THALES

www.thalesesecurity.com

‹Thales eSecurity›

VORMETRIC TRANSPARENT ENCRYPTION ARCHITECTURE

White Paper

Contents

Figures

Executive summary

Today's IT and security organizations need to continue to scale their capabilities. They need to employ safeguards around larger volumes of sensitive data. They have to guard against more persistent and sophisticated threats, and they must establish these safeguards in more places.

To address these expanding requirements, leading enterprises and government agencies rely on Vormetric Transparent Encryption by Thales eSecurity. This paper offers a detailed look at the capabilities and the architecture of the Vormetric Transparent Encryption offering.

Introduction

For IT and security teams in today's organizations, adaptation is a key part of the job description. Sensitive data continues to make it into a broader set of environments, including private, public, and hybrid cloud deployments; big data platforms; virtualized systems; and more.

The policies and regulatory mandates in effect continue to grow more stringent and IT and security teams must respond to these realities. At the same time, they have to guard against more sophisticated, persistent, and effective cyber attacks, and the continuous threats posed by malicious users with privileged access.

According to the 2018 Thales Data Threat Report[1], respondents feeling of being "very" or "extremely" vulnerable to security threats are soaring, reaching 44% globally and 53% in the U.S., compared with 30% globally and 29% in the U.S. just one year ago.

Further, the bad news is that rates of successful breaches have reached an all-time high for both mid-sized and enterprise class organizations, with more than two-thirds (67%) of global organizations and nearly three fourths (71%) in the U.S. having been breached at some point in the past. Nearly half (46%) of U.S. respondents reported a breach just in the previous 12 months, nearly double the 24% response from last year;

In response, IT and security organizations are increasingly focusing on protecting data at the source, namely servers and databases, whether they reside in internal data centers or external environments. Toward that end, it is critical to use encryption, privileged user access control, and security intelligence in order to establish persistent controls over sensitive and regulated data, no matter where it may be stored.

1 – 2018 Thales Data Threat Report, featuring findings from 451 Research, https://dtr.thalesesecurity.com/

Vormetric Transparent Encryption

Solution introduction

With Vormetric Transparent Encryption by Thales eSecurity, organizations can establish strong controls around their sensitive data, and do so with maximum efficiency. Vormetric Transparent Encryption enables data-at-rest encryption, external key management, privileged user access control, and the collection of security intelligence logs to protect structured databases and unstructured files—including those residing in physical, big data, and cloud environments.

PART OF VORMETRIC DATA SECURITY PLATFORM

Vormetric Transparent Encryption is part of the Vormetric Data Security platform by Thales eSecurity, a solution that makes it efficient to manage data-at-rest security across your entire organization. Built on an extensible infrastructure, Vormetric Data Security Platform products can be deployed individually, while sharing efficient, centralized key management. In addition to the Vormetric Transparent Encryption solution, the Vormetric Data Security Platform delivers capabilities for application-layer encryption, tokenization, dynamic data masking, cloud encryption gateways, and integrated key management.

Vormetric Transparent Encryption offers these distinctive capabilities:

- **Non-intrusive implementation.** By leveraging the solution's transparent approach, your organization can implement encryption, without having to make changes to your applications, infrastructure, or business practices.
- **Broad environment support.** The solution can be deployed quickly and easily and can be used in physical, virtual, cloud, and big data environments. Vormetric Transparent Encryption offers support for file systems and storage architectures and it supports a broad range of operating systems, including Microsoft Windows, Linux, Oracle Solaris, IBM AIX, and HP-UX.
- **Scale.** Vormetric Transparent Encryption features agents that are distributed across the server infrastructure. As a result, the product delivers scalability and eliminates the bottlenecks and latency that plague proxy-based solutions. Tens of thousands of agents can be quickly deployed and easily managed across a company, enabling support of many different use cases.
- **High-performance.** Vormetric Transparent Encryption offers maximum utilization of native hardware encryption capabilities, such as Intel AES-NI, AMD AES-NI, and SPARC encryption, to minimize computational costs and deliver optimal performance.
- **Privileged user access controls.** In addition to encryption and key management, the agent can enforce very granular, privileged user access policies, enabling protection of data from misuse by privileged users and APT attacks. Granular policies can be applied by user (including for administrators with root privileges), process, file type, time of day, and other parameters. Enforcement options are also very detailed; they can be used to control not only whether users can access clear-text data, but which file system commands are available.
- **Strong encryption.** Vormetric Transparent Encryption only employs robust, standard-based encryption protocols, such as Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. The agent is FIPS 140-2 Level 1 validated.
- **Flexible, streamlined administration.** All policy and key administration is done through the Vormetric Data Security Manager, which offers a Web-based management interface that makes policy creation easy. Administrators can also work with CLI- or API-based interfaces. Policies can be as granular as required for different business purposes. To facilitate development and to test access policies before they go into production, Vormetric Transparent Encryption features a "learn mode." Learn mode makes it easy for policy administrators to test new policies by only creating logs and not enforcing data access controls. In this way, new policies can be tested and tuned before enforcement begins. Learn mode is also very useful to form a baseline of access patterns of sensitive data.
- **Key rotation and data transformation features.** The product supports key rotation and it enables administrators to do periodic, in-place transformation of encrypted data. This enables key life cycle management best practices with no downtime.

Vormetric Transparent Encryption

Solution components

Vormetric Transparent Encryption solution deployments consist of two Thales products, Vormetric Transparent Encryption agent and Vormetric Data Security Manager (DSM). In addition, customers can deploy Vormetric Security Intelligence by Thales eSecurity to leverage the solution's granular logs. The following sections offer more details on each of these products.

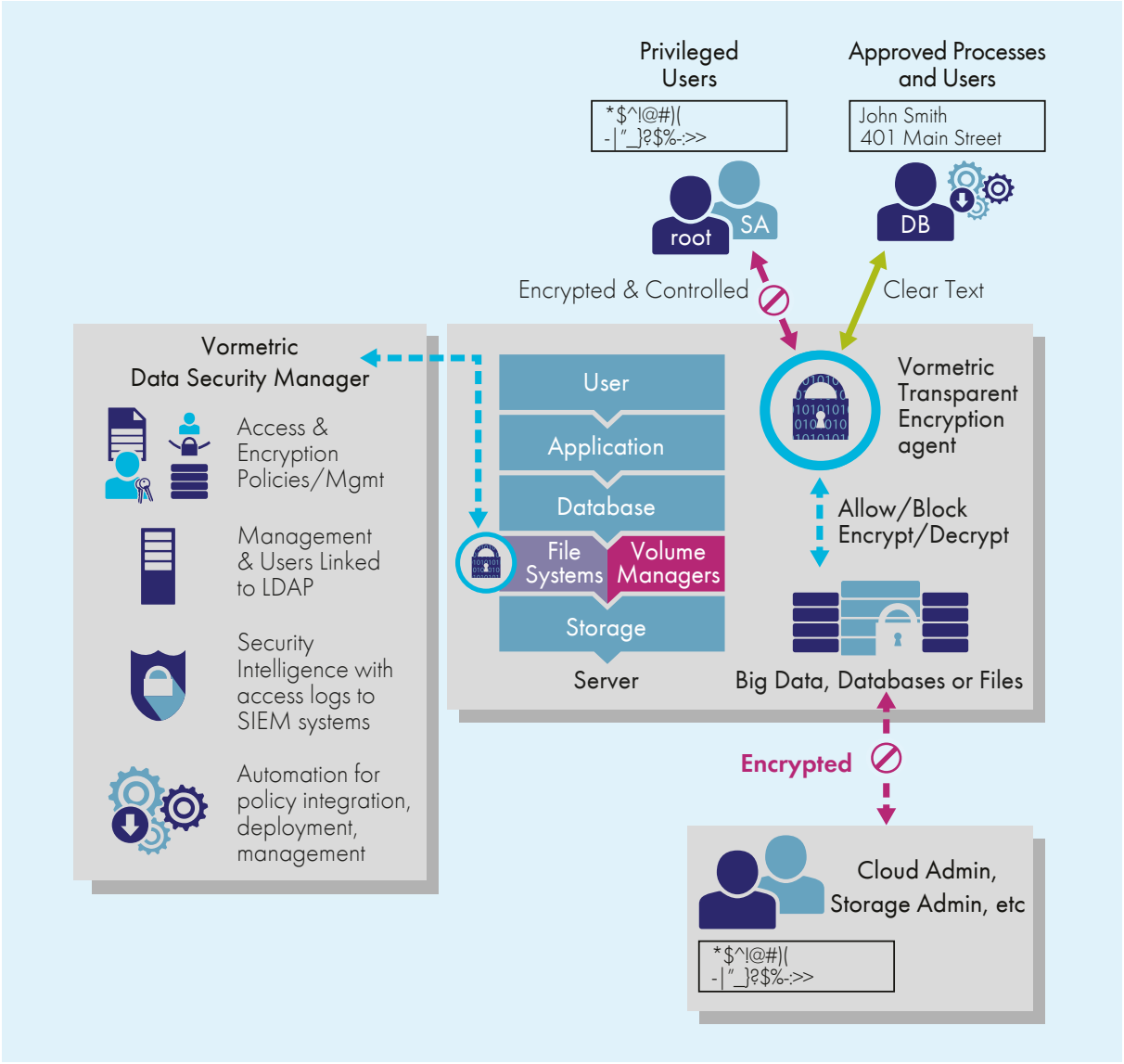

Fig 1 – Sample Vormetric Transparent Encryption deployment architecture.

VORMETRIC TRANSPARENT ENCRYPTION AGENT

Vormetric Transparent Encryption agents run at the file system level or volume level on a server. Agents perform encryption, decryption, access control, and logging. Agents employ logic and fine-grained policies to evaluate attempts to access protected data, and then either grant or deny access. All activities are logged. At the time of the writing this white paper, the agents support the following environments: (Note, Thales is regularly expanding platform support, so please contact Thales if a technology deployed in your environment isn't listed.)

Platforms:

- Microsoft: Windows Server
- Linux: Red Hat Enterprise Linux (RHEL/Centos), SuSE Linux Enterprise Server, and Ubuntu
- Unix: IBM AIX, HP-UX, and Solaris

Databases (partial list):

- IBM DB2
- Microsoft SQL Server
- MySQL
- NoSQL
- Oracle
- Sybase

Applications:

Transparent to all custom and commercial applications, including SAP, SharePoint, Documentum, and more.

Big data environments:

- Cloudera CDH 4/5 (Cloudera Certified)
- Couchbase
- DataStax
- Hortonworks (HDP Certified, HDP YARN Ready Certified)
- IBM Infosphere BigInsights
- MongoDB (MongoDB Enterprise Certified)
- Teradata

VORMETRIC DATA SECURITY MANAGER

The Vormetric Data Security Manager (DSM) enables organizations to centrally control policies and key management for multiple Vormetric solutions. You can use the DSM to provision and manage keys for other Thales eSecurity solutions including, Vormetric Application Encryption, and Vormetric Cloud Encryption Gateway. In addition, you can manage keys for Vormetric Tokenization.

DSM also provides a unified way to manage keys for third-party platforms, such as IBM Guardium Data Encryption (GDE), Oracle Transparent Data Encryption (TDE), Microsoft SQL Server TDE, and KMIP-compliant encryption products. The platform can vault X.509 certificates, symmetric keys, and asymmetric keys.

Flexible deployment models

The Vormetric Data Security Platform is flexible and offers support for a number of deployment models, helping customers address a range of business, security, and technical requirements. This product is available in the following form factors:

- A hardware appliance, with FIPS 140-2 Level 2 validation
- A hardware appliance, with an integrated HSM and FIPS 140-2 Level 3 validation
- A hardened virtual appliance
- As a service through the AWS Marketplace and other leading cloud hosting providers

Robust separation of duties

The DSM can be configured as a multi-tenant device that runs many different virtual DSMs, which are called "domains." The DSM can enforce strong separation of duties by requiring more than one data security administrator to manage or change key and policy permissions. DSM administration can be broken into three categories: system, domain, and security. In this manner, no one person has complete control over security activities, encryption keys, or administration. In addition, the DSM supports two-factor authentication for administrative access.

To further isolate and protect sensitive data, the DSM and Vormetric Transparent Encryption work in tandem in order to allow security administrators to create a strong separation of duties between data owners and privileged IT administrators, such as root, storage and cloud administrators. Vormetric Transparent Encryption encrypts files, while leaving their metadata in the clear. In this way, IT administrators can perform their system administration tasks, without being able to gain access to the sensitive data residing on those systems.

Because the metadata is in the clear, Vormetric Transparent Encryption doesn't have an impact on IT administrative activities like replication, backup, migration, and snapshots. However, it can keep administrators from having access to the data. The platform's fine-grained access controls can even be used to define what administrative access a privileged user can have to data. For example, functions such as copy, write, or directory listing can be controlled.

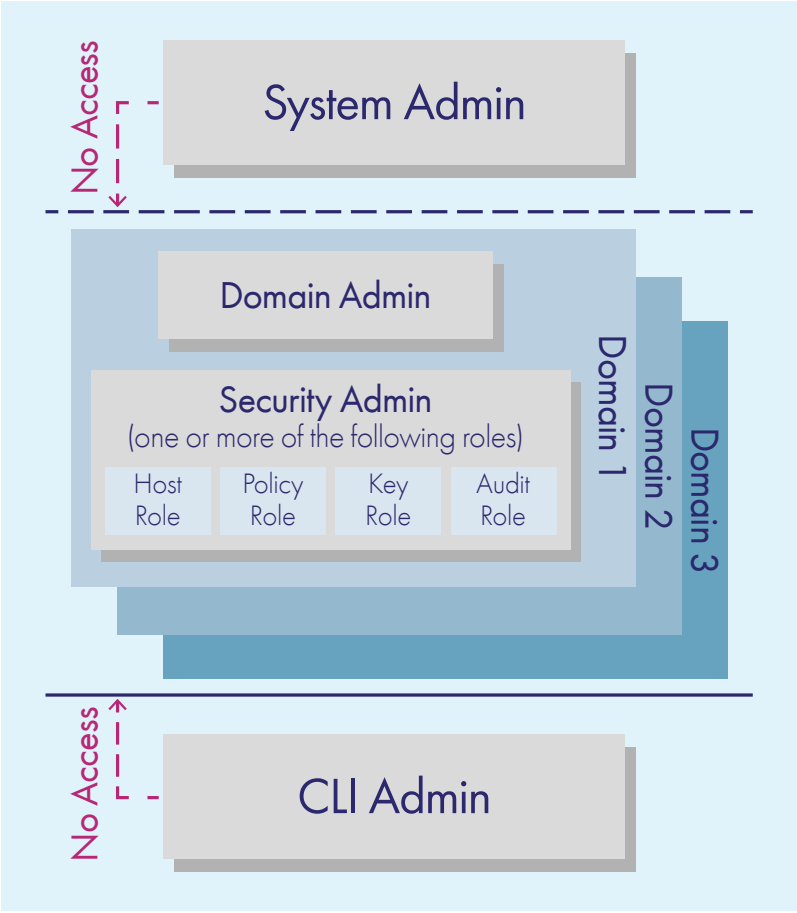

Fig 2 – Through its administrative domains, the DSM maintains strong separation of duties

VORMETRIC SECURITY INTELLIGENCE

With Vormetric Security Intelligence, organizations can harness the extensive logging capabilities of Vormetric Transparent Encryption. Vormetric Security Intelligence delivers detailed security event logs that are easy to integrate with security information event management (SIEM) systems, so you can efficiently detect risks as well as quickly produce compliance and security reports.

Detailed data and powerful insights

These logs produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into activities pertaining to sensitive data access. Logging occurs at the file system level, helping eliminate the threat of an unauthorized user gaining stealthy access to sensitive data. These logs can inform administrators of unusual or improper data access and accelerate the detection of insider threats, hackers, and advanced persistent threats (APTs).

Detailed logs can be reviewed to specify when users and processes accessed data, under which policies, and if access requests were allowed or denied. The logs will even expose when a privileged user leverages a command like "switch user" to imitate another user.

Broad SIEM Platform Integration

Traditionally, SIEMs relied on logs from firewalls, IPSs, and NetFlow devices. Because this intelligence is captured at the network layer, these approaches leave a commonly exploited blind spot: They don't provide any visibility into the activity occurring on servers. Vormetric Security Intelligence eliminates this blind spot, helping accelerate the detection of APTs and insider threats.

Sharing these logs with a SIEM platform helps uncover anomalous process and user access patterns, which can prompt further investigation. For example, an administrator or process may suddenly access much larger volumes of data than normal, or attempt to do an unauthorized download of files. Such inconsistent usage patterns could point to an APT attack or malicious insider activities.

Vormetric Security Intelligence offers proven integration with a range of SIEM platforms, including FireEye Threat Prevention Platform, HP ArcSight, IBM Security QRadar SIEM, Informatica Secure@Source, McAfee ESM, LogRhythm Security Intelligence Platform, SolarWinds, and Splunk.

EFFICIENTLY DELIVER COMPLIANCE REPORTING

In order to adhere to many compliance mandates and regulations, organizations must prove that data protection is in place and operational. Vormetric Security Intelligence delivers the detailed evidence needed to prove to an auditor that encryption, key management, and access policies are working effectively.

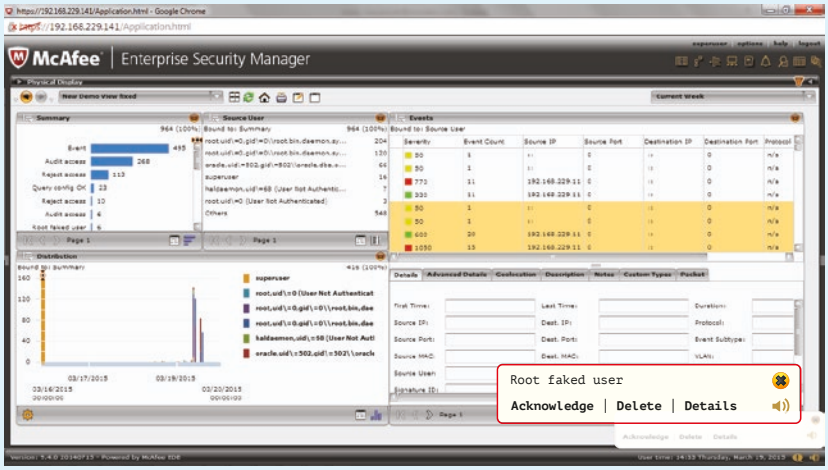

Fig 3 – Example of Vormetric Security Intelligence logs working with a SIEM for security reporting and detecting a possible threat.

Use cases

Vormetric Transparent Encryption can help organizations address many of their most significant business and technology objectives. Following are some of the most common objectives Vormetric Transparent Encryption is being employed to address.

SECURELY MIGRATING TO CLOUD AND HYBRID-CLOUD ENVIRONMENTS

The challenge

Today, enterprises are in the midst of a massive shift in the way they manage their business and IT services. In just the past few years, these organizations have gone from IT environments that were hosted in internally managed data centers, to a steadily increasing reliance on virtualization and external service providers and cloud models.

Now a single organization may be reliant upon a combination of cloud-hosted infrastructure, SaaS-based applications, private clouds, virtual private clouds, and a number of other models. Rather than a monolithic move from one approach to another, IT and business leaders are mixing and matching the approaches that make most sense for a given task, so they can best align service models with specific business and technology requirements.

To establish effective and consistent safeguards, enterprise security teams need comprehensive, centrally managed security capabilities that can be leveraged across all these dynamic environments. To leverage cloud resources while meeting their security and compliance requirements, enterprise security teams need robust, persistent, and granular controls that can be applied whether data is in their internal data center or at their cloud provider's facilities.

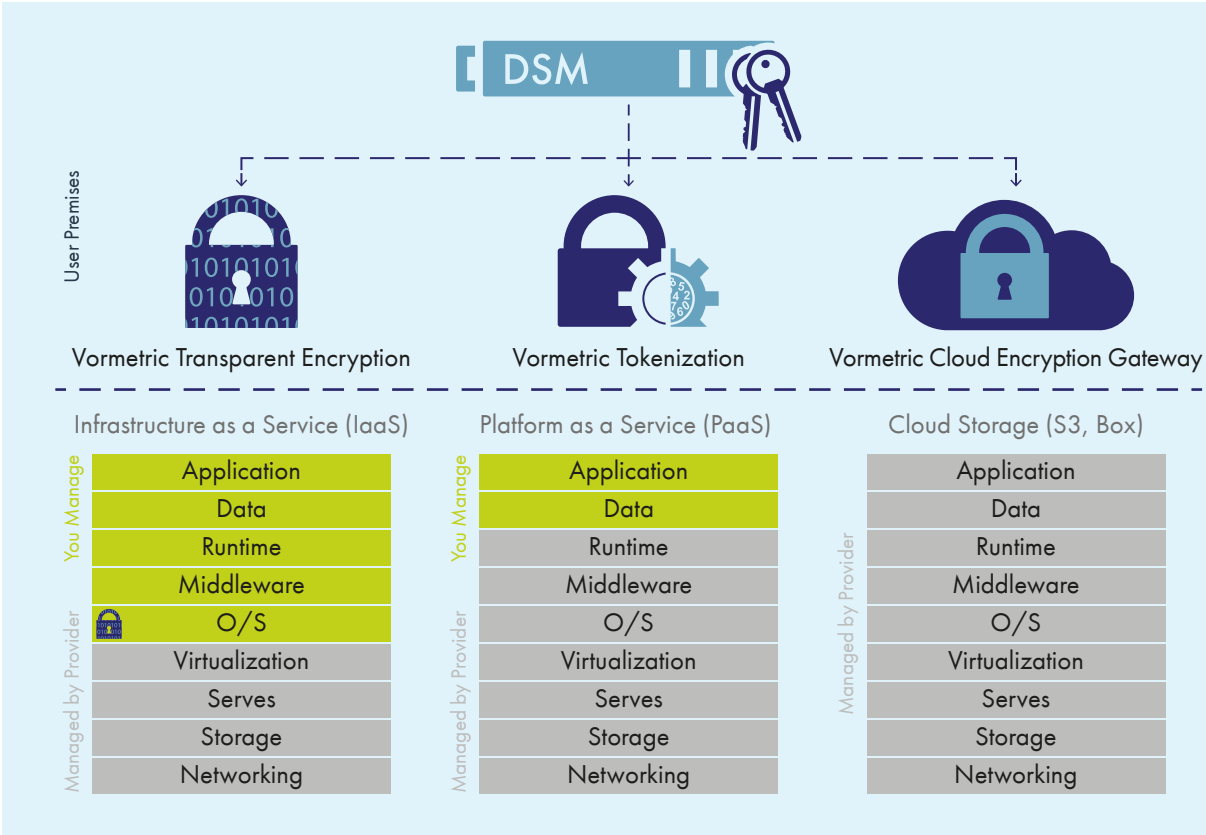

Fig 4 – DSM centralizes key management and control of data on-premises, while enabling the protection of data across different cloud environments.

How Thales helps

Organizations are increasingly leveraging Vormetric Transparent Encryption as they look to address data-at-rest encryption requirements in their hybrid, internally hosted, and cloud-based mix of environments. With Vormetric Transparent Encryption, security teams can encrypt data at the file system or volume level within virtual machines (VMs) and then use fine-grained, centrally managed policies to control access to protected data.

Vormetric Transparent Encryption encrypts data at the file system level within cloud instances and then provides fine-grained, centrally managed controls that help ensure that only authorized users and processes can decrypt data. In addition, now customers can leverage data security-as-a-service offerings from a number of leading cloud providers that are powered by Vormetric Transparent Encryption. Be sure to visit the Thales Cloud Partner Program[2] page for a complete list of partners and cloud offerings.

SECURITY AND COMPLIANCE IN BIG DATA ENVIRONMENTS

The challenge

Today, enterprises are growing increasingly reliant upon big data implementations so their staff can maximize the value of data in furthering a range of objectives, including making more informed plans and decisions, discovering new opportunities for optimization, and delivering breakthrough innovations. However, given the specific attributes of big data implementations, organizations adopting big data can also be exposed to increased risks. Big data implementations consolidate diverse data sets and yield high-value insights, which can make these environments a prized target for malicious insiders and external criminals.

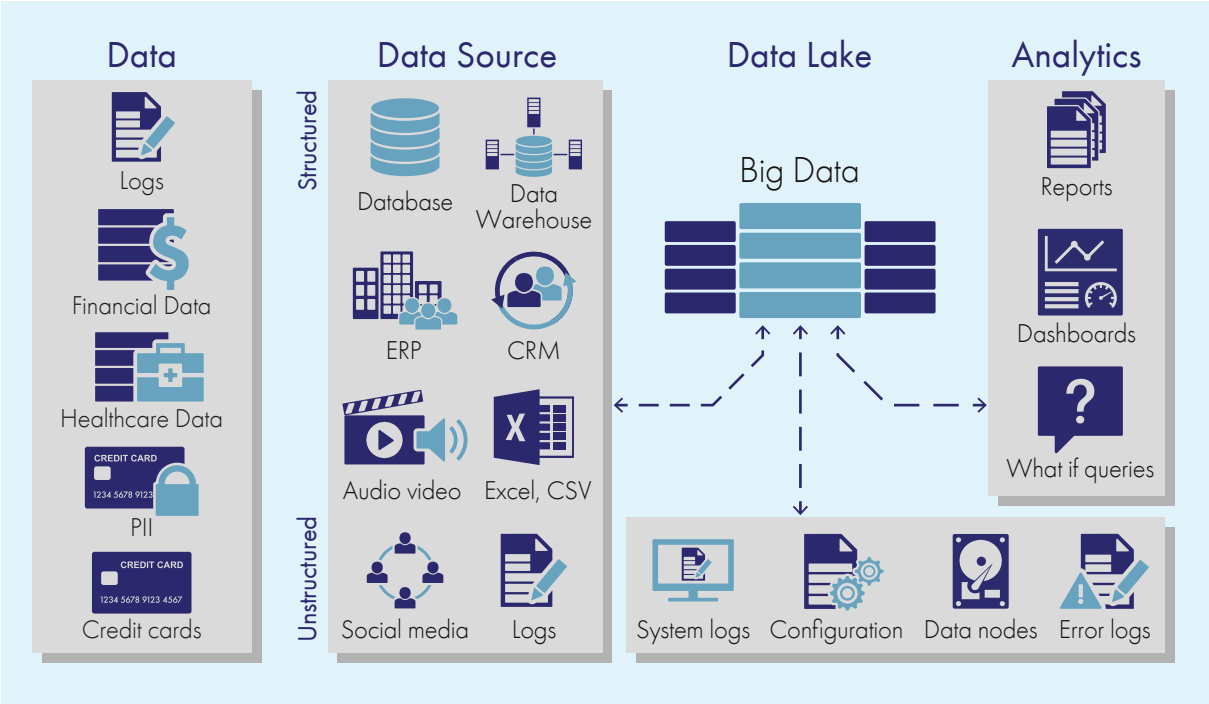

Fig 5 – Vormetric Transparent Encryption providing end-to-end data encryption, privileged user access control, and key management in a big data environment.

2 – https://www.thalesesecurity.com/partners/search

How Thales helps

Vormetric Transparent Encryption is a solution that organizations increasingly leverage to secure the sensitive assets in their big data environments. With the solution, organizations can secure sensitive data in big data environments based on Hadoop or NoSQL, including Hortonworks, MongoDB, Cloudera, DataStax, Couchbase, IBM BigInsights, Teradata, and more.

Vormetric Transparent Encryption can secure the entire big data environment, including the data sources that may be fed into the environment, the big data nodes and the "data lake", and the analytics and reports that get generated.

EFFICIENTLY SECURING SENSITIVE DATA ACROSS DISTRIBUTED OFFICES AND MOBILE ENVIRONMENTS

The challenge

While securing today's evolving data centers can be challenging, many IT organizations also have to contend with the security requirements of a large number of distributed entities. For a large retailer, this can include thousands of globally distributed stores. For banks, this can include branch offices, ATMs, and kiosks. For military organizations, this could include everything from field offices to naval vessels and ground transport vehicles. Especially in recent years, these remote and distributed environments have represented the Achilles heel of many organizations because they are targeted for both virtual and physical theft.

Establishing and sustaining security in these distributed environments can present several significant challenges. For example, they may be more vulnerable to theft or attack and they can be subject to intermittent connectivity. Further, for many organizations, securing these environments also poses significant challenges from a scalability standpoint, as often hundreds of locations need to be supported.

How Thales helps

Today, some of the largest retailers, financial institutions, and government agencies rely on Vormetric Transparent Encryption to efficiently secure their distributed environments. By leveraging the solution's robust encryption capabilities, organizations can establish the critical safeguards required to ensure that sensitive data remains secure from cyber attacks and even physical theft. The solution's encryption agents can be remotely deployed and managed, which makes them practical to deploy across large numbers of distributed locations. Further, Vormetric Transparent Encryption is optimally suited to the unique requirements of these distributed environments, offering the proven ability to scale to more than 10,000 sites and to deliver high availability, even in environments where connectivity isn't reliable.

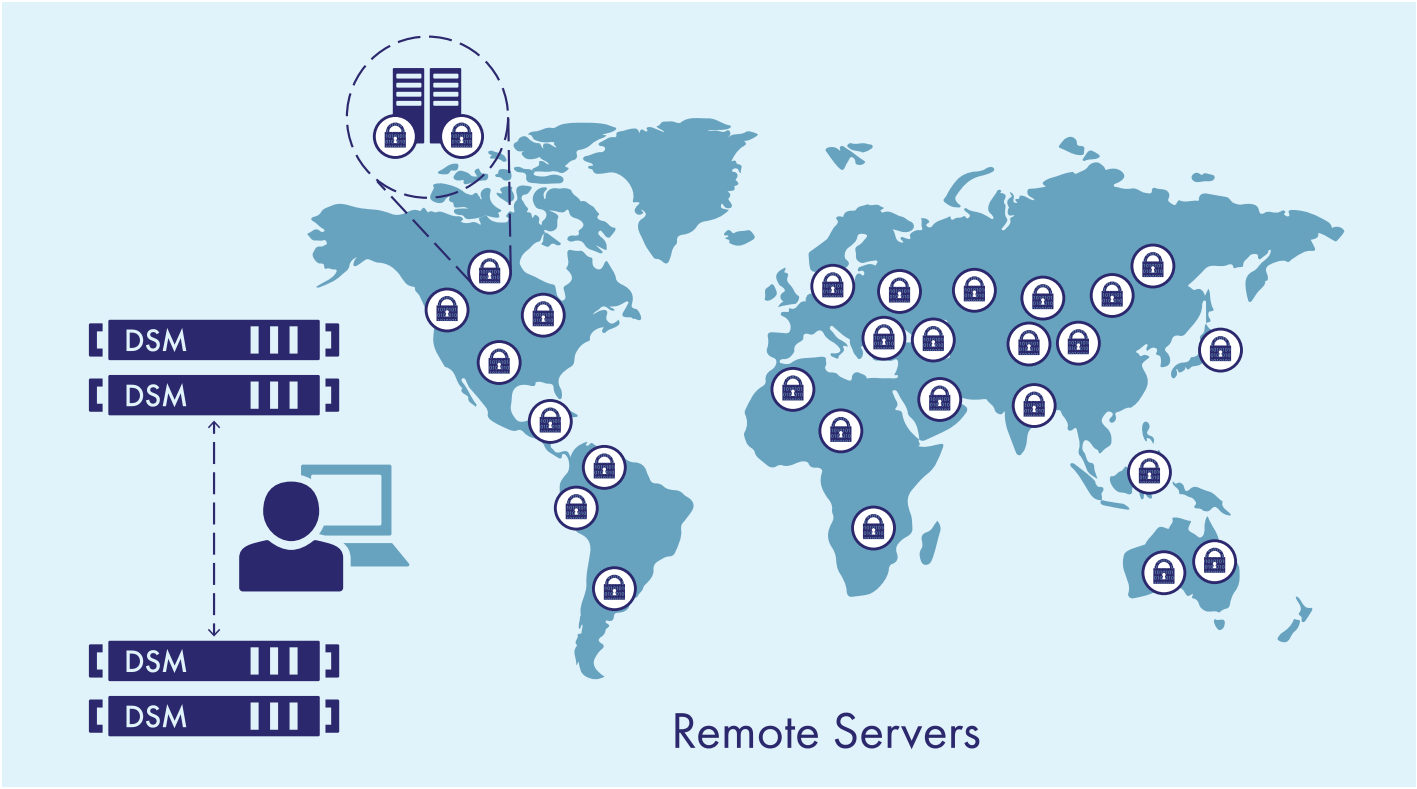

Fig 6 – Example of a geographically distributed cluster of DSMs providing high availability for thousands of protected servers.

Conclusion

The demands for data-at-rest encryption continue to grow more urgent. Now more than ever, encryption represents a critical means for guarding against data breaches and ensuring compliance with regulatory mandates. With Vormetric Transparent Encryption, organizations can leverage a comprehensive solution that can address a wide range of environments and use cases. Through these advanced capabilities, organizations can address their security mandates, while minimizing costs and administrative efforts.

Appendix: Vormetric Transparent Encryption performance benchmarks

The latest Intel® Xeon® processor family includes Intel® Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI). AES-NI accelerates AES encryption and has been optimized for fast throughput and low latency. Vormetric Transparent Encryption uses AES-NI instructions for hardware-based acceleration of data encryption and decryption. In fact, Vormetric Transparent Encryption has a proprietary encryption engine that is designed to take full advantage of the parallelism that can be achieved with multi-core processor chipsets and it specifically leverages the pipelining capabilities of AES-NI. As a result, the solution delivers the maximum performance possible.

In addition to leveraging hardware-based encryption capabilities, Vormetric Transparent Encryption is tightly integrated with, and optimized for, each supported operating system kernel. Consequently, Vormetric Transparent Encryption leverages the latest features available for every platform supported, rather than being coded to a lowest common denominator across multiple platforms. With each new release, Vormetric continues to add new capabilities that enable the solution to exploit the latest operating system features.

For many applications, the performance overhead that Vormetric Transparent Encryption introduces is negligible. However, as loads associated with input/output (I/O) increase, there will be increased overhead associated with encryption. Even with demanding, I/O heavy applications, such as databases or big data processing, Vormetric Transparent Encryption generally introduces less than 10% overhead.

One example can be seen in the chart below. In this example, the Yahoo Cloud Serving Benchmark (YCSB) was run against MongoDB 3.0.2, with the WiredTiger storage engine running on top of Vormetric Transparent Encryption. YCSB is a generally available open source framework that has a common set of workloads for evaluating the performance of different "key-value" and "cloud" serving stores. The workload was configured so that less than one-half of the data set could fit in memory, causing a heavy I/O load. As the chart illustrates, Vormetric Transparent Encryption only introduced minimal overhead.

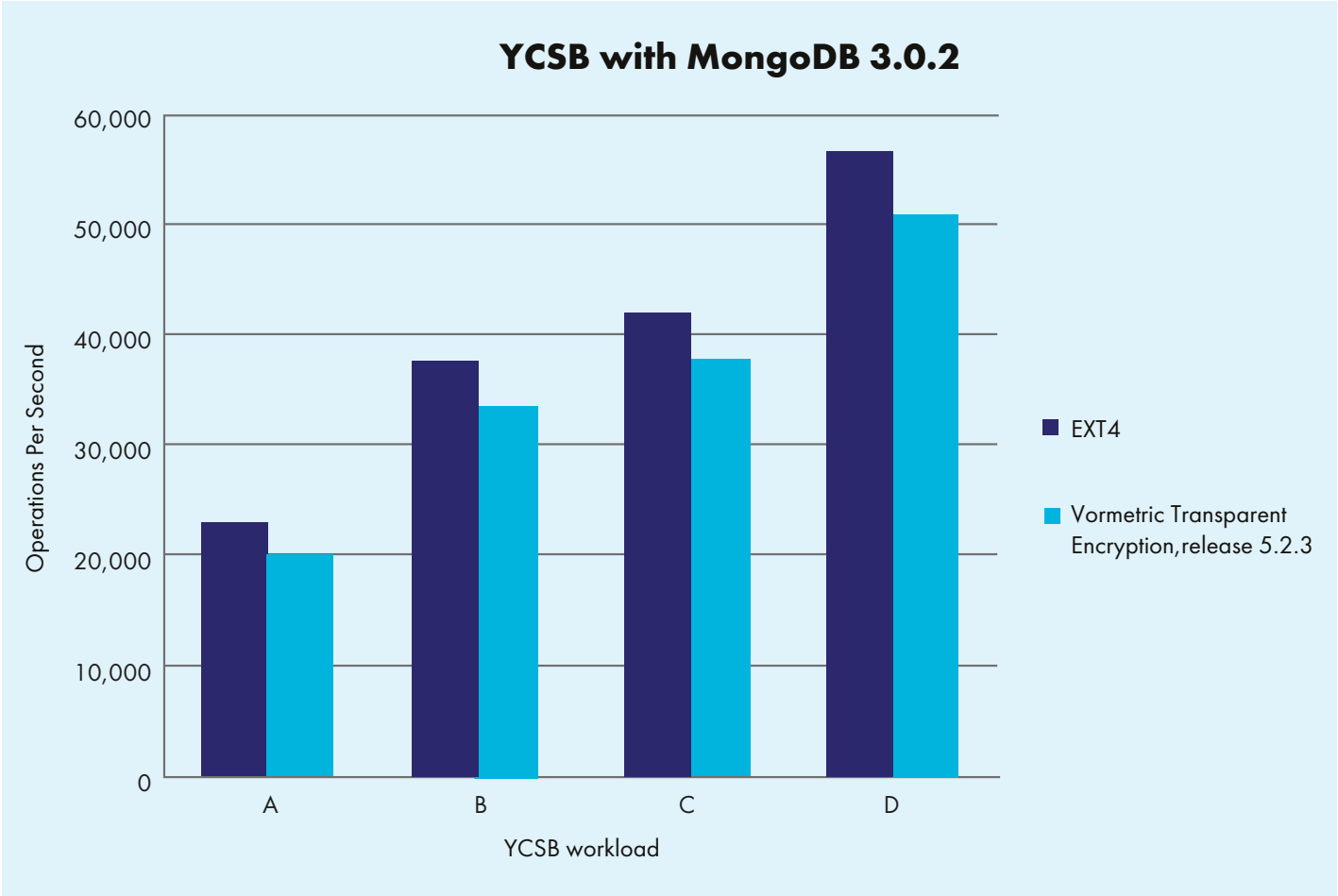

Fig 7 – Even when testing in a scenario with a heavy I/O load, Vormetric Transparent Encryption introduces minimal performance overhead.

THALES

www.thalesesecurity.com

About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com