



Trust Services Principles for Service Organization Controls Reports with Rocket Servergraph

Service Organization Controls (SOC) reports are an effective way for companies to provide assurance to their customers and prospects about the security, availability, confidentiality, integrity, and/or privacy of the systems they offer. SOC 2 and SOC 3 reports are popular with Software-as-a-Service (SaaS) providers and any company with access to its customers' critical systems and data.

Each Trust Services Principle includes a number of criteria that must be satisfied by the service organization, as well as illustrative controls for how an organization may meet the criteria.

Rocket® Servergraph helps an organization satisfy criteria related to data backup and availability, with reporting capabilities to provide the evidence you need for a successful audit. Relevant criteria, and the capabilities Rocket Servergraph offers to achieve each criterion, are listed on the following pages.



CRITERIA

ROCKET SERVERGRAPH CAPABILITIES

CC5.1

Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.

Servergraph supports unique user IDs for all individuals accessing the system, and uses LDAP integration with Active Directory credentials.

Detailed, customizable permissions can be configured for each user to support the rule of least privilege and segregation of duties.

Servergraph is agentless and only requires a read-only service account to operate, preventing unintentional or unauthorized modification of network systems and data.

CC5.2

New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.

System administration is performed through the separate administration client, with access restricted to designated administrative users.

CC5.3

Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).

Passwords are required for all users attempting to log into the system. Local credentials are stored in encrypted hash format.

Servergraph offers LDAP integration with Active Directory credentials, inheriting your organization's network-level authentication requirements.

CC5.4

Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.

Detailed, customizable permissions can be configured for each user to support the rule of least privilege and segregation of duties.

CC5.5

Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.

Systems are installed on premises, so your organization can implement physical and environmental controls as with all other computing equipment.

CC5.6

Logical access security measures have been implemented to protect against security, availability, processing integrity, or confidentiality threats from sources outside the boundaries of the system.

Systems are installed on premises, so your organization's perimeter network security will cover Servergraph systems.

CC5.7

The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security, availability, processing integrity, or confidentiality.

Users access the web-based Servergraph application using encrypted HTTPS sessions.



CRITERIA

ROCKET SERVERGRAPH CAPABILITIES

A1.1

Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.

Servergraph offers dashboards that let users monitor the status of your backup systems in real time.

A1.2

Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.

Systems are installed on premises, so your organization can implement physical and environmental controls as with all other computing equipment.

Servergraph collects information from backup software, hardware, and processes in your environment to document that data backups are operating in accordance with your organizational policies.

Traps, reports, and alerts are customizable to capture relevant information for all of your backup control requirements.

Reports and alerts can be automatically distributed to any individuals, supporting segregation of duties and facilitating review and monitoring processes.

Backup collection logs and reports are retained within Servergraph for a fully configurable duration to maintain historical evidence.

The Server Monitor feature shows real-time statistics and alerts for backup systems, such as storage utilization and disk capacity.

PI1.4

Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.

Servergraph collects information from backup software, hardware, and processes in your environment to document that data backups are operating in accordance with your organizational policies.

Traps, reports, and alerts are customizable to capture relevant information for all of your backup control requirements, including processing errors.

Backup collection logs and reports are retained within Servergraph for a fully configurable duration to maintain historical evidence.

C1.2


Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality requirements.

Detailed, customizable permissions can be configured for each user to support the rule of least privilege and segregation of duties.



 rocketsoftware.com

 info@rocketsoftware.com

 US: 1 855 577 4323
EMEA: 0800 520 0439
APAC: 612 9412 5400

 twitter.com/rocket

 www.linkedin.com/company/rocket-software

 www.facebook.com/RocketSoftwareInc

 blog.rocketsoftware.com