ACCUTIVE SECURITY

Accutive Data Discovery + Masking

Test Data Management Platform

Overview of Data Encryption, Tokenization, and Masking, including Post-Quantum Implications

Understanding the differences between data encryption, tokenization, and masking can be daunting. As a center of excellence, client education is a cornerstone of our approach. This whitepaper provides an in-depth analysis of data encryption, tokenization, and masking concepts and techniques. **With the imminent need for post-quantum cryptography, we have also outlined how quantum computing will impact each method.** We will explore their similarities, differences, and respective benefits in ensuring data protection. Furthermore, we will discuss compliance considerations and demonstrate how you can combine of leading cybersecurity solutions to construct a robust framework that provides robust protection for your critical data, at both the database and file-level.

Contents

Introduction

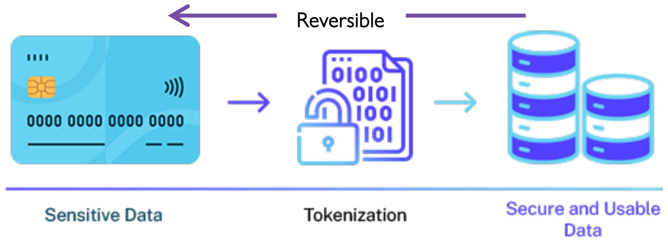
With the increasing volume and value of data in the digital age, your organization faces a significant challenge in safeguarding your sensitive information from unauthorized access. Data encryption, tokenization, and masking serve as three prominent methods to protect data, each with distinct characteristics. Understanding their similarities, differences, and benefits is crucial in designing a robust data protection strategy for your organization.

Data Encryption

Data encryption involves transforming plaintext into cipher text, making it unreadable to unauthorized individuals. This process typically employs encryption algorithms and cryptographic keys to secure data at rest, or in transit. At Accutive Security, our focus is on data-at-rest encryption. Encryption provides a high level of security, and it is a reversible process, thereby allowing authorized users to decrypt and access the data. This makes encryption well-suited for scenarios where authorized parties need to access and manipulate the data. Effective encryption must be sufficiently strong to deter unauthorized access, ensuring that only those with the necessary permissions can decode the data.

How is encryption impacted by quantum computing?

Quantum computing poses a significant threat to current encryption methods, as it has the potential to break widely used cryptographic algorithms, such as RSA and ECC, in a fraction of the time it would take conventional computers. This advancement necessitates the development of quantum-resistant encryption algorithms to safeguard data against future quantum-based attacks.



Tokenization

Tokenization substitutes sensitive data with unique identifiers, or tokens, maintaining referential integrity without revealing the data itself. Unlike encryption, which obscures data with a reversible algorithm, or masking, which partially hides data, tokenization completely detaches the original data from its operational use, storing it securely away from the tokens. Data tokenization is particularly effective in environments requiring data processing without exposing sensitive information, offering a distinct security advantage by isolating the actual data from the operational environment. This reduces the risk of data breaches.

How is tokenization impacted by quantum computing?

Data tokenization **is inherently less impacted by quantum computing than traditional encryption methods** because its security does not rely on computationally difficult mathematical problems that quantum computers can solve.

Masking

Masking modifies sensitive data by replacing or obscuring parts of it, preserving its format and length but preventing the original values from being discerned or reversed, ideal for non-production environments like development, testing, or analytics. Unlike tokenization, which swaps sensitive data for non-sensitive placeholders, or encryption, which secures data with a reversible algorithm, masking offers a non-reversible way to anonymize data.

How is data masking impacted by quantum computing?

Data masking is not directly impacted by quantum computing, as it relies on data obfuscation.

Comparing data encryption, tokenization, and masking

Data encryption, tokenization, and masking are all methods of data protection, each with distinct approaches and functionalities:

- **Encryption transforms data it into a secure format that can only be accessed with a decryption key**, allowing for a reversible process. It's widely used to protect data in transit or at rest from unauthorized access, ensuring that only those with the key can revert to the original data.
- **Tokenization substitutes sensitive data with non-sensitive placeholders or tokens**, which can be used in operational processes without exposing the actual data. These tokens retain the data's referential integrity, meaning they can be mapped back to the original data stored securely, typically in a token vault. This method is beneficial for transactions and data processing where actual data exposure is unnecessary.
- **Masking involves altering sensitive data irreversibly to hide its original content**, usually for use in non-production environments like testing or development. It maintains the data's format and appearance but prevents the actual information from being recovered or identified, providing a way to work with realistic data sets without compromising privacy.

While all three methods aim to protect sensitive information from unauthorized access, they each offer different levels of security and functionality suitable for various use cases, from secure data storage and transfer (encryption) to safe data handling in operational environments (tokenization) and privacy protection in development or testing scenarios (masking).

Masking in a Post-Quantum World

The advent of quantum computing brings both advancements and challenges, particularly in the realm of data protection. Among the three featured data security techniques—encryption, tokenization, and masking—masking is inherently less vulnerable to quantum threats, presenting a robust solution for safeguarding sensitive information in a post-quantum world.

Quantum Resilience: Unlike encryption and, to a lesser extent, tokenization, which rely on cryptographic algorithms potentially susceptible to quantum computing's vast processing power, masking stands apart. It does not encrypt data but rather alters it in a way that the original information cannot be recovered or deduced. This non-reliance on breakable algorithms positions masking as a future-proof technique against the quantum threat, ensuring that data remains secure even as quantum computing advances.

Compliance and Scope Reduction: Masking directly contributes to reducing the compliance scope for organizations by irreversibly anonymizing data, thereby minimizing the amount of data subject to stringent regulatory requirements. For instance, in environments governed by regulations such as GDPR, PCI DSS, or HIPAA, properly masked data may not be considered personal or sensitive anymore, easing compliance burdens. This reduction in compliance scope is a significant advantage, allowing organizations to focus their security resources more efficiently.

Irreversible Anonymization: The one-way nature of masking is perhaps its most critical feature. By irreversibly anonymizing data, masking ensures that sensitive information cannot be reconstructed or re-identified, even if the masked data falls into the wrong hands. This characteristic is especially valuable in non-production environments like development and testing, where the use of real data can pose a risk to privacy and security. Masking enables the use of realistic data sets without exposing actual sensitive information, facilitating development and testing processes without compromising security.

As we navigate the uncertainties of a post-quantum world, the role of masking in data protection becomes increasingly vital. Its inherent resistance to quantum decryption, ability to reduce regulatory compliance scope, and provision of a one-way algorithm for irreversible data anonymization mark it as a crucial strategy in the arsenal against emerging cyber threats. Masking offers a pragmatic and forward-looking approach to data privacy and security, ensuring you can safeguard your data assets against the quantum computing horizon.

Accutive Data Discovery + Data Masking (ADM)

The Accutive Data Discovery + Data Masking (ADM) test data management platform enhances your data security and compliance by enabling the discovery and masking of sensitive data across all major databases and file types. ADM offers advanced features like AI-powered configuration for optimal masking, high-speed data processing, and out of the box compliance with prominent regulatory requirements, such as PCI, GDPR, HIPAA, CCPA and more. ADM supports seamless integration with various data sources, ensuring data remains functional yet anonymized, and it provides customizable algorithms for precise data handling. This comprehensive approach not only reduces your risk of data breaches but also empowers efficient development and testing processes for your DevOps teams by unlocking secure production-like data.

ADM Features: Data Discovery + Masking

Data Masking: Rapid, consistent masking across multiple databases and data sources, including advanced functionality such as derived multi-field masking, programmable masking, and smart address masking with proximal address generation.

Data Discovery: Automated data discovery that aligns with major compliance standards and is easily customizable to your organization's specific data discovery and auditing requirements – regardless of how obscure, complex or specific.

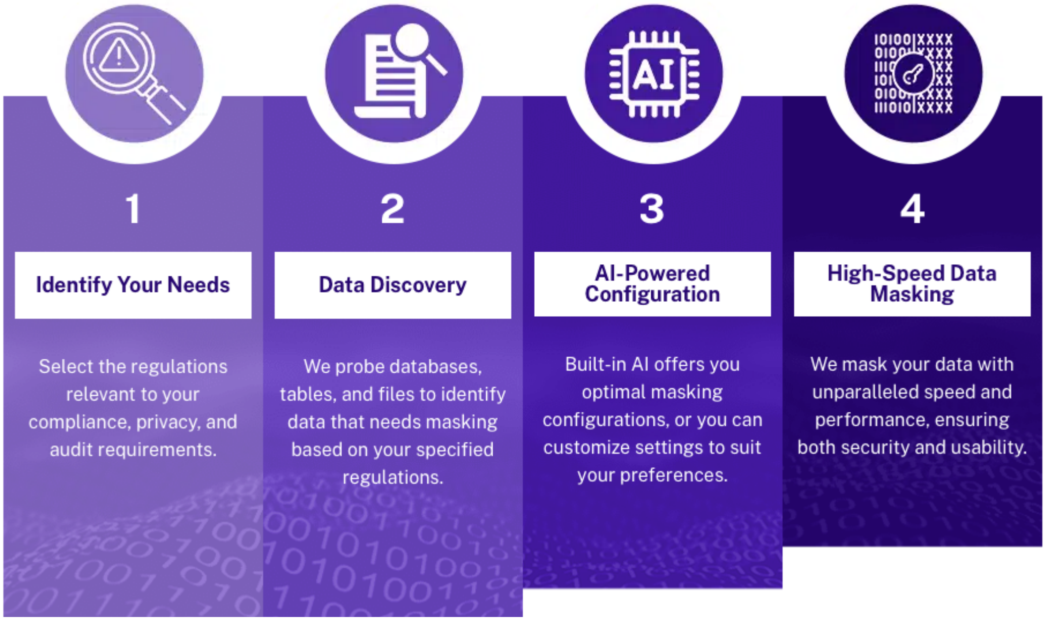
ADM Features: Beyond Masking

Data Automation: Seamless integration of data discovery, subsetting and masking into your CI/CD pipeline with AI-powered, API-driven data automation capabilities.

Data Subsetting: Efficient extraction of accurate and inclusive data subsets customized to your needs.

Data Tokenization: Advanced reversible data shielding that protects while preserving referential integrity.

Robust Test Data Management in 4 Easy Steps:



1 **Identify Your Needs**

Select the regulations relevant to your compliance, privacy, and audit requirements.

2 **Data Discovery**

We probe databases, tables, and files to identify data that needs masking based on your specified regulations.

3 **AI-Powered Configuration**

Built-in AI offers you optimal masking configurations, or you can customize settings to suit your preferences.

4 **High-Speed Data Masking**

We mask your data with unparalleled speed and performance, ensuring both security and usability.

Get Started

Data encryption, tokenization, and masking are powerful techniques for protecting sensitive data. At Accutive Security, we offer powerful solutions in all three forms of data protection. While encryption and tokenization provide secure access and storage, masking offers unique benefits such as one-way algorithms and anonymization. Additionally, compliance considerations are essential when designing data protection strategies, and Accutive Security's products and services, coupled with their expertise in authentication and cryptography, will effectively address your database and file-level data protection needs. By leveraging these techniques and solutions, your organization can safeguard your sensitive data and mitigate the risk of data breaches and compliance violations.

ADM provides data discovery, subsetting, masking, automation and tokenization solutions to suit your organization's needs in three tiers ranging from Starter (discovery and masking with basic support) to Professional (automated discovery + masking with advanced functionality) and Enterprise (data discovery, masking, subsetting, automation and tokenization with a full suite of enterprise-grade functions and 24/7 support). Additionally, Accutive Security partners with leading quantum-ready cryptography firms to offer advanced data-at-rest encryption solutions.

Email letstalk@accutive.com to unlock complimentary access to the Starter level of our ADM Platform.

CONTACT INFORMATION

27068 La Paz Road, Suite 245 Aliso Viejo,
CA 92656

Toll Free 888.666.8315

letstalk@accutive.com

Contact Us

www.accutivesecurity.com

Accutive Security provides comprehensive information technology solutions which include enterprise security; IT application development; systems integration; lending platform Services; and professional services to clients in industries ranging from financial services, healthcare, technology, entertainment, and retail. Accutive is a specialized team of experienced professionals with years of industry, business, and IT expertise dedicated to developing IT solutions that exceed our clients' expectations.