Secured cloud solutions
for production environments

A RICOH TotalFlow® Cloud Security Overview

RICOH
imagine. change.

Table of contents

Introduction

Cloud solutions for production environments: The next evolution of Ricoh software

RICOH Graphic Communications, referred to as "Ricoh" in this document, is focused on connecting operational data, devices, processes and people to cloud-resident business intelligence tools. Moving data analytics to the cloud delivers significant advantages to Ricoh customers, including:

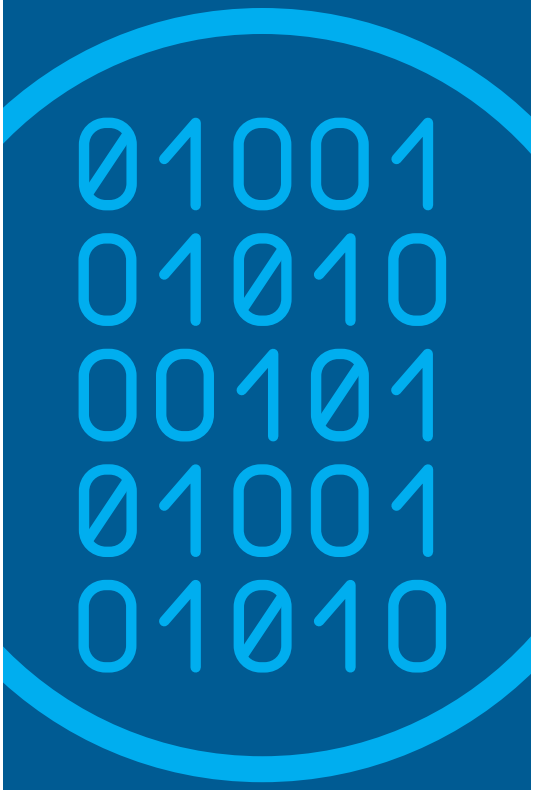
- Eliminating capital expense for server hardware
- Reducing costs associated with platform maintenance (updates to programs and operating systems)
- Access to on-demand expansion of system resources based on peak usage needs
- Use of a Software as a Service (SaaS) subscription model
- Built-in backup and disaster recovery capabilities of the cloud platform

Leveraging a new model of secured, cloud-hosted technologies, the RICOH Supervisor™ product is designed to streamline the transformation of data into actionable business intelligence and information output that can be accessed quickly and easily.

A security-first approach

Ricoh understands the importance of keeping information secured, and that is why Ricoh solutions have security as a fundamental requirement during design, implementation and ongoing operations. This overview addresses Ricoh's commitment to the important components of data and network security, providing customers the assurance they are looking for in their RICOH TotalFlow Cloud Platform solutions.

Keeping data safe and secured



Privacy and data handling

Ricoh recognizes the importance of the protection of personal information used in the global information society. The Ricoh privacy policy covers such topics as the type of data collected from customers, and how Ricoh uses that data to help deliver programs, products, information and services. The terms and conditions of the global subscription agreement covers such topics as service availability, subscriber data, sub-processors and cookie policy.

Data ownership

Under the Ricoh subscription agreement, any data, including personally identifiable information (PII), collected by Ricoh applications is owned by the customer.

Confidentiality

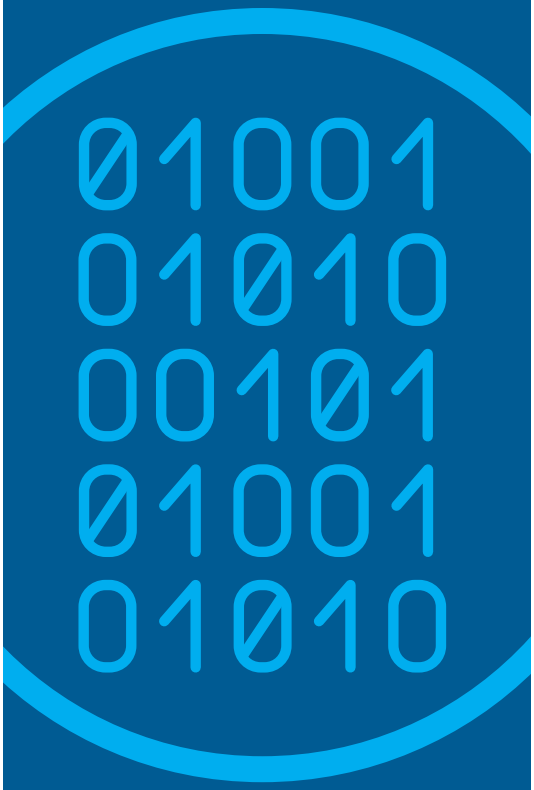
Ricoh agrees to treat all customer data as confidential information, including login credentials and subscriber data.

Compliance

Ricoh continuously works to ensure its cloud environment meets all obligations under applicable country, state and federal laws and regulations, as well as applicable industry rules and standards. When customers consider Ricoh as a partner, they should be confident that Ricoh applications meet their security, compliance and data processing needs.

Coalfire®, an independent cybersecurity consulting firm, has assessed the RICOH TotalFlow® Cloud product for SOC 2® Type 1 compliance. Click here to view the SOC 2 Certificate.

Keeping data safe and secured



Shared responsibility

All Ricoh cloud applications adhere to a shared responsibility security model, ensuring that customer data is protected while resident within the Ricoh cloud platform.

Ricoh, as a SaaS provider, is responsible for securing customer data in the cloud by securing the platform, applications, authentication credentials, operating systems, and networks, as well as by encrypting customer data.

The Ricoh cloud applications run on Amazon Web Services™ (AWS) which is an Infrastructure as a Service (IaaS) provider. AWS provides a highly-secured, reliable, and scalable infrastructure platform in the cloud capable of supporting clients on a global scale. AWS compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. For more information on AWS Compliance Programs, please refer to **https://aws.amazon.com/compliance/programs/.**

Securely controlling data access and transmission

Access control

A user must login with a secure password to Ricoh cloud applications. Ricoh implements industry-standard password controls including:

Complexity

- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 numeric digit
- At least 1 special character
- At least 8 characters

Expiration

- Password reset required for first login
- Password reset required every 60 days by default

Disallow reuse

- Last 12 passwords must be unique

Interacting with the platform

All access to Ricoh's cloud platform is via secure connections (e.g. HTTPS). A single administrator user login is created for each new customer account. The administrator user is responsible for creating additional customer logins with appropriate access for their roles. Role-based access applied throughout the system ensures each customer's administrators control what their users can (and cannot) see and do.

In order to further protect its customers, for system service and maintenance, Ricoh only grants access to authorized personnel on a need-to-know basis. Ricoh also applies least privilege rules, reviews permissions quarterly, and revokes access immediately after employee termination. All authorized personnel have unique user IDs.

Logging and monitoring

User, system and network activity is logged to a protected centralized logging cluster. The centralized logs are ingested into a cloud-based Splunk® solution where they are monitored by authorized personnel 24x7 and are analyzed and reviewed for anomalies and suspicious activity. The logs are preserved for multiple years in accordance with all regulatory requirements, and can be used to troubleshoot security incidents.

Securely controlling data access and transmission

Secured in-transit communications

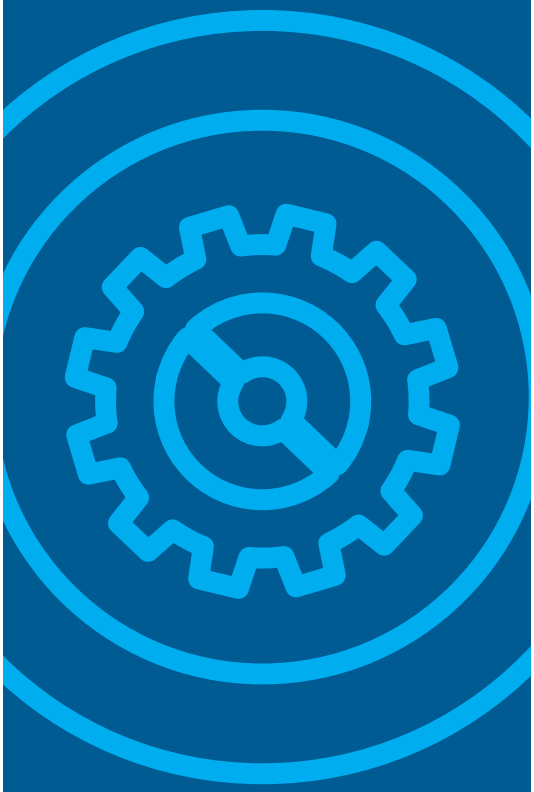
Data in-transit is protected by strong cryptography and security protocols (e.g. FIPS-140-2 validated encryption) to prevent eavesdropping, tampering, and forgery — this applies to all data in transit to and from the cloud as well as internal transfers of all customer data. Data can only be accessed through password-protected cloud applications and APIs, with the appropriate credentials.

Data storage and encryption at rest

Ricoh stores data in the cloud across multiple availability zones to ensure resiliency in the case of failure. All customer data at rest is encrypted using industry-standard encryption techniques to ensure data is secured and reliable.

For any on-premise tools that are part of Ricoh cloud applications, the customer is responsible for the encryption of their data at rest.

Building safer applications and a solid infrastructure



Development best practices

The Ricoh development team employs secure coding techniques and development best practices, including:

- ✓ Code reviews
- ✓ Defect management
- ✓ Performance engineering
- ✓ Unit testing
- ✓ Agile programming
- ✓ Continuous integration

Developers are provided regular training in secure web application development practices. To avoid unwanted access within an application, Ricoh follows a least-privilege design approach to clearly define and separate duties (e.g. read-only versus read & write). For example, a service API can only query the one table it is allowed to query and has no access to other tables.

Non-production and production environments are separated. All code changes are peer reviewed and tested before they are deployed to production. The same change control process is followed for any changes to the environment itself.

Network security

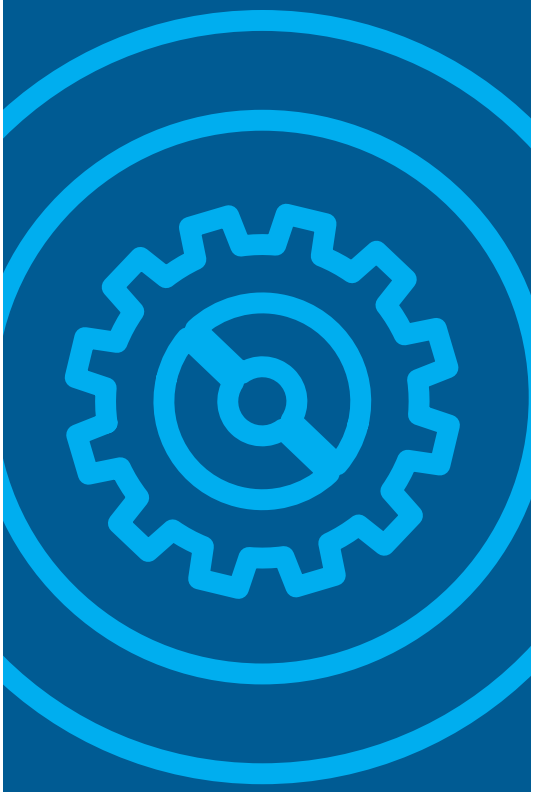
AWS instances deploy Trend Micro™ Deep Security's Anti-Malware, Firewalls and Intrusion Prevention to block viruses and malware, monitor incoming and outgoing traffic and protect against network attacks. Firewall rules are configured to deny everything by default and only allow protocols needed for the Ricoh applications. Ricoh also leverages AWS Security Groups for an additional layer of protection.

All publicly reachable web servers are located inside a controlled DMZ (perimeter). Ricoh also restricts traffic based on IP geolocation.

Ricoh corporate and development networks are both logically and physically separated from the AWS hosting facility.

All cloud services not required by Ricoh applications are disabled on the Ricoh servers.

Building safer applications and a solid infrastructure

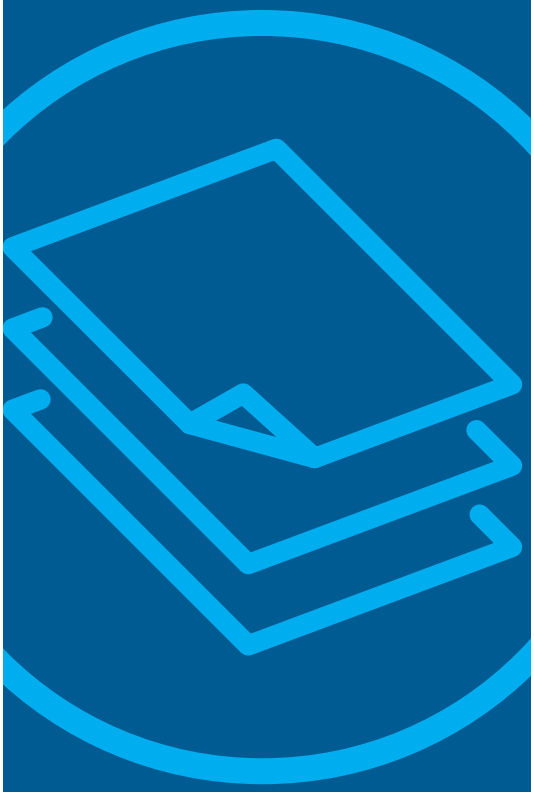


Vulnerability scans and patching

Ricoh has a vulnerability management program that focuses on the remediation of security vulnerabilities and threats. The Ricoh cloud environment is periodically scanned and annual penetration tests are run to identify any potential risks. Patches are applied proactively and on a when-needed basis.

Ricoh works with third-party companies to test and mimic outside attacks and internal threats on an annual basis to ensure that Ricoh network security is consistently reliable.

Protecting business with disaster recovery and business continuity



Information security plan

Ricoh's information security plan outlines our security practices, policies and procedures, disaster recovery and service continuity plan and incident response policy.

Business continuity

Ricoh maintains a disaster recovery and service continuity plan for recovering and restoring technology assets and services in the cloud which is tested periodically. The plan includes multiple availability zones and includes procedures to restore lost data from automated snapshots. Backups are stored redundantly in multiple AWS secured data centers.

Incident response plan and breach notification

Ricoh has a formalized incident response plan, which includes descriptions of the roles and responsibilities of each person as well as escalation procedures during an incident. The incident response plan covers the initial response to, investigation, notification, communication, and remediation of events. The incident response plan is tested and updated on a regular basis.

Should a security incident occur, notifications will be sent according to Ricoh legal and contractual obligations. Customers will be notified as soon as possible, following a proper investigation.

Review and use of third-party service providers

Ricoh works with third-party partners to provide some of the above-mentioned services to our customers. To ensure compliance with privacy and security standards, Ricoh maintains confidentiality and data processing agreements with each of our partners and regularly reviews these documents.

Should you have specific questions or concerns that are not addressed in this overview, please contact your Ricoh software representative.

To learn how RICOH Supervisor, our vendor-neutral, secured cloud solution can help maximize your resource utilization and support business decisions with real-time data, or to request a free 60-day trial, please visit www.ricohsoftware.com.

RICOH
imagine. change.

www.ricohsoftware.com

Ricoh USA, Inc., 300 Eagleview Blvd., Exton, PA 19341, 1-800-63-RICOH