IDC

ORACLE CLOUD INFRASTRUCTURE: Addressing Tenant Concerns with Deep Application Insights

RESEARCH BY:

Jay Bretzmann
Program Director,
Security Products, IDC

Philip Bues
Research Manager, Cloud Security, IDC

May 2022 | IDC Doc. #US49017122

Navigating this Lab Validation Brief

Click on titles or page numbers to navigate to each section.

Executive Summary

Public cloud infrastructure providers face some unique security challenges as they virtually allocate cloud tenant resources across hundreds to thousands of clients. They're a big target worthy of extensive malware engineering designed to compromise the whole environment. Organizations were originally reluctant to migrate applications to the cloud because they didn't understand the capabilities in place to protect their data from attackers or even simple mistakes made by other tenants.

An industrywide shared infrastructure model was defined, delineating what providers and tenants must each responsibly secure. Providers have subsequently developed capabilities and tools to help prospective tenants lift, shift, monitor, and adjust application deployments often augmented by machine learning insights. **Many adopters now believe public clouds are more secure than previous on-premises environments;** tenants benefit from savings opportunities and the ready availability of integrated tools and professional security services and resources.

This second IDC Lab Validation effort further reviews the Oracle Cloud Infrastructure (OCI), highlighting security measures available to tenants, specifically threat management, cryptographic services, and risk management capabilities.

Lab Validation

This Lab Validation effort reviews the Oracle Cloud Infrastructure (OCI) and highlights security measures that make it easier to encrypt, detect, and defend against emerging threats and to monitor security violations in Oracle owned and non-owned cloud infrastructure and software-as-a-service (SaaS) applications. Its security is "always on" by default approach, with management tools, baseline templates, policy recipes, and data-at-rest encryption.

These cloud security tools (often free) are another advantage OCI gives its customers because Oracle has defined a cloud environment where tenancies are secured, and isolated partitions are administered with limited visibility, even to OCI. This integrated and prescriptive security approach is unique.

LEVEL 4: **Threat Management**

- **FEATURE 1:** Oracle Cloud Guard Threat Detector
- **FEATURE 2:** Oracle Threat Intelligence (TI) Service
- **FEATURE 3:** OCI Web Application Firewall (WAF)

LEVEL 5: **Cryptography and Certificate Management**

- **FEATURE 4:** OCI Vault
- **FEATURE 5:** OCI Certificates

LEVEL 6: **Risk Management**

- **FEATURE 6:** OCI Vulnerability Scanning Service (VSS)
- **FEATURE 7:** Oracle Cloud Guard SaaS Fusion Apps Detector

Oracle Cloud Infrastructure (OCI) Security Validation Test Plan

LEVEL 4: **Threat Management**	Oracle Cloud Guard Threat Detector (free)	• Configure new Threat Detector recipes and validate impacted resources. • Generate security recommendations and remediate or dismiss.
	Oracle Threat Intelligence Service (free)	• Show Threat Intelligence back end with overall score, context, and feed source. • Review overall confidence score and mark as false positive if appropriate.
	OCI Web Application Firewall (free, paid)	• Select and configure access control, rate limiting, and protections. • Show WAF Activity Overview dashboard and review health, capacity, and performance of rules.
LEVEL 5: **Cryptography and Certificate Management**	OCI Vault (free, paid)	• Vault creation and replication use dedicated (physical) or shared (virtual) OCI HSMs and a bring-your-own-key option for external HSMs. • Key and secret creation, rotation, and deletion procedures use HSM (FIPS 140-3) or software (FIPS 140-1) encryption options.
	OCI Certificates (free)	• Build private certificate authorities and CA hierarchies for generating network TLS certificates inside OCI. • Bound certificate lifespans, monitor their renewal, and identify conditions required for revocation.
LEVEL 6: **Risk Management**	OCI Vulnerability Scanning Service (free)	• Navigate to scanning/scan recipes; select compute or container image. • Verify scanning report, vulnerability report, and metrics.
	Oracle Cloud Guard SaaS Fusion Apps Detector (free)	• Select preconfigured or customizable recipes. • Register HCM/ERP Fusion Apps within Cloud Guard and set up target creation flow.

Validation Test Bed

IDC validated the conditions as presented over five web sessions. The control criteria are defined below. Analyst requests for visual confirmations of successful operations varied by feature, with no “embedded” functions limited to command-line execution.

1 Threat Management	2 Cryptography and Certificate Management	3 Risk Management
BENEFITS / USER OUTCOMES		
• Security recommendations and insights provided by OCI and machine learning • Out-of-the-box integrations • WAF scalability across hybrid and multicloud environments • Time to value • Easy recipes to configure and activate	• Managed service, multitenant, and single-tenant separate vault solutions • Infrastructure or integration for sharing master keys within vaults • Three-level key management operations (vault, key/secret, key version) • Private certificate authority (CA) services	• Preconfigured and customizable recipes • Quick identification of risks in detector and image results • Consolidated view across IaaS and SaaS applications • Monitored and protected compartments beyond OCI
FEATURES TO BE TESTED		
• Prioritized alerts based on risk scoring and confidence assessments • Unified console visibility • Threat models based on MITRE ATT&CK techniques • CrowdStrike telemetry integration	• Vault and master key creation (Oracle Cloud ID) and key versioning for creation/rotation/deletion • Key sharing across databases, data, secrets/passwords, certificates, and blobs • Convenience and control for generating up to 100 private CAs with 10 levels of depth • User interface experiences	• Configurable “immutable” monitoring regions • Scan reports showing metrics, open ports, vulnerabilities • Unique data masking rules • Cloud Guard integrations

Notes: Lab sessions occurred December 7, 2021; January 12, 13, 27, and February 2, 2022. The sessions were viewed remotely via Zoom. Lab sessions were prefaced by a general discussion of the material to be viewed followed by a detailed demo. Each observed lab session ran approximately 60 minutes. Analysts were free to ask questions, confirm what they saw, propose alternate scenarios, and challenge assumptions. Road maps and future enhancements confirmed Oracle understood future requirements.

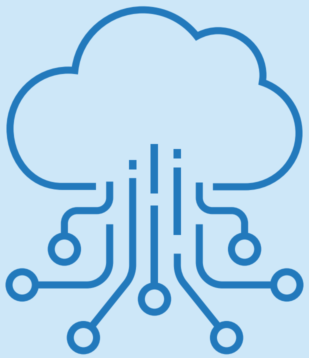
FEATURE 1

LEVEL 4: **Threat Management**

Oracle Cloud Guard Threat Detector

BENEFITS/FEATURES:

- Recipes provide tenants with best practices templates, reducing the configuration burden for new deployments or integrations.
- Continuous monitoring for malicious activities (insider threats, logs, and profiling anomalies) surfaces issues in near real time.
- Behavioral targeted machine learning modeling (aligned with MITRE ATT&CK Framework) and cross-referenced attack progression risk scoring reduces false alert fatigue while preserving security team bandwidth.
- Integration with Oracle Threat Intelligence Service.



As false positives proliferate and vulnerability fatigue sets in, OCI delivers detection, response, and threat intelligence as part of a modern multilayered defense.

FEATURE 1 VALIDATED

Oracle Cloud Guard Threat Detector

Lab Validated
IDC | 2022

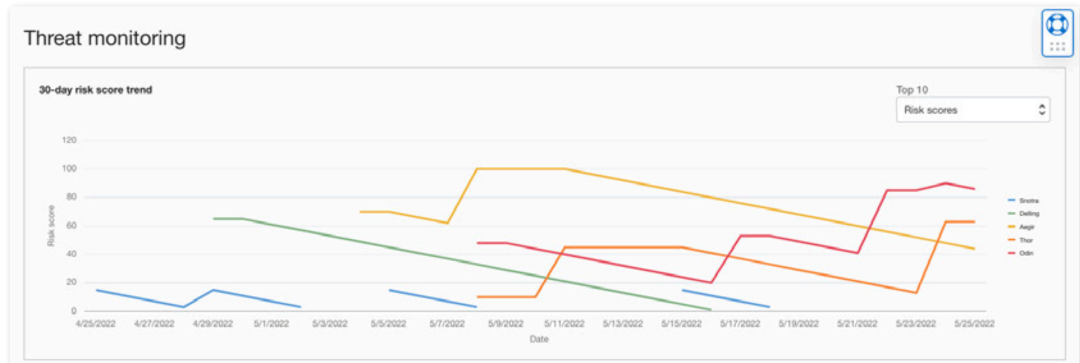
OBJECTIVE:

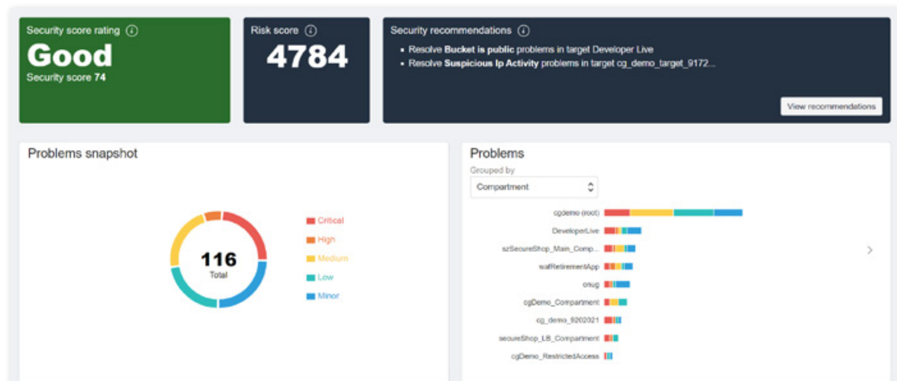
Detect and remediate malicious behavior patterns

VALIDATION PROCESS:

1. Apply Threat Detector recipe to the root target.
2. Apply responder recipe for automated remediation if desired.
3. Monitor evolving threats using 30-day risk score trend.
4. Monitor for "Rogue User" problems for users with a risk score above 80.
5. Validate impacted resources and blast radius with sighting details.
6. Develop and distribute security recommendations.
7. Remediate and mark as resolved or dismiss.

PROOF:





FEATURE 2

LEVEL 4: **Threat Management**

Oracle Threat Intelligence (TI) Service

BENEFITS/FEATURES:

- Indicator correlation spanning Oracle security expertise, CrowdStrike, open source, and honey pot network telemetry yields a transparent, single, high-confidence feed pushed to tenants.
- Out-of-the-box integrations activate TI for Cloud Guard and Threat Detector.
- If Identity, Load Balancer, and WAF are enabled, security operations center (SOC) teams can realize the full benefit of prioritized alerts.

FEATURE 2 VALIDATED

Lab Validated
IDC | 2022

Oracle Threat Intelligence (TI) Service

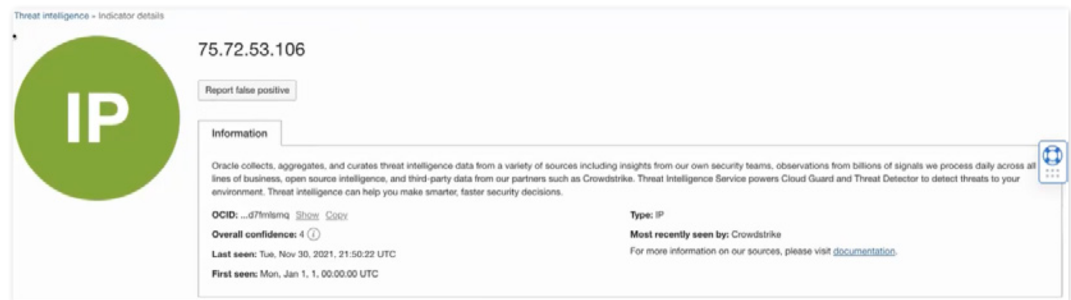
OBJECTIVE:

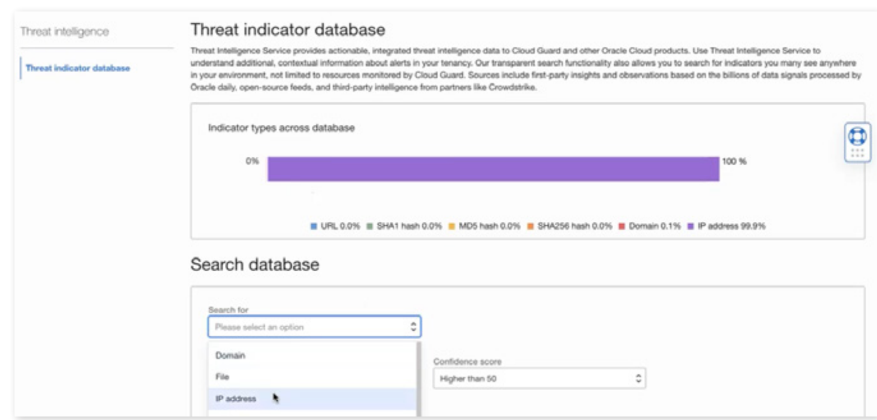
Aggregate and curate actionable vendor-agnostic threat intelligence telemetry and response

VALIDATION PROCESS:

1. Launch Cloud Guard or Threat Detector recipe directly.
2. Apply Cloud Guard activity and Threat Detector recipes to target.
3. Show Threat Intelligence back end with impacted resources, sighting score, recommendations, and feed source.
4. Review impacted endpoints within suspicious IP activity problems and threat detection problems.
5. Show Threat Intelligence indicator detail page for contextual information about suspicious endpoint, overall confidence score, indicator history, and feed source.

PROOF:





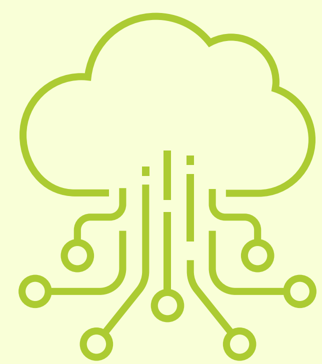
FEATURE 3

LEVEL 5: **Cryptography and Certificate Management**

OCI Web Application Firewall (WAF)

BENEFITS/FEATURES:

- OCI WAF protects against code injection, OWASP Top 10 threats, and common vulnerabilities and exposures (CVEs).
- Once a threat is detected, OCI WAF can drop malicious traffic, apply virtual patching for vulnerabilities, insert additional challenges or corrective actions such as limiting access to the application based on geography, or provide alerts and logging.
- Support covers four critical feature categories: protection rules, access control, bot management, and rate limiting.
- OCI WAF Team actively researches and monitors for new threats and vulnerabilities.
- Freemium service provides the first instance and up to 10 million requests per month. Afterwards, each additional instance is $5 per month and requests at $0.60 per million.



Hybrid and multicloud solutions have to be flexible and scalable. OCI WAF security differentiates by protecting applications hosted anywhere within reach, not just OCI.

FEATURE 3 VALIDATED

Lab Validated IDC | 2022

OCI Web Application Firewall (WAF)

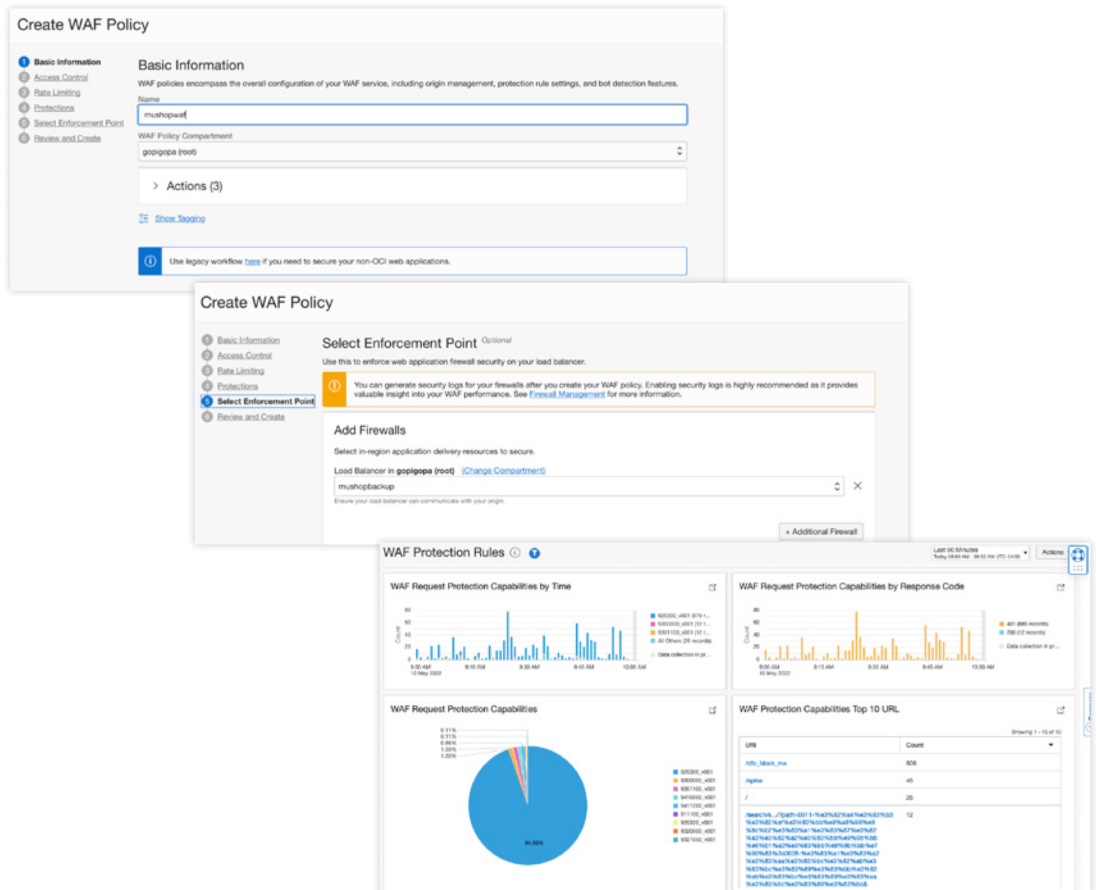
OBJECTIVE:

Provide end-to-end internet-facing and internal protection for web applications and API endpoints at the edge and in region; defend against all Layer 7 malicious traffic and insider threats

VALIDATION PROCESS:

1. Create WAF policy rule.
2. Select and configure access control, rate limiting, and protections.
3. Select enforcement point.
4. Review and create policy configuration.
5. Show WAF Activity Overview dashboard and review health, capacity, and performance of rules.

PROOF:



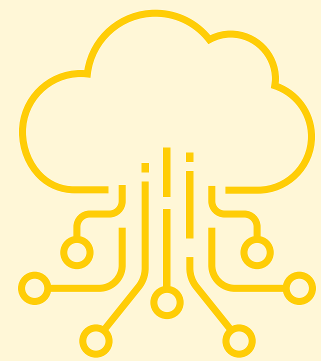
FEATURE 4

LEVEL 5: **Cryptography and Certificate Management**

OCI Vault

BENEFITS/FEATURES:

- Fully managed service option offers default data-at-rest encryption for applications.
- Organizations with limited cryptography experience can offload symmetric/asymmetric encryption key creation and management responsibilities.
- Flexibility allows organizations to control their key management operations per industry requirements using OCI multi- and single-tenant HSM partitions. Alternatively, bring your own HSM key (BYOK).
- Key proliferation is reduced by permitting use of generated keys across multiple encryption use cases.



This is cryptoprocessing that few organizations understand. An estimated 80% of tenants leave the driving to OCI, choosing to focus instead on SaaS application management.

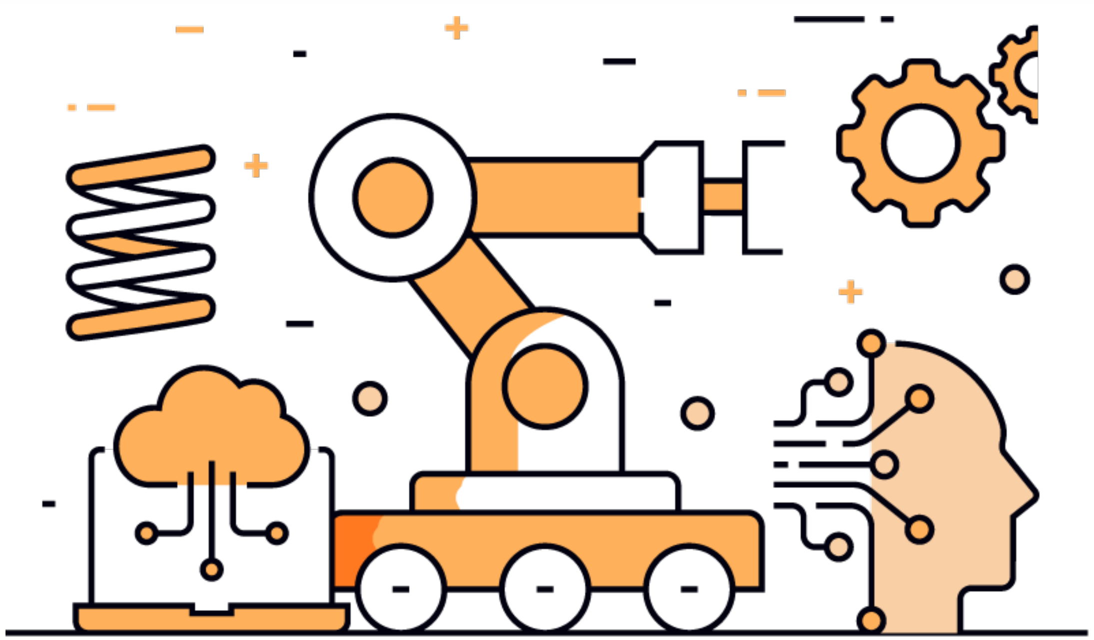
FEATURE 5

LEVEL 5: **Cryptography and Certificate Management**

OCI Certificates

BENEFITS/FEATURES:

- Flexible private certificate authority (CA) hierarchies enable tenants to create and manage their TLS certificates automatically.
- Automation capabilities and a simplified user interface deliver a "set it and forget it" experience.



FEATURE 4 VALIDATED FEATURE 5 VALIDATED

Lab Validated
IDC | 2022

OCI Vault and OCI Certificates:
Key and Secrets Management, Private Certificate Authority Services

OBJECTIVE:

Help tenants establish and manage encryption services;
simplify the establishment of certificate-based communications

VALIDATION PROCESS:

1. Create an OCI Vault. Select managed service, multitenant, and single-tenant virtual private options.
2. Choose a vault type (HSM or software key protection), considering key exportability needs.
3. Add encryption keys by type (AES, RSA, ECDSA).
4. Import keys and wrap inside OCI.
5. Set key rotation parameters.
6. Share keys to protect data and secrets.
7. Delete keys and adjust ultimate deletion timelines.
8. Create a certificate authority.
9. Assign certificate attributes.
10. Review certificate status.

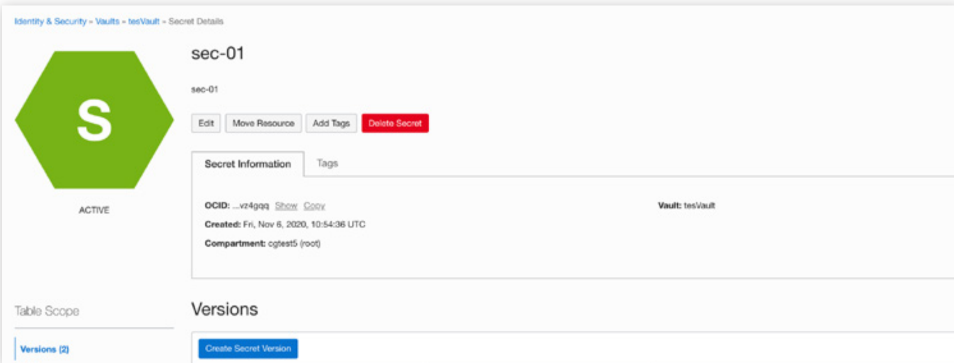
FEATURE 4 VALIDATED FEATURE 5 VALIDATED

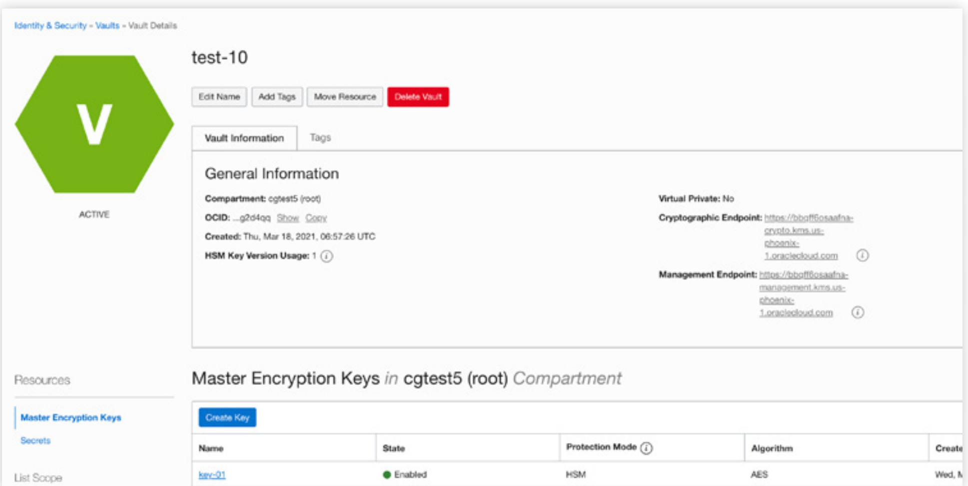
Lab Validated
IDC | 2022

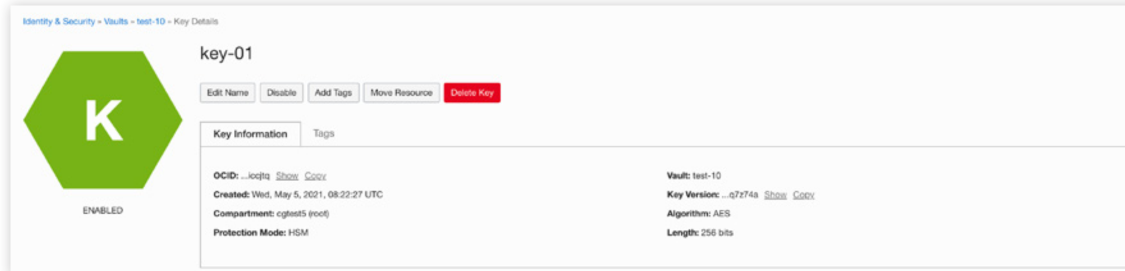
OCI Vault and OCI Certificates:

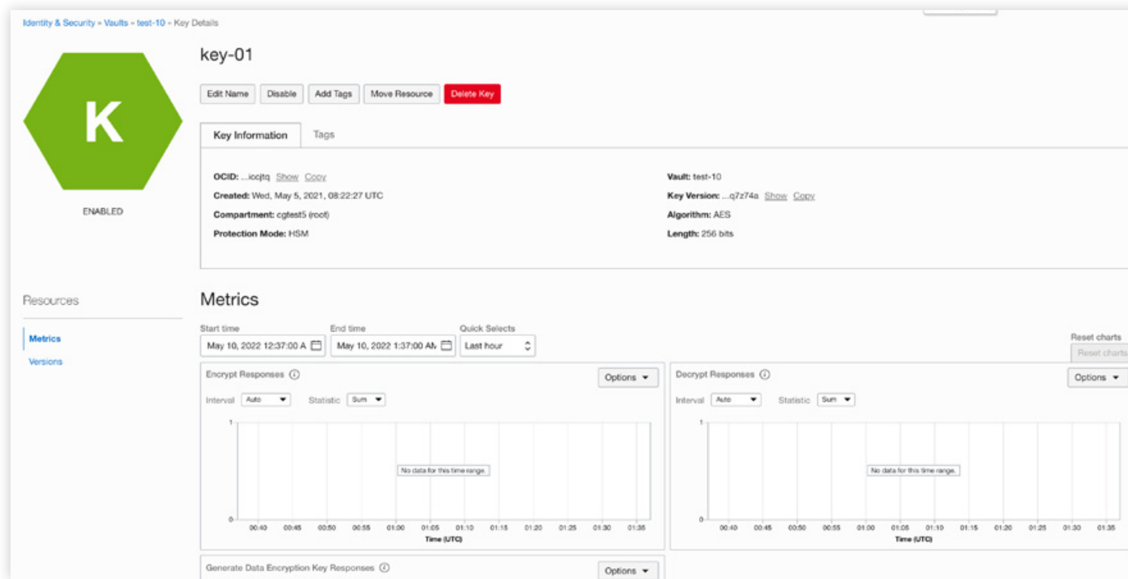
Key and Secrets Management, Private Certificate Authority Services

PROOF:









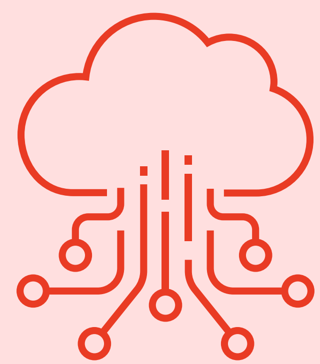
FEATURE 6

LEVEL 6: **Risk Management**

OCI Vulnerability Scanning Service (VSS)

BENEFITS/FEATURES:

- A simplified setup process covers both compute instances/VMs and container image scanning. Results are sent to OCI DB/UI, forwarded to event logging, and leveraged for other services.
- You can choose deployment-phase scanning, daily CVE checks, and automated rescanning of new images in any OCI container registry.
- Rules are applied to stop containers from running depending on CVE severity. Findings can be pushed out to OCI Cloud Guard or SIEM tools.
- Integration with major vulnerability management vendors enables ready-to-support multicloud vulnerability monitoring.
- Risks are made visible from a global reporting tool.



Risk management is as much about identifying vulnerabilities early as it is about saving users' time. VSS and Fusion Apps Detector provide a single view, indicate security issues, and flow into Cloud Guard for free.

FEATURE 6 VALIDATED

Lab Validated
IDC | 2022

OCI Vulnerability Scanning Service (VSS)

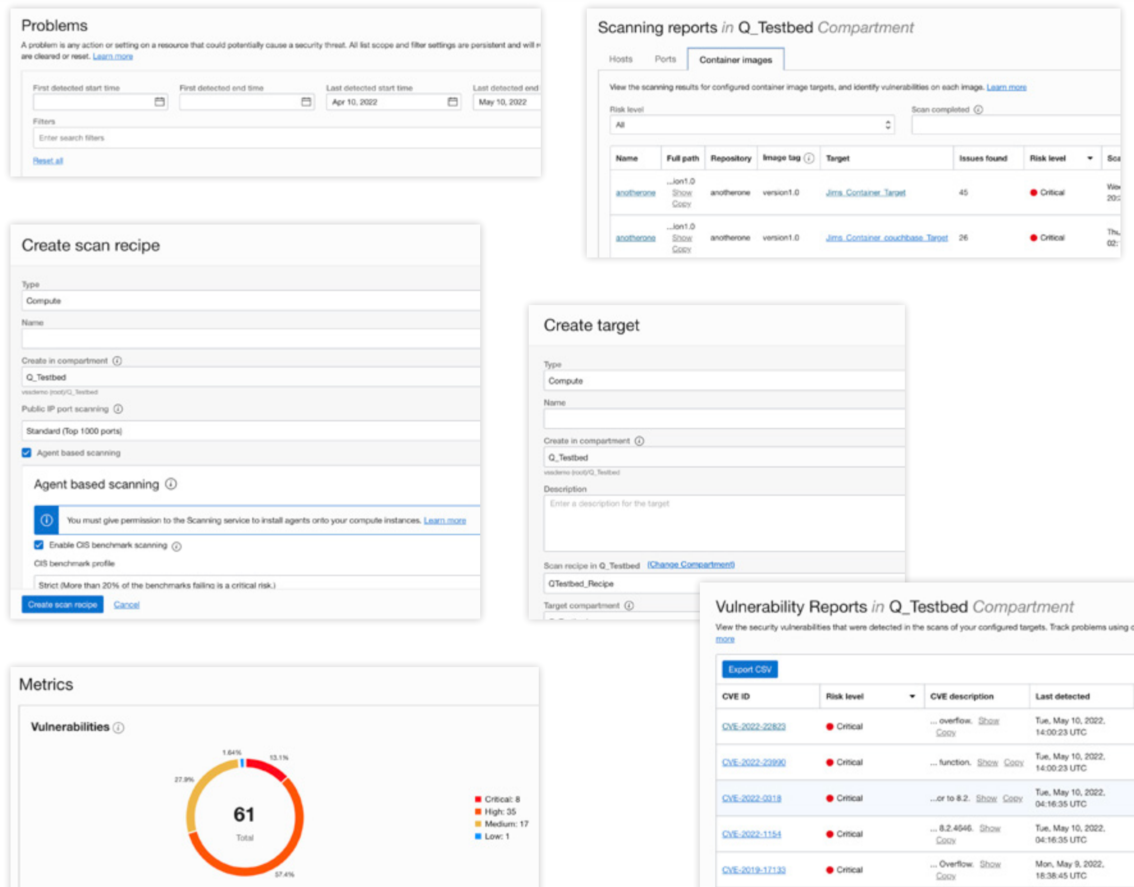
OBJECTIVE:

Identify vulnerabilities in dedicated compute instances and container images before they are exploited

VALIDATION PROCESS:

1. Establish required identity and access management policies.
2. Navigate to Scanning/Scan Recipes and select compute or container image.
3. Create scan recipe and choose light or standard public IP port scanning. Enable CIS benchmark profile and schedule scanning.
4. Create targets.
5. Scanning reports are available within one hour, showing metrics, open ports, vulnerabilities, and CIS benchmarks.
6. Reconfigure VSS recipes in Cloud Guard detectors if needed.

PROOF:



FEATURE 7

LEVEL 6: **Risk Management**

Oracle Cloud Guard SaaS Fusion Apps Detector

BENEFITS/FEATURES:

- Activities such as role provisioning, role management and sensitive object changes within Oracle Cloud HCM and Cloud ERP Fusion Applications are continuously monitored with out-of-the-box detectors or custom configurations.
- Limited visibility with sensitive object data masking is especially useful for HCM, ERP, or any time personally identifiable information or personal health information is exchanged.

FEATURE 7 VALIDATED

Lab Validated IDC | 2022

Oracle Cloud Guard SaaS Fusion Apps Detector

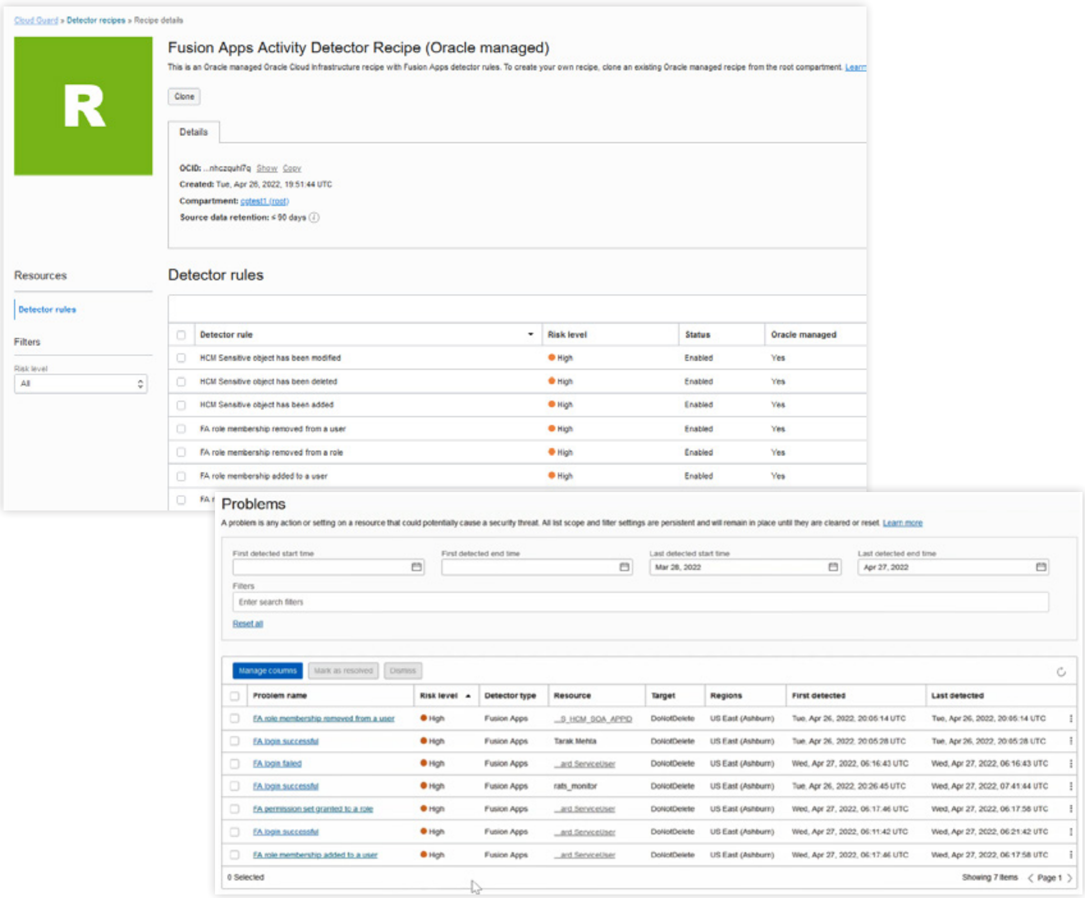
OBJECTIVE:

Monitor user activity around privileges, roles, and entitlements, akin to behavioral profile management

VALIDATION PROCESS:

1. Create target for Fusion Apps.
2. Establish user credentials for Cloud Guard integration.
3. Activate/add recipe. Configure monitoring region for data residency regulations.
4. Detect problems.
5. Review target details, including metrics.
6. Access advanced features, including unique data masking rules.

PROOF:



Key Findings

- Oracle-curated targeted threat models help OCI tenants spot malicious behaviors the SIEM and UEBA tools often miss, leaving attackers to dwell for months.
- Machine learning model works on regionally stored data that is correlated with global insights while reviewing active techniques and attacks to create better risk scores.
- Rogue user detector rule includes password guessing, password spraying, elevated number of PARs, impossible travel, and privilege escalation sightings to discover malicious activity.
- OCI has access to some audit logging resources across a large base of tenancies it can review for evidence of attackers trying to breach client environments but does not read any private data.
- OCI Vault offers the flexibility to serve the wide-ranging needs of tenants. It accommodates both crypto neophytes and experts in regulated and unregulated industries.
- Shared, private, and external HSM options balance savings with security, while OCI software facilitates key reuse across data, certificates, secrets, and other use cases.
- The OCI WAF security research (CSIRT) team actively monitors and discovers new vulnerabilities and releases virtual patches for many exposures within 24–48 hours. Other third-party vulnerabilities feeds, antivirus solutions, and suspicious IP address lists are all available at no charge.

IDC Opinion

IDC can validate the security technology applied to critical new components of OCI: monitoring and threat prevention, protection against anomalies and malicious behaviors, easy-to-use cryptographic technologies, and integrations for multicloud vulnerability management with ecosystem partners.

The nature of threat feeds, attack behaviors, indicators of compromise, and integrated telemetry feeds is that the work is never done. More policies, rules, and recipes are always needed to stay current. For a cloud service provider, the key part to get right is the framework for collecting all the data and the dashboards and single-pane-of-glass views that help security teams quickly spot the sightings.

With this second Lab Validation project, IDC believes OCI has tackled some of the harder elements of its IaaS solution, surrounded them with APIs, and done it in a very easy-to-consume and affordable manner for its customers.

About the Analysts

Jay Bretzmann
Program Director, Security Products, IDC

Jay Bretzmann is Program Director for IDC Security Products responsible for Identity & Digital Trust and Cloud Security. Jay focuses on identity management, privileged access management, identity governance, B2C identity management, and a multitude of other identity and cloud security topics.

More about Jay Bretzmann

Philip Bues
Research Manager, Cloud Security, IDC

Phil Bues is the Research Manager for IDC Cloud Security. In this role, Phil drives research, provides thought leadership and advises clients on complex issues including cybersecurity of the cloud and in the cloud. His commentary will address the benefits and challenges to what's been called the shared responsibility model and how that line may change going forward.

More about Philip Bues