Learnings from the State of Cybersecurity
Compliance Stress – Data Security

Gusztáv Szuhai
June-24-2020

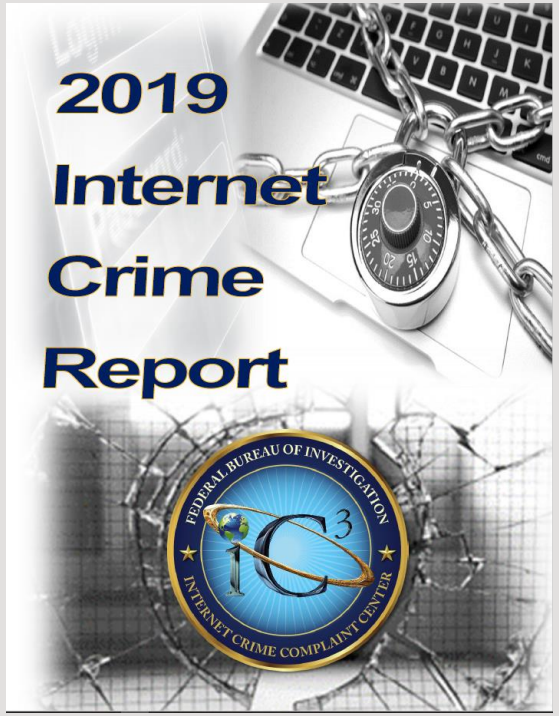
Cetral Europe Security & Systems Management

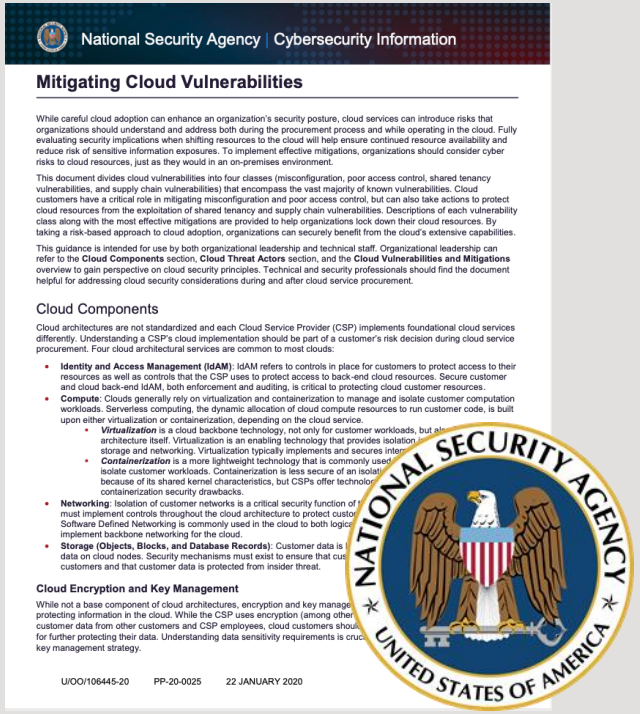
Safe Harbor

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at http://www.oracle.com/investor. All information in this presentation is current as of February 2020 and Oracle undertakes no duty to update any statement in light of new information or future events.

Current state of Cybersecurity – stay informed




National Security Agency | Cybersecurity Information

Mitigating Cloud Vulnerabilities

While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud. Fully evaluating security implications when shifting resources to the cloud will help ensure continued resource availability and reduce risk of sensitive information exposures. To implement effective mitigations, organizations should consider cyber risks to cloud resources, just as they would in an on-premises environment.

This document divides cloud vulnerabilities into four classes (misconfiguration, poor access control, shared tenancy vulnerabilities, and supply chain vulnerabilities) that encompass the vast majority of known vulnerabilities. Cloud customers have a critical role in mitigating misconfiguration and poor access control, but can also take actions to protect cloud resources from the exploitation of shared tenancy and supply chain vulnerabilities. Descriptions of each vulnerability class along with the most effective mitigations are provided to help organizations lock down their cloud resources. By taking a risk-based approach to cloud adoption, organizations can securely benefit from the cloud's extensive capabilities.

This guidance is intended for use by both organizational leadership and technical staff. Organizational leadership can refer to the **Cloud Components** section, **Cloud Threat Actors** section, and the **Cloud Vulnerabilities and Mitigations** overview to gain perspective on cloud security principles. Technical and security professionals should find the document helpful for addressing cloud security considerations during and after cloud service procurement.

Cloud Components

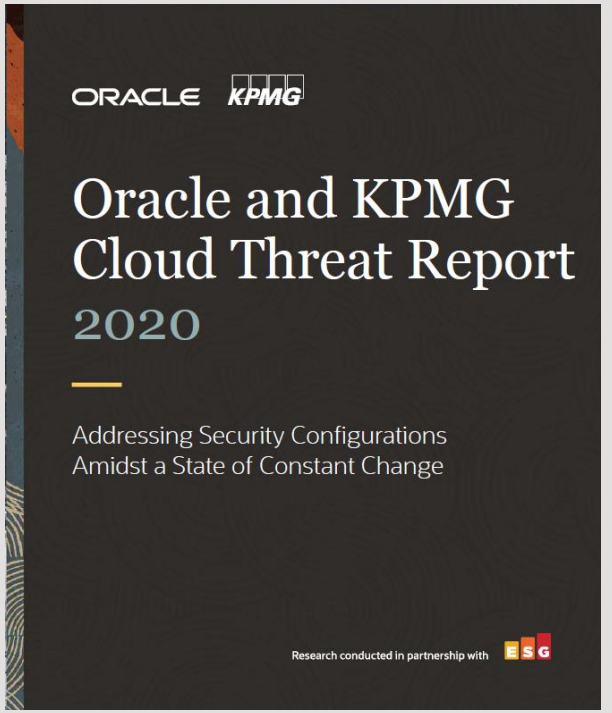
Cloud architectures are not standardized and each Cloud Service Provider (CSP) implements foundational cloud services differently. Understanding a CSP's cloud implementation should be part of a customer's risk decision during cloud service procurement. Four cloud architectural services are common to most clouds:

- **Identity and Access Management (IdAM)**: IdAM refers to controls in place for customers to protect access to their resources as well as controls that the CSP uses to protect access to back-end cloud resources. Secure customer and cloud back-end IdAM, both enforcement and auditing, is critical to protecting cloud customer resources.
- **Compute**: Clouds generally rely on virtualization and containerization to manage and isolate customer computation workloads. Serverless computing, the dynamic allocation of cloud compute resources to run customer code, is built upon either virtualization or containerization, depending on the cloud service.
  - ***Virtualization*** is a cloud backbone technology, not only for customer workloads, but al… architecture itself. Virtualization is an enabling technology that provides isolation … storage and networking. Virtualization typically implements and secures inte…
  - ***Containerization*** is a more lightweight technology that is commonly used … isolate customer workloads. Containerization is less secure of an isolati… because of its shared kernel characteristics, but CSPs offer technolo… containerization security drawbacks.
- **Networking**: Isolation of customer networks is a critical security function of … must implement controls throughout the cloud architecture to protect custo… Software Defined Networking is commonly used in the cloud to both logica… implement backbone networking for the cloud.
- **Storage (Objects, Blocks, and Database Records)**: Customer data is … data on cloud nodes. Security mechanisms must exist to ensure that cus… customers and that customer data is protected from insider threat.

Cloud Encryption and Key Management

While not a base component of cloud architectures, encryption and key manage… protecting information in the cloud. While the CSP uses encryption (among other… customer data from other customers and CSP employees, cloud customers shou… for further protecting their data. Understanding data sensitivity requirements is cruc… key management strategy.

U/OO/106445-20 PP-20-0025 22 JANUARY 2020



Download the 28 pages Report HERE

Download the 8 pages InfoSheet HERE

Download the 54 pages Report HERE

FBI ICC – Document ”Internet Crime Report” issued in 2020

2019 INTERNET CRIME REPORT

TABLE OF CONTENTS

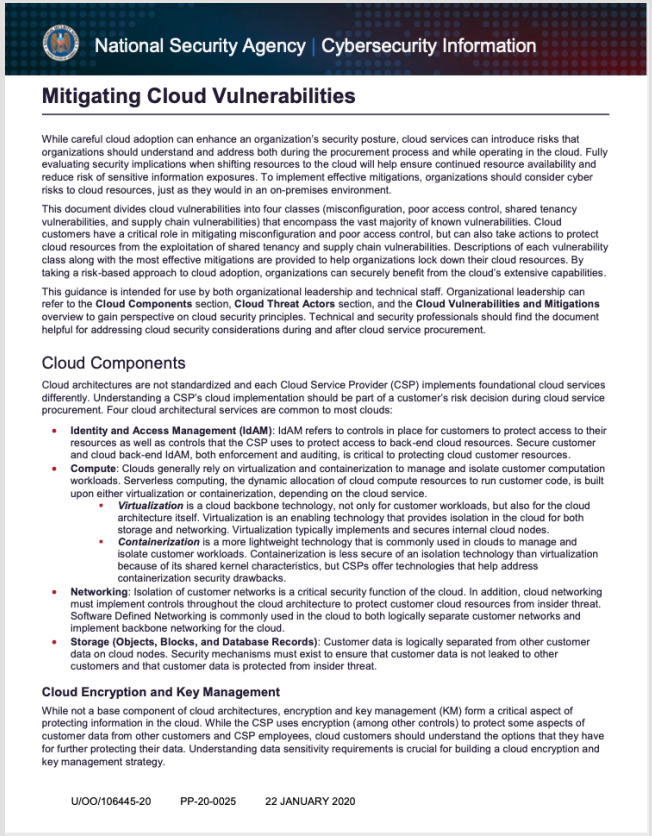
Introduction 3
About the Internet Crime Complaint Center 4
IC3 History 5
The IC3 Role in Combating Cyber Crime 6
IC3 Core Functions 7
Supporting Law Enforcement 8
IC3 Database Remote Access 8
Hot Topics for 2019 9
Business Email Compromise (BEC) 9
IC3 Recovery Asset Team 10
RAT Successes 11
Elder Fraud 12
Tech Support Fraud 13
Ransomware 14
2019 Victims by Age Group 16
2019 - Top 20 International Countries by Victim 17
2019 - Top 10 States by Number of Victims 18
2019 - Top 10 States by Victim Loss 18
2019 Crime Types 19
2019 Overall State Statistics 21
Appendix A: Crime Type Definitions 25
Appendix B: Additional information about IC3 Data 28

2019 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data Breach	38,218	IPR/Copyright and Counterfeit	3,892
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,775	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care Related	657
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	61
Real Estate/Rental	11,677	Hacktivist	39
Other	10,842		

NSA – Document ”Mitigating Cloud Vulnerabilities”



National Security Agency | Cybersecurity Information

Mitigating Cloud Vulnerabilities

While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud. Fully evaluating security implications when shifting resources to the cloud will help ensure continued resource availability and reduce risk of sensitive information exposures. To implement effective mitigations, organizations should consider cyber risks to cloud resources, just as they would in an on-premises environment.

This document divides cloud vulnerabilities into four classes (misconfiguration, poor access control, shared tenancy vulnerabilities, and supply chain vulnerabilities) that encompass the vast majority of known vulnerabilities. Cloud customers have a critical role in mitigating misconfiguration and poor access control, but can also take actions to protect cloud resources from the exploitation of shared tenancy and supply chain vulnerabilities. Descriptions of each vulnerability class along with the most effective mitigations are provided to help organizations lock down their cloud resources. By taking a risk-based approach to cloud adoption, organizations can securely benefit from the cloud's extensive capabilities.

This guidance is intended for use by both organizational leadership and technical staff. Organizational leadership can refer to the **Cloud Components** section, **Cloud Threat Actors** section, and the **Cloud Vulnerabilities and Mitigations** overview to gain perspective on cloud security principles. Technical and security professionals should find the document helpful for addressing cloud security considerations during and after cloud service procurement.

Cloud Components

Cloud architectures are not standardized and each Cloud Service Provider (CSP) implements foundational cloud services differently. Understanding a CSP's cloud implementation should be part of a customer's risk decision during cloud service procurement. Four cloud architectural services are common to most clouds:

- **Identity and Access Management (IdAM)**: IdAM refers to controls in place for customers to protect access to their resources as well as controls that the CSP uses to protect access to back-end cloud resources. Secure customer and cloud back-end IdAM, both enforcement and auditing, is critical to protecting cloud customer resources.
- **Compute**: Clouds generally rely on virtualization and containerization to manage and isolate customer computation workloads. Serverless computing, the dynamic allocation of cloud compute resources to run customer code, is built upon either virtualization or containerization, depending on the cloud service.
  - ***Virtualization*** is a cloud backbone technology, not only for customer workloads, but also for the cloud architecture itself. Virtualization is an enabling technology that provides isolation in the cloud for both storage and networking. Virtualization typically implements and secures internal cloud nodes.
  - ***Containerization*** is a more lightweight technology that is commonly used in clouds to manage and isolate customer workloads. Containerization is less secure of an isolation technology than virtualization because of its shared kernel characteristics, but CSPs offer technologies that help address containerization security drawbacks.
- **Networking**: Isolation of customer networks is a critical security function of the cloud. In addition, cloud networking must implement controls throughout the cloud architecture to protect customer cloud resources from insider threat. Software Defined Networking is commonly used in the cloud to both logically separate customer networks and implement backbone networking for the cloud.
- **Storage (Objects, Blocks, and Database Records)**: Customer data is logically separated from other customer data on cloud nodes. Security mechanisms must exist to ensure that customer data is not leaked to other customers and that customer data is protected from insider threat.

Cloud Encryption and Key Management

While not a base component of cloud architectures, encryption and key management (KM) form a critical aspect of protecting information in the cloud. While the CSP uses encryption (among other controls) to protect some aspects of customer data from other customers and CSP employees, cloud customers should understand the options that they have for further protecting their data. Understanding data sensitivity requirements is crucial for building a cloud encryption and key management strategy.

U/OO/106445-20 PP-20-0025 22 JANUARY 2020

- Introduction & Objectives
- Cloud Components:
  - IdAM, Compute, Network, Storage
  - Cloud Encryption & Key Management
  - Sharing Cloud Responsibility Model
  - Cloud Threat Actors
- Cloud Vulnerabilities and Mitigations (*with examples and recommendations*)
  - Misconfiguration
  - Poor Access Control
  - Shared Tenancy Vulnerabilities
  - Supply Chain Vulnerabilities

ORACLE-KPMG ”Cloud Threat Report” 2020

In Summary: Culture Is the Catalyst to Close the Readiness Gap

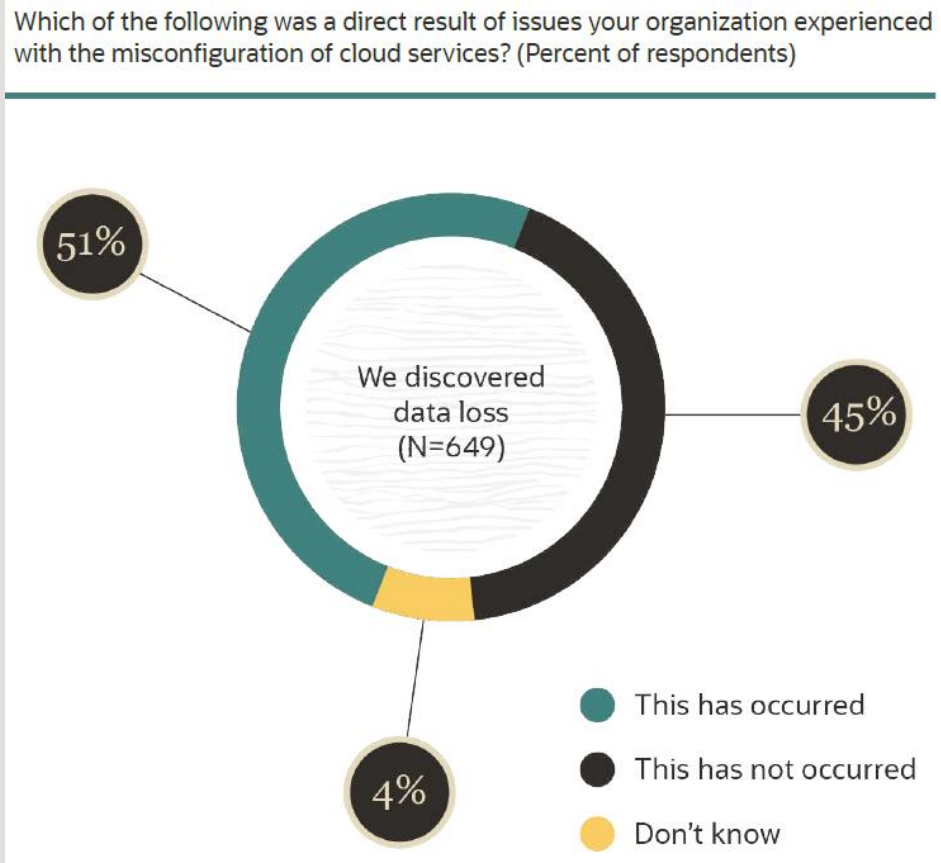
What Are the Common Denominators of Different Reports?

- Digital Transformation (DX) drives cloud usage
  - by containerizing existing apps
  - by using SaaS
  - by developing new, cloud-native custom apps
- DX is usually Department-driven
  - new apps don't get built-in security
  - Security Dept. is not involved, or lately involved
  - Shared Responsibility is not understood

- READINESS GAP – Mindset / Toolset

What Are the Common Denominators of Different Reports?

- Typical security problems are common
  - misconfiguration
  - shared resposibility of cloud not understood
  - cyber attacks
    - #1 PHISING
    - > DATA BREACH
    - > IDENTITY THEFT
- These are mostly HUMAN-related issues
  - a cultural change is needed
  - automation is needed, wherever possible



What to Do with Misconfiguration?

Malicious CSP Admins Malicious Customer Admins

NSA Report

Figure 2: Cloud Vulnerabilities – Prevalence versus Sophistication of Exploitation

Cyber Criminals Untrained or Neglectful Cust. Admins

Oracle-KPMG Report

88%

All workloads will be autonomously updated within 3 years.

92%

Have a cloud security readiness gap.

3/4

Feel the cloud is more secure than their data center.

3/4 Have experienced data loss from a cloud service more than once.

****

59% Have had privileged cloud credentials phished.

3x

More worried about corporate security than safety at home

50%

Will have all their data in public cloud stores in 2 years.

73%

Have or plan to hire a CISO with more cloud security skills.

87%

View artificial intelligence as a must-have for security controls.

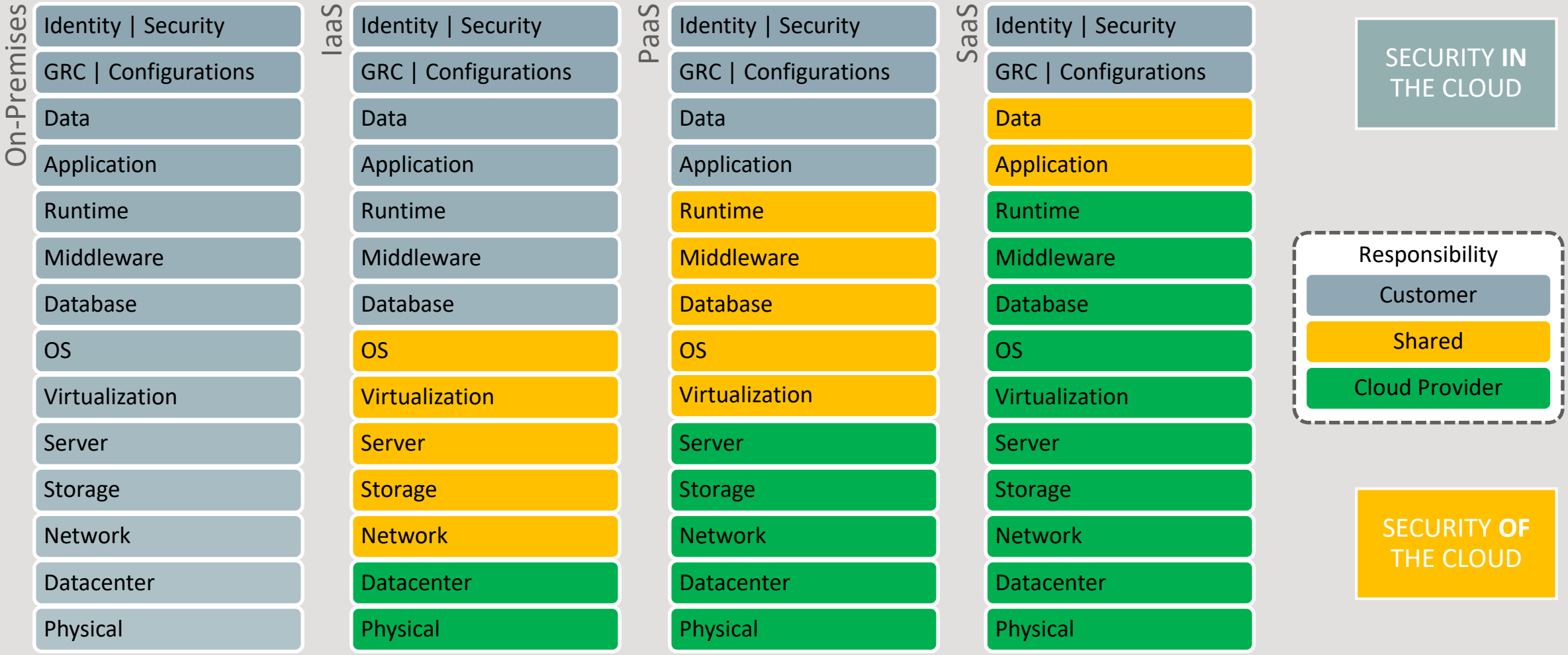
>10

Data loss events experienced by orgs with multiple misconfigured cloud services.

What to Do with Misconfiguration?

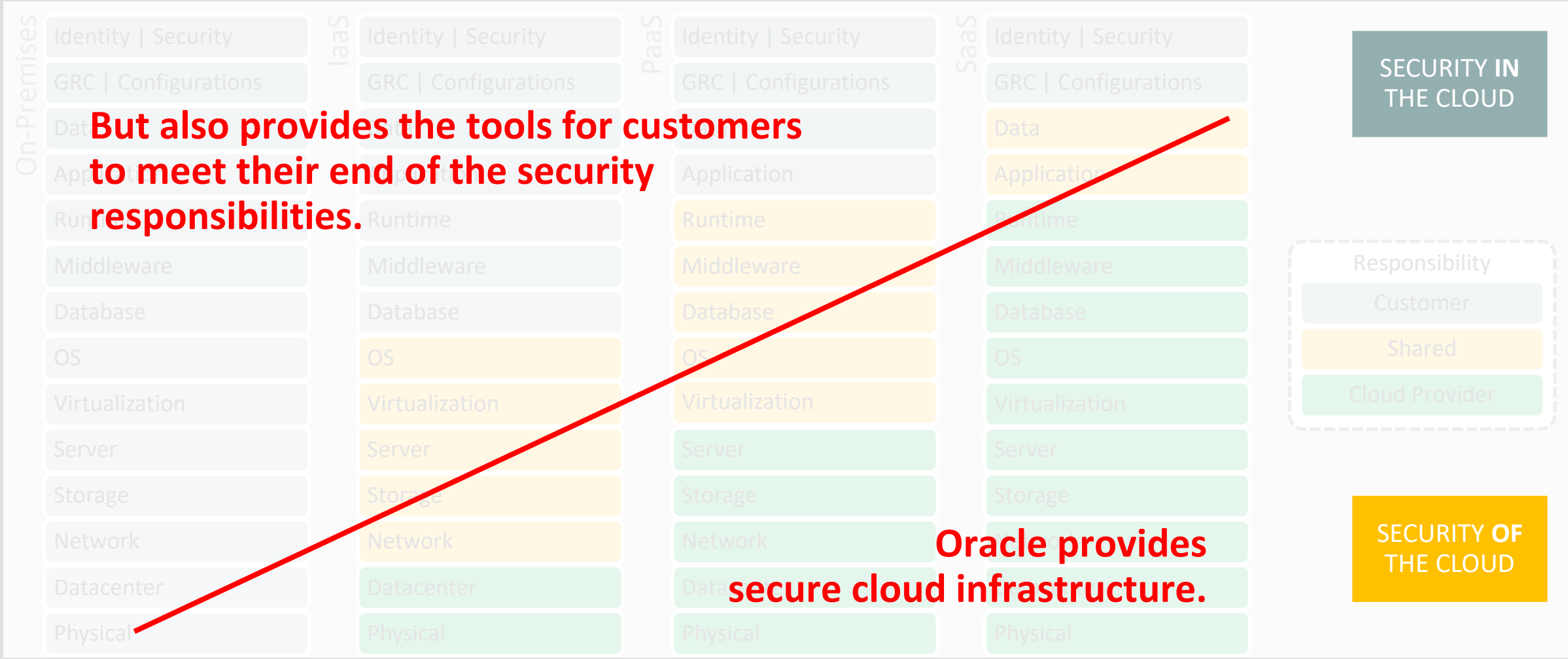
- Typical configuration problems
  - #1 over-privileged users, no identity governance
  - #2 exposed servers
  - #3 weak access control – lack of MFA
  - #4 log-collection is missing
  - #5 secrets (e.g. keys) are kept in unsafe places
- Most important step is to change Company culture
  - security to become a business reqirement (DevSecOps)
  - shared security responsibility of project team members
  - Organization changes: BISO together with CISO

Everyone Must Learn the Shared Responsibility Model



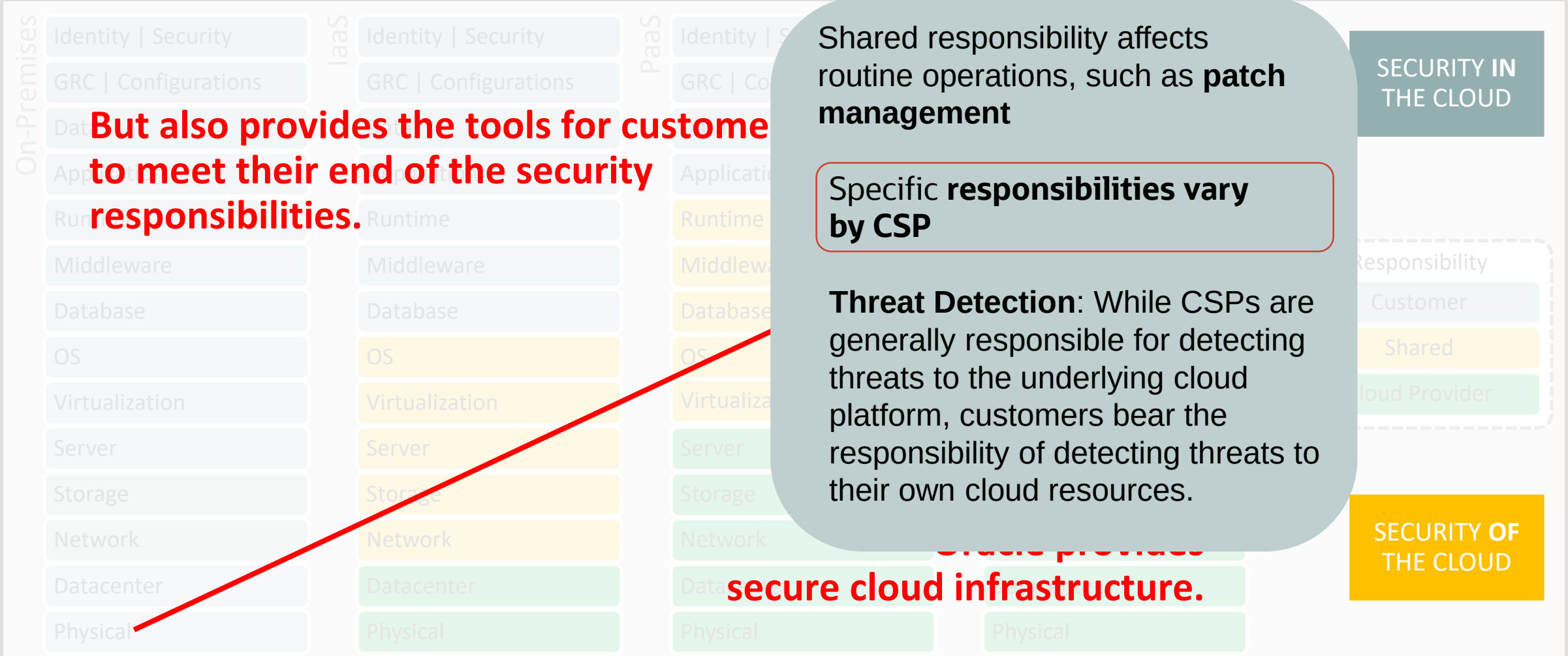
"Through 2024, 99% of cloud security failures will be the customer's fault." - Gartner

Tools to Apply the Shared Responsibility Model



"Through 2024, 99% of cloud security failures will be the customer's fault." - Gartner

Tools to Apply the Shared Responsibility Model



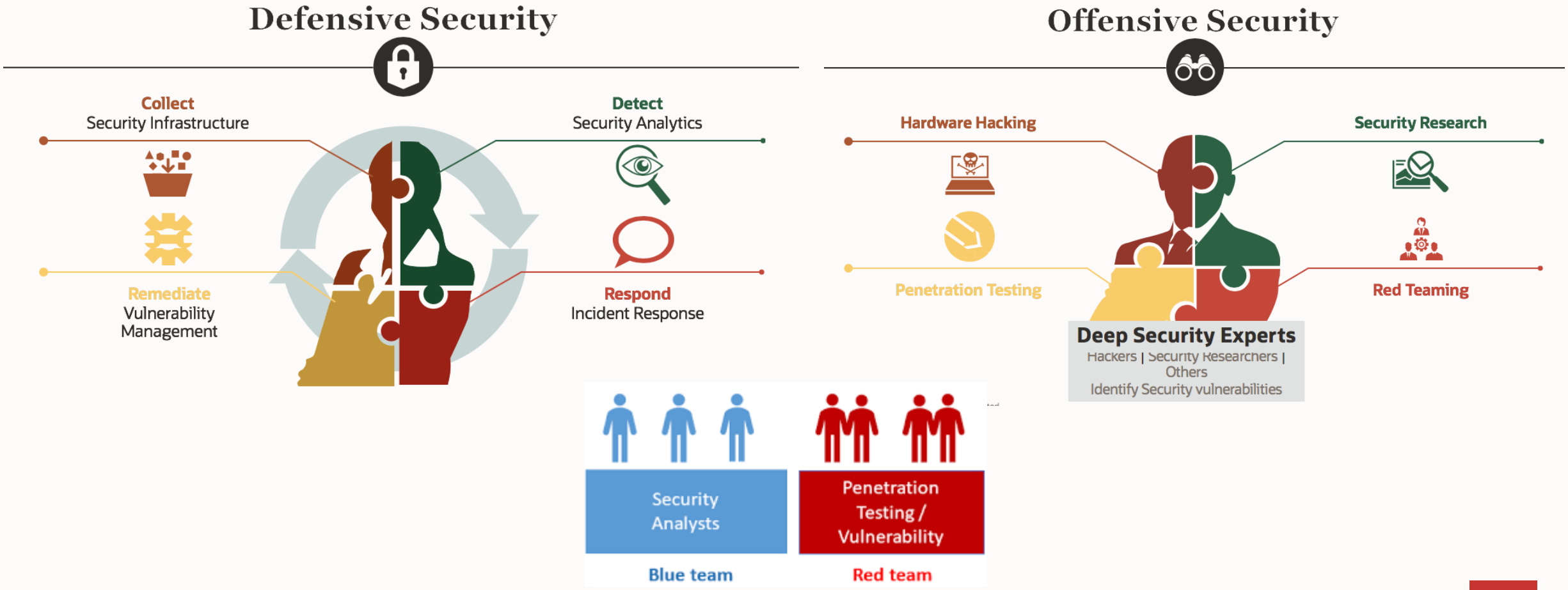
"Through 2024, 99% of cloud security failures will be the customer's fault." - Gartner

What to Do Against Cyber-Attacks?

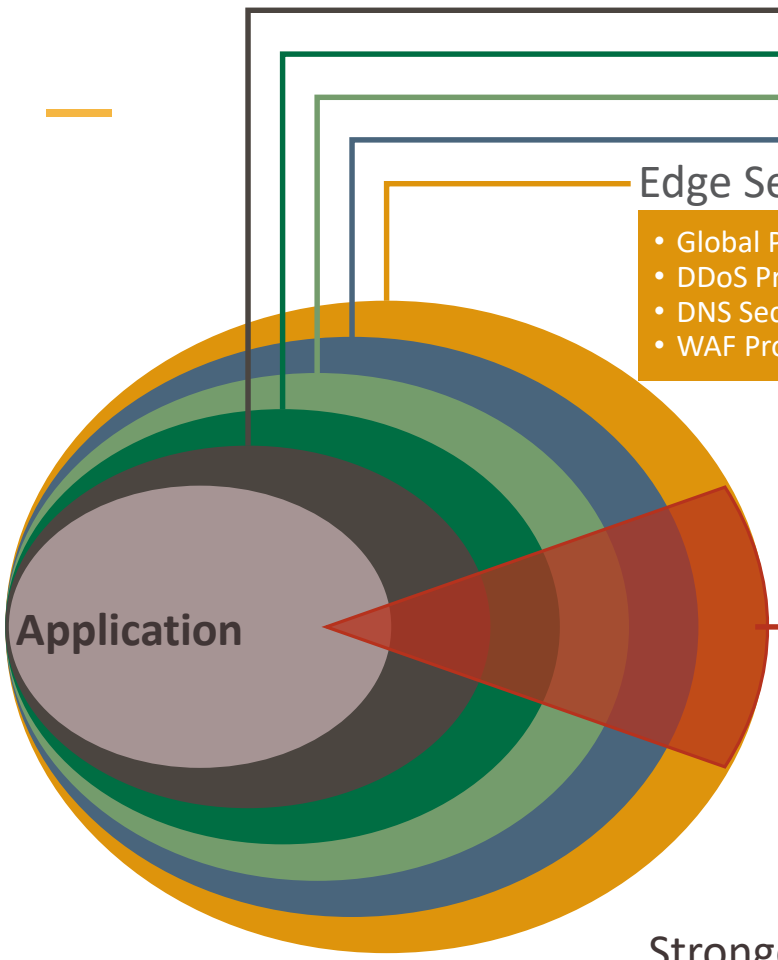
- Phising is still #1. Attackers go for not only admin rights but also for privileged service accounts (in applications)
  - COVID-19: number of remote workers jumped

- Secure the HUMAN perimeter vs. the Network perimeter
  - IDM with MFA + Identity Governance, Adaptive Authentication
  - End-user awareness training
  - User Behaviour Analysis (based on ML Anomaly Detection)
  - Continuous Red-teaming (identify baseline of successful phising attacks)

Security of Oracle Cloud: World-Class Security Operations



Oracle Cloud Security Architecture



Edge Services
- Global PoPs
- DDoS Protection
- DNS Security
- WAF Protection

Monitoring
- 3rd Party Security
  - FW
  - NGFW
  - IPS
- User Monitoring
- Configuration Monitoring
- Logging
- Compliance
- Cloud Gard
- CASB

Virtual Network
- Interface Segmentation
- Security Lists
- Private Networks
- Bastion Access
- SSL Load Balancing
- FastConnect (Direct)
- FastConnect (Carrier)
- IPSec VPN

Instance
- Tenant Isolation
- Hardened Images
- Virtual Taps
- Hardware Entropy
- SSH Keys
- Certificates
- Root-Of-Trust Card
- Signed Firmware
- Hardware Security Modules
- Autonomous Linux

Data/Database
- DataSafe
- At-Rest-Crypto
  - TDE
  - DataGuard
- In-Transit-Crypto
  - SSL/TLS
  - NNE
- Keys
- Managed Keys
- Custom Keys
- Managed Vault
- Autonomous Database

Identity
- Identity Federation
- Role-Based Policy
- Compartments & Tagging
- Instance Principals

1. Identity and Access Mgmt

2. Compute (Virtualization/Conteinarization)

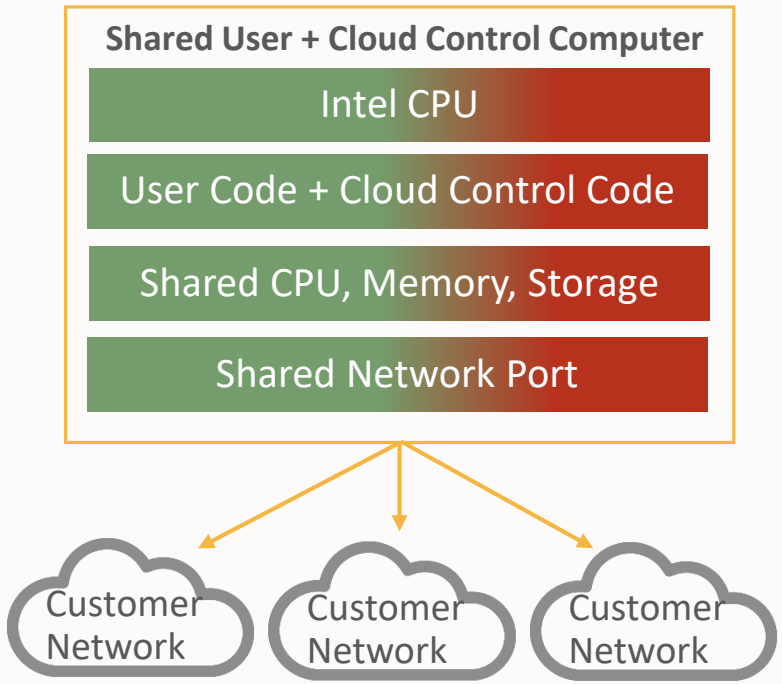
3. Networking Isolation

4. Storage (Object, Block, DB)

Stronger Isolation and Advanced Controls from Core to Edge

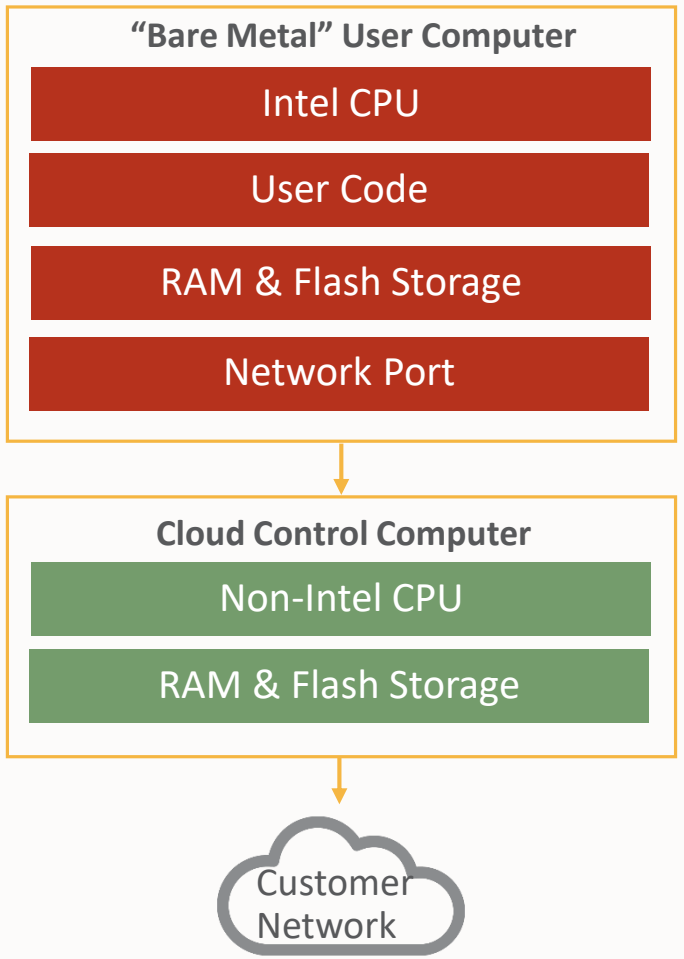
All Gen 1 Clouds
Shared Computers

- Cloud provider can see customer data
- User code can access cloud control code



Oracle Cloud Infrastructure
Separate Cloud Control Computers

✓ Oracle cannot see customer data
✓ No user access to cloud control computer



Security by Design

Architected from the ground up for maximum isolation and protection

Oracle Active Defense

Architected-in full-stack protection

- Secure isolation in OCI
- Least privilege design for OCI
- OCI Hardware root of trust
- Exadata configurations and isolation policies

Automated actions and threat response

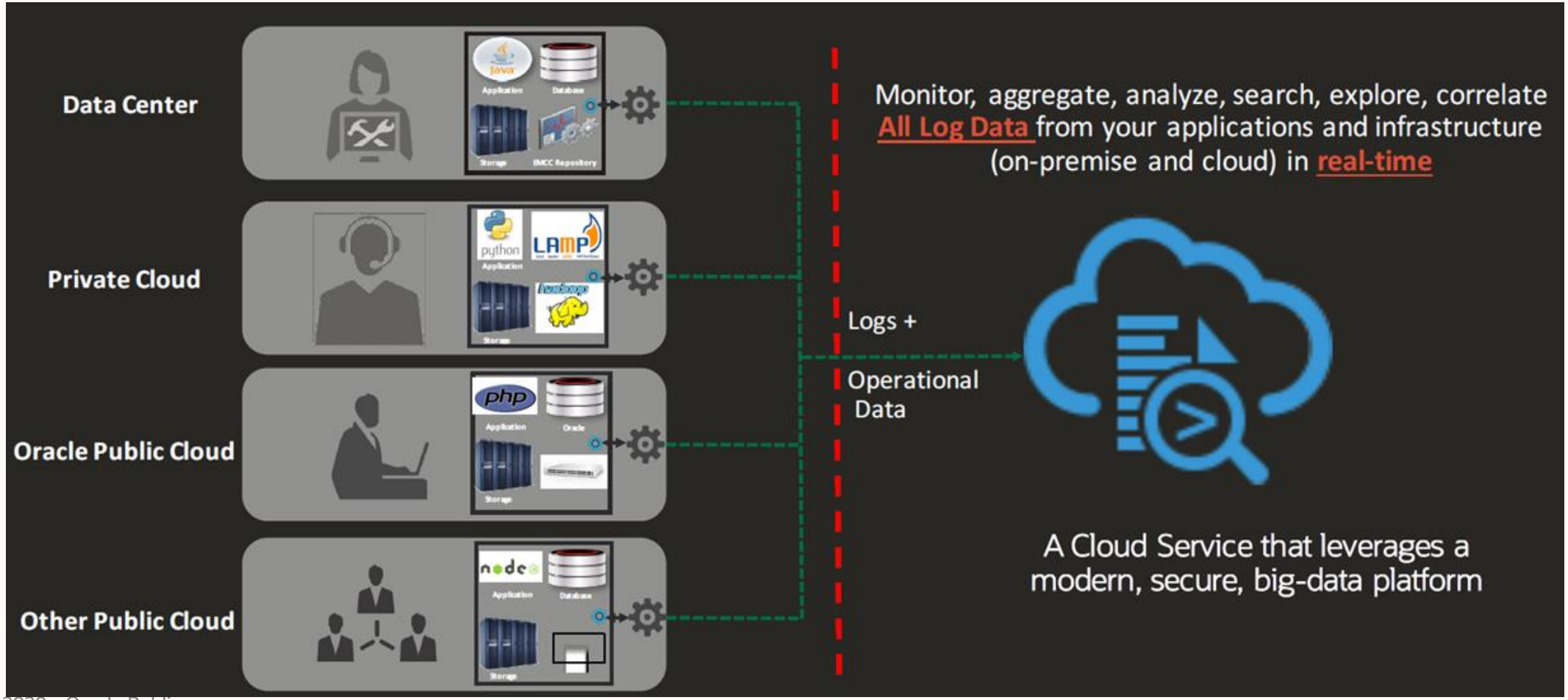
- Automatically identify and remediate user and event anomalies
- Self-Patching Autonomous Database and Autonomous Linux
- Automatic config for strong security posture for cloud infrastructure and database

Always-on for seamless protection

- Default-enabled encryption and TDE encryption
- Activity auditing and monitoring
- Adaptive authentication
- Defense in depth for full stack protection

Optional Operations Management Tool

Oracle Management Cloud Log Analytics (including OCI Logging) to audit access logs



Most of the Learnings Apply to both On-Premise and Cloud

- The vulnerabilities are the same (however, attack surface is bigger and more complex in cloud)
  - Human error, human error, human error
    - in cultural gap
    - in misconfiguration
    - in not understanding the responsibilities in outsource situation
    - in swallowing phising and other social engineering attacks

- Defense steps are mostly the same
  - Integrate security into business flow and app development
  - Streghten Identity and Access Management, Governance
  - Increase Data Security with encryption, key management, super-user control, user auditing and defending sensitive data in ALL environments

Thank You

Gusztáv Szuhai