Sharing the Cloud Security Responsibility and Mitigating the Top 5 Risks

Gusztáv Szuhai
Solution Sales Manager CEE
Manageability and Security

ORACLE

Managing Risk Ranks High on Global Concerns

The Economist INTELLIGENCE UNIT

"There is a risk that the frequency and severity of cyber-attacks increases to an extent that corporate and government networks could be brought down or manipulated for an extended period of time."

- The top 10 risks to the Global Economy, The Economist Intelligence Unit, 2018

ORACLE

Oracle and KPMG Cloud Threat Report 2019

Survey of 450 global security leaders

- Security risk and compliance issues that impact organizations
- Key Topics
  - Cloud adoption & keeping pace at scale
  - Global threat landscape
  - Role of identity management
  - Cybersecurity best practices
  - Emerging security technologies

www.Oracle.com/CTR

ORACLE

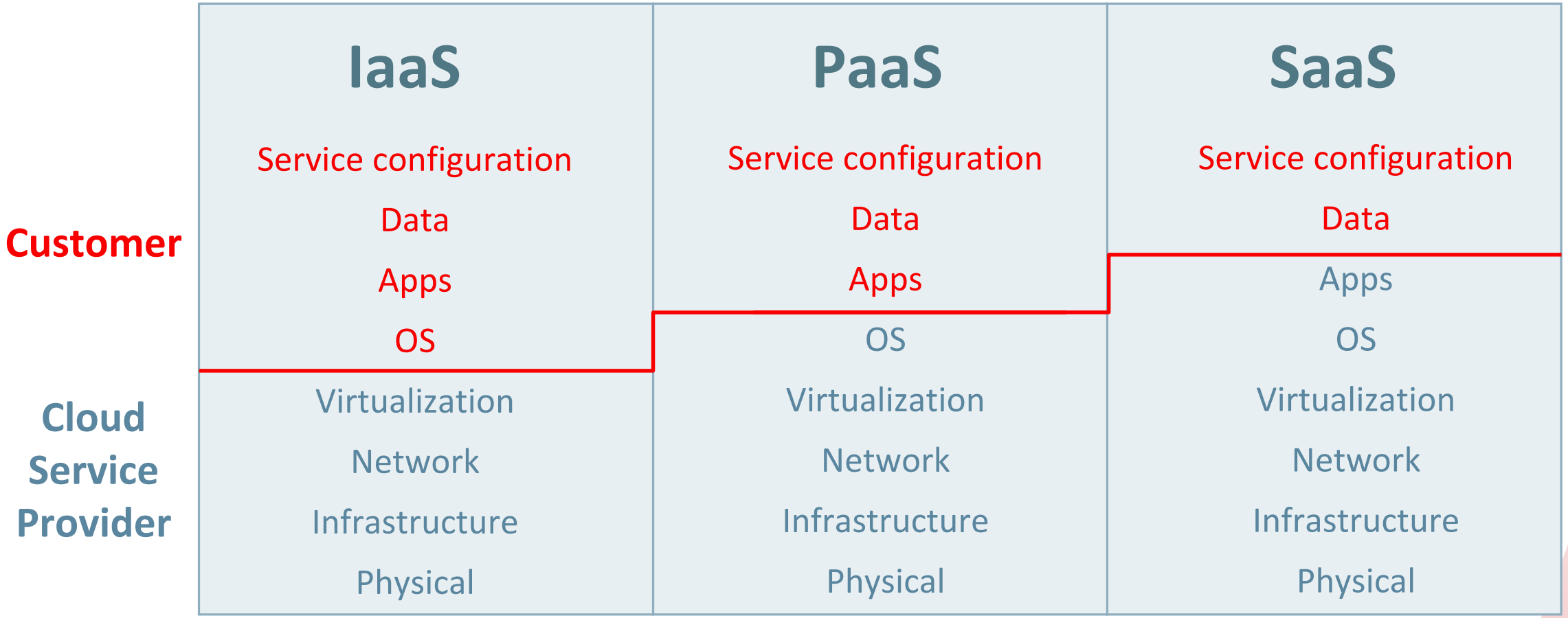
Risk #1: Lack of Responsibility

What is the cloud service provider shared responsibility model?

- Cloud Service Provider (CSP) Shared Responsibility Model
- A gap occurs between the customer's role and the CSP when the customer is not aware of responsibility
- 47% of organizations are not aware of IaaS responsibilities

Source: Oracle and KPMG Cloud Threat Report 2018

Understand the Shared Responsibility Model



Mistake #2: Lack of Training

How strong is your weakest link?

- #1/#2 most common attack vector are phishing scams
- General employees are most at risk to social engineering attacks
- #1 area of investment is employee awareness programs / sec. training

Source: Oracle and KPMG Cloud Threat Report 2018

Focus on Low-Hanging Fruit: Training

Training with a Focus

Employees are your top target on personal and corporate devices

Credential theft is the ultimate goal for these attacks

Generally leverage an email vector, web page redirect or man-in-the-middle attack

> “Email phishing campaigns with an explicit objective of gaining access to cloud-resident applications and data are a prime example of a threat that spans core-to-edge.”

Mistake #3: Reliance on Manual Processes

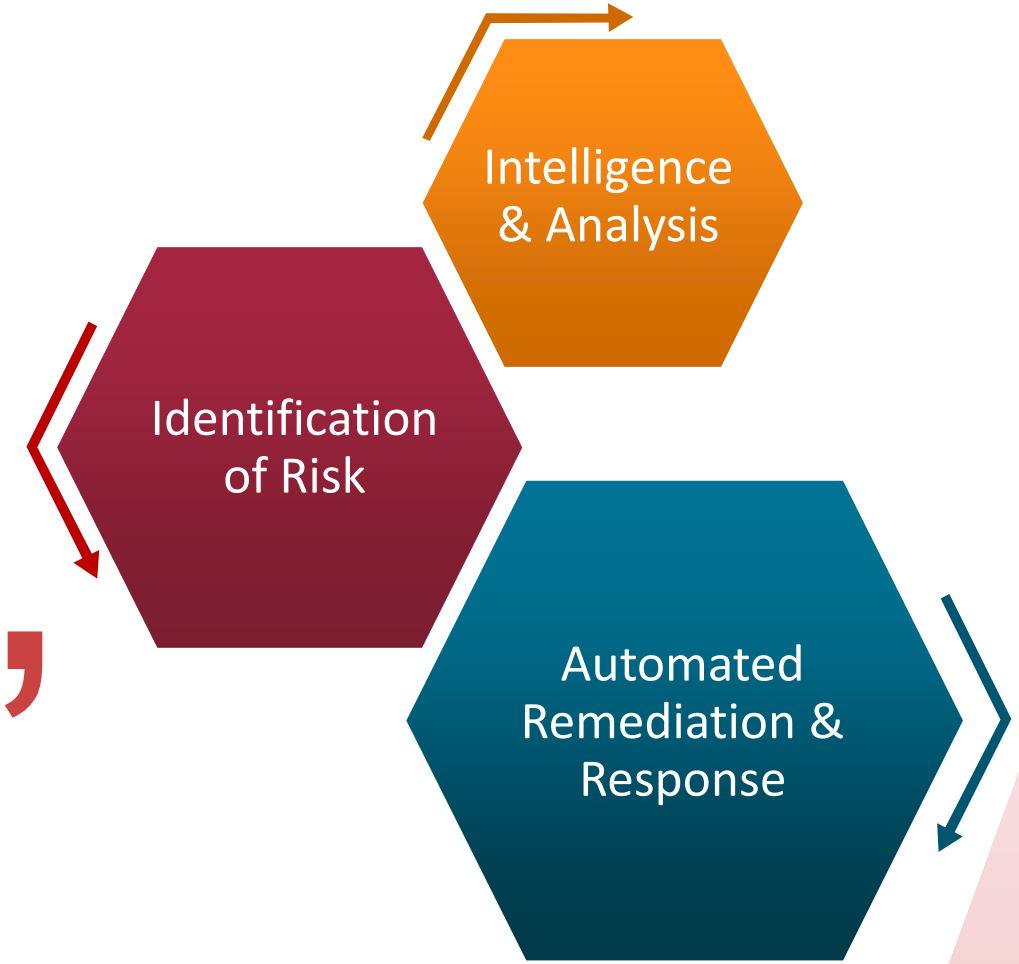
Is your current staff keeping up with event analysis?

- #1 challenge is detecting and reacting to cloud threats
- Cloud services roll out faster than SecOps can support, creating a “Pace Gap”
- 14% of organizations are unable to see majority of security events

Source: Oracle and KPMG Cloud Threat Report 2018

Automate with AI and Machine Learning

> We need a cyber defense system that automatically detects vulnerabilities and attacks. It can't be our people versus their computers. We're going to lose that war. It's got to be our computers versus their computers. And make no mistake, it's a war.
>
> – Larry Ellison, CTO and Founder, Oracle



Risk #4 Lack of Compliance

Are you looking at compliance holistically?

- Compliance = Confidentiality + Integrity + Availability
- Many struggle with compliance without top-down direction
- 95% cite that GDPR will impact cloud strategy….but there is more to compliance than GDPR

Source: Oracle and KPMG Cloud Threat Report 2018

Mistake #5: Lack of Leadership

Who is leading your cloud security journey?

- Many lack a cloud security "quarterback" to lead
- Cloud apps being rolled out by multiple LoB owners and limited oversight around security
- Cloud programs are often delayed by security risks at end of project

Source: Oracle and KPMG Cloud Threat Report 2018

Determine Your Leader: Cloud Security Architect

- SINGLE POINT OF CONTACT
  - One individual to become the subject matter expert (SME) on all regulatory & compliance requirements that impact the organization
  - Works to establish standards across PEOPLE, PROCESSES and TECHNOLOGY in support of the cloud
- ENABLED & EMPOWERED BY ORGANIZATION
  - Involved in the initial planning for new cloud projects, all the way thru to the go-live and ongoing use
  - Is empowered by C-Level to halt any cloud project or service that does not conform to cloud use policies
- ESTABLISH POLICY, CONTROLS, ENFORCEMENT & AUDIT REQUIREMENTS
  - Established cloud security policies, how those policies are implemented in the form of controls, how they are enforced and verified via regular audits
  - Creates a workflow and process for identifying violations in the standards and remediation planning

46% cite they are leveraging a Cloud Security Architect to lead

Hybrid Cloud Security Requirements

One View into All Data

Single pane of glass into all data collection and normalization

Artificial Intelligence Analysis

Machine learning to quickly remediate potential issues

Complete Threat Lifecycle

Prevent, detect, respond to, and predict sophisticated threats

Adaptive Response

Step-up security controls based on anomalous user behavior

Disparate Organizations

Heterogenous, on premises, cloud and multi-cloud coverage

Continuous Monitoring

Consistently assess suspicious activity; autonomous remediation

ORACLE

Oracle's Core to Edge: Security Layers of Defense

Edge

Apps

Web app firewall, malware protection, data redaction, access controls, CASB, DDoS/botnet protection, API security

Users

Identity & access governance, user & entity behavioral analytics, multi-factor auth., single sign-on

Data

Nonprod data masking, encryption and key management, privileged user access control, DLP online self-patching, database activity monitoring

Core

Infrastructure

Threat detection and response, monitoring and analytics, configuration and compliance

Application Layers of Defense

Cloud access security broker (CASB)

- Visibility into cloud apps that users access
- Automatic, continuous threat detection, remediation of config changes and threats
- Predictive analytics and incident response, security configuration management

Web application firewall

- Protects OCI-based applications
- Inspects all traffic destined for web apps, identifies and blocks malicious traffic

Application data redaction

- Remove application layer data on the fly
- Maintain least privilege for app users

User Layers of Defense

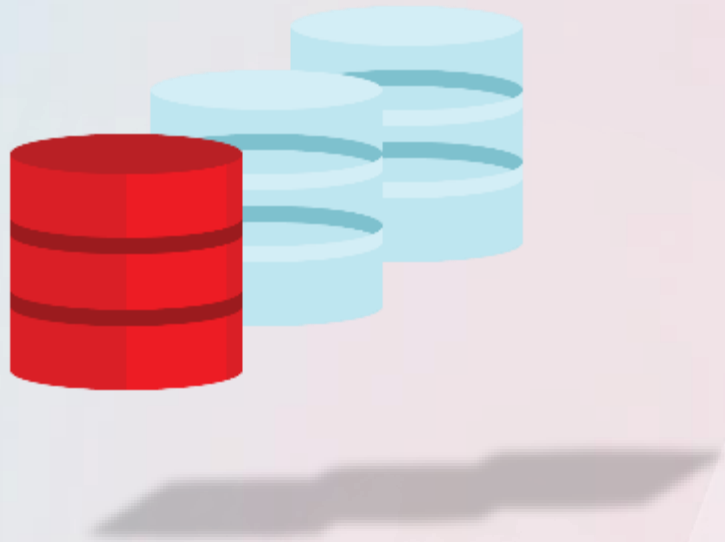
Identity and access management

- Complete lifecycle from on- to off-boarding
- Adaptive access controls based on behaviors
- Multifactor authentication and SSO

Super User Access Controls

- View privileges at runtime
- Detect and prevent suspicious user activity
- Separation of duties and least privilege

Data Layers of Defense



Data encryption by default and end-to-end
- Encrypted at rest: object, file, block, database
- Fully encrypted global backbone

Key management for complete key lifecycle
- Customer control of storage encryption keys
- Backed by Hardware Security Module (HSM)
- Heterogeneous, hybrid/multi-cloud support

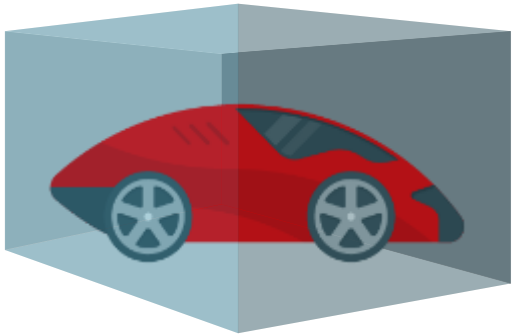
Separation of duties and access control
- Context-aware enforcement
- Control at all levels: data objects, commands

Database auditing and monitoring
- Audit collection for databases and OS
- Network-based monitoring detects anomalies

Masking for nonproduction
- Replace sensitive production data
- Maintain referential integrity

Oracle Autonomous Database

Goal - Eliminate human labor



Self-Driving

Automates all database and infrastructure management, monitoring, tuning

Self-Securing

Protects from both external attacks and malicious internal users

Self-Repairing

Protects from all downtime including planned maintenance

Infrastructure Layers of Defense

Deeper isolation from other customers
- Bare metal isolation
- Private off-box virtual networking
- Dedicated hardware – Exadata

Dedicated network of cloud control computers
- Protects cloud perimeter and customer zones
- Prevent customer access to cloud control computers and memory

AI and ML detects and prevents threats
- Autonomous Database self patching

Distributed denial of service protection
- Automated DDoS attack detection and mitigation of high volume layer 3/4 attacks
- Ensures availability of network resources

Network protection
- Security lists + private subnets
- Load balancer for layer 4 or 7
- IPSec VPN + FastConnect

Oracle University – Learning Subscription for Cloud Security

Cloud Services

- Cloud Access Security Broker (CASB)
- Identity
- Configuration and Compliance
- Security Monitoring and Analytics
- Oracle Management Cloud (OMC)

Job Roles:

- **Security administrators**
- **Identity administrators**
- **OMC security administrators**

Oracle Cloud Platform Identity and Security Management 2018 Associate

ORACLE

Oracle
Cloud Day

Thank you