Mitigating A Catastrophic Data Breach & Eliminating Data Breach Vectors With DataBath

White Paper by Kwikdesk

2016 Edition

CONTENTS

INTRODUCTION

A data breach can be catastrophic for a company or institution. It can result in the loss of customer/client trust and substantial financial loss. It is estimated that more than 75% of data breaches are internal. This percentage might seem high at first glance, but when you combine malicious activity from within a company (disgruntled employee), compromised employee credentials (phishing or man-in-the-middle attacks) and the accidental compromise (lost computer), it becomes clear that this is a massive problem that needs addressing.

MITIGATING BREACH VECTORS

The most effective way to thwart data breaches is by mitigating or altogether eliminating breach vectors. Standard security measures commonly used today offer a level of protection, but more often than not they introduce additional attack vectors that can lead to a catastrophic data breach. An insider threat is the most likely vector of attack that can undo all efforts of data security, and special measures are required to effectively mitigate and combat against it.

THE ENCRYPTION DILEMMA

If you have any experience with data security, you're already familiar with encryption. Data encryption is the most common method of keeping sensitive information secure, and thousands of companies rely on encryption to protect sensitive data. However, encryption brings with it vulnerabilities caused by the key that is the core part to its cryptographic operations. A common internal breach vector is to steal encryption keys, and once the keys are captured then decrypting the sensitive data is trivial.

THE DATABATH SOLUTION

DataBath is an innovative security solution developed to effectively stop potentially catastrophic internal data breaches. In order to achieve this goal, DataBath provides a security service that replaces sensitive data with tokens that hold no value if stolen. A token is a placeholder, with no inherent value.

The sensitive data is never stored, neither by DataBath or by the company that owns the data.

Where did the sensitive data go?

You might well be wondering how can the sensitive data be retrieved if it is never stored. DataBath's unique token exchange process is reciprocal in nature, allowing the exchange of sensitive data with tokens (and vice-versa) to work in both directions. Only the storage of tokens is required, and tokens can only ever be exchanged for their data counterparts through Databath's secure platform.

How is DataBath different from encryption?

It is important to be aware that, unlike encryption, DataBath's token exchange process is dependent on a substitution function that is based on a secure set of randomized token clusters, and not on a cryptographic algorithm. Therefore, DataBath's solution is not at risk from potential cryptography vulnerabilities.

DATABATH & ENCRYPTION MAKE FOR THE BEST DEFENSE

The most effective strategy in data security is defense in depth. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.

DataBath can be used as a vital complement to existing data security efforts that protect their sensitive data through encryption. Whilst encryption protects the data itself, DataBath goes a step further and protects the encryption keys by swapping them out with tokens.

DATABATH TOKEN EXCHANGE

DataBath uses a secure token exchange process that is dependent on a small set of randomized token clusters. DataBath is a multi-tenant platform, therefore a unique set of token clusters is generated for each tenant.

Each token cluster is generated at runtime using the Mersenne Twister pseudorandom number generator, and are only held in memory. A pseudorandom number generator (PRNG) has deterministic qualities whereby the generated random values are determined by a set of initial values, called the PRNG's seed. DataBath uses a combination of encryption and its own security solution to protect PRNG seeds. What's good for the goose is good for the gander.

The figure above highlights how the data “travels” through the small set of randomized token clusters and is iteratively substituted with random values until it finally becomes a token that can safely be stored. The reverse phase can be seen as a mirror function, whereby a token is exchanged with its data counterpart.

DATABATH DESIGN GOALS

DataBath has been designed from the ground up to meet the following requirements:

Internal data breach protection Implementing DataBath's security measures and its secure token exchange safeguards from data breaches that originate from insider attack vectors.

Secure platform Data traveling to and from DataBath is encrypted using HTTPS/TLS (Transport Layer Security). Secure access to the Databath API is achieved using API keys in the form of JSON web tokens. Using JSON web tokens instead of traditional API keys offers many advantages. The DataBath dashboard uses the strongest authentication and authorization practices, including mandatory multi-factor authentication.

Token exchange throttling To further mitigate against a data breach, DataBath gives the option to throttle access to its service according to business needs. Throttling introduces API rate limiting that enforces a threshold on how many tokens can be exchanged in a given time period. Additionally a second security measure can be activated that requires a token exchange to be approved within the DataBath dashboard before the exchange is allowed to take place. The second security measure can be mandatorily enforced or triggered once a rate limit threshold has been reached.

Easy development DataBath abstracts away the complexity of integration through a simple API that has only two, albeit very important, endpoints. DataBath's client SDKs help to speed up the integration phase even further.

High availability The components of the DataBath platform have been designed to be highly redundant. This redundancy applies to our servers, network, and the service itself.

High throughput and performance DataBath's unique in-memory token exchange process takes mere milliseconds to complete, therefore performance is tied only to network performance. The DataBath platform has been designed to horizontally scale and deliver on the required throughput.

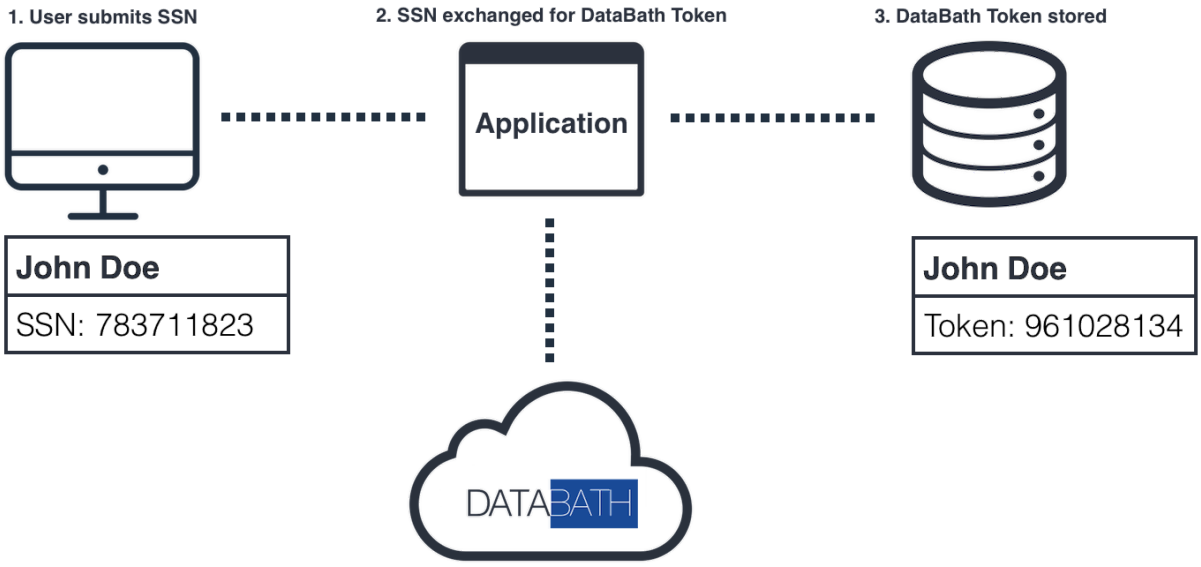
USE CASES

This white paper presents two use cases. The first demonstrates how DataBath protects Social Security Numbers by replacing them with 9 digit tokens. The second showcases how DataBath works alongside an encryption and Key Management solution to protect images and documents.

Protecting Social Security Numbers

Consider the challenge of securing Social Security Numbers. There have been thousands of Social Security Numbers that have already been compromised. When a hacker steals a person's Social Security Number, the consequences can be disastrous for the person involved.

The DataBath solution is a simple yet effective approach in combating identity theft. As Social Security Numbers are ingested, a call to the Databath platform returns a replacement 9 digit token that can be safely stored. Personnel can exchange the 9 digit token for its counterpart Social Security Number whenever the business need arises, as long as they have passed the authorization and throttling requirements imposed by DataBath.



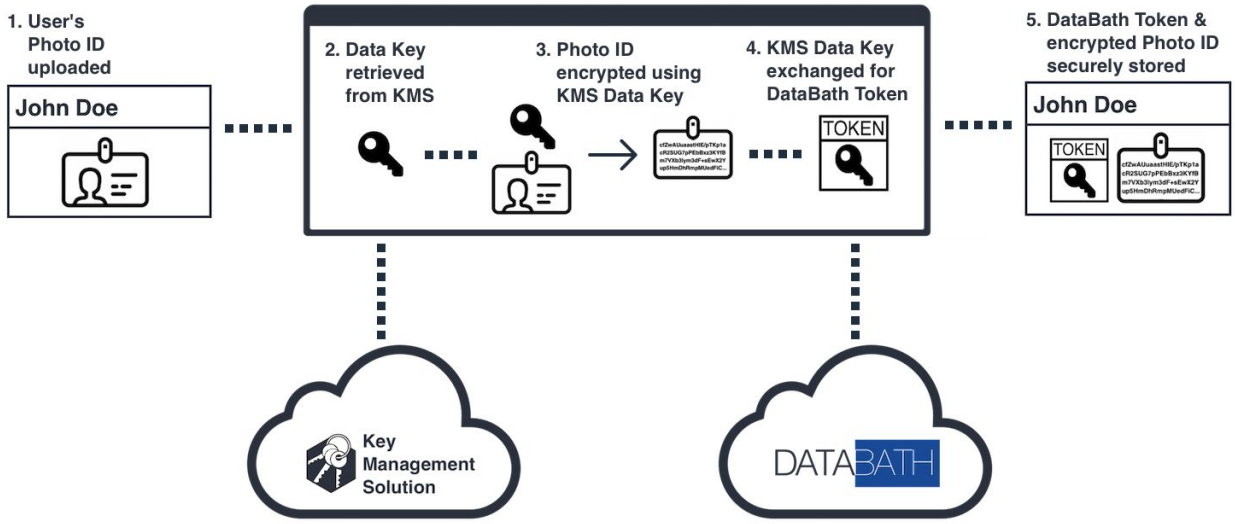
Protecting Images and Documents

Personal data documents like passports and driving licences are often required as proof of identity, and are therefore stored as images or documents for future validation. A good approach to securing these sensitive documents is ensuring that they are always encrypted when at rest. But is encryption enough? In the event of the encryption keys being stolen, it is only a matter of time when the data breach becomes catastrophic. Key Management Solutions (KMS) do a good job of easing the burden of securing and managing encryption keys, but even this strategy is at risk of internal breach vectors.

In this scenario, Databath becomes the security barrier between potential attackers and the encryption keys they look to steal:

1. Firstly, a user uploads their sensitive document to a secure environment.
2. A call to the KMS returns an encrypted data key and a plaintext version of the data key.
3. The sensitive document is encrypted using the plaintext version of the data key.
4. A call to DataBath exchanges the encrypted data key for a token.
5. The encrypted document and the DataBath token are safely stored.

Traditionally, in step 5 the encrypted data key would be stored alongside the encrypted document but that opens the door to a KMS vulnerability. Once an internal attack has access to the KMS or its master key, then it's an easy path to decrypting the sensitive document. Using DataBath though, the attack is blocked as the token has no direct link to the encrypted document and can not be used to unlock it.



CONCLUSION

DataBath provides strong security measures to effectively stop internal data breaches that are likely to ruin a business's profits and reputation. With DataBath's token exchange process, there is finally a primary defense against internal attack vectors that can circumvent the most hardened of security strategies. DataBath's security reach extends into safeguarding sensitive documents, such as passports and driving licences, by protecting the keys used to encrypt them. The DataBath solution is highly scalable, secure and meets strict service level agreements.

DATABATH

For more information:

Email sales@databath.com

Visit www.databath.com

Copyright © 2016 Kwikdesk. All rights reserved.