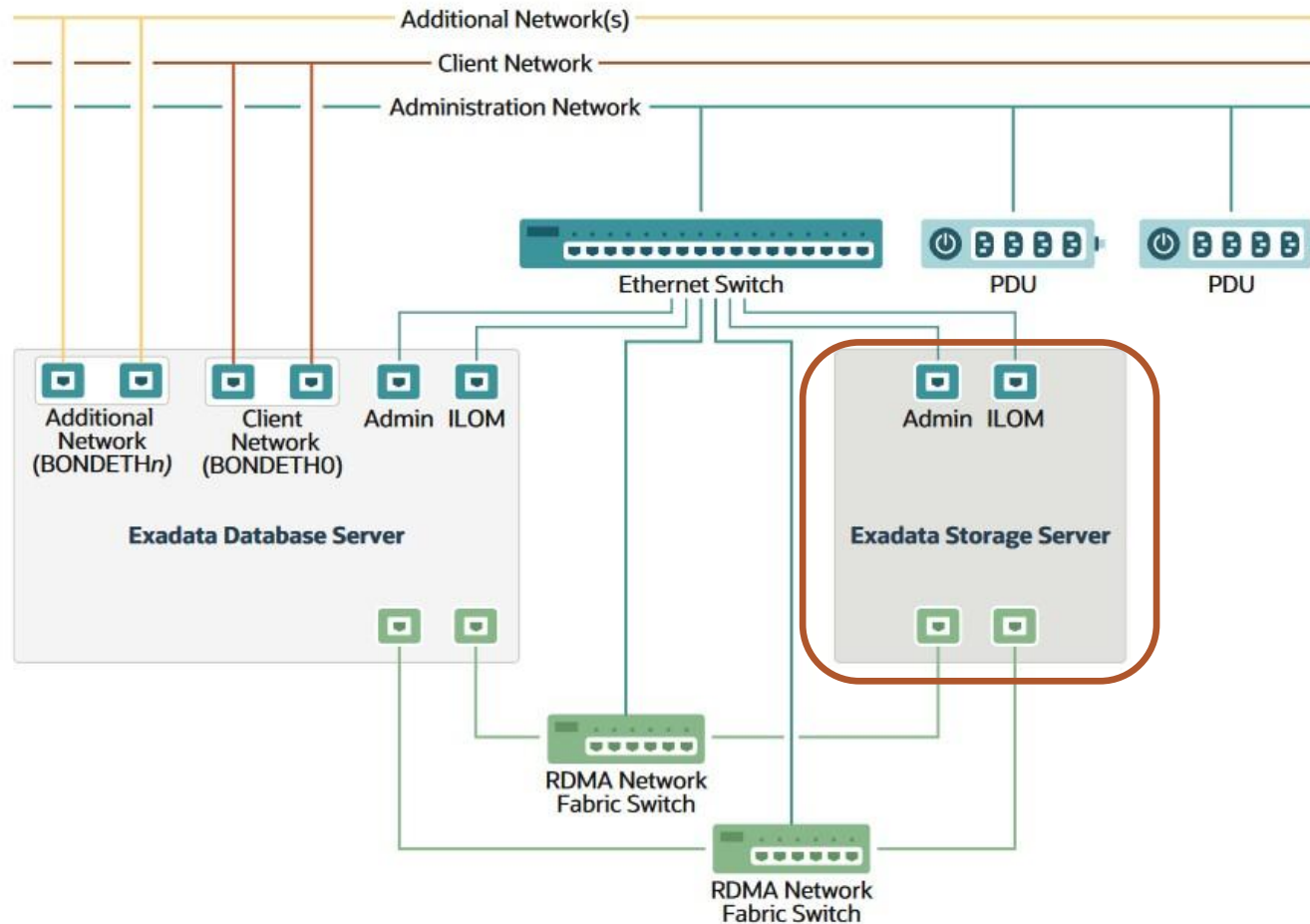
Exadata Oracle Linux 8 UEK7 kernel

- kernel-**uek-core**-5.15.<>.el8uek
- Guest kernel size **77MB**

Exadata **reduces the attack surface** by only including the software components required specifically to run the Oracle database.



Network Access to Storage Servers



- Oracle Exadata System Software includes the cellwall service that implements a **firewall** on each storage server.
- The SSH server is configured to respond to connection requests only on the management network (NET0) and the RDMA Network Fabric.
- The Exadata Storage Servers have no direct connectivity to the client network.

Pre-scanned full stack

Every Exadata release includes **security and emergency fixes** to address zero-day vulnerabilities discovered by our internal scanning tools.

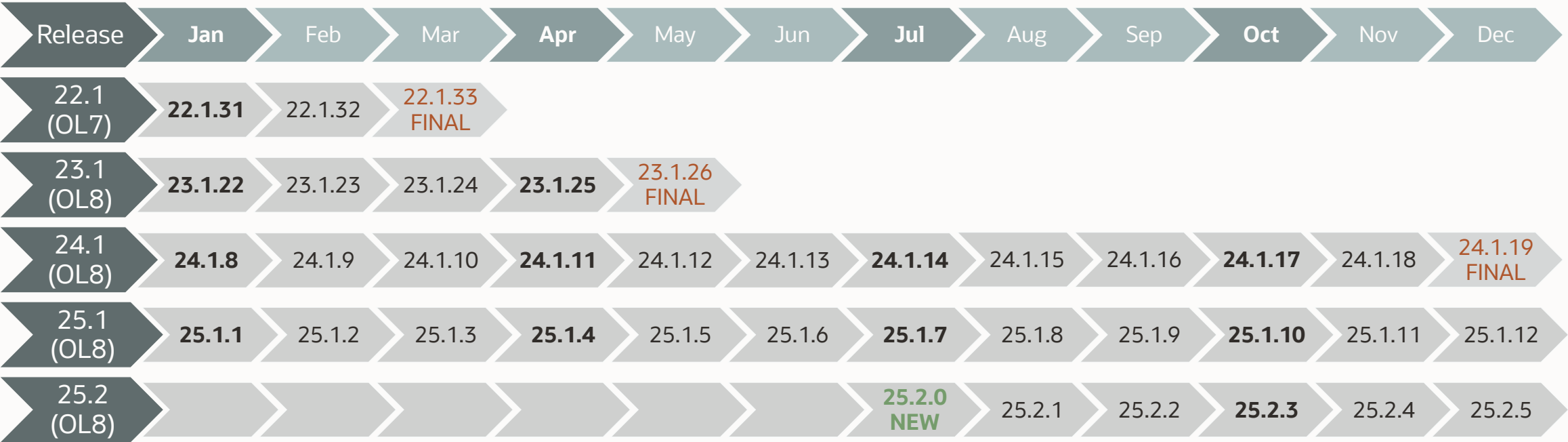
- Static/Dynamic code analyzing
- Malware scans
- Third-party software checks
- Vulnerability scans
 - Responses to common Exadata security scan findings (Doc ID 1405320.1)
- System hardening reviews (STIG)
 - Exadata OL8 System Hardening for STIG Security Compliance (Doc ID 2934166.1)

Customers take advantage of these fixes out of the box by just upgrading to the latest release.

- The number of annual issues reported is significantly less compared to a custom configuration with third party database, network and storage components.

Exadata Releases CY2025

Monthly Exadata System Software maintenance releases include the latest security updates to protect your data.



*Future releases and dates are **estimates** only.*



40,002

Common Vulnerabilities and Exposures (CVE) IDs issued in 2024 *across the international IT marketplace.*

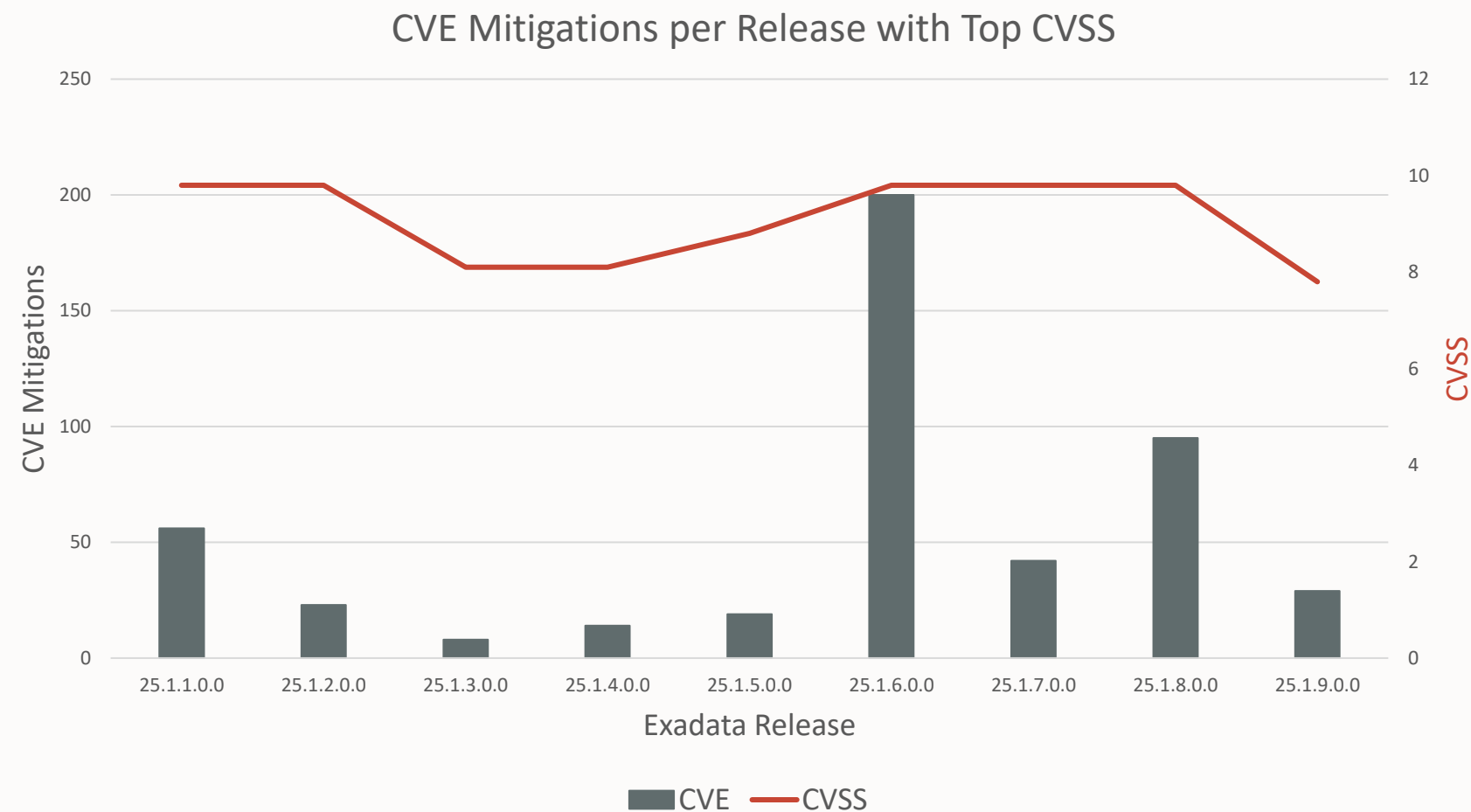
That's ~110 per day!

Exadata Security Value Add:

- Scanned images
- Monthly releases



Monthly Oracle Linux CVE Mitigations for Exadata 25.1.x



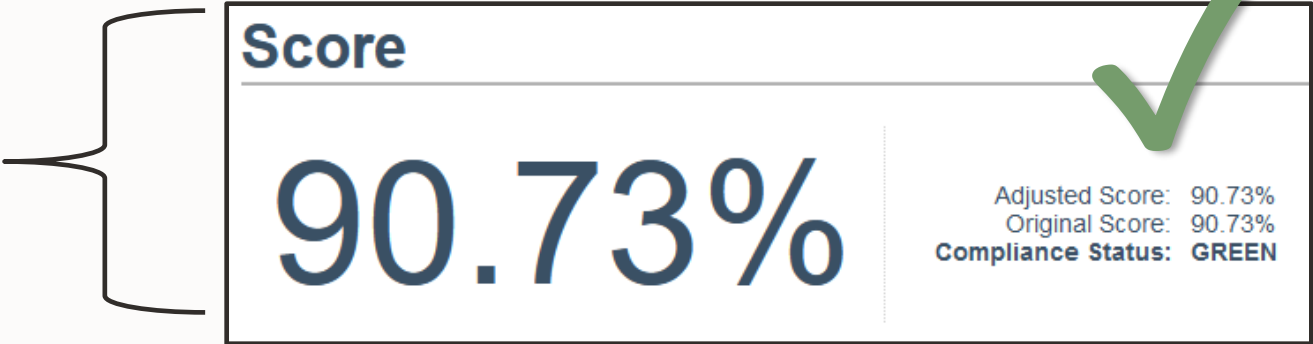
High STIG SCAP Oracle Linux 8 Benchmark from the Factory!

“The Oracle Linux 8 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of the Department of Defense (DoD) information systems.”

Standard Linux installation



Exadata KVM Guest Deployed



New Security Features in Exadata

Maximize Security, Maximize Performance, Maximum Availability

Security Enabled Linux (SELinux) – Permission Mode Enabled by Default

The SELinux enhancement to the Linux kernel implements the **Mandatory Access Control (MAC) policy**, which allows defining a security policy that provides granular permissions for all users, programs, processes, files, and devices.

- Starting with Oracle Exadata System Software release 25.2.0, all new Exadata implementations use SELinux in permissive mode by default, significantly strengthening the default Exadata security posture.
- The default configuration includes a pre-built SELinux policy that is custom-engineered for Exadata and Oracle Database, enabling seamless adoption. Additional custom policies are also allowed to support 3rd-party or implementation-specific software requirements.
- Monitoring SELinux in permissive mode enables the identification of potential issues, providing the opportunity to take corrective action to ensure the security and integrity of Exadata environments. Starting with permissive mode enables easy adoption and is the ideal preparation before manually moving to a mode that strictly enforces the SELinux security policies.

Exadata Security Capabilities

Maximize Security, Maximize Performance, Maximum Availability

Oracle Linux 8 – Unbreakable Enterprise Kernel 7 (UEK7)

Oracle Linux 8 Key security features

- Various SELinux improvements
- System-wide cryptographic policies applied by default
- OpenSSH updates
 - RSA min key 1024
 - DH module size 2048
 - DSA keys disabled
- TLS 1.3 cryptographic libraries added
- GPG key length increased to 4096 bits

Platform	Component	O/S	Kernel
RoCE	KVM Host	OL8	UEK7
	KVM Guest	OL8	UEK7
	Bare Metal	OL8	UEK7
	Storage Server	OL8	UEK7
Infiniband	Xen Dom0	OL7	UEK6
	Xen DomU	OL8	UEK6
	Bare Metal	OL8	UEK6
	Storage Server	OL8	UEK6

RDMA over Converged Ethernet (RoCE) server components move to UEK7



Simpler Linux Package Dependency Management

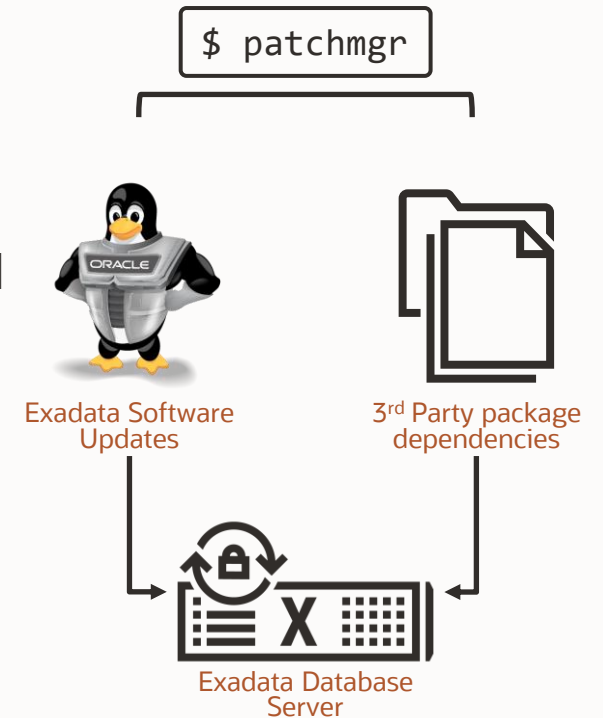
Customers often install 3rd party software on Exadata such as security, monitoring, and backup utilities.

These utilities often have additional Linux RPM dependencies over the curated Exadata repository.

Patch Manager enables additional non-Exadata software packages to be installed or updated as part of an Exadata database server update.

Avoids removal and reinstallation of 3rd party software during database server updates

- Validate package dependencies with `patchmgr --precheck`
- Update the Exadata database server software and additional packages simultaneously



```
$ patchmgr --precheck | --upgrade [ { --additional-rpms } | --additional-rpms-list } [ --additional-rpms-from-repo ]
```

Simpler Linux Package Dependency Management

Two phases of operation:

1. Precheck – iteratively test required packages are present in additional_rpms location and dependencies are resolved
2. Upgrade – applies database server update along with update and install of additional rpms

```
$ patchmgr --dbnodes db_group --precheck --iso_repo /u01/exadata_ol8_25.1.0.0.0.241130_linux-x86-64.zip  
--target_version 25.1.0.0.0.241130 --log_dir auto --additional_rpms /u01/additional_rpms/repo/
```

```
$ patchmgr --dbnodes db_group --upgrade --iso_repo /u01/exadata_ol8_25.1.0.0.0.241130_linux-x86-64.zip  
--target_version 25.1.0.0.0.241130 --log_dir auto --additional_rpms /u01/additional_rpms/repo/
```

/u01/additional_rpms/repo/ (example contents)

- elfutils-debuginfod-client-0.190-2.el8.x86_64.rpm
- elfutils-libelf-devel-0.190-2.el8.x86_64.rpm
- keyutils-libs-devel-1.5.10-9.0.1-el8.x86_64.rpm
- krb5-devel-1.82.2-28.0.1-el8.x86_64.rpm

Software Upgrade on Cisco Network Switches

Oracle Exadata System Software includes **NX-OS 10.3.(x)** Cisco system software release for the Cisco Management Network Switch and the Cisco RoCE Network Fabric Switches.

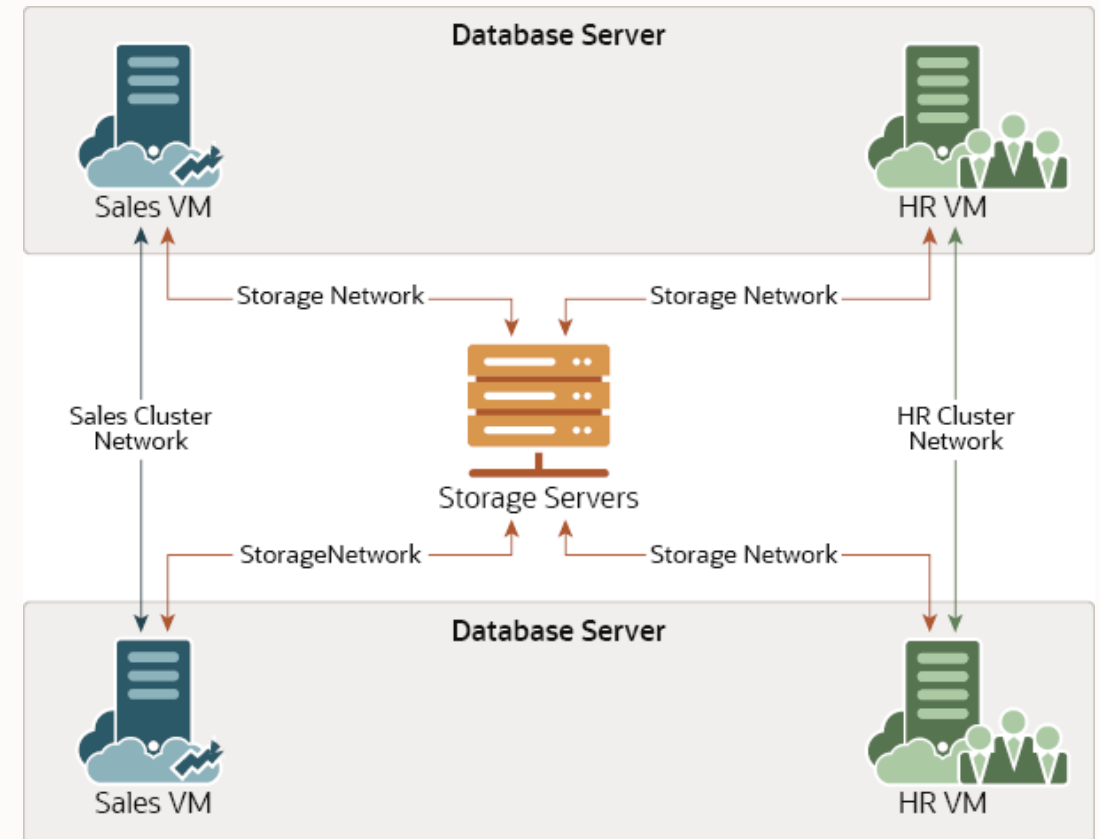
In addition to the general performance and security enhancements contained in NX-OS 10.3.(x), the update procedure for NX-OS has been optimized, resulting in substantially quicker updates.

- Depending on the switch being updated and its configuration, the overall time required to perform the update is reduced by up to 44%.

Secure Fabric is Recommended and Enabled by Default

Exadata Secure Fabric for RoCE systems implements **network isolation** for Virtual Machines while allowing access to common Exadata Storage Servers.

- Each Exadata VM Cluster is assigned a private network.
- VMs cannot communicate with each other.
- All VMs can communicate to the shared storage infrastructure.
- Security cannot be bypassed.
 - Enforcement done by the network card on every packet.
 - Rules programmed by hypervisor automatically.



Exadata Live Update

Exadata Live Update is a suite of enhancements to the mechanisms that orchestrate Exadata **software updates** on Exadata database servers.

Exadata Live Update uses online update capabilities based on standard Linux technologies, such as RPM and ksplice.

- Depending on the specific contents of the update, the update operation might occur without interrupting databases or rebooting the server.

Any update items that cannot be completed online are staged for completion during a later server reboot.

- You can schedule the outstanding items to be completed at a specific time or during the next graceful server reboot.
- You can also choose to defer the outstanding items indefinitely.

Exadata Live Update can be controlled using the Exadata patchmgr utility, which provides an easy and familiar experience for existing Exadata users.

Exadata Live Update

Exadata Live Update enables partial updates to address security issues, based on Common Vulnerability Scoring System (CVSS). When using Exadata Live Update, you must choose from the following options:

- **highcvss:** Performs only critical security updates to address vulnerabilities with a CVSS score of 7 or greater.
 - All new packages with High or Critical security mitigations
- **allcvss:** Performs only security updates to address vulnerabilities with a CVSS score of 1 or greater.
 - All new packages with any security mitigations (Low, Medium, High, Critical)
- **full:** Performs a full update, which includes all security-related updates and all other non-security updates.
 - All new packages in the image

Exadata Live Update

Patchmgr command

```
# ./patchmgr --dbnodes dbs_group --upgrade --repo <path>exadata_ol8_ 24.1.0.0.0.240517.1  
_Linux-x86-64.zip --target_version 24.1.0.0.0.240517.1 --log_dir auto --live-update-target  
allcvss
```

Imagehistory output from Exadata 23.1.x with Exadata Live Update to 24.1.0.0.0

```
Version : 23.1.1.0.0.230422  
Exadata Live Update Version : 24.1.0.0.0. 240517.1 (all) (CVSS 1-10) (Live Update  
applied. Reboot at any time to finalize outstanding items.)
```


Database and Storage Server Secure Boot

Oracle Exadata System Software extends Secure Boot to Storage Servers, KVM Host, KVM Guest*, and Bare Metal.

Secure Boot is a method used to **restrict** which **binaries** can be executed to boot the system.

- With Secure Boot, the system UEFI firmware will only allow the execution of boot loaders that carry the cryptographic signature of trusted entities.
- With each reboot of the server, every executed component is verified.
- This prevents malware from hiding embedded code in the boot chain.
 - Intended to prevent boot-sector malware or kernel code injection
 - Hardware-based code signing
 - Extension of the UEFI firmware architecture
 - Can be enabled or disabled through the UEFI firmware

**KVM Guest Secure Boot can be enabled during VM Cluster deployment in OEDA*

Access Control For RESTful Service

Oracle Exadata System Software includes the capability to **restrict access** to the HTTPs and RESTful interfaces using access controls.

- Specify a list of IP addresses or subnet masks to control access to the RESTful service via HTTPs.
- If not used, RESTful service can be disabled altogether.

```
# lsof -i -P -n | grep LISTEN | grep java
java          <pid> dbmsvc   55u  IPv4    40193      0t0  TCP *:7879 (LISTEN)

# dbmcli -e alter dbserver httpsAccess=none
This command requires restarting MS. Continue? (y/n): y
Stopping MS services...
The SHUTDOWN of MS services was successful.
Updating HTTPs access control list.
Starting MS services...
The STARTUP of MS services was successful.
DBServer successfully altered

# lsof -i -P -n | grep LISTEN | grep java
```

Listening Interface For RESTful Service

Oracle Exadata System Software includes the capability to **restrict the network interfaces** that listen for commands using the Exadata RESTful service.

- The following values are allowed for *listeningInterface*: ALL, NONE, or list of network interfaces.
- The listening interface attribute complements the *httpsAccess* attribute.

```
# lsof -i -P -n | grep LISTEN | grep java
java          63902  dbmsvc   34u  IPv6      157781      0t0  TCP *:7879 (LISTEN)

# dbmcli -e alter dbserver listeningInterface=vmeth0
This command will automatically restart and redeploy MS. Continue? (y/n): y
Stopping MS services...
The SHUTDOWN of MS services was successful.
Updating attribute "listeningInterface" before redeploying MS.
Starting MS services...
The STARTUP of MS services was successful.
DBServer scaqa104adm05 successfully altered

# lsof -i -P -n | grep LISTEN | grep java
java          237672  dbmsvc   34u  IPv6 308318206      0t0  TCP <ipaddress>:7879 (LISTEN)
```

SNMP Security Enhancements

SNMP V3 provides strong **authentication and encryption** and is highly recommended.

- SNMP V3 subscribers (type=v3 or type=v3ASR) uses SHA2 authentication protocols.
 - SHA-224, SHA-256, SHA-384, and SHA-512.
- SNMP V1 (type=v1 or type=ASR) remain available but are discouraged.
 - The administrator must specify the SNMP community (public and private are discouraged).

```
# cellcli -e alter cell snmpuser='((name=user01,authprotocol=SHA-512,authpassword=*))'  
snmpUser user01 authpassword: *****  
Confirm snmpUser user01 authpassword: *****  
Cell <host> successfully altered  
# cellcli -e alter cell snmpSubscriber='((host=localhost,port=162,type=V3,snmpUser=user01))'  
snmpSubscriber ((<host>,port=162,community=public,type=asr,asrmPort=16161)) has been replaced with  
((host=localhost,port=162,snmpUser=user01,type=V3)).  
Cell <host> successfully altered
```

Database 23ai Security Enhancements

The following features in Database 23ai are transparently available in Oracle Exadata System Software:

- **Smart Scan on AES-XTS Encrypted Data**
 - In conjunction with Oracle Database 23ai, Oracle Exadata System Software release 24.1.0 transparently enables Exadata Smart Scan on data in tablespaces encrypted using AES-XTS.
 - AES-XTS provides improved security and better performance, especially on Exadata where TDE can take advantage of parallel processing and specialized instructions built into processor hardware.
- **Smart Scan during Online Encryption**
 - Exadata Smart Scan remains fully enabled during long-running online encryption, decryption, and rekeying operations.
 - Previously, Exadata Smart Scan was disabled during such operations.

Centralized Identification and Authentication of OS Users

Oracle Exadata System Software offers support for infrastructure **centralized identification and authentication** of operating system (OS) users.

- LDAP identity management systems
- Kerberos authentication
- Linux System Security Services Daemon (SSSD)
 - Pre-configured with Exadata-specific custom security profile
 - Customizations preserved across upgrades

Centralizes accounts for enhanced security

- Easier administration provisioning/deprovisioning
- Easier password management
- Enterprise security controls

References:

- How to configure Kerberos and SSSD-KCM in Exadata compute nodes and cells (Doc ID 2948255.1)
- LDAP configuration example in Exadata compute nodes and storage servers using SSSD (Doc ID 3020122.1)

Implement Principle of Least Privilege

Security best practices require that each process run with the **lowest privileges** needed to perform the task. The following processes now run as non-privileged users:

- **Smart Scan processes:** Performing a smart scan predicate evaluation does not require root privileges.
 - User cellofl and group celltrace
- **Select ExaWatcher processes:** Some of the ExaWatcher commands that collect iostat, netstat, ps, top, and other information have been modified to run without requiring root user privilege.
 - User exawatch and group exawatch

Operating System Activity Monitoring

Each Exadata server is configured with auditd to **audit system-level activity**.

- Manage audits and generate reports use the auditctl command.
- When the auditd service starts, it runs the augenrules utility. This utility merges all component audit rules files found in the audit rules directory and places the merged results in the /etc/audit/audit.rules file.
 - Exadata specific audit rules are stored in /etc/audit/rules.d/01-exadata_audit.rules.
 - Customer custom audit rules may be stored in /etc/audit/rules.d/20-customer_audit.rules.

```
# auditctl -l
-a always,exit -F arch=b32 -S
chmod,lchown,fchmod,fchown,chmod,setattr,lsetattr,fsetattr,removexattr,lremovexattr,fremove
xattr,fchownat,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
...
```


Encrypting System Log Information (rsyslog)

Management Server (MS) on database and storage servers supports the syslogconf attribute.

- The syslogconf attribute extends syslog rules for a database server.
- The attribute can be used to designate that syslog messages be **forwarded to a specific remote syslogd service**.
- On the MS, the forwarded messages are directed to a file, console, or management application, depending on the syslog configuration on the MS.
- This enables system logs from different servers to be aggregated and mined in a centralized logging server for security auditing, data mining, and so on.

Use certificates and the syslogconf attribute to configure encryption of the syslog information.

Oracle Exadata Deployment Assistant (OEDA)

Use the deployment assistant for initial configuration, and when modifying or adding to an existing deployment. You can import an existing configuration when adding new components or modifying an existing deployment.

- When you first log in to a host following the **Resecure Machine** deployment step, you are prompted to reset the root password. This still occurs even when SSH key-based authentication is enabled, and password-based authentication is disabled.

Password
Complexity

Password
Aging

Password
Expiration

Permissions

host_access_control – system settings

Implement the available features and security plan post deployment via host_access_control.

```
# /opt/oracle.cellos/host_access_control apply-defaults --strict_compliance_only
INACTIVE=0
Deny on login failure count set to 3
Account fail_interval for failed login attempts set to 900
Account unlock_time after {deny} failed login attempts set to 900
Password history set to pam_pwhistory.so 5
Password strength set to pam_pwquality.so minlen=15 minclass=4 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=8 maxrepeat=3 maxclassrepeat=4 local_users_only retry=3 authtok_type=
PermitRootLogin no
hard maxlogins 10
hmac-sha2-256,hmac-sha2-512 for both server and client
Password aging -M 60, -m 1, -W 7
```

host_access_control – system settings

Subset of commands

- access - User access from hosts, networks, etc.
- auditd-options - Options for auditd
- banner - Login banner management
- fips-mode - FIPS mode for openSSH
- idle-timeout - Shell and SSH client idle timeout control
- pam-auth - PAM authentication settings
- password-aging - Adjust current users' password aging
- rootssh - Root user SSH access control
- ssh-access - Allow or deny user and group SSH access
- sshciphers - SSH cipher support control
- ssh-macs - SSH supported MACs
- sudo - User privilege control through sudo

FIPS 140-2 for Oracle Linux Kernel/SSH on Exadata Database Nodes

`/opt/oracle.cellos/host_access_control fips-mode -enable`

- Kernel settings - *Requires a reboot*
 - STIG mitigation: The Oracle Linux operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
 - STIG mitigation: The Oracle Linux operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.

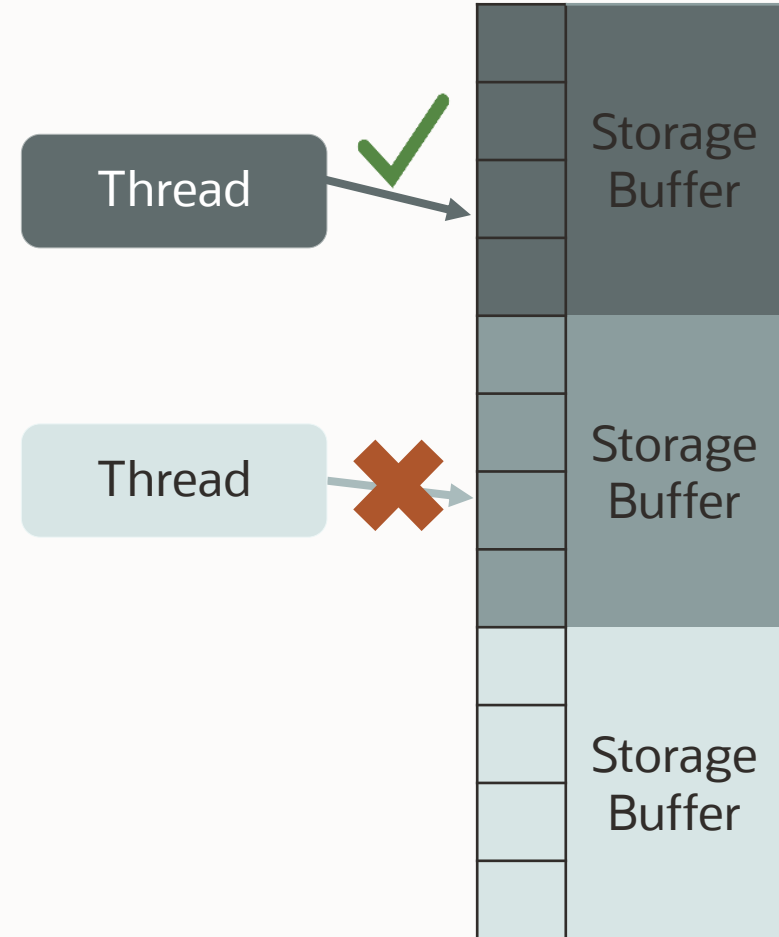
`/opt/oracle.cellos/host_access_control ssh-macs -secdefaults`

- SSH controls
 - STIG mitigation: The Oracle Linux operating system must be configured so that the SSH daemon is configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

Securing Storage Server Processes with Memory Protection Keys

Storage Server Software Memory is partitioned with 16 colors.

- Four bits in each page table entry used to identify the color.
- Each thread is allowed to read/write and enable/disable to its matching color.
- Any access to a piece of memory that does not have the correct color traps the process.
- Protects against inadvertent software defects.
- Enabled out of the box with no tuning needed.
- **Eliminates a class of potential memory corruptions.**



Other Security Capabilities for Storage Servers

Secure Computing (seccomp) feature in Oracle Linux Kernel used to **restrict system calls** that can be made.

- Kernel has hundreds of system calls, most not needed by any given process.
- A seccomp filter defines whether a system call is allowed.
- Seccomp filters installed for cell server and offload processes automatically during upgrade.
- Allow-list set of system calls are allowed to be made from these processes.
- Seccomp performance additional validation of the arguments.

Disabling SSH

- Storage servers can be **“locked”** from SSH access.
- ExaCLI can still be used to perform operations.
 - Communicates using HTTPS and REST APIs to a web service running on the server.
 - Temporary access can be enabled for operational access if required.

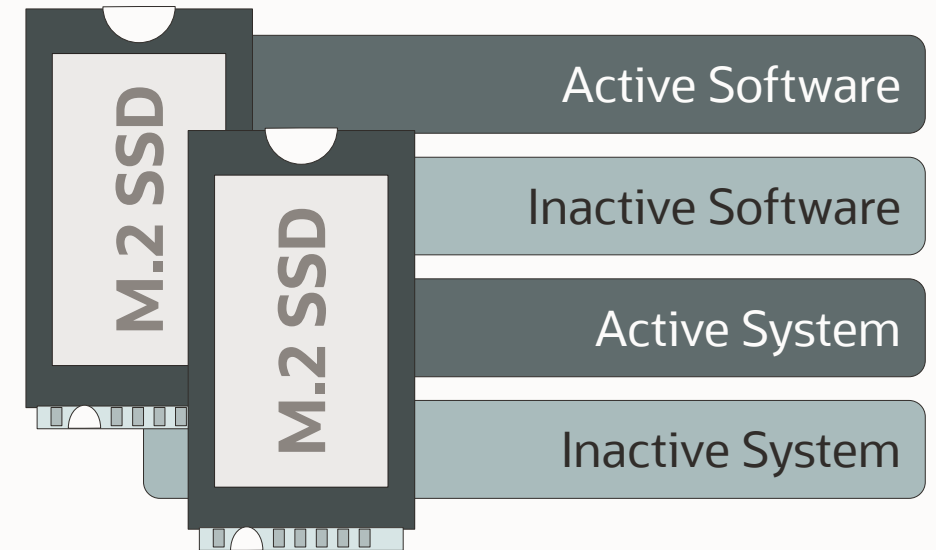
Storage Server Partition Installation

Exadata installs the system/software on alternating partitions.

- When upgrading to a newer version, the software is installed on the inactive partition and then booted to that partition.

This ensures a complete OS refresh is completed at each upgrade which **minimizes the propagation of infected files**. OS data is separate from database data.

- Database is safe from OS corruption.



Oracle Exadata Rack and Oracle Exadata Storage Servers can remain online and available while replacing an M.2 disk.

Advanced Intrusion Detection Environment (AIDE)

Help **guard against unauthorized access** to the files on your Exadata system.

- AIDE creates a database of files on the system and then uses that database to ensure file integrity and to detect system intrusions.

```
# /opt/oracle.SupportTools/exadataAIDE -status
```

```
AIDE: daily cron is currently enabled.
```

```
To add additional rules:
```

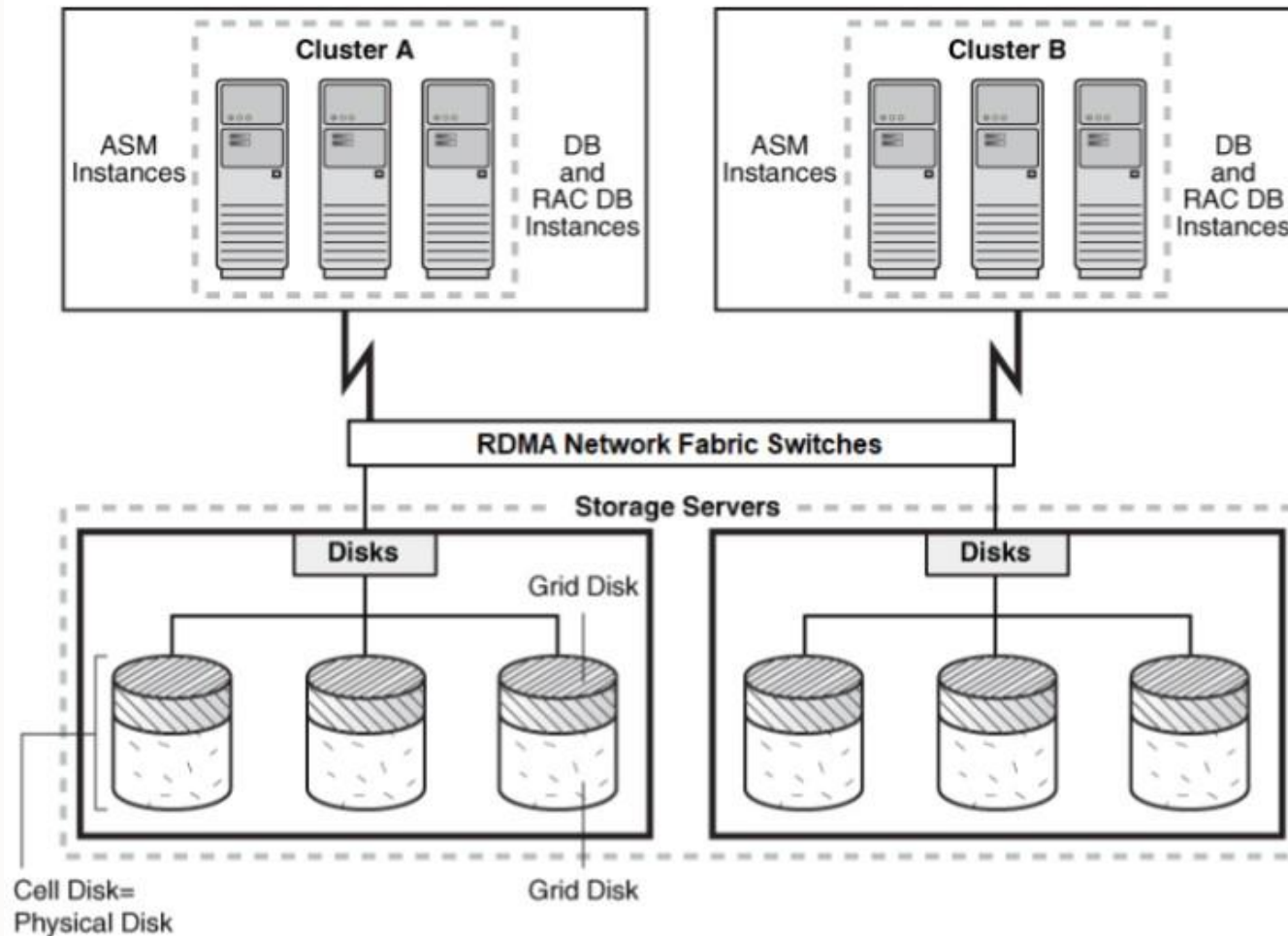
```
Edit the file /etc/aide.conf
```

```
Update the AIDE database metadata.
```

```
# /opt/oracle.SupportTools/exadataAIDE -u
```

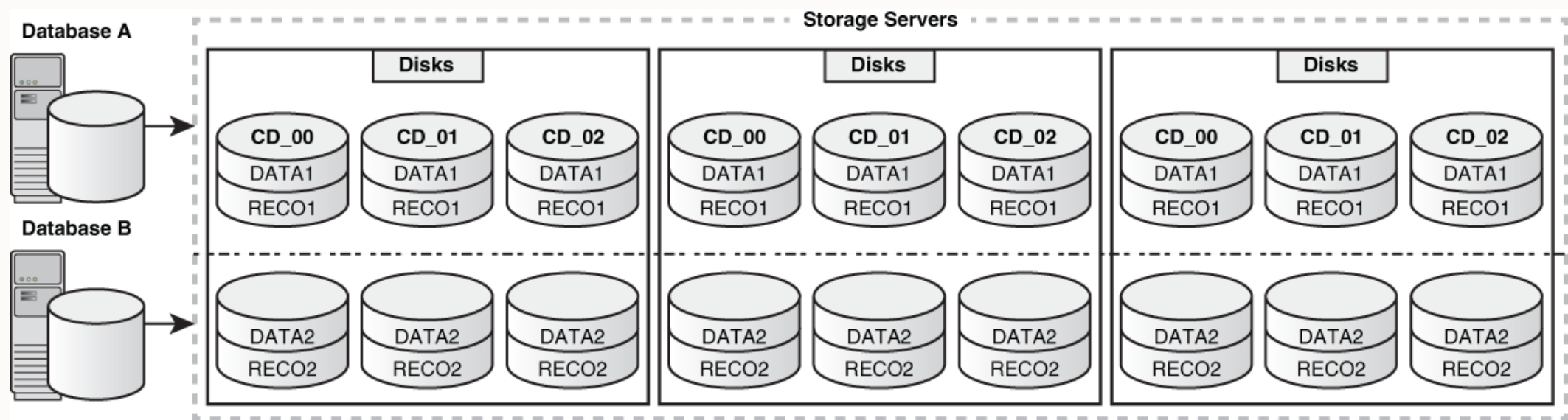
ASM-Scoped Security

Restrict access to only the grid disks used by the Oracle ASM disk groups associated with an Oracle ASM cluster.



DB-Scoped Security

Restrict access for an Oracle Database instance to a specific set of grid disks.



Secure Erase

Provide a **secure erase solution** for every component within Oracle Exadata Database Machine

- Crypto-erase is used whenever possible and is fully compliant with the NIST SP-800-88r1 standard

Component	Make or Model	Erase Method
Hard drive	<ul style="list-style-type: none">• 8 TB hard drives on Oracle Exadata Database Machine X5• All hard drives on Oracle Exadata Database Machine X6 or later	Crypto erase
Hard drive	All other hard drives	1/3/7-Pass erase
Flash device	Flash devices on Oracle Exadata Database Machine X5 or later	Crypto erase
Flash device	All other flash devices	7-pass erase
M.2 device	Oracle Exadata Database Machine X7-2 or later	Crypto erase





“Oracle Exadata Cloud@Customer uses the superior technology of Oracle Database as a cloud service delivered in our own data centers, **meeting all of our data sovereignty and compliance requirements** for the Regional Revitalization Cloud.”

Norihito Senda

Nagoya Branch

Advanced Solution Department

Corporate Business Headquarters

Nippon Telegraph and Telephone West Corporation (NTT WEST)

Security Best Practices

The security of a system is only as good as its weakest link.

- Regular scans should be **run by YOU the owner of the system** to ensure against any deviations from the delivered configurations.
- Maintaining the latest Software Update ensures the latest security vulnerabilities are mitigated.
- Tools and processes are there to assist in creating a secure environment, but they must be used!

References

—

Maximize Security, Maximize Performance, Maximum Availability

Security References

Oracle Exadata Database Machine Security FAQ

- My Oracle Support (MOS) note: **Doc ID 2751741.1**

Oracle Exadata Documentation

- <https://docs.oracle.com/en/engineered-systems/exadata-database-machine/books.html>

Oracle Corporate Security Practices

- <https://www.oracle.com/corporate/security-practices/>

Critical Patch Updates, Security Alerts and Bulletins

- <https://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Oracle Corporate Security Blog

- <https://blogs.oracle.com/security/>

Thank you

ORACLE

Companion Slides

MAA

Database

Cloud

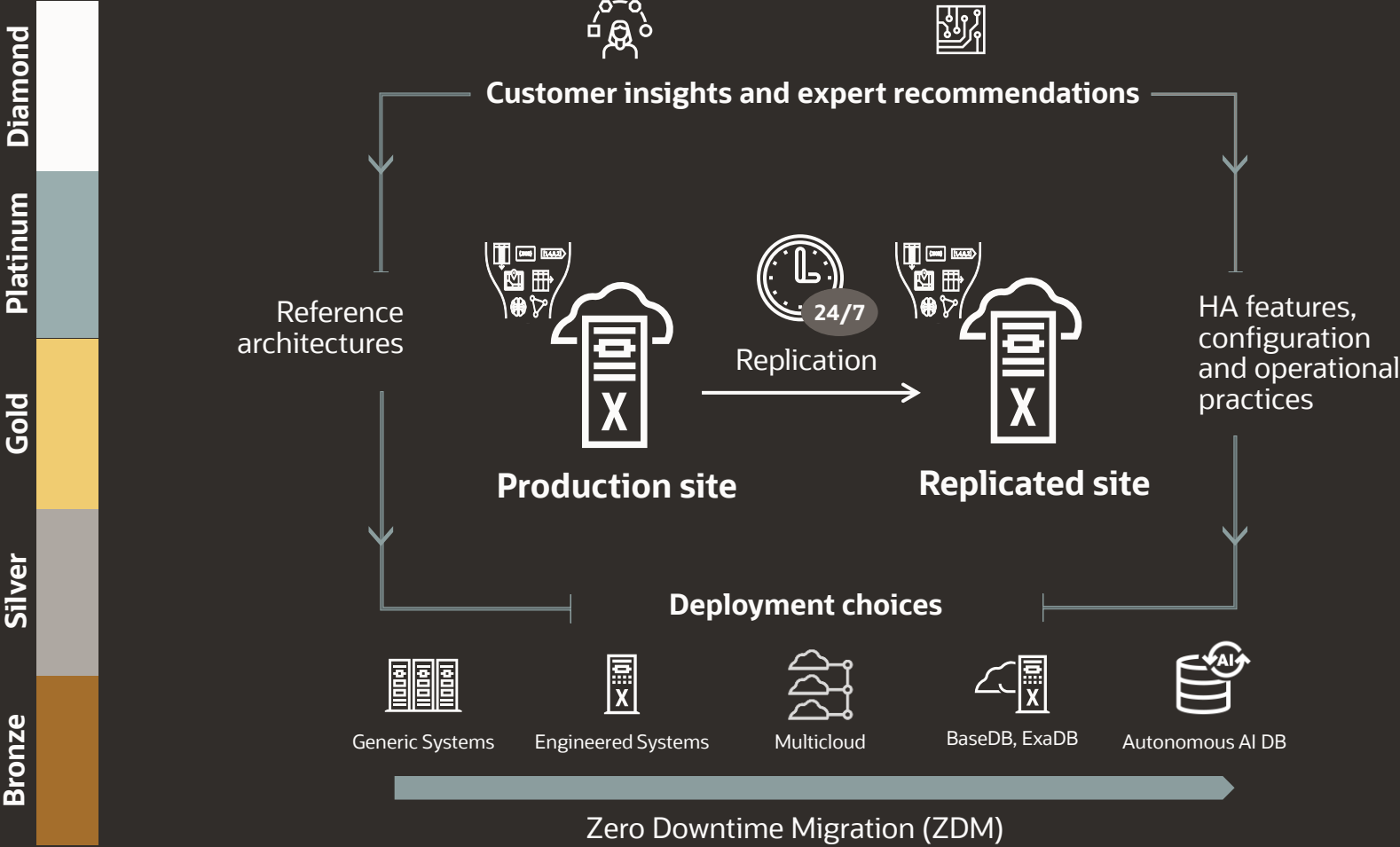
Supply Chain

Ransomware (RA)

Maximum Availability Architecture (MAA)

Maximize Security, Maximize Performance, **Maximum Availability**

Next Gen Maximum Availability Architecture (MAA)



High performance

Resource Management

Database In-Memory

True Cache

Continuous availability

Application Continuity

Online Redefinition

Edition-based Redefinition

Data protection

Flashback

RMAN

ZDLRA+ ZRCV

Active replication

Active Data Guard

Full Stack DR

GoldenGate

Scale out & Lifecycle

RAC

Globally Distributed AI Database






FPP

Real Application Testing



Next-Gen MAA Reference Architectures

Availability service levels for the next generation of Oracle AI Database

Bronze	Silver	Gold	Platinum	Diamond (NEW)
<div><div>Dev, test, prod</div><div>Single instance DB Restartable Backup/restore</div><div></div></div>	<div><div>Prod/departmental</div><div>Bronze + Database HA with RAC or Local Data Guard Client failover HA best practices Application Continuity (optional)</div><div></div></div>	<div><div>Business critical</div><div>Silver with RAC + DB replication with (Active) Data Guard with automatic failover Client failover DR best practices</div><div></div></div>	<div><div>Mission critical</div><div>Gold with Exadata and either option: Option 1: GoldenGate with Oracle Database 19c OR Option 2: (Active) Data Guard with Oracle AI Database 26ai</div><div></div></div>	<div><div>Extreme availability</div><div>Configuration GoldenGate 23ai replicas, <i>each running</i>: Oracle AI Database 26ai + RAC on Exadata + (Active) Data Guard</div><div></div></div>
Recoverable local failure: Minutes to hour Disasters: Hours to days RPO < 15 min	Recoverable local failure: seconds to minutes Disasters: Hours to days RPO < 15 min	Recoverable local failure: Less than 60 seconds Disasters: < 5 min RPO = zero or near zero	Recoverable local failure: Less than 20 seconds Disasters: < 1 min RPO = zero or near zero	Recoverable local failures: Less than 10 seconds Disasters zero to 10 secs RPO = zero or near zero



Exadata MAA for On Premises and Cloud

Many more features working to improve HA, QoS, data protection and life cycle

For more details , please refer to the [Exadata documentation](#), the [Exadata MAA presentation](#), and the [MAA website](#)

- Instant Death Detection
- Highly available Clusterware Services
- Real Application Clusters
- Client Failover, Transparent Application Continuity
- Resilient RDMA
- Graceful, coordinated network failback
- Client Failover, Transparent Application Continuity
- Flash cache health factor
- Auto disk management
- Prioritization of most critical files during rebalance
- Rebalance with optimized power
- Fast resilver after flash failure
- Fast resync maintaining cache state
- Smart OLTP caching
- Exadata Live Update
- Patchmgr support for RoCE switch upgrades (on premises and ExaCC)
- High redundancy
- RDBMS/RAC Hangman
- Cell side latency timeouts and capping
- Exaportmon
- RS restart capability
- Smart scan quarantine
- MS alerts for resource utilization
- Predictive failure/Confinement
- Do-Not-Service light integration
- ASMDactivationOutcome
- Flashback database
- Buddy instances, 2 pass instance recovery
- Online M.2, hard disk, and flash replacement

Database Security

Maximize Security, Maximize Performance, Maximum Availability

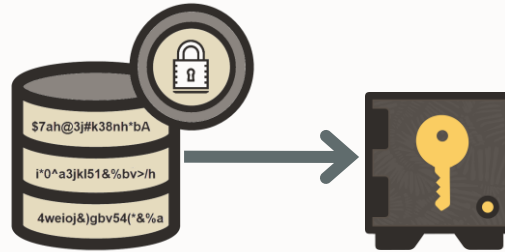
How do you protect the database?

Implement a secure configuration



- Ensure your database configuration follows policy
- Patch for known vulnerabilities
- Watch out for configuration drift

Control access to the data



- Encrypt data in motion and at rest
- Protect against network sniffing attacks
- Protect against data scraping attacks (e.g.: ransomware)

Encrypt the data and protect the encryption keys



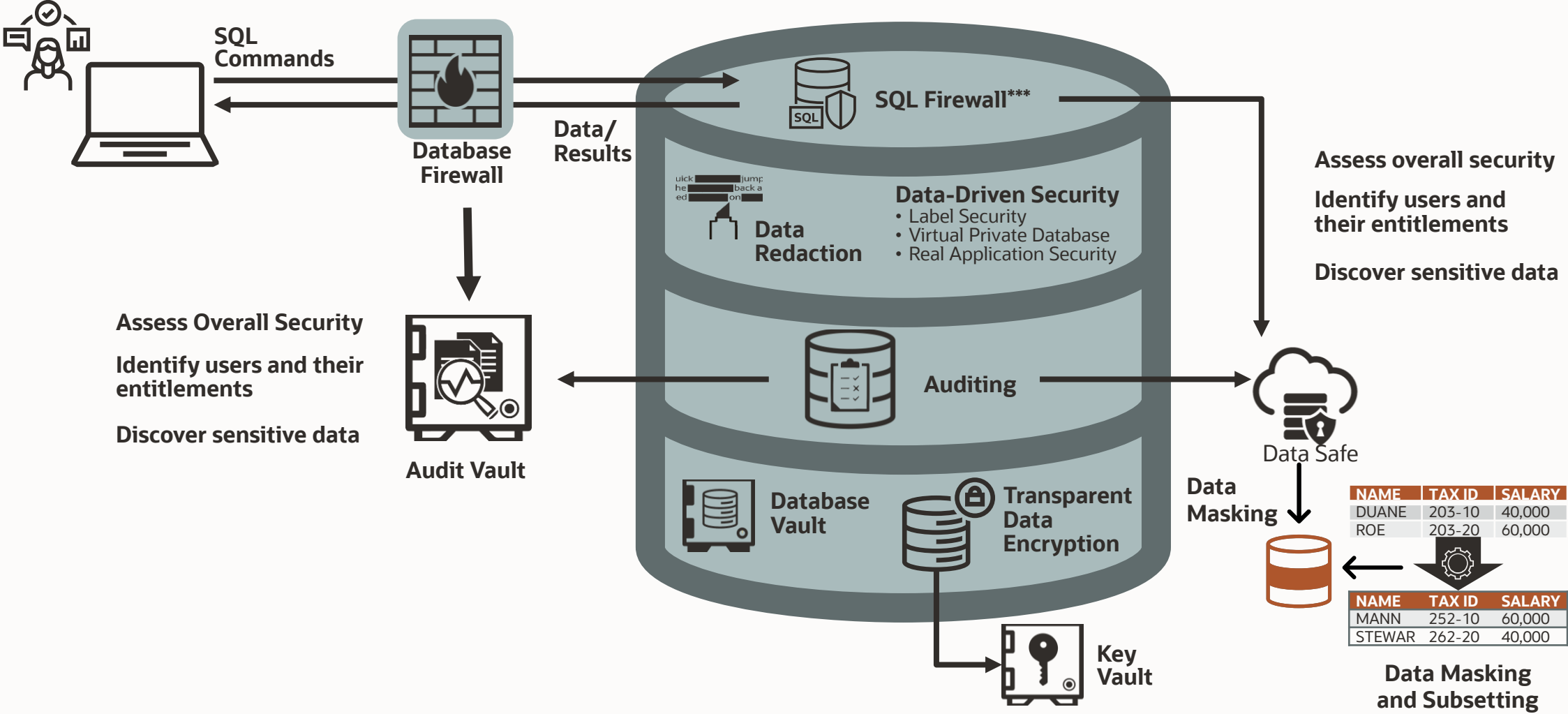
- Enforce least privilege
- Control privileged user access to data
- Enforce separation of duties
- Establish and enforce a trusted path to data

Monitor access to the data



- Use native auditing capabilities to capture high-value activity
- Use network-based monitoring to examine ALL activity

Oracle Database Maximum Security Architecture



*** Only available in Oracle Database 23ai



Oracle Data Safe

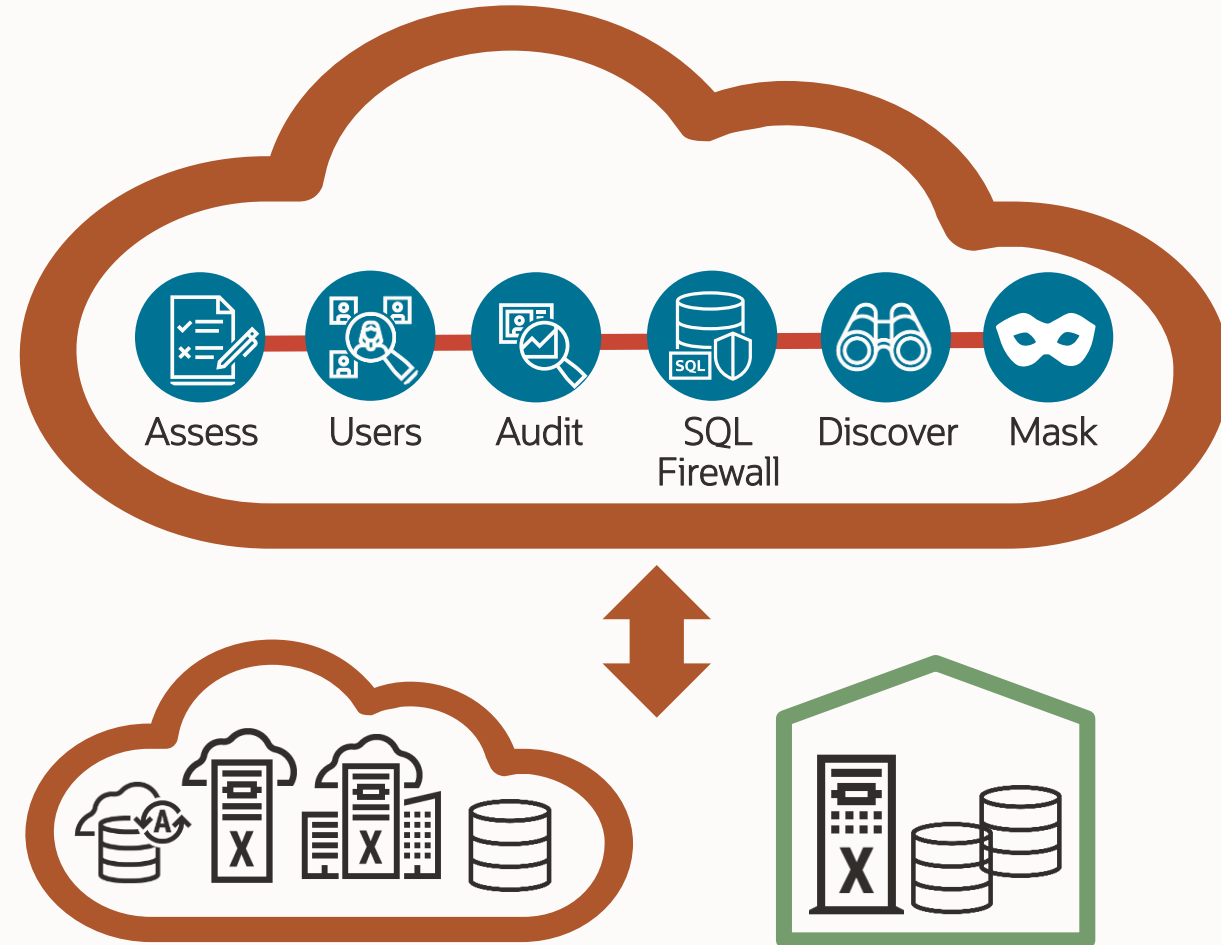
Unified database security control center

- Assess and secure database configurations
- Identify stale accounts and maintain password discipline
- Implement database audit policies
- Locate PII and other sensitive data in databases
- Protect sensitive data for test, development and analysis
- Manage SQL Firewall policies *

Benefits

- ✓ No special expertise needed: click-and-secure
- ✓ Save time complying with regulations and corporate policies
- ✓ Defense-in-depth security for all customers

*Available for Oracle 23ai



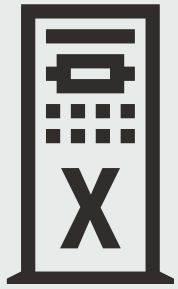
**Data Safe helps secure your
cloud and on-premises databases**

Cloud Security Considerations

Maximize Security, Maximize Performance, Maximum Availability

Exadata Runs Everywhere

On-premises, hybrid cloud, Oracle public cloud and multicloud



**Exadata Database
Machine**

(on-premises)



**Exadata
Cloud@Customer**

(hybrid cloud)



**Exadata Cloud
Infrastructure**

(Oracle public cloud)



Multicloud

(connect to other clouds)

Same Exadata technology | 100% compatible | Zero downtime migration

Exadata Platform Provides the Foundation for Exadata DB Cloud

Security overview

Exadata security practices and built-in security protection is applicable to Exadata on-premises

- Exadata Cloud (ExaDB-D, ExaDB-C@C, ExaDB-XS and Autonomous Database) inherit the benefits plus additional cloud software and security compliance is added

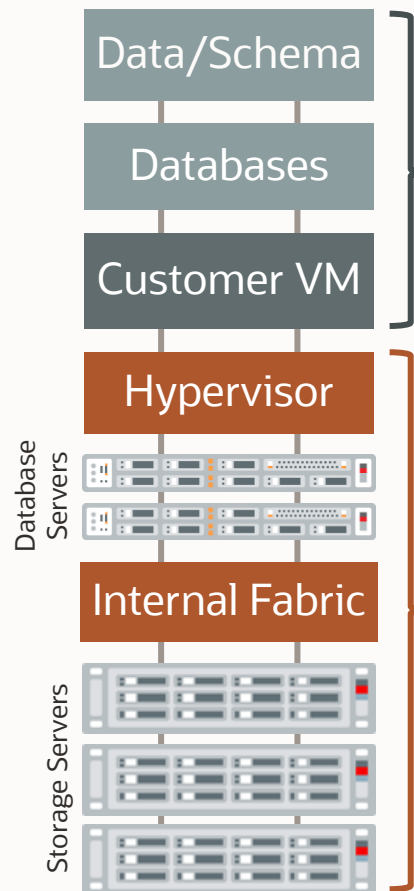
Exadata Cloud in OCI attains the following compliances, certifications, and/or attestations:

- | | |
|-------------|-----------------------|
| ✓ PCI DSS | ✓ C5/CSA STAR Level 2 |
| ✓ HIPAA | ✓ FedRAMP High |
| ✓ ISO 27001 | ✓ DoD IL5 |
| ✓ SOC 1/2/3 | ✓ UK Cyber Essentials |

Additional security collateral for DB Cloud offerings can be found at:

- <https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/exadata-cloud-at-customer-security-controls.pdf>
- <https://www.oracle.com/corporate/security-practices/cloud/>

Simple Cloud Management Model in Public Cloud



Customer owns everything inside database

- Data, schema, encryption keys

Customer subscribes to database services

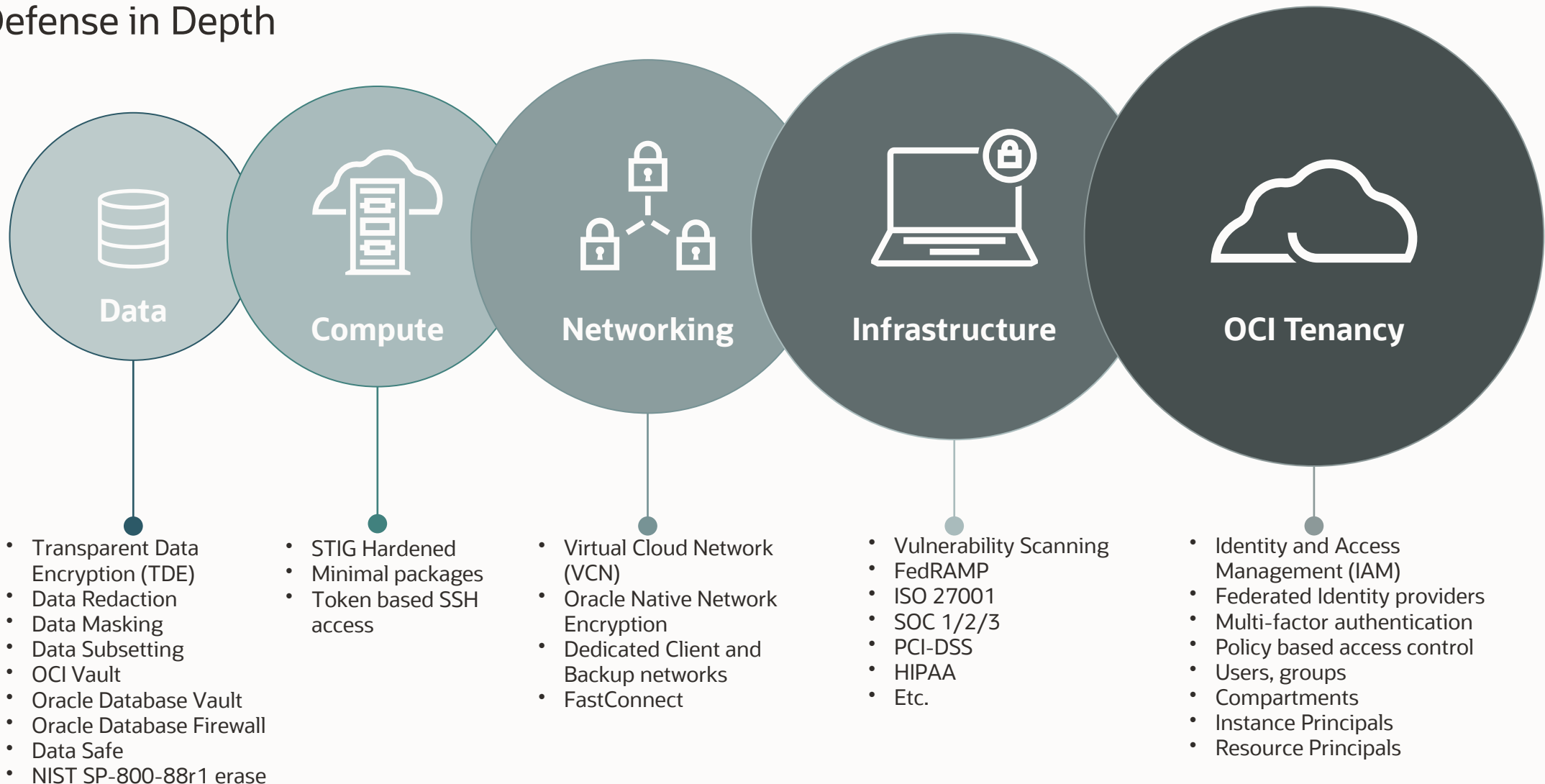
- Customer manages VMs and Databases using Cloud Automation (UI / APIs)
- Automation to create, delete, patch, backup, scale up/down, etc.
- Runs all supported Oracle Database versions
- Customer controls access to customer VM
- Customer can install and manage additional software in customer VM
- Oracle staff are not authorized to access customer VM

Oracle owns and manages infrastructure

- Hypervisor, database and storage servers, storage network
- Patching, security scans, security updates
- Monitoring and maintenance
- Customer not authorized to access Oracle infrastructure

Integrated Security from Data to Identity

Defense in Depth



Supply Chain Protection

Maximize Security, Maximize Performance, Maximum Availability

Exadata Supply Chain Risk Management

Identifying & mitigating risks in key threat areas

Ensure Genuine, Unaltered, according to specifications, no unwanted functionality

Protect Information
describing or traversing the supply chain or about the parties



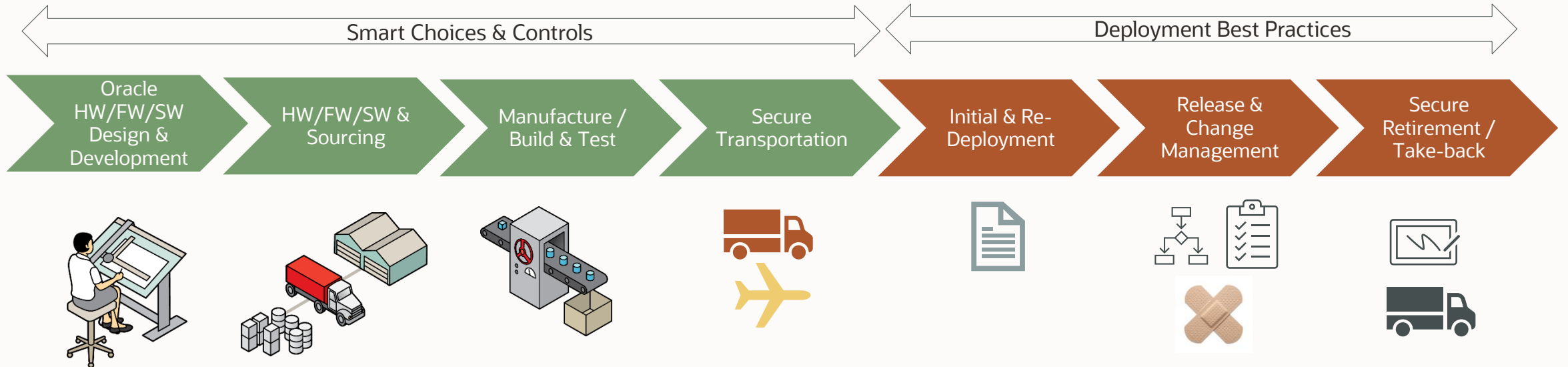
Supply Continuity
Providing required products and services under supply chain disruption

Reduce vulnerabilities that limit function, lead to failure, or enable exploitation

Based on **NIST SP 800-161** Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Across the Exadata lifecycle

Addressed by multiple layers of defense throughout Hardware, Firmware & Software lifecycle



Oracle Hardware Supply Chain Controls

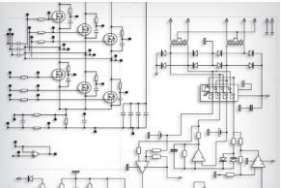
Exadata Policies / Updates

Oracle Corporate Processes / Standards

Product Lifecycle Security (OSSA), **Information** Security, **Physical** Security, **Deployment** Security

Exadata Hardware Supply Chain

Oracle's Deep Control + Deep Visibility



Oracle Design



Oracle Specified Parts



Oracle Approved List of Part Suppliers



Oracle External Manufacturer

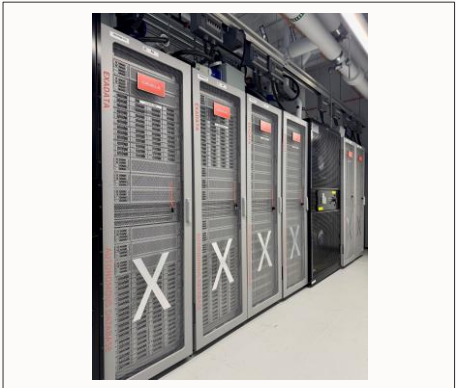
- Oracle specified manufacturing processes
- Oracle in-factory test infrastructure



Oracle Secure Transportation



Multi-Cloud



On-premises



Security throughout the Exadata supply chain

Oracle control and visibility via comprehensive processes + continuous improvement

Oracle owns core Exadata Hardware, Firmware and Software Intellectual Property

- Oracle designs hardware, develops software and core firmware
- Selectively uses third party technology under strict process controls

Oracle controls external manufacturing and secure transportation

- Contracted suppliers understand and must adhere to Oracle security policies
- Oracle specifies HW server manufacturing processes, every part and every supplier for every part
- Oracle specifies transportation processes, including chain of custody with tamper evident packaging
- Encrypted transmission of hardware design data and firmware to factories
- All firmware and software is digitally signed and certified

Oracle has mature security lifecycle processes

- Oracle Software Security Assurance (OSSA), Oracle Advanced Quality Processes (AQP)

Oracle verifies

- Security reviews / audits for all hardware design, software and firmware releases
- Oracle controlled in-factory systems qualification tests and validation

Option to order USA manufactured TAA compliant Exadata systems

Ransomware Protection

Maximize Security, Maximize Performance, Maximum Availability

Data Protection and Ransomware Challenges

With ever-increasing data volumes, organizations face growing risks to their databases:

- Data loss due to accidental deletions
- Data corruptions due to hardware failures
- Data hostage due to ransomware threats

Without a robust backup and recovery solution, critical data can be lost, leading to operational downtime, regulatory penalties, and reputational damage



Zero Data Loss Recovery Appliance (ZDLRA)

Next Generation Intelligent Data Protection against Ransomware

Ransomware resiliency

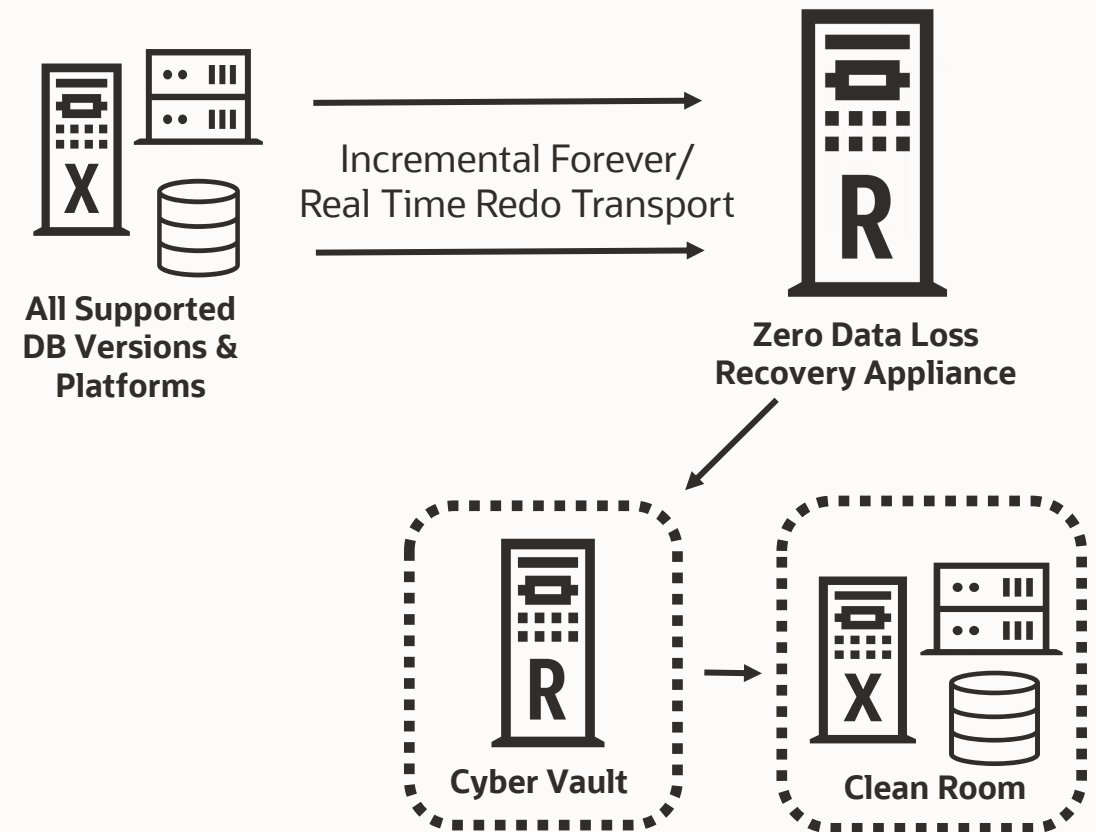
- Zero data loss protection
- Fast, transaction-level recovery
- Continuous data anomaly detection

Protect backups from attacks

- Immutable backups
- Role-based management framework
- End-to-end data encryption

Cyber recovery to clean room

- Air gap backup in cyber vault
- Independently managed access & policies
- Audit & compliance reporting

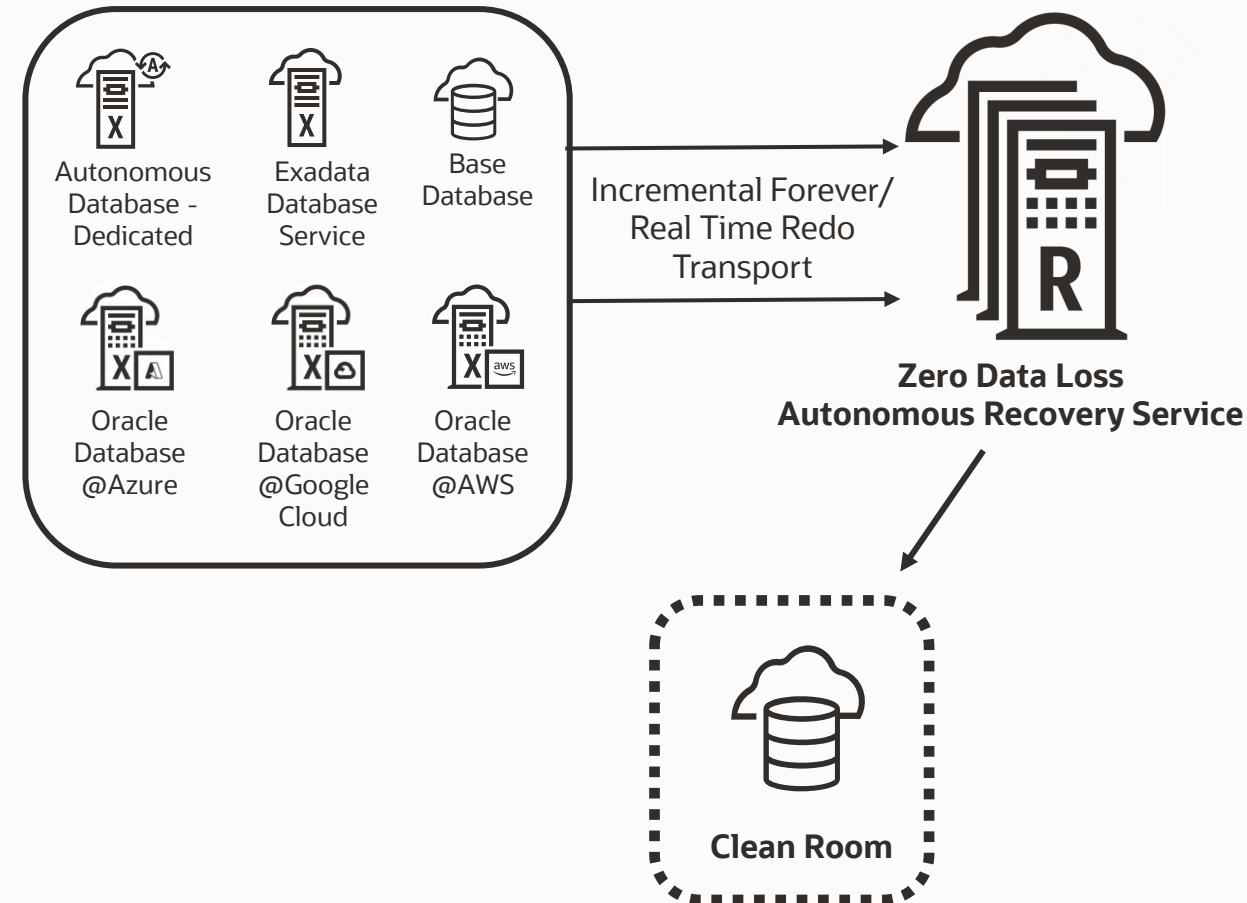


Zero Data Loss Autonomous Recovery Service (ZRCV)

Next Generation Intelligent Data Protection against Ransomware – in Cloud

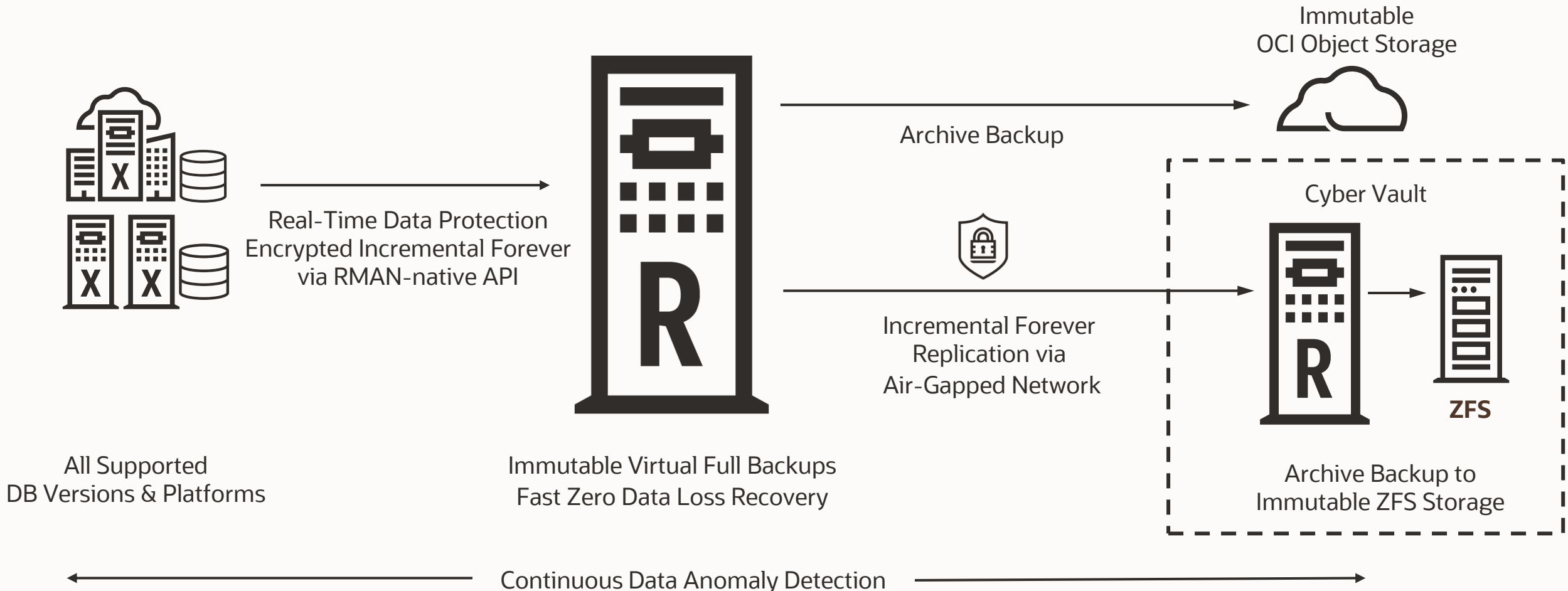
All ZDLRA benefits plus all Cloud benefits:

- Cloud observability, monitoring, & reporting
- Database cloud service-integrated experience
- Cyber recovery to clean room
- Logical air gap between customer & service tenancy
- Granular control via identity & access management



Zero Data Loss Recovery Appliance (ZDLRA)

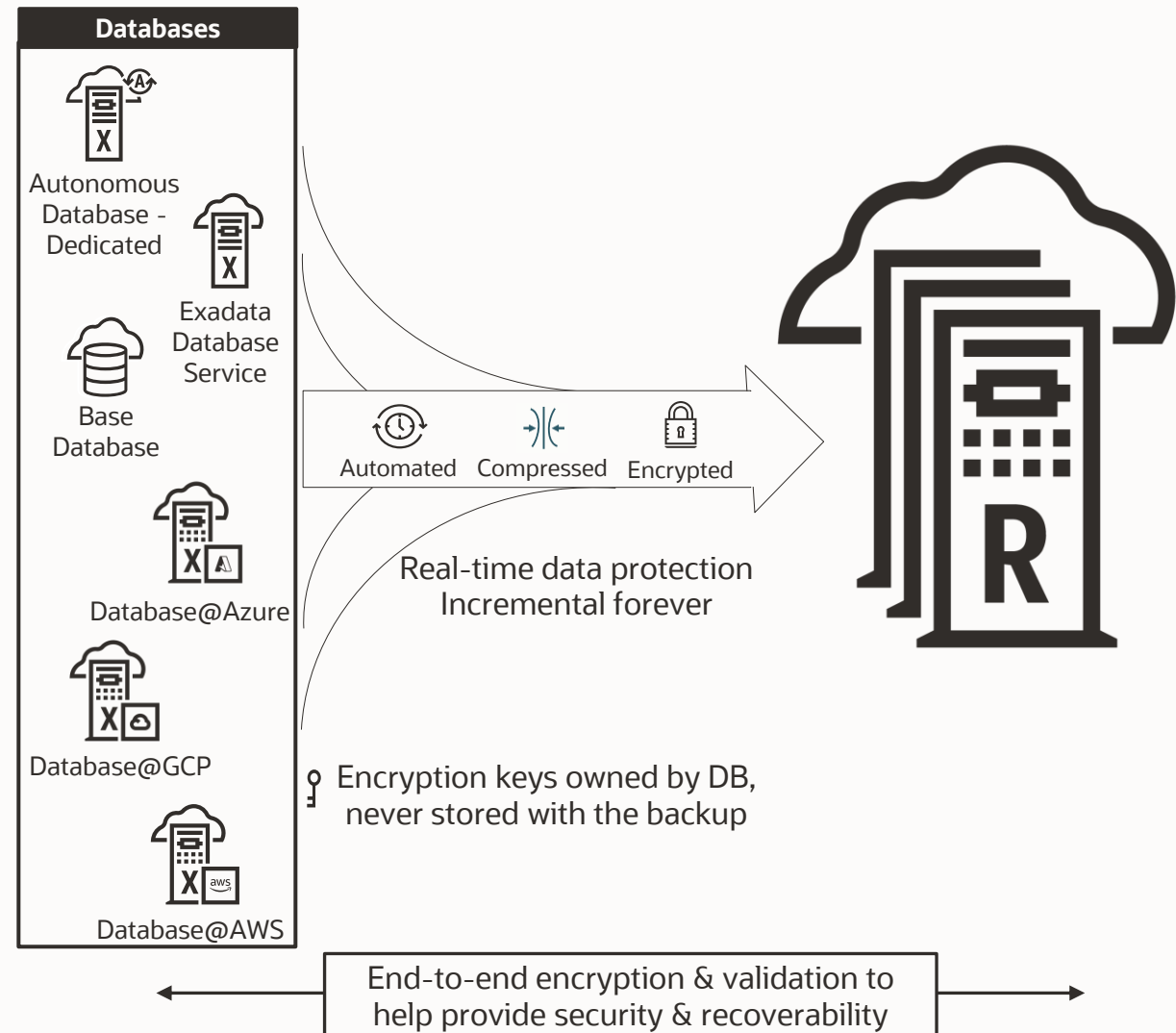
Next Generation Intelligent Data Protection against Ransomware



Zero Data Loss Autonomous Recovery Service (ZRCV)

Highly secure, scalable ransomware protection for databases in OCI, Azure, Google Cloud & AWS

- Zero Data Loss protection with fast recovery
- Enforced data encryption
- Continuous anomaly detection & validation
- Backup immutability & retention lock
- Separation of duties & granular access control
- Logical airgap between the customer tenancy and Oracle Cloud Operations
- Long-term backup retention up to 10 years



Protect your ability to restore

Build a framework for recovery

On-Premises:

Zero Data Loss Recovery Appliance (ZDLRA)

Best-in-class Ransomware Protection

- Industry leading restore times
- Invisible to the network - no filesystem exposed
- Databases access ZDLRA through RMAN-native API
- Supports air-gapped Cyber Vault for even higher levels of assurance
- Access management and authorization controls (Separation of duties / Admin Voting)

Operational efficiency

- No more weekly full backups – eliminates production overhead
- Shorter backup windows with incremental forever strategy
- Zero-impact continuous database recovery validation for every backup
- Gain deep data protection insights with granular recovery health dashboard

Ransomware resiliency

- Fast, zero data loss recovery with optimized backups
- Safeguards backups with policy-level database retention lock

OCI / Multicloud:

Zero Data Loss Autonomous Recovery Service (ZRCV)

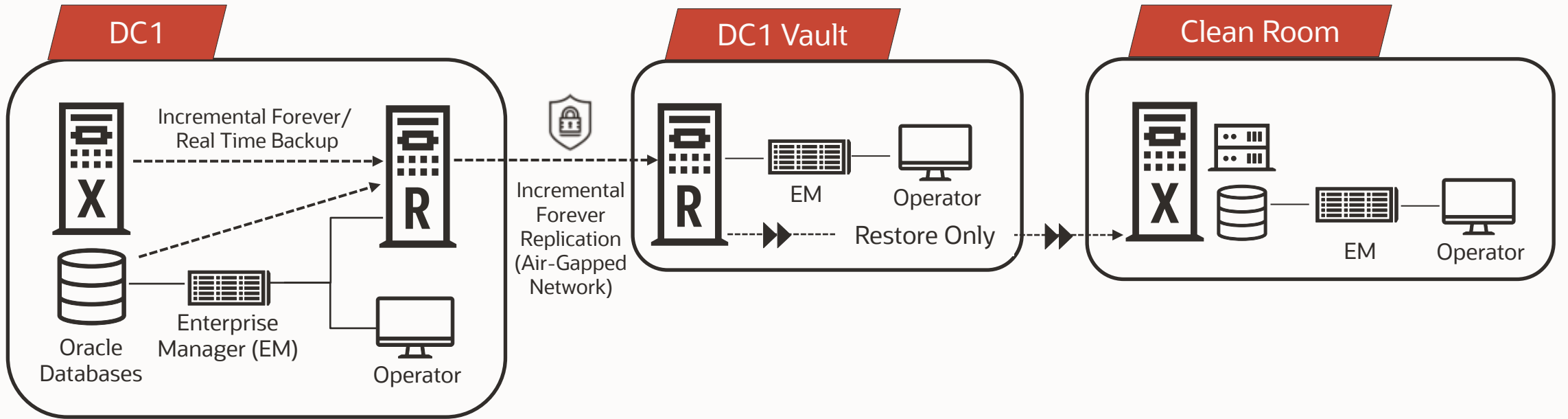
ALL ZDLRA benefits plus Cloud benefits:

- Quickly configure database protection at scale with zero data loss
- Control costs with database-specific backup consumption metrics
- Automated and mandatory encryption to help prevent data theft

Alternative Solutions

- Oracle Database Backup Cloud Service
- Air-gapped and offline media (e.g.: removable drives)
- Offline backup to storage media like magnetic tape

Recovery Appliance Cyber Vault Configuration



Real-Time Protection

- Latest validated backup always ready for replication

Network-Isolated Backup Copy

- Fast, incremental forever replication minimizes vault access time
- Independently validated backups for recovery

Fast Restore

- Quickly recover databases to clean room directly from vault with near-current RPOs

Recovery Appliance Archive to Cloud

Cost-effective, immutable secondary backup storage tier

Recovery Appliance integrated with OCI Object & Archive Storage

- Long-term retention & compliance backup requirements
- Leverages unlimited cloud storage tier managed by Oracle

Archived backups in Oracle Cloud can use standard RMAN format

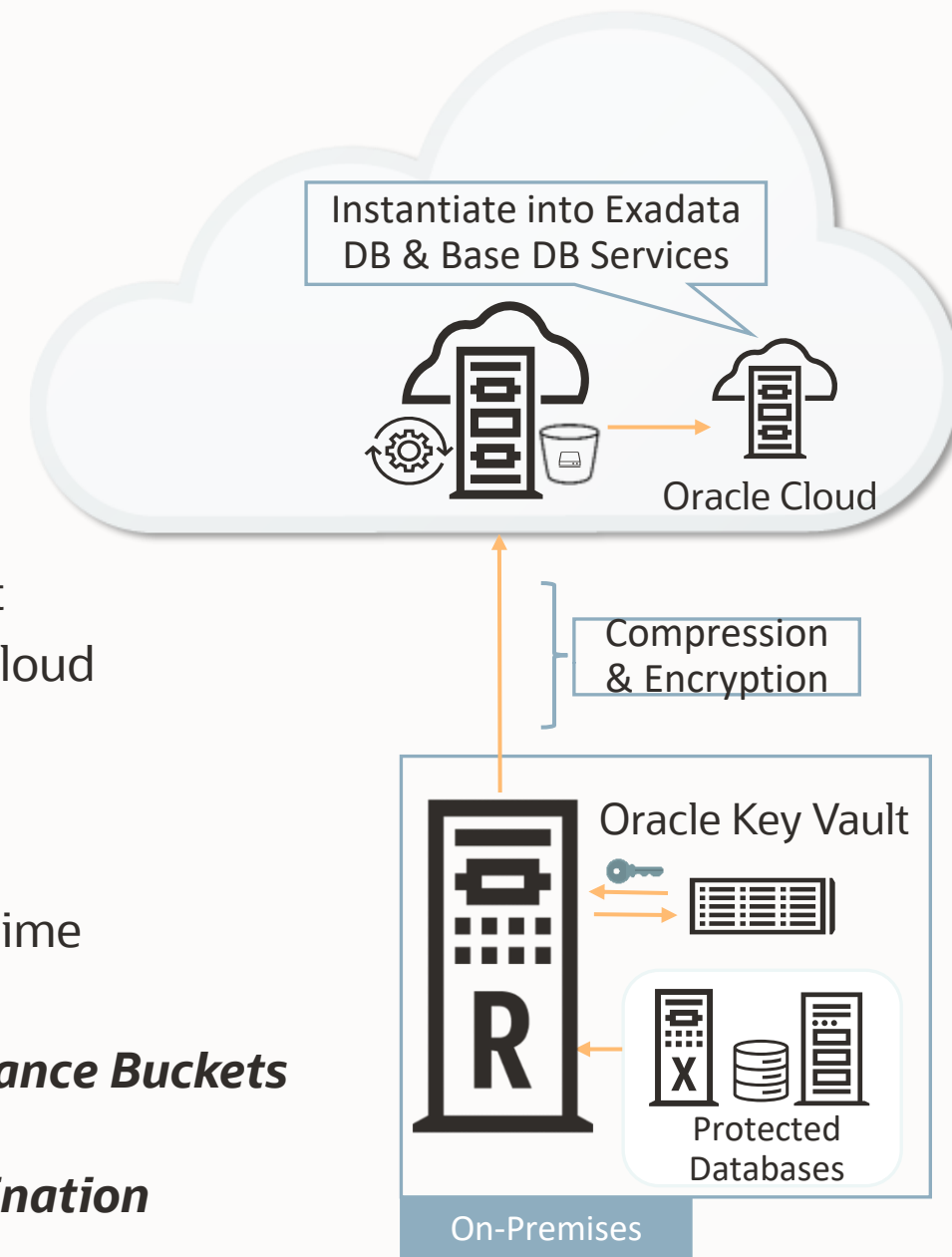
- Quickly provision new OCI databases – accelerate journey to Cloud

Archive backups are encrypted

- Leverages Oracle Key Vault for Key Management
- Protection Policies Drive Archival Operations and Retention Time

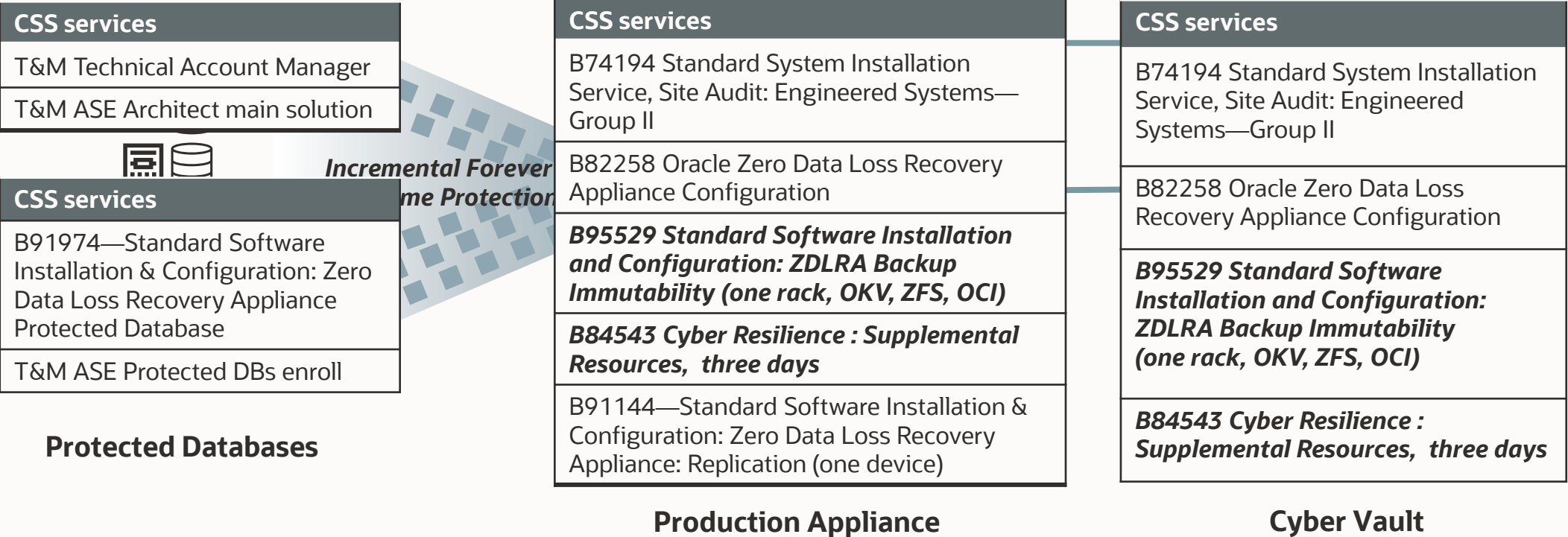
Enforce Immutable Cloud Backups via OCI Regulatory Compliance Buckets

Supports ZFS as on-premises OCI object storage archive destination



Oracle Customer Success Services for Recovery Appliance

Built to Defend and Recover Databases from Ransomware Attacks



For more information: [ZDLRA Services Data Sheet](#)

