Spectrum House
Beehive Ring Road
Crawley
RH6 0LG
020 3997 7979
transform@ithq.pro

ITHQ

Service Definition Document

Service Definition

ITHQ provide a solution which will capture the configuration of your IT assets and feed the results into an automated documentation system, tracking changes, detailing relationships between assets as well as reporting and alerting functionality.

Service Features

1. Automated polling of IT systems to track configuration changes
2. Historical snapshots of device configurations
3. Relationship mapping between devices and assets
4. Reporting and metrics on managed devices
5. Detect and alert on changes to critical infrastructure
6. Pre-Built integrations with all common enterprise software solutions
7. Enterprise-grade security with SOC2 compliance
8. DNS Domain & SSL Certificate tracking
9. Immutable audit trail

Service & Benefits

10. Reduce risk with automated documentation and change tracking
11. Single source of truth for enterprise configuration tracking
12. Ensure availability of system configuration data using SaaS solution
13. Actionable alerts if unexpected changes are detected
14. Monitor and report on cloud licensing utilisation
15. Automated system polling removes requirement for manual intervention
16. Self-Service functionality to remove silos of knowledge
17. Automated device discovery ensuring compliance with policies

Onboarding / Offboarding

Onboarding / Offboarding activities will be quoted as per our SFIA rate card. Please contact us for more information.

LionGard Data Security Measures

In order to protect Partner's Confidential Information, Liongard will (i) implement and maintain all reasonable security measures appropriate to the nature of the Confidential Information including without limitation, technical, physical, Confidential administrative and organizational controls, and will maintain the confidentiality, security and integrity of such Confidential Information; (ii) implement and maintain industry standard systems and procedures for detecting, preventing and responding to attacks, intrusions, or other systems failures, and regularly test or otherwise monitor the effectiveness of the system's key controls and procedures; (iii) designate an employee or employees to coordinate implementation and maintenance of its Reasonable Security Measures; and (iv) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Partner Confidential Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any systems in place to control these risks (collectively, Reasonable Security Measures).

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 acess is easily restricted to specific groups and users of your choosing.

Payment Terms

The Documentation Automation solutions is paid monthly in advance and comprises the LionGard and ITGlue licenses.