bicdroid

Make Data Immune to All Attacks

QDocument EE

Protect Endpoint Data Anytime & Against All threats

Abstract

QDocument EE (QDocEE) is the most innovative, secure, and efficient solution on the market for endpoint data protection. It protects endpoint data once and for all against data leaks/breaches and all known and unknown attacks including ransomware attacks, malicious insiders, fileless attacks, and supply-chain attacks. It always polices data access processes along with an end-to-end seamless cryptographically secure chain, provides detailed access and data governance reports in real time, and denies all unauthorized processes deviating from the secure chain, thereby defeating any attempted attacks.

BicDroid Inc.
Phone: 1-519-573-0096

Suite 104, 609 Kumpf Drive
Waterloo, ON, N2V 1K8, CA
www.bicdroid.com

Table of Contents

1. Overview

Data security is fundamental to our Internet-based economy. As the world is increasingly digital, our activities rely more and more on data technologies. Breaches of critical data such as core intellectual properties can compromise national and economy security. Alteration and/or loss of critical data can change the course of business with severe consequences, shut down production lines, and negatively affect people's lives. As such, protecting data anytime and against breaches and any known/unknown attacks is an urgent need for many industries.

At the same time, history tells us again and again that traditional cybersecurity solutions on the market all fail to satisfy the strong need of protecting data in real-time within a dynamic threat environment, as demonstrated by many headlines on victims of cyberattacks. Indeed, recent studies show that 90% of all large institutions including medicine, finance, government, and infrastructure, have experienced malicious attacks over the last year. These solutions fail because they play "catch-up" with hackers by design and look at security issues only from the perspective of networks and systems.

Using its patented technologies, BicDroid has developed a new paradigm of security solutions, which make data immune to all attacks (known and unknown) regardless of the conditions of networks and systems. In particular, BicDroid pioneered the concept of "data self-protection", which goes even beyond zero trust architecture. Regardless of network and system conditions, BicDroid builds an end-to-end seamless, cryptographically secure chain. This methodology can carve out dynamically and on demand (from the execution environment), a quarantined, secure activity space for data activities to take place, keeping looming threats at bay. Along the end-to-end secure chain, file encryption/decryption and strong mandatory access controls are smartly integrated together at the kernel of operating system (OS) to achieve data immunity to known and unknown attacks/threats, such as ransomware attacks, fileless attacks, malicious insiders, supply-chain attacks, and other known/unknown external attacks.

2. Description of QDocEE

QDocEE (hereafter referred simply to as "EE") is an enterprise-level endpoint data security solution. Building upon BicDroid's core technology of "cryptographic partition for data self-protection", it aims to solve the security problems related to data generation, storage, usage, transmission, and destruction throughout the entire life cycle of data on endpoints.

2.1 Architecture

As shown in Figure 1, EE has 3 main components: (1) EE Client, (2) EE CSP (Central Sentry Platform), and (3) EE OAS (Outbound Approval System). Sitting on your end-point, EE Client encrypts and protects simultaneously your data all the time by denying data access request from any process deviating from the end-to-end cryptographically secure chain. EE CSP, installed on your corporate server, allows IT admins to manage, control, monitor, analyze, and visualize data security and the health of all QDocEE protected computers. Furthermore, EE OAS enforces mechanisms to approve or deny requests for sending protected files out. Their inter-working mechanism is further described below.

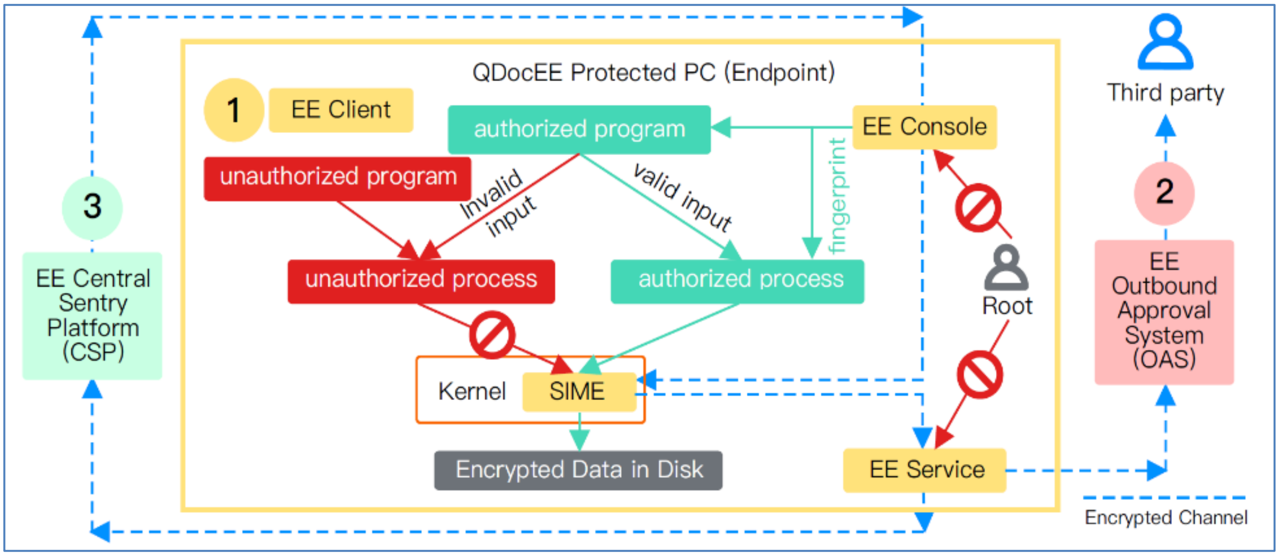


Figure 1: The main components of QDocEE: EE Client, EE CSP, and EE OAS.

1. EE Client

   Installed on your endpoint, EE Client consists of Smart Integration of Mandatory Access Control and Encryption (SIME), EE Console, and EE Service. SIME enables data self-protection against any attack while removing the need for key management. With mandatory access control (MAC) and file system encryption coupled into a single unit, there is no data breach even when MAC is hacked. EE Console takes inputs from EE CSP and configures the data security policy, which is enforced by SIME. EE Service ingests logs of authorized accesses and blocked access attempts from SIME, and then sends the information to EE CSP for analysis, visualization, and alerting.

   Interacting with EE CSP, EE Client establishes an end-to-end seamless cryptographically secure chain, starting from CSP, to programs, dynamic link libraries, executable scripts, input parameters, environmental variables, respective processes, and to protected and encrypted data. It denies data access requests from any process deviating from this end-to-end secure chain, keeping looming threats at bay and thus protecting data in real time within a dynamic threat environment.

2. EE OAS

   Installed on a server along with EE CSP, EE OAS provides another level of data security by enforcing mechanisms to approve or deny requests for sending protected files to third parties. Adopting multiple-level approval, EE OAS ensures that sensitive data remains protected, while maintaining a record of all outbound decrypted files for future traceability and auditing.

Through its OAS, QDocEE also prevents malicious insiders or negligent employees from leaking data. For example, if a malicious insider tries to upload some protected files to unauthorized public clouds such as Google drive, it will be blocked automatically. The only way to send out protected files is to go through OAS.

3. EE CSP

   EE CSP allows IT admins to manage, control, monitor, analyze, and visualize data security and health of all EE protected endpoints. Empowered by strong authentication and advanced multi-level authorization, EE CSP makes overwhelming data security management operations on any number of endpoints simple, swift, and secure.

Adopting a data centric security model, QDocEE puts zero trust on any of networks, systems and even users themselves. By enhancing the security of operation systems from a data perspective, it protects data against ransomware, malicious insider, supply chain, fileless attacks, and other known/unknown threats, providing truly unparalleled data security for endpoints.

2.2 Deployment and System Requirements

Figure 2 provides an example deployment of QDocEE. Its system requirements are as follows:

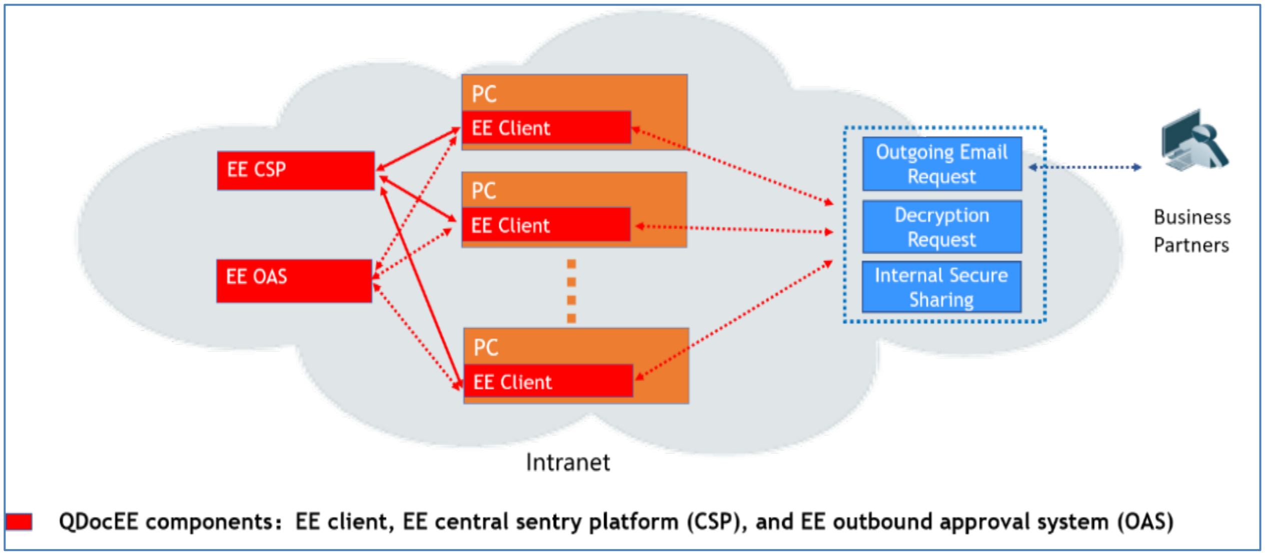


Figure 2. The deployment diagram of EE.

2.2.1 Client OS requirements

EE Client supports 64-bit Windows OS, including Windows 7, Windows 8, Windows 8.1, Windows 10 and above.

2.2.2 Server OS requirements

The EE server (OAS and CSP) supports CentOS 7.6 and above.

2.2.3 System/third-party software compatibility requirements

EE is compatible with all commonly used third-party software and anti-virus software, such as Windows Defender, Norton, McAfee, Kaspersky, etc.

2.3 Functionality Modules

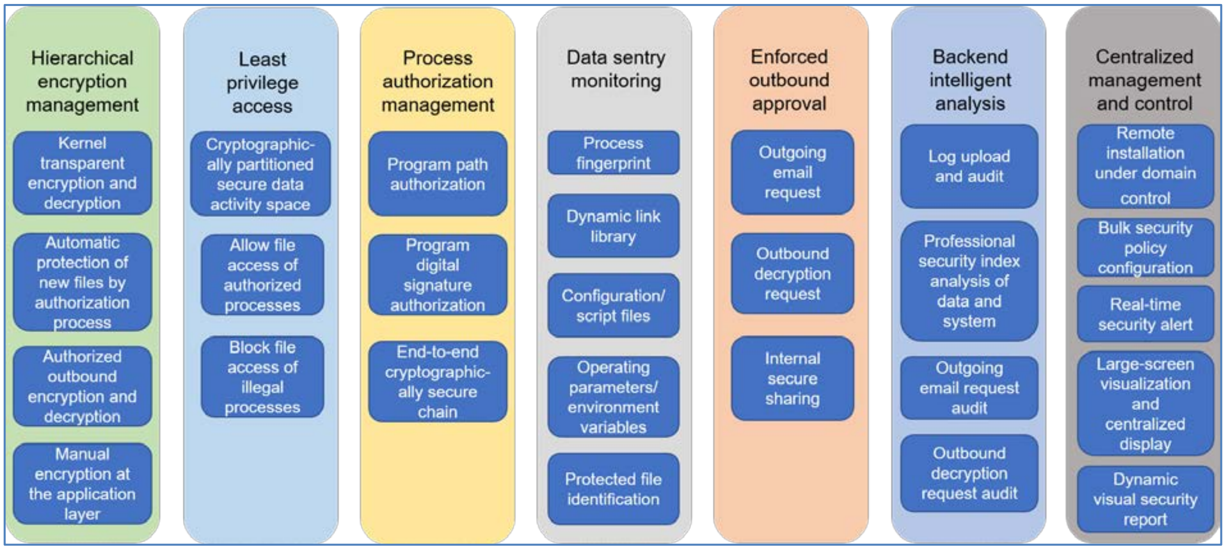

Hierarchical encryption management
Kernel transparent encryption and decryption
Automatic protection of new files by authorization process
Authorized outbound encryption and decryption
Manual encryption at the application layer
Least privilege access
Cryptographically partitioned secure data activity space
Allow file access of authorized processes
Block file access of illegal processes
Process authorization management
Program path authorization
Program digital signature authorization
End-to-end cryptographically secure chain
Data sentry monitoring
Process fingerprint
Dynamic link library
Configuration/ script files
Operating parameters/ environment variables
Protected file identification
Enforced outbound approval
Outgoing email request
Outbound decryption request
Internal secure sharing
Backend intelligent analysis
Log upload and audit
Professional security index analysis of data and system
Outgoing email request audit
Outbound decryption request audit
Centralized management and control
Remote installation under domain control
Bulk security policy configuration
Real-time security alert
Large-screen visualization and centralized display
Dynamic visual security report

Figure 3: Main functionality modules of EE.

Figure 3 shows the main functionality modules of EE: (1) the hierarchical encryption management module, (2) the least privilege access module, (3) the process authorization management module, (4) the data sentry monitoring module, (5) the enforced outbound approval module, (6) the backend intelligent analysis module, and (7) the centralized management and control module. These modules are implemented inside the combination of EE Client, EE OAS, and EE CSP

(1) The hierarchical encryption management module contains four levels of encryption and decryption functions: (a) transparent encryption and decryption at the kernel of OS, (b) automatic encryption of new files generated by authorized processes, (c) encryption and

decryption of authorized outgoing files, and (d) encryption of files manually selected by users for protection. After a process is authenticated and authorized to access protected data, the transparent encryption and decryption module steps in to provide automatic encryption and decryption services for the process. Likewise, when an authorized process generates a new file, the new file will be automatically encrypted for protection. When users are authorized to send out requested protected data, that data will be decrypted through OAS. The fourth encryption function provides users with a flexible tool to encrypt and protect some selected files which may not, otherwise, be included for protection by the security policy determined by the IT Admin through CSP.

(2) The least privilege access module grants the right to access protected data only to those processes which follow strictly along the end-to-end seamless cryptographically secure chain, ensuring that the access right to protected data is most restrictive. All processes deviating from the end-to-end secure chain, including those spawn from unauthorized programs and those spawn from authorized programs, but contaminated along the way, are blocked.

(3) Process authorization management starts with the authorization of trusted programs through CSP, covering the establishment of the end-to-end seamless cryptographically secure chain. Through CSP, IT admins can authorize a specific trusted program through either its full path or its digital signature certificate. Starting from there, the process authorization management module then applies cryptographic techniques to link the authorized program, dynamic link libraries, configuration/script files, input parameters, environment variables, respective spawn processes, and encrypted protected data together to establish the seamless end-to-end cryptographically secure chain.

(4) The data sentry monitoring module determines whether a process comes strictly along the seamless end-to-end cryptographically secure chain, or deviates from the end-to-end secure chain by monitoring and verifying the program from which the process originates, configuration/ script files, input parameters, environment variables, and protected data. Only the process following strictly along the secure chain would be authorized. All processes deviating from the end-to-end secure chain are unauthorized, and will be blocked from accessing protected data in real time. At the same time, the respective records are sent to CSP in real time for alerting and analysis.

(5) The enforced outbound approval module includes three interactive modes for file outgoing approval, file decryption approval, and ciphertext security sharing. Mail outgoing approval is designed to address the needs of corporate employees to send protected data to external business partners under certain circumstances through email (for example, sending out documents to third-party customers). Once the request is approved, the protected data will be automatically decrypted and sent to the recipient in plaintext. File decryption approval is designed to address the need for enterprise employees to access the plaintext of protected data under certain circumstances (for example: uploading plaintext materials through web portal). Once the request is approved, the protected data will be automatically decrypted, and a plaintext link will be generated for end users to download. The secure sharing of cipher text allows the fast, efficient, and secure sharing of protected data within the company, without limiting transmission tools (such as email attachments,

Skype, FTP/SFTP servers, etc.), and through any type of storage media (such as: NTFS USB disk, SAN, NAS, DAS network disk, etc.).

(6) The backend intelligent analysis module collects fine-grained sentry records from each protected endpoint, including requested data for access, requesting processes, request time, access results (allowed or blocked), etc., as well as CPU usage, memory usage, disk usage and other system running status information. The collected records could be further analyzed for alerting, tracing, and auditing.

(7) The centralized management and control module provides IT admins with the ability to remotely configure, manage each endpoint, and set individual or group security policies for endpoints according to actual needs. At the same time, combined with the results of background intelligent analysis, the status of the data security and system performance of each protected endpoint can be visualized. The details are as follows:

Real-time security warning: While ensuring data security, according to the specific index analysis of data and system security, the system health and safety are classified, and real-time warning is able to be provided.

Big-screen visualization and centralized display: The highly condensed data and the overall status of system security are visually displayed on a large screen/full screen to provide accurate information for operation monitoring, analysis, and decision support.

Dynamic visual security report: It supports dynamic and customized queries and graphical presentations of the respective search results.

2.4 QDocEE Makes Data Protection Easy

From the moment QDocEE is installed on an endpoint, QDocEE starts to protect important data on that endpoint during its entire life cycle from its generation, storage, use, transmission to its destruction. And yet in the eyes of IT Admins and endpoint users, the data protection process is easy. Figure 4 shows the data protection flowchart once QDocEE is installed:

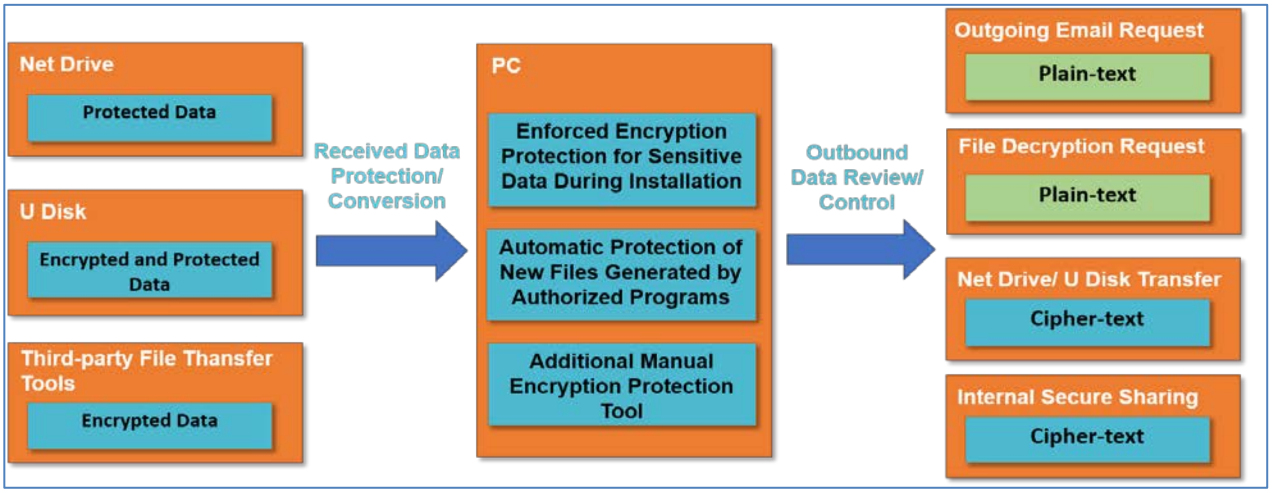

Net Drive
Protected Data
U Disk
Encrypted and Protected Data
Third-party File Thansfer Tools
Encrypted Data
Received Data Protection/ Conversion
PC
Enforced Encryption Protection for Sensitive Data During Installation
Automatic Protection of New Files Generated by Authorized Programs
Additional Manual Encryption Protection Tool
Outbound Data Review/ Control
Outgoing Email Request
Plain-text
File Decryption Request
Plain-text
Net Drive/ U Disk Transfer
Cipher-text
Internal Secure Sharing
Cipher-text

Figure 4: Data protection flow chart of QDocEE.

Data encryption protection inside endpoints: Once QDocEE is installed on an endpoint, data protection inside that endpoint takes immediate effect in two stages: (1) initialization stage, and (2) automatic stage. The initialization stage happens at the moment QDocEE is installed. During the initialization stage, IT admins can remotely enforce encryption protection of the existing important data on the endpoint through CSP by selecting data for protection and authorizing trusted programs. Selected data will be encrypted and protected, and thereafter can be accessed only by processes spawn from authorized programs and following strictly along the respective end-to-end cryptographically secure chain. Immediately after the initialization stage follows the automatic stage, during which all new data files generated by authorized processes will be automatically encrypted and protected without any impact on users' behavior. In addition, EE Client also provides users with a flexible tool to encrypt and protect some files which may not, otherwise, be included for protection by the security policy determined by IT Admins through CSP during the initialization stage.

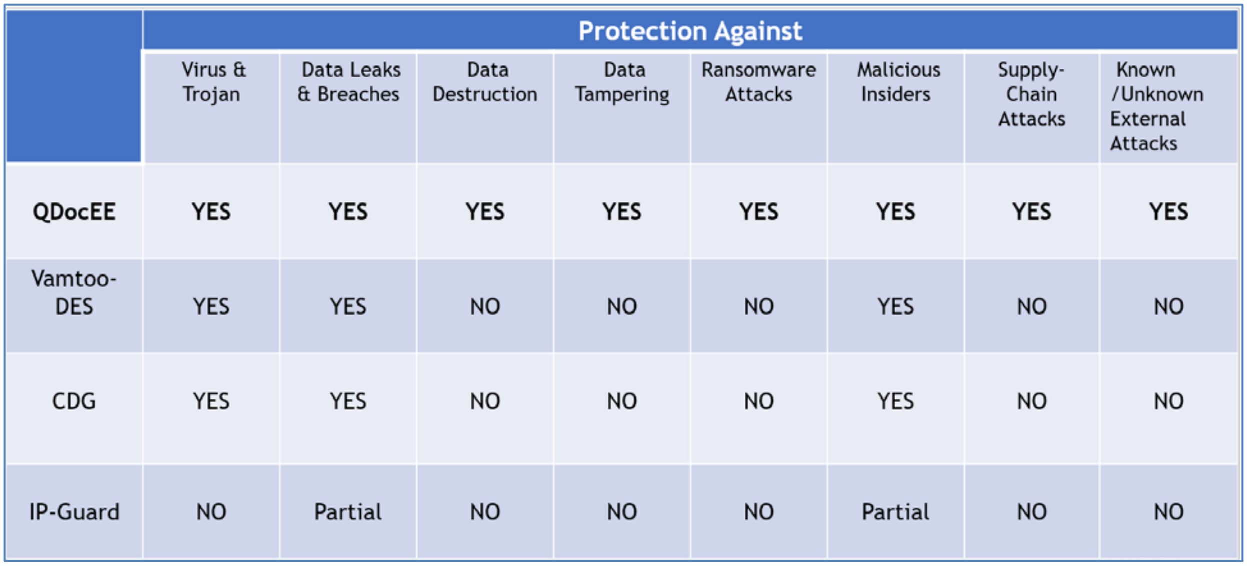
Outbound data review/control: Once QDocEE is installed, you can operate your endpoint as usual while your data is fully protected throughout its entire life cycle. You may not notice any difference until and unless you want to send out protected date from your endpoint, which is tightly controlled. There are four ways to send out protected data from your endpoint through either requested outgoing email, requested file decryption, network disk/USB disk, or internal secure sharing. Requested outgoing email and file decryption require review and approval by designated managers. Once approved, the protected file will be automatically decrypted and sent out in plaintext or for download. When the user runs an authorized program to save the protected data to a network disk/USB disk, the data will be stored in cipher text. Only the authorized process on the managed endpoint can access the protected data, and the protected data cannot be accessed by non-managed endpoints. The secure sharing of ciphertext is a fast and safe data interaction method specially provided by EE for endpoint users, so that the protected data can be efficiently circulated within the company, while ensuring seamless sharing among various managed endpoints.

Protection/conversion of received data: There are three main ways for endpoints to receive new protected data: shared network disk (such as: SAN, DAS, NAS device, etc.), USB disk, or third-party file transfer tools (such as email attachments, Skype, FTP/SFTP server, etc.). When using an authorized program, the data will be automatically encrypted and protected. If the user receives encrypted data (files ending with ".bic") through a third-party application, it will be automatically converted/re-encrypted and protected once it is read once.

3. Competitive Analysis

3.1 Data Security Comparison

Table 1 provides comparison between QDocEE and other endpoint security products in terms of protecting data against various attacks. Compared with traditional endpoint security products, QDocEE is more advanced. In particular, QDocEE is not only fully capable of defending against common viruses, Trojan horses, data leaks, and insider intruder leaks among competing products, but due to the uniqueness of its core technology and design concepts, also has advantages in protecting data against tampering, ransomware attacks, phishing attacks, and other known/unknown external attacks.

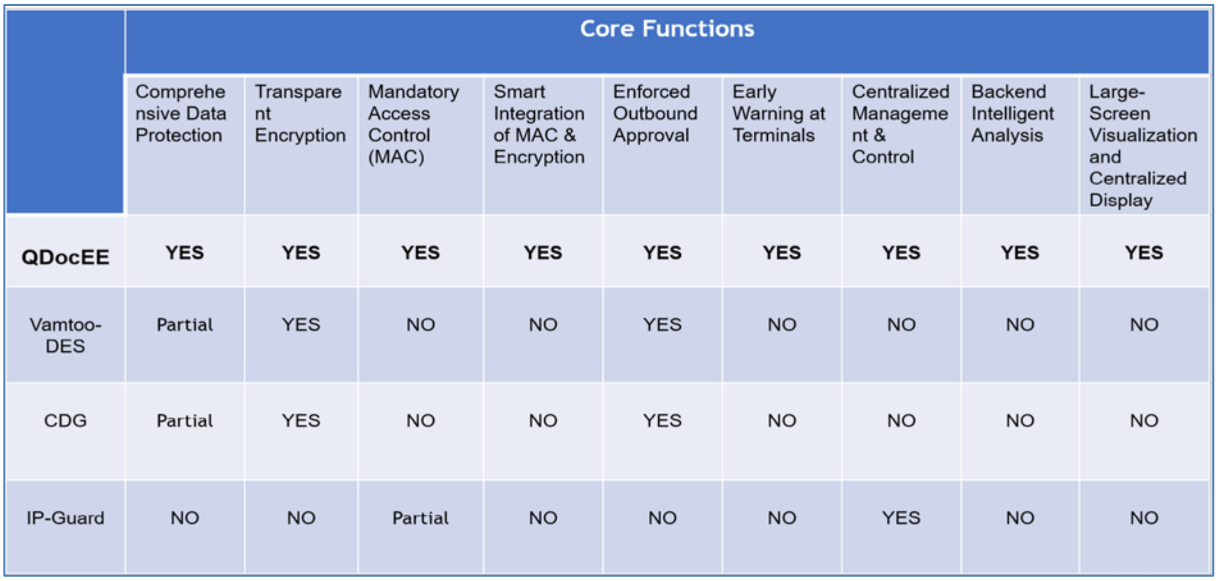


	Protection Against							
	Virus & Trojan	Data Leaks & Breaches	Data Destruction	Data Tampering	Ransomware Attacks	Malicious Insiders	Supply-Chain Attacks	Known /Unknown External Attacks
QDocEE	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Vamtoo-DES	YES	YES	NO	NO	NO	YES	NO	NO
CDG	YES	YES	NO	NO	NO	YES	NO	NO
IP-Guard	NO	Partial	NO	NO	NO	Partial	NO	NO

Table 1: Comparison of data protection against various attacks.

3.2 Core Functionality Comparison

Table 2 provides a core functionality comparison between QDocEE and other competing products. From Table 2, it is clear that QDocEE not only ensures the highest level of data security, but also provides many other functionalities which are desirable for management, analysis, monitoring, auditing, visualization, etc.



	Core Functions								
	Comprehensive Data Protection	Transparent Encryption	Mandatory Access Control (MAC)	Smart Integration of MAC & Encryption	Enforced Outbound Approval	Early Warning at Terminals	Centralized Management & Control	Backend Intelligent Analysis	Large-Screen Visualization and Centralized Display
QDocEE	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Vamtoo-DES	Partial	YES	NO	NO	YES	NO	NO	NO	NO
CDG	Partial	YES	NO	NO	YES	NO	NO	NO	NO
IP-Guard	NO	NO	Partial	NO	NO	NO	YES	NO	NO

Table 2: Comparison of core functionalities between QDocEE and other endpoint security software.

4. Summary

By establishing an end-to-end seamless cryptographically secure chain to enhance the operating system security, QDocEE regulates which processes can access important endpoint data. It puts zero trust on any of networks, systems, and even users, adopts the data centric security model, and can protect endpoint data even when hackers break into the system with full administrative privileges. It is one of few on the market that can protect endpoint data in real time within a dynamical threat environment and against ransomware, malicious insider, supply chain, fileless attacks, and other known/unknown threats. It is easy to set up, easy to use, and highly efficient.

About BicDroid Inc.

Located in Waterloo, ON, Canada, BicDroid Inc. ("BicDroid") is a world technology leader in data and cyber security and has been selected by "Fortune Global 500" companies to protect their server data, enhance the security of their smartphones, and provide secure and reliable remote work solutions for their employees. Built on patented key technologies including quantum safe key management, end-to-end cryptographically secure access control (ECSAC), smart integration of ECSAC and encryption, secure hardware and OS level virtualization, and cryptographic partition for data self-protection, BicDroid’s products make data immune to malicious attacks, protecting data anytime, anywhere, and against any known/unknown threats including ransomware, malicious insiders, supply chain attacks, and fileless attacks. They include QDocument (server-side, client-side, and transmission security) and Quarantined Work Space (QWS), the most innovative, secure, reliable remote work solution on the market, and have been deployed in hundreds of millions of devices.

https://bicdroid.com business@bicdroid.com Call: (519) 573-0096