SECURING DATA IN AN UNSECURE WORLD

Vormetric.com

Vormetric
Data Security™

THE STATE OF DATA SECURITY

Individuals and organizations today are generating more sensitive data than ever before. And with big data and the virtualization of many applications to scale across a distributed architecture, the sensitive data that organizations manage is proving to be highly vulnerable to security breaches. Consider these statistics:

THE NUMBER OF BREACHES DETECTED CONTINUES TO GROW—DRAMATICALLY.

Between 2009 and 2014, the number of detected security incidents has risen 66% year over year.[1]

THE SCALE OF ATTACKS IS MASSIVE.

In 2014, the total number of **breaches detected climbed** to **42.8 million**, which amounts to more than 117,000 attacks per day.[2]

WHEN BREACHES ARE DETECTED, IT'S TYPICALLY LONG AFTER THE DAMAGE HAS BEEN DONE.

Most organizations don't find out about breaches until it's far too late—if ever. Once threat groups establish a presence on a victim's network, the median days they remain undetected is 229.[3]

ON THE RISE

In 2014, **40% of organizations experienced a data breach** or failed a compliance audit.[4]

[1] PwC , "Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015."
[2] PwC , "Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015."
[3] Mandiant, "Mandiant 2014 Threat Report."
[4] Vormetric Insider Threat Report: http://www.vormetric.com/insiderthreat/2015

BEWARE OF THE INSIDER

ONE REASON FOR INCREASING SECURITY THREATS IS THE MISCONCEPTION THAT MOST THREATS COME FROM THE OUTSIDE.

In fact, your biggest threat may be the individual you least expect. These are employees, suppliers, and partners who have access to information, but leverage it for nefarious activity by either using it themselves or selling it to the highest bidder.

In the last year alone, **44% of US organizations experienced an insider attack** or failed a compliance audit.[5] Meanwhile, **28% of organizations detected insider attacks**, and almost one-third say the crimes perpetrated by insiders were more costly than those inflicted by outsiders.[6] Further, among all the categories within the "insider misuse" category, **88% of breaches occurred** through privileged abuse, and 72% were financially motivated.[7]

The potential for insider attacks is widespread considering the number of privileged users, contractors, and partners with access to sensitive internal data.[8]

55%

Privileged Users

46%

Contractors/Service Provider Employees

43%

Partners with Internal Access

[5] Vormetric Insider Threat Report: http://www.vormetric.com/insiderthreat/2015
[6] PwC, "US cybercrime: Rising risks, reduced readiness: Key findings from the 2014 US State of Cybercrime Survey."
[7] Verizon, "2014 Verizon Data Breach Investigations Report."
[8] Vormetric Insider Threat Report: http://www.vormetric.com/insiderthreat/2015

THE EVER-EVOLVING SECURITY THREAT

Just as security threats are rising, so is the amount of sensitive data that your organization is managing and storing. Moreover, as your organization increasingly relies on big data analytics, mobile applications, and cloud services, the number and location of different data points that you need to secure also keeps growing.

Any challenges that you've been having with compliance multiply under these conditions. Ultimately, ensuring consistent policies and adherence to regulatory mandates becomes a more difficult and resource-intensive process. And if your business processes or stores data for others, you'll face additional demands, including the need to provide data protection assurances or meet security service-level agreements (SLAs).

LACK OF CONTROL IS A KEY CONCERN

TOP 3 DATA SECURITY CONCERNS FOR CLOUD SERVICES

1	LACK OF CONTROL OVER THE LOCATION OF DATA	82%	U.S.
		56%	Others
2	INCREASED VULNERABILITIES FROM SHARED INFRASTRUCTURE	79%	U.S.
		52%	Others
3	PRIVILEGED USER ABUSE AT THE CLOUD PROVIDER	78%	U.S.
		56%	Others

Source: Vormetric Insider Threat Report: http://www.vormetric.com/insiderthreat/2015.

YOUR RESPONSE AND THE IMPLICATIONS

Your IT security teams may have invested heavily in perimeter security solutions to address evolving security, compliance, and contractual obligations. Yet, as earlier statistics show, these efforts are proving insufficient at safeguarding sensitive data from internal and external threats.

MEANWHILE, OTHER CONCERNS FURTHER COMPLICATE MATTERS:

- As IT manages more security-related tools and technologies, complexity, costs, and administrative overhead can quickly escalate.
- Individual business groups may be selecting their own method to secure data. The result? Many different solutions of varying security postures, inconsistent operating models, and high capital expenditures for your company overall.

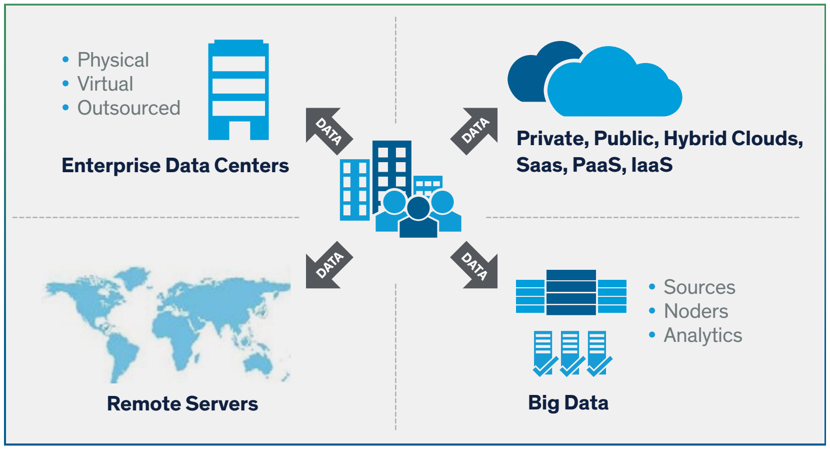
GROUND ZERO – DATA AT REST

Data at rest is the primary target of data theft – no wonder since that's where the most sensitive data is stored. It includes the volumes of unstructured files (often documents that contain analytics, customer data, and intellectual property) and structured databases that house social security numbers, credit cards, and other valuable information.

THE SECURITY INFLECTION POINT AND NEED FOR CHANGE

In a nutshell, you're dealing with more sensitive data in more locations, used by a more heterogeneous user community on more devices. These combined conditions make it difficult for your organization to:

- Migrate to and operate securely in the cloud
- Move and store big data in a variety of platforms and environments
- Ensure security and compliance of users and data across all applications, locations, and platforms



In fact, you can't move forward effectively to achieve these goals when your security infrastructure and management practices continually expose data at rest due to:

- The spread of sensitive data across discrete systems, including legacy platforms, virtualized, cloud, and big data environments
- A lack of granular safeguards to prevent uncontrolled, inconsistent access to business systems
- Compromised user credentials that enable external attackers to gain unrestricted access
- The ability for privileged users, including database, server, and cloud administrators, to access the specific systems they manage, as well as all the data held on these systems
- Disparate security policies and controls, which create administrative overhead and inconsistency in policy enforcement

WITHOUT A STANDARD WAY TO MANAGE AND SECURE DATA AT EVERY DATA SOURCE, YOU COULD PUT USERS, STAKEHOLDERS, AND, ULTIMATELY, YOUR BUSINESS AT RISK DUE TO SECURITY HOLES AND NON-COMPLIANCE.

A BETTER APPROACH: FOLLOW THE DATA

To address these challenges and threats to sensitive data, you need an approach that enables you to establish comprehensive security defenses across a distributed organization.

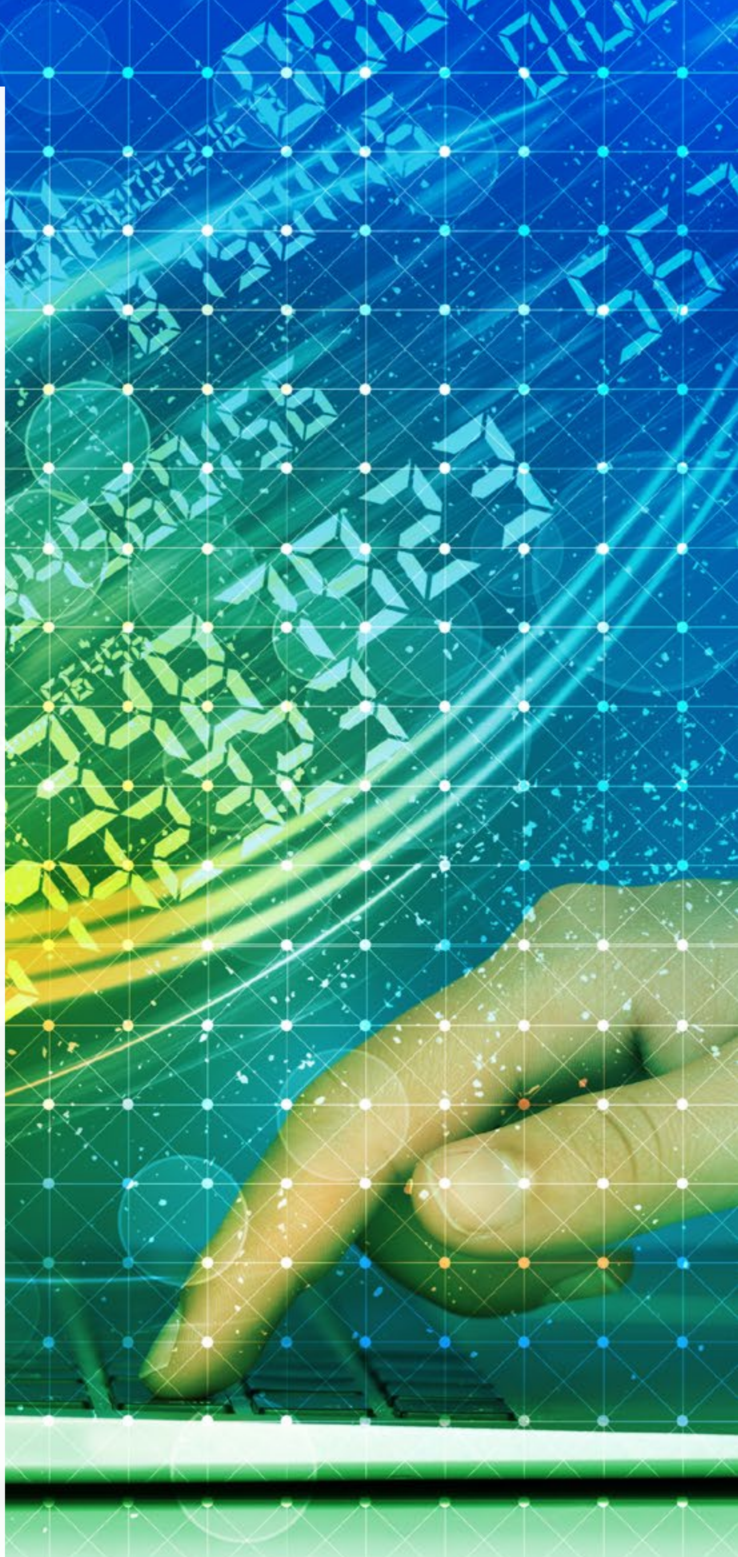
Traditional measures focused on securing your network perimeter to keep "the bad guys" out. But with more users on more devices, in more locations, leveraging big data and cloud applications, that tactic is insufficient because the perimeter no longer exists.

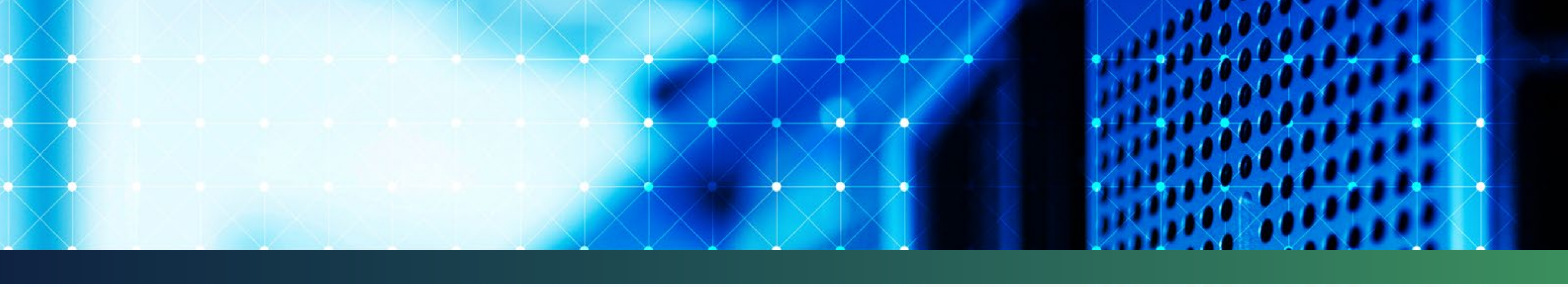
Instead, the new approach involves a shift from defending an attack vector (the perimeter) to defending the target, namely, your data.

This approach calls for the centralized deployment and administration of tokenization and encryption. It also requires giving your team the ability to establish security controls that guard against abuse by administrators and other privileged users.

Specifically, your organization needs to leverage a model that offers:

- **MINIMAL DISRUPTION** of (both on-premise and off-premise) business and operational processes
- **OPERATIONAL CONSISTENCY** to ensure a non-siloed approach to security and compliance
- **BREADTH OF COVERAGE** to decrease security-related capital expenditures
- **ABILITY TO SCALE** and flexibility to meet current and future deployment use cases





AT ISSUE

RISKY CLOUD MIGRATION

You have numerous options to consider when you undertake a cloud migration, including SaaS solutions like Box and Amazon S3, IaaS platforms from vendors like AWS and Rackspace, and many others.

These different cloud environments can pose serious risks if you don't have proper controls in place. First, cloud administrators—individuals you haven't met or vetted—can access the infrastructure and your data. Second, if a cloud service provider is subpoenaed, they may be required to furnish your data to authorities. Any unsecured sensitive data is ripe for exposure in this scenario.

PRIVACY MANDATES AND OTHER RISK FACTORS

When moving to the cloud, you must still address regulatory mandates such as PCI and HIPAA, as well as contractual SLAs, regional data jurisdiction requirements, and more.

Without addressing risks, you and your security team may be forced to stop or minimize the adoption of cloud offerings—or move forward and deal with outcomes ranging from security compromises to failed compliance audits.

SOLUTION

ENSURE A SMOOTH AND SAFE CLOUD MIGRATION

WITH VORMETRIC, YOU CAN CONFIDENTLY MEET DATA SECURITY AND COMPLIANCE REQUIREMENTS AS YOU MOVE INTO THE CLOUD.

Specifically, you can:

- Store your encryption keys in an enterprise-class, on-premise key manager
- Flexibly migrate into various cloud environments while maintaining control over user/administrative access
- Efficiently and centrally encrypt and secure both your on-premise data and the data that resides in cloud service provider environments
- Fully leverage a range of cloud services and offerings, while ensuring compliance with relevant mandates and security policies
- Support a wide range of public cloud environments, including AWS, Microsoft Azure, and Google Cloud Platform
- Support hosted and cloud environments offered from CenturyLink, Rackspace, IBM, FireHost, and many other providers
- Protect data as it moves into SaaS environments, such as Box and Amazon S3

SECURING DATA IN THE CLOUD

“With Vormetric, we’ve added new capabilities to extend data security practices to our customer implementations across our managed cloud platform.”

John Engates, CTO, Rackspace

AT ISSUE

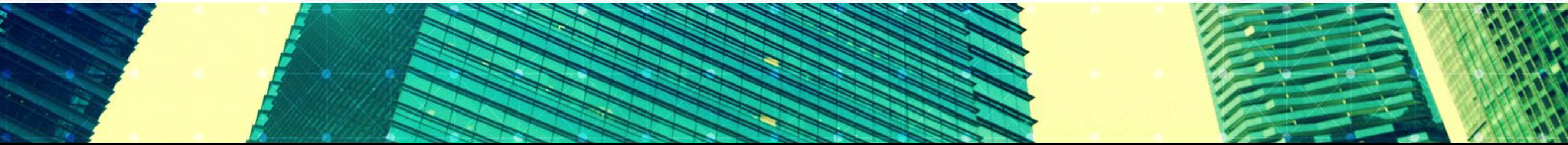
DIFFICULTY SECURING BIG DATA DEPLOYMENTS

BIG DATA INITIATIVES MAY ALSO PRESENT YOU WITH COMPLEX REQUIREMENTS:

- Different business units with different ideas about how to adopt big data, including requests to deploy different platforms, such as NoSQL, Hadoop, SAP HANA, and Teradata
- The need to leverage data from existing databases and files, which may contain sensitive and regulated data
- New schema-less platforms, which make it hard to distinguish sensitive from non-sensitive data and then implement security to ensure policies are enforced

It doesn't help that many of the new big data solutions don't supply built-in security capabilities. Compounding matters is the fact that big data is increasingly being run in outsourced or cloud environments. Consequently, sensitive source data and analytics could be exposed to attacks and to administrators you haven't met or vetted.

On top of this, you want to keep all your data secure without compromising analytics or impacting performance levels, so you can maximize the strategic value of big data.



SOLUTION

ACHIEVE YOUR BIG DATA ADOPTION GOALS

WITH VORMETRIC, YOU CAN EMPOWER YOUR ORGANIZATION TO FULLY LEVERAGE BIG DATA ANALYTICS, WITHOUT JEOPARDIZING ITS ABILITY TO COMPLY WITH SECURITY POLICIES AND REGULATORY MANDATES.

The Vormetric Data Security Platform enables you to **protect data at the block, file system, cell, or operating system level**—regardless of the data source and type, and the big data environment.

This solution offers extensive capabilities for securing sensitive data in big data environments. And its transparent encryption capabilities allow you to **avoid any application rewrites and minimize implementation efforts**.

In addition, it provides tokenization capabilities that allow you to mask specific records, so you can **institute granular controls** in your big data environment. As a result, you can help ensure that confidential data is not shared with people who do not require it.

EMPOWER YOUR ORGANIZATION TO FULLY LEVERAGE BIG DATA ANALYTICS

REAL-WORLD SUCCESS:

PROMOTING FULL COMPLIANCE WITHIN BIG DATA OPERATIONS

PHARMACEUTICAL FIRMS LIVE AND DIE BY HOW QUICKLY THEY CAN BRING THE NEXT NEW WONDER DRUG TO MARKET.

Key to accomplishing this is gathering and interpreting the mountains of clinical trial data that flow in from all research locations.

A major pharmaceutical firm knew that optimizing its data assets for similar purposes was critical to its success. But before it could kick-start its big data initiative and enable analysis of wide-ranging data, the firm had to address the security concerns of its risk and compliance team, which required encryption of regulated data for project approval.

Working with Vormetric, the company implemented a solution to centrally manage encryption and key management within a single infrastructure in a way that was transparent to its big data operations.

Now its security team can easily handle data encryption and access control requirements in full compliance with industry mandates. They can also concentrate on their core business to speed drug development and delivery.

AT ISSUE

BREAKING THE BANK WITH POINT SOLUTIONS

SECURITY TEAMS ARE TASKED WITH IMPLEMENTING EFFECTIVE SECURITY IN COMPLEX ENVIRONMENTS.

They are faced with:

- Safeguarding multiple platforms, data types, and storage locations leveraging different security methods and policies
- Departments or business units that may unilaterally move servers into the cloud or acquiring their own cloud and related security solutions
- Adoption of big data and implementing new cloud-based storage options, such as Amazon S3 and Box, and deploying additional security measures in the process

This myriad of data security solutions taxes staff resources, while substantially driving up costs for maintenance and management

> “We will undoubtedly continue to see more moves towards increased transparency following security breaches and data loss, tougher penalties and sanctions for those that fail to keep data secure.”[9]

[9] Fieldfisher White Paper: The legal obligations for encryption of personal data in the Unites States, Europe, Asia, and Australia, 2014.

SOLUTION

STRENGTHEN SECURITY AND SAVE MONEY WITH A SINGLE PLATFORM

With Vormetric, your organization can leverage a unified platform to address a broad range of threats, use cases, and environments by:

- Securing data and reducing the exposure to the traditional hacker, as well as the insider threat
- Centrally managing keys for Vormetric encryption products, as well as many other encryption platforms
- Managing keys locally, so they can retain visibility and control over sensitive data—even if data is migrated into external cloud or big data environments
- Employing robust, granular controls to guard against abuse by privileged users and by external attacks that attempt to exploit compromised administrators' credentials
- Leveraging detailed logs that proactively support compliance audits, and can be integrated with SIEM tools to improve forensics and intelligence
- Addressing data-at-rest security requirements, including those associated with cloud and big data environments

In the end, this approach enables administrators to focus on supporting the business while securely providing authorized users with the data they need to do their jobs.

SECURITY WITH LESS COST AND EFFORT

By eliminating disparate point tools and consolidating on Vormetric, organizations have **reduced costs by 50 to 70 percent.***

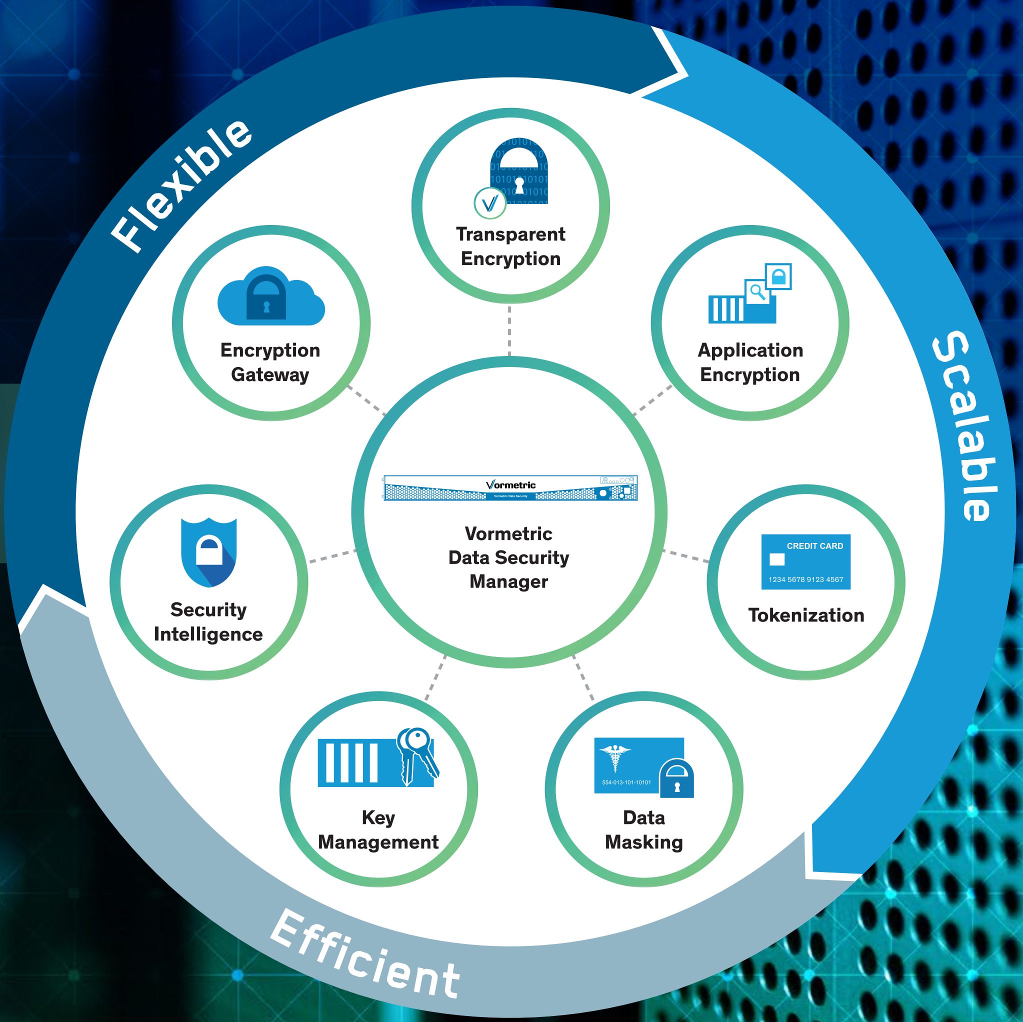
* Based on Vormetric TCO analysis from published pricing and average opex costs.

THE VORMETRIC DIFFERENCE

The Vormetric Data Security Manager makes it efficient to manage data-at-rest security across your entire organization. It comprises a broad set of products that share a centrally managed and extensible infrastructure for simple **one-stop data-at-rest security**.

LEARN MORE. VISIT **VORMETRIC.COM**

@vormetric @vormetricpartnr



Flexible

Scalable

Efficient

Vormetric Data Security Manager

Transparent Encryption

Application Encryption

Tokenization

Data Masking

Key Management

Security Intelligence

Encryption Gateway

Securing Data In an Unsecure World.

Vormetric.com

Vormetric
Data Security™