ivanti

Ivanti Cloud Security

White Paper

Contents

Welcome to Ivanti Cloud

Ivanti Cloud is the embodiment of our mission to Unify IT, and our 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 our satisfied customers that utilize Ivanti Cloud.

Executive Summary

Security is one of the most important considerations when choosing your cloud partner. We, on the Ivanti Cloud team take our security and data privacy obligations very seriously, and we implement 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 starts at product inception and continues through a "security by design" model that includes security considerations in all phases of the product—from design, implementation, and continuing through operations.

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

1. Security Organization and Culture

1.1 Security Organization

Multiple layers of security are set in place within the Ivanti organization. Ivanti's Corporate Security Council (CISO) and cloud security office are responsible for overall security communication, implementation, and response reporting to executive management. On our cloud security team, part of the overall security umbrella organization has a specialized focus on implementing and maintaining security best practices within the cloud services provided. In our engineering organization, our separate architecture team provides independent, secure design reviews.

1.2 Background Checks

All Ivanti employees in the United States go through industry-standard background checks upon hiring to verify education, previous employment, and references.

1.3 Security Training

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

2. Cloud Development Security

2.1 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 our software development lifecycle. This process includes security training for our architects, developers, QA, and our support staff.

2.2 Security Testing

Security testing is part of the development cycle with use of security scanners to identify vulnerabilities throughout the cycle. We use industry-leading, third-party tools to test and validate secure implementation as well as reduce flaws. We closely monitor, respond to, and resolve potential security issues as defined by our Computer Security Incident Response Plan (CSIRP). We employ a multi-tiered approach to ensure a comprehensive and secure development process.

3. Operations Security

3.1 Physical Security

Ivanti leverages the security provided by our 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. We also comply with local and state, federal and international regulations regarding security, privacy and data handling, and use facilities that are ISO and SOC-compliant. Enhancing our geographical dispersion and redundancy is a key focus of the Ivanti Cloud Team in 2019.

3.2 Logical Security

Ivanti employs the industry-wide best practice Defense-in-Depth strategies, placing multiple layers of defense

throughout the cloud environment. We rely on security appliances from multiple vendors, at multiple layers of the OSI model.

ISC2 CISSP-certified engineers actively monitor and manage security incidents in cloud security infrastructure. The engineers are available to address any kind of security issue for the cloud datacenter. We have a 24x7x365 Security Operations Center that monitors and responds to SIEM alerts.

3.3 Transport Security

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

To support back-end integration from your network, Ivanti can provide VPN connections using industry-standard AES (128 or 256) IPSec encryption. VPN's are optional and depend on the security practices of our customers and whether or not a VPN is required.

3.4 Data Privacy

Ivanti's Data Privacy Policy satisfies General Data Privacy Regulation (GDPR), 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.

3.4.1 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.

3.4.2 Data Access Controls and Auditing

The Ivanti cloud environment has restricted access to customer data. We use 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.

3.4.3 Ivanti Cloud Storage Data and Privacy

Data stored in the cloud will be stored in the cloud 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. Ivanti Cloud Ops teams are available to troubleshoot any issues that may arise with a customer, but Ivanti Cloud Ops will not provide 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 does not store customer credentials in the Ivanti Cloud. Any customer credentials cannot be decrypted by Ivanti or anyone else. 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

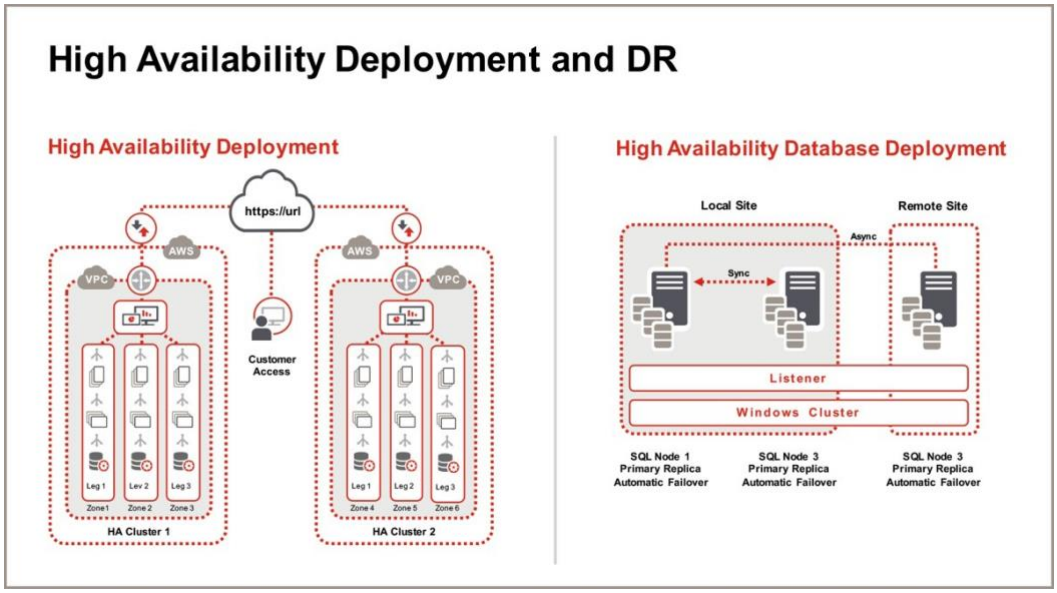

Figure 3.5.1

3.5 Availability

3.5.1 High-Availability Deployment

As seen in figure 3.5.1, we designed our application to be multi-tenant with high levels of availability. Web application tiers are redundant in design with individually scalable application components, deployed across multiple fault- tolerant zones. Application and infrastructure monitoring is available to regulate flow of traffic automatically across these zones to maximize application performance and availability. Continuous monitoring detects anomalies, and self-healing processes reduce the need for human intervention and recovery.

3.5.2 Disaster Recovery

We use always-on replication for near real-time replication of data to provide a low Recovery Point Objective (RPO) and minimize data loss in the low-probability event of a naturally occurring or human-induced disaster. We use hot backup sites for our core services that our 24X7 NOC Operations can switch to if deemed necessary. Customers choosing our advanced reporting option can get access to this read- only database for reporting purposes without impacting their transactional system."

3.6 24X7 Network Operations Center (NOC) and Security Operations Center (SOC)

We leverage an ISO27001-certified 24x7x365 network operations team, focused on Tier 12 and Tier 2 response with Tier 3 and 4 staff on pager duty. We monitor our NOC operations responses regularly for quality and adherence to SLA. Executive staff reviews NOC SLA reports to ensure optimal operations. The SOC actively monitors security incidents using SIEM.

4. Cloud Premise Synchronization

To power Smart Advisors and other features in Ivanti Cloud, End Point Manager (EPM) synchronizes data to Ivanti Cloud.

4.1 Configuration and Set Up On the EPM Core

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

- .NET Requirements - .NET 4.7.2
- Port – 443 (Inbound and Outbound)
- Protocol – HTTPS
- Hostname - *.ivanticloud.com
- EPM 2017.3 SU5 is the minimum supported version

4.2 Ivanti Cloud Agent Communication with EPM Core

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 and SSL 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.

4.3 Ivanti Cloud Data Importing

In addition to EPM, Ivanti Cloud will import data from other sources including:

- Active Directory
- Microsoft's System Center Configuration Manager (SCCM)
- Data Center Discovery
- CSV

5. Conclusion

Ivanti recognizes and implements security best-in-class practices with world class products that unify IT. Teams within Ivanti 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.

Our cloud services are delivered by our professional cloud-hosting organization with data protection, high availability, and performance standards. Our goal is not only to educate and support our customers into 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 our cloud services and other products, please visit www.ivanti.com.

Learn More

www.ivanti.co.uk
+44 (0) 1344 442100
sales@ivanti.com