COMPLIANCE

Trust Services Principles for Service Organization Controls Reports with Rocket® BlueZone

Service Organization Controls (SOC) reports are an effective way for companies to provide assurance to their customers and prospects over 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 or criteria that must be satisfied by the service organization, as well as illustrative controls for how an organization may achieve the criteria.

Rocket BlueZone terminal emulation solutions effectively leverage the security of your host system environment, while adding strong encryption for all data transfers and enhanced remote access and authentication capabilities, to achieve your logical security, integrity, and confidentiality objectives. BlueZone's distributed architecture also serves your availability and continuity goals. Relevant Trust Services principles and criteria, along with BlueZone's capabilities to meet them, are detailed below.

CRITERIA	BLUEZONE 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.	BlueZone provides communication between clients and backend host systems by utilizing the user access permissions inherent to the backend host system environment. BlueZone cannot provide any capability for data access that is not already specifically authorized within your host system O/S to the logged in user. Security Server provides an additional, optional layer of security by acting as a proxy between your host system and clients. Clients must first connect and authenticate to your Security Server using an established user ID, which may be integrated with other Identity Access Management systems including RSA and Active Directory. After authenticating to Security Server, users must then also login to the host system directly, applying the host system-level access permissions. The built-in logging mechanisms inherent to your host system environment record all activities initiated through BlueZone sessions. There is no need to maintain a separate log management function specifically for BlueZone. As a supplemental logging mechanism, Rocket BlueZone Web records a log of all client connections to the web server. This does not record commands issued through the sessions, which would be logged through the built-in host system functionality, but provides an additional layer of security by showing how many users and terminals are connecting, when, and from where.
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.	BlueZone leverages your host system credentials and all associated authentication mechanisms. There is no need to maintain a separate user account list in BlueZone.
CC5.3 Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	Authentication is performed against the host system directly, applying its password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems. When using Security Server, a second layer of authentication against the Security Server directly before a user may attempt to authenticate to the host system. Security Server supports integration with RSA SecurID and Active Directory for user credentials and authentication.

CRITERIA	BLUEZONE CAPABILITIES
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.	All access permissions are inherited from the host system. BlueZone cannot provide any capability for data access that is not already specifically authorized within your host system O/S to the logged in user.
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.	To insulate host systems from direct external access, Security Server may be implemented as a proxy within your DMZ to enhance the security of remote access.
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.	BlueZone products supports state-of-the-art encryption methods for all communications between clients and the backend host system environment, including the TLS1.2 are SSHv2 protocols with FIPS-compliant encryption algorithms. BlueZone Web applies this level of encryption to both the end user-to-web server session, and the web server-to-host system session. While support for older protocols is available to support legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. In environments where the host system cannot support encrypted sessions, the optional Security Server allows for plaintext communications to be isolated within a secure, local network, while applying strong encryption methods to all external connections with clients.
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.	The distributed nature of BlueZone's architecture allows administrators to connect to the host system environment from anywhere, to anywhere in order to perform routine maintenance or emergency corrections. During a technical incident or disaster scenario, BlueZone can help continue or restore operations and data access. BlueZone clients can specify alternate hosts for instant cutover to disaster recovery facilities. BlueZone Web can support redundant web servers to withstand a technical incident and continue operating in other environments, while allowing administrators from any location to continue working.

CRITERIA	BLUEZONE CAPABILITIES
PI1.6 Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	All access permissions are inherited from the host system. BlueZone cannot provide any capability for data access that is not already specifically authorized within your host system O/S to the logged in user. Encryption of data in transit protects the integrity of all such data, preventing technical errors, corruption, or malicious alteration in transit that could impair its accuracy and reliability.
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.	All access permissions are inherited from the host system. BlueZone cannot provide any capability for data access that is not already specifically authorized within your host system O/S to the logged in user.
C1.3 Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements.	The encryption of all data in transit to and from the host system prevents unauthorized access via eavesdropping to the data itself, as well as protecting the administrative credentials used to establish sessions.

Rocket

rocketsoftware.com
info@rocketsoftware.com
US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com