Ivanti Cloud Security

White Paper

Contents

1.0 Welcome to Ivanti Cloud

Ivanti Cloud is the embodiment of Ivanti's mission to Unify IT, and the customers who utilize this tool enjoy the convenient and secure gateway that it provides to all Ivanti products. Service management, end point management, security, identity, and automation tools are securely and intelligently accessible by the satisfied customers that utilize Ivanti Cloud.

2.0 Executive Summary

Security is one of the most important considerations when choosing a cloud partner. Ivanti takes security and data privacy obligations very seriously and implements best-in-class security and hosting practices.

Today's global, mobile workforce requires services that are always available and ubiquitous. This requires a high level of availability and vigilant industry security practices. At Ivanti, security and data protection start at product inception and continue through a "security by design" model that includes security considerations in all phases of the product—from design and implementation through operations.

This paper highlights Ivanti's approach to a comprehensive security model that encompasses the people, the organization, development, and operations.

3.0 System Description

The Ivanti Cloud Platform is comprised of five services including:

1. Ivanti Cloud – The overarching product that provides the cloud-based functionality.
2. Ivanti Discovery – This product is used to discover and inventory the hardware deployed throughout a company. In addition, it can create an inventory of devices that can then be utilized by many other Ivanti and third-party products.
3. Ivanti IT Analyst Workspace – This workspace provides tools, insights, and reporting to help IT analysts perform their job function faster and more efficiently.
4. Ivanti Real Time –This module provides a real-time view of devices and their status on the network.
5. Ivanti Patch Intelligence – This tool provides insight into the safety of the latest patches and helps manage the risk of deploying patches across an estate.

Ivanti services are hosted in Microsoft Azure data centers around the globe. The Ivanti Cloud Platform is hosted in the Microsoft Azure data centers in the following locations:

1. East US (Northern Virginia) (NVZ)
2. UK South (London) (UKS)
3. Australia East (Sydney) (MLZ)

4.0 Security Organization and Culture

4.1 Security Organization

Multiple layers of security are set in place within the Ivanti organization. Ivanti's Chief Security Officer (CSO) and Security Council are responsible for overall security communication, implementation, and response reporting to executive management. Ivanti's overall security organization includes a specialized focus on implementing and maintaining security best practices within the cloud services provided. Ivanti's engineering and architecture teams provide independent, secure design reviews.

4.2 Background Checks

All Ivanti employees go through industry-standard background checks as permitted by local legislation upon hire to verify education, previous employment, and references.

4.3 Security Training

As part of Ivanti's ongoing security awareness training, all employees are required to complete security training upon hire. Ivanti regularly trains all staff members with anti-phishing campaigns, annual acceptable use attestation, and Open Web Application Security Project (OWASP) Top 10 training for development. Ivanti also provides role-specific security training modules to employees.

5.0 Cloud Development Security

5.1 Design Reviews

Prior to and during implementation, architects trained in security best practices review designs to ensure developers adhere to security decisions on implementation. Ivanti follows best-practice models for the software development lifecycle.

5.2 Security Testing

Security testing is part of the development cycle with the use of security scanners to identify vulnerabilities throughout the cycle. Ivanti uses industry-leading, third-party tools to test and validate secure implementation as well as reduce flaws. Ivanti closely monitors, responds to, and resolves potential security issues as defined by Ivanti's Incident Response Plan (IRP). Ivanti employs a multi-tiered approach to ensure a comprehensive and secure development process.

6.0 Operations Security

6.1 Physical Security

Ivanti leverages the security provided by its hosting providers, and additionally provides physical security access to its own sites. This includes a secure environment with established security controls to prevent, detect, and respond to vulnerabilities and data breaches. Ivanti also complies with local, state, federal, and international regulations regarding security, privacy and data handling, and use facilities required for ISO 27001 and SSAE 18 compliance.

6.2 Logical Security

Ivanti employs industry-wide best practice Defense-in-Depth strategies, placing multiple layers of defense throughout the cloud environment. Ivanti relies on security appliances from multiple vendors, at multiple layers of the OSI model.

6.3 Transport Security

The Ivanti Cloud transfers data securely through industry-standard methods such as HTTPS using TLS and AES 256-bit encryption.

6.4 Data Privacy

Ivanti's Data Privacy Policy satisfies General Data Privacy Regulation (GDPR) and, the California Consumer Privacy Act (CCPA) requirements, and governs Ivanti Cloud information-handling practices. See this link to access the Ivanti Privacy Policy: https://www.ivanti.com/company/legal/privacy-policy.

Privacy laws and contract compliance prevent the use of customer data for any non-customer contractual processes. Ivanti staff members are not allowed to move customer data from a customer environment for the purposes of development, test, or research. Additionally, Ivanti's Data Classification and Handling Policy and Customer Data Transfer Standard require customer data to be classified and handled such that data is protected to a level commensurate with the sensitivity of the data.

6.4.1 Separate Tenant Databases

Securely housing customer data in separate databases ensures tenant data confidentiality. Additional application-specific controls protect data from unauthorized access across multiple layers of the application.

6.4.2 Data Access Controls and Auditing

The Ivanti Cloud environment has restricted access to customer data. Ivanti uses several layers of controls for monitoring, including administrative and technical controls. Customers can choose to authorize access to Ivanti Cloud Operations staff for testing or validation purposes.

6.4.3 Ivanti Cloud Storage Data and Privacy

Data stored in the cloud will remain there until the customer requests its removal. To request removal of data, the customer simply sends a request to the assigned Ivanti representative. The data is stored in tenant-specific blob storage to ensure customer security and privacy.

Tenant-specific Azure SQL databases or Elasticsearch databases can only be accessed by the tenant. Customers only have access to their own data. No customer can access, view, or alter any data from any other customer. Teams are available to troubleshoot any issues that may arise with a customer, but Ivanti will not conduct any action without written approval from that customer. Audit trails are in place to record any actions performed on the customer's behalf, along with a traceable link of their express approval.

Ivanti offers a credential vault which stores Customer credentials in the cloud. Controls are in place to ensure that only services on behalf of the tenant can request credentials from the credential vault. Customer data in the cloud is stored by tenant, meaning that only that customer (tenant) can access the data.

Anonymized data is applied to Data Science/Machine Learning for research purposes, to develop machine learning models and or peer data evaluation. Per the EULA, no customer Personally Identifiable Information (PII) will be shared with the data science team or any other customer.

- Ivanti GDPR Documentation

https://community.ivanti.com/docs/DOC-67844

- Ivanti Privacy Policy

https://www.ivanti.com/company/legal/privacy-policy

6.4.4 GPS Location Data

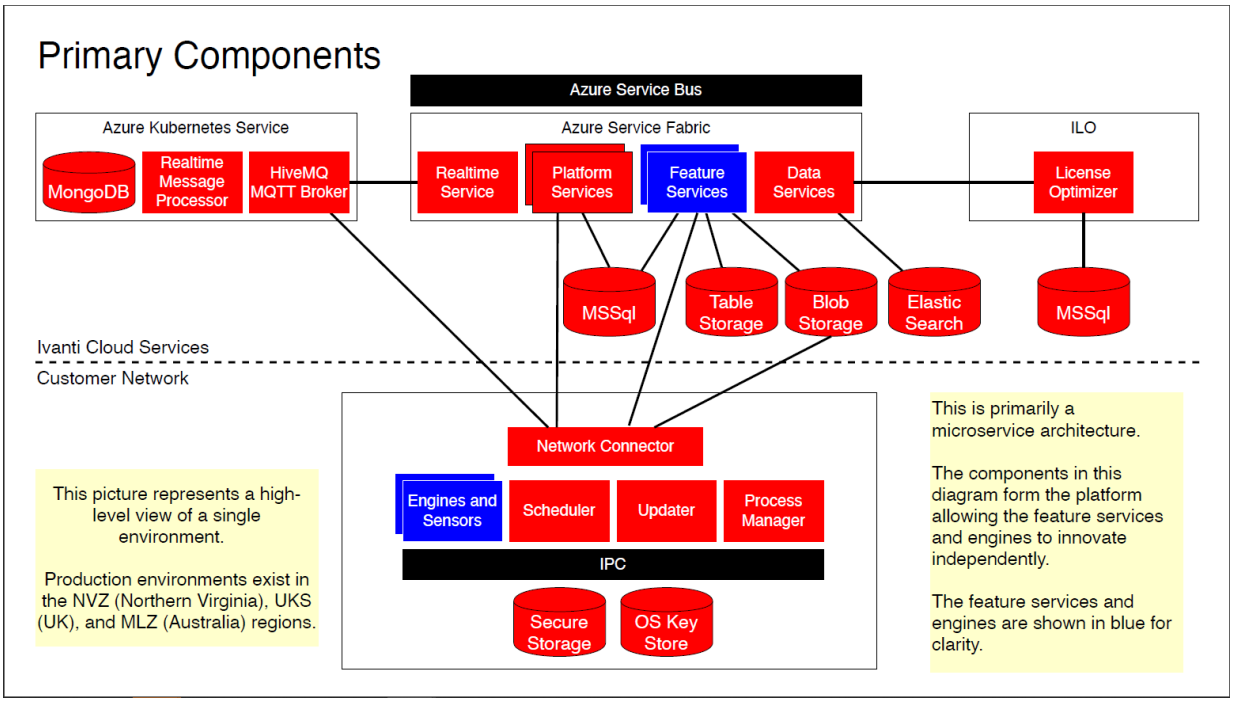
GPS Location data is gathered using Windows Location Services. This means that it uses multiple mechanisms to determine the computer's location in order of their trustworthiness. The data is provided through an Ivanti Cloud Realtime sensor and can be turned on or off.

6.5 Disaster Recovery (DR)

Disaster Recovery tests are performed annually. Ivanti's DR Plan addresses restoring databases, restarting Configuration Services, and completing testing to ensure the restoration is complete. In the event of a disaster, Ivanti personnel will also investigate to see if any components are missing or not connecting properly.

Ivanti Cloud databases are backed up and can be restored to the minute. Ivanti's Cloud Infrastructure team uses Azure interfaces to bring the database to the point and time where damage occurred. Ivanti Cloud maintains an RTO of four (4) hours and an RPO of 15 minutes.

6.5.1 Architecture Diagram



6.6 Cloud Premise Synchronization

Ivanti Cloud can import data from several sources such as EPM, Active Directory, Microsoft's System Center Configuration Manager (SCCM), Data Center Discovery, and CSV reports. Data import services are continually enhanced to achieve maximum value to Ivanti Cloud users.

6.7 Ivanti Cloud Agent

The Ivanti Cloud Agent consists of multiple components, including the Agent Framework, a set of Engines, and a set of Sensors that are executed by the Realtime Engine. The Agent Framework networking component runs as Network Service so that it has network access but strictly limits privileges on the local machine. It communicates through an authenticated local IPC channel with a Dispatcher component that runs as a Local System, so that it has local privileges to perform the work it needs to do, but it does not have any networking privileges.

6.7.1 Communication

The Ivanti Cloud Agent communicates with the cloud several times a day. Discovery data is uploaded as often as daily or as little as weekly depending on how the customer has configured it. The agent will retrieve the latest connector settings from the cloud every 1-2 minutes. The time frame is not configurable in agent settings but is configurable within the discovery data collection. The method is secured using TLS Encryption.

The Ivanti Cloud Agent collects complete device inventory from the core, along with the software usage and all attributes associated with the devices. The data collected is then stored in the Ivanti

Cloud in a tenant database saved by customer ID to prevent other customers from viewing the data. Powered by Microsoft Azure, the information is uploaded via secure network connection over HTTPS.

6.8 Configuration and Set Up Requirements

The communications that the Ivanti Cloud Agent requires are the following:

- .NET Requirements - .NET 4.7.2
- Ports – 443 (Outbound) and 8883 (MQTT)
- Protocol – HTTPS
- Hostname - *.ivanticloud.com

7.0 Conclusion

Ivanti recognizes and implements best-in-class security practices with world-class products that unify IT. Ivanti teams and customers alike utilize the Ivanti Cloud to safely access and store data and make full use of Ivanti's full artillery of product solutions.

Ivanti's cloud services are delivered with data protection, high availability, and performance standards in mind. Ivanti's goal is not only to educate and support customers with tool acquisition, but to create a lifelong relationship of trust and reliability. The genuine desire to nurture this culture of trust is evidenced by the rapid growth and development of Ivanti's cloud services.

For more information on Ivanti's cloud services and other products, please visit www.ivanti.com.

www.ivanti.com
1.800.982.2130
sales@ivanti.com