Glassbeam White Paper

Data Security In the Cloud

Contents

Data security in the Glassbeam cloud

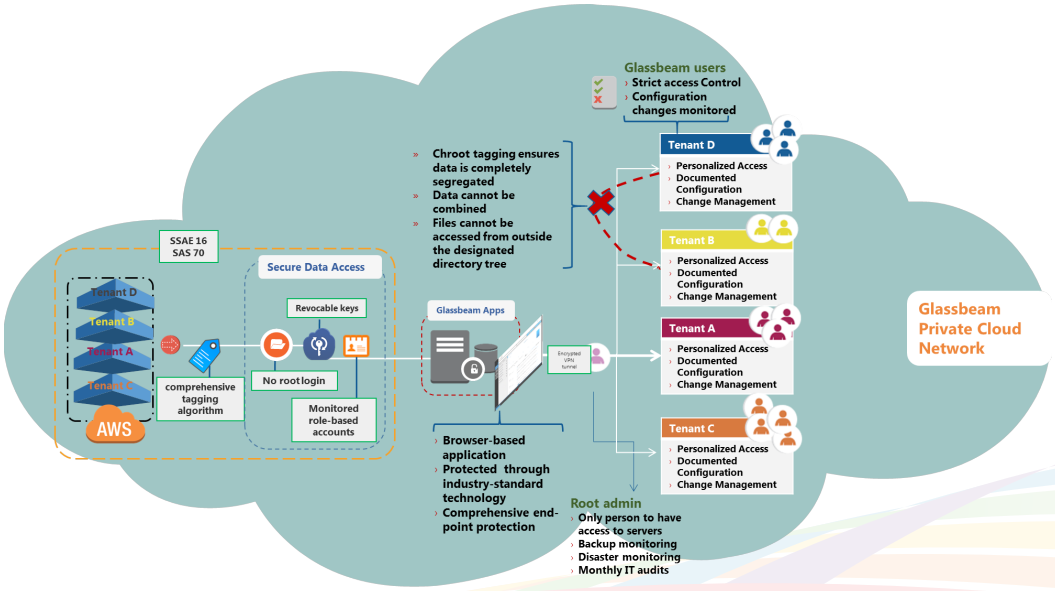
Whether your focus is machine data, financial and healthcare information, or confidential intellectual property, data security is a vital concern. At Glassbeam, we make sure that your data is absolutely safe by integrating security technology and best practices into every aspect of our operations. All the data in our cloud is protected by the same standards and certifications that safeguard sensitive information around the world. And we make sure that your data is never at risk as it flows from your network to ours.

Security starts at home

We exist to help you gain the most value from your machine data, so you can troubleshoot faster, build better products, and increase revenues. We do this by analyzing structured and unstructured data generated by your machines.

Machine data is a collection of product operational data such as system identifiers, configuration information, performance statistics, and system notifications. It should not contain sensitive information such as credit card or social security numbers. But it is your intellectual property, and we make absolutely certain that it is protected.

Figure 1. Secure Transmission Through the Public Network



We start with a one-way transmission from your system to our cloud. It's based on secure mechanisms such as the public key that you provide us, which is stored on our server. Our preference is that you use a 2048 bit key, but that is up to you. The point is that you have access to our system with the level of security that you select, but we can't access your systems.

We ask you to send your data to us using standard encryption protocols, with the strongest encryption key that you can provide up to 2048 bits and no less than 256 bits. Glassbeam can capture data sent via cryptographic network protocols for secure data communication such as Secure Shell (SSH), Secure Copy (SCP), SSH File Transfer Protocol (SFTP), or through an encrypted tunnel over a virtual private network (VPN).

We support all the standard encryption protocols, so your encrypted data is safe as it travels through the public network to our server. Data in transit is further protected because each TCP/IP packet is sent via a different route, and the packets are sent out of sequence (see "Figure 1. Secure Transmission Through the Public Network").

Protecting data in the cloud

After its safe journey through the public network, your data's destination is one of our cloud-based infrastructures. We have infrastructures hosted at Amazon Web Services (AWS) and Dimension Data. Both of these partners are industry-leading Platform-as-a-Service providers, and both are fully SSAE 16 (SAS 70) compliant. Your data is never stored at a Glassbeam business office, and access to your data by Glassbeam personnel is controlled by strict security measures:

Revocable keys: Your data repository is only accessible via the public SSH key that you provide. You can request that your public key be removed or replaced at any time, for any reason.

Role accounts: Access to your data by Glassbeam employees is controlled by role-based accounts. Only a few experienced system administrators are empowered with the Operations Role required to access your data, and their activities are monitored.

No root login: The root login to the system is prohibited and permanently closed in all

Glassbeam cloud environments. All system access is personalized and monitored. And all critical system and configuration changes are monitored and documented through configuration management and change management processes.

The receiving servers in our cloud also use elite security best practices. The entire architecture is a next-generation stack, built for secure multi-tenancy. The heart of our multi-tenancy security system is its comprehensive tagging algorithm, which tags all data to a unique hierarchical combination of manufacturer, product, and schema. Data is also tagged at the end customer level, so users only have access to the data for which they are authorized (see “Figure 2. Data Segregation in the Cloud”).

The tagging algorithm uses chroot to ensure that each customer’s data is completely segregated and cannot be combined. The chroot operation changes the apparent top directory in the file system, which ensures that files cannot be accessed from outside the designated directory tree. Even we could not combine data from different customers; it simply is not possible. All customer data is separate and secure.

The Glassbeam application that runs on these servers uses the Apache Cassandra database for analytics, which delivers both high performance and high availability for large amounts of data. Full-text search is supported through the Apache Solr platform. Each platform is secured with a separate primary authentication key.

The application is browser based, with Internet security provided through industry-standard technology. Data security within the application is assured by access control and employee life cycle management. Because the only access to your data is provided through our application, we have the power to implement secure business rules on that data for absolute security.

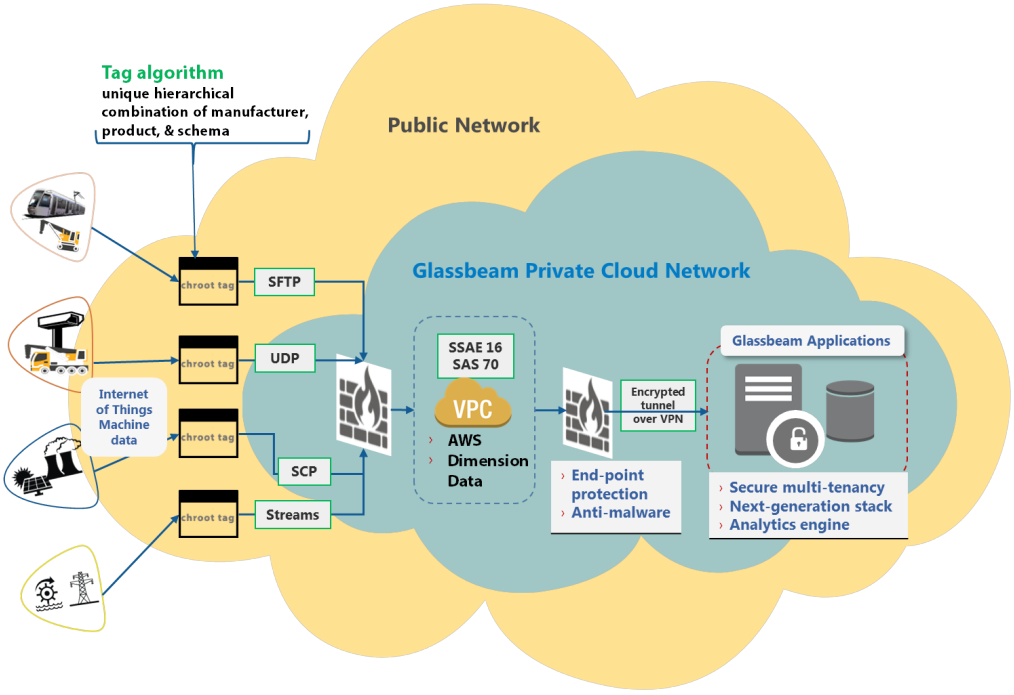
Access to servers is limited to IT personnel, who connect through a secure VPN (or SSH) with Endpoint Protection. Endpoint Protection ensures that no malicious software can be introduced through the VPN tunnel. Root access is only provided to the system administrator. All other authorized users are provided limited application-level access.

Stringent security measures are in place at all stages of the employee lifecycle

for granting and revoking access to the data. Roles are restricted such that no sensitive information can be copied without leaving a trace. Monthly IT audits are conducted to ensure that the security policies have been enforced.

Additional capabilities ensure that your data remains secure, available, and consistent in the event of an unforeseen disaster. A comprehensive backup policy covers raw log files, processed data, installed software, and operating systems. Cloud storage lets us use geographically dispersed data centers for remote disaster recovery. Our combination of full and incremental automated backups with zero downtime ensures that the latest data is available at any point in time. And our support staff regularly monitors the backup process to make sure that recovery is performed in a timely manner.

Figure 2. Data Segregation in the Cloud



Conclusion

Ensuring the safety of the data that you entrust to us is central to our business. That's why we partner with the best cloud service providers in the business, and why we use the same standard, industry-recognized security mechanisms in our own network. But at Glassbeam, security means more than implementing the right products and technologies.

We understand that every bit of customer data is critically important, and must be protected at all costs. Our experts are constantly evaluating new security threats and solutions, and are committed to providing the finest security to our customers and within our own facilities. In 2015, Glassbeam addressed an exhaustive questionnaire related to security and compliance issues as part of a customer engagement. The findings are summarized in the next section.

Appendix – Security Audit

Glassbeam worked with a third-party firm to assess the robustness and completeness of its security apparatus to address these security questions.

The questions were broken down into these categories:

- Risk Assessment and Treatment
- IS Policy Management
- Organization of Information Security
- Asset Management
- HR Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition Development and Maintenance
- Information Security Incidence Management

Risk Assessment and Treatment: The questions here relate to processes to manage 3rd party relationships, procedures for access controls, procedures to documents and manage security terms, periodic review of 3rd party providers, managing inventory of risk items, timing of vulnerability scans, timing and frequency of penetration tests, and more.

IS Policy Management: The questions in this category relate to IS policies and procedures and the timing and processes for their periodic review.

Organization of Information Security: This Category deals with documents that outline the scope, objectives and responsibilities that deal with IS policy, roles and responsibilities of the Chief Security Officer (CSO), timing of periodic reviews of these documents, and security awareness programs.

Asset Management: The questions here involve procedures for data classification, inventories of the following items: customer classifications, application data elements and service documentation, annual reviews of classification schemes, procedures for media handling/protection, and certificates of destruction.

HR Security: The questions in this category relate to background screening programs, employee access control, technology control plans to maintain compliance, background checks of employees with access to customer data, and documented procedures for people leaving the organization.

Physical and Environmental Security: These questions relate to the following attributes of data centers: access control, physical layout, material used in construction of data centers, and security of access points like HVAC, air-conditioners etc. Additionally, the category has questions relating to characteristics of service centers: authorization of employees, receiving/delivery procedures, physical control mechanisms, visitor management procedures, CCTV coverage, resolution of CCTV cameras and more. Finally, there are questions that relate to procedures like badge control, key control and trash control.

Communications and Operations Management: This section covers policies and procedures to guard against viruses and malicious software including escalations, alerting, incident management, training personnel in AV management, updating malicious code signatures. It also covers areas like data replication, logical destruction, backward compatibility, change control procedures, firewall deployment, and network operation procedures. Finally, this section covers areas like Intrusion Detection Systems (IDS), Backup scheduling and Management and Maintenance reviews.

Access Control: This category deals with access control procedures, access

assignment, training and external documentation, creation and reuse of unique identifiers, multi-factor access controls, password management and procedures for remote access.

Information Systems Acquisition Development and Maintenance: This is a broad category that touched upon numerous topics: Message integrity, Application Security (Training, Source Code Protection, Confidentiality, Segregation of duties, and so on), Cryptography, design of Cryptographic controls, key management, control of operational software, input data validation, change control procedures, restrictions on changes to software packages, control of technical vulnerabilities, Shared IDs, logging and monitoring, and protection of system test data. Of the 145 questions, Glassbeam was found to be compliant in 139 areas. Of the 6 areas of non-compliance, some were being implemented but not documented as formal procedures.

Information Security Incidence Management: The questions in this category relate to annual playbook testing, incident training, annual training refreshers, and external facing documents.

Glassbeam was found to be fully compliant with all security requirements mandated by this questionnaire. We have instituted strict processes for periodic review of our policies, documentation, procedures and technology systems to ensure that we stay compliant with these stringent requirements. Glassbeam stays committed to maintain the highest level of security required to keep your machine data completely safe and private.

Contact us at sales@glassbeam.com

Glassbeam, Inc.
5201 Great America Parkway, Suite 360 • Santa Clara, CA 95054
Phone: 408-740-4600 • www.glassbeam.com