VORMETRIC

Vormetric Data Security

Securing and Controlling Data in the Cloud

Vormetric, Inc.
Tel: 888.267.3732
Email: sales@vormetric.com

www.vormetric.com

VORMETRIC

Table of Contents

VORMETRIC

Executive Summary

Enterprises are embracing the compelling economic and operational benefits of cloud computing. By virtualizing and pooling computing resources, enterprises can reduce operational costs and accelerate the deployment of new applications and services. While cloud computing does not change the fundamental principles of information security, taking advantage of cloud computing's benefits requires reconsideration of how enterprises maintain security of data in the cloud model.

Deploying sensitive information and critical IT resources into the cloud raises concerns about data security, especially when one considers the loss of custody for data in the cloud. Applications and data can reside adjacent to a potentially hostile environment, risking theft, unauthorized exposure or malicious manipulation of information.

As an established leader in high-performance data encryption solutions, Vormetric enables enterprises to leverage the cloud while maintaining control and security around sensitive data. Vormetric Data Security enables enterprises to protect and govern data in physical, virtual and cloud environments so that enterprises can take advantage of cloud computing's benefits while minimizing security risks.

"In order for organizations to move computing resources and applications to the cloud, the value must exceed the risk. The risks of cloud migration are largely captured in one word — 'security'. Half of the organizations that are not adopting cloud computing cite security as the reason. As cloud adoption moves to the mainstream and expands from tactical uses to strategic platforms, enterprises will need to address cloud security and compliance issues more holistically. This will be especially true as organizations look to use cloud in cases where highly sensitive data is involved, where rigorous compliance requirements apply, or for business-critical applications."

Forrester Research, Inc.
"Security And The Cloud", 20 October 2010

Cloud Computing Definitions

Cloud computing is the latest step in evolution of distributed computing that takes advantage of technology innovations and the internet evolution. It provides convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly provisioned and released with minimal management effort or cloud provider interaction.

Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The security challenges cloud computing presents, however, are formidable, especially for public clouds whose infrastructure and computational resources are owned by an outside party that sells those services to the public.

The US National Institutes of Standards and Technology (NIST) recently published a definition of cloud computing[1] that provides a useful model for the cloud that has been widely accepted in the IT industry.

1. NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (January 2011)

VORMETRIC

Service Models—SaaS/PaaS/IaaS

The NIST model provides for three service models and four different deployment models (sometimes referred to as cloud formations).

Software as a Service

Software-as-a-Service (SaaS) is capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. The cloud service provider typically takes responsibility for data security in this model, but the enterprise is ultimately accountable and needs to review security practices. Prime examples of SaaS include Salesforce.com and Google Apps.

Platform as a Service

With Platform as a Service (PaaS), the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. The cloud service provider usually takes responsibility for much of data security in this model, but this can be a shared responsibility for some PaaS vendors. Examples of PaaS include Microsoft™ Windows Azure, Salesforce.com Force.com, and Google App Engine.

Infrastructure as a Service

Using Infrastructure-as-a-Service (IaaS), the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). Data security is typically a shared responsibility between the cloud service provider and cloud consumer in this model. Examples of IaaS include Amazon Elastic Cloud Computing (EC2), Terremark, and Rackspace.

Deployment Models[2]

Private Cloud
Operated solely for a single organization. It may be managed by the organization or a third party and may exist on-premise or off-premise.

Community Cloud
Shared by several organizations in support of a specific community that has shared concerns (e.g. business need, policy, compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public Cloud
Made available to the general public or a large industry group. Owned by an organization selling cloud services.

Hybrid Cloud
A composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

2. NIST Definition of Cloud Computing , http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (January 2011)

Cloud Computing Security Challenges

The traditional security model of a hardened perimeter around the datacenter protecting everything inside the "glass house" has eroded with the advent of virtualization and cloud computing. Virtual servers and the data they contain can now be easily moved between locations inside the enterprise perimeter or in the public cloud. This dynamism poses new security challenges as enterprises strive to protect and control access to their sensitive data.

Understanding Your Data

Understanding what information needs to be protected ensures that security budgets are optimally invested to focus on data that must be protected. This can involve considering the data being deployed in the cloud and what information needs to be protected.

A traditional datacenter had a perimeter that protected everything inside the perimeter, but that perimeter is becoming permeable and enterprises need to decide what needs protecting. In general terms, data can be considered to be either sensitive or non-sensitive. Compromising non-sensitive data can have few negative consequences and typically does not require the safeguards required for sensitive data. If your organization does not mind information being published in the newspaper or an embittered former employee's website, it is probably non-sensitive information.

Sensitive data typically falls into one of two categories: confidential data and regulated data.

Confidential data is comprised of information such as intellectual property, confidential business information or trade secrets. While a compromise of such data may not result in regulatory fines or legal sanctions, it can result in lost revenues, diminished trust, reduced competitive advantage, damaged reputations and other negative consequences.

Regulated data is confidential data that is governed by government regulations such as Sarbanes-Oxley (SOX), Graham-Leach-Bliley Act (GLBA), US Health Insurance Portability and Accountability Act (HIPAA), UK Data Protection Act, US state data breach laws or by industry rules such as the Payment Card Industry Data Security Standard (PCI DSS). Enterprises need to take security measures to comply with the law, avoid fines or legal sanctions. Sensitive data in the cloud, whether confidential or regulated, needs to be secured and enterprises need to ensure that there are no residual remnants when they eventually decide to move to another cloud service providers.

VORMETRIC

Isolation in Multi-tenant Environments

The world of one application inside one physical computer has rapidly changed with the advent of virtualization and cloud computing. Enterprises have embraced virtualization that enables one physical server to host multiple virtual machines (VMs) and enterprises are extending this concept to embrace cloud service models which have multiple tenants sharing the same infrastructure, be it SaaS, PaaS or IaaS. While cloud providers have an interest in sharing resources to make their economic model work, cloud customers have an interest in isolation and security of their data. The risk of this model is that cloud customers are sharing the infrastructure with "strangers", and some of the "strangers" could be careless, ignorant, or hostile. Similar to a tenant renting space in a building, the cloud consumer needs to ensure that the contents of their space is separated and secured.

Information residing in a common storage environment risks compromise due to lax management or malicious attacks. The Open Web Application Security Project (OWASP) project on "Multitenancy and Physical Security" highlighted multi-tenancy risks including:

- Inadequate Logical Security Controls
- Malicious or Ignorant Tenants
- Shared Services can become single point of failure
- Uncoordinated Change Controls and Misconfigurations
- Co-mingling of Tenant Data
- Performance Risks
- SaaS/PaaS/IaaS-specific risks such as sharing the platform stack.

Controlling Data Movement

Data moving from direct-attach storage into a virtual and cloud world has become particularly portable and mobile. Storage administrators can replicate storage and reassign information across datacenters for the purposes of availability, disaster recovery, or maintenance with little or no notice to information owners. In the public cloud, cloud providers follow operational best practices and must routinely replicate data for availability purposes. For example, Amazon Web Services (AWS) Elastic Block Store[3] (EBS) provides that "Each storage volume is automatically replicated within the same Availability Zone. This prevents data loss due to failure of any single hardware component." Such replicated data needs to be secured from prying eyes.

Data mobility can also cause legal complications. Regulations such as the EU Data Privacy Directive forbid data processing or storage of an EU residents' data within foreign data centers. Controls must be applied to data in cloud computing environments to avoid inadvertently breaking such rules by migrating regulated data across national borders. In addition, the USA PATRIOT Act allows US Federal agencies to use subpoenas to compel providers to provide data (which can include trade secrets or sensitive electronic conversations) without informing or gaining data owner's consent.

3. Amazon Elastic Block Store webpage, http://aws.amazon.com/ebs/ (March 2011)

VORMETRIC

Maintaining Data Privacy

Data breaches have proven to be embarrassing and costly for enterprises, and the prospect of data being lost in a public cloud has been a major inhibitor to cloud computing adoption. Data breach laws in US states such as Massachusetts, California and Nevada have put the burden on enterprises to ensure the security of customer or citizen data and or face significant fines over data breaches. Data breaches also pose the risk of damaged corporate and organizational reputations, an asset that can take years to repair following an unauthorized disclosure.

Maintaining Separation of Duties

Separation of duties (SoD) as a security principal is focused on avoiding fraud and reducing risk by segregating duties or tasks. As enterprises extend operations to the cloud, SoD changes to ensure that IT operations, IT security and cloud management duties are separated to establish the necessary checks and balances and minimize the possibility of fraud or misuse. While application developers are embracing the cloud to get their jobs done more quickly and cost-effectively, security processes need to be established to ensure that sensitive information is protected against prying eyes. This might mean that an IT administrator can only backup/restore files while the application developer has the privilege to manipulate data. Excess authority in the hands of one party risks a careless or rogue employee taking actions that result in compromised data.

Information Persistence: Residual Data After You Depart

Recycling of storage resources is a common practice in cloud computing and essential to leveraging the economies of scale promised by the cloud, but no clear standard exists around how cloud service providers securely recycle disk space and erase existing data. The cloud tenant faces the risk that after releasing the storage they have used, the next tenant might be able to see fragments of residual data if storage is not securely recycled.

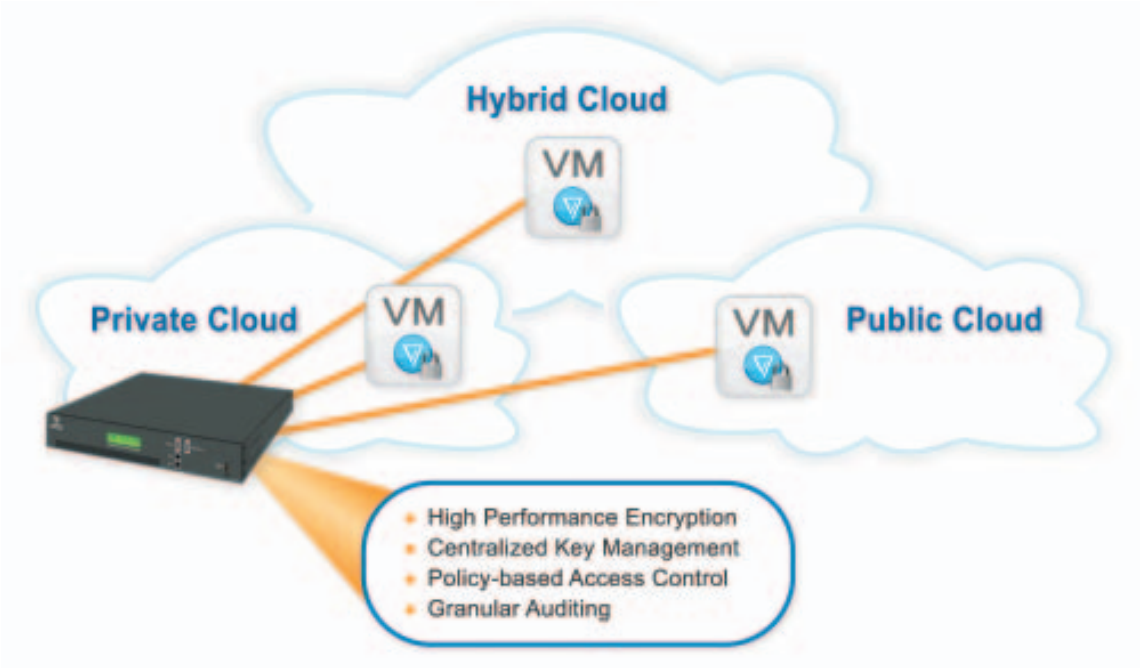
Auditing, Reporting, and Compliance

While cloud computing opens up new horizons in reducing costs and rolling out applications more quickly, it does not obviate the need for standard IT policies around auditing and reporting. As enterprises consider moving applications with sensitive or regulated data into the cloud, they need to ensure that they achieve equal or superior levels of auditing and reporting so that they can reduce the scope of audits and satisfy regulatory requirements.

VORMETRIC

Overcoming Cloud Security Challenges: Vormetric Data Security

Vormetric Data Security helps to alleviate security and data governance concerns surrounding cloud computing using the same encryption, policy and key management and reporting that enterprises use today for securing on-premise data. By securing data with encryption and controlling the security policies around data usage, Vormetric allows organizations to overcome the cloud security challenges of multi-tenancy, data privacy, data remanence, separation of duties, and reporting. Vormetric protects data and controls access no matter whether the data is located - in private, public or hybrid clouds.



Rapid Deployment

Vormetric Data Security transparently encrypts data without requiring application or database redesign or recoding. Enterprises can rapidly deploy cloud applications with encryption of specific files in place. Inserted above the file system and logical storage volume layers, Vormetric Data Security is transparent to users, applications, and cloud storage. No modification to the application or database is required, enabling enterprises to leverage cloud agility with security. In IaaS environments like Amazon EC2, enterprises can spin up EC2 instances to encrypt structured and unstructured data without re-architecting or recoding applications.

VORMETRIC

Centralized Key and Policy Management

Insider threat issues, such as those posed by WikiLeaks, and increased audit scrutiny are driving greater focus on how enterprises manage the security of their data. While data is protected in the cloud, Vormetric Data Security allows enterprises to directly maintain control over key and policy management through a FIPS-validated system that can ensure the custody and security of encryption keys needed for regulated data. In addition, the solution's granular auditing provides immediate insight into cloud data access, highlighting potential security issues and providing essential information to auditors. Using an on-premise hardware appliance, the Vormetric Data Security solution delivers a single system to protect all sensitive enterprise data residing in physical, virtual and cloud environments.

Enforcing Separation of Duties

The cloud poses new security challenges for maintaining Separation of Duties (SoD) between IT Operations, IT Security and cloud management. While the cloud can speed development and deployment of new applications, the cloud can also pose security risks if the SoD security discipline used in the physical and virtual world is not expanded to the cloud. Vormetric Data Security enforces SoD by allowing developers do their work in developing and deploying applications in private cloud or Infrastructure-as-a-Service environments while IT Security establishes and enforces policies around data access via the Vormetric Data Security console. This approach ensures that policies are enforced and avoids the possibility that operational or cloud staff accidentally "turn off" policies.

Precise, Granular Encryption

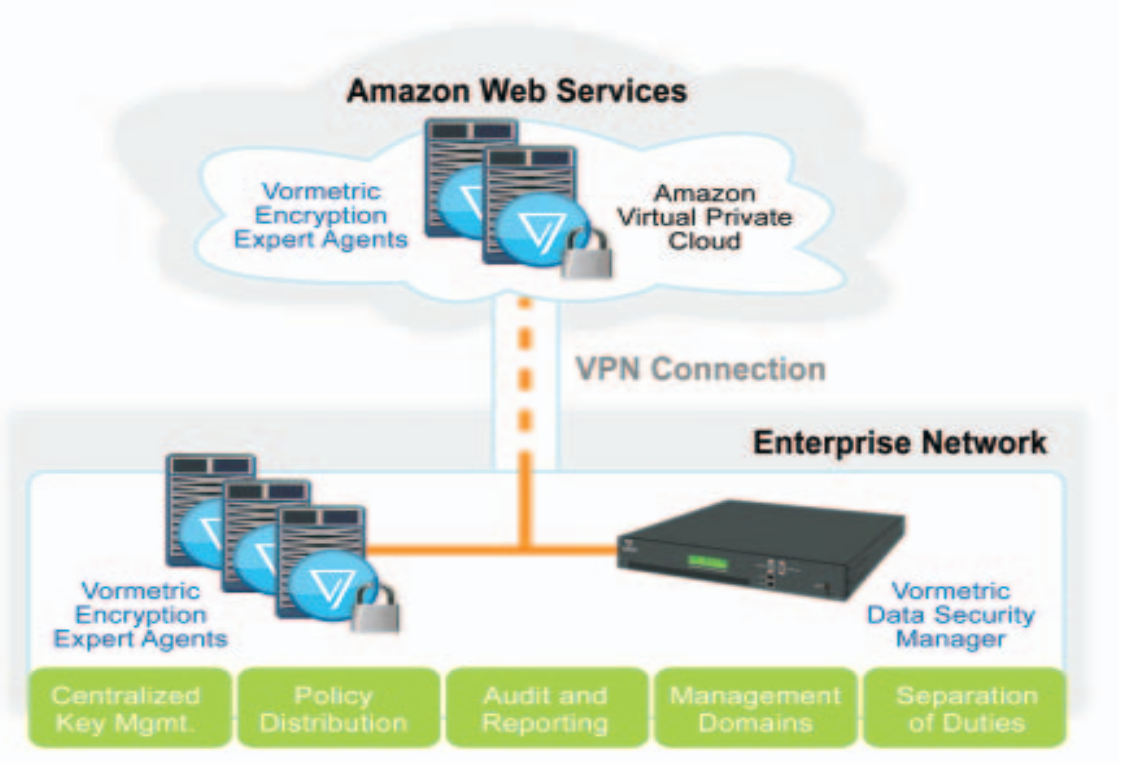
To overcome the limitations of volume-level cloud encryption solutions that only provide control over a storage volume, Vormetric operates at a granular file level to enforce encryption, enable access control policies and audit usage at the server, process and user layers. This approach extends the security value of encryption beyond simple media theft protection and allows enterprises to address insider threat, separation of duties and gain insight into access activity for data in the cloud. IT administrators can mount storage volumes, but cannot access data unless the policy established via the Vormetric console permits such access.

While encrypting mounted storage volumes in the cloud allows some control of data, it provides limited Separation of Duties functionality and risks policy non-compliance since all files and folders are available once a storage volume is mounted by a server instance. Similar to full disk encryption of laptop computers, encrypting a mounted storage volume can help safeguard against lost data, but does little to control data access by individuals once the storage volume is mounted. Anyone with access to the server can read and manipulate data. By encrypting specific files and folders and delivering robust logging of data access, Vormetric provides data security along with granular access control at the file/user/process level, control that is unavailable with a volume-level encryption providing a simple "on/off switch". Vormetric not only protects data at rest, but also ensures that trusted users such as administrators can perform their duties without reading the actual data.

VORMETRIC

Portability from Physical to Virtual To Cloud Environments

Evolving business requirements are causing enterprises to consider moving data between private and public clouds, driving a need for data centric controls that travel with data. Vormetric addresses this need through an encryption and access control policy model that can automatically follows data. This capability eliminates redundant policy stores for on-premise/private cloud and public cloud infrastructures, while ensuring consistent enforcement of security standards and adherence to compliance requirements wherever the data resides. Data can be secured with encryption whether distributed in a physical, virtual or cloud environment like Amazon EC2 (see diagram).



Management Simplicity – One solution for all environments

Managing encryption has proven problematic with pools of discrete encryption that can consume increasing amounts of time. Vormetric's approach is to provide a single console that can manage encryption policies and keys and generate audit reports across a broad variety of operating systems, irrespective of whether data is located in physical, virtual or cloud environments. The Vormetric approach logs only access requests that require attention or retention (e.g. denied access attempts and certain permitted activity) to avoid burdening security staff with superfluous event data.

VORMETRIC

Conclusion

As enterprises plan to deploy applications in private and public cloud environments, new security challenges need to be considered. When enterprises look to deploy applications using sensitive data in the cloud, they need to consider how to secure the data and apply policies for the cloud similar to what already exists in their physical and virtual environments. Some best practices to protect such information includes encrypting sensitive data, establishing appropriate separation of duties between IT operations and IT security, and ensuring that the use of cloud data conforms with existing enterprise policies.

Vormetric Data Security enables businesses to apply a consistent and rigorous set of data encryption and governance policies across physical, virtual and cloud environments. By controlling how, where, and by whom data is accessed, Vormetric enables enterprises to take advantage of cloud economics while maintaining the necessary security and control. Vormetric Data Security protects information against theft of illicit manipulation, and helps ensure compliance with encryption requirements. Vormetric provides a complete solution for enterprises seeking to safeguard information in physical, virtual, private cloud and public Infrastructure-as-a-Service environments.

For more information about Vormetric, please contact us at
+1 (888) 267-3732 or sales@vormetric.com