bicdroid

Make data immune to all malicious attacks.

BICDROID QDocEE FUNCTIONALITIES

#	Core Functions	Technical Points	Detailed Descriptions
1	System compatibility	Client OS	64-bit Windows 7/8/8.1/10
		Server OS	CentOS 7.6
		Third-party software compatibility	Compatible with all commonly used third-party software and anti-virus software, such as Windows Defender, Norton, McAfee, Kaspersky, etc.
2	End-point data protection	Data security	Support data protection of the entire life cycle from generation, storage, use, transmission to destruction: 1. Prevent data leaks/branches 2. Prevent data tampering 3. Prevent data destruction 4. Prevent ransomware attacks 5. Prevent phishing attacks 6. Prevent malicious insiders 7. Prevent all known/unknown external attacks
		Encryption/decryption functions	1. The end user has no visibility into the file encryption and decryption process. As such, QDocEE does not change the user's usage habits, maintaining work efficiency 2. Support automatic decryption access of encrypted files on managed clients where QDocEE is installed 3. The encrypted files are not readable on unmanaged clients where QDocEE is not installed 4. Support encrypted storage of protected files in removable media 5. The encrypted and protected on removable media can be accessed only on managed clients, not by unmanaged clients

			6. Support the transmission and storage of protected files through network drives, such as SAN, NAS, DAS, etc. 7. Support the transmission of protected files through any third-party file transmission tools
		File protection methods	1. Support the file protection of designated file paths 2. Support the file protection of designated file suffixes in designated directories 3. Support automatic file protection of newly created files by authorized programs
		Program authorization methods	1. Support program authorization based on its digital signature 2. Support program authorization based on its path
		Viewing function of file protection status on clients	1. Display file protection and encryption status 2. Display the list of authorized programs 3. Display the digital signature list of authorized programs
		Encryption algorithms	Support common 128 & 256-bit commercial encryption algorithms, including AES, AES_NI, DES, 3DES or SM
3	Outbound approval enforced	Outbound approval function (it can be configured as enforced approval, or automatic approval depending on requirements)	1. Support outbound approval of protected data 2. Support a two-level approval mechanism 3. After approval, the protected file will be automatically decrypted and sent out in plain text 4. Plaintext protected files are never cached on clients 5. Support to view the outbound status in real time on clients

		Post-event traceability function	1. The audit results are automatically synced to clients 2. The audit system records and archives all outgoing requests, approval procedures and outgoing file lists
4	Cipher decryption approval	Pre-event approval function	1. Support outbound approval of protected data 2. Support a two-level approval mechanism 3. After approval, the protected file will be automatically decrypted, and a plaintext link will be generated for the end user to download
		Post-event traceability function	1. The audit results are automatically synced to the client 2. The audit system records and archives all decryption requests, approval procedures and decrypted file lists
5	Cipher secure sharing	Secure internal circulation of cipher and seamless sharing on managed terminals	1. Support the transmission of protected files through third-party file transfer tools (i.e., email attachments, Teams, Skype, FTP/SFTP server, etc.) 2. Support transfer and storage of protected files via removable media (for example: NTFS U disk) 3. Support the transmission and storage of protected files through network drives (i.e., SAN, NAS, DAS, etc.)
6	Centralized control	Remote installation, configuration and management	Support remote installation, configuration, and management of clients through the Central Sentry Platform (CSP). There are strict authorization and decentralization management procedures for configuring the data security strategy of each client. Specific functions include: 1. Support multi-level group client management

			2. Support remote configuration of file path protection 3. Support remote configuration of designated suffix protection in designated directories 4. Support remote program authorization of digital signatures 5. Support remote program authorization of program paths
		Granular security perception	Sentry records (target data, path information of the visiting process, visiting time, access result (allowed or denied), etc.) and system operating status (CPU ratio, memory ratio, disk ratio, etc.) are sent to the CSP in real time for normalized processing, realizing real-time supervision and comprehensive auditing
		Professional index analysis of data and system security	Support professional index analysis of data and system security through modeling, including system vitality, load mutation index, attack mutation index, etc., which can be graphically displayed
		Real-time security alert	According to analysis results of professional indexes, the system health and safety are classified, and real-time warnings are provided when needed
		Large-screen visualization and centralized display	The highly concentrated data and the overall situation of system security are visually displayed to provide accurate information for operation monitoring, analysis, and decision support
		Dynamic visual security report	Support dynamic and self-defined condition combination queries for data self-protection, system health and safety status, with graphically presented search results

7	Log and audit	Log upload and centralized management	1. The client provides complete log management, including granular access records of protected data and critical system performance data, and timely uploads to the central sentry platform for intelligent analysis 2. Administrators can conduct log audits and queries on the CSP as well as export, backup, cleanup and other operations
8	Software self-protection function	Installation directory protection and process status monitoring	1. Provide installation directory and process protection on clients, and real-time secure synchronization with CSP 2. Administrators can monitor the running status of each client in real time through the CSP, and prevent users from uninstalling the client software
9	Non-security function	System performance	Support kernel-level encryption and decryption, which does not increase I/O cost and has low system performance impact, minimizing delay to normal R/W operations of protected files
		Ease of use	1. The client software is easy to operate. File encryption and decryption is transparent to users, does not change user habits, maintaining work efficiency 2. Administrator can use CSP to configure, manage and monitor clients in a hierarchical grouping manner, which is simple, efficient and safe