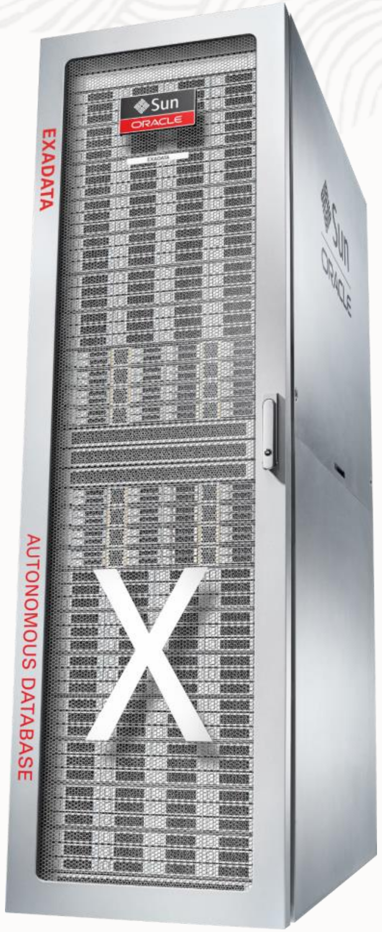
ORACLE

Oracle Exadata Database Machine

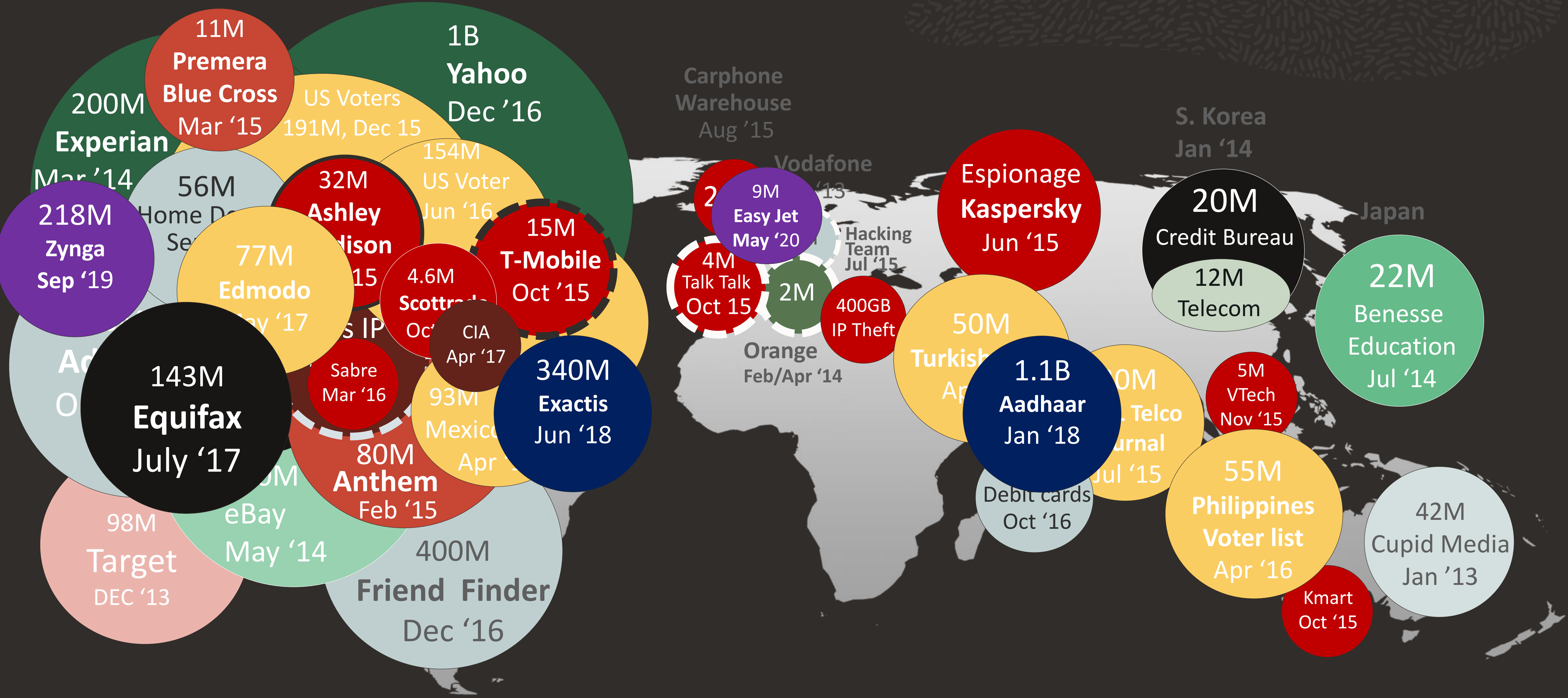
Maximum Security Architecture

Security Maximum Availability & Architecture (MAA) Team

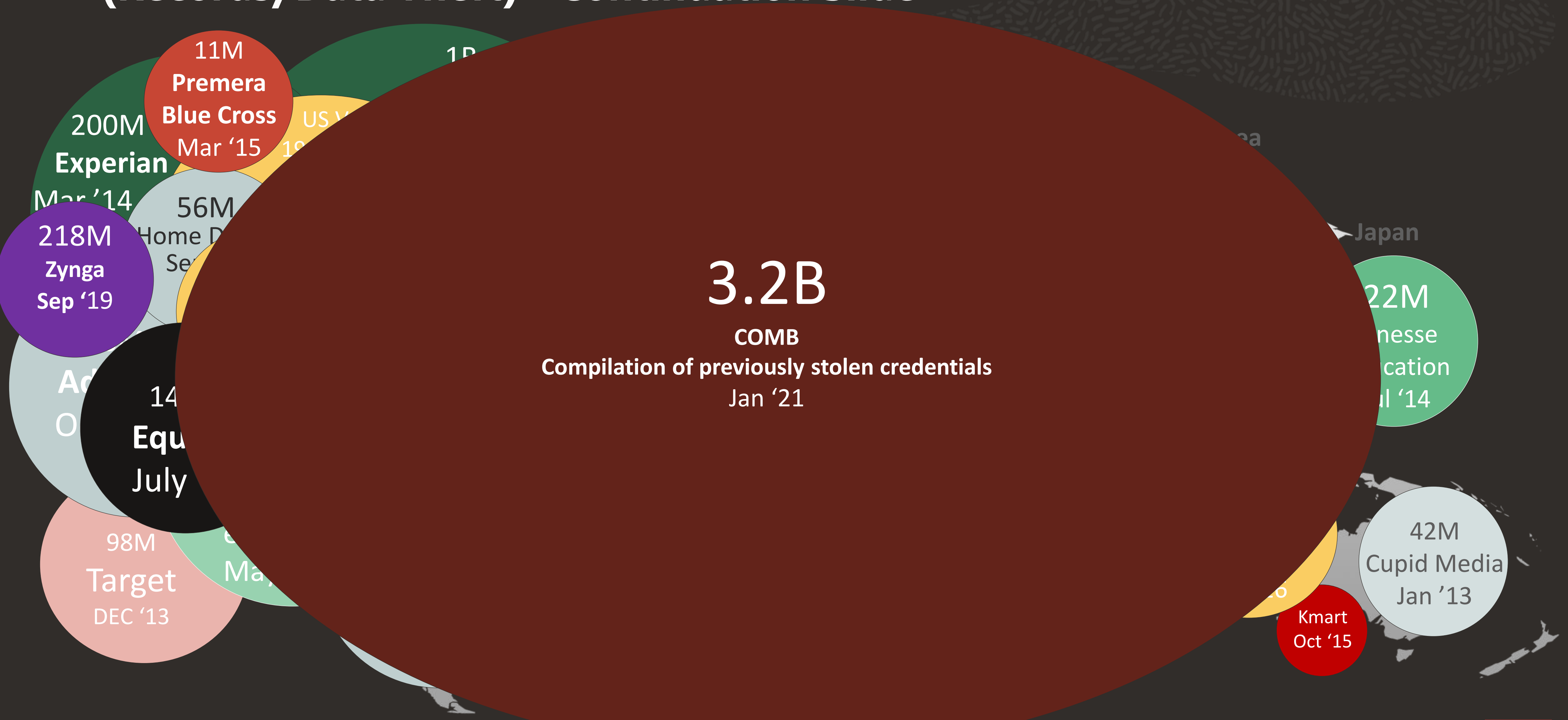
Exadata Product Development



Security Breaches: High Costs to Businesses and Customers (Records/Data Theft)



Security Breaches: High Costs to Businesses and Customers (Records/Data Theft) – Continuation Slide



3.2B
COMB
Compilation of previously stolen credentials
Jan '21

11M
Premera Blue Cross
Mar '15

200M
Experian
Mar '14

218M
Zynga
Sep '19

56M
Home D
Se

98M
Target
DEC '13

22M
nesse
cation
l '14

42M
Cupid Media
Jan '13

Kmart
Oct '15

Exadata Platform provides the foundation for Exadata DB Cloud

This presentation is primarily geared towards on-premises Exadata deployments; however:

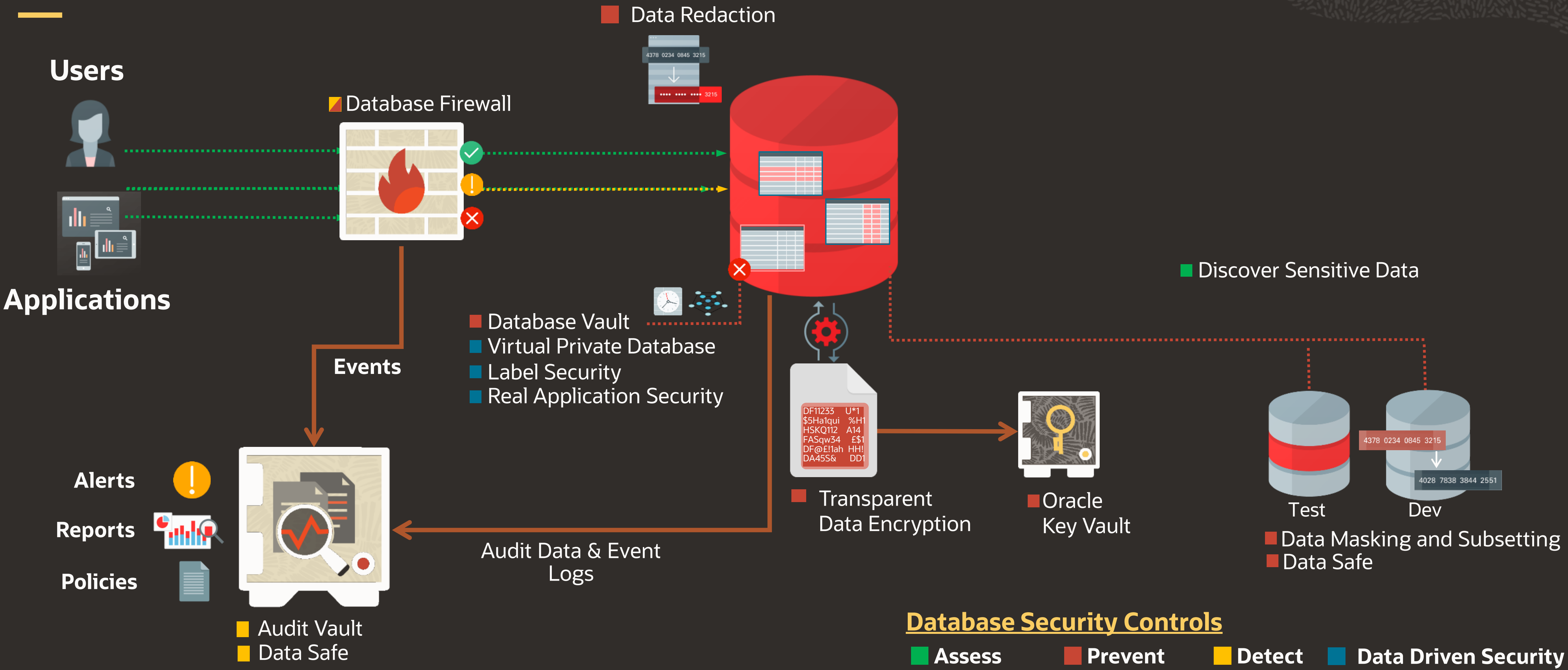
- Exadata is the baseline platform for ExaCC, ExaCS, and Autonomous Database
- These DB Cloud offerings inherit the security from the Exadata baseline image and further layer their own software and security
- Additional security collateral for DB Cloud offerings can be found at:
    - https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/exadata-cloud-at-customer-security-controls.pdf
    - https://www.oracle.com/corporate/security-practices/cloud/

ExaCS OCI attains the following compliances, certifications, and/or attestations:

Audit Reports

- PCI DSS
- HIPAA
- ISO 27001
- SOC I/SOC II
- C5/CSA STAR
- FedRAMP Moderate/DISA IL5

Database Security



Users

Applications

◪ Database Firewall

🟥 Data Redaction

Events

🟥 Database Vault
🟦 Virtual Private Database
🟦 Label Security
🟦 Real Application Security

🟩 Discover Sensitive Data

Alerts

Reports

Policies

🟨 Audit Vault
🟨 Data Safe

Audit Data & Event Logs

🟥 Transparent Data Encryption

🟥 Oracle Key Vault

Test

Dev

🟥 Data Masking and Subsetting
🟥 Data Safe

Database Security Controls

🟩 Assess 🟥 Prevent 🟨 Detect 🟦 Data Driven Security

Open Season for Attacks on Hardware, Firmware and Supply Chain

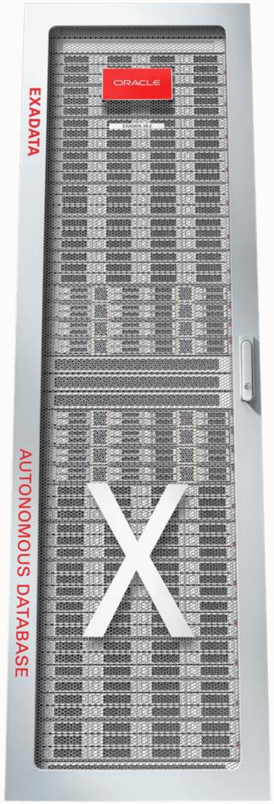
- Securing application and network perimeter is no longer sufficient
- Attacks are more sophisticated and getting deeper into the hardware
- Environments are more complex and distributed
- Server subcomponents are more capable but “soft”
  - More interesting to hackers
  - More potential for vulnerabilities and exploits
- Supply chains are at risk

Security Through-Out The Supply Chain

- Oracle supply chain is closely integrated and monitored
  - Oracle ownership of core Hardware and Firmware IP
  - Security audit for all design releases
  - Suppliers understand and adhere to Oracle security policies
  - Encrypted transmission of design data
  - Oracle controlled systems qualification tests and validation
  - All firmware and software is digitally signed and certified
  - Secure Trade Agreements Act (TAA) compliant manufacturing for system integration

Exadata 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

Exadata Development Focus

Security Optimized

✓ Optimize the installation by removing access to features that do not accomplish Exadata’s primary purpose

✓ Restrict access to features when not required

Security Focused

✓ Disable all unnecessary and insecure services unless required for system functionality

✓ Modify resulting services to run with lowest privileges

Security Hardened

✓ Conduct regular, extensive security scans across the entire stack using industry leading security scanners

✓ Integrate security fixes into each release and provide emergency fixes to address zero-day vulnerabilities

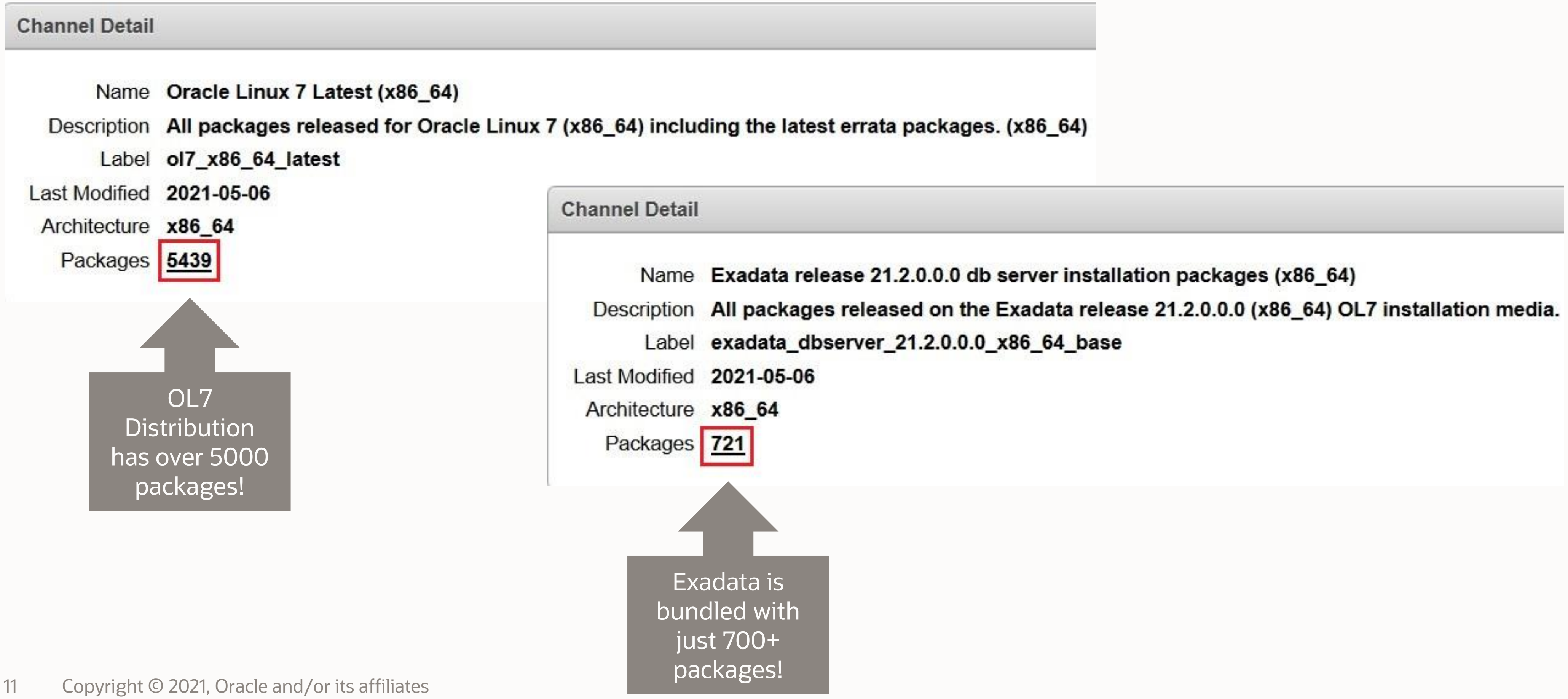
“The Oracle Autonomous Database, which completely automates provisioning, management, tuning, and upgrade processes of database instances without any downtime, not just **substantially increases security and compliance of sensitive data stored in Oracle Databases** but makes a compelling argument for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

KuppingerCole Analysts

Small Installation Footprint

Security: Optimized

Exadata **reduces the attack surface** by only including the software components required specifically to run the Oracle database (e.g. minimum Linux distribution)



Channel Detail

Name	Oracle Linux 7 Latest (x86_64)
Description	All packages released for Oracle Linux 7 (x86_64) including the latest errata packages. (x86_64)
Label	ol7_x86_64_latest
Last Modified	2021-05-06
Architecture	x86_64
Packages	5439

OL7 Distribution has over 5000 packages!

Channel Detail

Name	Exadata release 21.2.0.0.0 db server installation packages (x86_64)
Description	All packages released on the Exadata release 21.2.0.0.0 (x86_64) OL7 installation media.
Label	exadata_dbserver_21.2.0.0.0_x86_64_base
Last Modified	2021-05-06
Architecture	x86_64
Packages	721

Exadata is bundled with just 700+ packages!

Nano Linux Kernel Installation

Security: Optimized

Exadata uses a custom, nano (micro) kernel with removed dependencies that reduce size and features that are not needed in an enterprise data center.

- Fewer device drivers
- Smaller footprint
- Improved upgrade time

Standard kernel for OL7:
kernel-3.10.0-1127.13.1.el7.x86_64

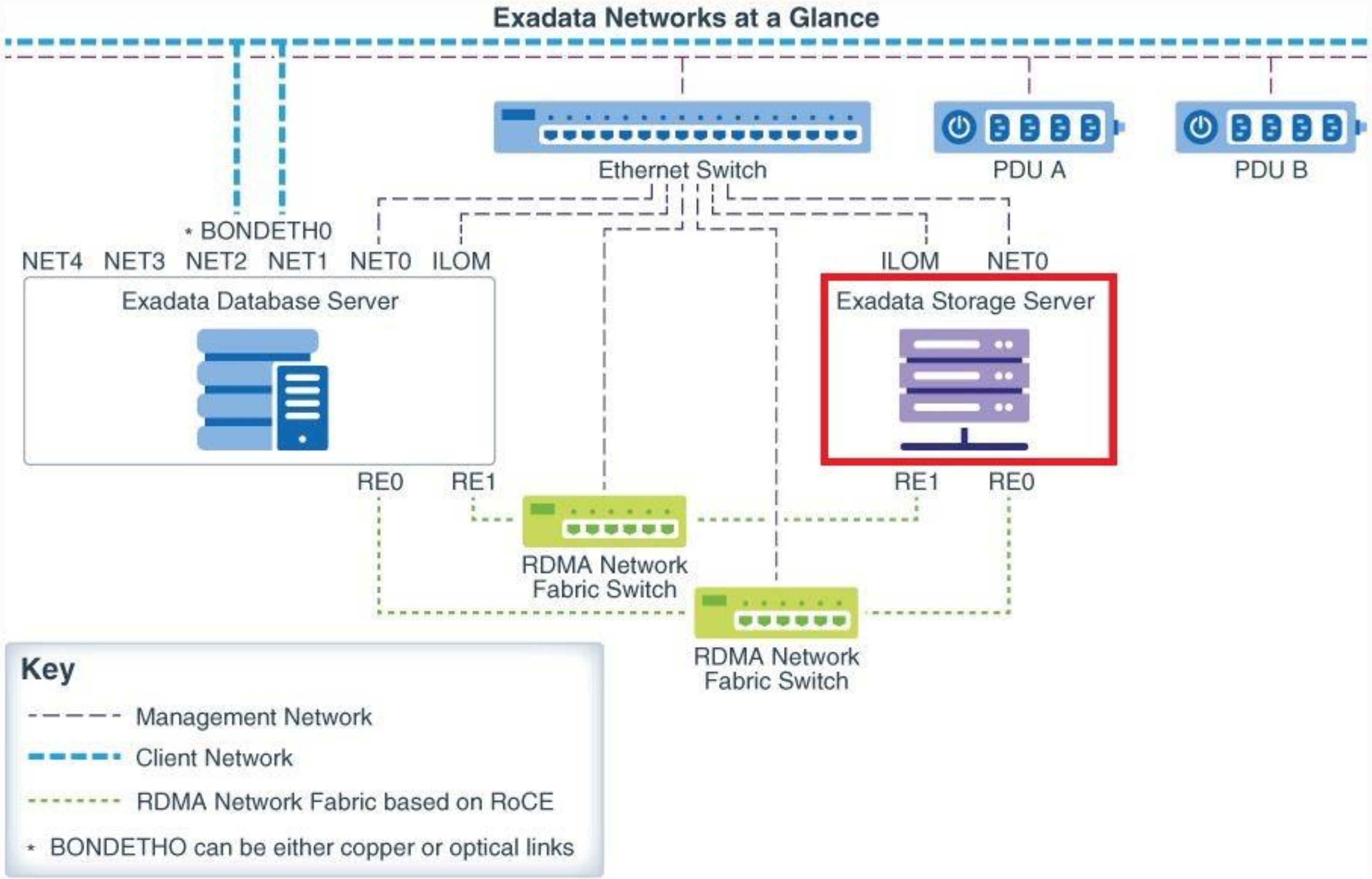
- DomU kernel size 167MB

Exadata kernel (21.2.0.0.0):
kernel-ueknano-4.14.35-2047.502.5.el7uek.x86_64

- DomU kernel size 38MB

Network Access to Storage Servers

Security: Optimized


Exadata Networks at a Glance
Ethernet Switch
PDU A
PDU B
* BONDETH0
NET4
NET3
NET2
NET1
NET0
ILOM
Exadata Database Server
ILOM
NET0
Exadata Storage Server
RE0
RE1
RE1
RE0
RDMA Network Fabric Switch
RDMA Network Fabric Switch
Key
Management Network
Client Network
RDMA Network Fabric based on RoCE
* BONDETH0 can be either copper or optical links

- 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

No Unnecessary Services - Implement Principle of Least Privilege

Security: Focused

Unnecessary insecure services such as telnet, ftp are disabled in the system

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

Access Control For RESTful Service

Security: Focused

Oracle Exadata System Software release 19.1.0 introduces a new capability for users to configure access control lists on the HTTPs access to the RESTful service

- 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
- Applies to both Oracle Exadata Database and Storage Server

```
# 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
```

Operating System Activity Monitoring

Security-Focused

- Each Exadata server is configured with auditd to audit system-level activity
- manage audits and generate reports use the auditctl command.
- Exadata specific audit rules are stored in the **/etc/audit/rules.d/01-exadata_audit.rules** file

```
[root@vm01 ~]# auditctl -l
-a always,exit -F arch=b32 -S
chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat
,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S
chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat
,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=access
-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)

Security-Focused

- 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

Resecure Machine

Security-Hardened

- Implement the available features and security plan at deployment via OEDA
  - password complexity requirements are added
  - passwords are expired
  - password aging implemented
  - permissions tightened

host_access_control – system settings

Security-Hardened

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 5
- Account lock_time after one failed login attempt set to 600
- Password history (pam_unix remember) set to 10
- 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
- **get-runtime - Maintenance command: import system configuration settings, storing them in host_access_control parameter settings files.**
  - **Important for users that modify system parameters outside of host_access_control**

Pre-scanned full stack

Security-Hardened

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
  - How to research Common Vulnerabilities and Exposures (CVE) for Exadata packages (Doc ID 2256887.1)
- System hardening reviews (STIG)
  - Exadata OL7 System Hardening for STIG Security Compliance (Doc ID 2614471.1)

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

- Number of issues reported should be much less compared to a custom configuration

Exadata Releases CY2021

Security: Hardened

Monthly Exadata Security Software Updates:

- Security fixes
- CVE mitigations

JAN	**20.1.6** **19.3.16** **19.2.22** **18.1.32**	**APR**	**20.1.9** **19.3.19** **18.1.33**	**JUL**	**21.2.2** **20.1.12** **19.3.20** **18.1.34**	**OCT**	**21.2.5** **20.1.15**
FEB	20.1.7 19.3.17	MAY	21.2.0 20.1.10	AUG	21.2.3 20.1.13	NOV	21.2.6 20.1.16
MAR	20.1.8 19.3.18	JUN	21.2.1 20.1.11	SEP	21.2.4 20.1.14	DEC	21.2.7 20.1.17

- *Future releases and dates are estimates only*

18,353

Common Vulnerabilities and Exposures (CVE) IDs issued in 2020 alone *across the international IT marketplace*.

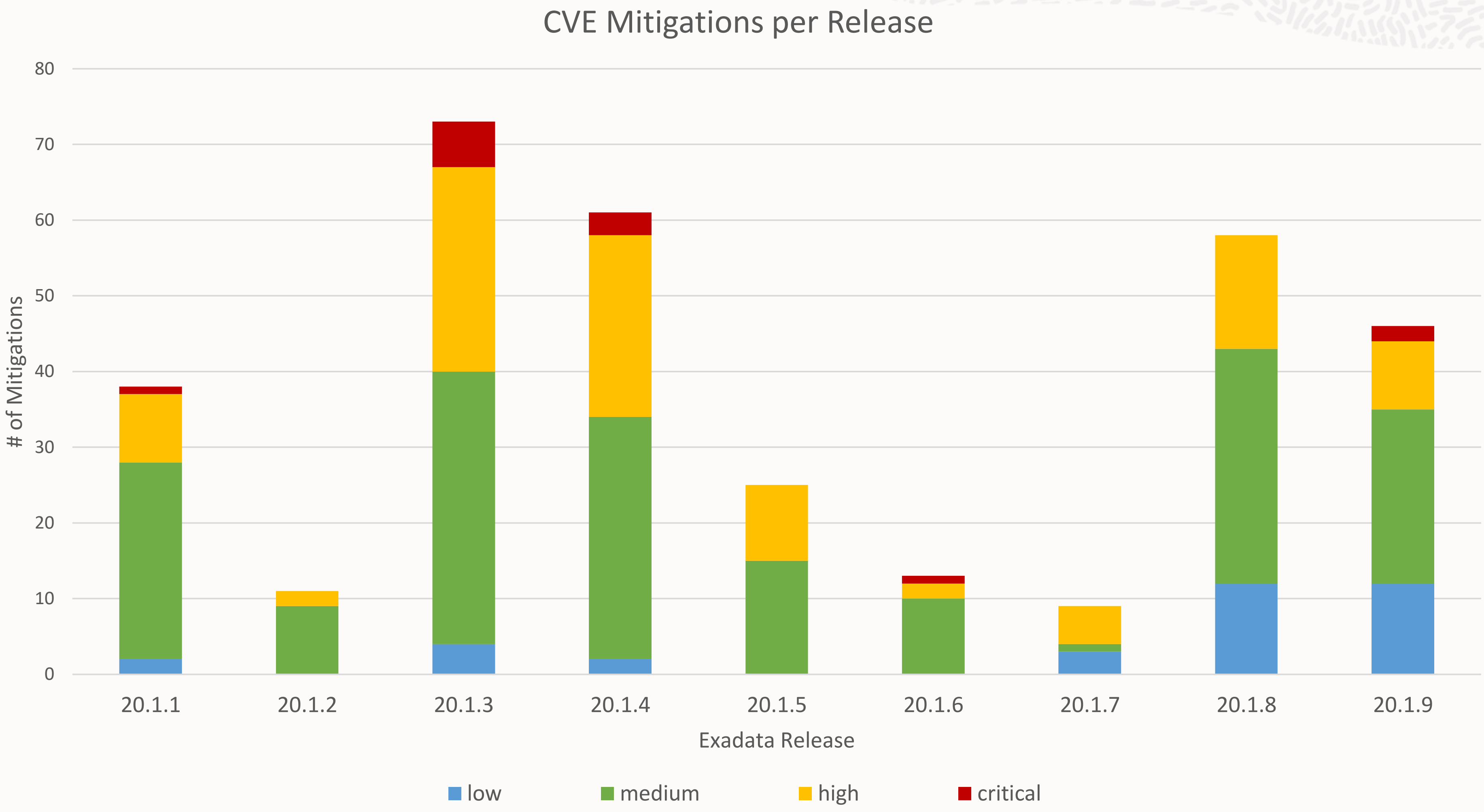
That’s 50 per day!

Exadata Security Value Add:

- Scanned images
- Monthly releases

Oracle Linux CVE Mitigations for Exadata 20.1.x

Security-Hardened



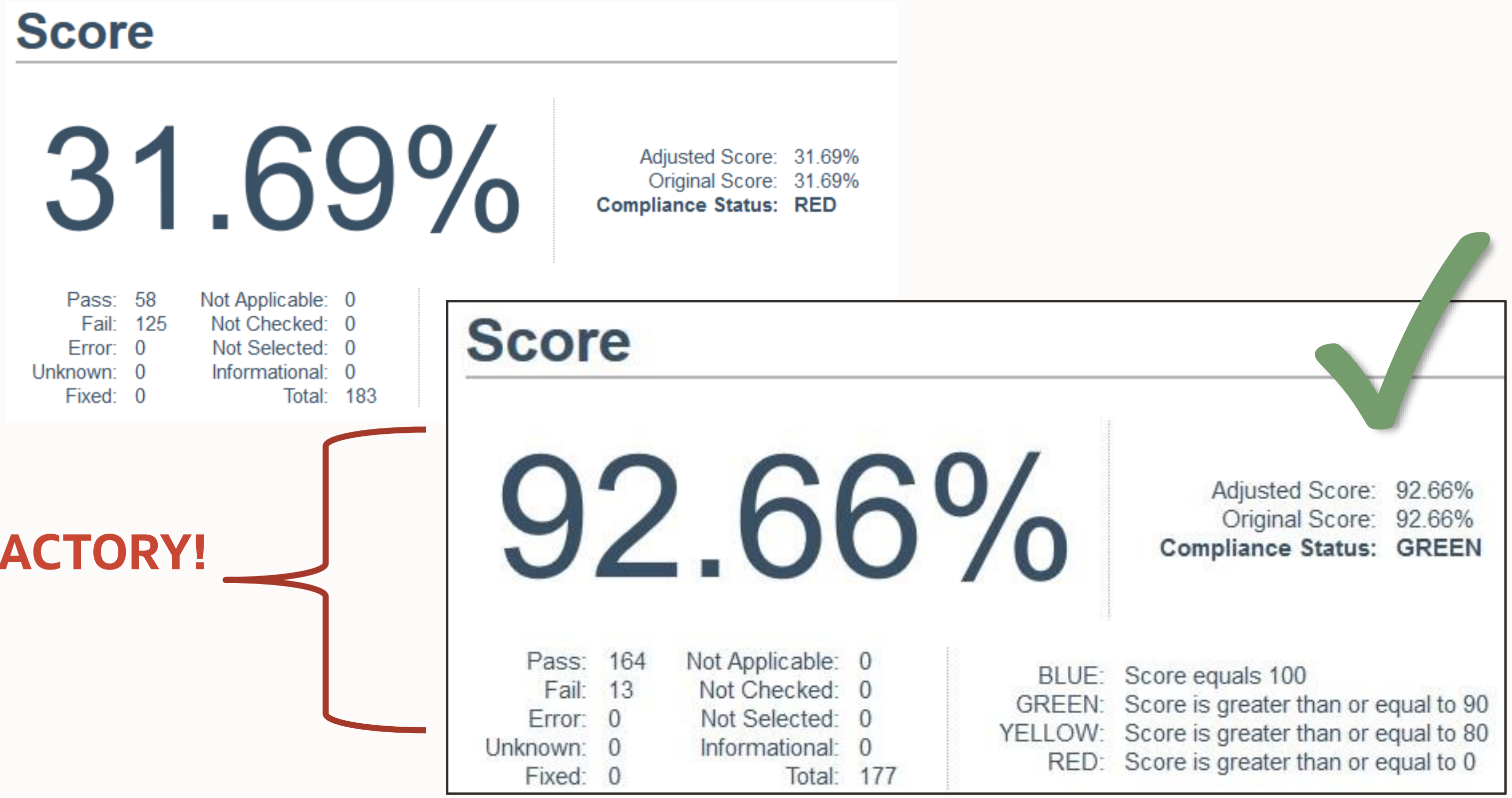
Secure from Factory – Oracle Linux 7 STIG SCAP Benchmark DomU on 21.2.0.0.0 X8M

Security: Hardened

"The Oracle Linux 7 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of the Department of Defense (DoD) information systems"

Generic Linux installation

Delivered straight from the FACTORY!



Score

31.69%

Adjusted Score:	31.69%
Original Score:	31.69%
Compliance Status:	**RED**

Pass:	58	Not Applicable:	0
Fail:	125	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Informational:	0
Fixed:	0	Total:	183

Score

92.66%

Adjusted Score:	92.66%
Original Score:	92.66%
Compliance Status:	**GREEN**

Pass:	164	Not Applicable:	0
Fail:	13	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Informational:	0
Fixed:	0	Total:	177

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

New (and existing) Security Features in Exadata

Maximize Security, Maximize Performance, Maximum Availability

Security Enabled Linux (SELinux)

Feature Available in Exadata Software 21.2 onwards

- 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.
- The system should first be placed in permissive mode to see if any Access Vector Cache (AVC) denials would need to be addressed BEFORE going to enforcing mode.

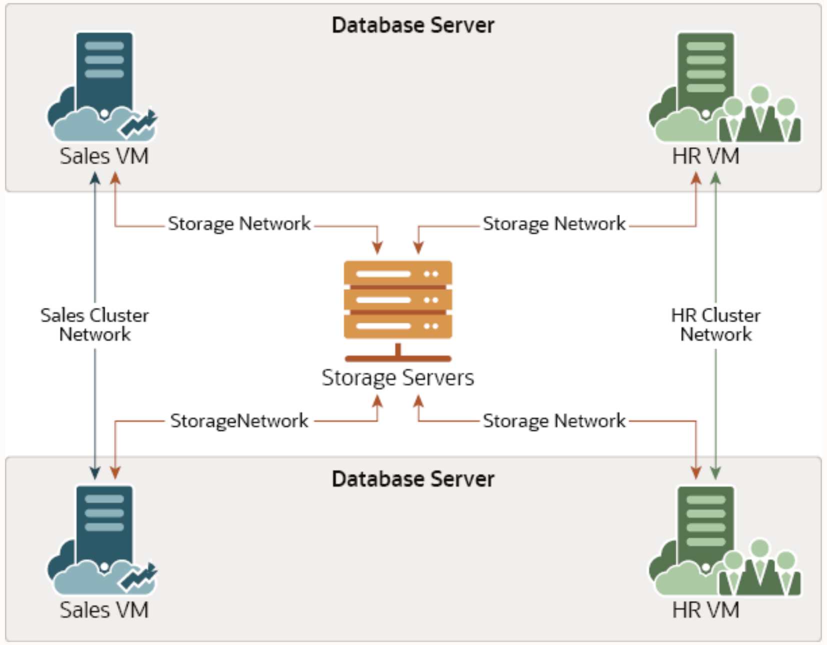
```
/opt/oracle.cellos/host_access_control selinux --help
Options:
  -h, --help          show this help message and exit
  -e, --enforcing     set the SELinux state to enforcing
  -p, --permissive    set the SELinux state to permissive
  -d, --disabled      set the SELinux state to disabled (Exadata default)
  -r, --relabel       Set the system for relabling
  -c, --config        Display the configured SELinux state
  -s, --status        Display the current SELinux status
```

Exadata Secure RDMA Fabric Isolation for RoCE

Feature Available in Exadata Software 20.1 onwards

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



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

Feature Available in Exadata Software 20.1 onwards

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

- *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

- 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.

Management Server App Engine Update

New in Exadata Software 20.1

Exadata 20.1 - Eclipse Jetty

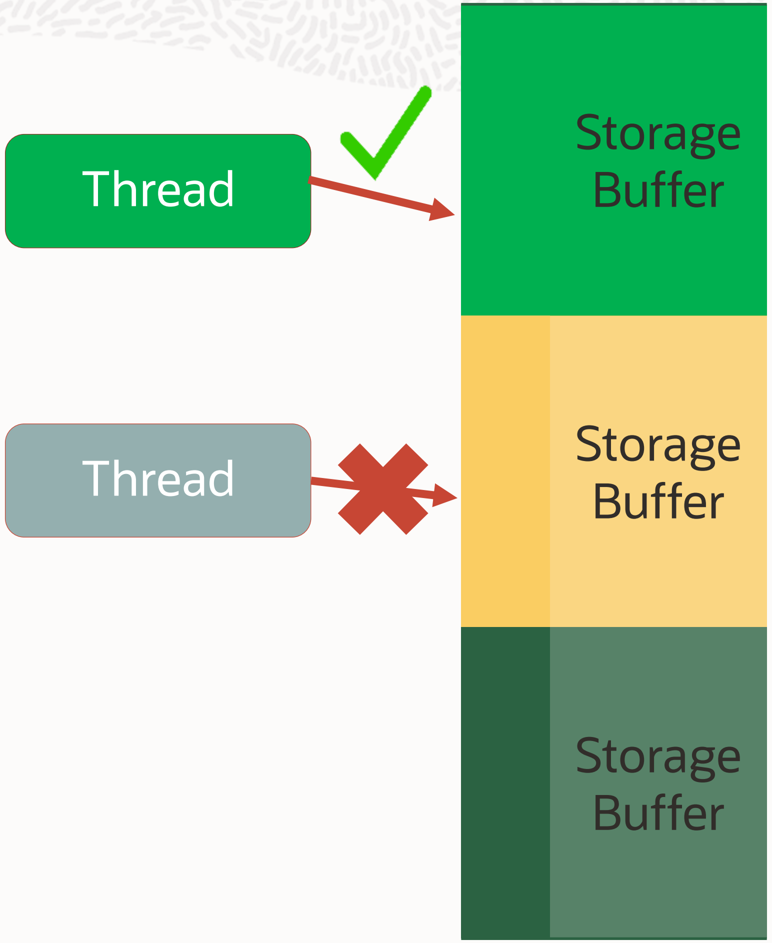
- Light-weight web server
- Consumes considerably fewer system resources
- Basic functionalities supported, extensible modules
- Fewer CVE vulnerabilities – smaller attack vectors
- Does not require a dedicated HTTP port for configuration purposes

Securing Storage Server Processes with Memory Protection Keys

Introduced in Exadata 19.3 for X7 and newer

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 Processes 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
- White-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

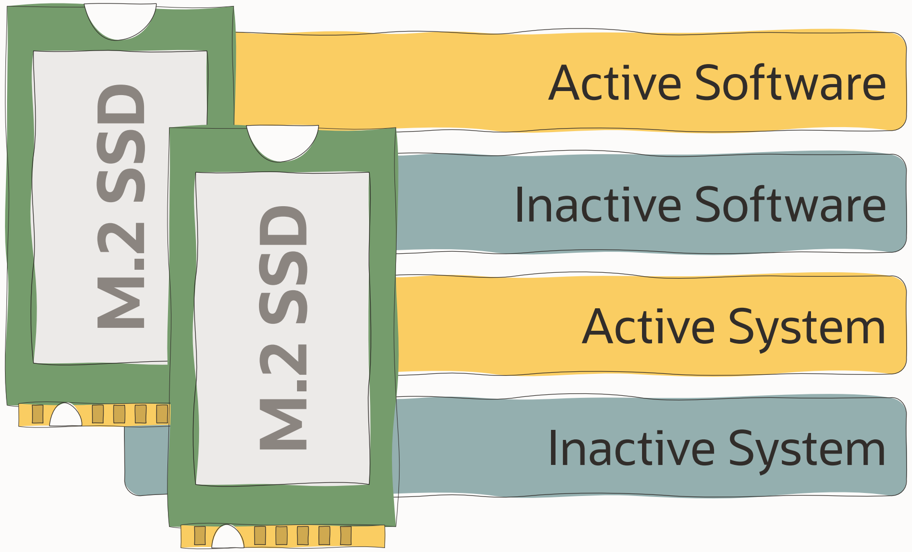
Exadata installs the system/software on alternating partitions

- e.g. 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



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.

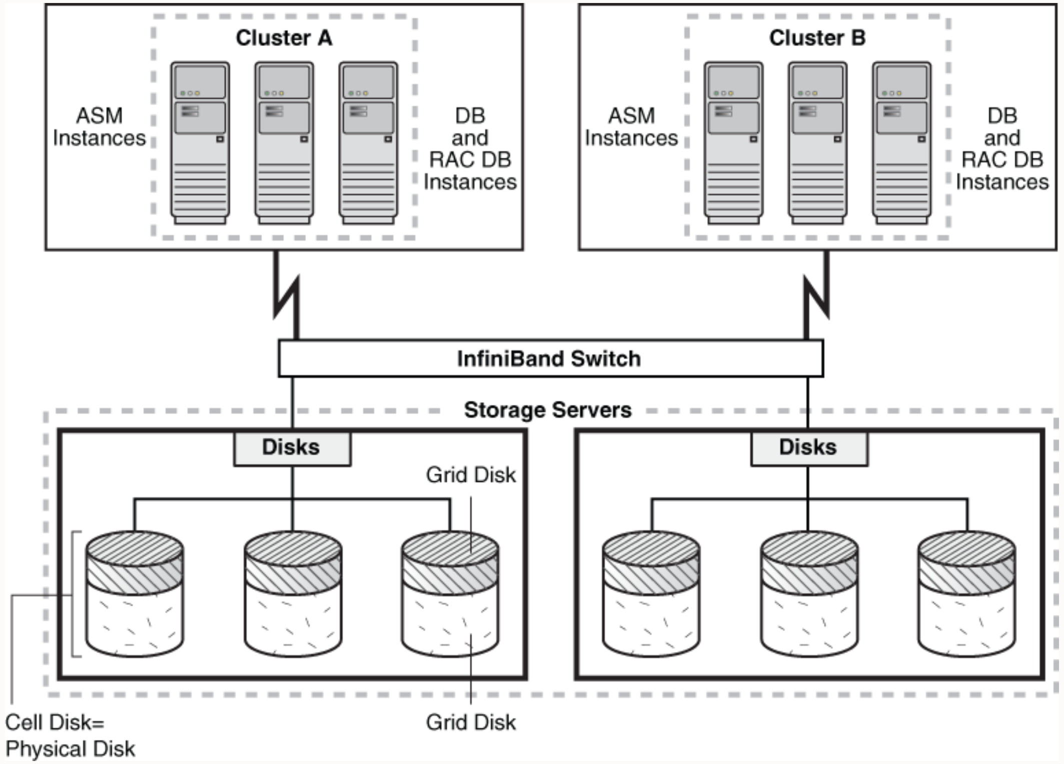
```
# /opt/oracle.SupportTools/exadataAIDE -status
AIDE: daily cron is currently enabled.

To add additional rules:
Edit the file /etc/aide.conf

Update the AIDE database metadata.
# /opt/oracle.SupportTools/exadataAIDE -u
```

Database and Storage Server Secure Boot

- 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

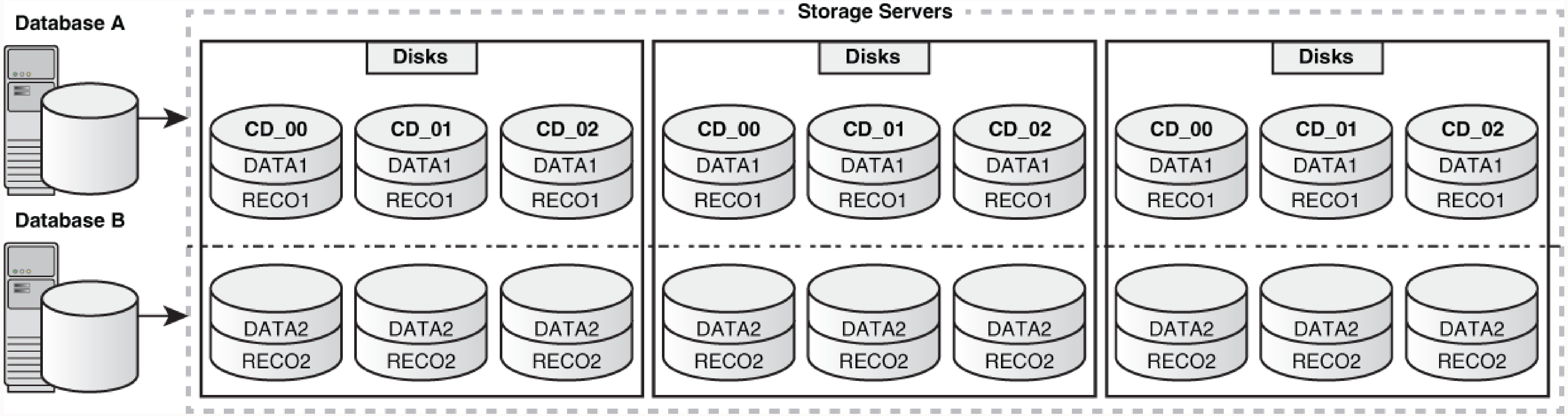
ASM-Scoped Security

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



DB-Scoped Security

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



NTT WEST

"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 must be used to actually create the secure environment

Secure Eraser

- Provide a secure erasure 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	Erasure Method
Hard drive	• 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

Security References

Oracle Exadata Database Machine Security FAQ

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

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/

Oracle Exadata Documentation

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

Thank You!

Security MAA Team

Exadata Product Development
Oracle Corporation

ORACLE