

Enhancing Database Encryption Solutions with Data-centric Security

When examining enterprise data security and risk, data can be classified into three obvious groups:

- **Data-in-use:** data that is the least at risk
- **Data-at-rest:** data that is at moderate risk
- **Data-in-motion:** data that represents the greatest risk for an organization

Data-in-use represents the class of data that benefits from the greatest scrutiny and the most automated systems of protection. A production database is surrounded by significant physical and logical perimeter defenses, robust user access, authentication, and auditing controls, and will have many people looking at it from different perspectives constantly. Anytime a cybercriminal attempts to attach to a production database, that person puts themselves at severe risk of being identified. In order to effectively gather enough material, the cybercriminal must

Risks of Typical Sensitive Data Exchanges

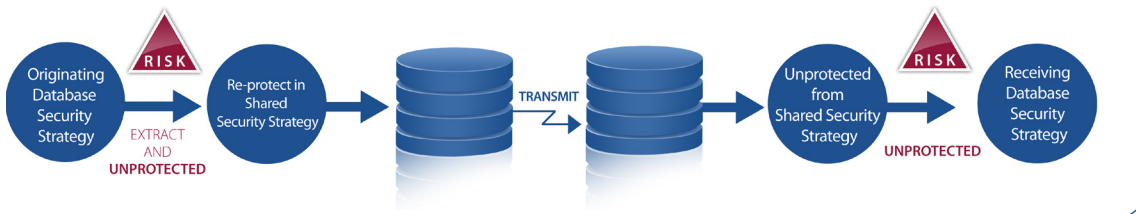


Diagram 1-1

remain attached directly to the production database, the most heavily monitored and managed environment in an organization's infrastructure.

The risks to the cybercriminal increase the longer they stay attached to the database. Even the bulk copy of an encrypted database can take considerable time, increasing the chance of being caught.

Data at rest is more vulnerable, as it can go missing for significant periods before a loss is discovered. A database extract written to tape has the tape volser recorded at time of creation but, once that tape is hung on a rack, no one may monitor its well being or location for weeks or months. Additionally, when such extracts are being transmitted or transported outside the organizational perimeter, the degree of risk increases exponentially. Not only is a large aggregation of data subject to less scrutiny than a production database, it actually leaves the direct control of the originating organization, increasing opportunities for compromise.

Moreover, a cybercriminal that obtains a database extract tape or

transmission containing hundreds of thousands or even millions of sensitive records stands to gain far more than the cybercriminal who extracts a few hundred details from a production database, and at far less risk to the criminal.

As a result of these risks, enterprises dedicated to preserving the privacy of sensitive data and integrity of corporate brands, as well as controlling costs of compliance, look to supplement database security to mitigate these greater risks.

Protecting data beyond the [physical or logical]

Database security is effective only as long as the protected data remains within the originating database's protection strategy. Effectively exchanging data with business partners, or even other locations within

the same enterprise, requires the data be extracted from these database protection strategies into a format that can be consumed by the receiving applications.

Diagram 1-1 illustrates the risks typical sensitive data exchanges impose on

organizations. An originating organization may have a durable protection strategy within their database, implemented through a commercial product or open source technology. The sensitive data protected in this strategy must be shared with an outside party. However, the outside party's receiving database or application has an entirely different data protection strategy, using a different technology.

In order for the data exchange to be effective, the originating company needs to decrypt the data and place it, unprotected, on a disk. They then need to re-protect it using a security strategy shared with the receiving organization. That period when the sensitive data is between the originating and shared security strategies represents an unmitigated risk. When the data is received, the same process must take place, once again leaving data unprotected, and introducing unmitigated risk.

In today's environment, businesses are subjected to increasing regulations and legislation. Organizations must seek additional security to ensure data extracted from their databases is appropriately protected. What's needed is protection that travels with the data itself, from the

moment it is extracted from the database.

SecureZIP from PKWARE provides exactly that - the means to apply immediate data-centric security to data extracted from databases. It applies data encryption directly to the extracted data streams and places them inside the universal ZIP container that provides the additional benefit of cross-platform portability. SecureZIP uses strong encryption algorithms, sufficient to meet the expectations of regulators and stakeholders, using either passphrases or digital certificates for encryption/decryption keys.

This data-centric approach ensures that when data is extracted from the database, the data remains protected while at rest locally or in transit outside the organization. It ensures that only someone (i.e. the recipient) with the appropriate credentials (either the passphrase or the private key) will be able to open and access the database extract contained inside the secure archive. This approach also ensures the data is protected even if intercepted in transit or lost.

Equally important, SecureZIP offers the operational profile required by organizations to meet their Service Level Agreements (SLA) operationally while still ensuring that risk to the data is minimized to the greatest degree. The data protection offered by SecureZIP is supported by Application Integration that allows organizations to stream (for UNIX, Windows, & Linux servers) or protect record-by-record (mainframe) data from a database extract program directly into a protected SecureZIP archive. Since the data is never staged to disk in the clear, the risk for interception of unprotected sensitive data either internally or within the receiving data center is effectively eliminated.

Diagram 2-1 demonstrates the process of Application Integration – SecureZIP offers both a cost and operationally effective shared security strategy for the transfer of data between organizations. This ability to effect extraction, data protection, and transmission as parallel operations allows the addition of required data protection even within tight

Data Exchange with Application Integration

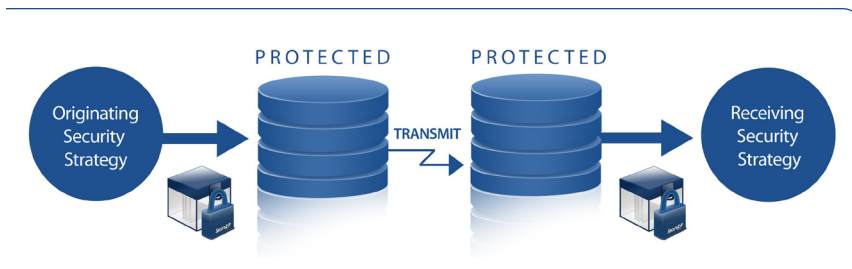


Diagram 2-1

operational batch windows.

This benefit is significantly enhanced by SecureZIP PartnerLink, a packaging of the product that allows a SecureZIP customer the right to distribute SecureZIP Partner licenses for any supported operating system to an unlimited number of partners for secure bi-directional data exchange with those partners.

Make an informed decision when planning for data protection

Effective and secure data management is critical to the success of modern business. The need for effectiveness encourages organizations to use centralized data management, aggregating large volumes of data in production and MIS databases. Since these databases frequently contain sensitive information (i.e. credit card data, Social Security numbers, health information, intellectual property, and other proprietary data elements) that should be protected, some organizations look to database encryption to mitigate their risks.

Advances in technology have made database encryption more feasible than in prior years. Database vendors have advanced to the point where encryption can be applied to the granular level of columns within a specific table of the database. In addition, some contemporary database engines accommodate queries being submitted against this encrypted data from both those who have the rights to the keys to decrypt the data and those who do not. While this extra layer of data protection will always be caught between the need for data security and that for operational performance, pursuing database encryption is now a feasible consideration.

When assessing risk from the perspective of financial or reputational impact rather than that of technology, database encryption by itself is insufficient to meet the needs of large organizations. In fact, in many cases, it does not protect the most significant risks organizations face.

While database encryption has become technically possible, it still comes at a high cost in terms of performance. Many of the business processes that typically use database technology, such as electronic payments, have high expectations of real-time performance. Many organizations elect to delay consideration of database encryption and focus instead on the greater risks of data-at-rest and data-in-motion. Assessing their areas of greatest risk, many of these organizations confidently point to their existing physical and logical perimeter protections and robust authorization/access controls as sufficient in protecting their data-in-use within the production databases. Therefore, they focus first on protecting their data-at-rest and data-in-motion using SecureZIP.

Summary

Database encryption strategies are used by some organizations to mitigate their risks of data-in-use with increasing effectiveness as that technology matures. However, database encryption does not mitigate the risks to data-in-motion or data-at-rest outside the database. Data-centric protection provides a necessary supplement to database encryption and, in some cases, may be the best place for an enterprise to apply data protection first. SecureZIP is a cross-platform application that is being adopted worldwide to provide data-centric security to protect sensitive data outside the database.