IDC | ANALYZE THE FUTURE

ORACLE CLOUD INFRASTRUCTURE:

Putting Tenant Data Safety and Privacy First with Automated Operations

RESEARCH BY:

Jay Bretzmann
Program Director,
Security Products, IDC

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

October 2020 | IDC Doc. #US46883820

Navigating this Lab Validation Brief

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

Executive Summary

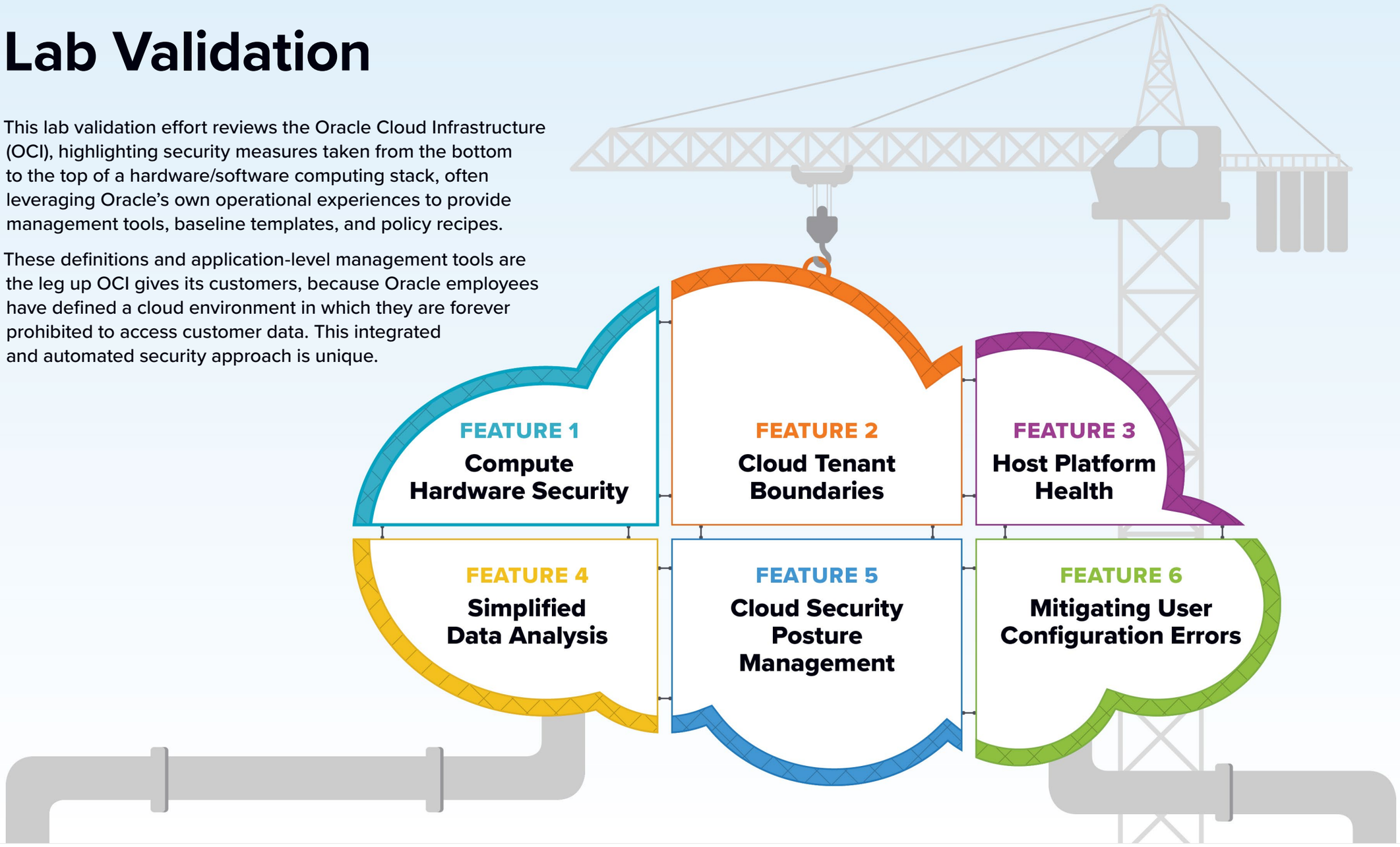
Public cloud infrastructure providers face some unique security challenges because of what they do: virtually allocate cloud tenant resources across hundreds or thousands of clients. They're a big target worthy of extensive malware engineering designed to compromise the whole environment. Organizations 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 just other tenants.

An industry shared infrastructure model developed, delineating what providers versus tenants must retain responsibility for securing. Providers have subsequently developed capabilities and tools that help prospective tenants lift, shift, monitor, and adjust, often augmented by machine learning insights. Many believe that public clouds are now more secure than on-premises environments, allowing organizations to benefit from savings opportunities and availability of professional security resources.

Lab Validation

This lab validation effort reviews the Oracle Cloud Infrastructure (OCI), highlighting security measures taken from the bottom to the top of a hardware/software computing stack, often leveraging Oracle's own operational experiences to provide management tools, baseline templates, and policy recipes.

These definitions and application-level management tools are the leg up OCI gives its customers, because Oracle employees have defined a cloud environment in which they are forever prohibited to access customer data. This integrated and automated security approach is unique.



Oracle Cloud Infrastructure (OCI) Security Validation Test Plan

LEVEL 1: **OCI Architecture**	**Root of Trust**	1. Create and delete firmware module within defined instance. 2. Command shell validation after resource reassignment.
	Isolated Network Virtualization	1. VNIC dashboard displays network packet activity traversing SmartNIC. 2. Redefine network packet egress rule to control/block traffic from virtual servers.
LEVEL 2: **OS and Data Integrity**	**Autonomous Linux**	1. Apply and remove security patches on the fly. 2. Monitor status via CLI.
	Data Safe	1. Assess configuration, users, and sensitive data to validate in-the-cloud controls. 2. Monitor changes to detect configuration drift and out-of-policy data access.
LEVEL 3: **Advanced Security Services Controls**	**Cloud Guard**	1. Run analyses using Oracle-provided Detector recipes to create baselines and discover problems. 2. Use graphical dashboard to investigate problems and trigger defined Responders to apply remediation (or dismiss and modify the recipe if required to prevent reoccurrences).
	Security Zones	1. Create a Maximum Security Zone compartment and define simplified policies to permit or deny activities. 2. Observe how customers can modify the Oracle managed policy recipes to create Custom Security Zones.

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 "embedded" functions often limited to command-line execution.

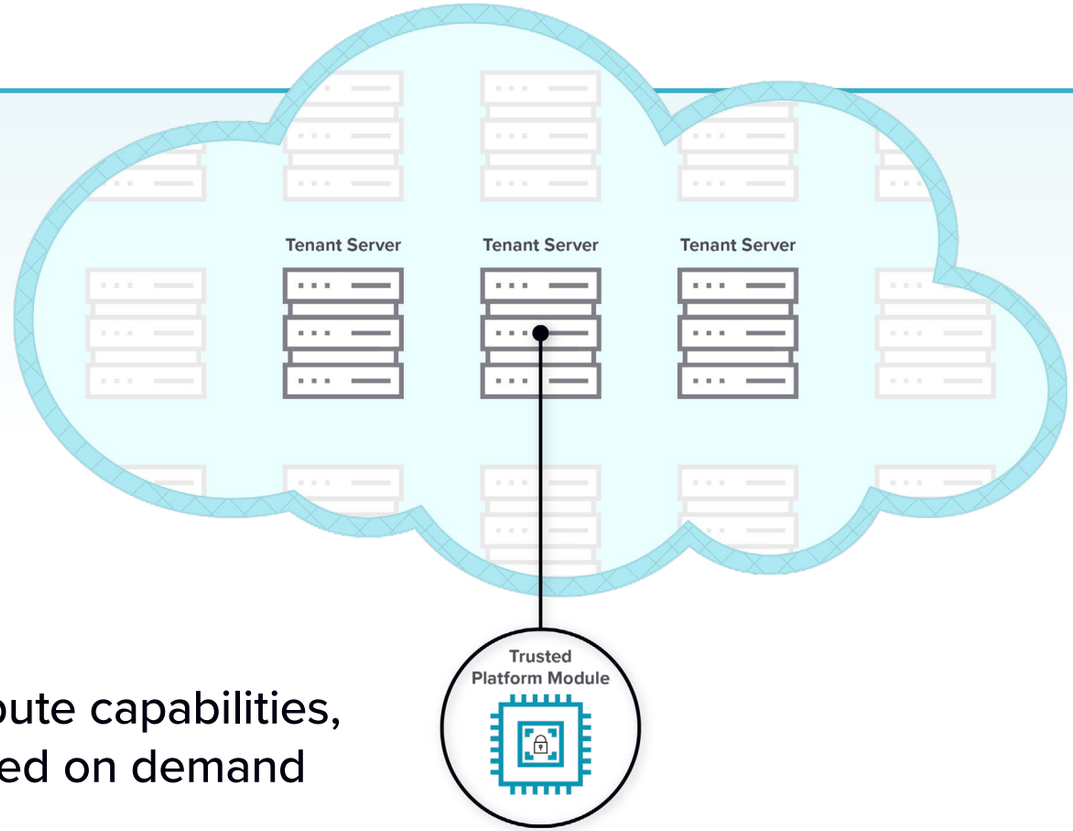
#1 Cloud Architecture	#2 Autonomous Software	#3 Security Controls
BENEFITS / USER OUTCOMES		
• Creation of secure server instances • Obtain enterprise-wide visibility • Integrated business context • Time to value • Get more out of investments ("collect once, reuse many times")	• 100% uptime for OS platform with the ability to apply security and OS patches on the fly • Data and user analysis for in-the-cloud activity	• User configuration and activity monitoring tools to control compartments • Automate the routine, analyze the unique problems • Defend tenant compartments with simplified and consistent policies in real time
FEATURES TO BE TESTED		
• Creation of development and production resources for demo • Removal of server instances and secure recycling of tenant resources • Virtualized networking resources • Control of network traffic using routing table and ingress/egress rules	• Command-line view of kernel status • Removal of all CVE patches • Reapplication of all CVE patches with no platform interruption • Data and user analyses, discovery and masking	• Configurational scan to detect problems • Remediation options and tenant adjustments to baseline recipes • Security Zone policies • Cloud Guard coordination

Notes

Lab sessions occurred May 14, 20, 22, 28 and July 15, 2020. The sessions were viewed remotely via Zoom. Most lab sessions were prefaced by a general discussion of the material to be viewed (some were more cryptic). Analysts were free to ask questions, confirm what they saw, propose alternate scenarios, and challenge assumptions. Each observed lab session ran 60–70 minutes in length.

FEATURE 1

Compute Hardware Security



BENEFITS/FEATURES:

- Public cloud services offer clients elastic compute capabilities, deploying and destroying cloud instances based on demand
- Recycled resources are scrubbed at the firmware level to remove any malware injections introduced by previous tenant
- Eliminates UEFI vulnerabilities for intercepting boot scripts in unprotected memory
- Defends against OS kernel attacks (Spectre/Meltdown) exploiting eBPF bytecode interpreter capabilities

FEATURE 1 VALIDATED

Lab Validated
IDC | 2020

Oracle Cloud Infrastructure Architecture: **Hardware Root of Trust**

OBJECTIVE:

Create and restore cloud hardware back to a known good state when provisioned between customers

VALIDATION PROCESS:

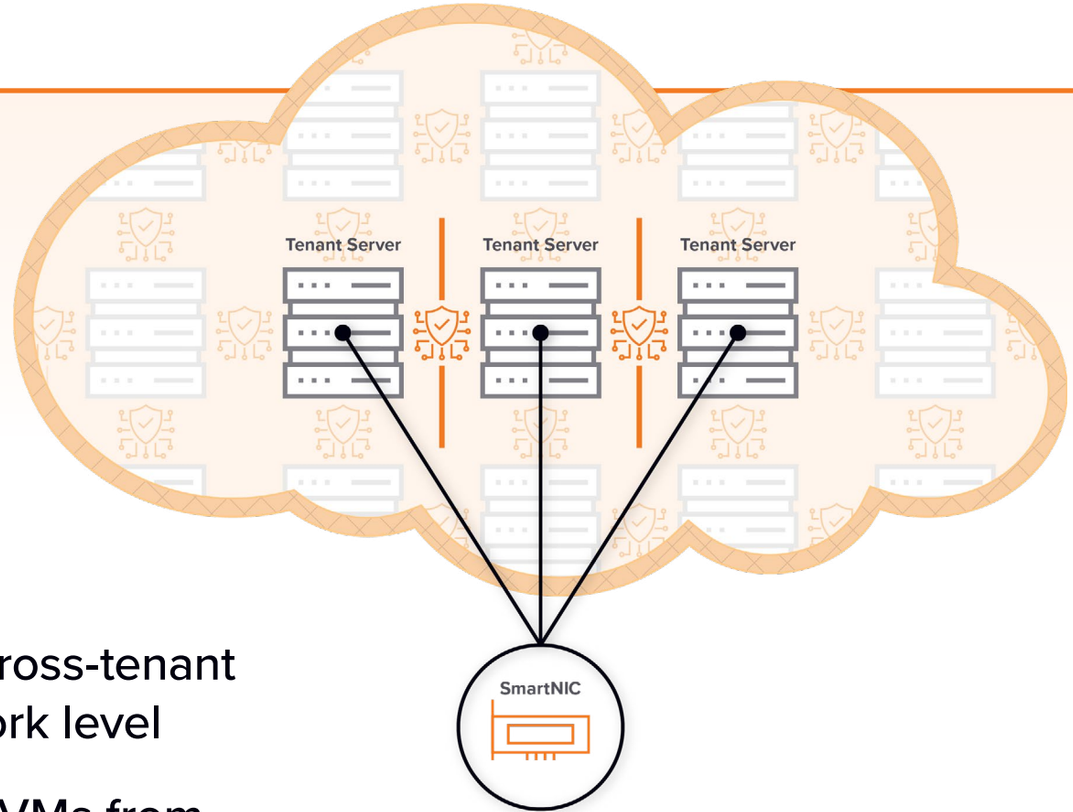
1. ID provisioned instance
2. Create new NVRAM firmware variable (Wipetest)
3. Show persistence of new variable post reboot
4. Terminate instance including boot volume
5. Reprovision instance and show it is the same host as the original
6. Show that the NVRAM variable no longer exists

PROOF:

```
root@wipe-demo:/home/ubuntu# efivar -n 00112233-4455-6677-8899-aabbccddeeff-WipeTest -p
GUID: 00112233-4455-6677-8899-aabbccddeeff
Name: "WipeTest"
Attributes:
        Non-Volatile
        Boot Service Access
        Runtime Service Access
Value:
00000000  00                                               |.              |
root@wipe-demo:/home/ubuntu# # adding some content...
root@wipe-demo:/home/ubuntu# cat test
this is a test
root@wipe-demo:/home/ubuntu# efivar -n 00112233-4455-6677-8899-aabbccddeeff-WipeTest -w -f test
root@wipe-demo:/home/ubuntu# efivar -n 00112233-4455-6677-8899-aabbccddeeff-WipeTest -p
GUID: 00112233-4455-6677-8899-aabbccddeeff
Name: "WipeTest"
Attributes:
        Non-Volatile
        Boot Service Access
        Runtime Service Access
Value:
00000000  74 68 69 73 20 69 73 20  61 20 74 65 73 74 0a     |this is a test.|
```

FEATURE 2

Cloud Tenant Boundaries



BENEFITS/FEATURES:

- Introduces hardware-based barrier to defeat cross-tenant (horizontal) attacks below the VM at the network level
- Isolates, abstracts, and offloads tenant server VMs from processing network-level activities and boosting overall cloud performance
- Leverages SmartNIC technology, safeguarding and accelerating external tenant communications
- Complements other OCI platform security capabilities with a bottom-up defense immune from phishing and configuration errors

FEATURE 2 VALIDATED

Lab Validated
IDC | 2020

Oracle Cloud Infrastructure Architecture: **Isolated Network Virtualization**

OBJECTIVE:

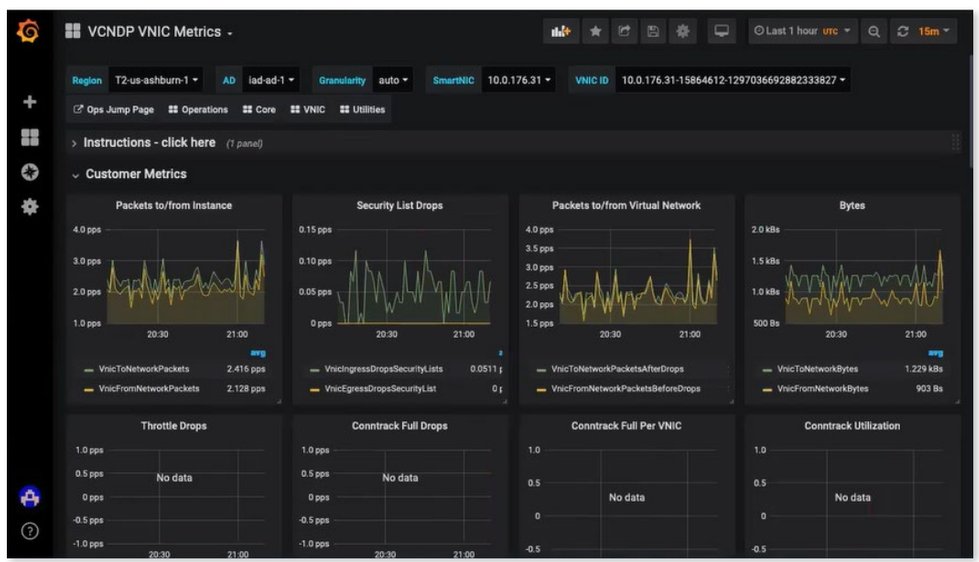
Utilize a SmartNIC to isolate (hardware and software) network processing from the host, preventing a compromised instance from modifying others

VALIDATION PROCESS:

1. Show SmartNIC networking policies
2. Demonstrate network going through the SmartNIC and not the tenant host
3. Route table definitions for subnet configurations
4. Use ingress and egress rules to control traffic contents
5. Review VNIC packet drops after changing an egress rule

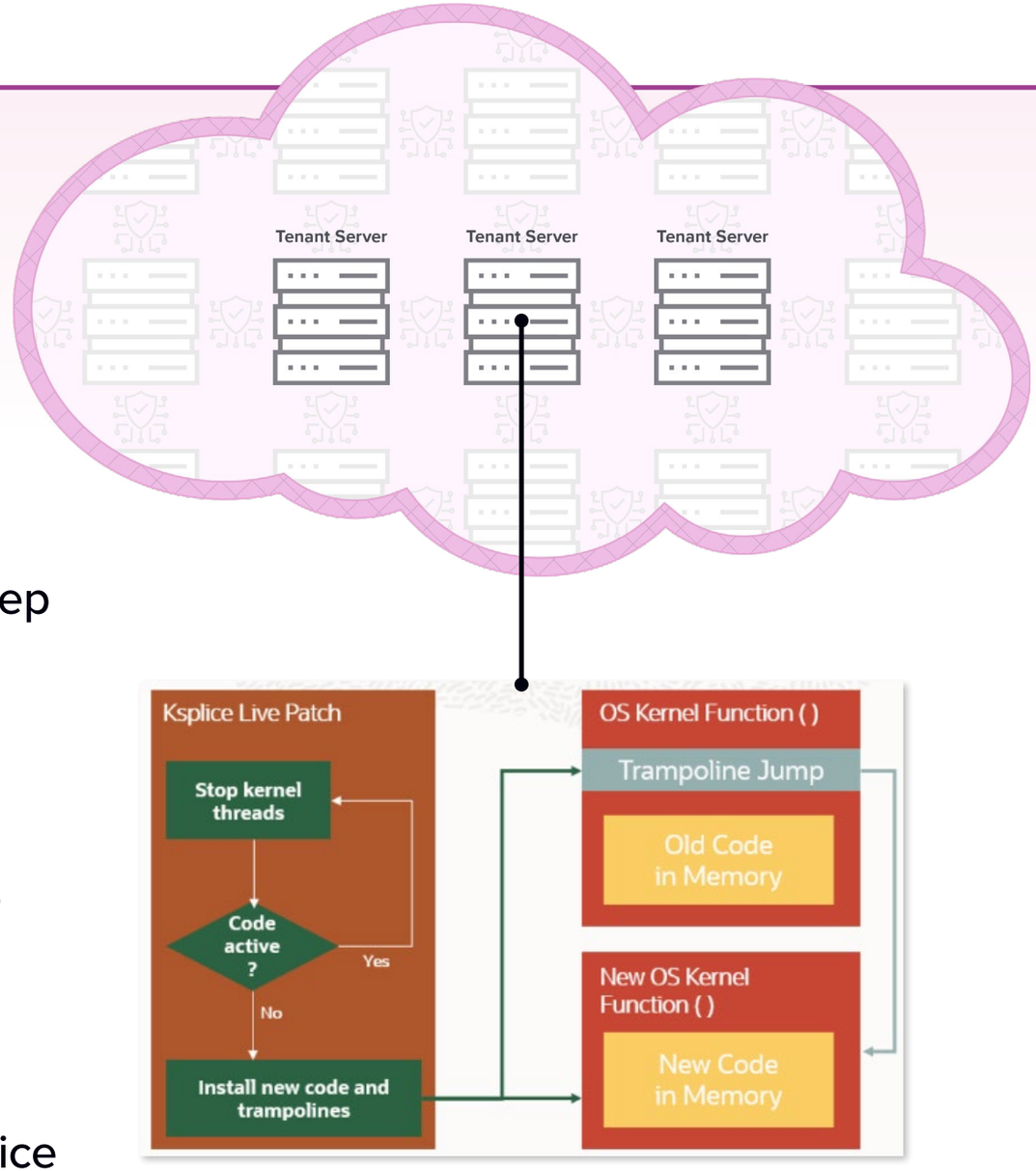
PROOF:

```
Route Tables:
VCN: 15864612  RT: 43384958
  CIDR: 0.0.0.0/0
    Route Type: ig  Physical IP: 172.24.255.255  Slot: 1000000
    Encap Type: gateway_v2  NAT: true  Target: 194233791
  CIDR: 10.1.0.0/16
    Route Type: vnic  Physical IP: 10.8.129.19  Slot: 204661
    Encap Type: vnic_mapping_v1  NAT: false  Target: 18446744071947046365
```



FEATURE 3

Host Platform Health



BENEFITS/FEATURES:

- Performing patch management activities to keep current with CVEs and Linux kernel updates
- Extends autonomous database capabilities to continue live operation with zero downtime
- Protect against executional exposures such as Spectre/Meltdown processor security flaws
- Detection and notification of known exploit attempts made on privilege escalation vulnerabilities that have been patched by Ksplice

FEATURE 3 VALIDATED

Lab Validated
IDC | 2020

Oracle Cloud Infrastructure Architecture: **Autonomous Linux**

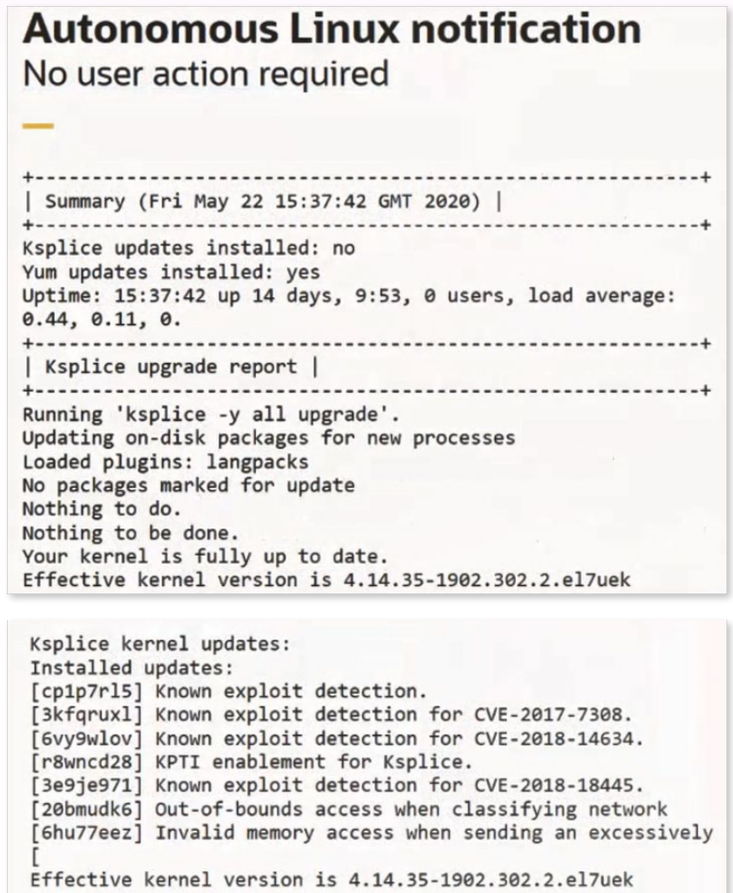
OBJECTIVE:

Apply available security vulnerability patches and Linux kernel updates with no service downtime

VALIDATION PROCESS:

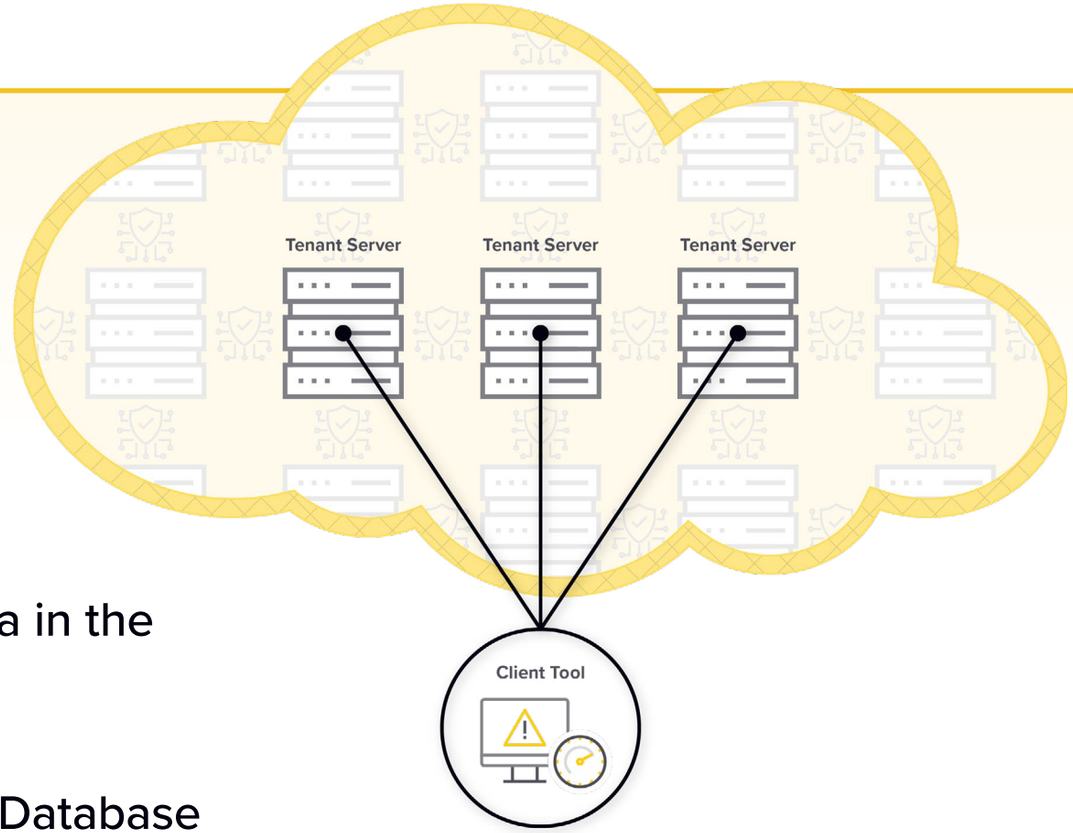
1. Show Linux kernel status
2. Remove all CVE patches
3. Show kernel status
4. Apply all available kernel patches
5. Review patch status
6. Show Ksplice email reports

PROOF:



FEATURE 4

Simplified Data Analysis



BENEFITS/FEATURES:

- OCI administrators cannot directly see the data in the tenants, and thus cannot immediately address security threats of the data
- Free client tool developed as an Autonomous Database spin-off that requires no security training to investigate organizational data realities
- Performs sensitive data discovery and masking tasks with 129 profiles currently defined for pattern spotting
- Mitigates user, data, and configuration risks associated with customer “in the cloud” responsibilities

FEATURE 4 VALIDATED

Lab Validated
IDC | 2020

Oracle Cloud Infrastructure Architecture: **Data Safe**

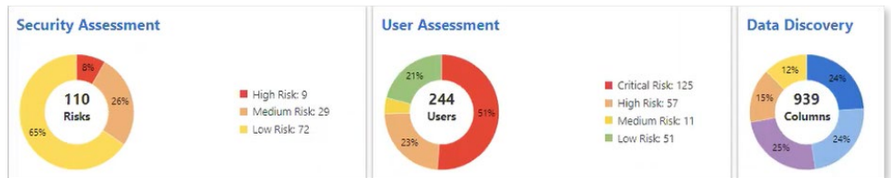
OBJECTIVE:

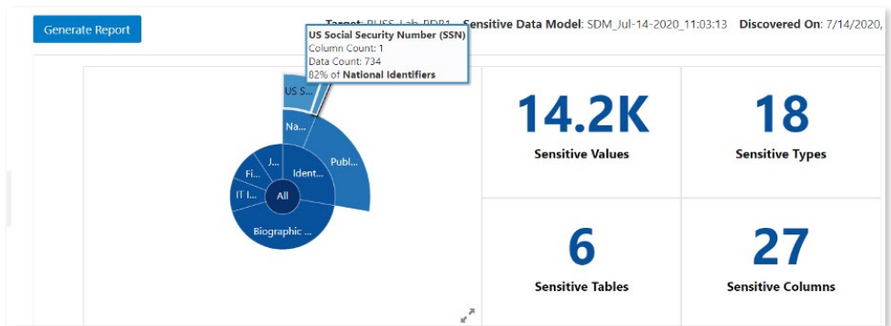
Provide tenants with tools to help manage data OCI can't see

VALIDATION PROCESS:

1. Run a security assessment on a database to create a default baseline
2. Identify results associated with configuration issues or compliance violations
3. Remediate conditions and set an adjusted baseline
4. Run a user assessment
5. Review roles, privileges, and activity for any risky users
6. Run a sensitive data discovery activity
7. Revisit all pre/post baseline adjustments
8. Apply/create data masking templates

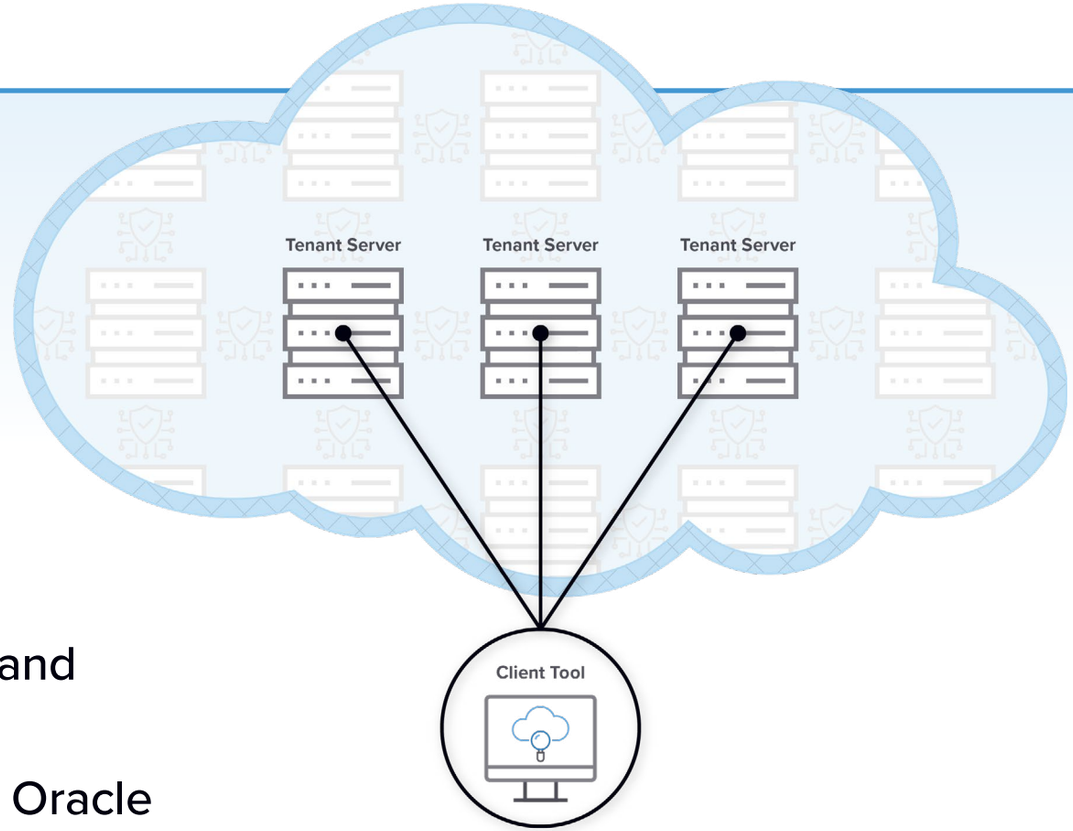
PROOF:





FEATURE 5

Cloud Security Posture Management



BENEFITS/FEATURES:

- Free OCI platform client tool for configuration and activity analysis
- Detect problems generated by out-of-the-box, Oracle best practice recipes
- One-button action to remediate, resolve, or dismiss
- Fix the problem or fix the baseline to prevent reoccurrence next scan
- Future machine learning (ML) technology coming to generate recommendations for previously dismissed conditions

FEATURE 5 VALIDATED

Oracle Cloud Infrastructure Architecture: **Cloud Guard**

Lab Validated IDC | 2020

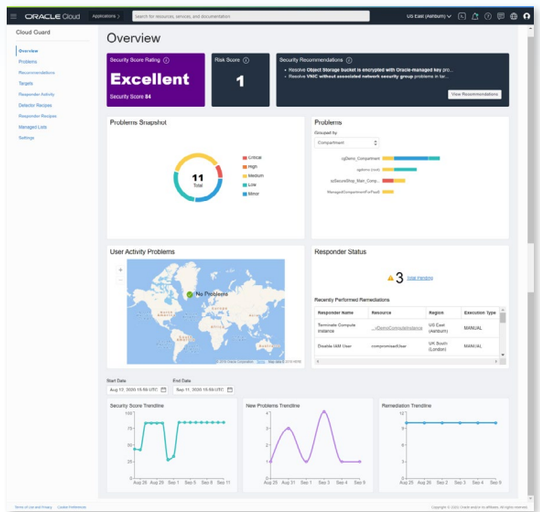
OBJECTIVE:

Provide Oracle baseline Detector and Responder technologies to help users manage their cloud security

VALIDATION PROCESS:

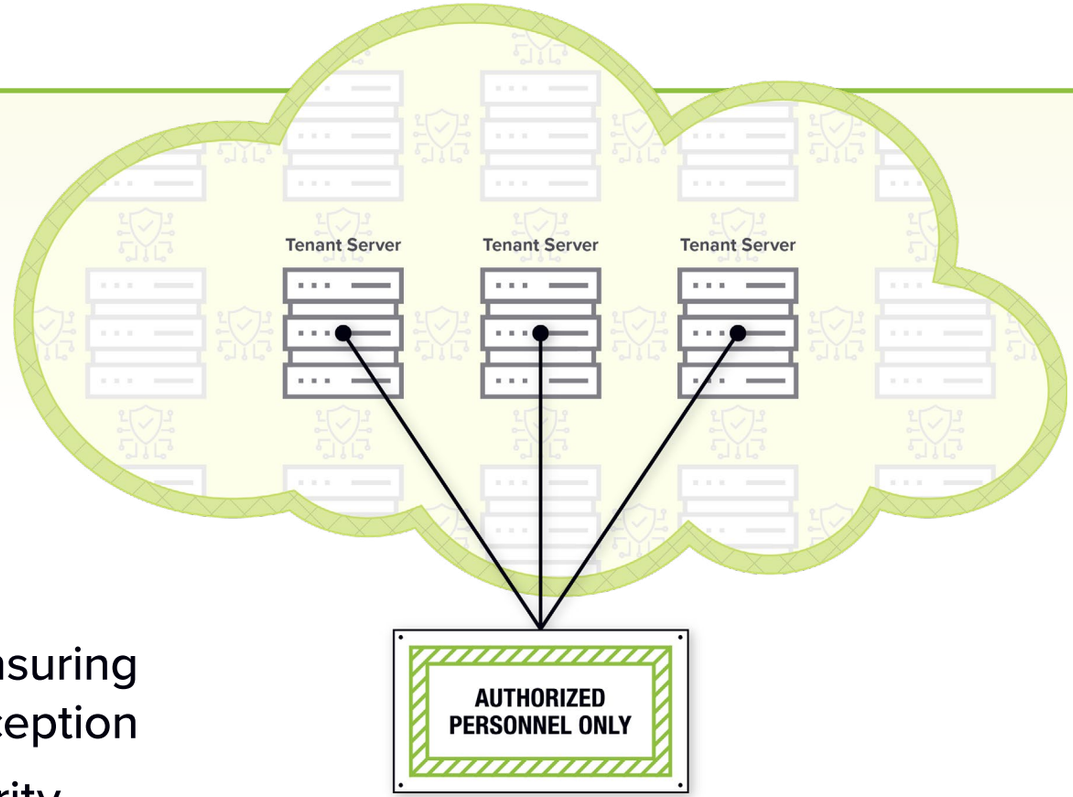
1. Select OCI region and review security scores and risks for a chosen target (default is global)
2. Choose Oracle's baseline configuration detector and run an analysis
3. Select problem associated with open buckets
4. Remediate problem using responder rule and review any related history
5. Review associated detector rules and recipes for targets within compartments
6. Change recipe to diverge from Oracle baseline

PROOF:



FEATURE 6

Mitigating User Configuration Errors



BENEFITS/FEATURES:

- Define a compartment as a protected zone, ensuring resources are secure in real time and since inception
- Addresses problems of applying uniform security policies consistently at scale
- Implements OCI-defined best practices (Maximum Security Zones) or user-adjusted practices (Custom Security Zones)
- Appropriate for highly sensitive workloads with forthcoming vertical market templates to help with compliance mandates

FEATURE 6 VALIDATED

Lab Validated
IDC | 2020

Oracle Cloud Infrastructure Architecture: **Security Zones**

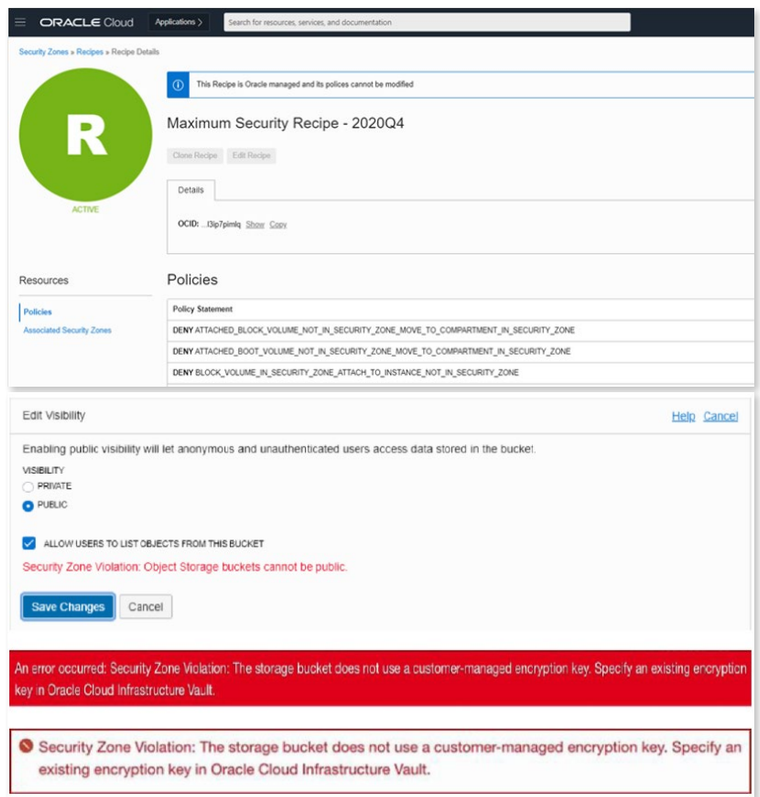
OBJECTIVE:

Provide tenants with an ability to apply simplified security policies within specific compartments to protect sensitive workloads in real time

VALIDATION PROCESS:

1. Review compartment status as enabled or disabled
2. Understand the simplified policy syntax to permit or deny either Oracle best practice recommendations or include custom modifications
3. Review and confirm security zone violation message disallowing the creation of open storage buckets

PROOF:



Key Findings

1. All required IAM and key management plumbing exists to ensure compliance with admin versus developer versus user identities, role definitions, and data access controls. Permissions are only assigned to groups — not to individual users — helping limit the total quantity of unique definitions.
2. Ability to define compartments provides a convenient logical abstraction for organizing cloud resources, including instances, buckets, and applications for groups of users.
3. Policy definitions are manually entered, requiring familiarity with the natural language-oriented engine syntax, or created via automation through the API. They can create very granular controls for providing permissions to user groups assigned to a tenancy or a compartment.
4. Infrastructure hardware is protected against contaminations and takeovers at the server and network levels using firmware wipes and SmartNICs to control tenant assignments and access.
5. Software platform and database technology is kept up to date with patches and application improvements applied automatically and without service disruptions.
6. By design, OCI employees cannot see or change any tenant data, so it developed Data Safe to perform automated data discovery and masking using 100+ pattern templates, resolving one of the toughest client challenges.
7. Cloud Guard is another free tool (including Oracle managed basic recipes) for helping clients understand where problems exist using Detectors and remediate or dismiss conditions using Responders — optionally tuning the "rule" so remediated or dismissed problems don't reoccur.
8. Maximum Security Zones are the real-time capability to provide policy protections at scale for sensitive workloads. This definition will deny configurational errors such as publicly exposed storage buckets, bucket without KMS keys, creation of public subnets, etc.

IDC Opinion

IDC can validate the security technology applied to critical components of Oracle Cloud Infrastructure protecting against low-level device takeovers, subnetwork breaches, operating system status and health, and application-level errors and misconfigurations. These measures guard against:

1. **Top-down attacks coming from user mistakes, software misconfigurations, unapplied patches, and account takeovers**

2. **Bottom-up attacks coming from successful firmware injections able to survive reassignments of cloud resources or lateral, cross-tenant attacks at the network layer**

Any breaches that occur will be contained to a single tenant and even subsets of cloud instances defined and protected by security teams using advanced Oracle hardware and software implementations. The OCI platform is especially suited for security teams who prefer ultimate control over their tenants and data and are comfortable with defining their own controls.

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

Frank Dickson
Program Vice President, Cybersecurity Products, IDC

Frank leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO); Identity & Digital Trust; Legal, Risk & Compliance; Data Security; IoT Security; and Cloud Security. Topically, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701
USA
508.872.8200

idc.com

@idc

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

IDC Doc. #US46883820