Cloud Partner™

PROTECTING YOUR DATA IN THE CLOUD

QTS Data Security: Encryption, Key Management, Access Controls, and Data Event Information to Safeguard Sensitive Data at Rest

Vormetric, Inc.
2545 N. 1st Street, San Jose, CA 95131
United States: 888.267.3732
United Kingdom: +44.118.949.7711
Singapore: +65 6829 2266
info@vormetric.com
www.vormetric.com

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

Across your enterprise, decision makers are recognizing the benefits of cloud services—and moving to capitalize on them. At the same time, addressing your compliance and security requirements continues to grow more urgent and challenging. How does your organization more fully leverage cloud services, while addressing the risks of data breaches and failed compliance audits?

This paper offers a detailed look at the requirements for establishing data-centric security in today's cloud environments—and it shows how QTS Data Security, utilizing the Vormetric Data Security Platform uniquely addresses these requirements, so you can more confidently and swiftly adopt cloud services for your business. This paper offers details on the platform's solution architecture and it reveals how this architecture helps to maximize the security and satisfaction of compliance requirements of sensitive data, while making it simple and efficient to manage data security throughout the enterprise, including in the cloud. Finally, this paper looks at common cloud deployment models, illustrating how the solution can be employed to address a range of environments, security requirements, compliance needs, and business objectives.

INTRODUCTION: THE MOVE TO THE CLOUD, AND THE CONCERNS THAT ARISE

If your business handles confidential, personal, healthcare, or financial data, it's essential for your IT and security teams to protect this information and ensure compliance with security policies and regulatory mandates. In today's environments, where nation states fund hackers, abuse by privileged insiders and advanced persistent threat (APT) attacks continue to make headlines, establishing and maintaining security and compliance grows increasingly challenging. Further, the stakes of failure are high: A single breach can leave an organization exposed to damaged business reputation, business disruption, intellectual property losses, fines, and privacy disclosures.

These security responsibilities—and these risks—only expand as your organization moves to private, public, and hybrid cloud environments. According to 451 Research, these are the most prevalent security concerns associated with cloud adoption:

- **Data privacy and security—**How do you secure data in the cloud?
- **Access and control—**How do you control data access in the cloud?
- **Auditing and compliance**—How do you stay compliant in the cloud?
- **Control of data**—How do you track data as it moves in the cloud?

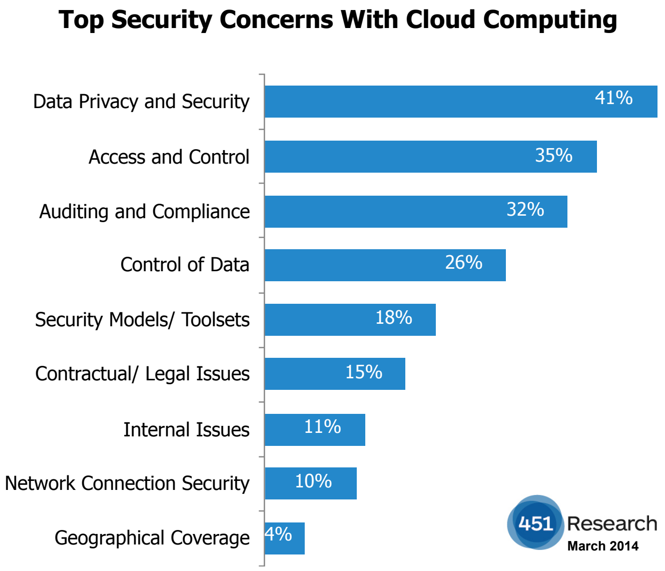


Figure 1. Top Security Concerns with Cloud Computing

THREATS IN CLOUD AND VIRTUALIZED ENVIRONMENTS

When organizations leverage cloud services, they rely on their cloud service providers (CSPs) to host, manage, and support all or part of the IT infrastructure. Depending on the provider and service, the CSP may support computing, storage, and even application infrastructure services. As organizations grow more reliant on cloud services and virtualized environments, data protection efforts continue to become increasingly complicated. When sensitive assets are housed in the cloud, they are susceptible to a range of risks:

- **Vulnerable to advanced attacks.** While CSPs typically establish strong controls around their data center infrastructure and network perimeter, these defenses continue to be proven vulnerable to advanced cyber attacks.

- **Potential exposure to CSP administrators and other tenants.** In virtualized cloud environments, a new set of privileged super users, such as hypervisor administrators, are introduced. These privileged users and others with access to shared cloud resources can potentially gain access to sensitive assets, and leave organizations exposed to data theft and sabotage.

- **Data proliferation and portability.** Compared to traditional server environments, in cloud and virtualized environments the portability of data expands dramatically. In these environments, data is constantly being duplicated and backed up, often leaving administrators with little control or visibility into where sensitive assets may reside at any given time.

THE REQUIREMENTS: DATA-CENTRIC SECURITY CONTROLS

To address the risks above, there's an urgent need for organizations to employ data-centric security controls. When moving data into the cloud, the scope of your data security mechanisms needs to expand. To establish trust in your cloud deployment, your organization must address the leading cloud security concerns and threats outlined above. To do so, you need to deploy strong solutions that deliver these capabilities:

- **Data encryption and key management.** To establish strong controls for sensitive data in the cloud, security teams must institute encryption of sensitive assets, while retaining control over the keys. Data encryption renders the data stored in the cloud unreadable if it is accessed by an unauthorized user. Only users that provide an encryption key can access the data in the clear.

- **Granular access controls.** To establish complete and persistent control, security teams need mechanisms to ensure that their organization's data is kept isolated from the CSP's administrators and the staff of other tenants sharing the cloud infrastructure. This requires granular access control policies that allow your organization to establish controls over who can access data, what data they can access and when, and how the data can be accessed. Through these policies, security teams can govern permissions for both business users and CSP administrator accounts.

- **Central management across environments.** Data encryption and access controls should be uniformly applied across all data on the premises of your company and across your private, public, or hybrid cloud deployments. This is vital to establishing consistent security policies and controls for your enterprise. Without a unified approach, security teams risk losing control and visibility of data as it moves to different environments, and the different systems and policies protecting these environments. These mechanisms are integral to guarding against an array of threats and sustaining compliance with the increasingly stringent industry and privacy mandates in effect. Further, they're vital to managing security in the most cohesive and efficient manner possible.

- **Complete visibility and auditability.** Once your enterprise data is stored in the cloud, your team must monitor, log, and report on data access activity by users and applications. These capabilities are essential in being able to demonstrate to auditors that requirements of compliance regulations like the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) are being met in the cloud. Further, all data access event activity should be recorded and available for detailed analysis. This is vital for helping staff more quickly detect any data access anomalies and more effectively thwart potential data breaches.

- **Persistent control of data in dynamic environments.** As organizations move sensitive data into the cloud, security teams have to be able to apply persistent protections, even as copies of data continue to be migrated and copied across the CSP's virtualized cloud environments. By encrypting sensitive assets and retaining control over cryptographic keys, your organization can effectively mitigate the risks of data proliferation in virtualized and cloud environments. When data sets no longer need to be retained in the cloud, your organization can destroy the associated cryptographic keys. This effectively digitally shreds all copies of the data, no matter where it may have been saved, so you can ensure that this information will never be accessed in the clear.

- **Unobtrusive implementation.** Data encryption and access controls must be transparent to users and minimize any disruption to existing processes, workflows, and infrastructures. In cloud environments, enterprise security teams must institute the controls needed to ensure CSP administrators can't get access to sensitive data, while at the same time ensuring these administrators can still perform their cloud infrastructure management functions.

When security teams can address these requirements, they can help support their organizations in moving more quickly and confidently into cloud environments.

THE SOLUTION: QTS DATA SECURITY FOR THE CLOUD

With QTS Data Security – powered by Vormetric's Data Security Platform – enterprise security teams can establish the controls they need to secure sensitive data, both across the enterprise and in the cloud. As a result, organizations can ensure their data remains in their control while leveraging all the benefits of the cloud.

The solution features capabilities for data-at-rest encryption, key management, privileged user access control, and data event tracking information. Through the platform's centralized policy and key management, customers can address security policies and compliance mandates across databases, files, and big data nodes—whether they're located in traditional infrastructures, virtualized environments, or private, public, or hybrid clouds.

The Vormetric Data Security Platform features the following services:

- **Key Management and Access Control.** The Data Security Manager (DSM) offers capabilities for centrally managing the Vormetric Data Security Platform. DSM enables centralized storage and management of host encryption keys, data access policies, administrative domains, and administrator profiles.

- **Data Encryption.** A data encryption agent runs in the file system to provide high-performance encryption and granular access controls for files, directories, and volumes.

- **Data Event Information.** Granular file access logs are captured and can be delivered to popular security information and event management (SIEM) systems.

Below are more service details to understand how they function and work together to provide the data security solution capabilities to secure data across the enterprise and in the cloud environment.

KEY MANAGEMENT AND ACCESS CONTROL

The Data Security Manager (DSM) centralizes control of the Vormetric Data Security Platform. DSM changes the data security game by enabling an IT organization to have a consistent and repeatable method for managing encryption, keys, access policies, and data event tracking information for all structured and unstructured data.

By delivering centralized control of a breadth of data-at-rest security capabilities and enabling application of those controls across all enterprise and cloud deployments, DSM provides low total cost of ownership, efficient deployment, and improved visibility and control. Further, once the DSM is in place, organizations can leverage these broad capabilities to quickly address new security mandates, compliance requirements, and emerging threats as they arise.

DSM enables you to assign specific infrastructure and policy management permissions to specific administrator groups across internal IT organizations and cloud service provider resources to fit your IT deployment scenario. In addition, the product employs a domain-based approach that enables security teams to segment and manage keys, policies, and users for specific groups or departments.

The DSM is available as a virtual or physical appliance with options to be FIPS 140-2 Level 3 compliant.

DATA ENCRYPTION

High-performance data encryption services enable enterprises to protect, control, and track sensitive data wherever it resides—including in the cloud.

The data encryption services are transparent to the user and performed by agents that run at the file system level on a server within cloud instances. These agents can encrypt structured and unstructured data and then enforce fine-grained, centrally managed access controls that help ensure that only authorized users and processes can decrypt data. They evaluate all attempts to access protected data, apply predetermined access control policies to either grant or deny data access, and log attempts. The data encryption service employs only standard-based encryption protocols, such as Advanced Encryption Standard (AES).

Data protection does not end after the encryption key is applied. The solution continues to enforce least-privileged user access policies, meaning users and administrators will be granted the level of access that they need—and nothing more. Further, the service continues to protect against unauthorized access by users and processes, and it continues to log access. With these capabilities, security teams can ensure continuous protection, monitoring and control of their organization's data.

With QTS Data Security, securing data is easy. Unlike other encryption offerings, this product offers a transparent approach, enabling security teams to implement encryption without having to make changes to their organization's applications, infrastructure, or business practices. The data encryption service achieves security with complete transparency to end users as well, helping minimize the cost and effort associated with implementing encryption.

DATA EVENT INFORMATION

Traditionally, Security Intelligence Event Management (SIEM) relied on logs from firewalls, intrusion prevention systems (IPS), 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 within your network or across your cloud deployments. The data access event information fills this blind spot, helping accelerate the detection of APTs and insider threats.

The information service provides logs that detail which processes and users have accessed protected data. Sharing these logs with a SIEM platform helps analysts uncover anomalous patterns in processes and user access, 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. These activities could point to an APT attack or malicious insider activities.

In order to adhere to many compliance mandates and regulations, many organizations must be able to prove that data security is in place and operational. The data event logs are commonly used to prove to an auditor that encryption, key management, and access policies are working effectively. The detailed logs are shared and 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 submits a command like "switch user" in order to attempt to imitate another user.

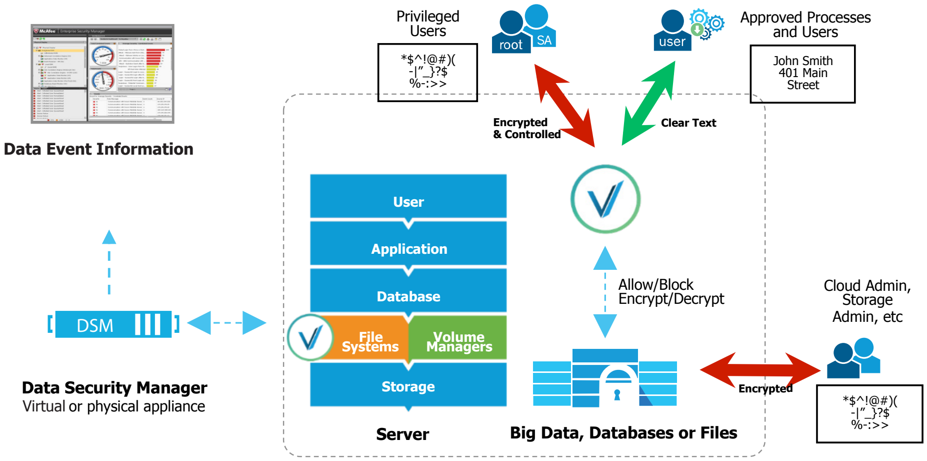


Figure 2. QTS DataAtRest Encryption deployment architecture

STRONG SEPARATION OF DUTIES AND FLEXIBLE KEY MANAGEMENT

The Vormetric architecture inherently offers solution capabilities that meet security best practices including the strong separation of duties of who can control the DSM device, create DSM administrators, and what rights each administrator has. In this way, no one administrator has complete control over the security of your data.

The DSM features a role-based approach, enabling the assignment of specific infrastructure and policy management permissions to three key administrator types: system administrator, domain administrator, and security administrator. (A domain is a group of one or more protected hosts and their associated keys and policies.)

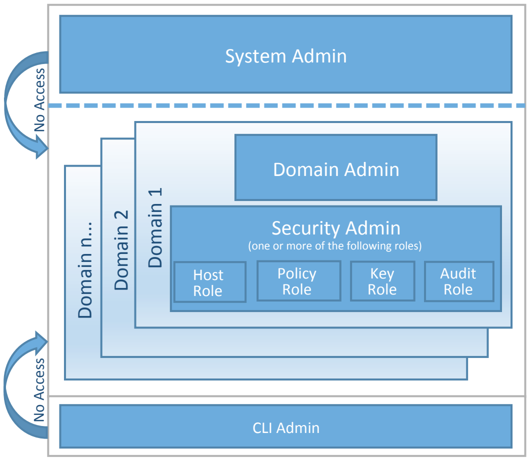


Figure 3. DSM Administration Roles

Here are the permissions and administrative tasks for each type of DSM administrator:

System Administrator	Top-level administrator who creates domains and administrator accounts, typically assigning at least one administrator to each domain. The system administrator has no visibility into domains or access to protected data.
Domain Administrator	Assigns all administrators, except the original administrator, to domains. The domain administrator assigns roles to security administrators. Domain administrators cannot remove users or domains and they can't access protected data.
Security Administrator	This administrator can perform roles that were assigned by the domain administrator. Each security administrator can be assigned different roles, and specific roles can be assigned for each domain. Through the assignment of roles, security administrators can be allowed to handle a range of tasks: • **Audit.** This role grants access to purge and export audit logs. • **Key.** This role enables the creation, modification, and removal of encryption keys. • **Policy.** This role enables administrators to create, modify, and remove policies. • **Host.** This role enables administrators to register hosts, apply access controls to file hierarchies, and modify hosts' audit configurations.

Figure 4. Permissions and administrative tasks for each DSM administrator type

The architecture allows the DSM to be deployed on-premises at an enterprise customer data center, or in the cloud enabling customers to retain key management controls desired while adapting to different distributed IT cloud deployment environments. The DSM can also serve as central key management for other KMIP compatible devices simplifying overall data security administration across your organization.

The Vormetric Data Security Platform is flexible and offers support for a number of deployment models, helping customers address a range of business, security, compliance and technical requirements across the enterprise and in the cloud.

CLOUD DEPLOYMENT MODELS

The DSM is a very flexible key and policy manager that can be deployed in the most convenient and cost effective manner. In this paper two deployment models are discussed to help you understand the model that best fulfills your needs.

The DSM architecture enables QTS to distribute administrative roles and responsibilities to different individuals in their respective organizations. In this way, customers can leverage outsourced cloud IT resources, while addressing security operating requirements, for example, in areas like key management. At the same time, these capabilities enable authorized QTS staff to perform their required administrative tasks.

Customers can work with their QTS staff to understand which DSM cloud deployment model below works best for their specific security, staffing, and operational environment. For the cloud deployment models below, the DSM domain and DSM security administrator roles are combined into a single DSM security administration role.

MODEL #1: CLOUD MANAGED DSM DEPLOYMENT MODEL

In this fully outsourced model, QTS hosts, manages, and controls all aspects of the DSM, and manages keys and access policies for customers. QTS hosts and manages the DSM in their cloud infrastructure. QTS' team members obtain the DSM system administration and security administration roles and they work with each customer to define, configure, and deploy keys and access policies in order to protect the customer data hosted in their cloud. The customer will have limited or no access to the DSM and will rely on QTS to implement and deploy the data security solution and policies so they meet any applicable data security service contract terms and conditions.

For customers with little or no IT resources, this model offers a practical way to protect cloud-hosted data. When employing this model, customers may choose to separate different roles depending on the CSP deployment options available. For example, they could allow QTS to create keys and policies, but only allow internal infrastructure administrators to deploy the policies on the cloud-hosted servers. DSM data event logs can be used to monitor and report on data security activity for compliance and audit purposes.

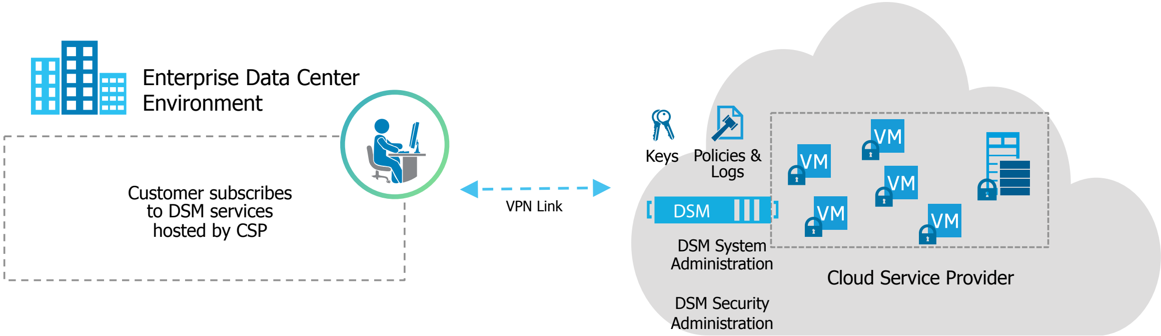

Enterprise Data Center Environment
Customer subscribes to DSM services hosted by CSP
VPN Link
Keys
Policies & Logs
DSM
VM
VM
VM
VM
VM
VM
DSM System Administration
DSM Security Administration
Cloud Service Provider

Figure 5. Model #1: QTS hosts, manages and administers the DSM for the customer

MODEL #2: CLOUD MULTI-TENANT DSM DEPLOYMENT MODEL

In this multi-tenant model, QTS hosts the DSM infrastructure for multiple customers. QTS hosts a high availability cluster of DSM appliances in their multi-tenant cloud infrastructure, and offers DSM-based services to multiple customers.

QTS' team members obtain the DSM system administration role needed to create DSM domains for each customer. Each customer will obtain a DSM security administration role in order to manage keys and access policies within their assigned domain. Within their domain, a customer will have their own DSM workspace, which they can use to set up their specific data security controls. By setting up and enforcing these domain-specific policies, customers can keep their data secure and isolated from QTS staff and other cloud tenants. QTS' staff is not allowed any DSM security administration privileges for any customer domains. The QTS extends secure VPN access for each customer, while ensuring a customer's DSM administrators can only access their organization's specific domain. As a result, customer data remains secure, while enabling the QTS to share the DSM appliance infrastructure and costs with other customers.

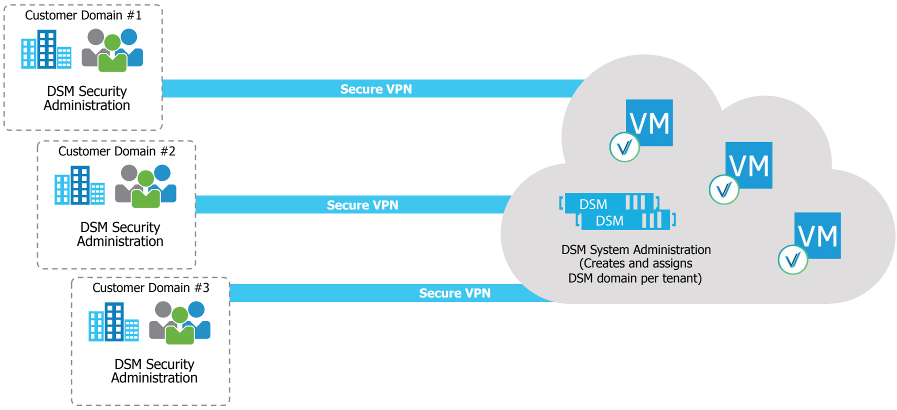

Customer Domain #1
DSM Security Administration
Customer Domain #2
DSM Security Administration
Customer Domain #3
DSM Security Administration
Secure VPN
Secure VPN
Secure VPN
VM
VM
VM
DSM
DSM
DSM System Administration (Creates and assigns DSM domain per tenant)

Figure 6. Model #2: QTS hosts DSM domains for each customer to administer keys and policies

In this multi-tenant model, customers can easily leverage the DSM to establish the data security controls they need to protect their cloud-hosted data. At all times, they maintain keys, access controls, and security administration roles within their assigned domain.

CONCLUSION

With QTS Data Security, your organization can employ a data security solution that enables you to secure your data, control data access, and stay compliant. With the solution, you can establish strong controls over your data and adopt a distributed cloud IT deployment model that fits your business needs across your enterprise and in the cloud. With these data security controls, you can confidently move your business' most valuable data into the cloud.

QTS Data Security delivers a flexible, highly available solution that offers robust capabilities for data encryption, access controls, key management, and event logging to protect your data uniformly wherever it resides. With the solution, you can work with QTS to address a range of cloud security requirements and your unique deployment needs. As a result, your company can reap a range of business benefits:

- More effectively guard against data breaches.
- More consistently address compliance mandates.
- Protecting your brand and reputation.
- Better safeguard customer privacy, loyalty, and trust.
- Focus on your core business by outsourcing data encryption and key management.

QTS Data Security is scalable, efficient, and simple to deploy and operate—making our offering an attractive data security solution to help enterprises secure their valuable data assets in the cloud.

Learn more about Vormetric at www.vormetric.com.

APPENDIX: FAQs

When moving sensitive and regulated data to the cloud, security management has to contend with a range of questions and concerns. Following are a few of the most common questions, and the answers:

Will I be able to establish strong security over sensitive data in the cloud?

With QTS Data Security, powered by Vormetric, you can employ robust encryption and key management in order to establish maximum security for your most sensitive assets. In addition to encryption and key management, the Transparent Encryption agent can enforce very granular least-privileged user access policies, enabling protection of data from misuse by privileged users and APT attacks.

How can I make sure authorized staff can work with the data they need, but keep it protected from all other users and administrators?

Enterprise security teams can establish privileged user access controls and access policies that govern who, what, when, and how data can be accessed. Granular policies can be applied by user, process, file type, time of day, and other parameters. Enforcement options can be used to control not only permission to access clear-text data, but what file system commands are available to a user. For example, a security team could institute a policy that enabled senior financial management to view personnel file, enable authorized human resources staff to modify and edit those files, and restrict access to all other individuals in the organization.

Will I be able to maintain control of data in virtualized cloud environments, where my data will be constantly copied and migrated to various physical and virtual machines?

By encrypting data and maintaining control over keys, your enterprise can maintain control over data, no matter where it is migrated or copied in the cloud environment. Even if copies of data are produced that security administrators don't know about, the data will not be useable to any unauthorized users.

How can we institute strong separation of duties in the cloud, so we can comply with our security policies and compliance mandates?

When QTS Data Security is deployed, access control management is done in the DSM, while data access enforcement is done on the data encryption agents residing on hosts in the cloud. This separation helps ensure that no one person has complete control over the security of data.

Through its role-based administrative architecture and support for domains, DSM enables separation of duties between data owners, server administrators, and security administrators. As a result, security teams can establish the granular privileges and access controls that enable strong, auditable security of sensitive data in a range of environments.

Will I be able to establish enterprise ownership of cryptographic keys?

DSM enables you to administer and control the keys and access policies for all the data encryption agents across your enterprise. These policies enforce least privileged access to your data. As a result, your enterprise can own the keys—and so who can access encrypted data—even when your data is stored in the cloud.

Will our administrators and the QTS administrators still be able to complete their tasks, or will encryption break their workflows?

Data encryption encrypts sensitive data, while leaving file metadata in the clear. As a result, administrators can do their ongoing tasks, without gaining access to clear-text data.

What if I want to secure data in our data centers as well as in cloud environments?

With Vormetric Transparent Encryption, security organizations can safeguard critical data in the enterprise, as well as private, public, and hybrid cloud environments. The solution encrypts data at the file system or volume level within virtual machines and applies fine-grained, centrally managed policies to control access to protected data across your enterprise and cloud environments.

How can we make sure our data isn't exposed to unauthorized third-party access?

By separating DSM key management administration from data storage, you can ensure your data remains protected from unauthorized third-party access, even if the cloud provider receives a government subpoena demanding access to your data.

If a service is turned down or the data is no longer required, deleting a key digitally shreds the data so no one can access the data in the clear again.

How can I be sure my data won't be exposed to other tenants in a multi-tenant cloud environment?

With QTS Data Security, your organization retains control over keys at all times. Through the DSM's support for domains, QTS establishes isolated partitions for multiple clients. As a result, you can still ensure that only your authorized users will be able to access keys, and so only those users will be able to access encrypted data in clear text.

When we have sensitive data in the cloud, how will we identify data access anomalies and demonstrate compliance for auditors?

QTS Data Security provides security information and visibility by logging details about all users and application processes attempting to access your files. Detailed event logs and monitoring reports alert you to any anomalies and demonstrate that security controls are being enforced in the cloud environment. In addition, these security event logs can be uploaded to SIEM applications so you can gain a holistic view of the organization's data security status. Detailed reporting capabilities enable your organization to comply with applicable regulations and provide audit documentation.

What impact will encryption have on performance?

Data encryption agents are distributed across the server infrastructure. As a result, the product delivers scalability and eliminates the bottlenecks and latency that plague proxy-based solutions.

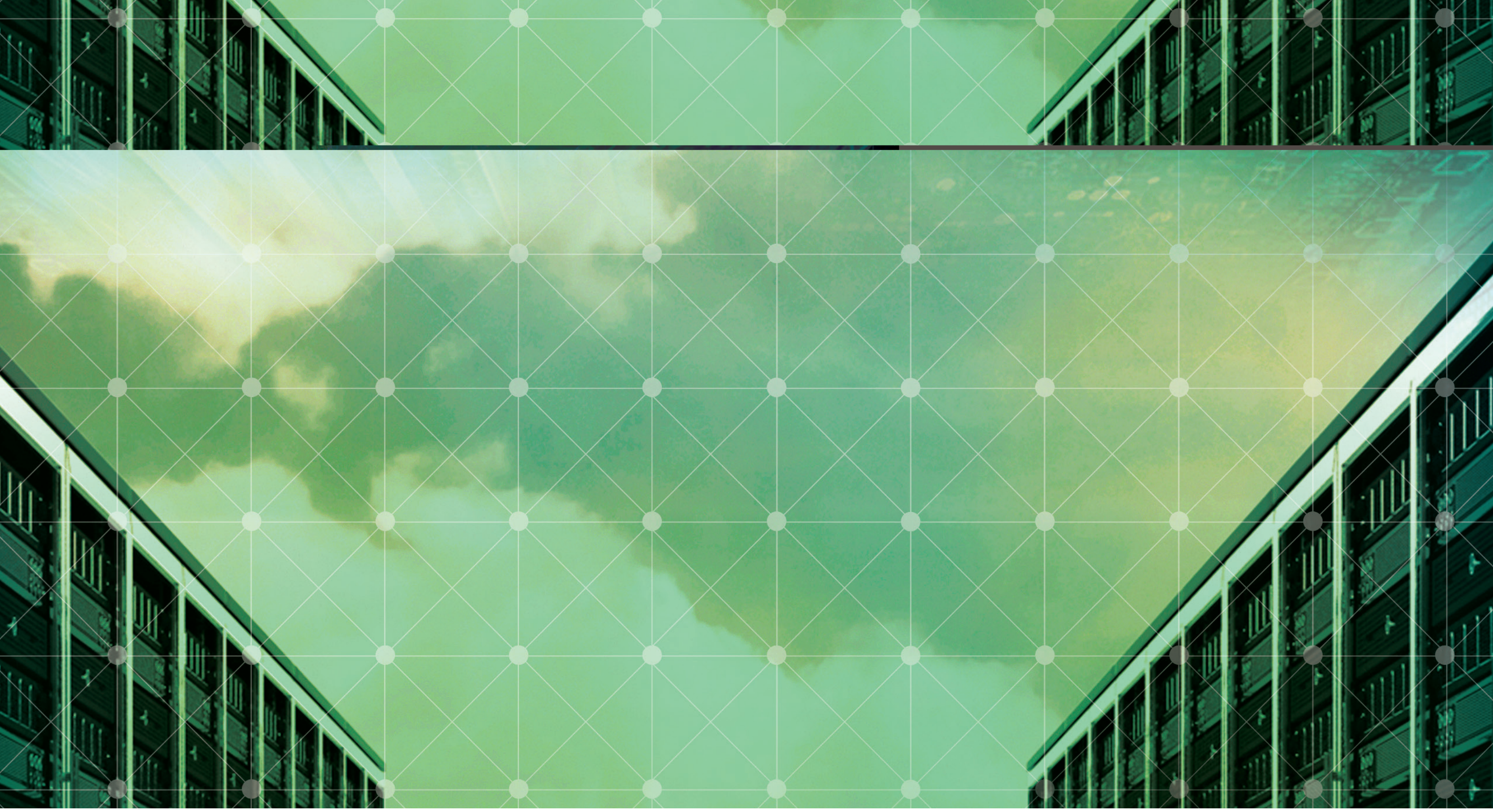
ABOUT QTS

QTS Realty Trust, Inc. (NYSE:QTS) is a leading provider of secure, compliant data center solutions and fully managed services, and the owner of Carpathia Hosting, a leading provider of hybrid cloud services and managed hosting. QTS' integrated technology service platform of custom data center (C1), colocation (C2) and cloud and managed services (C3) provides flexible, scalable, secure IT solutions for web and IT applications. QTS' Critical Facilities Management (CFM) provides increased efficiency and greater performance for data center owners and operators. QTS owns, operates or manages 25 data centers and supports more than 1,000 customers in North America Europe and Asia Pacific.

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual, big data, and cloud environments. With data at risk as never before, Vormetric helps over 1500 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.

QTS® | Vormetric Cloud Partner™



QTS®

Vormetric Cloud Partner™