ProvenDB

Secure Database

Solution Brief

ProvenDB
Secure Database

Overview

Gartner estimates that global spending on Data security will exceed $72 Million in 2020. Data security attacks are increasingly pervasive, sophisticated and costly, and consequently, Data security is one of the fastest-growing segments in the Information Security landscape.

Historically, Data theft has been the most prevalent type of Data security incident, and subject to the most attention. However, attackers are also increasingly manipulating data within target Databases in order to accomplish a malicious objective, to cover tracks of a breach, or to create permanent back doors into an organization.

ProvenDB Compliance Vault is a tamper-proof, highly secure Database system. Best of breed Database security and encryption prevents any unauthorized Database access, while Blockchain integration prevents any undetected tampering of data. With ProvenDB Secure Database, you can have 100% certainty that data integrity has been maintained and that no undetected manipulation of data has occurred.

Information and Data security

Security of Information has been a concern for governments and enterprises well before the transition to digital storage technologies. Information security has always had two key concerns:

1. Preventing unauthorized access to Information
2. Preventing unauthorized modification of Information

Before the emergence of digital storage technologies and the internet, physical security (vaults, secure premises, etc.) were generally sufficient to prevent unauthorized access of Information. The threat of unauthorized modification of data – especially from insiders – was mitigated by the use of ledgers and other records that were inherently tamper-evident. Backdating entries in a business ledger was hard to achieve without leaving evident traces. Nevertheless, "cooking the books" was and remains a typical element in financial crime.

With the emergence of digital storage technologies and the internet, the scope of Information risk has magnified dramatically. All critical information is now held on digital media, and almost all of that information is directly or indirectly accessible via the internet. A sophisticated hacker has an extremely target-rich environment. An attacker can mount attacks against virtually any organization and exploits that allow access to a single organization can almost always be used against other organizations.

https://www.gartner.com/en/newsroom/press-releases/2019-10-28-gartner-forecasts-enterprise-security-and-risk-manage

Unlike pre-digital technologies, records in digital storage can be modified without leaving any evidence. Information is stored on disk in the form of magnetic or electro-static charges. Changes to data on digital storage create no meaningful forensic traces. The world's entire information architecture is built on a storage medium which is far more susceptible to malicious tampering than the humble paper ledger.

Defence in Depth

Traditional mitigation for the extreme inherent vulnerabilities created by digital storage technologies attached to the internet is often summarized as "Defence in Depth".

Defence in Depth involves a multi-layered approach to protecting information assets. In a typical application architecture, the raw data on disk might be accessible only to a Database Server which implements its own stringent access controls. The Database Server is only accessible from the Application Server which employs a distinct set of access control mechanisms. Access to the Application Server is restricted by network security, while the network is protected by the firewall, and so on.

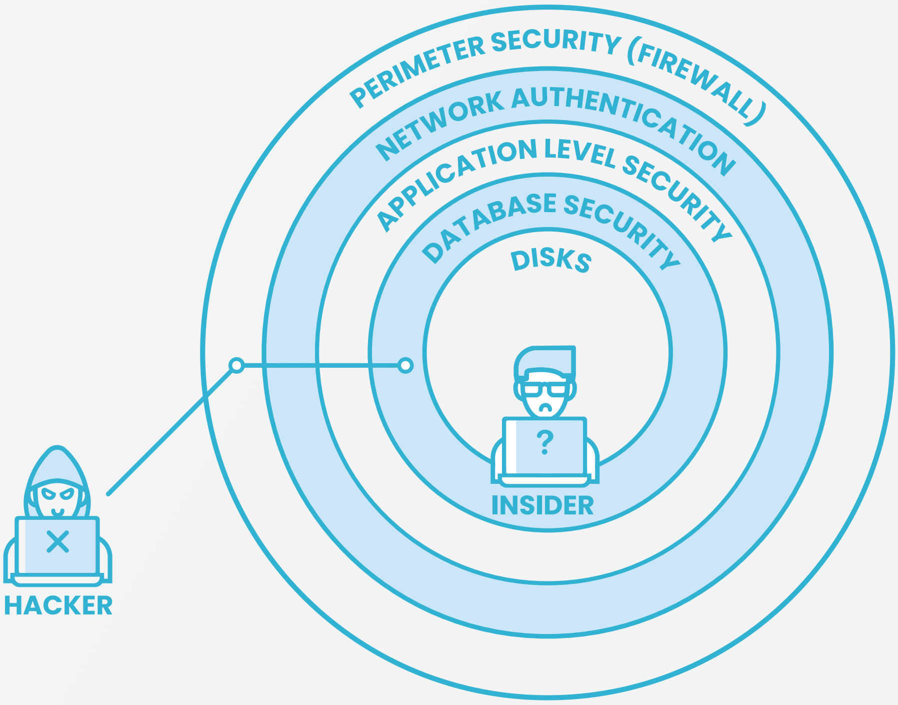


Figure 1: Defence in depth provides a multi-layered approach to protecting information assets

Defence in Depth is a valid and vital paradigm. However, in today's threat environment, it provides more psychological assurance than actual hard protection.

Currently, there are at least two attack vectors for which we have little protection:

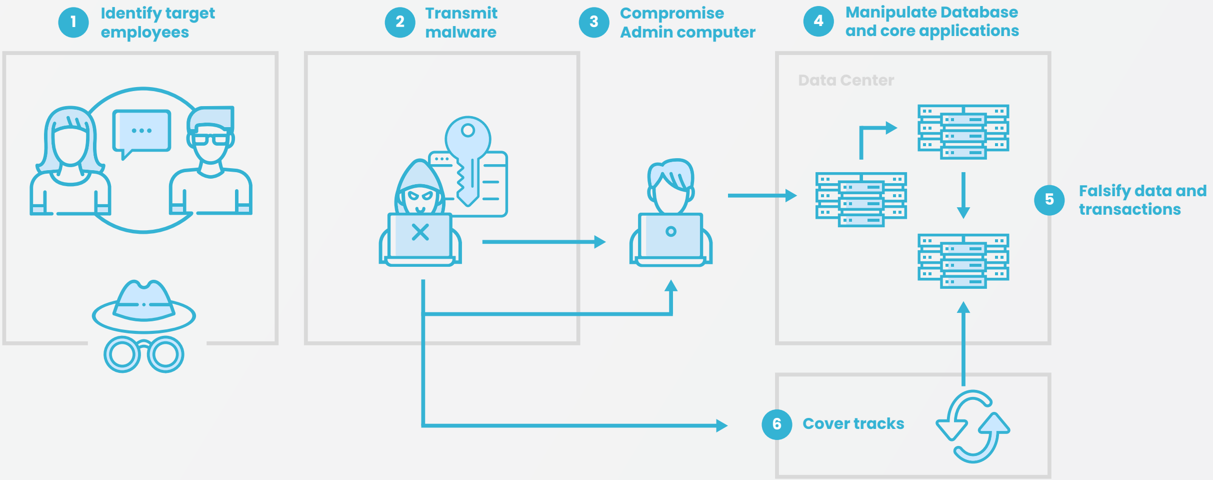
1. Almost all organizations have applications and systems within the internal network that are connected to the internet. A hacker that compromises one of these applications has effectively bypassed the outer layers of defence.

2. In every system, there are insiders – System and Database Administrators – who have virtually unrestricted access to the innermost tiers of information. These individuals can perform exploits for which there is little defence, and which can mostly go undetected. Even if an insider is entirely trustworthy, their credentials can be stolen and used without their knowledge by a malicious outsider.

Anatomy of an Advanced Incident

Advanced Incidents, such as Advanced Persistent Threats (APT) clearly illustrate these vulnerabilities. These are incidents that involve sophisticated attackers utilizing multiple techniques over an extended timeframe to accomplish a high-value attack.

The Carbanack attack is probably the best-known example of an APT. In Carbanack, hackers identified critical individuals within a target organization who were then targeted with carefully constructed malware delivered via email. This malware eventually allowed the attackers to compromise one or more admin accounts. From there, they were able to modify Database records to falsify account balances. They also used these elevated privileges to remove all trace of the exploit.



1 Identify target employees
2 Transmit malware
3 Compromise Admin computer
4 Manipulate Database and core applications
Data Center
5 Falsify data and transactions
6 Cover tracks

Figure 2: Anatomy of an Advanced Persistent Threat

Defending against APT and other advanced threats requires mitigating three particularly difficult vulnerabilities implicit in the Defence in Depth paradigm:

1. Privileged insiders with administrative access are generally capable of accessing and tampering with data in even the most secure systems. In some contexts (for instance, in the Intelligence community) these insiders might be compromised directly by an outside agency. In other contexts, insiders might be tempted to manipulate data in pursuit of financial gain.

2. Even if insiders are entirely trustworthy, the authorizations granted to privileged insiders may be compromised without their knowledge or consent, through malware or another exploit.

3. Attackers routinely modify log and audit data to cover their tracks – a Carbon Black threat report found that in 72% of cases, Incident Response professionals had encountered destruction of logs as a mechanism for concealing a Security Incident.

The Blockchain Paradigm shift

Blockchain represents a paradigm shift in digital storage. Unlike previous digital storage technologies, data written to a public Blockchain cannot be overwritten. As a proof point, in the just over ten years of operation of the Bitcoin Blockchain, no one has successfully tampered with Bitcoin Blockchain records – despite the billions of dollars that could be stolen should such an attack succeed.

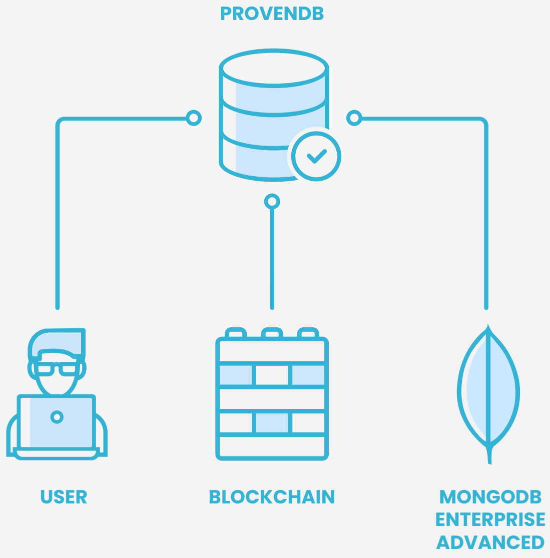
Unfortunately, the economics of the public Blockchains are prohibitive. While public Blockchains offer unparalleled security for transactions, the data payloads that may be associated with these transactions is typically less than a Kilobyte. As a result, storing just a GB of information on a public Blockchain costs millions of dollars. And while private Blockchains can achieve better economics, they cannot provide the security of a public Blockchain.

In addition to economic obstacles, Blockchains offer none of the features that have made Databases the cornerstone of information storage. Blockchains offer no structured storage, support minimal transaction rates, and provide no flexible query mechanisms.

In short, while public Blockchain technology represents a real breakthrough by providing a tamper-proof digital data storage mechanism, public Blockchains are not suitable for use as general-purpose data storage solutions.

https://usa.visa.com/dam/VCOM/download/merchants/Alert-CARBANAK.pdf

ProvenDB Secure Database



ProvenDB Secure Database combines Blockchain technology and traditional Database technology to provide a uniquely secure and tamper-resistant, yet functional and performant Database solution.

The foundation of ProvenDB Secure Database is **MongoDB Enterprise Advanced**. MongoDB is the world's most popular and widely deployed NoSQL Database, and MongoDB Enterprise Advanced includes advanced security features including:

- TLS/SSL encryption of data transmitted over the network
- Client-side Field Level encryption
- Encryption of data at rest
- Auditing and access control features

ProvenDB offers most of the functionality of MongoDB Enterprise, but adds the following features:

- **Immutable Data:** Data in ProvenDB is not destroyed when update or delete operations are issued. Old versions of data remain available indefinitely.
- **Versioned Data:** Multiple versions of the Database state are maintained. The user can navigate to a previous version - "time travelling" within Database history.
- **Blockchain Data:** Database versions and individual documents are anchored to the Blockchain. These Blockchain proofs substantiate the existence, ownership and integrity of specific documents or a complete Database version.
- **Data Provenance:** The complete history of a data item can be retrieved, with Blockchain proofs testifying to that history.

ProvenDB architecture

One of the key differences between a Blockchain and a Database is that a Blockchain is an immutable, append-only datastore. In a Blockchain, data items are never overwritten: all changes to the Blockchain are appended as new blocks in the chain.

ProvenDB brings immutability to the Database world by using **versions**. In ProvenDB, a delete operation does not remove a document. Instead, it creates a sort of "tombstone" marker, hiding apparently deleted documents from view.

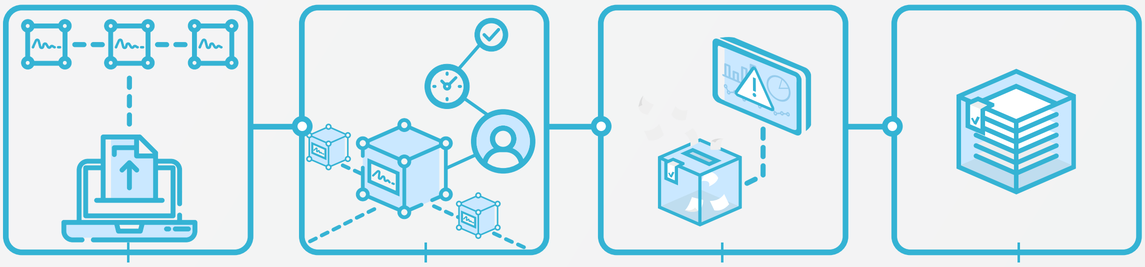
https://www.carbonblack.com/global-incident-response-threat-report/november-2018/

Likewise, an update operation does not replace an existing document: rather, it hides the old document and adds a new version of the document in its place.

Old versions of the Database can be viewed in a read-only mode, creating a sort of "time travel" view of Database history.

Versions of the Database or specific documents are anchored to the Blockchain using **proofs**. Proofs are cryptographic structures that amalgamate the digital signatures (hashes) of multiple documents into a single "root" hash. This hash is placed on a public Blockchain potentially providing proof of state for hundreds of thousands or millions of Database records.

ProvenDB bridges the gap between database systems and Blockchain, providing you with a proven data storage solution.



When information is added to ProvenDB, digital signatures are created and posted to the immutable Blockchain.

These signatures can prove the integrity, ownership, and creation date of your information.

ProvenDB will promptly Identify any attemtps to tamper with underlying data.

Data within ProvenDB Is completely trustworthy and Immune from undetected tampering.

ProvenDB Secure Database features

ProvenDB Secure Database offers the following features:

- **MongoDB compatible** document model and API. ProvenDB is fully compatible with any application development framework that supports MongoDB including popular frameworks for Java, JavaScript, Python, GoLang, and other languages.
- **Blockchain proofs** of integrity for the entire Database, individual documents or collections of documents.
- A **GDPR compliant** "forget" feature that redacts Information without compromising cryptographic proofs.
- A complete **history of changes** for documents.
- **Compaction** of data between blockchain proofs to reduce storage overhead.
- **Exports** of data and proofs to a provable archive which does not require the ProvenDB engine.
- **MongoDB Enterprise Advanced security features** such as encryption at rest and in transit.
- **Support for multiple Blockchains** including Bitcoin, Ethereum, Quorum and Elastos.

ProvenLogs

ProvenLogs is a ProvenDB Secure Database utility that prevents tampering with log data. It is implemented as a transparent listener on a logging stream that digitally signs log entries, stores the signed logs in a ProvenDB Database and submits Blockchain proofs for batches of log data. Any attempt to manipulate logs by an attacker can be quickly identified by checking the hash values submitted to the Blockchain, and the log data stored in the ProvenDB Database can be used as a secure backup.

Conclusion

ProvenDB Secure Database is a tamper-proof, extremely secure Database system. Best of breed Database security and encryption prevents any unauthorized Database access, while Blockchain integration prevents any undetected tampering of data. With ProvenDB Secure Database, you have 100% certainty that data integrity has been maintained and that no undetected manipulation of data has occurred.

ProvenDB is an ideal basis for building highly secure systems in finance, government, defence and other enterprises.

Using ProvenDB Secure Database, you can prevent insiders and outsiders from tampering and manipulating with your data. Visit www.provendb.com to sign up for a ProvenDB cloud service, or email us at support@provendb.com to explore options for deploying ProvenDB Compliance Vault within your organization.

https://medium.com/provendb/prove-logs-on-blockchain-with-go-and-provendb-ca53d8a907e1

ProvenDB

www.provendb.com
info@provendb.com

/provendb

L3, 20 Queen Street, Melbourne VIC 3000, Australia.