DATA SHEET

AutoRABIT Platform

Built for Security and Compliance

Flexible deployment models support risk reduction, privacy, cost control and security

SaaS | Self-Managed Cloud | On-Premises

Flexible Deployment Options to Support Data Sovereignty

We have several hosting options available including choice of AWS, Azure or GCP (and all in the region of your choice). Alternatively, you can choose a private cloud or on-premise deployment. Data backup locations for AutoRABIT Vault have similar choices, regardless of application instance deployment location.

Certified and Compliant

ISO 27001, SOC2, and certified for the USA's HIPAA compliance. Supports the "right to be forgotten" for GDPR and California's Consumer Privacy Act (CCPA).

Encryption and Data Masking

With the AutoRABIT platform, your data-at-rest and in-transit is secured with AES-256 encryption. For data-at-rest - Data backups with Vault use "bring your own key" (BYOK) for AWS storage so that only you have access to your data. Data Masking capabilities ensure that developers can use a full representation of your data for development, QA, and Test – without exposing PII. Integration with Salesforce Shield ensures that your production deployment compliance and regulatory requirements are supported. For data-in-motion – VPN support public and private cloud environments and secure communications for sessions and integrations.

Support for Quality Code at Speed

Poor quality code and improperly handled Salesforce Metadata can expose sensitive information in violation of compliance and regulatory requirements. AutoRABIT's quality gates, unlimited metadata depth and awareness, automation (to reduce errors from manual processes), and control of metadata at a granular level directly support high-quality code and metadata handling.

Audit and eDiscovery Support

Audit and eDiscovery support Detailed reporting of who, when, where, and what changes were made by developers, salesforce admins, release managers, etc., directly supports compliance auditing and eDiscovery requirements.

Access Controls

Segregation of duties and role-based-access controls (RBAC) are directly supported on our platform. Integration to SSO (available for an additional fee) authentication using any SAML 2.0 provider (Octa, ADFS, and others) enables multi-factor authentication support. Secure access to integrations with Salesforce and integrated tools are also supported - Oauth 2.0 JWT token-based authentication for integration to Salesforce and certificate-based Git authentication.

Salesforce's Unique Security and Compliance Challenges

Sensitive Information is Pervasive

Repositories of operating data, customer personal information, business methods, healthcare records, and financial accounts require:
DevOps: Developer-level data-specific controls and auditability. DataOps: Backup and restore capabilities that meet compliance and IT security requirements.

Salesforce Metadata Increases Risk

Unique Salesforce metadata persists, inherits, and propagates:
DataOps: Can lead to exposure of sensitive or protected data without Salesforce-specific backup and restore controls.
DevOps: Can compromise release quality, leading to downtime and exposure of sensitive or protected data if improperly handled.

DevOps Tool and Integration Complexity

Source control, code quality analysis, testing, build, automated lifecycle management, and other tools can increase exposure risk with each additional step.

DataOps RPO and RTO Objectives

Operational compliance requirements mandate minimum objectives for availability and service restoration.