SecureAge

Databases, a hot spot for data leakage

- Close Your Security Gaps with a simple and complete solution

SecureAge Whitepaper 2021

Database security is paramount

With businesses becoming ever more data-driven and data-reliant, databases have become their default digital asset storehouse, providing immense benefits of organisation, retrievability, and analytical insight. Covid-19 and the move to remote or hybrid work have only intensified the demand for databases, particularly those distributed through cloud technology. But that concentration of information, however convenient, makes databases a singular target for attacks and a primary security concern.

According to Noel Yuhanna, a VP and Principal Analyst with Forrester Research and a specialist in big data and data warehousing, there has been a marked increase in the number of enquiries related to data security for databases and data warehouses over the course of the pandemic. He noted that 'many organisations have given data security the highest priority during the pandemic, especially those that deal with highly sensitive personally identifiable information, personal health data and compliance data'.[1]

Common misconceptions about database security

Databases are at the very centre of how companies of all size operate. And given that breaches of databases happen routinely, every business could be affected at some time. Debunking a few common misconceptions may save your business time, money, and reputation from data exposure. Here are a few of those false security beliefs:

1. My business is too small for anybody to bother hacking it

Research shows that small businesses have a false sense of security. A majority (66%) felt confident that their data and devices are secure and safe from hackers, with 77% responding that they haven't been hacked or attacked. This is undermined by digital forensic studies revealing that 72% of data breaches occur in companies with fewer than 100 employees.

Effectively, small businesses are not aware that they've been attacked and have lost data, especially since such data breaches at this scale rarely make headlines. See our SME whitepaper for more.

2. Our IT staff put database security at the forefront

These days, automation and push-button deployments are the new normal, with vendors offering database applications with standard factory settings. Those default configurations are in place as fast start and stopgap measures while IT Infrastructure Managers or Database Administrators learn how to properly setup and protect the data within. Most often, though, security is not a top priority: only an estimated 7% of database administrators spend any time at all on security, favouring instead data organisation, access, and performance.[2]

3. Databases aren't inherently secure, particularly cloud-based ones run by big operators

Although security features have become more robust within database applications, readily available commercial ones don't come with much security control enabled – passwords are usually simple and repeated default ones for both end-user and administrator accounts. Part of the attraction of cloud-based database deployments is getting the presumed security of those large and well-funded cloud operators. Reading their fine print, however, you'll find that security is a shared responsibility between the operators and the customer.[3]

Cloud operators are responsible for security of the cloud (eg: hardware, infrastructure and software), while customers are responsible for security in the cloud (eg: your data, platform, applications, Identity and Access Management, and operating systems).

1 Pandemic triggered data security movement to DBaas: https://searchdatamanagement.techtarget.com/feature/Pandemic-triggered-data-security-movement-to-DBaaS

2 4 Common Misconceptions about Small Business Data Security: https://www.whoa.com/4-common-misconceptions-about-small-business-data-security/

3 Shared responsibility model explained: https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

4. Database security is best handled by the administrators who specialise in it

Database administrators constantly need to look into backups, recovery, patching and software updates. Sometimes they have to leave some systems unpatched for a period of time due to incompatibilities with other systems, opening up possibilities for vulnerabilities and data breaches. Juggling the amount of data they need to manage and coupled with the mixture of new and legacy IT systems, database administrators are focused on keeping the lights on, rather than on the intricacies of protecting data in today's interconnected world. Unless given the proper tools, training, personnel, and incentives, database administrators may not be best suited for ensuring security.

Protecting your databases with file-level encryption

Most businesses store customer details, such as payment or personally identifiable information, or their own operational or financial records or intellectual property within databases. Any leakage of that data at any scale would be detrimental to the company's reputational, regulatory, and legal positions. Securing data at the most basic level, the file, with file-level encryption can be an effective solution that provides both security and regulatory compliance, if chosen and enabled correctly.

File-level encryption (FLE) protects your company's data

A Ponemon 2021 Global Encryption Trends Study observed a steady increase in enterprises adopting encryption strategies across their organisations. [4]These days, network perimeter security is no longer sufficient to protect businesses, as vulnerable employees and technical vulnerabilities exist within that presumably secure perimeter. Encrypting the data itself, at the file level, is often the best option. Doing so means that data remains protected even in the event of a data breach, whether by an external attack or an internal data leak.

FLE protects against internal and external threats

An effective data security strategy these days covers both internal risks and external attacks. If there is anything that 2020 has taught us, it's that adopting the Zero Trust approach to IT security has become essential. There were more attacks in the first half of 2020 alone than in all of 2019 combined.[5] A recent 2021 Data Exposure Report found that it is now 85% more likely for sensitive files to be leaked outside the company's control by internal employees than before Covid-19.[6]

By extending protection to the data itself, Zero Trust can finally be realized. With every data file demanding an assurance of access rights before revealing its contents, all information remains protected when files land in the wrong hands. SecureAge Security Suite for Database's File-level encryption protects every data file. If a database is breached by accident or intention, the entire data file remains encrypted, and external parties will not be able to make sense of the data. Furthermore, privileged internal users, such as database administrators, can still continue maintaining systems and performing backups without requiring or having access to the contents of the database. Public Key Infrastructure (PKI) technology inherent within each file makes this all possible.

FLE reduces misconfiguration risks from cloud-based deployments

The speed and ease of adopting cloud-based deployments make it a convenient choice. The potential for misconfiguration can also, however, lead to security vulnerabilities with broad-reaching consequences. According to Gartner, misconfiguration accounts for 99% of cloud security failures.[7] As a test, a group of researchers left open to the public internet a poorly configured database with only a couple of megabytes of meaningless data to learn who might

4 Ponemon 2021 Global Encryption Trends Study

5 https://www.darkreading.com/attacks-breaches/more-cyberattacks-in-the-first-half-of-2020-than-in-all-of-2019/d/d-id/1338926

6 https://beta.darkreading.com/vulnerabilities-threats/insider-data-leaks-a-growing-enterprise-threat

7 Shared responsibility model explained: https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

connect to it and what they would steal. Despite the lack of any value to it, the database was attacked roughly eight-and-a-half hours after deployment, with a total of 610 attacks in just under a month.[8]

Protecting data at the file-level and in real time ensures that all data remains secure whichever database it resides in.

FLE covers security gaps left by common database encryption approaches

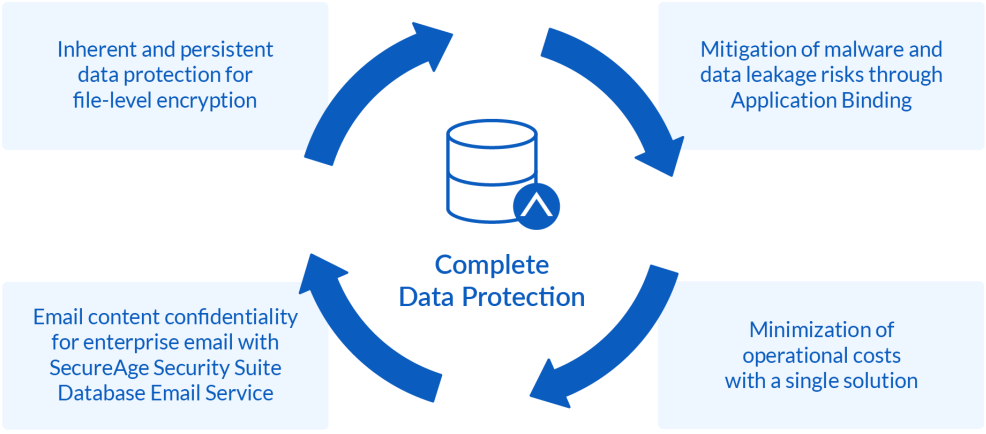
Most database encryption is deployed as Transparent Data Encryption (TDE), Column-level Encryption, or Tokenization. These methods can only protect structured data, leaving unstructured data unprotected and vulnerable. And data columns left plain offer enough information to deduce identification or cause material damage if exposed. In order to protect both structured and unstructured data, businesses have to incur additional investment costs to implement additional solutions.

SecureAge Security Suite for Database's File-level encryption is a scalable and extensible data protection approach to help enterprises minimise their data protection operational costs. Able to encrypt both structured and unstructured data, it can function as a solitary, all-in-one solution to secure any type of data (including temporary and log files) across heterogeneous databases and applications.

SecureAge Security Suite for Database – a complete solution

While there is a multitude of encryption solutions out there, they are not all created equal. SecureAge Security Suite for Database offers a unique approach to Data encryption through our SecureData technology. Advancing Public Key Infrastructure (PKI), SecureData invisibly employs asymmetric encryption to protect data by inextricably linking unique keys for each user and each file. SecureData technology proactively and persistently protects every file at all times, regardless of where it resides. With a commitment to usability as a critical line of defence, it is designed to inherently protect data without forcing users to change the way they work. To find out more about our technology, check this link out.

SecureAge Security Suite for Database is a complete solution that helps organisations protect their data in use, in transit, and while at rest through these features:



8 Misconfigured Databases Targeted Hours After Deployment: https://www.darkreading.com/cloud/misconfigured-databases-targeted-hours-after-deployment/d/d-id/1338052

Inherent and persistent data protection for file-level encryption

Rather than deciding which data is sensitive and worthy of protection, SecureAge Security Suite for Database recognizes that every file is sensitive, protecting all data automatically and without any change in user workflows. It protects the entire database, securing all forms of data organized within, both structured and unstructured, including any reports or data downloads extracted from the database. As the encryption process is transparent to databases and applications, everything remains accessible to authenticated users while encrypted, ensuring that query results are available in real time and that changes to the data are incremented as they happen.

Mitigation of malware and data leakage risks through Application Binding

SecureAge Security Suite for Database's application binding feature allows users to specify rules that bind specific database files only to specific applications. This prevents any other compromised application from accessing the database. In effect, any malware that infiltrates a company's server will be unable to access the randomised content of the encrypted data without the right key and proper authorisation. Similarly, it also means that system administrators themselves will not be able to access sensitive information within databases when performing maintenance or backups.

Minimization of operational costs with a single solution

Noted above, not all database encryption solutions are created equally. Though Transparent Data Encryption and Column Level Encryption are the most commonly used solutions, they can only protect certain tokenized fields or columns within structured data, leaving plain columns and unstructured data files entirely vulnerable. Moreover, proprietary encryption tools from database vendors incur additional costs to implement and maintain. Of course, additional solutions to plug those database security gaps have a cost of their own. SecureAge Security Suite for Database uses file-encryption to protect all data types, whether structured or unstructured. This single, complete solution helps businesses minimise operational costs while meeting their evolving security requirements across heterogeneous databases and applications.

Email content confidentiality for enterprise email with SecureAge Security Suite Database Email Service

Companies routinely send transactional emails such as billing information, bank account statements or insurance contract documents to their customers. These emails and attachments inevitably contain personally identifiable information that requires encryption to ensure they are viewed by the intended recipient only. SecureAge Security Suite Database Email Service provides secure end-to-end email encryption of both the email contents and any attachments. Decryption requires the recipient to input a uniquely generated password that is provided to them after a simple email verification process to ensure user authenticity.

Security Suite for Database adopted as a single solution to secure government databases

> A government agency in Southeast Asia was looking for a single solution to protect all of its data stored in an Elasticsearch database. It wanted to prevent data leakage from internal threats (IT and database administrators) while also preventing any leakage during backups. Using SecureAge Security Suite for Databases' unique approach to file-level encryption, the agency was able to persistently and completely protect all of the data regardless of user or storage location, wiping out any 'whack-a-mole' maintenance complexities. With SecureAge Security Suite for Databases' PKI technology, it was also able to ensure that any duplication of plain, unencrypted data would require authorisation from the creator of the data, minimising data leakage possibilities.

Close your security gaps

System and data security is rightly approached by deploying multiple levels of protection. But it must be recognised that there will always be gaps in and between security layers, leading to the inescapable conclusion that it is simply not possible to keep the 'bad guys' out 100% of the time.

By implementing file-level encryption using SecureData technology, protection is built into the data itself. Extending this approach with SecureAge Security Suite for Databases delivers peace of mind over data leakages and theft. This solution provides protection against data breach while making no changes to the way people, applications or databases work.

Stay safe, Stay data safe.

To find out more about our SecureData encryption technology visit here.

To find out more about our Security Suite for Databases solution visit here.

To talk to us, see a demo, or discuss partnership opportunities, reach out to us directly at protect@secureage.com.

Frequently Asked Questions

Who is SecureAge?

SecureAge Technology is a data security company headquartered in Singapore with a record of protecting government and enterprise data from the most advanced and persistent cyber threats since 2003. SecureAge's government clients include the Monetary Authority of Singapore, all Singapore Ministries and Statutory Boards, the Singapore Military and the Government of Japan. Commercial clients include NTT, Narita Airport, Sony, British American Tobacco, Temasek Holdings, the Government Savings Bank of Thailand, and GRG Banking.

Why has no-one offered this before?

Early encryption technologies have been disruptive for users and applications, leading to approaches where users were forced to select only those categories of data that were felt to need strong protection. Encryption has been seen as difficult. In light of this, 'full disk encryption' has been deployed widely because it implements data encryption without impacting users, applications or servers. This has allowed organisations to check the 'data encryption' box. The problem is that full disk encryption only protects a machine that is switched off, and encryption only applies to disk drives where encryption is enabled. Data copied to another drive is no longer secure.

SecureAge's next generation product implements data encryption properly so that information remains encrypted while the system is running and even while data is being modified. It is the data that is important, so with SecureAge, information protection and authentication is an inherent part of the data. By operating at the file system level, SecureAge transparently supports all applications, databases, and services so that no user or app has to change the way they work at all.

What impact does SecureAge have on performance?

SecureAge employs specialist encryption functions on the CPU so that normal data processing does not have to wait for cryptographic operations. In addition, only the portion of data that needs to be in system memory gets decrypted, leaving the file on disk encrypted at all times. This 'streaming' of the data through the SecureAge encryption engine combined with hardware cryptographic functions means that the user perceives no impact on performance.

Which file types, formats and databases does SecureAge support?

Because SecureAge works at the file system level, all file types, data stores, and all databases are supported without impact on applications. No software changes are required. Data security and authentication is built into each file so that it can be read and modified without having to decrypt the entire file before use.

Can I search file contents which have been encrypted by SecureAge?

Yes, the contents of all files, such as Microsoft Word, Excel, and PowerPoint or Adobe PDF are still accessible to searches by users who are authorised to access the data.

How comprehensive is Security Suite for Database as a data protection solution?

Security Suite for Database can work as a sole, all-in-one solution to secure both structured and unstructured data of any type, across heterogeneous databases and applications. This scalable and complete data protection approach minimises data protection operational costs from having to keep and maintain multiple solutions.

How does Security Suite for Database help with regulatory compliance?

Global privacy regulations require businesses to ensure a level of security on stored data. Security Suite for Databases protects all data through encryption, mitigating risks associated with data transfer or cyberattacks. Even if an attack happens and data is leaked, these businesses will not have breached these regulations since the data breached is unintelligible without the decryption key.

It helps organisations to comply with and avoid a data breach for the following regulations:

a. Payment Card Industry Data Security Standard (PCI DSS)
b. Data Privacy Bill (e.g. GDPR, CCPA)
c. Protection of Sensitive Agency Info (White House OMB)
d. Health Insurance Portability & Accountability Act (HIPAA)
e. Gramm-Leach-Bliley Act (GLBA)
f. Sarbanes-Oxley (SOX)
g. Monetary Authority of Singapore Technology Risk Management (TRM)

Will there be visibility of data access?

Security Suite for Database provides a complete data access audit log to continuously monitor data access. The audit trail provides detailed information of database accessed by application, moving of information to external devices, and blocked operations.

Does Security Suite for Database allow for two-factor authentication options?

Yes, Security Suite for Databases provides optional two-factor authentication with Smart Card, USB Token, or HSMs. Its two-factor authentication support enables users' public and private keys to be stored on any PKCS#11-compliant smart card, USB token, or HSM. This provides organisations with stronger two-factor protection.

Can malware risks be mitigated with Security Suite for Database solution?

Security Suite for Database solution comes with an extended feature, Application Binding, that allows users to specify rules that bind specific databases to specific applications only. This helps to prevent any other application from accessing the database.

Can I implement higher levels of security in some areas?

All information encrypted by SecureAge is protected by modern, standard cryptographic algorithms which provide the highest data security. However, the level of security for authentication can be chosen to meet differing security requirements. For example, staff with access to 'highly sensitive' information may be required to use smartcards with multi-factor authentication to protect their decryption keys, while other individuals may use 'soft' tokens and password authentication for key storage.

Do I need to deploy SecureAge in one 'Big Bang'?

No. SecureAge can be implemented in a phased fashion at a pace that is convenient for you. Individuals, groups, departments, or divisions can install the product to enhance their data security without impacting the way they work or interact with others in the organisation.

What should I do next?

With information being accessed from uncontrolled environments, the growth in both quantity and sophistication of cyberattacks, and the threat of insider data theft, the status quo must now be questioned. 100% data encryption is already a principle that you accept – full disk encryption fulfils this. But this principle must be implemented better, so that when a file on a running system is copied from one silo to another location, it remains encrypted. Furthermore, authentication should be built into the encrypted file so that only authorised individuals – not the 'bad guys' – can decrypt the data.

SecureAge Technology

Placing real security and usability on equal footing, SecureAge Technology is a data security company headquartered in Singapore. SecureData was first launched in 2003 for the Singapore government, based on a refinement of PKI security techniques. SecureAge made its patented PKI-based encryption an inherent and invisible component of data protection, soon becoming the preferred data encryption partner for additional government and public entities. These long-term and deeply integrated relationships have provided SecureAge with extensive experience of securing the data of large and complex organisations.

SecureAge data security solutions provide public and private entities complete control over data movement within their networks. Every File, Every Place, and Every Time.

Security products from SecureAge have been selected by organisations that need the highest levels of data protection. Customers include various agencies in the Singapore, Hong Kong and Japanese governments; British American Tobacco; Sony; Narita Airport Technologies; the Government Savings Bank in Thailand and GRG Banking.

SecureAge Technology: our approach to data security

Proactive protection, which is:

Data security

Data security means pervasive encryption. Data should be secured at the most basic, self-contained unit: the file. Competitive solutions only protect some of the data some of the time, focus on compliance rather than security, or add complexity that introduces risk. Perimeter defences are insufficient as users (the most vulnerable segment of any system) are already inside.

Application integrity

Application integrity means control through 'allow listing' and binding of data to applications. Only authorised processes should access specific data for specific purposes. Traditional anti-malware systems represent passive protection, which is too late. They focus on previously known malware and attempts to stop malicious processes that are already active.

Usability

Usability means inherent and invisible technology. Solutions should remove the human element entirely rather than try to account for or change it. Training and monitoring don't work all of the time, and if the solution is not natural, people will create their own (non-secure) methods. Users should be able to work just as they want or need to without additional considerations.

No trade-offs

In SecureAge there are no trade-offs between these principles, and especially, usability is not sacrificed to strengthen data security. Recognising that individuals will find other ways of achieving something if the 'proper' way is difficult is a fundamental principle of SecureAge product design.

Find out more

To see more of our whitepapers click HERE. Please get in touch to find out more about SecureAge's enterprise data security solutions. We're happy to discuss the ways in which SecureAge can improve your data security and arrange a free trial: protect@secureage.com.

Website www.secureage.com
Contact protect@secureage.com

SecureAge

Singapore 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
United Kingdom 74 Mackie Avenue, Brighton, BNI 8RB, Company No. 11734665
Japan 1-16-6, Toranomon, Minato-ku, Tokyo 105-0001, Japan
North America 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA