Informatica

19 October 2022

# Architect Workshop

## *Cloud Data Management Security*

*What are critical Security considerations for adopting Cloud Data Management solutions at Enterprises?*

Deloitte.

# Agenda

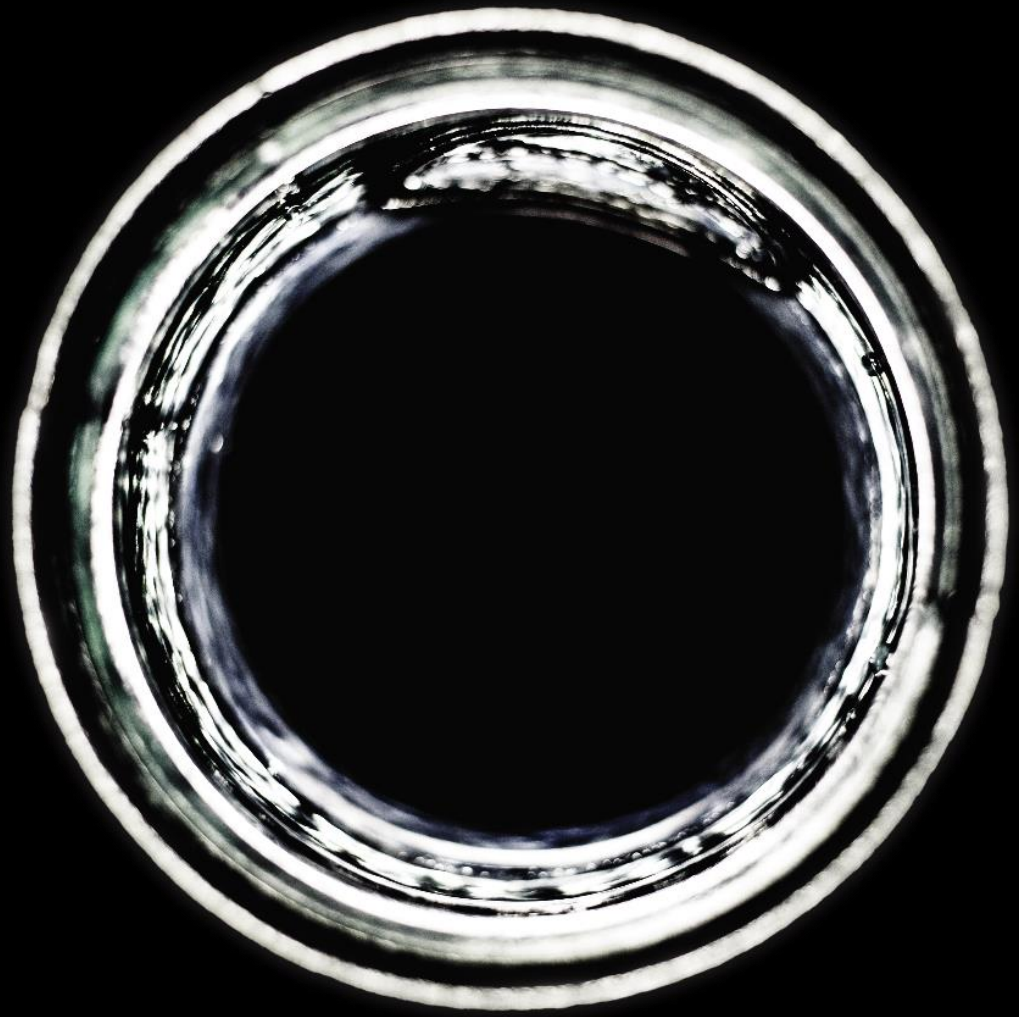
1. Security in Cloud Data Management companies
2. Compliance of IDMC technology with the highest security standards
3. Discussion on Cloud Security Aspects
4. Q&A



Informatica

Deloitte.

Informatica



# Cloud Security Awareness

# Agenda

- Introduction to the Cloud
- Cloud Adoption: main impacts, threats and risks
- The importance of the Cloud Security

# Agenda

- **Introduction to the Cloud**
- Cloud Adoption: main impacts, threats and risks
- The importance of the Cloud Security

# Introduction to the Cloud

The term **Cloud Computing**, or simply **Cloud**, refers to a set of technologies and ways of using computer services that facilitate the use and delivery of software and the ability to store and process large amounts of data via Internet.

The Cloud offers, as depending on the cases, the transfer of data storage or data processing from users' computers to the provider's systems.

Cloud services can be delivered through **three different Service Models:**

**IaaS**
(Infrastructure as a Service)

amazon web services EC2 · Azure · Google Cloud

Cloud infrastructure **made available as a service**. The cloud service provider offers, on a "pay-as-you-go" model, the hardware and software tools (i.e. operating systems), which are considered remote virtual servers that the user can use as a substitute or alongside the systems already present on company or administration premises.

**PaaS***
(Platform as a Service)

heroku · salesforce force.com

Software **delivered as a cloud service**. The provider delivers via Internet a set of application services by making them available to the user. For example, applications commonly used in offices delivered in Web mode such as contact address book and shared calendars, but also to more advanced e-mail services.

**SaaS***
(Software as a Service)

Office 365 · workday. · G Suite · servicenow · Dropbox · slack

Software platforms **delivered via Internet as a service.** The provider offers advanced software development solutions that meet the specific needs of the customer. In general, this type of service is aimed at market players who use them to develop and host their own application solutions for the purpose of fulfilling internal needs.

**In case of PaaS and SaaS, the service provided requires the user to have to equip themselves internally with **specific or additional hardware or software tools***

# Deployment Models in the Cloud

Cloud services can be delivered through **four different Deployment Models.** These models describe how services (or technologies) are deployed and are applicable to all Service Models (IaaS, PaaS and SaaS):

### Private Cloud

The environment is **entirely dedicated to a single organization** (primarily IaaS).
It can be compared to traditional "data centers"

### Public Cloud*

The Cloud infrastructure is set up **to be freely used by the public** (i.e. Amazon AWS)

### Hybrid Cloud

**Combination of private and public cloud** integrated with each other (i.e. private cloud & Salesforce)

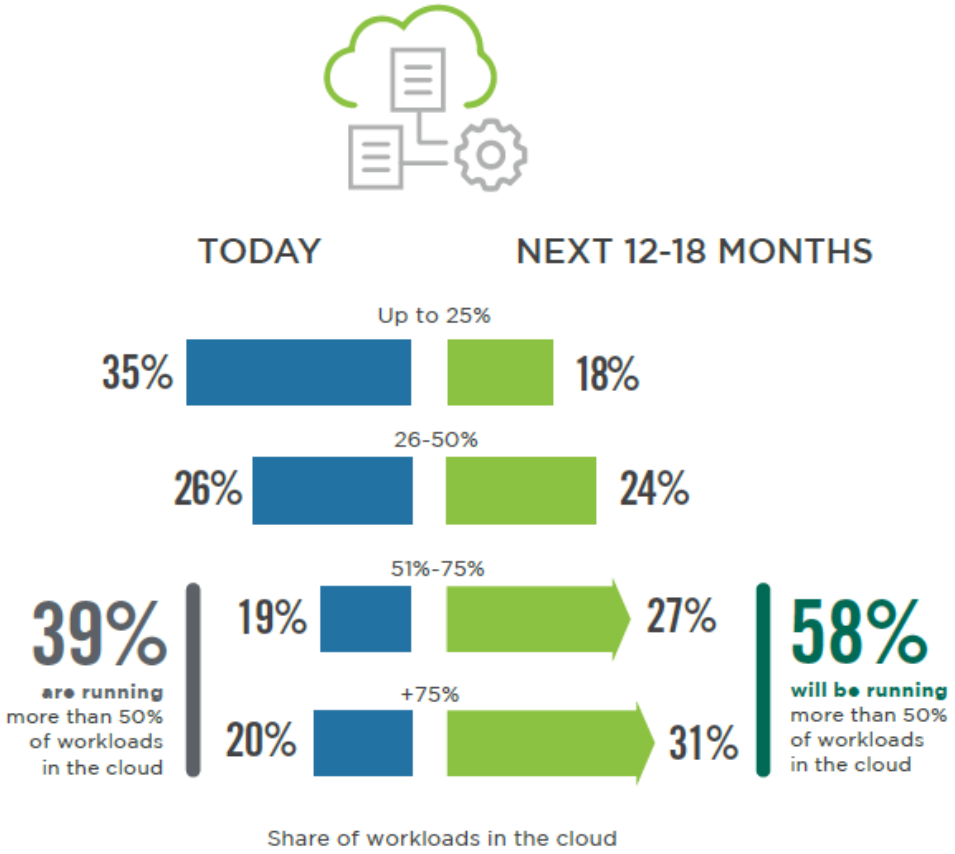
### Community Cloud

Cloud shared **by a specific sector or group of organizations**, usually temporary in nature (i.e. PlayStation network)

**The use of Public Cloud implies the transfer of processing or data only to the systems of the service provider, which assumes an important role with regard to the **effectiveness of the measures taken to ensure the protection of the data!***

# Some Insights: Workloads in the Cloud

Organizations continue to shift workloads to the cloud at a rapid pace. According to the 2022 Cloud Security Report of (ISC)[2], today the 39% of the organizations have more than half of their workloads in the Cloud, while the **58% plan to make this shift in the next 12-18 months**.




*(ISC)[2] is an international nonprofit membership association focused on inspiring a safe and secure cyber world.*

# Agenda

- Introduction to the Cloud
- **Cloud Adoption: main impacts, threats and risks**
- The importance of the Cloud Security

# Main Impacts of the Cloud Adoption

The adoption of the Cloud impacts organizations in their entirety. In order to take full advantage of its benefits, it is necessary to adapt **organizational structure, processes and technologies** by ensuring a coherent evolution with the new approach:

## Architecture & Infrastructure

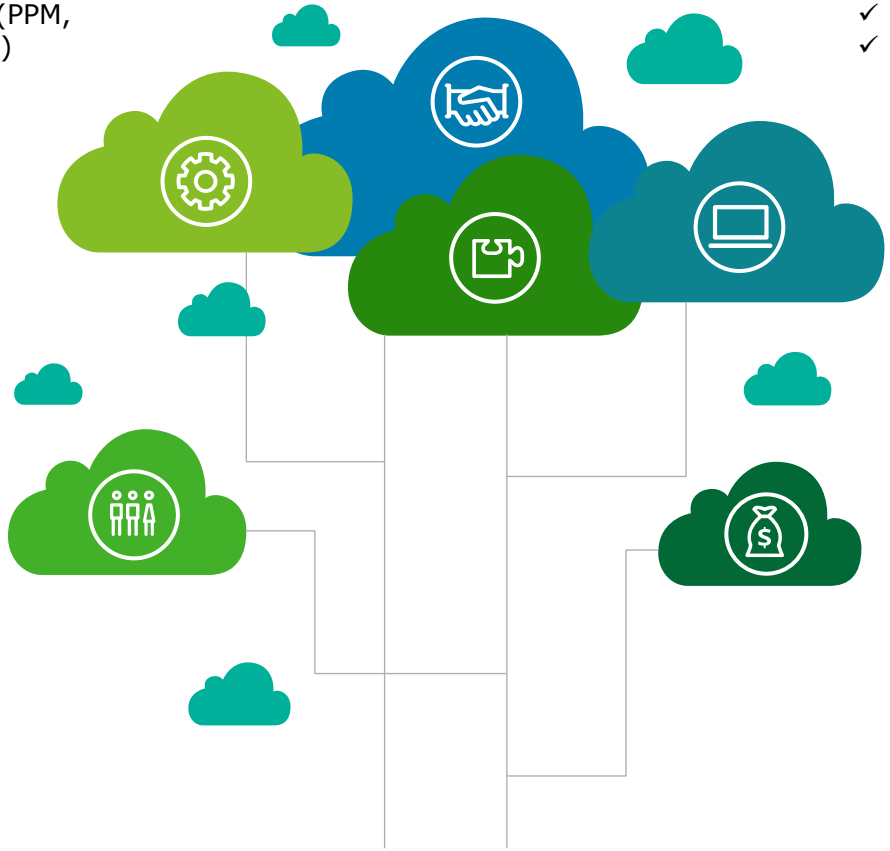
- ✓ Definition of **standard architectures**
- ✓ Integration with **application and infrastructure monitoring tools**
- ✓ Integration with **enterprise ITSM** (PPM, Incident Mgmt, Configuration Mgmt)

## Operating Model

- ✓ Review of the **operating model**
- ✓ Definition of the **Governance model**
- ✓ Definition of **processes and procedures** for Cloud Governance
- ✓ **Review of software development processes**
- ✓ Definition of **Cloud service brokerage** to the business

## People

- ✓ Evaluation of the **skills needed**
- ✓ Definition **of roles *ad hoc* for Cloud Governance**
- ✓ **Hiring & Retention**
- ✓ **Change Management**
- ✓ **Training Courses & Knowledge** Sharing



## Partner / Ecosystem Model

- ✓ Cloud Service **Provider Management**
- ✓ Review of Service **Level Management policies**
- ✓ **Vendor Management**
- ✓ **Ecosystems & Alliances** management

## Application Portfolio

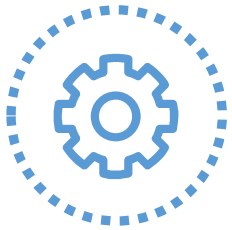
- ✓ Evaluation of applications **suitable for the Cloud**
- ✓ **Migration Roadmap**
- ✓ **Application Modernization**
- ✓ **Execution of the migration**
- ✓ Monitoring and control of **migrated applications and workloads**

## Financial Management

- ✓ Integration with **IT Financial Management processes**
- ✓ **Business Case / TCO** Evaluation
- ✓ **Investment estimates / projections** on the use of Cloud solutions in the business budgeting process
- ✓ **ROI Evaluation**

# Biggest Security Threats in the Cloud

Cloud adoption is also characterized by the following **most common Cloud Security threats***:



***62%***

**Misconfiguration of the cloud platform/wrong setup**

***54%***

**Insecure interfaces/APIs**

***51%***

**Exfiltration of sensitive data**

***50%***

**Unauthorized access**

***44%***

**Hijacking of accounts, services, or traffic**

***39%***

**External sharing of data**

***37%***

**Foreign state-sponsored cyber attacks**

**According to the 2022 Cloud Security Report of (ISC)[2]*

# Focus on Data Security Risks in the Cloud

The presence of common threats that can affect the Cloud world, can often lead to the **materialization of significant Data Security Risks**, such as:


**LEGEND**

*In-flight: During the migration phase*

*Arrival: Fully adopted*

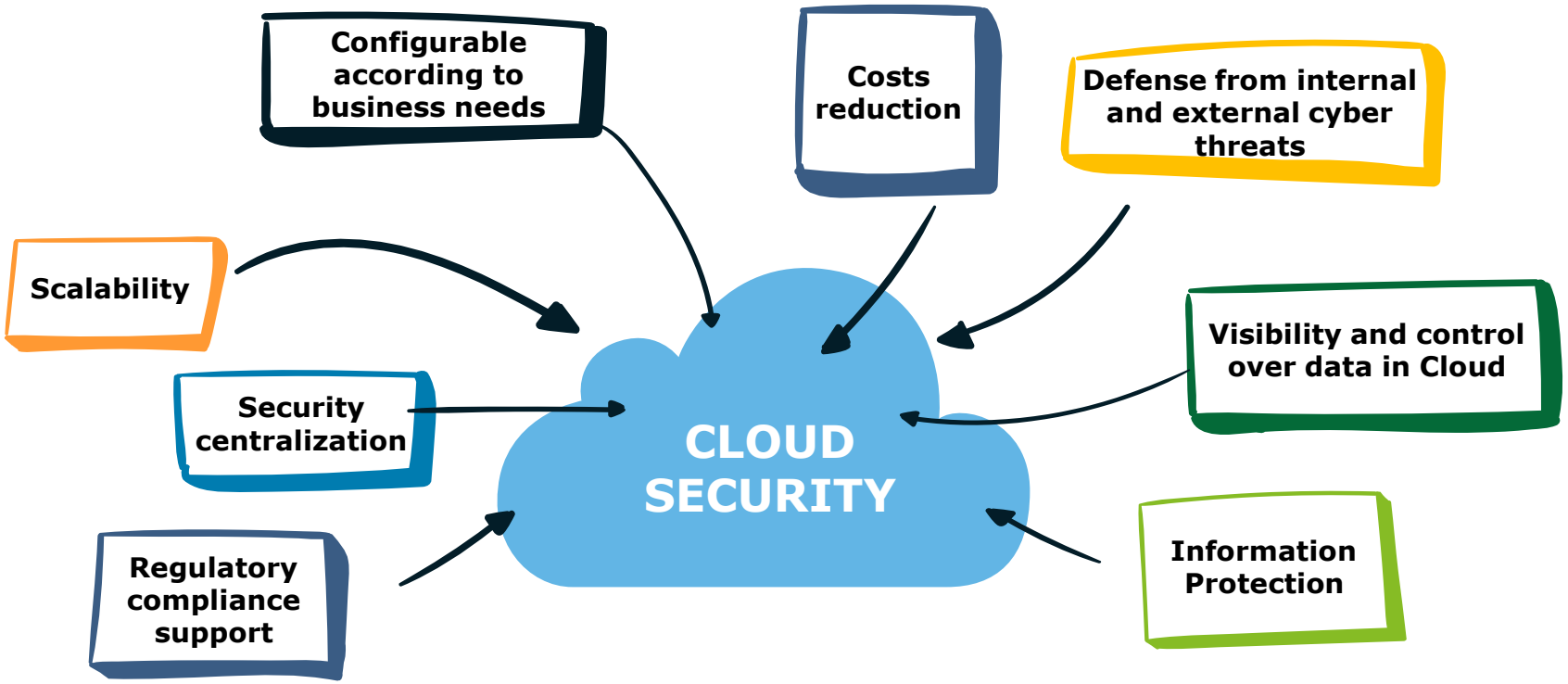
# Agenda

- Introduction to the Cloud
- Cloud Adoption: main impacts, threats and risks
- **The importance of the Cloud Security**

# Cloud Security: a way to handle the ever-changing security needs

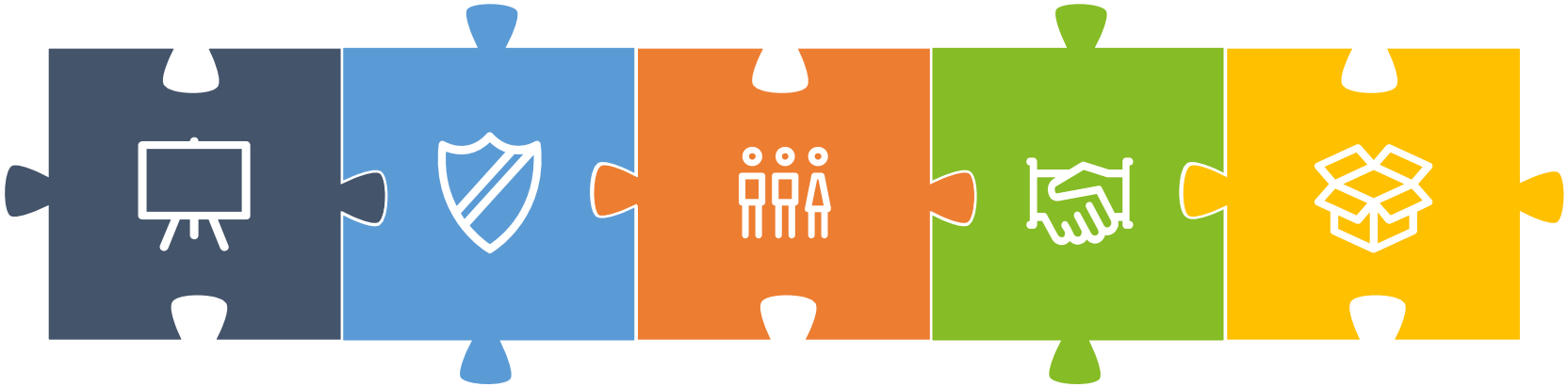
Cloud Security consists of a **set of policies, controls, procedures, and technologies designed to protect cloud-based systems, data, and infrastructure.** These security measures are configured to protect information, support regulatory compliance, protect customer privacy, and set specific authentication rules for individual users and devices.

Here below, **some benefits of the Cloud Security**:



# Ever-changing security needs: Common Responses

When moving to the Cloud, **how practically the Organizations can handle their ever-changing security needs?** Here below some common responses* from the market:



**Training and/or certifying existing IT staff**

**Using native and secure Cloud provider security tools (i.e. Informatica)**

**Hiring staff dedicated to cloud security**

**Partner with a Managed Security Services Provider (MSSP)**

**Deploying security software from independent vendors**

**According to the 2022 Cloud Security Report of (ISC)²*

# Ever-changing security needs: Main Technical Measures

Finally, it's important to highlight that in order to handle the ever-changing security needs, it's also necessary that the Organization takes actions in implementing **Technical Measures in order to make the Cloud more secure, such as**:

## MAIN TECHNICAL MEASURES

**Data Encryption**
Cloud data encryption can be used to ***prevent unauthorized access to data, even if that data is exfiltrated or stolen***.

**Identity and Access Management (IAM)**
Access control tools (password management solutions, multi-factor authentication, etc.) ***assume a key role in limiting the compromise of data, systems and platforms by users***. Indeed, such solutions make possible to manage and monitor the behavior of those accessing resources, preventing access by unauthorized or malicious parties.

**Data Backup**
It's crucial to have a ***contingency plan in place should anything happen to data***, such as data loss.

**Disaster Recovery**
Provide organizations with the tools, services, and protocols necessary to expedite the recovery of ***lost data and resume normal business operations.***

**Data Loss Prevention (DLP)**
Use a combination of ***remediation alerts, data encryption, and other preventative measures to protect all stored data***, whether at rest or in motion.

2022

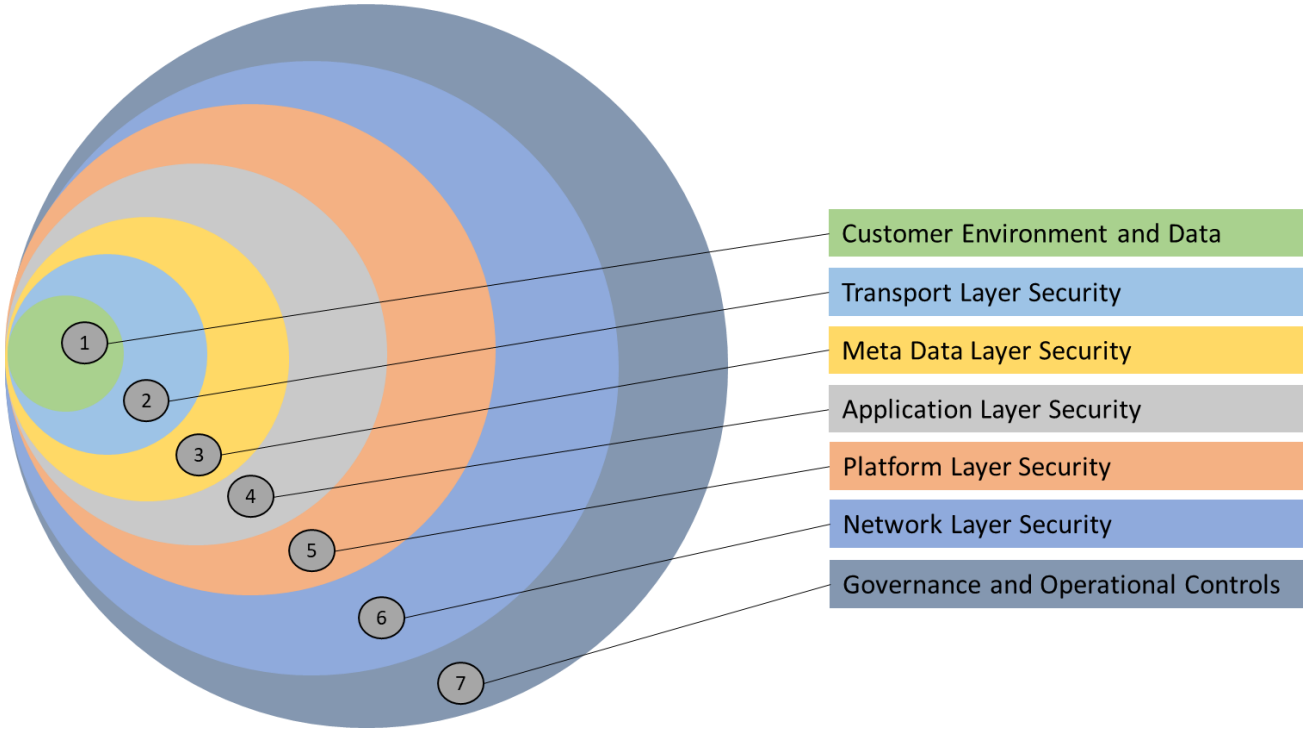
# IDMC Security Overview

Informatica

# IDMC Security and Defense in Depth

## Shared Responsibility Cloud Security Model

The level of security provided for customers and their data is achieved not through a single control, but through **multiple, overlapping layers**. Informatica embeds security in **every layer of the infrastructure stack** and in every aspect of accessing and processing cloud integration data.

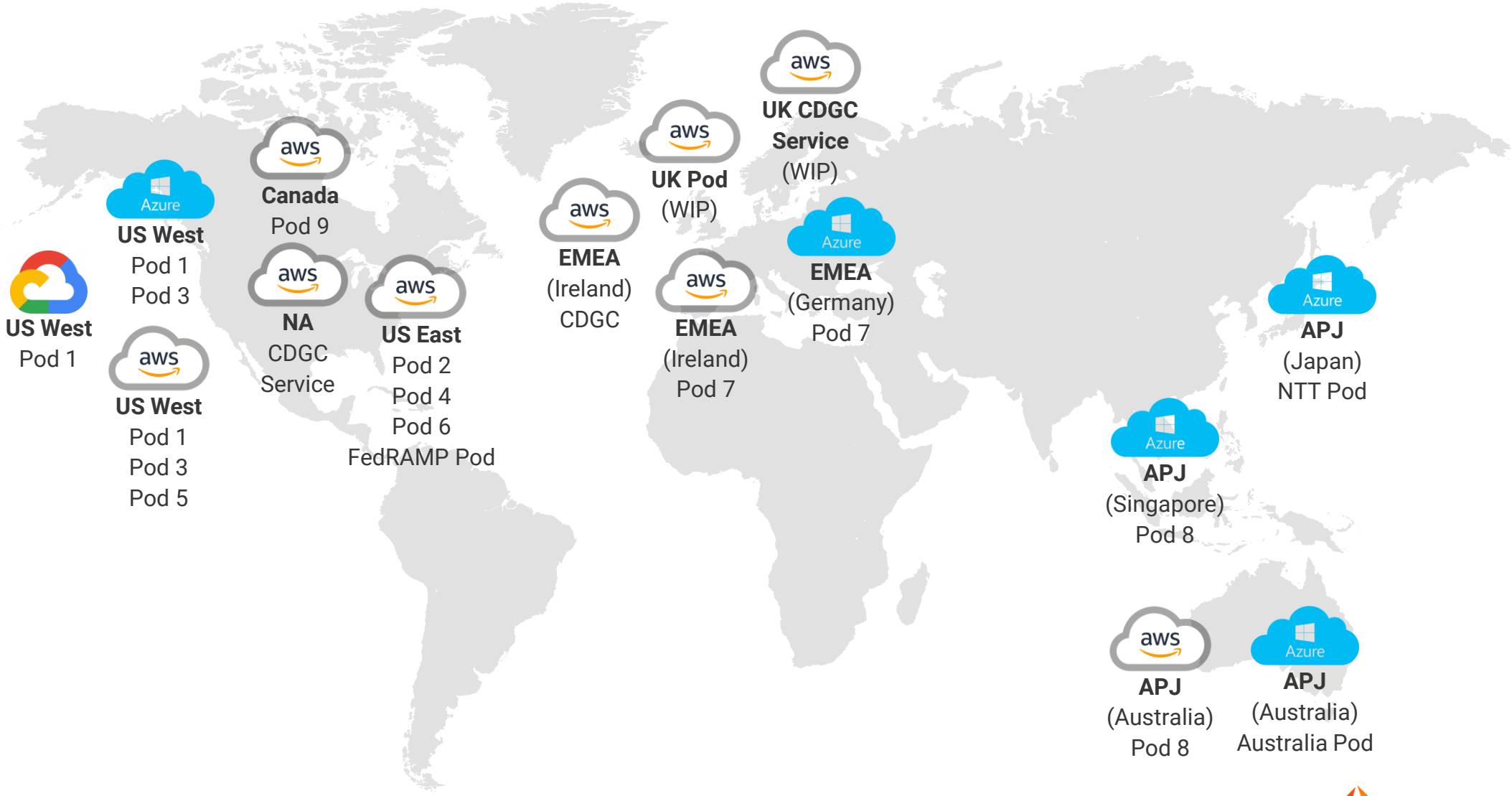







Informatica

# Informatica PODs Globally

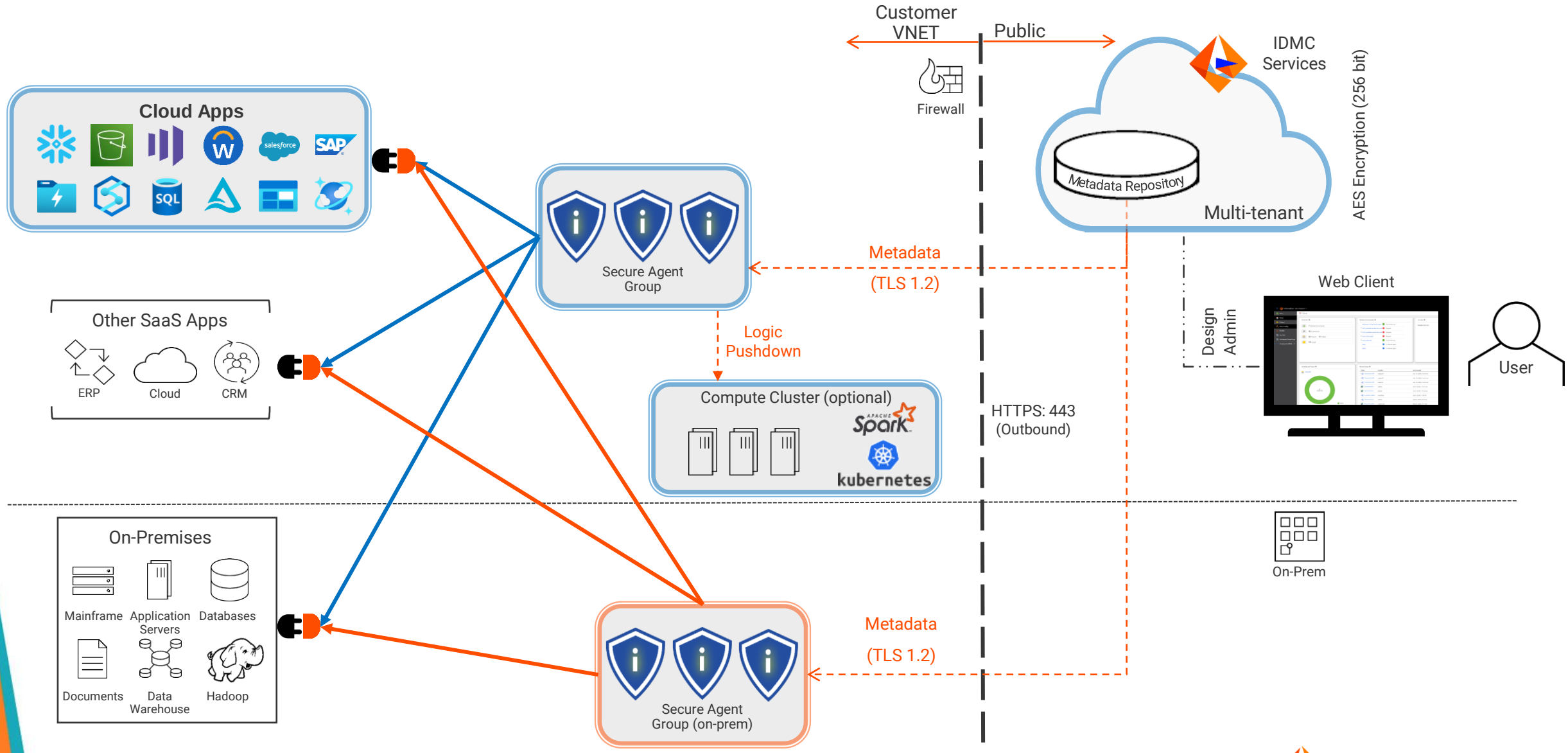







Informatica

# Network Architecture








Informatica

# Informatica Software And Development Practices

## Informatica SDLC Practices

- **Security Architecture Design Reviews**
- **Secure Coding Procedures:** Documentation, testing, reviews. change controls to our software. Follow OWASP standards.
- **Manual Code Reviews:** Functional and design reviews, manual code reviews by lead engineers/architects. Automated notifications at check-in.
- **Vulnerability and License Compliance:** Static, Dynamic, Third-Party Library source code analysis; risk-based remediation.
- **Manual Penetration Testing:** Trusted third-parties every major product release, Informatica teams every minor release.
- **Responsible Disclosure Program:** Security researcher discrete disclosure and Hall Of Fame.

**Secure Software Development Lifecycle**






Informatica

# Certifications and Independent Verifications

Third-party attestations, memberships, and industry certifications relevant to the IDMC platform


Additionally, Informatica partners with 3rd party consulting and security expert firms to assess IDMC security performing analysis, penetration and vulnerability tests…

Deloitte.

nccgroup

CROWDSTRIKE

hackerone

MANDIANT

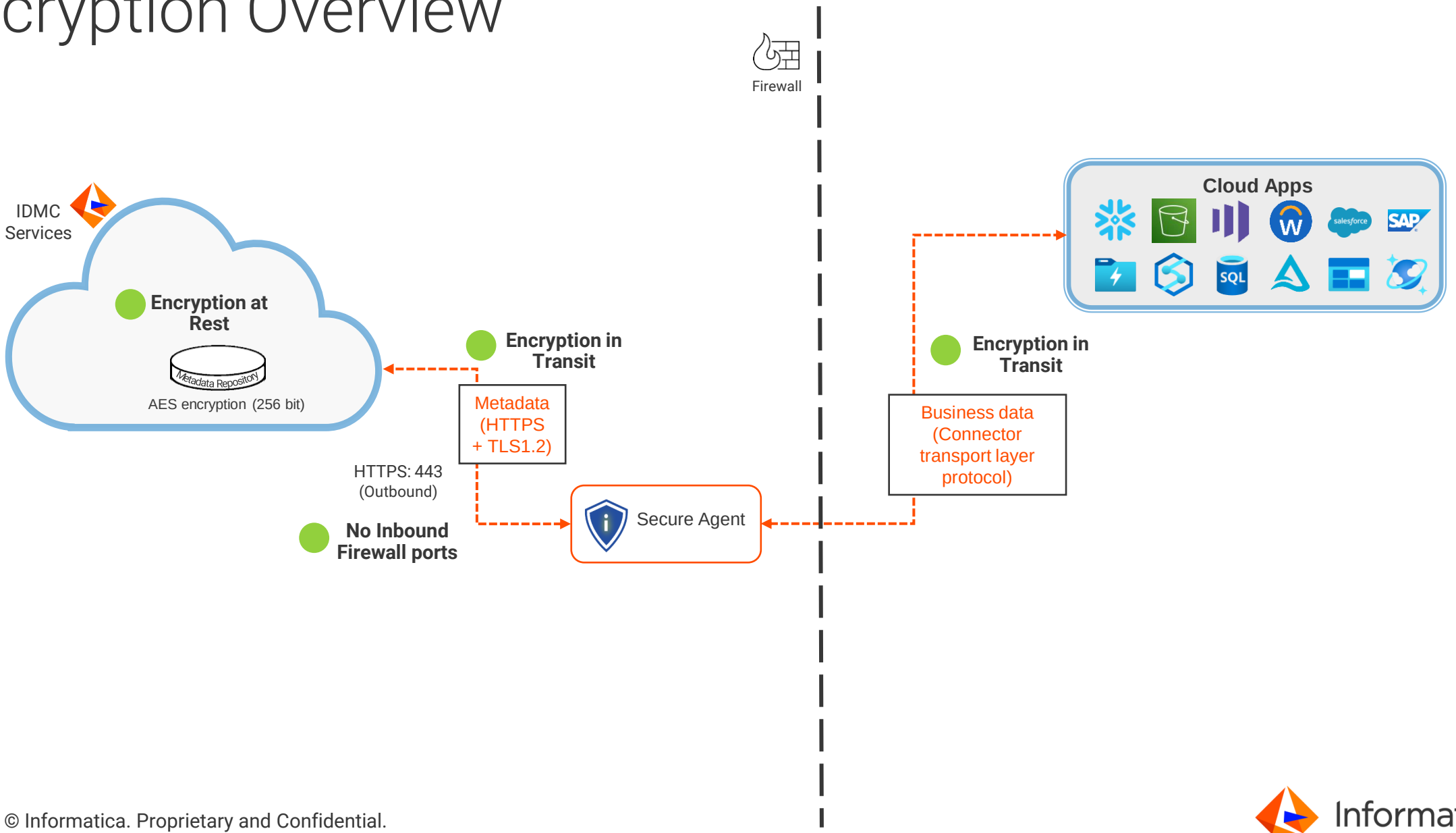
schellman
Quality, above all.





Informatica

# Encryption Overview





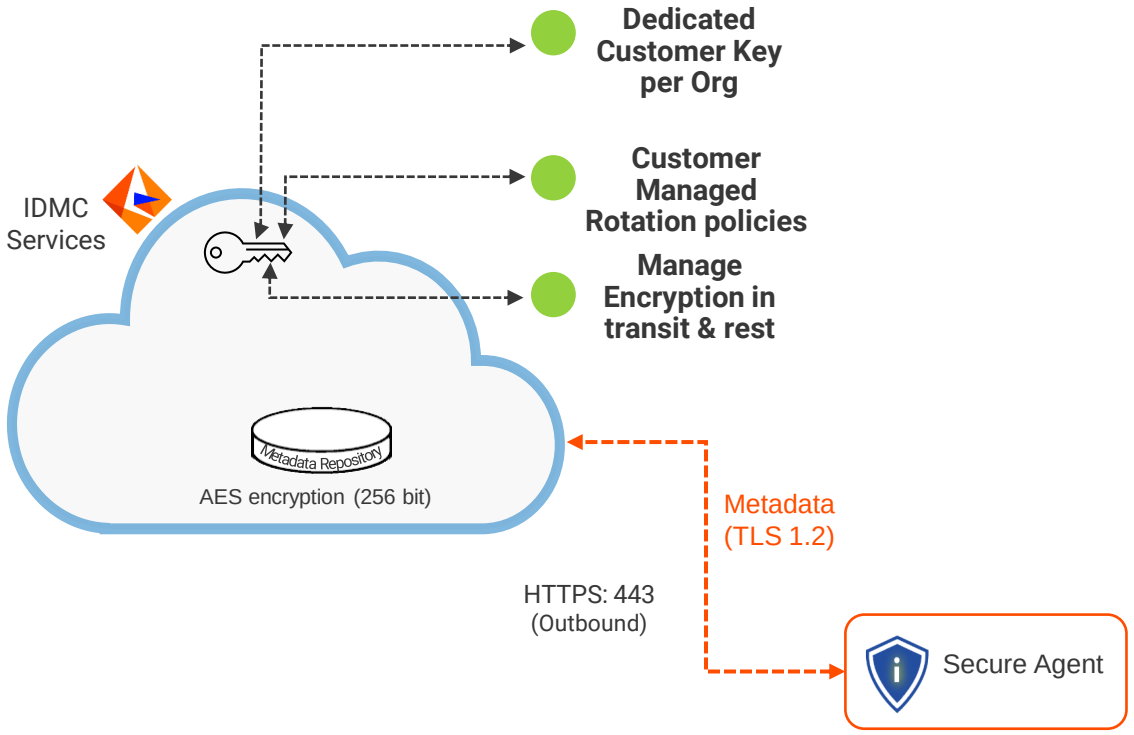



Informatica

# Encryption Protocols

- Encryption keys are stored in our internal database in encrypted form
- Secure Agent authenticates with the IDMC host first using a 10 SSL handshake and a digital certificate
- All communication from the Secure Agent to the IDMC host is TLS 1.2 encrypted using AES256-SHA (256 bit) cipher
- Encryption in Transit is unique per Secure Agent and each IDMC Service
- When connecting to sources/targets via connectors, Informatica leverages the underlying transport layer of these connector communication protocols. Customer data is transmitted encrypted via Transport Layer Security (TLS) using AES (256 bit) cipher
- No inbound firewall ports needed
  - The Secure Agent creates a virtual socket connection to communicate to IDMC through port 443 for all outbound communication

# Key Management Overview




- IICS uses Organization-level AES-256 symmetric encryption keys (Tenant Keys) to encrypt sensitive data at rest and in transit. These Tenant Keys are rotated once a year in conformance with NIST 800-57 Part 1 Rev 5 guidelines
- Additionally, we have a feature in which the customer can manage the current keys via API
  - CUSTOMER can initiate and adjust the rotation intervals

## Changing key rotation intervals

**You can use the key resource to change the key rotation interval for the organization.**

### PATCH request

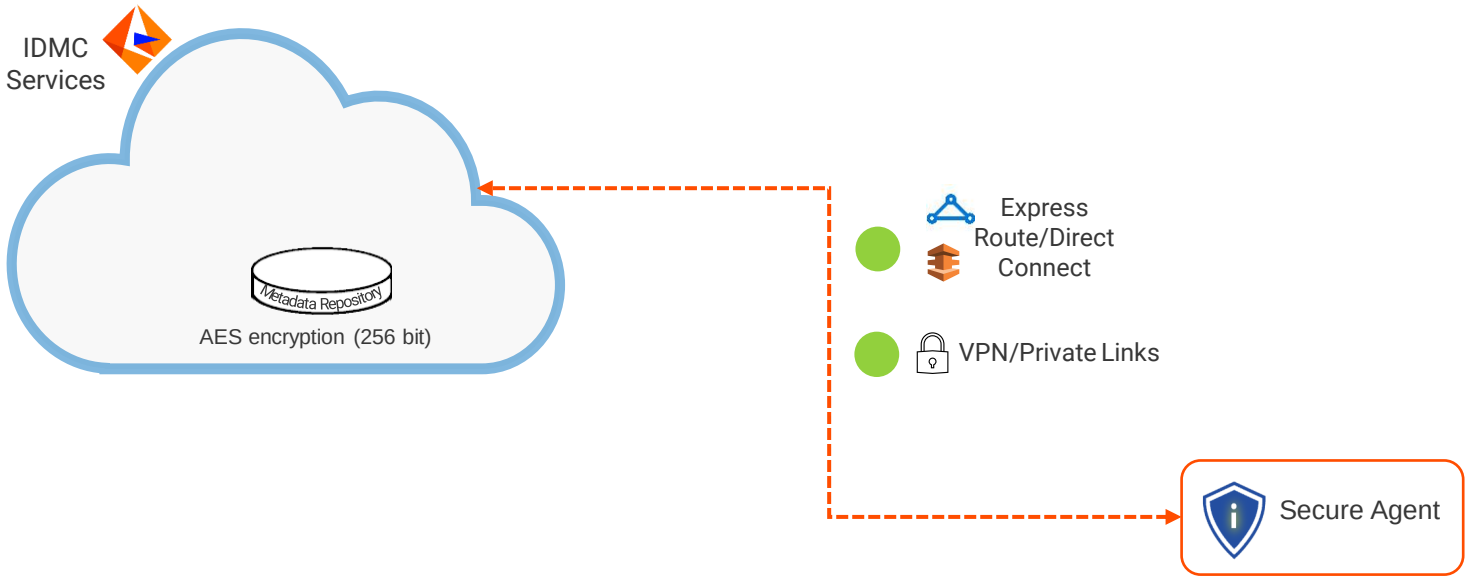
To change the key rotation interval, send a PATCH request using the following URI:

```
/public/core/v3/key/rotationSettings
```

Include the following information:

| Field | Type | Required | Description |
|---|---|---|---|
| rotationInterval | String | Yes | The key rotation interval to use for the organization. Use one of the following values:<br>• 90_DAYS<br>• 120_DAYS<br>• 180_DAYS<br>• 365_DAYS<br>Default is 365_DAYS. |

# Private Connectivity




**ExpressRoute** lets you create private connections between Azure datacenters and infrastructure that's on your premises or in a co-location environment

**DirectConnect** lets you create private connections between AWS datacenters and infrastructure that's on your premises or in a co-location environment

**VPN/Private Links** are point to point connections between infrastructures that maybe on your premises or in a co-location environment

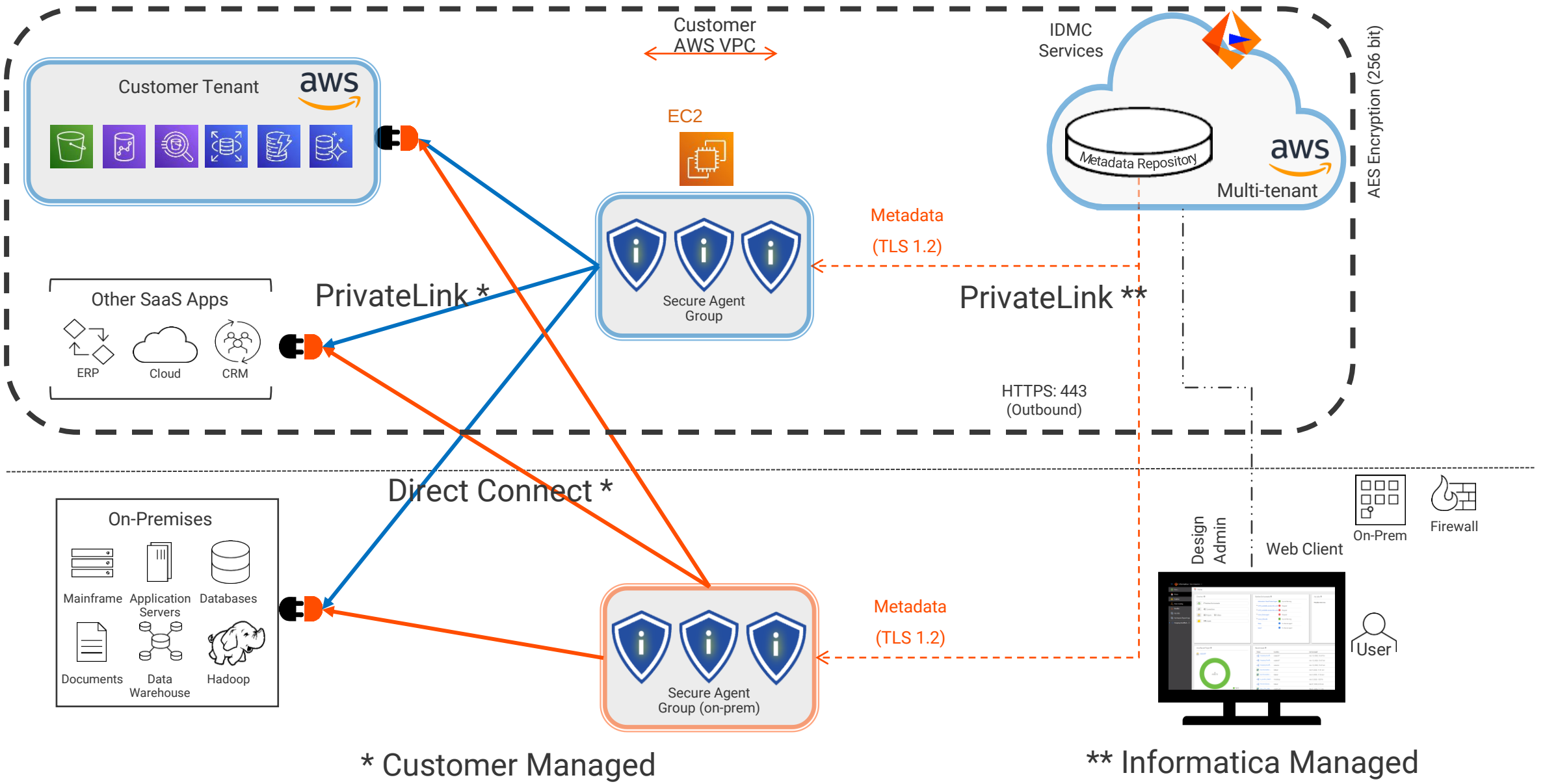
**ALL OPTIONS AVOID USE OF PUBLIC INTERNET**



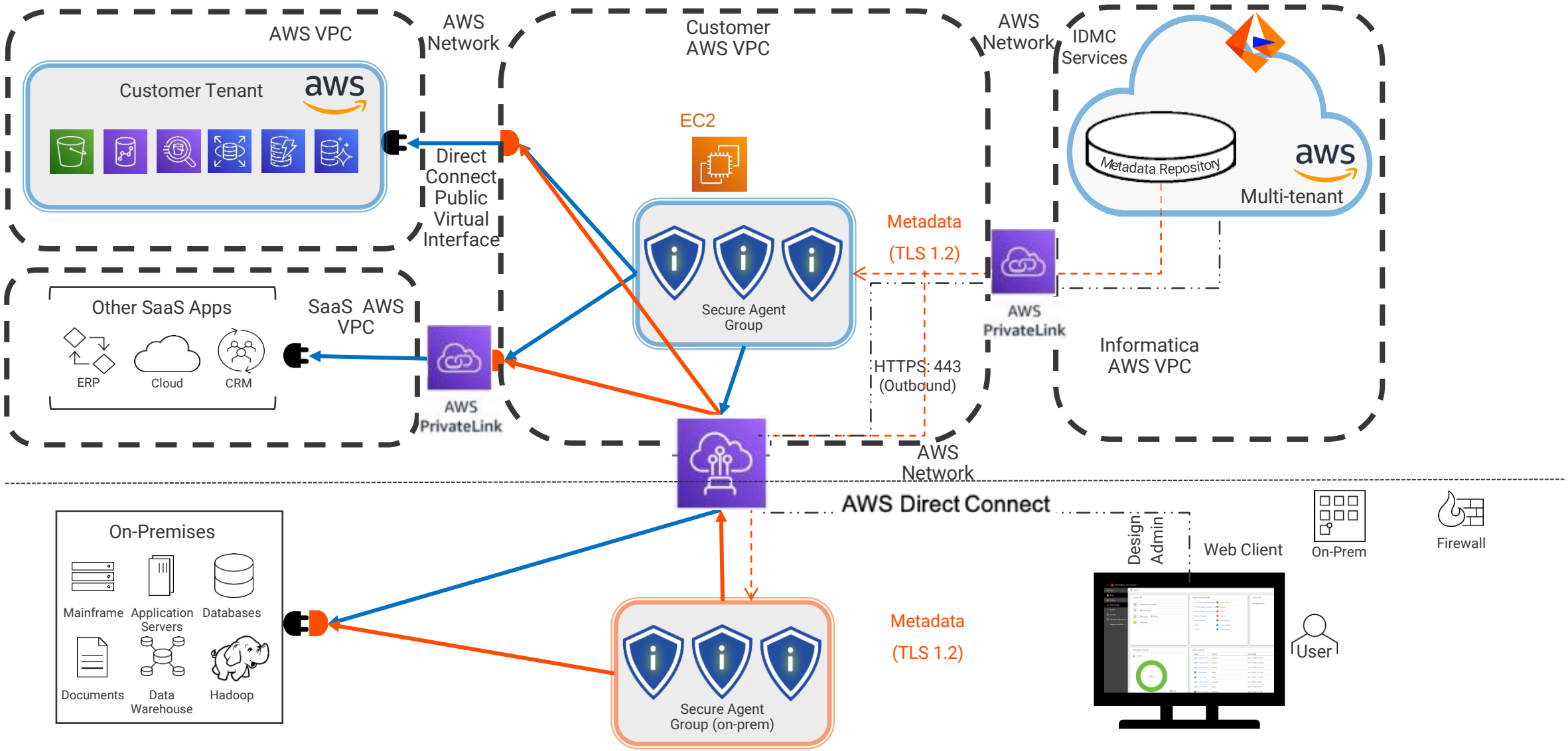


Informatica

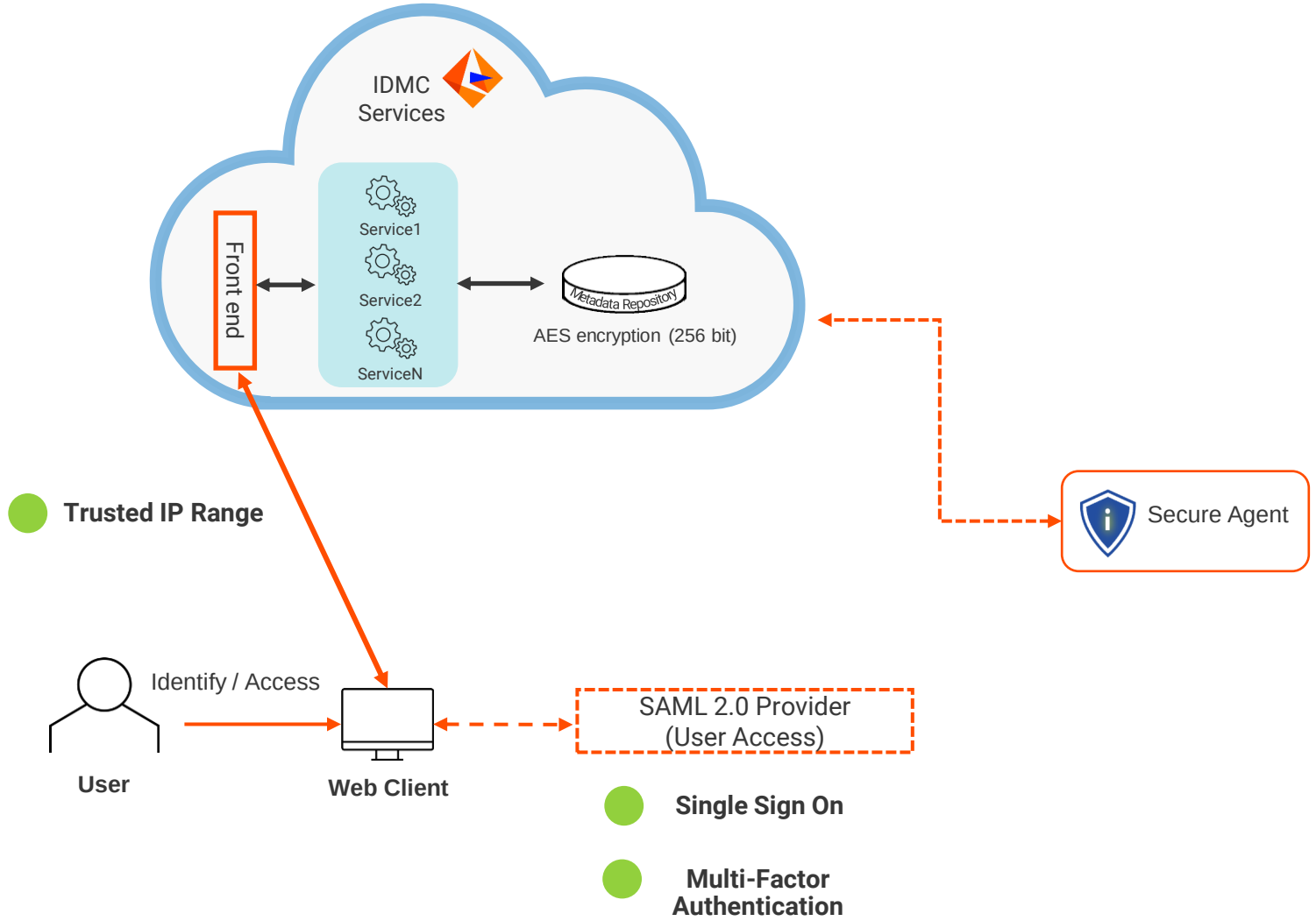
# IDMC Service Architecture – PrivateLink (logical view)



# IDMC Architecture – PrivateLink and Direct Connect



# User Authentication / Authorization Overview



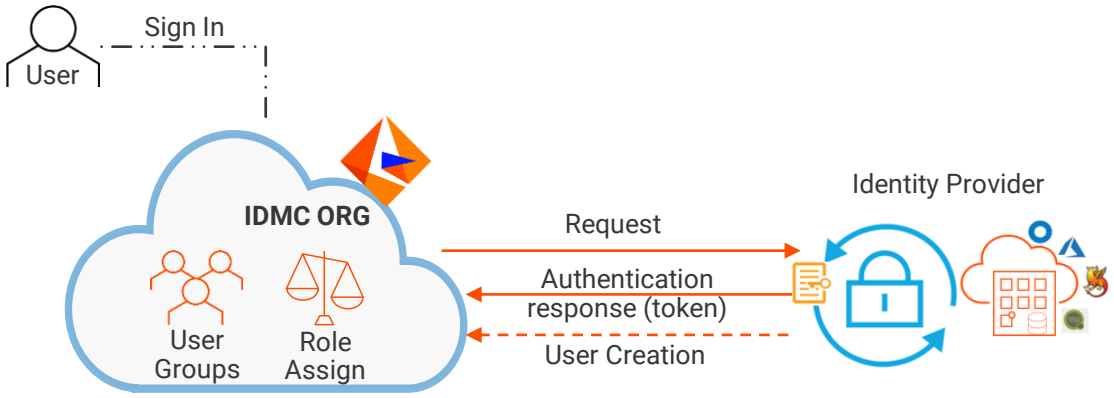





Informatica

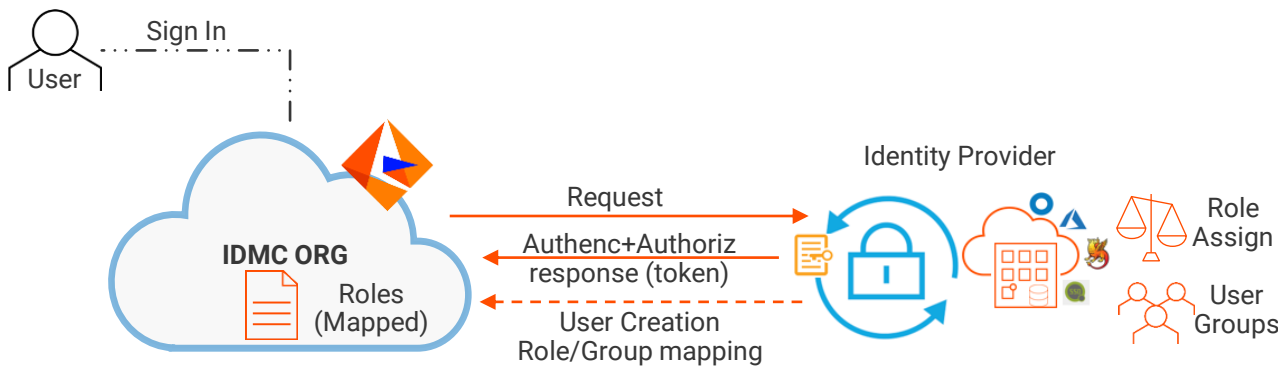
# SSO SAML Scenarios

**SAML Authentication**




- User authorization is managed within Informatica through the users' group and role assignments
- Informatica verifies the user credentials each time a user attempts to sign in
  - Existing user: user is authenticated, but roles and groups are taken from IDMC. You can update this information within IDMC
  - New user with auto-provisioning: IDMC gets user attributes from SAML token and stores in the repository to create user and assign default group and role (if configured)
  - New user without auto-provisioning: logs in fails, you need to create the user within IDMC

**SAML Authentication and Authorization**



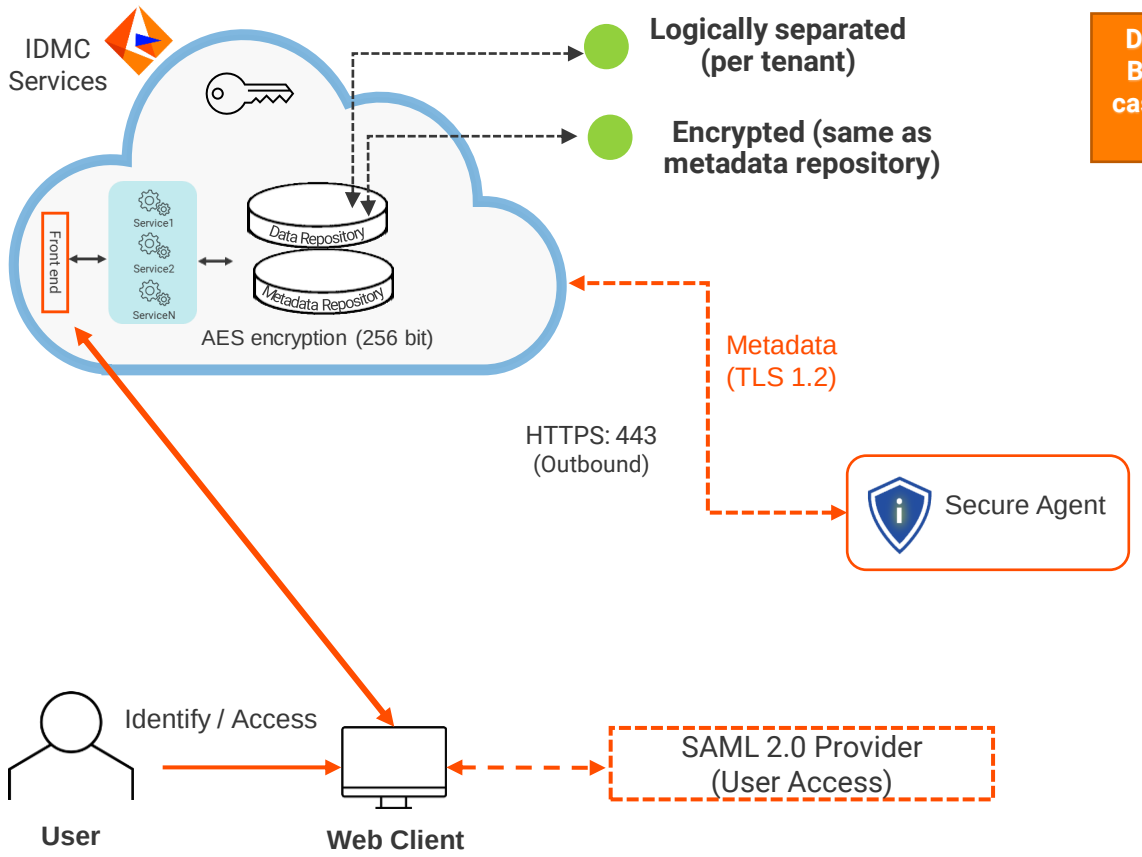

- Informatica verifies the user credentials each time a user attempts to sign in. It also gets the user's SAML groups and roles and assigns the user the corresponding IDMC roles
  - Existing user: Informatica authenticates the user and gets the SAML roles, groups, and user attributes from the SAML token. If this information has changed since the last login, Informatica updates the user attributes and roles
  - New user with auto-provisioning: Informatica gets the SAML roles, groups, and user attributes from the SAML token and stores them in the repository. It creates and authenticates the user and assigns the user the Informatica roles that are mapped
  - New user without auto-provisioning: logs in fails, you need to create the user within IDMC
- For some identity providers, you can also choose to push user and group information to IDMC using SCIM 2.0





Informatica

# Data Storage Overview




**Data Repository can contain Master Data (in case of Business 360 service), metadata or profiled data (in case of Data Governance & Catalog, Data Marketplace or Data Quality services)**

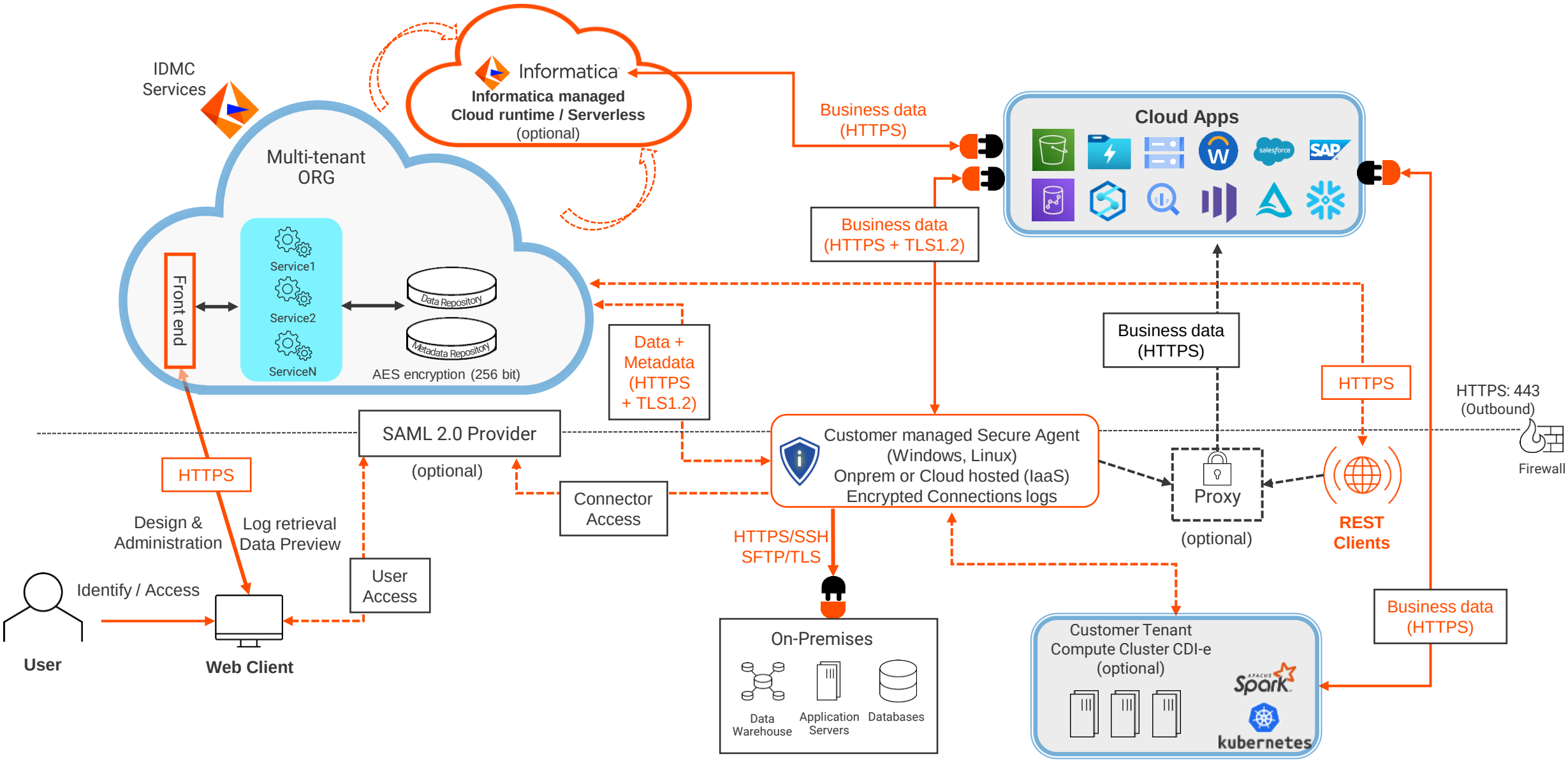




Informatica

# IDMC Security Architecture Diagram

IDMC is built on microservices-based technology architecture and cloud native frameworks. The diagram below shows all major components of the IDMC security domain and lays out the areas of metadata and data persistence and data movement



# Questions?

While we answer some of your questions please feel free to also share your thoughts about the session today

Informatica

# Further reading

- IDMC Security Whitepaper
  - https://knowledge.informatica.com/s/article/DOC-18220?language=en_US



Informatica

# Thank You!