ORACLE®

Enterprise Trusted Cloud:

Una Responsabilità Condivisa

Angelo Maria Bosis
Solution Engineering Director
Cloud Platform
Oracle Italia

Milan, Oct 31st, 2018

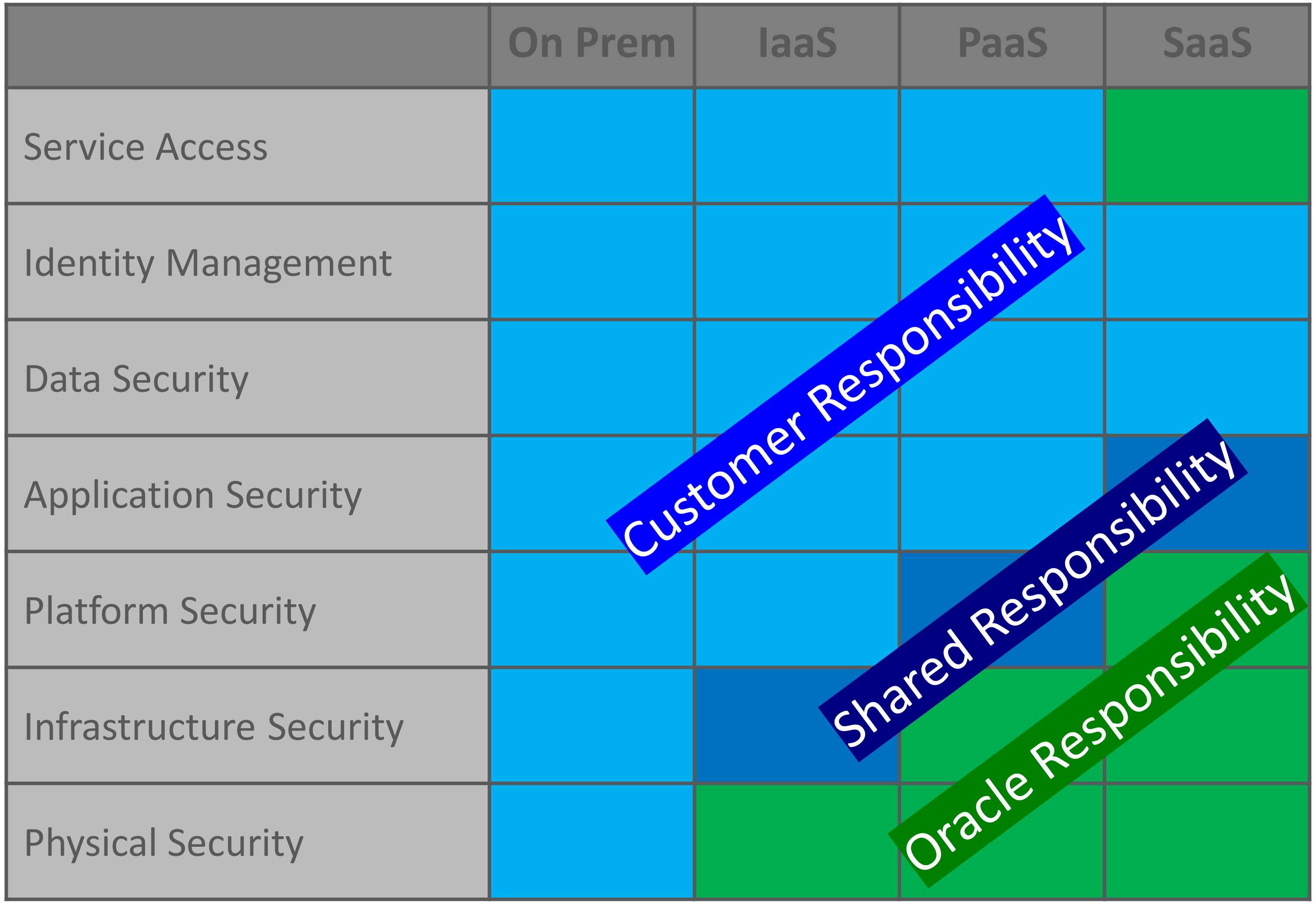
Safe Harbor Statement

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, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

ORACLE®

Shared Responsibility Model

- Security is a **shared** responsibility between the **customer** and the **cloud provider**
- The **cloud provider** is responsible for **the security "of"** the cloud and **customers** are responsible for **their security "on"** the cloud



	On Prem	IaaS	PaaS	SaaS
Service Access	🟦	🟦	🟦	🟩
Identity Management	🟦	🟦	🟦	🟦
Data Security	🟦	🟦	🟦	🟦
Application Security	🟦	🟦	🟦	▨
Platform Security	🟦	🟦	▨	🟩
Infrastructure Security	🟦	▨	🟩	🟩
Physical Security	🟦	🟩	🟩	🟩

🟦 Customer Responsibility

▨ Shared Responsibility

🟩 Oracle Responsibility

Shared Responsibility Model (for IaaS)

Responsibility	Customer	Oracle Cloud Infrastructure

Shared Responsibility Model (for IaaS)

Responsibility	Customer	Oracle Cloud Infrastructure
Physical Security	Not applicable	**Protect the global infrastructure** (hardware, software, networking, and facilities) that runs all of the services in Cloud Infrastructure

ORACLE

Shared Responsibility Model (for IaaS)

Responsibility	Customer	Oracle Cloud Infrastructure
Network Security	**Securely configure** network elements such as virtual networking, load balancing, DNS, and gateways	**Provide secure network** infrastructure
Physical Security	Not applicable	**Protect the global infrastructure** (hardware, software, networking, and facilities) that runs all of the services in Cloud Infrastructure

Shared Responsibility Model (for IaaS)

Responsibility	Customer	Oracle Cloud Infrastructure
Host Infrastructure Security	**Securely configure and manage** compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform services (database configuration)	Ensure that the **service is optimally configured and secured**, including hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices
Network Security	**Securely configure** network elements such as virtual networking, load balancing, DNS, and gateways	**Provide secure network** infrastructure
Physical Security	Not applicable	**Protect the global infrastructure** (hardware, software, networking, and facilities) that runs all of the services in Cloud Infrastructure

Shared Responsibility Model (for IaaS)

Responsibility	Customer	Oracle Cloud Infrastructure
Data Classification and Compliance	**Correctly classify and label data** and meet compliance requirements; **audit solutions** to meet compliance requirements	**Provide compliance reports** for underlying infrastructure
Host Infrastructure Security	**Securely configure and manage** compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform services (database configuration)	Ensure that the **service is optimally configured and secured**, including hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices
Network Security	**Securely configure** network elements such as virtual networking, load balancing, DNS, and gateways	**Provide secure network** infrastructure
Physical Security	Not applicable	**Protect the global infrastructure** (hardware, software, networking, and facilities) that runs all of the services in Cloud Infrastructure

ORACLE

Shared Responsibility Model (for IaaS)

Responsibility	Customer	Oracle Cloud Infrastructure
Workload Security	**Patch** apps and OS, configure OS, and **protect against** malware and network **attacks**	**Secure images** and make it simple for customers to bring existing **third-party security solutions**
Data Classification and Compliance	**Correctly classify and label data** and meet compliance requirements; **audit solutions** to meet compliance requirements	**Provide compliance reports** for underlying infrastructure
Host Infrastructure Security	**Securely configure and manage** compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform services (database configuration)	Ensure that the **service is optimally configured and secured**, including hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices
Network Security	**Securely configure** network elements such as virtual networking, load balancing, DNS, and gateways	**Provide secure network** infrastructure
Physical Security	Not applicable	**Protect the global infrastructure** (hardware, software, networking, and facilities) that runs all of the services in Cloud Infrastructure

Shared Responsibility Model (for IaaS)

Responsibility	Customer	Oracle Cloud Infrastructure
Identity and Access Management	**Protect** credentials and manage access	**Provide** effective and easy-to-use **identity management**, authentication, authorization, and auditing **solutions**
Workload Security	**Patch** apps and OS, configure OS, and **protect against** malware and network **attacks**	**Secure images** and make it simple for customers to bring existing **third-party security solutions**
Data Classification and Compliance	**Correctly classify and label data** and meet compliance requirements; **audit solutions** to meet compliance requirements	**Provide compliance reports** for underlying infrastructure
Host Infrastructure Security	**Securely configure and manage** compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform services (database configuration)	Ensure that the **service is optimally configured and secured**, including hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices
Network Security	**Securely configure** network elements such as virtual networking, load balancing, DNS, and gateways	**Provide secure network** infrastructure
Physical Security	Not applicable	**Protect the global infrastructure** (hardware, software, networking, and facilities) that runs all of the services in Cloud Infrastructure

Shared Responsibility Model (for IaaS)

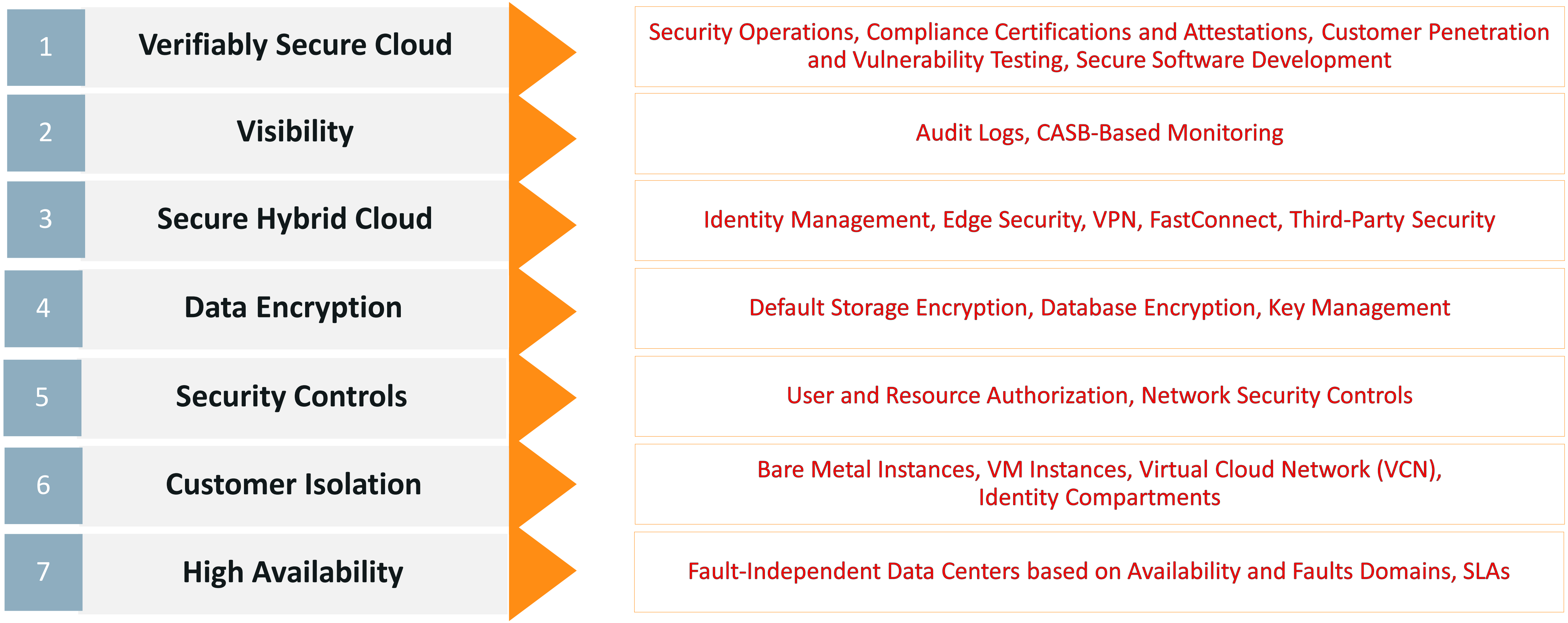
Responsibility	Customer	Oracle Cloud Infrastructure
Client and End-Point Protection	**Secure all clients and endpoints** that are used to access Cloud Infrastructure services	Not applicable
Identity and Access Management	**Protect** credentials and manage access	**Provide** effective and easy-to-use **identity management**, authentication, authorization, and auditing **solutions**
Workload Security	**Patch** apps and OS, configure OS, and **protect against** malware and network **attacks**	**Secure images** and make it simple for customers to bring existing **third-party security solutions**
Data Classification and Compliance	**Correctly classify and label data** and meet compliance requirements; **audit solutions** to meet compliance requirements	**Provide compliance reports** for underlying infrastructure
Host Infrastructure Security	**Securely configure and manage** compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform services (database configuration)	Ensure that the **service is optimally configured and secured**, including hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices
Network Security	**Securely configure** network elements such as virtual networking, load balancing, DNS, and gateways	**Provide secure network** infrastructure
Physical Security	Not applicable	**Protect the global infrastructure** (hardware, software, networking, and facilities) that runs all of the services in Cloud Infrastructure

ORACLE

The 7 Pillars of a Trusted Enterprise Cloud Platform

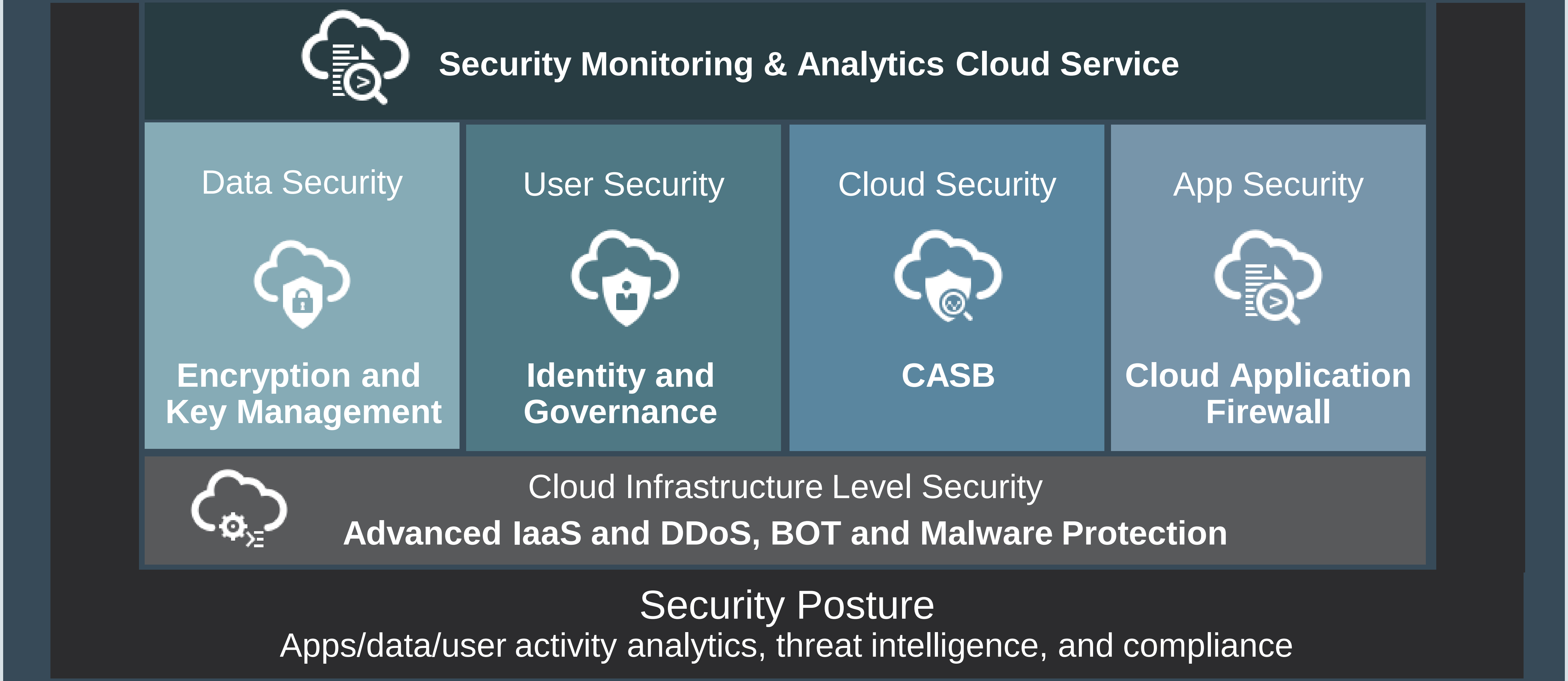
1	**Verifiably Secure Cloud**	Transparency about processes and internal security controls | Third-party audits and certifications | Customer pen-testing and vulnerability scanning | Jointly demonstrated compliance
2	**Visibility**	Provide log data and security analytics for auditing and monitoring actions on customer assets
3	**Secure Hybrid Cloud**	Enable customers to use their existing security assets | Integrate with on-premise or cloud security solutions | Support for third-party security solutions
4	**Data Encryption**	Meet compliance requirements regarding data encryption, cryptographic algorithms, and key management
5	**Security Controls**	Effective and easy-to-use security management to constrain access and segregate operational responsibilities
6	**Customer Isolation**	Full isolation from other tenants and Cloud Provider’s staff, and between a tenant’s workloads
7	**High Availability**	Fault-independent data centers that enable high-availability scale-out architectures and are resilient against attacks

Oracle Cloud Security Capabilities at a Glance



1	**Verifiably Secure Cloud**	Security Operations, Compliance Certifications and Attestations, Customer Penetration and Vulnerability Testing, Secure Software Development
2	**Visibility**	Audit Logs, CASB-Based Monitoring
3	**Secure Hybrid Cloud**	Identity Management, Edge Security, VPN, FastConnect, Third-Party Security
4	**Data Encryption**	Default Storage Encryption, Database Encryption, Key Management
5	**Security Controls**	User and Resource Authorization, Network Security Controls
6	**Customer Isolation**	Bare Metal Instances, VM Instances, Virtual Cloud Network (VCN), Identity Compartments
7	**High Availability**	Fault-Independent Data Centers based on Availability and Faults Domains, SLAs

Oracle Cloud Security & Identity Platform



Security Monitoring & Analytics Cloud Service

Data Security

Encryption and Key Management

User Security

Identity and Governance

Cloud Security

CASB

App Security

Cloud Application Firewall

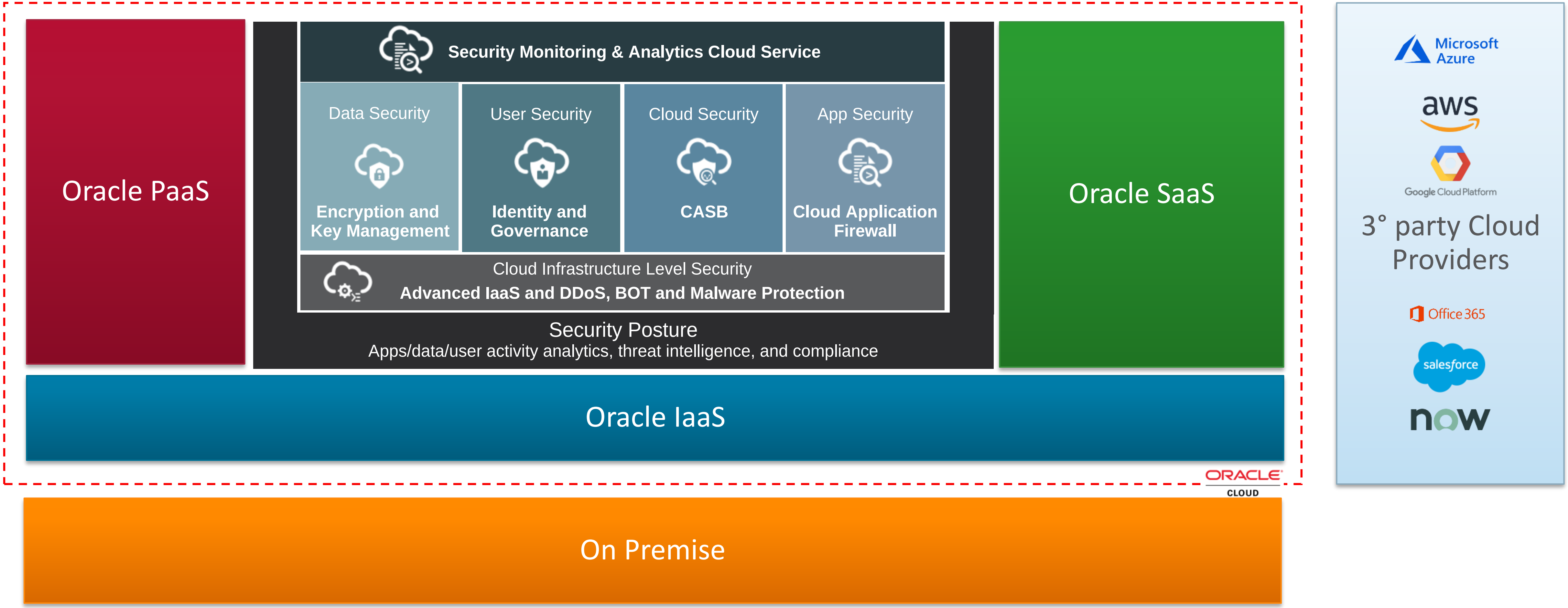
Cloud Infrastructure Level Security

Advanced IaaS and DDoS, BOT and Malware Protection

Security Posture

Apps/data/user activity analytics, threat intelligence, and compliance

Oracle Cloud Security & Identity Platform



Oracle PaaS

Security Monitoring & Analytics Cloud Service

Data Security
Encryption and Key Management

User Security
Identity and Governance

Cloud Security
CASB

App Security
Cloud Application Firewall

Cloud Infrastructure Level Security
Advanced IaaS and DDoS, BOT and Malware Protection

Security Posture
Apps/data/user activity analytics, threat intelligence, and compliance

Oracle SaaS

Oracle IaaS

ORACLE CLOUD

On Premise

Microsoft Azure

aws

Google Cloud Platform

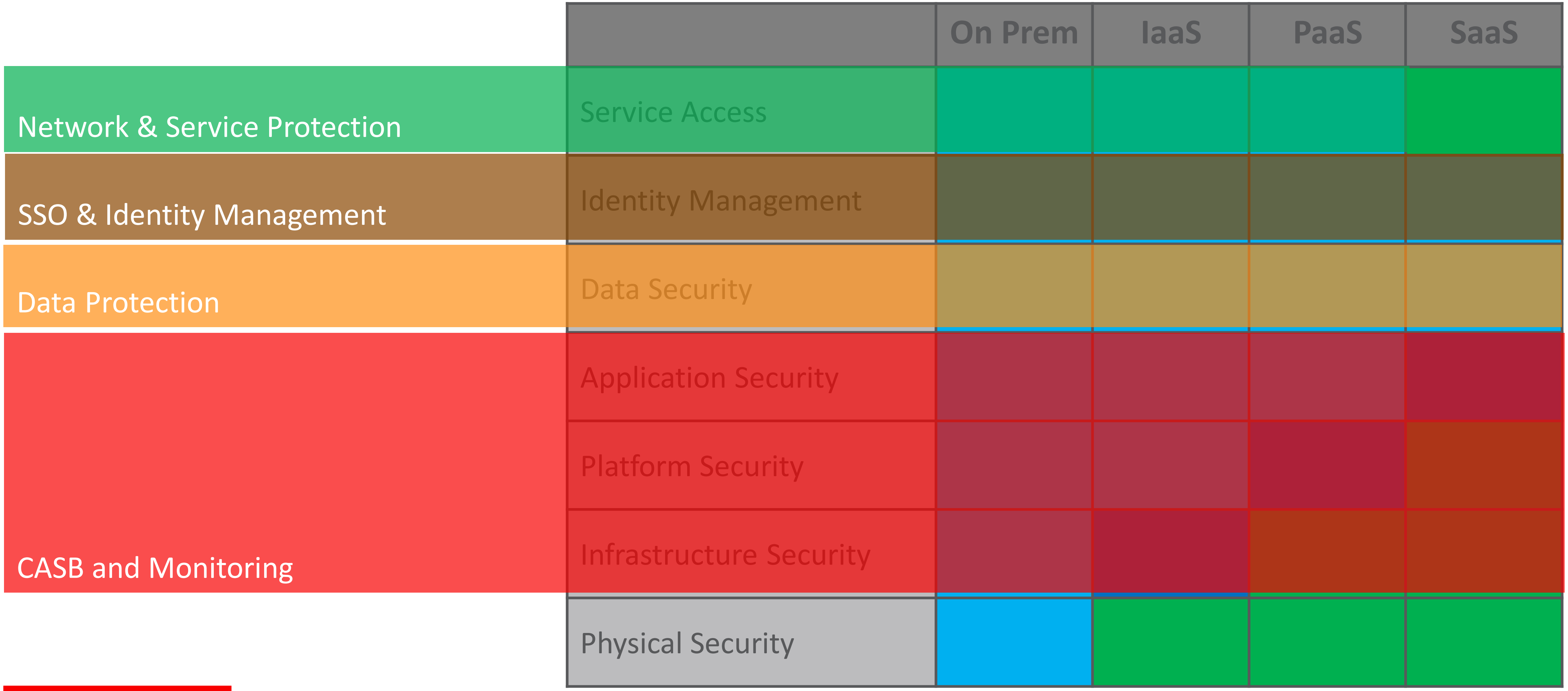
3° party Cloud Providers

Office 365

salesforce

now

A Trusted Cloud in a Shared Responsibility Model



		On Prem	IaaS	PaaS	SaaS
Network & Service Protection	Service Access				
SSO & Identity Management	Identity Management				
Data Protection	Data Security				
CASB and Monitoring	Application Security				
	Platform Security				
	Infrastructure Security				
	Physical Security				

Oracle **Cloud** Day

Your Future Runs on Cloud

22 novembre 2018
MiCo, Milano Congressi

www.oracle.com/it/cloudday

ORACLE

Integrated Cloud

Applications & Platform Services

ORACLE®

ORACLE®