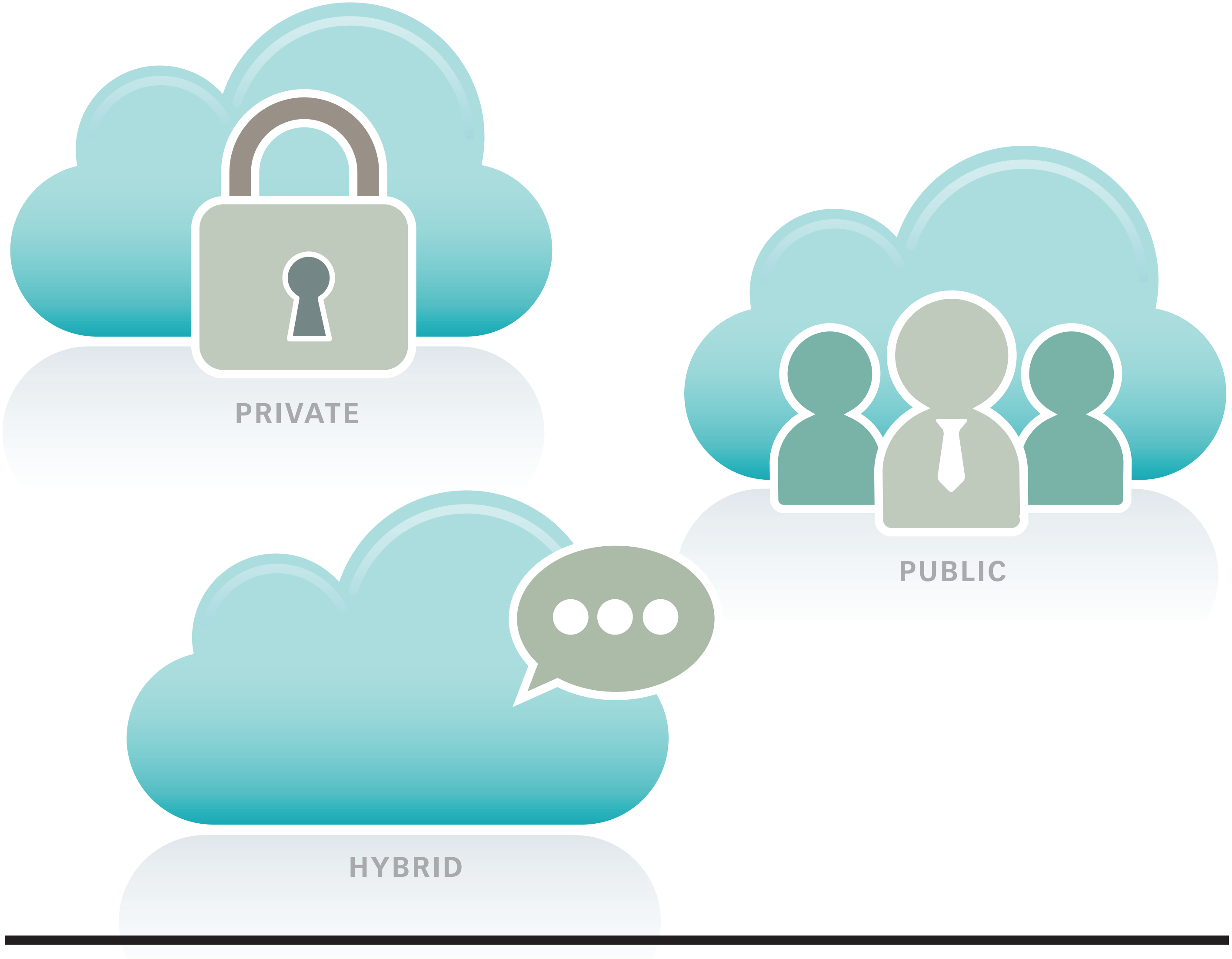

Data Security in the Cloud

PROTECTING BUSINESS-CRITICAL INFORMATION IN PUBLIC, PRIVATE, AND HYBRID CLOUD ENVIRONMENTS

CSO
Custom Solutions Group

Vormetric
Data Security Simplified

Executive Summary:

Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. 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 cloud computing landscape continues to realize explosive growth. The worldwide public cloud services market was projected to grow nearly 20 percent in 2012, to a total of $109 billion, with 45.6 percent growth for Infrastructure as a Service (IaaS), which is the fastest growing market segment.[1]

Yet for security professionals, the cloud presents a huge dilemma: How do you embrace the benefits of the cloud while maintaining security controls over your organizations' assets? It becomes a question of balance to determine whether the increased risks are truly worth the agility and economic benefits.

Maintaining control over the data is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity.

[1] Gartner Inc., "Worldwide Cloud Services Market Is Expected to Surpass $109 Billion in 2012," press release, September 18, 2012

This shift in control is the number one reason new approaches and techniques are required to ensure organizations can maintain data security. When an outside party owns, controls, and manages infrastructure and computational resources, how can you be assured that business or regulatory data remains private and secure, and that your organization is protected from damaging data breaches—and feel you can still completely satisfy the full range of reporting, compliance, and regulatory requirements?

This white paper describes:

- Cloud Computing Security Challenges
- Techniques for Protecting Data in the Cloud
- Strategies for Secure Transition to the Cloud

◗ Cloud Computing Security Challenges

Data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic value, reports the 2012 *Computerworld* "Cloud Computing" study, which measured cloud computing trends among technology decision makers.

When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often uneasy about granting them visibility into sensitive data.

Derek Tumulak, vice president of product management at Vormetric, explains, "Everyone wants to use the cloud due to cost savings and new agile business models. But when it comes to cloud security, it's important to understand the different threat landscape that comes into play."

There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data

Such issues give rise to tremendous anxiety about security risks in the cloud. Enterprises worry whether they can trust their employees or need to implement additional internal controls in the private cloud, and whether third-party providers can provide adequate protection in multitenant environments that may also store competitor data. There's also ongoing concern about the safety of moving data between the enterprise and the cloud, as well as how to ensure that no residual data remnants remain upon moving to another cloud service provider.

Unquestionably, virtualized environments and the private cloud involve new challenges in securing data, mixed trust levels, and the potential weakening of separation of duties and data governance. The public cloud compounds these challenges with data that is readily portable, accessible to anyone connecting with the cloud server, and replicated for availability. And with the hybrid cloud, the challenge is to protect data as it moves back and forth from the enterprise to a public cloud.

Specific security challenges pertain to each of the three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

◗ **SaaS** deploys the provider's applications running on a cloud infrastructure; it offers anywhere access, bu-t also increases security risk. With this service model it's essential to implement policies for identity management and access control to applications. For example, with Salesforce.com, only certain salespeople may be authorized to access and download confidential customer sales information.

◗ **PaaS** is a shared development environment, such as Microsoft™ Windows Azure, where the consumer controls deployed applications but does not manage the underlying cloud infrastructure. This cloud service model requires strong authentication to identify users, an audit trail, and the ability to support compliance regulations and privacy mandates.

◗ **IaaS** lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. As with Amazon Elastic Compute Cloud (EC2), the consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared respon¬sibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data.

> "Everyone wants to use the cloud due to cost savings and new agile business models. But when it comes to cloud security, it's important to understand the different threat landscape that comes into play."
>
> —DEREK TUMULAK, VORMETRIC

Meanwhile, conventional security considerations must be addressed in the cloud environment. These include implementing best practices and real-time security intelligence, protecting data security, and preventing advanced persistent threats (APTs) or attacks that exploit social engineering. It's also critical to plan for the added risks posed by big data mined across different cloud environments and mobile devices that store information in the cloud infrastructure.

Techniques for Protecting Data in the Cloud

Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks.

Many enterprises use database audit and protection (DAP) and Security Information and Event Management (SIEM) solutions to gather together information about what is happening. But monitoring and event correlation alone do not translate into data security.

At a time when regulation and compliance issues are at an all-time high, it's dangerous to assume that monitoring, collecting, and storing logs can protect the organization from security threats, as they are reactive controls. In today's environment, both data firewalls and data security intelligence are essential to adequately protect the enterprise from new and different types of attacks.

It's critical that CISOs implement a data security strategy that provides a veritable firewall around the data itself for comprehensive protection. Advanced data security solutions provide CISOs with an early warning system about an attack, render the content unusable, and leverage automation and big data analytics to continu¬ously analyze logs and other information about their environment such as security events and data flow.

While many organizations have implemented encryption for data security, they often overlook inherent weaknesses in key management, access control, and monitoring of data access. If encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers. Vulnerability also lies in the access control model; thus, if keys are appropriately protected but access is not sufficiently controlled or robust, malicious or compromised personnel can attempt to access sensitive data by assuming the identity of an authorized user.

The encryption implementation must incorporate a robust key management solution to provide assurance that the keys are sufficiently protected. It's critical to audit the entire encryption and key management solution. Encryption works in concert with other core data security technologies, gleaning increased security intelligence, to provide a comprehensive multilayered approach to protecting sensitive data—and mitigate risk in or out of the cloud.

Therefore, any data-centric approach must incorporate encryption, key management, strong access controls, and security intelligence to protect data in the cloud and provide the requisite level of security. By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently than by focusing exclusively on traditional network-centric security methods.

The strategy should incorporate a blueprint approach that addresses compliance requirements and actual security threats. Best practices should include securing sensitive data, establishing appropriate separation of duties between IT operations and IT security, ensuring that the use of cloud data conforms to existing enterprise policies, as well as strong key management and strict access policies.

"It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility," says Tumulak. He emphasizes that an effective cloud security solution should incorporate three key capabilities:

- Data lockdown
- Access policies
- Security intelligence

First, make sure that data is not readable and that the solution offers strong key management. Second, implement access policies that ensure only authorized users can gain access to sensitive information, so that even privileged users such as root user cannot view sensitive information. Third, incorporate security intelligence that generates log information, which can be used for behavioral analysis to provide alerts that trigger when users are performing actions outside of the norm.

"As we go forward and think about how applications are secured in the cloud, the application should be designed so you don't know whether it is running in the cloud or your own infrastructure," says Tumulak. "The underlying platforms and solutions of the future that these applications run on will have cloud security built right into the DNA of the framework."

> "It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility."
>
> —DEREK TUMULAK, VORMETRIC

In the future, Tumulak anticipates greater pressure for increased data security as the cloud comes more into the mainstream. He predicts increased organizational cooperation, greater standardization, and certification requirements.

Strategies for Secure Transition to the Cloud

The fundamental key to data security is to protect what matters. Solutions that enable companies to confidently transition to the cloud while still leveraging many of their traditional infrastructure and investments offer significant advantages.

Vormetric Data Security solves the enterprise cloud security conundrum by protecting data inside of the operating environment while establishing security policies and maintaining control through a centralized management interface. One key differentiator is that Vormetric works with cloud providers and enterprises to protect data regardless of whether it is located in physical, virtual, or cloud environments. This architecture enables enterprises to control access to the data itself, even as the virtual machine migrates to the virtual and cloud world. Organizations can establish access policies and achieve complete control of data in private, public, or hybrid cloud environments.

By providing a solution that protects both data and encryption keys, Vormetric Data Security provides the necessary safeguards to keep companies from facing breach notifications, and protects their most valuable business assets—their customers, brand, and the bottom line.

When transitioning to the cloud, only Vormetric offers a complete platform for protecting both local data within the internal environment as well as cloud-based data within infrastructure or hosted application sites. Unique to the solution is the combination of protection for both structured data (transparent encryption within databases) and unstructured data (encryption for files, file systems, volumes, big data repositories, and more) as well as fine-grained user and process access controls that guard against unauthorized access to protected data (even by administrators). A secure repository (or vault) also provides reporting, alerts, and FIPS 140-2 levels 2 and 3 protection for encryption keys. Vormetric Data Security even provides critical security intelligence information to SIEM solutions to allow identification of unusual and unauthorized access patterns that may represent a threat. No other offering provides a single solution to all of these problems, across all of these environments.

Vormetric Data Security transparently secures data without requiring application or database redesign or recoding, and is transparent to users, applications, and cloud storage because it is inserted above the file system and logical storage volume layers. Enterprises can rapidly deploy data security for cloud applications. Since no modification to the application or database is required, enterprises can securely leverage cloud agility. In IaaS environments such as Amazon EC2, IBM SmartCloud, Savvis, Rackspace, etc., enterprises can spin up instances to encrypt structured and unstructured data without rearchitecting or recoding applications.

For more information, visit
http://www.vormetric.com/data-security-solutions/overview/index.html

IaaS User Case: Virtustream

Virtustream, a leading enterprise-class cloud software and IaaS provider, has partnered with Vormetric to add database encryption and key management to its xStream cloud solution for enterprise compliance requirements. With this extra protection, Virtustream's xStream cloud management software and Virtustream cloud IaaS services provide highly secure and compliant solutions that enable enterprises, governments, and service providers to safely run mission-critical applications in private, public, and hybrid clouds.

"It can be challenging to get large enterprises to trust the cloud, so this partnership with Vormetric provides a significant security measure required to overcome that concern," says Pete Nicoletti, director of security and compliance at Virtustream.

The company now offers Vormetric's database and file encryption solution to customers needing an additional layer of security to satisfy internal sensitive data policies and compliance mandates regarding business data. For enterprises required to comply with regulatory guidelines and compliance frameworks such as NIST 800-53, DIACAP, FedRAMP, FISMA, ICD503, G-Cloud, CSA Recommendations, ISO27001, HIPAA/HITECH, PCI, SSAE16/SAS70, and other industry standards, this new service provides a sophisticated approach to protecting highly sensitive data in the cloud.

Nicoletti explains, "With Vormetric's solution, we now have a database encryption security option suitable for customers who are required to comply with executive mandates or compliance frameworks, but have not yet deployed encryption at their database or application layer. Adding this capability will make moving mission-critical data to the cloud a more feasible option for any enterprise looking for immediate risk reduction and cost savings."

With this encryption service, Virtustream also offers and manages encryption of client databases at their location in the client's data center before they even move the workload to the Virtustream cloud. This capability allows customers concerned with protecting personally identifiable information (PII) and other sensitive information to achieve regulatory compliance and avoid potential data breach costs.

"By partnering with Vormetric, we are able to combine its nimble and powerful security solution with our cloud solution for increased data protection with high performance and low overhead," says Mike Olson, vice president of operations and service delivery for Virtustream. "Together, we offer customers a more secure, compliant cloud environment with reduced infrastructure costs, and increased performance and uptime."