ProvenDB

ProvenDB for Oracle

Solution Brief

ProvenDB for Oracle Solution Brief

Overview

Databases are at the core of all Applications. The integrity of data in an Oracle database is critical to the integrity of all applications built on that database.

Gartner estimates that global spending on Data security will exceed $72 Billion in 2020[1]. 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. At the same time, we live in an era of decreasing trust in digital information – the prevalence of falsified and fabricated digital information is increasing, with a corresponding decrease in trust. Regulators, customers and business partners are increasingly unwilling to take digital information on trust – they want proof!

ProvenDB for Oracle adds proof, trust and integrity to the data in an Oracle database. Using ProvenDB for Oracle, you can prove the provenance, integrity and ownership of data to regulators, business partners and customers, and respond efficiently to the most rigorous compliance audit. You can detect and rapidly respond to any data manipulation cyberattacks and ensure the integrity of your audit logs and access controls. ProvenDB achieves this by anchoring digital signatures to immutable public or private blockchains that attest to the ownership, provenance and integrity of your Oracle data.

How it works

ProvenDB for Oracle brings the strength of blockchain immutability and tamper-proofing to Oracle databases.

When data is added to or modified in a database being monitored by ProvenDB for Oracle, cryptographic signatures of the data are created. These signatures can be "signed" by your company's cryptographic key (possibly the same key that guarantees the identity of your website). These signatures are aggregated and anchored to a public Blockchain such as Bitcoin, Hedera or Ethereum.

---

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

Figure 1 ProvenDB for Oracle architecture

Once anchored to the public Blockchain, the signatures form an impeccable and irrefutable proof of the integrity and origin time of the Oracle rows. The Blockchain record – which cannot be altered by any known technology – proves the overall integrity and timestamp of items in the database, eliminating any possibility of undetected tampering or backdating.

ProvenDB for Oracle integrates with the Oracle Flashback query and Oracle Flashback Data Archive technologies. If these are enabled, ProvenDB for Oracle allows you to generate and validate proofs for historical data as well as the current contents of the database. Using ProvenDB for Oracle in conjunction with Oracle Flashback technologies, you can maintain a fully auditable, tamper-proof history of data changes with the integrity and provenance of every data item backed by immutable blockchain proofs.

Oracle Blockchain tables

Oracle 21c supports a new "Blockchain" table type. A blockchain table is an append-only table in which each new row is cryptographically dependent on a previous row. Oracle Blockchain tables serve a useful purpose, but are not truly immutable or tamper proof. A Database Administrator could potentially "fake" a blockchain table with an apparent timestamp simply by manipulating the system clock. To prevent tampering, Oracle recommends that you periodically export hashes and sequence numbers from the database so that any attempt to change these within the database can be detected[2].

ProvenDB for Oracle is compatible with Oracle Blockchain tables and can be used to create "real" blockchain anchors that will detect any attempt to create a falsified blockchain ledger. Furthermore, ProvenDB for Oracle offers capabilities in advance of the Oracle Blockchain table capability – it can be used with any table types, and can be used with Oracle versions prior to 20c.

---

[2] https://blogs.oracle.com/imc/managing-blockchain-tables-in-oracle-database-20c

ProvenDB for Regulatory Compliance

It is well known that the potential penalties for non-compliance far outweigh the costs of compliance. According to a Ponemon study of large US-based multi-national corporations, the cost of not being compliant is roughly three times the cost of implementing effective compliance measures[3].

Maintaining compliance documentation in a central data store is an obvious measure that an organization can establish to prove compliance. However, regulators require far more than a simple database of compliance documents and datasets. For instance, the following regulator's guidelines clearly articulate the high bar for data integrity (our emphasis):

> *Auditability (the ability to **confirm the origin of data** and provide **transparency of all alterations**) is a key element to verifying data quality. It involves the examination of data and associated audit trail, data architecture and other supporting material. APRA envisages that a regulated entity would ensure that **data is sufficiently auditable** in order to satisfy the entity's business requirements (including regulatory and legal), facilitate independent audit, assist in **dispute resolution (including non-repudiation)** and **assist in the provision of forensic evidence** if required*[4]

Only with ProvenDB for Oracle can you fully meet these regulatory requirements. ProvenDB for Oracle completely eliminates the possibility of undetected improper manipulation of data. In the event of an attempt to modify historical data, immutable blockchain proofs would be violated. The timestamps on the blockchain proofs provide absolute proof of the data's origin time and contents. Regulators, business partners and internal compliance teams can have complete confidence in the contents of the database.

ProvenDB for Cybersecurity

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

---

[3] https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf

[4] https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_1.pdf

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.

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 suspectable to malicious tampering than the humble paper ledger.

Data in an Oracle database is protected by multiple layers of security – database access controls, operating systems authentication and network security. However, in the event that these controls are breached, data in an Oracle database can be manipulated potentially leaving no trace of the manipulation.

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 Database Administrator accounts. From there, they were able to modify Oracle Database records to falsify account balances[5]. They also used these elevated database privileges to remove all trace of the exploit.

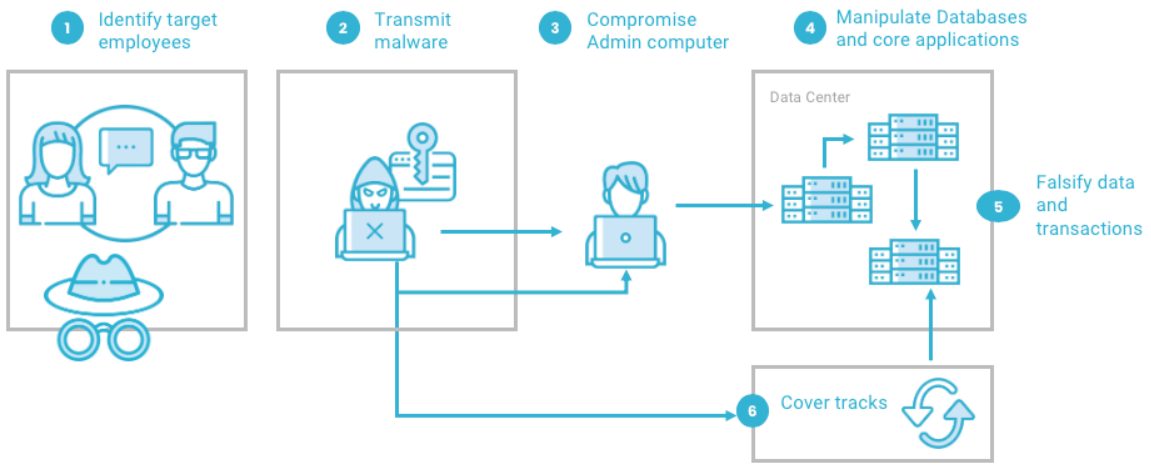

Figure 2 Anatomy of an Advanced Persistent Threat

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

ProvenDB for Oracle mitigates against these threats by providing absolute certainty of the provenance and integrity of database records. Every database record's origin date and contents can be validated by reference to an immutable blockchain transaction that cannot be altered by any known technology. Although no technology can guarantee the correctness of transactions, with ProvenDB for Oracle, you can have absolute certainty of the provenance and integrity of your data. Any attempts to backdate or fabricate transactions cannot go undetected.

Conclusion

ProvenDB for Oracle allows you to have complete trust in the integrity and provenance of Oracle data.

Oracle database entries are mutable by design - anything inserted can be updated or deleted. This can lead to problems ensuring the accuracy of legally sensitive records or financial information since there's no way to guarantee that data has not been backdated or tampered with. Sophisticated cyberattacks that modify the contents of databases are also possible.

ProvenDB for Oracle uses blockchain technology to provide proof of origin and integrity of selected rows within an Oracle database. Using ProvenDB, you can prove the provenance and integrity of your data and prevent against cyberattacks that manipulate sensitive data.

support@provendb.com
www.provendb.com

/provendb