COMPLIANCE

Payment Card Industry Data Security Standard (PCI-DSS) Compliance with Rocket® BlueZone

The Payment Card Industry requires all organizations who store or process credit card data and transactions to implement technical security requirements over all systems involved in the data storage and transmission. The scope of these control requirements range from encryption methods to access rights management to vulnerability testing.

Rocket BlueZone terminal emulation solutions would not typically store or transfer Cardholder Data (CHD) directly, reducing the impact on your PCI compliance requirements. However, some of BlueZone's security features do have a direct impact on your ability to satisfy certain PCI-DSS requirements for the overall Cardholder Data Environment (CDE). For these areas, BlueZone provides strong encryption, multifactor authentication, and remote access security capabilities for administrative access to your host system environment. Relevant requirements, and the capabilities BlueZone offers in order to achieve each, are listed below.

PCI-DSS REQUIREMENTS	BLUEZONE CAPABILITIES
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Security Server can function as a proxy in your DMZ between your host system and remote clients, eliminating the need for direct access and ensuring secure, encrypted communications throughout the transmission.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	BlueZone leverages your host system credentials and all associated authentication mechanisms. There is no need to maintain a separate user account list in BlueZone.
2.3 Encrypt all non-console administrative access using strong cryptography.	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.
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements. • Processes for secure deletion of data when no longer needed. • Specific retention requirements for cardholder data. • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	BlueZone does not store any CHD directly; it provides a command interface between clients and the backend host system. No additional data storage and retention controls are needed for using BlueZone.

PCI-DSS REQUIREMENTS	BLUEZONE CAPABILITIES
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	BlueZone does not transmit any CHD directly. While all communications are strongly encrypted, there is no direct exposure to this control requirement.
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Define access needs for each role, including system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources. Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. Assign access based on individual personnel's job classification and function. Require documented approval by authorized parties specifying required privileges.	All access permissions are inherited from the host system. There is no separate user access schema to maintain within BlueZone, and 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.
8.1 Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows: • Assign all users a unique ID before allowing them to access system components or cardholder data. • Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. • Immediately revoke access for any terminated users. • Remove/disable inactive user accounts at least every 90 days. • Manage IDs used by vendors to access, support, or maintain system components via remote access • Limit repeated access attempts by locking out the user ID after not more than six attempts. • Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. • If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	BlueZone leverages your host system credentials. There is no need to maintain a separate user account list in BlueZone. Session security settings, including account lockout and session timeout, are inherited from your host system configurations.

PCI-DSS REQUIREMENTS	BLUEZONE CAPABILITIES
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric.	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.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Multifactor authentication is supported for BlueZone client access, supplementing passwords with additional authentication factors including physical tokens and digital certificates.
10.1 Implement audit trails to link all access to system components to each individual user.	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.

Rocket

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