Security Whitepaper | 2020

Introduction

SecureReview is an innovative new security platform that enables unprecedented information security and performance for document review projects.

Corporate legal departments, law firms, document review staffing agencies, and e-discovery data hosting providers can all use SecureReview to greatly reduce the risk of confidential information disclosure, data loss, and malicious attacks on their document review systems.

SecureReview provides an additive layer of security to the document review process ensuring a consistent security posture across multiple service providers

Core Security Principles

SecureReview provides a high-performance, sterile and project-specific virtual PC service that ensures that all the informational artifacts — cached documents, search terms, custodian's names — of the document review process are never downloaded to local computers, effectively isolating sensitive discovery information and significantly decreasing the security risks associated with the project.

SecureReview does not have possession of credentials to the 3rd party hosted document repositories that are accessed by SecureReview users on the WorkSpaces.

System Architecture and Security

Dedicated Project Infrastructure

SecureReview leverages hardened instances of the Amazon Workspaces PCOIP Virtual Desktop Service. Workspace configurations and security settings are controlled at a project/matter level which ensures a consistent application of security policies and permissions across the project team.

SecureReview WorkSpaces are project/matter and user specific and are permanently destroyed at the end of the project.

SecureReview provides a project-specific email address for each user to ensure segregation of information and documents that may be exchanged during the course of the project.

SecureReview matter-specific email stores ensure that emails are never co-mingled with another matter's confidential information even in system backups, assuring a matter-specific document retention lifecycle policy.

Global Hosting Locations

SecureReview infrastructure is available in the following global locations:

- US East (N. Virginia)
- US West (Oregon)
- EU (Ireland)
- EU (Frankfurt)
- Asia Pacific (Sydney)

- Asia Pacific (Tokyo)
- Asia Pacific (Singapore)

Security Principle of Least Privilege

SecureReview implements the Security Principle of Least Privilege at the project/matter as well as Workspace/User levels, permitting only necessary network and web traffic to flow between WorkSpaces and designated project-specific web and email endpoints.

Security policies applied to the workspaces disables clipboard operations, printing, saving, USB access helping ensure that users cannot transfer data to or from the SecureReview environment.

Authentication & Session Security

SecureReview users are provided credentials to access a single Workspace which is configured according to project-specific security requirements. Authentication occurs via a customized PCOIP AWS Client after which the user is logged on to his or her SecureReview Workspace.

Multi-Factor Authentication and Single Sign On are features that can be enabled for SecureReview Enterprise customers.

SecureReview Workspaces offer the following Session Security options:

- Print/Save/Copy Restrictions
- Browsing URL Restrictions
- Permissible Login Time Schedule
- Dedicated Project and User email address
- Host IP Whitelisting

SessionGuardian

SessionGuardian is an optional authentication module available for Windows Host computers that provides additional SecureReview lockdown capabilities including webcam integration for security purposes:

- User Image Authentication
- Gaze Tracking (blur screen when authorized user not looking at screen)
- Single Authorized user detection (blur screen when other users present)
- Unauthorized object in webcam field of view such as an iPhone, camera, etc. (blur screen and log)
- Screenshare / Screenshot Blanking
- End-point PC Verifications
    - Anti-Virus Installed and current
    - Unauthorized applications blacklist
    - Allowed IP whitelist
    - Prevent host sessions within a virtual machine to prevent embedded screenshots or screen sharing

Encryption

All SecureReview data is encrypted at rest and access to that data is encrypted in transit for internal and external access (system and users).

SecureReview WorkSpaces data storage are encrypted at creation, providing encryption for data stored at rest, disk I/O to the volume. Encryption keys are unique at the user/workspace level and never shared.

Optional SecureReview Email Service encrypts email objects at rest and in transit.

Audit Trails

SecureReview employs extremely robust audit trails and security logging mechanisms that track project, workspace and user lifecycles as well as any administrative activity by IT personnel that occurs on SecureReview.
A rotating network activity log tracks all user connections within the SecureReview network and between SecureReview workspaces and the designated cloud endpoints.

Audit trails cannot be disabled (or re-enabled) without triggering audit alerts which ensure a consistently compliant security environment.

Vulnerability Assessments and Penetration Testing

SecureReview infrastructure and workspaces are subject to annual 3rd party vulnerability assessments.

SecureReview also performs daily automated penetration testing to ensure an aggressive security posture is maintained at all times.

Patch and Vulnerability Management

SecureReview Workspaces, images and server infrastructure are patched quarterly with urgent patches released daily on an as-needed basis.

SecureReview Workspaces and servers are protected with an AntiVirus software which is updated daily.

Privacy Policy & Confidentiality

Customer Data

Any customer data on the SecureReview Platform or in the SecureReview WorkSpaces remains the sole property of our customers.

Customer Data Retention and Destruction

At the end of the project SecureReview will provide encrypted archives of any project email messages and attachments after the data will be permanently destroyed.

Any temporary data store in the SecureReview Workspaces will also be permanently destroyed at the end of the WorkSpace lifecycle.

Dedicated Customer Environments

SecureReview can build and deploy WorkSpace images and policies based on customer request, for example installing specific viewing software to facilitate the review of non-standard file formats.

Security Compliance

Customer Regulatory Compliance

SecureReview can help customers achieve compliance with content protected by HIPAA, GDPR, ITAR and other regulatory regimens.

Company Operations

SecureReview company operations are broken down into four general areas: Engineering, Technical Operations, Customer Support, and

Business Operations. Each area, and team within the area, has specific roles, responsibilities, and access for operating SecureReview systems.

Security Team

SecureReview's Chief Security Officer (CSO) leads the security team responsible for application information, and physical security. The security team works internally and with SecureReview customers to identify, track, and resolve vulnerabilities and to mitigate risk.

Software Development Life Cycle (SDLC)

SecureReview utilizes best practice agile software methodologies within a GxP compliant SDLC framework to ensure a consistent level of quality.

Employee Screening and Policies

All SecureReview employees, prior to their employment, undergo background checks. They agree in writing to comply with all company policies including security and acceptable use policies. Upon joining, employees and contractors undergo security training.

Vendor Management

Vendors are subject to a SecureReview on-boarding process and annual requalification process to ensure compliance with SecureReview's Security and Risk Management policies.

Physical Security

SecureReview offices are physically controlled using electronic badge readers that log access events.

Certifications

SecureReview Workspaces are hosted in Amazon hosting facilities and managed under contract by RackSpace with the following certifications:

- ISO 27001
- SOC 1 and SOC 2
- PCI Level 1
- FISMA Moderate
- SOX
- FedRAMP
- HITRUST/HIPAA

