bicdroid

Make Data Immune to All Attacks

QDocument SE

Protect Server Data Anytime & Against All Threats

Abstract

QDocument SE (QDocSE) is the most innovative and reliable solution on the market to secure server data. It protects server data once and for all against data breaches and all known and unknown attacks including ransomware, phishing, and malicious insider attacks. It polices data access processes at all times, provides detailed access and data governance reports in real time, and denies all unauthorized processes, 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. Introduction

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, 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. Its solution, QDocument SE (QDocSE), protects server data anytime and against data breaches and all known and unknown attacks including ransomware, phishing, and malicious insider attacks. It polices data access processes at all times, provides detailed access and data governance reports in real time, and denies all unauthorized processes, thereby defeating any attempted attacks. It is the most innovative and reliable solution on the market to secure server data.

2. BicDroid's Data Security

History tells us again and again that no matter how they are managed and how often they are updated, networks and systems will be compromised. To make the matter even worse, one often does not know when networks and systems are actually compromised since incidents of attacks are often discovered months or even years later. With this in mind, the most effective defense strategy is how to make your data and cyber activities coexist with all looming threats and continue to function normally even within compromised networks and systems. This is what we call *data security*. Using its patented technologies, BicDroid has developed such data security solutions, which make data immune to all attacks (known and unknown) regardless of the conditions of networks and systems.

Encryption with Post-Quantum Secure Key Management

Encryption is essential for protecting data against data breaches among other things. Once a file is encrypted with a strong key, it is near impossible for anybody without the key to view the plaintext file. However, it is generally not safe to use one key to encrypt all files---once the key is compromised, all files are at risk. As such, it is often required that each file be encrypted using its own unique key. As the number of files increases, the list of keys also grows without bound. Unlike encryption applied for secure data transmission, none of these keys can be deleted---the growing list of keys has to be securely maintained all the time in data protection even after they are securely distributed/established. If keys are being lost, stolen, or misplaced, the respective files are deemed lost, resulting in major headaches for IT departments. Indeed, the daunting task of managing the growing list of encryption keys is the major challenge for enterprises to apply encryption to data protection today. The widely used public key encryption systems are neither convenient nor secure for this purpose---they are vulnerable to resourceful attacks, especially with quantum algorithms, due to the one to one correspondence between public keys and private keys.

Moving beyond public key encryption systems and quantum key distribution, BicDroid has developed the first post-quantum secure key management solution for securely generating, distributing, and maintaining a growing list of encryption keys among multiple devices and multiple users. It enables one-file-one-key encryption. It has the strongest key generation and the most secure key distribution---the distributed keying materials disclose zero information about the actual encryption key---while removing the challenges and headaches of key maintenance. Encryption with BicDroid's post-quantum secure key management provides the first layer of data security with ease:

- Automatic military grade encryption immediately on any device.
- Transparent key management without user interaction and without third party involvement.
- Ensuring the user is always in full control of sensitive data access.
- Ease of use including the securing of cloud services, email attachments, and portable USB media.

Smart Integration of Encryption and MAC (SIME)

Encryption alone is not enough. Although it protects data against data breaches, it is in general ineffective against other attacks such as ransomware attacks. To overcome this, BicDroid has further combined encryption with Mandatory Access Control (MAC) which was first invented to protect US government classified information. Addressing great technical complexities such as cache/non-cache IO, file cache conflicts, random access reading/writing etc., BicDroid has smartly integrated MAC with its patented post-quantum secure file system-level encryption in OS kernels, resulting in security solutions that protect data anywhere (on servers, on endpoints, and in clouds), anytime (at rest, in use, in transmit, and when shared) and against all malicious attacks. With SIME, protected data remains encrypted except when it is accessed by legitimate processes (programs) from legitimate users authorized for plaintext, in which case it will be decrypted by SIME to maintain transparency for such authorized processes and users. Any access to protected data by unauthorized processes will be blocked immediately by SIME.

Fingerprinting

To enforce a tight security policy in SIME, BicDroid has developed a rigorous fingerprinting procedure to authenticate applications (processes) that are authorized to access protected data. The fingerprint of a process is a collection of factors that determine the behavior of the process, including the binary code of the program that spawns the process, dynamic linked libraries the process loads, parameters used to create the process, environmental variables used by the process and etc. When an application is tampered, its fingerprint will be modified, and the application will be immediately blocked from accessing protected data. Meanwhile, any update to the authorized application by its legitimate developers will not affect its fingerprint, and therefore no re-configuration of the security policy is needed after updates, requiring minimum input from the user.

Likewise, BicDroid has also invented a fingerprinting scheme for identifying protected data as well. This enables BicDroid’s solutions to focus on critical data protection and not to interfere all other system operations, achieving efficient, robust and secure data protection while causing no interference with users’ own activities.

In addition, BicDroid has creatively designed a fingerprinting method for identifying each instance of the running engine of QDocSE with a randomly generated number to support tasks such as activation or configuration without revealing any information of user systems.

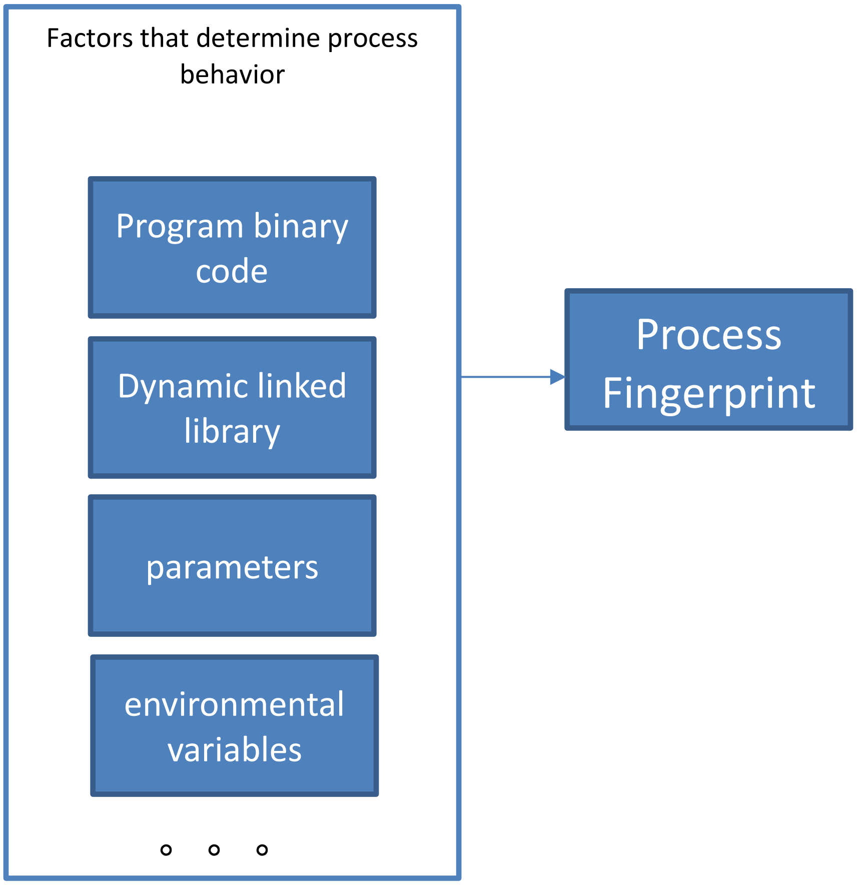

Figure 1 Process Fingerprint

Security module in the Kernel

The kernel is the hard core of a computer's operating system (OS), managing all other programs in the OS. All critical resources in a computer, including persistent and non-persistent data storages (aka hard drives and RAMs), are controlled by the kernel of the OS on the computer and any request to those resources must be served by the kernel. To provide ultimate data security, BicDroid has developed a kernel module to enhance the OS kernel by implementing SIME through the kernel module, a guardian that oversees data storages. The kernel module inspects any requests to data in hard drives or RAMs from any computer process and grants those requests only if they are authorized according to the security policy configured in SIME and its fingerprint. As the OS kernel has the complete control over everything in the system, BicDroid kernel module can prevent any action of malicious processes on protected data, and therefore provides unbreakable data security. BicDroid kernel module is also extremely efficient and has no impact on the performance of the computer, which is essential for any performance-critical computer systems such as database servers.

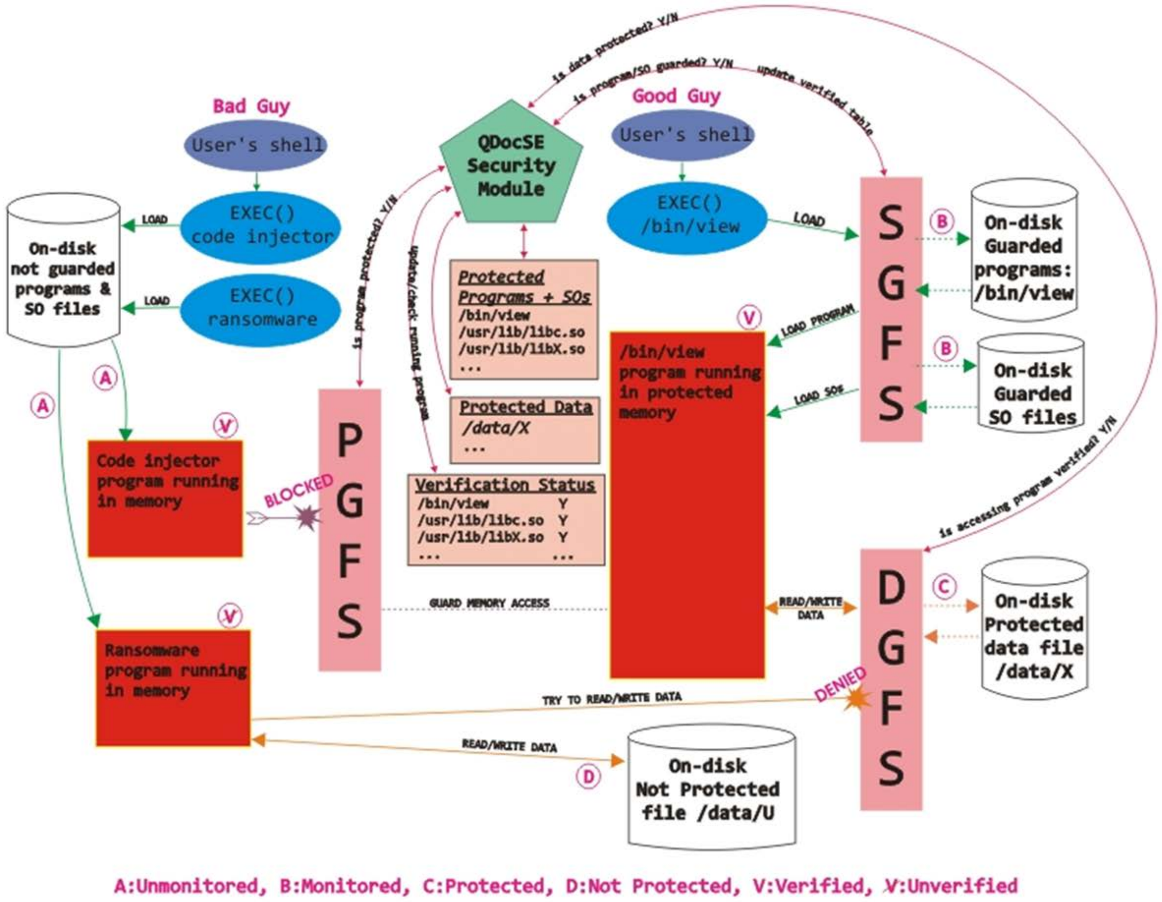

Figure 2 Security module in the kernel

Data Governance

To complement data protection against data breaches and all known and unknown attacks, BicDroid's data security solutions also include real time data governance by integrating reporting & alerts, data access control, and post-quantum secure key management.

Data governance is concerned with how data is created, used and managed. As data becomes the most valuable asset for enterprises and organizations, good data security solutions should include data governance as a component. However, complicating data governance is that there are nowadays more and more diverse ways to access data. For example, due to the popularity of Bring Your Own Device (BYOD) policy among enterprises, it is reported that 80% employees are using personal smartphones and tablets for work. Inevitably, enterprise data will be accessed on employees' mobile devices. Then how to ensure those data are properly handled and how to make people accountable for adverse events such as data leaking and tampering becomes extremely difficult.

BicDroid approaches the data governance problem from a completely new angle, resulting in an innovative “data centric” solution. With BicDroid’s data security solutions, protected data remains encrypted at all places and at all times except when it is accessed by legitimate processes (programs) from legitimate users authorized for plaintext. Any person or computer program trying to touch data has to go through a rigorous authorization procedure before the data is unlocked for accessing. During the authorization procedure, reports about legitimate data access or alerts about attempts of unauthorized data access (which are blocked by BicDroid’s solutions) are collected in real time by a central monitor for analyzing and auditing. Consequently, with BicDroid’s data security solutions in place, data access (when, where and by whom) becomes totally transparent to the management of enterprises in real time.

3. BicDroid QDocSE

Integrating BicDroid’s patented technologies, BicDroid QDocSE is the most innovative and reliable solution on the market to secure server data. It protects server data once and for all against data breaches and all known and unknown attacks including ransomware, malicious insider attacks, etc. It polices data access processes at all times, provides detailed access and data governance reports in real time, and denies all unauthorized processes, thereby defeating any attemptedattacks.

How Does QDocSE Work?

QDocSE provides proactive protection to critical data on servers such as Exchange, SQL, Hadoop, Sharepoint, etc. It includes conceptually three components: SIME kernel module, SE Console & Service, and Central Sentry Platform (CSP). Figure 3 illustrates a typical deployment of QDocSE to protect a single server, where the CSP Admin is an employee of the organization responsible for the server data security. Different from the CSP Admin, the server administrator with root privilege of the server, who is in charge of the daily maintenance of the server, is completely kept out of QDocSE.

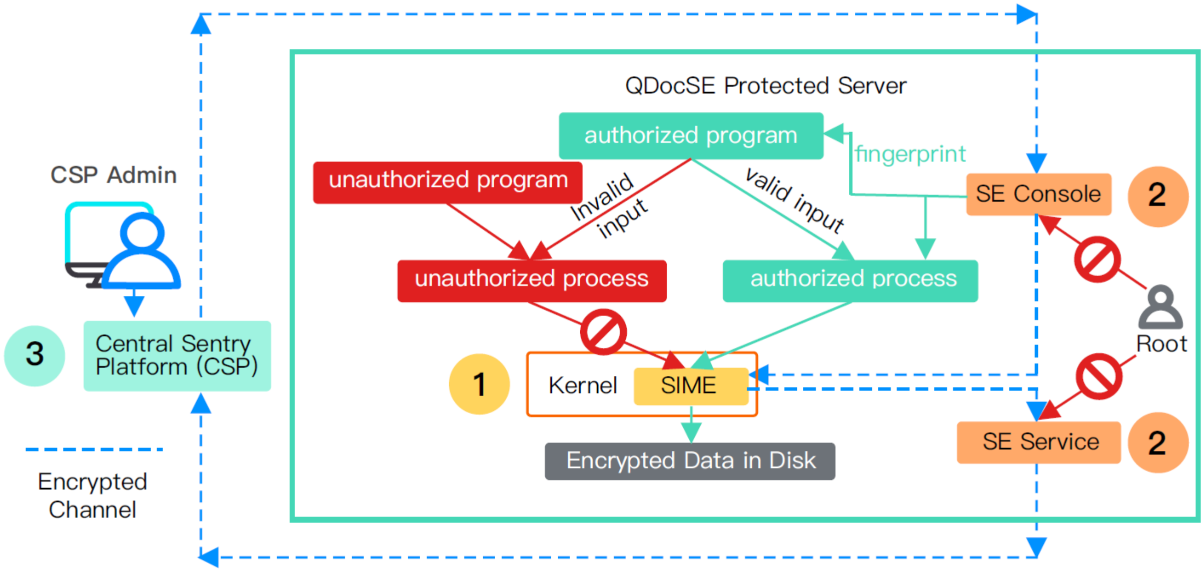

Figure 3 QDocSE deployment

SIME kernel module

Smart Integration of Mandatory Access Control and Encryption (SIME) inside OS kernels is a key module to enable data self-protection against any attack by allowing only processes spawned from authorized programs with valid input to access encrypted data. With mandatory access control (MAC) and filesystem encryption coupled into a single unit, there is no data breach even when MAC is hacked. In addition, thanks to Quantum Safe Key Management Service (QSKMS) embedded inside SIME, each protected file is encrypted by a unique encryption key with no key management headache.

SE Console & Service

Taking inputs from CSP, SE Console configures data security policy, which is in turned enforced by SIME, while SE Service ingests logs of authorized accesses and blocked access attempts towards protected files from SIME, monitors server health, and then sends observed information to CSP for analysis, visualization, and alerting. Both SE Console & Service are protected by encryption against root attacks.

Central Sentry Platform

Connected to SE Console & Service installed on servers in a cluster, CSP is the one-stop web portal to manage, control, monitor, analyze and visualize data security and health of the server cluster. Empowered by strong authentication and advanced multi-level authorization, CSP makes overwhelming data security management operations and data governance on server clusters simple and swift.

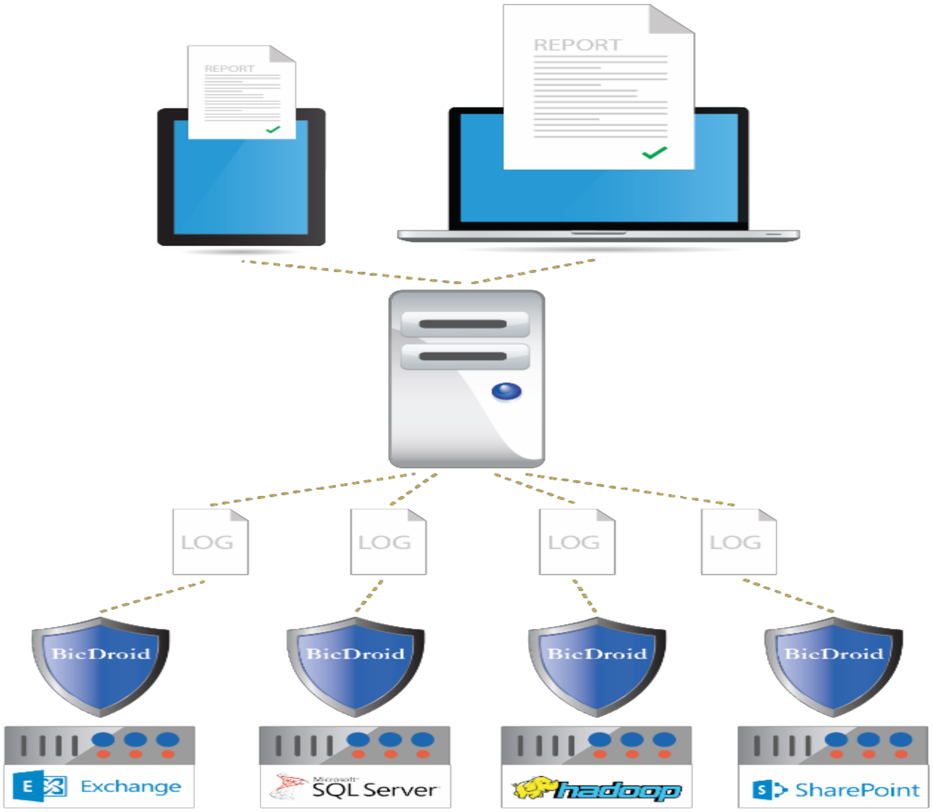

Figure 4. Data Security Management and Data governance by CSP

4. Competitive Advantages of BicDroid QDocSE

Table 1 shows the comparison of BicDroid QDocSE and other competitive products in the server data protection market. Competitor A is a world-known security vendor, who adopts the white-list methodology and develops a comprehensive application control framework. It can protect data against known and unknown ransomware attacks, to a large extent, with significant degradation in server performance.

Competitor B is a large anti-virus company, whose solution is based on a globally synchronized black list. It does very well on catching known ransomwares. However, it is completely ineffective to unknown ransomwares. Due to its interference with the system's operation, it is generally not recommended for servers.

Both Competitor A and Competitor B don't protect data against malicious insider attacks, nor do they prevent data breaches. Furthermore, both Competitor A and Competitor B suffer from a system loophole. I.e., when a system loophole, such as the

Eternal Blue, is discovered and leaked, the data security will be immediately compromised, because the white-list in Competitor A has to contain system processes and the black-list in Competitor B will have to exclude every system process until one is proven to have a loophole. On the contrary, with the protection of QDocSE, the data security will not be impacted even if a new system loophole is found, because by default QDocSE will not trust any system process unless it is explicitly authorized by the user.

Compared with Competitor A and Competitor B, another clear advantage of QDocSE is that it remains zero knowledge of any information about servers in the user organization while both Competitor A and Competitor B have to extract user's system data and send it to a vendor's server or third party cloud, leaving a security hole of possible data leaking. Actually, in August 2017, Competitor A has been reported to be responsible for leaking Terabytes of confidential data from Fortune 100 companies due to its practice of synchronizing users' system data to the public cloud.

QDocSE also leads in the comparison of computational efficiency. Both Competitor A and Competitor B show a significant impact on the computational performance, because Competitor A has to maintain a whitelist of the whole system and Competitor B has to constantly scan the whole system while synchronizing its blacklist globally through public cloud or private vendor networks. QDocSE, on the other hand, is designed to manage a short list of authorized processes for critical data. Our performance tests with QDocSE on various SQL servers have shown that QDocSE leaves no impact on the computational performance of the system.

Competitor C provides a conventional encryption solution, which secures data against breaches, yet fails to protect data against any ransomwares, malicious insider attacks, etc.

Table 1 Comparison with Competitive Products

Server Data Protection				
	QDocSE	Competitor A	Competitor B	Competitor C
Data protection against known ransomware	✓	✓	✓	✕
Data protection against unknown ransomware	✓	✓	✕	✕
Data protection against Malicious insiders	✓	✕	✕	✕
Data protection against phishing	✓	✓	✕	✕
Data breach prevention	✓	✕	✕	✓
Data encryption	✓	✕	✕	✓
Data protection any time (at rest and in use)	✓	✕	✕	✓
Robustness against system loopholes	✓	✕	✕	✕
User's complete control	✓	✕ (User's system data extracted to vendor's server or third party cloud)	✕ (User's system data extracted to vendor's server or third party cloud)	✓
Data access governance	✓	✕	✕	✕
Server performance	No impact	Significant degradation	Significant degradation	Negative impact

5. Conclusion

As a response to the rapidly evolving threat landscape, BicDroid QDocSE represents a paradigm shift in cybersecurity technology. By a smart integration of encryption with post-quantum secure key management and MAC in the OS kernel, QDocSE provides a guaranteed server data protection against data breaches, ransomware attacks, malicious insider attacks, and all other known and unknown threats without any impact on the system computational performance.

6. Specifications

QDocSE supports both Windows and Linux servers including:

- Windows Server 2008R2 and above
- CentOS 6 & 7
- Ubuntu 18 and above

QDocSE is compatible with all mainstream data storage technology including:

- NAS
- DAS
- SAN

QDocSE can protect all mainstream database servers including:

- MSSQL
- MySQL
- Oracle
- PostgreSQL

QDocSE can protect big data platform including:

- Hadoop

CSP must be deployed on CentOS 7.6 with minimum hardware specification:

- 4 cores
- 8G memory
- 500GB disk space

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