Security Whitepaper

Security White Paper
Oct 28, 2019

Contents

About IT Glue

As the industry standard for documentation trusted by thousands of Managed Service Providers and IT professionals, we take our commitment to security seriously. IT Glue abides by strict measures to protect the security and privacy of your valued data. In addition, we understand that having reliable access to your data, with no downtime, is critical for your business. To ensure both of these objectives are met, we have adopted industry-leading security measures including SOC 2 (Type II), multi-factor authentication (MFA), Single-sign-on (SSO), host-proof hosting, and many others.

Our Security Promise

As the industry standard for documentation and trusted by thousands of Managed Service Providers and IT professionals, we take our commitment to security seriously. IT Glue abides by strict measures to protect the ongoing security and privacy of your valued data. In addition, we understand that having reliable access to your data with no downtime is critical for your business. To ensure both of these main objectives are met, we have adopted industry-leading security measures including SOC 2 (Type II), multi-factor authentication (MFA), single-sign-on (SSO), host-proof hosting, among others.

Summary of Key IT Glue Security Principles

Summary of Key IT Glue Security Principles

- **SOC 2 (Type II) Compliance:** IT Glue is the only IT documentation platform in the channel that has acquired Service Organization Control 2 (SOC 2) Type II, an internal controls report that captures how well data is safeguarded and the degree to which those controls are operating at industry best practices. This report ensures we are meeting stringent requirements set by the AICPA. The result is a platform that has been developed under an audited process to guarantee the highest level of trust and security.
- **Secure Platform:** Using Amazon's hosting platform, AWS, we ensure the most flexible, reliable, and secure computing environment with the best global network performance available today. AWS is designed and built for redundancy and, through their denial-of-service protection and PCI-level security measures, we can monitor your data on a 24-7-365 basis.
- **Password Encryption:** Rely on the highest standard of encryption in the industry today. Passwords are encrypted with AES-256-bit encryption including 2048-bit RSA public key with unique keys for each customer and secure random keys unique to each password.
- Host-Proof Hosting: IT Glue Vault is designed to allow a user to only decrypt exclusively at the endpoint level on the user's browser with a user-specific passphrase rather than syncing it to the IT Glue system.
- **Multi-Factor Authentication (MFA):** Once enabling MFA, users cannot log in to the app and view any passwords without having their username, password, and virtual appliance, thereby securing enabled IT Glue IDs. All users employing MFA are prompted for their username and password plus an authentication code generated by an authenticator application.
- **Enterprise Features:** IT Glue allows Administrators and Manager users to add layers of control to establish security permissions where needed. Password changes are version controlled and access is easily restricted to specific groups and users of your choosing. Passwords that are viewed are then automatically tracked in an audit trail entry within the activity logs.

For more information, please visit our online resources:

- Trust – www.itglue.com/about/trust
- Privacy Policy – www.itglue.com/privacy
- Terms of Service – www.itglue.com/terms
- SOC 2 (Type II) Compliance

SOC 2 (Type II) Compliance

We have always operated by a comprehensive set of security systems based on industry best practices, including ISO 27001 and PCI-DSS. As of March 2017, we have been officially SOC 2 (Service Organization Control 2) compliant and we are also audited on an annual basis. IT Glue is the only IT documentation platform in the channel that has maintained SOC 2 (Type II) compliance.

This is one of the many ways that we demonstrate our commitment to security and follow industry best practices to secure your valued data. Type II requires the implementation of the controls over a minimum six-month period in addition to the ongoing attestation of the operating effectiveness of the controls. Comparatively for Type I, controls needs to be in place, however acceptable security processes only need to be verified at a specific point in time.

Our security infrastructure and procedures are tested and audited by third-parties on a regular basis as they relate to the Trust Services Principles and Criteria; the security, availability, processing integrity, confidentiality, and privacy of a system.

Trust Service Principles & Criteria

In compliance with SOC 2 (Type II), IT Glue has worked to meet every Trust Service Criteria by effectively operating within the controls required to meet them. Not only is this a testament to the security of our platform, this is also our way of securing our business.

Logical Access Protection

IT Glue has implemented a layered security system to restrict logical access and detect potential harmful actions. This includes firewalls, network segmentation, hardened servers, IP white-listing and encryption to ensure data is protected. Logical access rights are tested as part of our quality assurance (QA) process. Logical access controls and change management tools restrict the ability to migrate between development, test, and production to change deployment personnel.

Firewalls are in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks. We have also established firewall rules and the online system limits the types of activities and service requests that can be preferred from external connections.

Production Security Architecture

IT Glue's production systems leverage AWS security systems in a layered security model. Each layer provides role-based controls to limit access to systems and users. Systems are hardened, changed-controlled, and monitored 24/7 by IT Glue. System logs are sent to the AWS CloudTrail for monitoring and review.

Security controls are monitored using several methods:

- Vulnerability Scanning - Vulnerability scans are performed internally and at least quarterly. Independent vulnerability scans are performed by a third-party vendor at least quarterly.
- Penetration Testing - External penetration testing is performed by an independent third-party at least annually.
- Internal Reviews - IT Glue performs a review of the hardening standards and its implementation at least annually. Firewall rules are reviewed at least semi-annually.
- Internal Audit - Independent internal auditing is performed on the controls at least annually.
- System Monitoring - IT Glue's Development Operations Team monitors the availability of production systems through automated systems. Logs and events are then centrally managed and analyzed by the team.

Change Management

We have implemented a change management process within our production teams, including segregated development, integration, test, and production environments. Our software change control process requires all changes to code to be documented, a risk assessment completed, a code review completed by a senior developer or engineer, and Quality Assurance (QA) processes to be completed which evidences that approval for change was obtained before production. Change management is also implemented on our production servers, including documentation of changes, risk assessments, and approval processes.

All incidents are documented, including steps to contain the issue, root cause analysis, long term solutions, and related evidence and communications. High severity incidents require an analyst to determine the root cause and changes are recommended to eliminate the incident from reoccurring.

Availability

To manage the demand for processing capacity and to enable the implementation of additional capacity commitments, we ensure that systematic network and monitoring is in place. Daily and monthly task and event logging is maintained. Automatic backup systems are utilized to perform scheduled system backups of target data while backup jobs are monitored with notification alerts sent out in the event of backup failure. IT Glue has a backup schedule in place to automatically initiate production backup jobs. Finally, restore operations from backup media are performed as a component of disaster recovery operations to verify that out system components can be recovered.

Secure Platform by Amazon Web Services

IT Glue uses Amazon Web Services Inc. (AWS), a third-party data centre provider, to host and maintain its production computing systems. Currently, AWS is responsible for the physical security of our environmental protection, power and environmental protection, networking, database platform, and hosting infrastructure. We utilize the AWS security group and load balancer functionality as the primary firewall. Data within IT Glue is stored using serval AWS data storage solutions. We provide an integration engine called Sync which automates data synchronization with several sources. Sync runs within IT Glue's production infrastructure.

Amazon's hosting platform is one of the most secure and highly-tested systems in existence. Their entire infrastructure is PCI-DSS certified. AWS services maintain PCI-DSS Level 1, SSAE16 SOC 1, SOC 2 and SOC 3, ISO 27001, 27017 and 27018. These certifications cover selected AWS services, including their security governance, physical security, network infrastructure, change management, and administration practices. Leveraging these established services, IT Glue delivers a secure, reliable application you can trust with your operational documentation.

Reliability and Disaster Recovery

Our goal is 100% uptime. To meet this goal, the IT Glue team has architected our infrastructure and applications to be both robust and scalable. We monitor security, uptime, and performance 24/7/365 and have a dedicated team proactively managing the environment at all times. Our service is protected from external attacks through Amazon's denial-of-service protection and PCI-level endpoint security measures. Leveraging this low-latency, high-availability cloud infrastructure enables IT Glue to maintain almost five (5) nines of uptime with a 200ms average response time.

AWS has built its data centers in multiple geographic regions, with multiple Availability Zones within each region. AWS regions are completely isolated from one another for maximum fault tolerance and stability. Even though regions are isolated, they are connected to the rest of the AWS network through low-latency links to offer maximum resilience against disruptions.

IT Glue's concept of a "Datacenter" (e.g. our "North America Datacenter" or our "European Union Datacenter") refers primarily to a continental grouping of resources. For instance, in each continent, IT Glue operates its primary infrastructure within a specific AWS region, leveraging real-time data replication to a secondary region within the same continent (e.g. us-west-1 and us-east-1).

We also have two backup and disaster recovery strategies: daily backups and replications between AWS zones. In the case of a disaster, we are able to operate on a secondary AWS region. Currently, IT Glue replicates its databases between two North American AWS regions. If a catastrophic failure occurs, we have implemented failover capabilities, allowing regional failover. The database is also backed up on a daily basis in case of data corruption. IT Glue ensures that our Disaster Recovery Plan (DRP) is tested at least annually.

In the event of a region failure, data which is already replicated to another region in real-time, can be made "primary", with roughly only a 1,500ms lag in the cutover of workloads. In addition to that, IT Glue performs nightly snapshots of critical database infrastructure to be able to recover data in the event of a disaster-recovery scenario.

Password Encryption

All data transfer to and from the IT Glue application is through SSL encryption, reducing any opportunity for attacks through active connections.

Passwords are encrypted with AES-256-bit encryption and a unique AES key is generated for each encrypted password. RSA encryption is then used to encrypt the AES key used in the AES-256 password encryption with a 2048 bit RSA key pair. The RSA key pair is then encrypted with a secure RSA key passphrase and stored in an isolated key management system that is locked down to only allow access from our application servers as required for decryption.

To decrypt the data, an attacker would need to effectively access each element of our encryption process. In addition, the web servers for our application are also locked down with multiple firewalls, whitelisting incoming and outgoing traffic, key-based access, and many other measures.

When a user needs to access a password, the decryption key that is stored in the isolated key management system and the encrypted password that is stored in the database are both sent to the IT Glue application to be processed. Then, it is sent to the user browser securely through HTTPS for consumption (see Figure 1).

User accessing a password stored in IT Glue

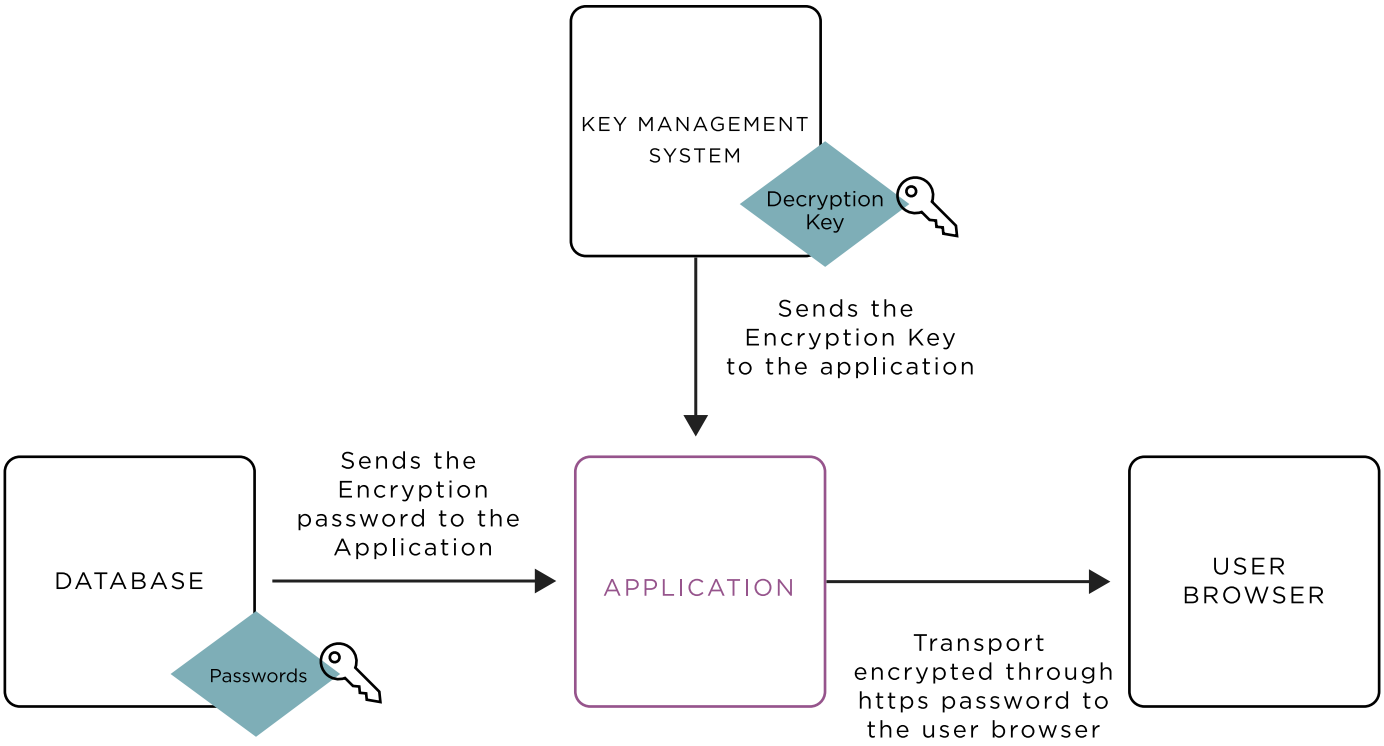

Figure 1. A user accessing a password stored in IT Glue.

Host-Proof Hosting - IT Glue Vault

Users also have the option to add an additional security layer to their most sensitive passwords.

With IT Glue Vault, host-proof hosting or client-side only encryption and decryption is designed to allow a user to only decrypt exclusively at the endpoint level on the user's browser with a user-specific passphrase rather than syncing it to the IT Glue system.

User-based passphrase

IT Glue Vault is encrypted using AES-256-GCM and a unique AES key is generated for the Vault. An IT Glue Administrator may choose to grant Vault access to other users by giving them a copy of the Vault AES key. RSA encryption is then used to encrypt the user-based AES key with a 2048 bit RSA key pair. This unique RSA key pair is then protected by the user-based Vault passphrase which only the user has access to. Each IT Glue user granted access can only access the passwords within the Vault based on their security permissions.

A number of encrypted keys are sent to IT Glue but none may be decrypted without the user-based Vault passphrase which IT Glue servers do not have access to at any point so, it is not possible for us to decrypt the data (see Figure 2).

User accessing a password stored in a Vault within IT Glue

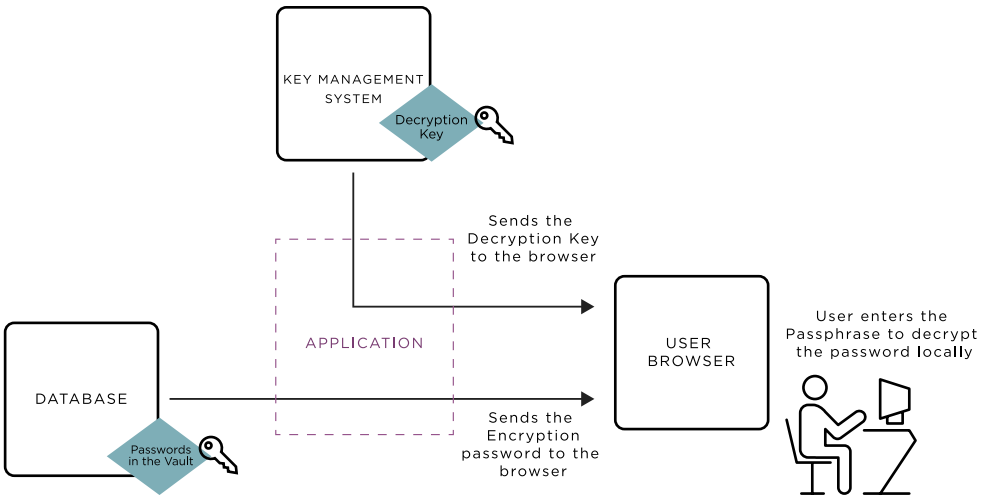

Figure 2. A user accessing a password stored in the Vault within IT Glue.

We have consulted many security and software experts and incorporated industry-leading security practices as we were developing the Vault. The Vault gives each user the total control with a user-based passphrase, not an organization-based passphrase that every employee shares. Having a user-based passphrase means that only the user has the decryption key to the Vault and that the encrypted Vault passwords are meaningless to IT Glue or anyone else without the decryption key. Having a user-based passphrase also means an IT Glue administrator doesn't have to change the passphrase every time an employee leaves.

Multi-Factor Authentication

IT Glue encourages all users to enable Multi-Factor Authentication (MFA) to add an additional layer of protection on top of your username and password when accessing IT Glue. With MFA enabled, a user will be prompted for their credentials, as well as another piece of login information, when signing in to IT Glue.

IT Glue currently supports most one-time password (OTP) compliant applications and can be used as an additional factor for MFA logins to IT Glue: https://kb.itglue.com/hc/en-us/articles/213293197-Set-up-multi-factor-authentication-MFA-

Enterprise security features

IT Glue also offers additional layers of control and protection via security permissions and activity logs. Access to passwords can be controlled at a granular level by limiting access to any combination of users and groups. Revealed passwords only remain visible for a short time with each reveal resulting in an audit trail entry. In addition, all password changes are version controlled and immutable with full roll-back capabilities.

Conclusion

One of IT Glue's core values is Trust: Champion complete vigilance for the privacy and security of information. We take our internal processes and compliance with industry-level security standards seriously. Through our platform, IT Glue offers you a way to effortlessly maintain the integrity and safeguarding of your data and documents. By embedding security features into our software and maintaining rigorous adherence to our third-party audits, we continue to provide you the documentation services you use in your business daily.