Informatica
from Salesforce

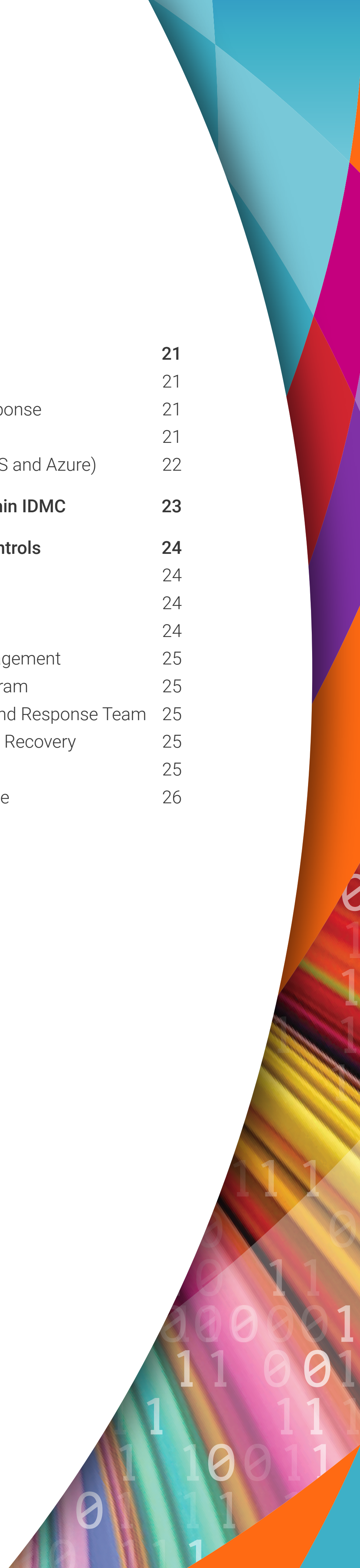
White Paper

Intelligent Data Management Cloud

Security Architecture Overview

Where data
& AI come to LIFE™

Contents

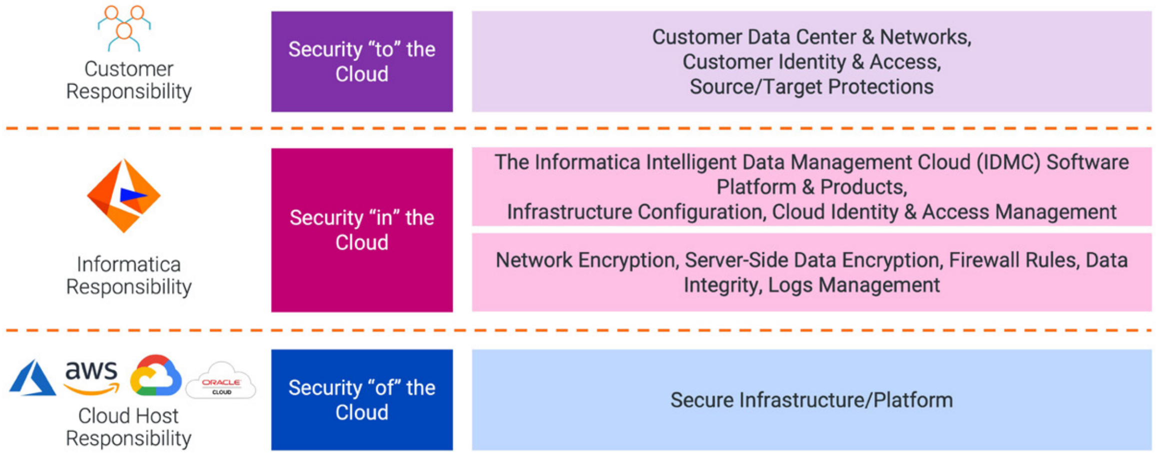


Shared Responsibility Models

In today's digital landscape, cloud technology has revolutionized the way we store, access and manage data. In this paradigm, the traditional boundaries of security have blurred, requiring a collaborative effort between cloud service providers and valued customers. This shared responsibility model is a fundamental principle that underpins the protection of customer data and digital assets. As we explore Informatica's security architecture, it is important to clarify the role(s) all stakeholders, including our customers, our host providers Informatica® plays in fortifying the security of our cloud-based solutions.

As it pertains to Informatica's **Intelligent Data Management Cloud® (IDMC)**, the shared responsibility model consists of three roles (See Figure 1):

- Customer responsibility - Security "to" the cloud
- Informatica responsibility - Security "in" the cloud
- Cloud host responsibility - Security "of" the cloud



Customer Responsibility	Security "to" the Cloud	Customer Data Center & Networks, Customer Identity & Access, Source/Target Protections
Informatica Responsibility	Security "in" the Cloud	The Informatica Intelligent Data Management Cloud (IDMC) Software Platform & Products, Infrastructure Configuration, Cloud Identity & Access Management Network Encryption, Server-Side Data Encryption, Firewall Rules, Data Integrity, Logs Management
Cloud Host Responsibility	Security "of" the Cloud	Secure Infrastructure/Platform

Figure 1. IDMC Security Shared Responsibility Model

Security "to" the Cloud

Customers play a pivotal role in the shared responsibility model. This responsibility encompasses the protection of the customer's data center, network infrastructure and any associated components. Customers are also accountable for configuring and managing identity and access controls, ensuring that only authorized individuals receive appropriate privileges. Additionally, customers must oversee the protection and proper configuration of sources and targets within their cloud deployment.

This comprehensive responsibility not only includes maintaining data security but also enforcing security policies that align with industry-specific compliance standards. There are some additional aspects of security “to” the cloud that are also the responsibility of our valued customers. These additional control responsibilities can be found in our SOC1 and SOC2 documents under the “Complementary User Entity Controls (CUEC)” section.

Security “of” the Cloud

Our cloud-hosted solution utilizes our cloud ecosystem partners, including Amazon Web Services (AWS), Microsoft Azure (Azure), Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI). These partners bear the vital responsibility of ensuring the robustness and reliability of the cloud infrastructure. As your infrastructure partner, Informatica inherits controls from our ecosystem that includes physical and environmental security, redundancy of data centers and high availability of cloud services.

Security “in” the Cloud

At Informatica we are dedicated to maintaining the highest standards of security to protect our environment, as well as our customer data and environments. This whitepaper will provide in-depth details on how Informatica manages its commitment and responsibility for security “in” the cloud.

Security Architecture Overview

Informatica understands how critical information security is to businesses. Informatica implements security as a foundational design principle for IDMC. IDMC adheres to industry best practices for security with broad support for global regulatory and compliance requirements. IDMC embeds security in every layer of the technology stack and aspect of accessing and processing data. This is achieved through a “Defense-in-Depth[1]” approach to security as noted below in Figure 2.

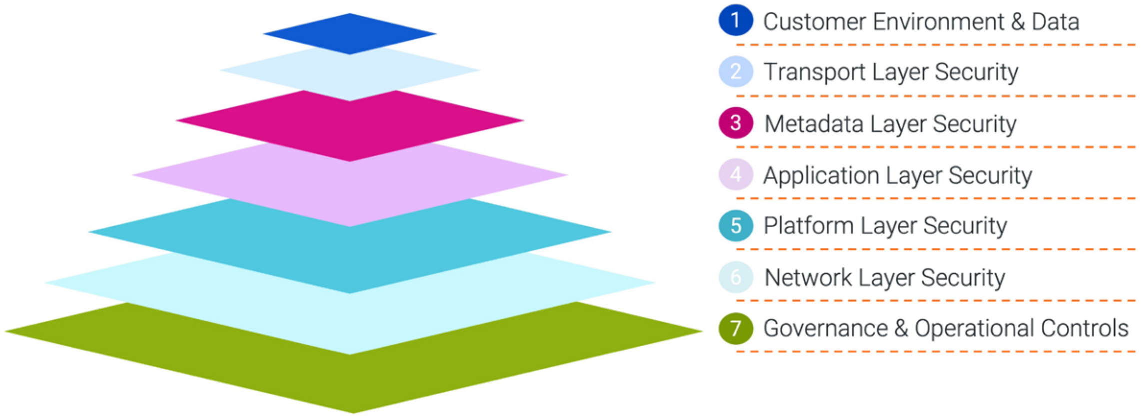

1 Customer Environment & Data
2 Transport Layer Security
3 Metadata Layer Security
4 Application Layer Security
5 Platform Layer Security
6 Network Layer Security
7 Governance & Operational Controls

Figure 2. Defense-in-Depth Security Approach

[1] Defense in depth is a security strategy that leverages multiple security measures to protect an organization’s assets. This ensures that if one line of defense is compromised, additional layers exist as backups to ensure that threats are stopped along the way.

IDMC Architecture Components

IDMC is built on a microservices-based technology architecture and cloud-native frameworks. The following illustration in Figure 3 shows all major components of the IDMC security domain and highlights the areas of metadata, data persistence and data movement.

IDMC Security Architecture Diagram

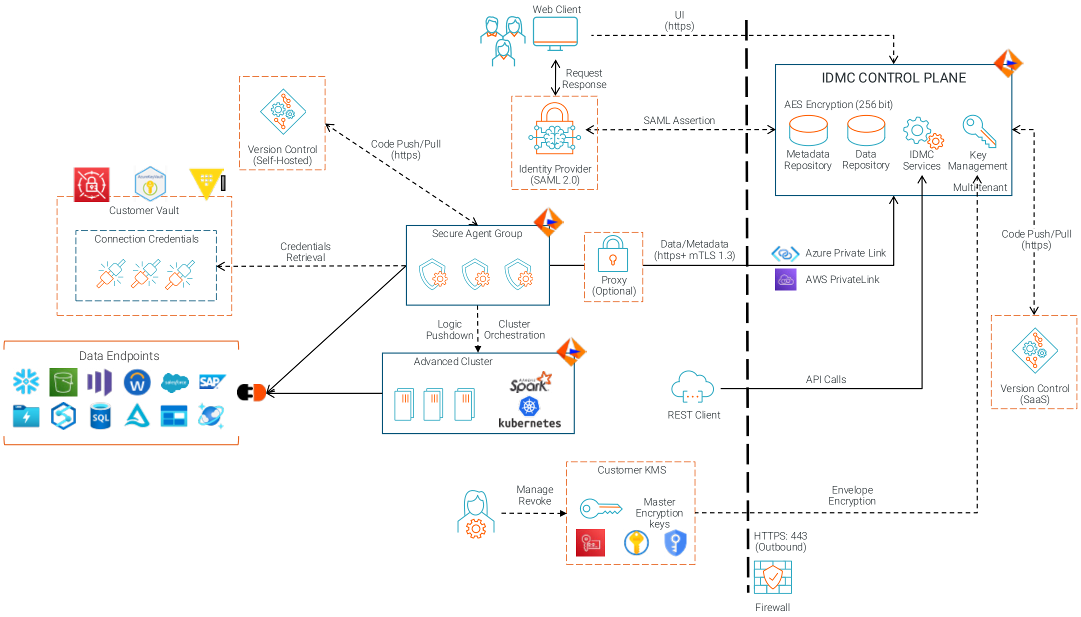


Figure 3. IDMC Security Architecture – The Key Components

IDMC contains services that both users and the system account access. Informatica services include, but are not limited to, **Data Integration**, **Application Integration**, **API Center**, **Data Quality**, **Data Ingestion and Replication** and **Data Governance and Catalog**. These services are built on microservices and multi-tenant repositories on the backend with a common login page and user interface shell on the front end. Users interact with IDMC via a web client through the HTTPS protocol for design-time activities.

The customer employee acting as an administrator for their tenant configures and manages the security of the customer organization. Integration developers and business users use the web-based visual designer and wizard tools of IDMC to design integration and data management flows. The metadata that defines these designs is stored in a multi-tenant metadata repository in the IDMC solution. Unique tenant IDs and tenant specific encryption keys are used to ensure separation of the metadata across tenants. The multi-tenant data repository backend is used for securely storing customer metadata on the IDMC solution.[2]

[2] The majority of IDMC services only store metadata in the customer's tenant. Cloud Integration Hub customers can choose to store data in their IDMC tenant but is only done at customer request. By default, customers host their own databases. MDM customer data is stored in the customer's tenant and is protected by the same safeguards described in this document.

Informatica ensures secure and isolated operations for each individual tenant despite hardware sharing by implementing several mechanisms.[3] Virtualization and containerization provide isolation through hypervisors and containers, ensuring independent operations and process/resource separation. Storage isolation is achieved via logically separated volumes and encryption, along with strict access controls. Network traffic is segmented into subnets, with firewalls regulating access to prevent unauthorized entry. Resource quotas and limits ensure equitable resource allocation, avoiding performance issues. Security is strengthened by strict access control policies and continuous monitoring of security threats or breaches.

The Informatica runtime environments (Secure Agent, Elastic Cluster and Serverless) execute customer-authored integrations and processes. They connect, transform and move the data between source and target data applications in batch, real-time and streaming integration patterns. Customer-managed runtime environments (Secure Agent, Elastic and Serverless) can be deployed within the customer security context, whether it is in an on-premises environment or the customer's cloud VPC.[4, 5] The Informatica-managed cloud runtime is deployed on the IDMC solution.

Security of Customer Environment and Data

Identity and Access Management

Controlling and auditing user access can often prevent security problems. Identity and access management help administrators and security personnel pinpoint and analyze any issues that arise. Informatica provides rich support for enterprise user identity and access management.

Authentication

IDMC supports the following authentication mechanisms: password-based, single-sign-on (SSO)-based, certificate-based and token-based authentication. Multi-factor authentication (MFA) mechanisms, such as trusted IP address ranges, also enable rigorous user authentication.

For native password-based authentication, user credentials are hashed and securely stored in the IDMC solution. Administrators of the customer organization can configure policies for password strength and rotation to suit their business needs. IDMC enables you to provision human users who securely access the system with multi-factor authentication, as well as non-human users designed for API calls and automations that do not require MFA, ensuring both security and seamless machine-driven operations.

IDMC supports web SSO-based security assertion markup language (SAML) 2.0 providers, which include support for technologies such as Okta, Azure AD, ADFS or any third-party identity provider (IDP) that supports SAML protocol for authentication and authorization. Additionally, IDMC also supports service-to-service authentication using short-lived token-based authentication (OAuth 2.0).
This allows customers to set up job configurations based on specific service accounts.

[3] For detailed information on how Informatica facilitates Tenant segregation, refer to **IDMC Tenant Segregation**

[4] While our whitepaper cites Virtual Private Cloud (VPC), which is an Amazon Web Services term, IDMC is a cloud-agnostic solution.

[5] Secure Agent runtimes can be deployed in customer on-premises or cloud VPC environments. Elastic and Serverless runtimes can be deployed in supported customer cloud VPC environments.

Access Provisioning

The IDMC org, sub-org, project and folder constructs enable the customer's administrators to effectively secure and govern the structure of their IDMC artifacts and intellectual property. Access to projects and folders can be controlled by permissions to ensure separation of work and authorized-only access.

IDMC supports fine-grained access management both at the asset-type level and at every asset level. Administrator-level privileges manage access to asset types, while permissions control access to the asset level. Access is enabled at both org and sub-orgs. The org and sub-org administrators can also manage the user, user role or user group that can access asset types in IDMC. For example, an administrator can configure create, read, update, delete, run and set permissions for a user ID, user role and/or user group for all the mapping tasks in IDMC.

Similarly, at each asset level in IDMC, permissions can be set to manage read, update, delete, execute and change access for users, user roles and user groups. IDMC additionally supports the system for cross-domain identity management (SCIM) protocol for users auto-provisioning in a sub-org via Okta and Azure AD.

Role-Based Access and Provisioning Least Privilege

Administrators can assign different roles to users to maintain the principle of least privilege. Users can be granted access to only the capabilities needed to perform their function. Administrators can control who does what, such that some users are managing project and folder structure, some are designing, some are running jobs and so on (which could allow for strict separation of duties, essential for enterprises with demanding SDLC requirements). IDMC provides predefined roles to facilitate user role assignments for most common needs, and custom roles for administrators, to define new roles to meet the unique needs of their organization.

When an IDMC org or sub-org is configured with a customer's IDP via SAML protocol, the IDMC user role and user group are synced with the customer's enterprise user role and user group setup based on one-time user role and user group mapping, defined by administrator for that org during IDMC SAML setup.

Figure 4 depicts this "Role-Based Access Control" (RBAC) model of the IDMC platform. In this example, the administrator role has access to all assets, including security configuration, while the designer and service consumer roles have only limited privileges and permissions needed to perform their functions.

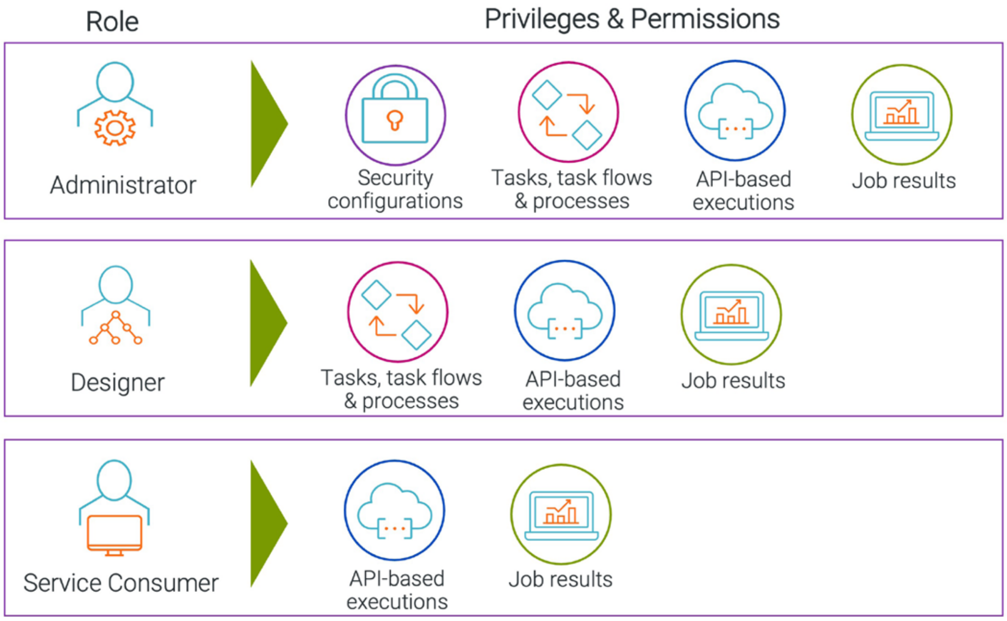


Figure 4. IDMC Role-Based Access Control Model

Role privileges grant users access to asset types. Access control lists (ACL), in conjunction with RBAC, allow organizations to control permissions at the asset level in IDMC.

Sub-Organizations

Administrators can create sub-organizations to easily classify and group users (very common to segment users according to their line of business). Segregating users in this way allows different departments (or other logical groupings of users) to see only their relevant work. The administrator can also assign licenses for each organization and sub-organization and can create delegated administrators. Privilege levels are configured to allow only specified users to exercise administrator-like functions without giving them full administrative control.

Figure 5 below illustrates the Informatica “Delegated Admin” function. The example shows the parent organization defining policies for the environment, including authentication options, licenses, logging options, job execution compute and content distribution options. The delegated admins can then be created and given control over each of their subordinate organizations. These admins can create any additional policies they deem necessary, as long as the policies do not conflict with the core policies configured by the parent administrator.

The delegated admin function easily enables customers to extend integration services to downstream enterprise users. Additionally, this helps to promote reuse and best practices across departments through “Integration Competency Center” (ICC) initiatives.

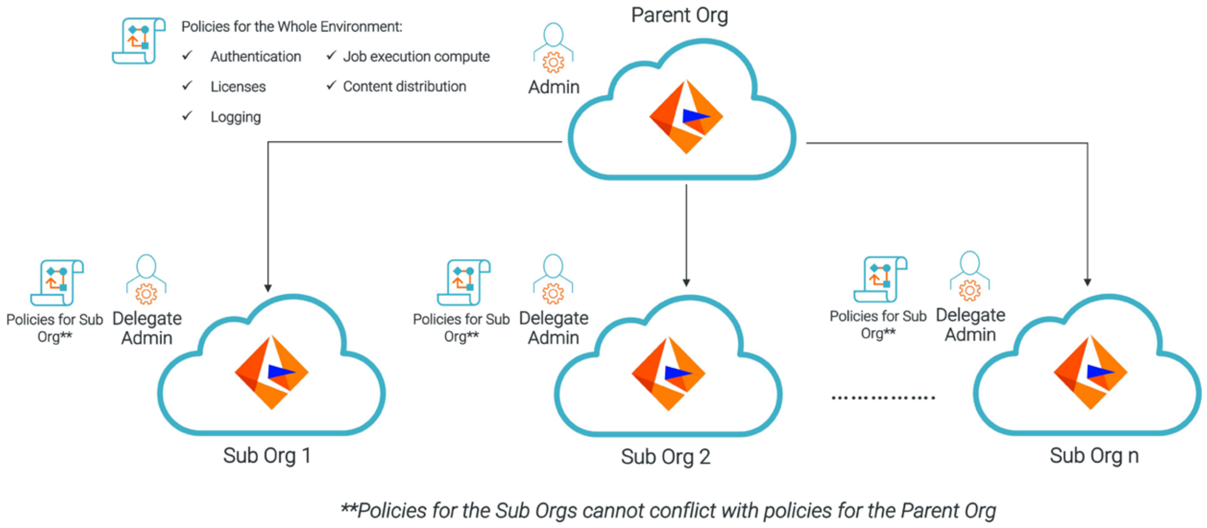


Figure 5. IDMC Delegated Admin Function Example

Transport Layer Security

Encryption Key Management

IDMC uses organization-level Advanced Encryption Standard (AES) 256-bit symmetric encryption keys (tenant keys) to encrypt sensitive data at rest and in transit. By default, these tenant keys are rotated annually in conformance with National Institute of Standards and Technology (NIST) Special Publication 800-57 Part 1 Revision 5 guidelines. However, customers can choose to configure key rotation for 90, 120 or 180 days. When a key is rotated, the new key is used for subsequent encryption requests and the old key is preserved to decrypt previously encrypted data.

Data Transmission Security

Data transmission security is a key aspect of securing customer data and metadata. When processing data, the Secure Agent communicates with both the IDMC solution and customer data stores or software-as-a-service (SaaS) applications.

The Secure Agent initiates communication with Informatica's IDMC through a secure channel initially authenticated through a shared secret credential. Customers do not need to open inbound firewall ports at their site to allow the Secure Agent to communicate with the IDMC solution. The Secure Agent code communicates with the host and uses port 443 for all outbound communication, including via proxy. The Secure Agent avoids data loss and transport delays by checking for availability before connecting. The Secure Agent also performs network resiliency checks and retains full audit and session logs for a configurable duration to support troubleshooting and audits. Additionally, logs can be sent to a customer's centralized logging systems to comply with security and regulatory requirements.

Encryption for Data in Transit

To defend against man-in-the-middle attacks, the communication channel between the customer-deployed Secure Agent and Informatica Cloud must be authenticated to maintain its integrity, as well as ensure transport encryption. All communication from the Secure Agent to the IDMC solution is encrypted through Transport Layer Security (TLS) 1.3, employing the AES256-SHA (256-bit) cipher.

The Secure Agent connects to source and target data stores and cloud applications using connectors. Connectors are configured by customers and support a variety of secure communication protocols such as Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP) and File Transfer Protocol Secure (FTPS). Informatica leverages the underlying transport layer of these connector communication protocols to ensure that customer data is transmitted securely across data stores and applications. Customer data is encrypted via TLS 1.3 by default and is customer-configurable to lower versions if needed.

See "Service Messaging Encryption" for further information about encrypting data in transit between the Secure Agent and Informatica Cloud.

Proxy Configuration

IDMC supports proxy configurations for connections between the Secure Agent and the control plane or the data endpoints.[5] Customers can benefit from increased privacy and security when connecting to the internet via proxy. This is supported in two main deployment patterns:

- To connect the Secure Agent with the control plane, customers can use an explicit proxy server.
- To connect the Secure Agent with a data endpoint, customers can use a pass-through proxy that provides transparent access to the database.[6]

Please note that while this is a supported pattern, this pattern paired with PrivateLink may cause DNS routing issues. Informatica recommends speaking with your network architecture team on supportability for your network.

Metadata Layer Security

Metadata and Persistence

The metadata within the IDMC solution can include details such as data mappings, processes, application connection details, object definitions and transformation rules.

IDMC has the following categories of metadata:

- **Organizational and user/security metadata**: Describes the structure of the organization; defines users and groups and their privileges, permissions and license information; and tracks audit logs. The audit logs are highly detailed and provide a complete record of user logins and activity sorted by time of day.
- **Design metadata**: Defines integration tasks and processes, including data synchronization, data replication, mappings and templates, task flows, process definitions and connectors.
- **Runtime metadata**: Contains agent definition data and other information crucial for runtime activities, like connection and schedule information and job and process logs and states.

User access controls are closely tied to metadata that details user actions within the system. Role-based controls grant users access to the metadata and specific functions. All IDMC services adhere to contractual obligations for the retention and disposition of the above metadata. See **https://www.informatica.com/legal.html** for further information.

[6] Informatica doesn't support reverse proxy.

Encryption for Data at Rest

Sensitive customer data persisted in the customer's IDMC multi-tenant data[7] repository is encrypted using the "Advanced Encryption Standard" (AES) algorithm, which uses a 256-bit key. The key is unique to the customer tenant. By default, it is rotated annually, but customers can configure rotation every 90, 120 or 180 days.

Customer-Managed Encryption Keys

IDMC supports "Customer-Managed Keys," empowering tenants with enhanced control over the encryption of their metadata and data within IDMC.

Tenants generate a master key in their preferred cloud provider's key management service (KMS). With customer authorization, Informatica uses this master key to encrypt tenant-specific data keys, which in turn secure all metadata and data stored at rest within the tenant's IDMC environment. IDMC periodically communicates with the customer's KMS to encrypt and decrypt data keys, ensuring the master key remains exclusively within the customer's KMS.

This approach, as shown in Figure 6, grants customers greater control and ownership over the encryption process by enabling:

- **Key lifecycle management:** Customers fully manage their key lifecycle, including key creation and rotation policies, within their own KMS
- **Key revocation:** Customers can revoke keys independently. Upon revocation, all IDMC operations will halt, preventing data access by any party or process

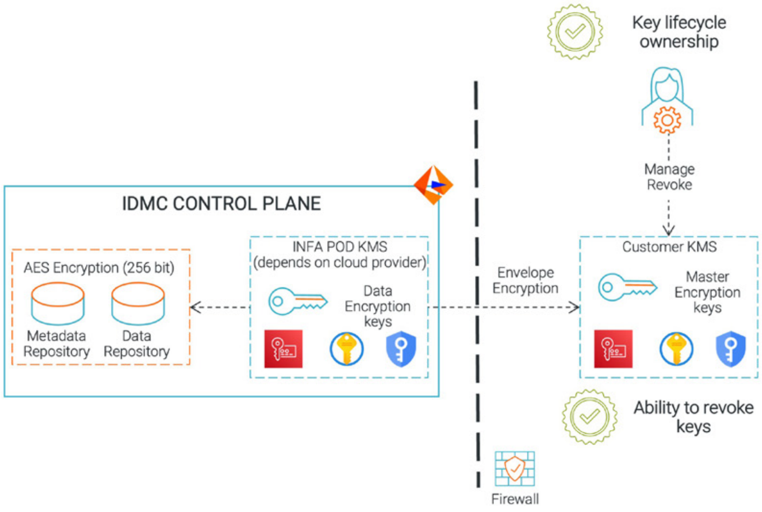


Figure 6. Customer-Managed Keys with IDMC

[7] This does not include customer data stored within the MDM solution. For information about the MDM purposes, refer to Security and Compliance Overview: Customer 360.

Application and Service Layer Security

Service Messaging Encryption

Each service-level message is encrypted uniquely for each service by the Secure Agent and the Encryption in Transit protocol, thus creating two encryption layers on all communications between the IDMC solution and the "Secure Agent." See **Encryption for Data in Transit** for more information.

Application Connection Encryption

Informatica empowers users to configure secure connections to data stores, such as customer databases and SaaS applications, in three different methods: (i) stored in the cloud within IDMC, (ii) stored within the locally hosted Secure Agent or (iii) stored within a customer-configured "Secrets Manager" (or "Vault"). These storage options can be managed using the IDMC "Web" client.

IDMC Cloud Storage

Connector credentials to data stores and applications (along with the connection metadata) are stored securely using unique tenant-specific encryption keys.

Local Secure Agent

This option can be selected if users require credentials to be stored within the confinement of their firewalls and adhere to their security requirements. A specific run-time pattern is required to configure this option. See **"Customer-Managed Secure Agent"** for more information.

Secrets Manager Configuration Service

Users are also offered the option of credential storage within the customer's enterprise "Secrets Manager" (or "Vault"). As illustrated in Figure 7, customers have the ability to configure this option if they prefer a centralized storage and management mechanism (rotation) for all of their credentials. This is a flexible option that customers can utilize on a per-connection basis. The current supported "Secret Managers" are documented in our IDMC "Product Availability Matrix."[8]

[8] IDMC's Product Availability Matrix (PAM) can be found at **https://docs.informatica.com/integration-cloud/data-integration/current-version/introduction/informatica-resources/informatica-product-availability-matrices.html**

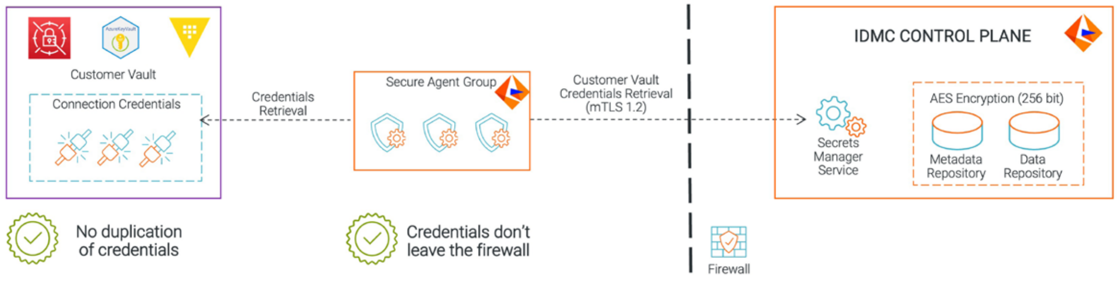


Figure 7. Secrets Manager Configuration Service in Action

Process States and Integration Variables

Process state information that is needed for process recovery is stored within the IDMC solution to allow long-running processes and the recovery of such processes. Similarly, integration mapping variables are stored within the IDMC solution to keep track of data integration logic. State information may include elements of payload data and is persisted temporarily, then cleaned up as processing completes.

Data Preview Functionality

A key aspect of customer data processing is data transformations as defined by customer integration logic. Some IDMC services provide a data preview capability that helps customers effectively develop and debug their data integration logic. Similarly, customers can view process data elements via the web interfaces for debugging purposes. This capability allows customers to view a subset of their business data through the web client at one or more stages of data transformation. The desired transformed customer data is directly fetched from the Secure Agent/Process Server, cached in memory[9] and rendered via the web client. Customer business data is not persisted on the IDMC solution to enable this functionality. The data preview feature is enabled by default and can be disabled by the administrator to comply with a customer's security policy. While this feature provides an effective means to debug the developmental process, Informatica recommends that data preview be disabled for customer production organizations.

[9] Data Preview data is cached in memory for the session of the user. The data is not stored on disk and is immediately deleted on termination of the session.

Informatica Secure Development Practices

Informatica has designed, implemented and enforces rigorous software development practices as part of its overall security posture. This process is assessed several times annually by independent, globally recognized auditors. This section describes the different security elements of Informatica's "Software Development Cycle" (SDLC) processes.

Securing Coding Procedures

Informatica follows secure coding procedures that are based on "Open Web Application Security Project®" (OWASP) recommendations for developing software. Informatica's secure coding procedures provide a comprehensive framework for the thorough documentation, testing and evaluation of all coding changes made to our software. The secure coding procedures mitigate risks to Informatica's production applications and infrastructure that could threaten stability, resiliency, security, regulatory compliance and availability. These procedures are applicable to the entire workforce at Informatica and pertain to any modifications made in production environments. These environments predominantly consist of hardware, system software, application software, communication equipment, as well as all documentation and procedures related to the operation and maintenance of these systems.

These secure coding procedures are defined around the following OWASP recommended controls:

- Input validation
- Authentication and password management
- Access control
- Error handling and logging
- Communication security
- File management
- Output encoding
- Session management
- Cryptographic practices
- Data protection
- Data security
- Memory management

Informatica enforces secure coding procedures as part of its policies and procedures, which are part of Informatica's mandatory security awareness training for all applicable personnel and role-specific security training for its research and development (R&D) organization.

Software Security Training

All Informatica development teams are required to complete annual software security training that covers secure coding and design practices. Training is provided through Informatica's learning management system and other methods, as necessary.

Security Architecture Design Reviews

Security architecture reviews are continuously performed on Informatica products by our Global Security, Product Security and Engineering teams. This process is integrated by design into our change workflow and tooling and is therefore automatically triggered based on change criteria.

Automated Code Reviews

Informatica has implemented globally recognized Automated Secure Code reviews in our development pipeline as part of our efforts to ensure best practices for systematic code reviews. These automated code reviews come into play whenever code is checked. This process not only identifies publicly known security vulnerabilities but also identifies vulnerabilities introduced through custom-developed code and ensures adherence to best coding practices. Additionally, it identifies potential points of security breaches.

Manual Code Review

During the regular development cycle, the engineering team conducts functional and design reviews of product components. During the code development phase, all code that's checked in to the source code repository goes through manual code reviews by lead engineers and architects to ensure adherence to strict security guidelines and to identify gaps for immediate remediation. Production check-ins for any emergency bug fix undergo strict scrutiny and code reviews to ensure proper and expected behavior.

Static Analysis Scans

Informatica secures propriety code through the integration of an industry-leading static application security testing (SAST) solution into our SDLC process. This integration ensures regular security gate checks, identifies security vulnerabilities, maintains a risk-driven inventory of all identified security vulnerabilities and alerts all key stakeholders of those vulnerabilities. Additionally, this allows for continuous learning and improvement. The detected vulnerabilities are governed through our vulnerability management process.

Software Composition Analysis (SCA)

Informatica uses an SCA solution to further secure our cloud products. This helps detect security vulnerabilities included in third-party libraries. The detected vulnerabilities are also governed through our vulnerability management process.

Dynamic Analysis Scans

Informatica uses third-party commercial dynamic application security testing (DAST) to perform continuous dynamic analysis scans on its services in production. The detected vulnerabilities are governed through our vulnerability management process.

Manual Penetration Testing

Informatica uses various internal and external application penetration testing teams to perform regular manual penetration testing on its products. Our manual application penetration testing teams perform regular application security assessments/pen tests monthly with every release. Additionally, an external third party performs a product penetration test at least once a year, which can be shared with our customers. Customers can contact their Informatica account executives to get the executive summary of this third-party pen test.

Platform Layer Security

In IDMC, the runtime environment is responsible for processing data. The Secure Agent and the other available runtime environments play a major role in securing customer data and applications and contain several security features. The Secure Agent supports microservice characteristics such as pluggable engines, load balancing, scalability and high availability. It consists of data integration, process server and mass ingestion engines, and other services, as well as connectors to external data sources. These components enable the execution of batch, streaming and real-time integrations, as well as other aspects of data management like **data quality** and **data cataloging**.

The deployment of the runtime environment is flexible for customers. They can deploy the Secure Agent on-premises or on a public cloud, such as AWS, Azure, GCP and OCI. Additionally, they can choose to have the runtime environment managed by Informatica on the IDMC solution. (See Figure 8.)

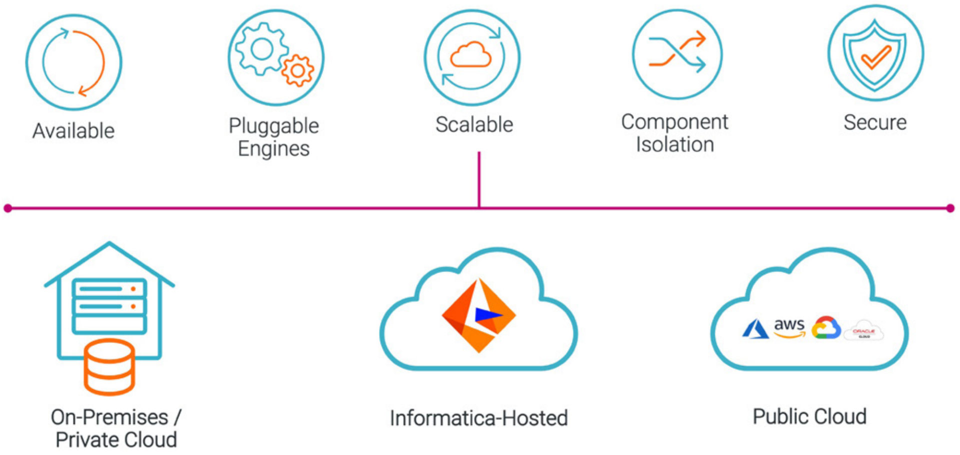


Figure 8. Secure Agent Characteristics and Deployment Options

Customer-Managed Secure Agent

Customer-managed Secure Agent deployments can accomplish ground-to-ground, cloud-to-ground and cloud-to-cloud integrations. With customer-managed “Secure Agents” either on-premises or a public cloud service such as AWS or Azure, the customer has full control of their deployed Secure Agent runtimes. No inbound firewall ports need to be opened at the customer site for the customer-managed “Secure Agents” to operate successfully (though outbound 443 traffic will be required to designated Informatica IP addresses associated with the POD that their organization is deployed on).[10]

For customer-managed deployments, the Secure Agent is downloaded by the customers and placed in a location that best fits customer requirements. The IDMC solution verifies the Secure Agent binaries and associated payload before the binaries get downloaded and deployed in the customer environment.

Secure Agent Authentication

The Secure Agent is attached to the customer organization at the time of its registration. The Secure Agent installer uses token-based authentication to complete this registration. When registering the Secure Agent, the customer needs to supply the token generated at the time of the Secure Agent installation. Note that the key has a limited lifespan. If it expires, a new Secure Agent installation token will be required. Customers can also optionally configure a proxy server at the time of Secure Agent registration for its communication with cloud applications. Upon successful authentication, the Secure Agent will be attached to the customer’s IDMC organization.

After the Secure Agent is attached to the customer organization, it downloads binaries associated with services and connectors that the customer is licensed for, and it initiates the corresponding service engines. The agent also downloads any updates to engines or packages associated with the connectors during the customer subscription and service upgrade lifecycle. The binaries sent to the customer’s Secure Agent are signed and hashed, preventing man-in-the-middle attacks.

[10] For more information about IDMC IP addresses, see https://knowledge.informatica.com/s/article/524982.

Secure Agent Fingerprinting

Administrators have the option of enabling Secure Agent fingerprinting. This functionality acts as a digital signature and is generated by using the machine ID of the virtual machine being utilized for the Secure Agent. The Secure Agent's fingerprinting[11] capability offers an added layer of security to the existing transport layer controls, making it significantly harder for malicious actors to compromise the command channel or inject unauthorized commands. (See Figure 9.)

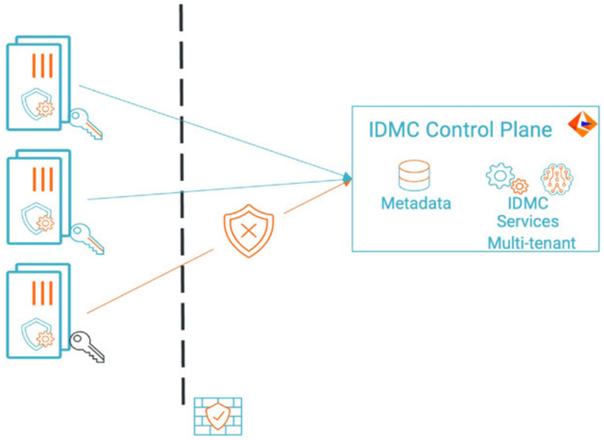


Figure 9. Secure Agent Fingerprinting in Action

Communication Protocol

The communication between the customer-managed Secure Agent and IDMC is initiated by the Secure Agent (located within the customer environment). The Secure Agent continuously communicates with IDMC. There are two types of communication:

1. **System Communication:** This type of communication occurs between IDMC and the Secure Agent and is always ongoing. This communication is used to establish connection between IDMC and the Secure Agent to determine the health of the Secure Agent, to send runtime execution instructions to the Secure Agent, to monitor the progress of a job, as well as to perform lifecycle management activities like connector package updates and Secure Agent upgrades.
2. **User-initiated Communication:** This type of communication is initiated by the customer. Only a customer-authorized or provisioned user can initiate this type of communication with the Secure Agent through the IDMC web client. This communication is used to fetch agent and job session logs from Secure Agent hosts for troubleshooting purposes, to validate connections with source and target systems, as well as to fetch schema or data from source and target systems while authoring and validating integrations.

[11] Steps to configure Secure Agent Fingerprint can be found at the following Knowledge article – Fingerprint Authentication Properties.

Secure Agent Release Packages

IDMC has monthly releases on a predetermined schedule.[12] Informatica will periodically have a major release during which the customer-managed Secure Agent is upgraded. Like the initial download of the Secure Agent, multiple validation and authentication checks are performed prior to the upgrade. Informatica Cloud® ensures runtime continuity during upgradation and uninterrupted job execution for key services during the upgrade window.[13] Figure 10, illustrated below, showcases the step-by-step Secure Agent upgradation flow.

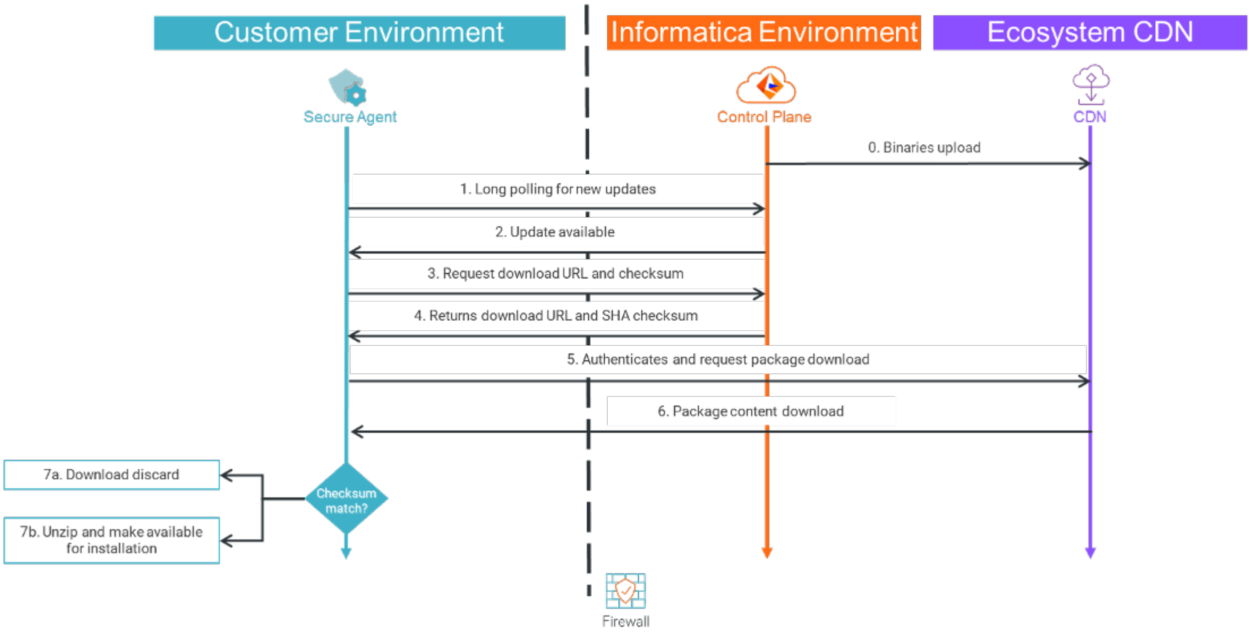

Customer Environment
Informatica Environment
Ecosystem CDN
Secure Agent
Control Plane
CDN
0. Binaries upload
1. Long polling for new updates
2. Update available
3. Request download URL and checksum
4. Returns download URL and SHA checksum
5. Authenticates and request package download
6. Package content download
7a. Download discard
7b. Unzip and make available for installation
Checksum match?
Firewall

Figure 10. Secure Agent Upgrade Flow

[12] For information about upcoming IDMC releases and upgrade schedules, please visit https://status.informatica.com.

[13] For more details on upgradation cycle, refer to this document - IDMC Release Readiness

Network Layer Security

Web Application Firewall

The IDMC product perimeter is monitored and protected by an Intelligent Web Application Firewall (WAF) for malicious traffic and anomalous activity. Implementing a WAF allows Informatica to dynamically protect web applications by filtering, monitoring and blocking certain HTTP traffic between a web application and its client endpoints, based on customized rule sets.

Extended Detection and Response

Throughout the IDMC infrastructure, Informatica has deployed Extended Detection and Response (XDR) agents. XDR provides real-time visibility into potential threats. It unifies and correlates data from multiple sources, such as endpoints, networks and cloud environments, empowering our security team to proactively identify and mitigate security risks before they escalate.

IP Allow Lists

IDMC Administrators can configure specific IP range authorization to access their org. By defining specific IP addresses that are granted access, customers create a virtual perimeter against unauthorized entry and potential threats. This approach significantly reduces the attack surface, minimizing the risk of malicious actors. (See Figure 11.)

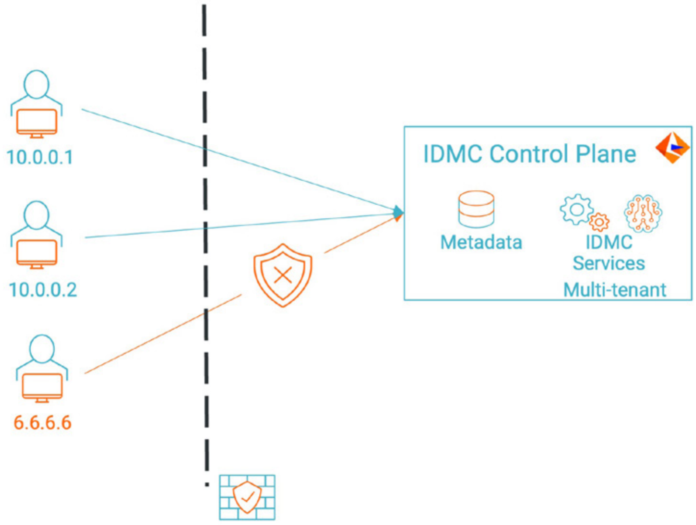


Figure 11. In-Transit Security with IP Listing

PrivateLink Connectivity (AWS and Azure)

Informatica supports AWS and Azure PrivateLink. This feature provides private connectivity between customer-managed Secure Agents deployed in their AWS or Azure Virtual Private Cloud (VPC) and the Informatica Cloud, without exposing their traffic to the public internet by routing traffic through the Cloud providers' network.[14] PrivateLink offers a secure and controlled approach by exposing only the specific services or endpoints, ensuring tight access boundaries and minimizing the attack surface.[15]
(See Figure 12.)

Informatica also enables PrivateLink connectivity across different regions, where customers can connect from their VPC in one region to an Informatica POD in a different region across the globe for both AWS and Azure pods. Customers can refer to the product availability matrix for further information on availability.

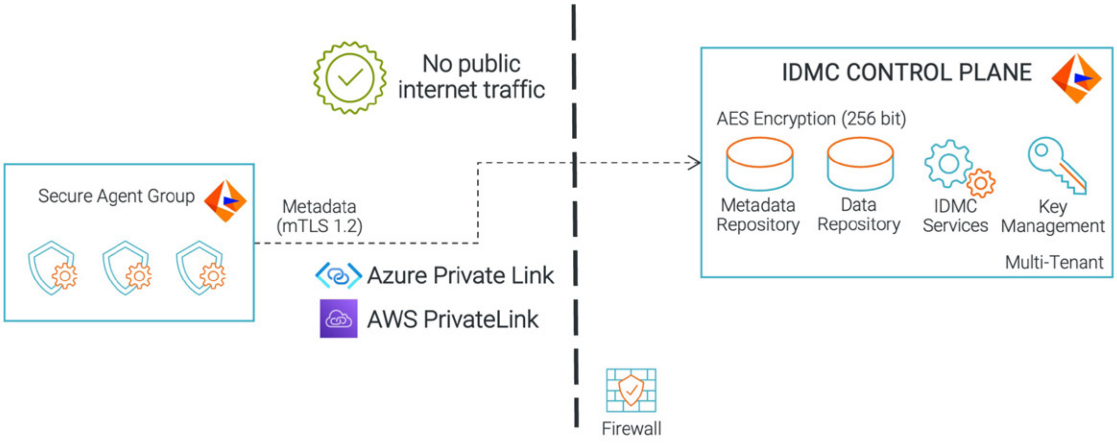


Figure 12. Private Link Connectivity with AWS or Azure

[14] Requires the respective IDMC org to be deployed on an IDMC POD running on AWS or Azure infrastructure. Each cloud provider may vary with additional requirements to utilize PrivateLink and can be found respectively here: **AWS PrivateLink Requirements**; **Azure PrivateLink Requirements**.

[15] Informatica doesn't support VPC peering or site-to-site VPN connections since they are inherently non-transparent and lack fine-grained access controls. Once a connection is established, there is no native mechanism to restrict or isolate access to specific resources within the connected networks, which introduces security and governance concerns.

CLAIRE® and AI Technology Within IDMC

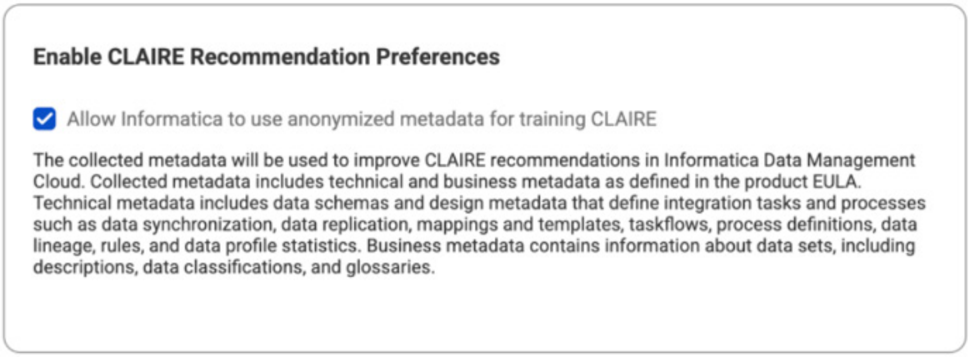
CLAIRE is a metadata-powered AI engine that is a key component and unique selling proposition (USP) of the Informatica Intelligent Data Management Cloud (IDMC) platform. It uses artificial intelligence and machine learning to enhance and automate data management capabilities.

IDMC implements various AI models with different scopes to deliver CLAIRE functionality:

- **Customer-specific models:** CLAIRE models that are tailored to meet the unique needs of individual customers. Accordingly, these models allow Informatica to provide services customized for that customer only. Hence, these models are not shared with any other customers
- **Customer-agnostic models:** CLAIRE models that serve all customers, including CLAIRE GPT

CLAIRE customer-agnostic models are trained on metadata, which includes technical metadata, operational and usage metadata, and customer business metadata. This metadata is always anonymized before being used for training, ensuring that no sensitive information is exposed during the process.

In all cases, customers can opt out of allowing Informatica to use anonymized metadata to train CLAIRE models. (See Figure 13.)



Enable CLAIRE Recommendation Preferences

☑ Allow Informatica to use anonymized metadata for training CLAIRE

The collected metadata will be used to improve CLAIRE recommendations in Informatica Data Management Cloud. Collected metadata includes technical and business metadata as defined in the product EULA. Technical metadata includes data schemas and design metadata that define integration tasks and processes such as data synchronization, data replication, mappings and templates, taskflows, process definitions, data lineage, rules, and data profile statistics. Business metadata contains information about data sets, including descriptions, data classifications, and glossaries.

Figure 13. In-Tool Opt-In Option for CLAIRE Recommendation Preference

Informatica never uses customer data stored in IDMC for training CLAIRE customer-agnostic models. This approach ensures that the customer's data remains private and secure. Informatica does not access customer data endpoints (such as Salesforce, SAP, Snowflake and others) or other cloud applications, databases or data warehouses for CLAIRE or LLM training.

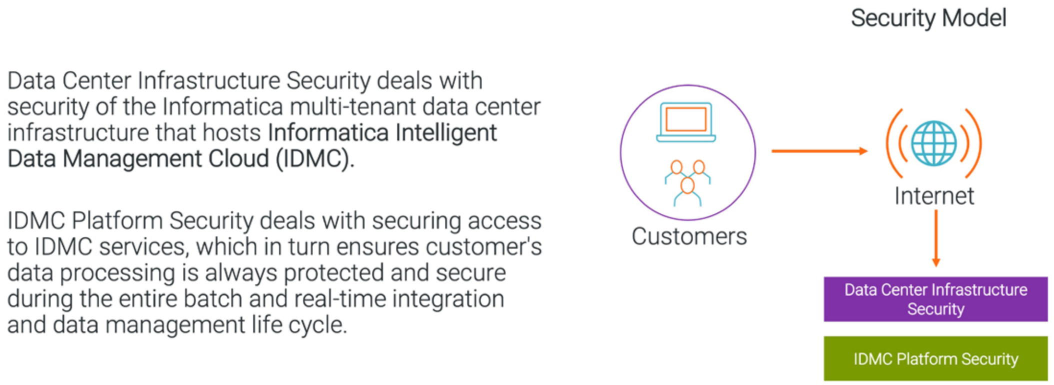
For customer-specific models, data from a customer's tenant can be used for fine-tuning a model that is used within that same tenant. For example: In Informatica Master Data Management (Cloud MDM), fine-tuning of match and merge customer-specific models is explicitly performed by the customer for de-duplicating MDM entities. This data is not used to cross-train CLAIRE models and is only utilized by customer-specific CLAIRE models.

These services are only activated upon customer action on the IDMC administration console.

Governance and Operational Controls

Security Model

IDMC security architecture is logically divided into the IDMC platform and cloud-native infrastructure layers. This layered, holistic security structure provides resistance to attack and resiliency against failure. See Figure 14 for details.



Data Center Infrastructure Security deals with security of the Informatica multi-tenant data center infrastructure that hosts **Informatica Intelligent Data Management Cloud (IDMC).**

IDMC Platform Security deals with securing access to IDMC services, which in turn ensures customer's data processing is always protected and secure during the entire batch and real-time integration and data management life cycle.

Figure 14. IDMC Security Model

Decentralized Development

Microservices have segregated development teams for which access is managed with least privilege. The overall build is centralized by a non-development operations team. This allows Informatica to secure deployment, ensuring no single set of developers has access to the full release.

Data Center Security

Informatica products are available in multiple data centers across the globe. Each data center uses redundant power and cooling systems to ensure that uptime and service-level agreements (SLAs) are met. Data centers are protected 24x7 using state-of-the-art security systems.

Vulnerability and Patch Management

Informatica scans its cloud infrastructure on a continuous basis. Identified vulnerabilities are reported on a scheduled cadence to the security stakeholders, who work with the Quality Assurance (QA) team to ensure that patches are available and can be applied during the scheduled maintenance windows. For urgent or zero-day vulnerabilities, the operations and QA teams coordinate to expedite patch availability and application. Visit **https://www.informatica.com/legal.html** for more information about vulnerability management and SLAs.

Responsible Disclosure Program

Informatica has established a responsible disclosure program, also known as a bug bounty program. This initiative invites ethical hackers, security researchers and the public to report any potential vulnerabilities or security concerns they come across within our software. This effort helps Informatica identify and address vulnerabilities, thereby reducing the risk of malicious exploitation and enhancing the overall security of our cloud software.

Security Operations Center and Response Team

Informatica's Security Operations Center (SOC) team is at the forefront of safeguarding our cloud operations. The SOC team is comprised of dedicated professionals who maintain 24/7 surveillance, real-time threat detection and swift incident response capabilities.

High Availability and Disaster Recovery

Each Informatica Cloud data center uses (n+1) configuration at all levels of infrastructure. If there is a system failure at any time, another system is assigned in lieu of the failed system. Each data center is paired with a disaster recovery region. In case of catastrophic failure, the primary region will be failed over to a disaster recovery region. Backups to the Disaster Recovery Pod are conducted daily, with real-time database replication to the Disaster Recovery Pod for most services.[16, 17]

Global Footprint

Informatica cloud data centers are available globally, providing our customers a choice for their provisioned IDMC Orgs, often required when the customer is subject to data residency regulations. Informatica provides points-of-delivery (PODs)[18] in North America (US West, US East, Canada), EMEA (Ireland, Germany, UK, UAE and France) and APJ (Australia, Singapore and Japan).

[16] See https://knowledge.informatica.com/s/article/524982 for required information about configuring firewalls for DR PODs.

[17] See the Security Addendum listed on https://www.informatica.com/legal.html for information about RTO and RPO periods.

[18] Informatica's Point of Delivery (POD's) cloud data centers are across the four major cloud providers AWS, Azure, Google Cloud and Oracle. More details of these PODs can be found at https://docs.informatica.com/cloud-common-services/pod-availability-and-networking/current-version.html.

Certifications and Compliance

The security of customer data is a critical objective of the IDMC platform. Informatica established a risk-based information security program protecting Informatica and its customers' data security and privacy.

Three principles govern Informatica's information security program to earn and maintain customers' trust:

- Maintain a safe, secure and compliant ecosystem for customer data.
- Provide Informatica and customers a trustworthy environment to conduct business.
- Consistently maintain applicable security controls, certifications and regulatory compliance.

The security program focuses efforts and resources across the following areas:

- Application and infrastructure security
- Identity and access management
- Information protection
- Supply chain risk management
- Consulting and enablement services
- Privacy protection
- Brand reputation management
- Incident response services
- Threat and vulnerability management
- Training and awareness
- Business continuity and disaster recovery
- Governance, risk and compliance

Informatica has adopted specific security framework elements, processes and controls derived from known industry standards, such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), that are applicable to the types of data processed and stored by Informatica, the industry and regulatory environment in which Informatica participates and the geographic locations in which Informatica conducts business.

Informatica has developed, implemented and applied a proven approach to identifying, measuring, managing and reporting information security and privacy-related risks applicable to the organization through its Security and Privacy Risk Management Program. This risk management program is used globally throughout Informatica and with partners or third parties that have access to Informatica systems or manage, store or process information on Informatica's behalf.

Informatica has voluntarily undertaken and/or is required by contractual obligation to perform in accordance with the below listed standards, which are measured through internal security teams and champions, third parties and external assessment partners, such as AICPA-accredited external audit firms.

ISO/IEC 27001

ISO/IEC 27001 is an internationally recognized standard for establishing, implementing, maintaining and continually improving an “Information Security Management System” (ISMS). This certification underscores Informatica’s commitment to proactively identifying and managing information security risks through a structured framework of policies, procedures and controls. The alignment of IDMC with ISO/IEC 27001 standards ensures Informatica adheres to the confidentiality, integrity and availability of customer data, incorporates ongoing risk assessments and embraces continuous security improvements.

SOC1 Type II

These reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to financial controls, operations and IT and business processes that are tied to their financial reporting. These reports are intended to be used by customers’ external auditors.

SOC 2 Type II (Scoped to IICS/IDMC; DaaS and Axon products)

These internal-controls reports capture how a company safeguards customer data and how well those controls are operating in accordance with applicable “Trust Services Criteria.” These reports are intended to be used by customers.

UK Cyber Essentials (Scoped to systems and personnel within the United Kingdom)

The Cyber Essentials Assessment is a set of baseline technical controls produced by the UK government and industry to help organizations, large and small, public and private, improve their defenses and publicly demonstrate their commitment to cybersecurity.

GxP / HIPAA Other

Informatica is validated for HIPAA controls for its handling of protected health information (PHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. This report provides Informatica’s commitment to data privacy and security compliance to protect sensitive healthcare information and implement the necessary administrative, physical and technical safeguards to ensure compliance with HIPAA regulations. (Scoped to IICS/IDMC; DaaS products.)

Informatica’s software can be used in industries that are subject to GXP regulations, such as the pharmaceutical and healthcare industries, but the company itself is not subject to GXP regulations. Informatica develops solutions that are designed to help its customers comply with GXP regulations. For example, Informatica’s MDM SaaS solution includes features that support data validation, data quality monitoring, and audit trail creation and management, which are all critical components of GXP compliance.

Informatica also provides documentation and guidance to its customers on how to configure and use its products in a way that complies with GXP regulations. (Scoped to MDM SaaS products.)

Compliance with Applicable Law

Informatica's data privacy program is designed to comply with all applicable privacy laws in the jurisdictions where we do business, including the General Data Protection Regulation, the California Consumer Privacy Act, and other state, national and international laws. The program addresses both how we use personal data that we control in the operation of our enterprise and how we protect and process personal data on behalf of customers via our services. The program is managed in accordance with a set of policies, procedures and standards governing program elements, including data management, risk assessment, employee training and awareness, consent management, incident response, vendor management and internal governance and reporting.

Informatica classifies data per our data classification policy and consistently applies protections per that classification; observes privacy principles such as transparency, purpose limitation and data minimization; honors the rights of data subjects; complies with data localization and transfer requirements; analyzes, determines lawful basis for and records processing activities; and negotiates and honors contractual and statutory obligations with respect to both vendors processing data on our behalf and customers on whose behalf we process data.

About Informatica

Informatica from Salesforce is a leader in AI-powered enterprise cloud data management. Its Intelligent Data Management Cloud (IDMC) platform enables organizations to connect, manage and unify AI-ready data across the enterprise. With capabilities spanning data cataloging, integration, governance, quality, privacy, metadata management and master data management, Informatica supports a broad partner ecosystem and helps customers unlock the full value of their data and AI initiatives.

About Salesforce

Salesforce is the #1 AI CRM, empowering companies to connect with their customers in a whole new way through the power of artificial intelligence, data, and trust. For more information about Salesforce (NYSE: CRM), visit: www.salesforce.com.

Where data & AI come to LIFE™

Informatica

Worldwide Headquarters
2100 Seaport Blvd.
Redwood City, CA 94063, USA
Phone: 650.385.5000
Fax: 650.385.5500
Toll-free in the US: 1.800.653.3871

informatica.com
linkedin.com/company/informatica
x.com/Informatica

CONTACT US