VORMETRIC VAULTLESS TOKENIZATION WITH DYNAMIC DATA MASKING

Efficiently De-Identifying Sensitive Data and Reducing PCI DSS Audit Scope
# TABLE OF CONTENTS:

**THE CHALLENGE: SO MANY SECURITY DEMANDS, SO LITTLE TIME** ......................... 3

**THE SOLUTION: EFFICIENTLY DE-IDENTIFY SENSITIVE DATA** ................................. 4
    How Vaultless Tokenization Works ............................................................... 4

**DELIVER ROBUST DATA SECURITY** ................................................................. 4
    Strong Access Controls .............................................................................. 4
    Flexible Tokenization with Dynamic Data Masking ........................................ 5
    Deployment and Administrative Efficiency .................................................... 6
    Efficient Scalability and Agility .................................................................. 6

**KEY BENEFITS** ......................................................................................... 7

**SAMPLE IMPLEMENTATIONS** ...................................................................... 7
    PCI DSS 3.0 Compliance ............................................................................ 7
    Customer Contact Centers ......................................................................... 7
    Outsourced Development .......................................................................... 8
    Big Data .................................................................................................... 8
    Cloud Services .......................................................................................... 8
    Static Data Masking .................................................................................. 8
For too many IT organizations, complying with the Payment Card Industry Data Security Standard (PCI DSS) and corporate security policies has been far too costly, complex, and time consuming. Now, Vormetric offers a better way: Vormetric Vaultless Tokenization with Dynamic Data Masking. The solution’s vaultless tokenization capabilities enable your security team to address its compliance objectives, while gaining breakthroughs in operational efficiency. With this solution, you can remove sensitive data like personally identifiable information (PII) and payment data from databases—and do so with minimal disruption and administrative overhead. With the solution, you can remove databases from PCI DSS scope, and so significantly reduce your compliance costs and efforts. Vormetric Vaultless Tokenization is part of the Vormetric Data Security Platform, which delivers a comprehensive range of security and compliance controls that help IT teams efficiently address their requirements for encryption, privileged user access control, file access auditing, and more.

THE CHALLENGE: SO MANY SECURITY DEMANDS, SO LITTLE TIME

For today’s security teams, it seems virtually everything is proliferating:

- **Threats.** Risks posed by nation-states, cyber criminals, and malicious insiders continue to grow more sophisticated and more persistent.

- **Data and repositories.** The volume and diversity of assets and repositories that need to be protected continues to see explosive growth. Instead of just managing the traditional data center, which was challenging enough, there are now virtualized systems, big data environments, outsourced services, private clouds, public clouds, and hybrid models to contend with.

- **Mandates and tools.** As the number of repositories continues to grow, so do the number of systems that fall within the scope of PCI DSS and other regulations. Further, the scope and complexity of these regulatory mandates also continues to expand. As a result, security teams are compelled to deploy more safeguards and tools in order to establish the controls these mandates require. In particular, security teams face increased pressures to prepare for PCI DSS 3.0 audits, and adapt their security approaches as cardholder data moves into new environments—such as cloud and big data implementations—and is shared with outsourced service providers, such as analytics, development, and engineering firms.

All this proliferation continues to place increasing demands on security teams—but these teams don’t see their time, staffing, or budgets undergoing any commensurate expansion. To contend with these realities, many security professionals have explored the use of tokenization, which has the potential to provide a convenient way to protect sensitive assets. At a high level, tokenization is the process of replacing a sensitive record with a token, effectively a meaningless placeholder for the data that can’t be exploited or reverted back to its original form.

While tokenization offers the potential to address a wide range of security and compliance objectives, traditional tokenization tools and solutions have been far too costly and complex to procure and manage. These tools typically require security teams to invest in expensive appliances and contend with software agents that are difficult to deploy and manage. More than ever, security teams need to be able to leverage the benefits of tokenization—and they need to do so in a scalable, efficient, and cost effective manner.
THE SOLUTION: EFFICIENTLY DE-IDENTIFY SENSITIVE DATA

The Vormetric Data Security Platform offers tokenization capabilities that can dramatically reduce the costs and effort associated with complying with security policies and PCI DSS. With Vormetric Vaultless Tokenization with Dynamic Data Masking, your organization can efficiently address its objectives for securing sensitive assets and cardholder records—whether they reside in the data center, big data environments, or the cloud.

HOW VAULTLESS TOKENIZATION WORKS

For illustration purposes, we’ll outline the process of tokenizing a credit card number:

1. The customer submits a credit card number into an application.
2. The application submits the credit card number to the Vormetric Token Server via the REST API.
3. The key associated with the token is retrieved from the Vormetric Data Security Manager appliance and subsequently cached on the Vormetric Token Server. Through format-preserving encryption (FPE), the credit card number is converted (tokenized) into a token.
4. Through the REST API, the Vormetric Token Server returns the token to the application.
5. The application server then submits the tokenized value into the database.

DELIVER ROBUST DATA SECURITY

STRONG ACCESS CONTROLS

Vormetric supports and recommends creating at least two user accounts on the tokenization server: one with the permission to tokenize but not to detokenize, and another with the permission to detokenize. The user account with tokenization privileges would be utilized by multiple servers, including a public-facing web server, for example.
On the other hand, the user account with detokenization privileges would be limited to a specific server that needs these permissions. For example, detokenization privileges could be restricted to a server that’s responsible for submitting credit card numbers to a remote card processing service. IT teams should ensure only the minimum number of administrators can access accounts with detokenization privileges.

With Vormetric Vaultless Tokenization, administrators can create a strong separation of duties between privileged administrators and data owners. In this way, IT staff—such as hypervisor, cloud, storage, and system administrators—can perform their system administration tasks, without being able to gain access to the sensitive data residing on those systems. Further, Vormetric offers a high availability, standards-based, FIPS 140-2 and Common Criteria validated platform that can provide maximum security for cryptographic keys and policies.

**FLEXIBLE TOKENIZATION WITH DYNAMIC DATA MASKING**

Vormetric Vaultless Tokenization offers the flexibility to establish varying levels of data redaction. Administrators can establish settings to have an entire field tokenized or to do dynamic data masking so part of a field remains in the original clear-text.

You can integrate Vormetric Vaultless Tokenization with your existing Active Directory (AD) and Lightweight Directory Access Protocol (LDAP)-based identity directories, so your security teams can efficiently set granular policies for specific users and groups. For example, a user with customer service representative credentials can obtain a credit card number with the last four digits visible for customer identification purposes, while a customer service supervisor may be able to access the full credit card number in the clear.

The process of setting these policies is done using an intuitive administrative interface. Through the interface, administrators can choose exactly how they want data to be redacted, including specifying whether to replace a value with such characters as a pound sign, asterisk, or hyphen.

**Sample deployment scenario:** With Vormetric Vaultless Tokenization, policies could be implemented so that a customer service supervisor could see credit card numbers in the clear, while a customer service representative would only see the last four digits.
DEPLOYMENT AND ADMINISTRATIVE SIMPLICITY

With Vormetric Vaultless Tokenization, you can capitalize on a range of features that streamline up-front implementation and ongoing operations. Vormetric Vaultless Tokenization:

- **Enables efficient, enterprise-wide administration.** With the capabilities offered by the Vormetric Data Security Platform, you can choose from a range of technologies and employ the mix that's optimally suited to your specific projects and use cases. At the same time, you gain the cost savings and operational benefits of working with solutions that can be centrally and uniformly managed. With the Vormetric Data Security Platform, your organization can centrally manage keys for Vormetric Vaultless Tokenization, as well as for Vormetric Transparent Encryption, Vormetric Application Encryption, other Vormetric products, and third-party devices.

- **Offers non-disruptive implementation.** With the solution's format-preserving tokenization capabilities, you can restrict access to sensitive assets, yet at the same time, format the protected data in a way that reduces the operational impact typically associated with encryption and other obfuscation techniques. For example, your organization can tokenize a credit card field in a database, yet keep the tokenized information in a format that is compatible with associated applications. Further, you can create tokens that appear to be real credit card numbers and pass LUHN validation, so tokenization does not break existing validation processes.

- **Eliminates manual efforts and complexity.** The Vormetric solution employs tokenization at the application layer, and it streamlines all the application development efforts associated with implementing tokenization in an enterprise. With the solution, developers don't have to manually institute identity management or redaction policies. Vormetric Vaultless Tokenization offers an easy-to-use REST API for integration with the Vormetric Token Server, so your application developers can simply and quickly add tokenization and dynamic data masking to applications.

- **Provides investment protection.** Customers that have already invested in the Vormetric Data Security Platform can get even more out of their investments. Leveraging your existing Vormetric Data Security Manager installation, you can quickly and cost effectively add Vormetric Vaultless Tokenization to your environments through an all software deployment.

EFFICIENT SCALABILITY AND AGILITY

Vormetric Vaultless Tokenization delivers the high performance needed to address the operational demands of the most processing-intensive environments, enabling organizations to do millions of tokenization or detokenization operations per second. The Vormetric Token Server runs on virtual machines and can be quickly and efficiently scaled up and scaled down to accommodate changing workloads. For redundancy, Vormetric recommends deploying a cluster with at least two nodes. A three-node or four-node cluster multiplies the throughput, while providing added redundancy. Performance realized will vary depending on hardware platforms, cluster sizes, and client parallelism employed. It should be noted that Vormetric doesn't charge for the Token Server or the number of processed transactions, so you can add servers to accommodate your requirements for high availability and scalability, without having to add to your procurement costs.

In addition, because this solution doesn’t require a traditional database running as a token vault, lookup latency is greatly reduced. This is because there is no need for the token server to make calls to the token database to identify original data. The entire process occurs within the Vormetric Token Server. This also simplifies operations, as there are no databases to back up, synchronize, and maintain.
KEY BENEFITS

With Vormetric Vaultless Tokenization, your organization can realize the following benefits:

• **Reduce PCI DSS compliance effort and scope.** By leveraging Vormetric Vaultless Tokenization, you can minimize the repositories and processes that can gain access to payment data in the clear, so your organization can significantly reduce its PCI DSS compliance costs and efforts.

• **Fully leverage cloud, big data, and outsourced models.** Vormetric Vaultless Tokenization enables organizations to more fully leverage cloud services, big data models, and outsourced environments, while retaining the security controls required. For example, you can migrate tokenized data into a public cloud, and ensure sensitive data won’t be exposed to unauthorized individuals, even administrators in the cloud provider’s environment.

• **Establish broad safeguards around sensitive assets.** Unlike other dynamic data masking tools, the Vormetric solution tokenizes sensitive fields in the production database. As a result, your organization can establish comprehensive safeguards around sensitive assets across the organization. Because the source and display data remain protected, you can establish strong safeguards against cyber attacks from criminals and nation-states, as well as from insider abuse.

• **Minimize data security overhead and training.** With the Vormetric Data Security Platform, your organization can leverage a platform to centrally manage keys for Vormetric Vaultless Tokenization and as well for multiple encryption solutions. By leveraging a central platform that offers comprehensive capabilities, your organization can minimize the cost, effort, and training associated with managing point-products.

SAMPLE IMPLEMENTATIONS

Following are some of the common ways Vormetric Vaultless Tokenization can be used:

**PCI DSS 3.X COMPLIANCE**

The more locations that hold primary account numbers (PANs), the more locations that fall under PCI DSS regulations. As the number of locations grow, so too do the cost and effort associated with establishing and sustaining compliance, preparing for audits, and so on. With Vormetric solutions, you can tokenize PANs, and significantly restrict the number of users, processes, and repositories that can get access to this data in the clear. As a result, you can dramatically reduce your compliance efforts and costs. Further, through such capabilities as Luhn check support, Vormetric Vaultless Tokenization enables organizations to implement tokenization with minimal impact on applications and processes. In addition, the Vormetric Data Security Platform offers the controls you need to address many PCI DSS requirements, including least privileged access controls, encryption, key management, and file access audit logs.

**CUSTOMER CONTACT CENTERS**

Vormetric Vaultless Tokenization helps mitigate the threats that can be posed by support staff exploiting their access privileges to steal or leak sensitive data. Vormetric solutions can be effective both for securing sensitive data in internal contact centers and in outsourced or geographically distributed support environments. With Vormetric, you can enable a support agent to access only the information they require to do their jobs, for example, the last four digits of a customer’s Social Security number, without ever having to grant them access to the entire number. As a result, agents can conduct any required customer verification processes, without being put in a position where they can maliciously or inadvertently leak sensitive and regulated PII.
OUTSOURCED DEVELOPMENT

For many organizations, application development is done by an increasingly dispersed set of teams, including geographically distributed employees as well as external contractors and service providers. While these distributed teams have helped improve the cost efficiency and agility of development efforts, they can pose significant challenges for those organizations that manage sensitive and regulated data. From initial development to testing and staging, developers need access to data repositories. If all data is left in the clear, it exposes a range of sensitive regulated data and intellectual property to any number of threats. With Vormetric Vaultless Tokenization, organizations can quickly and efficiently provide internal and external development teams with access to corporate data repositories, while tokenizing the specific assets that pose security or compliance risks.

BIG DATA

To capitalize on the opportunities presented by big data, your organization needs to aggregate information from a broad range of repositories—and in the process you can create massive collections of highly sensitive and proprietary data. With Vormetric, your organization can fully leverage big data, without introducing risk to the business. You can tokenize sensitive records before they get migrated to big data repositories, so big data scientists, developers, and business analysts don’t gain access to sensitive data they don’t need. At the same time, the solution’s flexible tokenization options ensure that tokenized records don’t disrupt big data migration, calculation, and analytics processes.

CLOUD SERVICES

When your organization moves to cloud computing models, whether infrastructure as a service (IaaS), software as a service (SaaS), platform as a service (PaaS), or hybrid approaches, you may offload a number of responsibilities and efforts, but your organization ultimately still bears responsibility for the security of its sensitive and regulated data. With Vormetric Vaultless Tokenization, your organization can leverage the cloud models it needs, while managing tokenization policies locally. As a result, you can retain complete control and visibility over who can access sensitive assets in the clear, no matter where tokenized information ultimately resides.

STATIC DATA MASKING

Organization can replace sensitive assets with tokens, so outsourced application development and testing teams can run QA and analytics using realistic looking data, without having access to any sensitive assets. Once sensitive values in the database are tokenized, your organization simply needs to create a copy of the production database and give that copy to the outsourced development team. If they don’t have access to both the Vormetric Tokenization Server and user credentials to detokenize, they won’t be able to access sensitive data in the clear. This protects your business, maintains compliance, and enables outsourced development teams to access and test realistic production data.
ABOUT VORMETRIC, A THALES COMPANY

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual and cloud environments. Data is the new currency and Vormetric helps over 1,500 customers, including 17 of the Fortune 30 and many of the world’s most security conscious government organizations, to meet compliance requirements and protect what matters—their sensitive data—from both internal and external threats. The company’s scalable Vormetric Data Security Platform protects any file, any database and any application—anywhere it resides—with a high performance, market-leading data security platform that incorporates application transparent encryption, privileged user access controls, automation and security intelligence.

For more information, please visit: www.vormetric.com and find us on Twitter @Vormetric.

GLOBAL HEADQUARTERS
2860 Junction Ave, San Jose, CA 95134
Tel: +1.888.267.3732
Fax: +1.408.844.8638

EMEA HEADQUARTERS
200 Brook Drive
Green Park, Reading, RG2 6UB
United Kingdom
Tel: +44.118.949.7711
Fax: +44.118.949.7001

APAC HEADQUARTERS
Level 42 Suntec Tower Three
8 Temasek Boulevard
Singapore 038988
Tel: +65 6829 2266