ReadyRedact Security White Paper

Overview

The ReadyRedact cloud platform is designed to help customers securely redact and store their digital documents to meet their own compliance and security needs. ReadyRedact realizes that helping to protect its customer's data, to mitigate potential risks, and to comply with relevant data protection laws, regulations and standards is essential to building trust and delivering a high-level of service. ReadyRedact treats security with the highest priority and embeds security protocols in all aspects of the business. This paper outlines the company's approach to security and compliance standards.

Application Security

Integrations and APIs

All integrations with the ReadyRedact application programmatic interface (API) leverage HTTPS/TLS encryption. The user security model is enforced at the API level, ensuring that data retrieved through the API is still subject to user authentication and access privileges. ReadyRedact also provides the ability to terminate API keys and create new API keys. ReadyRedact encourages customers to routinely rotate API keys as a standard best practice.

Databases

All ReadyRedact databases follow these security standards:

- All data is encrypted at rest using the latest encryption algorithms.
- All PII and otherwise sensitive data is encrypted at a column level.
- Communications between the ReadyRedact application and databases are only sent over SSL/TLS connections.
- Master database credentials are never utilized by ReadyRedact employees or applications. Additionally, these credentials are secured via two factor authentication.
- Application database credentials are rotated regularly on an ongoing basis.
- All databases are behind network firewalls and are isolated to private network subnets.
- Database access logs are maintained and stored for 180 days.

User Access

End users may access the data only through the application layer. Whether this access is through the user interfaces or through the publicly available API, it enforces user access controls to limit access to customer data only to authorized users and personnel. For security purposes ReadyRedact does not

provide end users with direct access to any database. This approach prevents unauthorized services or systems from accidentally or maliciously retrieving or modifying customer data. Additionally, ReadyRedact allows end users to create roles that grant and deny access to any users in the account. Every action taken by a user in the application is logged and available via user facing reports.

Application and Data Resiliency

All application and database servers are load balanced across multiple data centers to aid in application availability and to prevent from data loss. At a minimum, ReadyRedact spreads these servers across two or more data centers. Additionally, automation is in place to automatically heal and/or replace unhealthy servers as needed to maintain this configuration.

User Security

Authentication

ReadyRedact's architecture relies on a centralized authentication and authorization security framework to control access to services. The security framework enables the enforcement of security policies by requiring password strength, algorithms to set minimum password length
and complexity, and progressive timeout on the login API to mitigate the risks related to password-guessing attacks. Customers may also choose to utilize two-factor authentication, which adds another level of security to user logins.

Role Based Access Control

ReadyRedact users are assigned to roles that are created and managed by users of the account with permissions. Roles grant and deny access to functionality within the application. All user actions, regardless of role, are audited and made available via user facing reports.

User Session Expiration

User sessions automatically expire after 30 minutes of inactivity at which time the user's session is forcibly logged out of the system.

Access Control

ReadyRedact has implemented access control policy and enforcing mechanisms which comply with industry best practices. The rules are applied across all internal systems and the ReadyRedact platform to ensure that only authorized users with proper business justification
have access to internal and customer data.

ReadyRedact enforces the principle of least privilege for all systems with data classified as confidential, restricted, or highly restricted. It applies industry standard password policies, and, whenever possible, uses a single sign-on for access to internal company systems.

Two-factor authentication is enforced for administrative access to the ReadyRedact platform and key internal systems. ReadyRedact regularly reviews access entitlements across all company systems on an ongoing basis. .

Encryption and Cryptography

ReadyRedact uses state-of-the-art cryptography technology to achieve protection of data in transit and at rest and has documented cryptographic policy and standards. All traffic outside of ReadyRedact data center(s) is encrypted in transit using TLS 1.2 and AES-256 by default.

The entire platform infrastructure is encrypted at rest on the file system level. Depending on the environment and underlying hardware, ReadyRedact uses AES-256.

Backups are encrypted using AES-256-based symmetric cryptography as well.

Physical and Environmental Security

Best-in-class providers host ReadyRedact data centers. AWS operates and maintains ReadyRedact's data centers. AWS has obtained a wide range of security certifications and compliance standards, including ISO 27001:2013, SOC 2 Type II, PCI-DSS, HIPAA, and GDPR.

All data centers also feature at least N+1 redundant HVAC and UPS, diesel-powered generators, and multiple internet connections by independent Tier-1 providers. The physical security adheres to the best practices in the industry and include:

- Keycard protocols, biometric scanning protocols, man traps, review of door logs, and round-the-clock interior and exterior surveillance.
- Access limited to authorized data center personnel - no one can enter the production area without prior clearance and appropriate escort.
- Assurance that every data center employee undergoes thorough background security checks.

Operations Security

A formal change control process minimizes the risk associated with system changes. The process enables tracking of changes made to the systems and verifies that risks have been assessed, inter dependencies explored, and necessary policies and procedures considered and applied before any change is authorized.

The production environment may be accessed only by authorized personnel and when adequately justified by business needs. Operations personnel have administrative access only to the system components they are responsible for, and all access is fully logged and regularly audited. Access to the infrastructure is controlled via a separate network which is physically isolated from the ReadyRedact corporate network. This ensures that only personnel authorized to access the data center may do so.

A limited number of key personnel have “super admin” access to the entire platform, which they may use in emergencies. Such access triggers an alert for immediate independent review. All privileged session logs are subject to ongoing monitoring by a session audit tool with 200+ custom alerts for high-risk events and triggers for non-standard activity.

Development, testing, and production environments are strictly separated both on the logical access level and on the network level to reduce risks related to unauthorized or unexpected changes to the production environment.

The ReadyRedact platform is protected both internally and externally by firewalls and security groups. ReadyRedact deploys host-based intrusion detection systems as well as a variety of network-level controls to detect attempts for unauthorized access or circumvention of security controls. ReadyRedact uses industry standard hardening procedures including installation of only the minimum software necessary, changing default system passwords or disabling implicitly created accounts, and making sure that firewalls let through only explicitly allowed traffic.

The entire production infrastructure, as well as all platform components, is monitored, and alerts are addressed by operations personnel 24x7x365. The platform team is responsible for capacity monitoring and planning to ensure the timely scaling of systems, as necessary.

Network Security

The ReadyRedact platform servers are allocated to the respective security groups, characterized by specific security settings (TCP/IP level), and supplemented by individual instance-level stateful firewalls. Separate VLANs are used to split production, testing, and development environments, as well as to segregate end-user and administrative traffic.

All network access to the virtual hosts is protected by a multi-layered firewall operating in a deny-all mode. Internet access is only permitted on explicitly opened ports for only a subset of specified virtual hosts. A separate set of firewall rules manage access to database instances
within the internal environment.

Software Development and Maintenance

ReadyRedact follows industry standard secure development life cycle practices. A formal change control process minimizes the risks associated with system changes. The process enables tracking of changes made to the systems and verifies that risks have been assessed, inter dependencies explored, and necessary policies and procedures considered and applied before any code change is formally authorized. ReadyRedact has integrated static and dynamic security testing in its CI/CD infrastructure, and peer code review includes secure development considerations.

Development of new platform features follows agile project management principles. Security architecture considerations are part of all architecture design and reviews. Before new platform features are rolled out to production, the implementation is reviewed against design, and for new or significantly modified components, external penetration tests are also executed.

Security Incident Management

ReadyRedact has established an industry standard security incident response plan. Staff is trained to ensure all potential security incidents are identified and reported in a timely manner. ReadyRedact's security operations team is on call 24x7x365. There are defined protocols and escalation trees for the handling of security incidents and, when required by the nature of the incident and applicable contractual commitments and regulatory requirements, for the notification of the affected parties as well as the authorities. Procedures for collection of evidence ensure chain of custody.

Disaster Recovery

ReadyRedact has automated backups in place for all application and database servers that include:

1. Cross data center backups to avoid specific data center outages and/or data loss.
2. Backups are taken every hour, 24x7x365.
3. All backups are encrypted at rest and in transit.
4. Backups can be restored to Production environments, as needed, in under 1 hour.
5. Backups are retained for 30 days.
6. Database backups have the potential to perform point-in-time restores, to the minute, for 30 days.