Technical white paper

HP Atalla Cloud Encryption

Securing data in the cloud

Table of contents

A cloud majority world

We are rapidly moving towards a cloud majority world, but the problem of full trust remains unresolved.[1] In applying encryption to protect sensitive data, the most crucial secret is the encryption key itself. For organizations moving workloads to the cloud, e.g., public clouds, retaining ownership and control of encryption keys while realizing the benefits of the cloud are often competing concerns.

Protecting data in the cloud

While more than half of those using the public cloud are confident that critical and sensitive data can be secured in the public cloud, security breaches are a reality in the cloud. Of the companies in the cloud surveyed, 16 percent reported at least one public cloud breach in the past 12 months.[2]

There are many compelling reasons to migrate applications and data to private or public clouds: scalability, agility, cost savings—to name a few. But along with benefits come increased risks to the safety of business-critical data. Any organization that is migrating data to the cloud needs to manage the risk to data at rest with a robust solution for data encryption and encryption-key management.

Securing data—at rest and in use—is simpler when the data is located within the four walls of a data center. Once data is moved to the cloud, it becomes vulnerable to a number of new threats ranging from stolen administrator credentials to new hacking techniques. In addition, new legislation, such as the USA PATRIOT Act, is making it possible for competitors and governments to access data from cloud providers without the consent of the data owner. Many cloud providers thought they could achieve data sovereignty through locating cloud services in different jurisdictions, but this theory has been shaken by the subpoena classification ruling handed down recently in the U.S. federal court.[3] It is now unclear if merely locating data in foreign jurisdictions puts customer data out of reach from disclosure demands.

For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all require that organizations protect their data at rest and provide defenses against threats. Cloud providers offering infrastructure as a service (IaaS) and platform as a service (PaaS) offer a "shared responsibility" model for customer applications and data, so companies that are migrating to the cloud are responsible for finding a solution.

This white paper examines the risks to data in the cloud and introduces HP Atalla Cloud Encryption running the Porticor® engine, which combines state-of-the-art encryption with patented key management to protect critical data in public, private and hybrid cloud environments. HP Atalla Cloud Encryption uses three core technologies to deliver trust in the cloud:

1. Robust, standards-based data encryption with a convenient, fast, and simple management interface
2. Cloud-ready key management using patented split-key encryption
3. Homomorphic key encryption techniques that protect keys even when they are in use

Each of these plays a vital role in helping ensure that your data is safe and that your encryption keys are protected, both when in storage and when in use in the cloud. Together, they make HP Atalla Cloud Encryption the only solution that offers the convenience of encryption and key management in virtualized environments, without sacrificing trust.

[1, 2] HP Cloud—public cloud security research, November 2013, go.hpcloud.com/security-survey

[3] ZDNet—U.S. search warrant can acquire foreign cloud, email data, judge rules: zdnet.com/u-s-search-warrant-can-acquire-foreign-cloud-email-data-judge-rules-7000028828/

The challenges of securing data at rest in private and public clouds

Data encryption is one of the most important methods of protecting data at rest in the cloud and as a result, the number of solutions available—from open source application programming interfaces (APIs) to proprietary turnkey projects—has mushroomed. In order to select the most effective solution for your needs, it is vital to understand the primary challenges of encrypting data in the cloud.

- Managing the encryption process: For complex applications with large amounts of data, the most time-consuming aspect of data encryption is management: deployment, setting up, adding and removing disks, etc. An effective encryption solution can reduce the time required for each of these tasks from hours to minutes.
- Securing the data lifecycle: An organization's data is the valuable asset that needs protection from the adversary. Encryption keys are the secrets behind encryption; therefore, they must be handled and deployed correctly to ensure protection of data in use or at rest. An effective encryption solution must address every stage in the lifecycle.
- Delivering high performance: To ensure that the quality of service (QoS) for your business applications meets expectations, the encryption solution must offer very high performance.
- Ensuring trust in the cloud: Trust is the major problem with hosting encryption key management in the cloud. For both security and compliance reasons, an organization should not allow a third party to completely manage its encryption keys for sensitive data. In order to benefit from the convenience and low cost of cloud-based key management, enterprises need a sophisticated solution that leaves the root of trust in the trust of the enterprise.
- Storing and managing the encryption keys: Every time the application accesses the data store, it needs to use encryption keys. There is generally one key per disk or data store and all of them must be managed on a key management server. Hosting a key management server in the data center is expensive, undermining the cost benefits of cloud projects. On the other hand, storing keys in the cloud raises the very important issue of trust.
- Protecting the keys from theft when they are in use: Encryption keys are most vulnerable at two points—when in storage and while in use. A truly effective key management solution will be able to protect the keys at both times.

Data encryption: how does it work?

The most secure data encryption solution must support all of the major business use cases: full disk encryption, database encryption, file system encryption, distributed storage encryption, and even row or column encryption. HP Atalla Cloud Encryption applies the same encryption technology to all of these needs.

Whenever an application (such as a database server) writes a disk block, it goes through a secure virtual appliance where the data is encrypted and sent to the disk volume. The plain text data is seldom written to persistent storage. All requests to read data from the disk are sent to the secure virtual appliance, which reads the encrypted data blocks, decrypts them, and then sends the plain text data back to the requesting application.

HP Atalla Cloud Encryption provides the unique ability to invisibly "hook" the encryption solution between your data storage and your application or database servers in the cloud. Once you grant permission, the encryption solution is transparent to the application and can be integrated quickly and easily without any application changes at all.

HP Atalla Cloud Encryption uses industry-standard high-grade Advanced Encryption Standard (AES) encryption algorithm with a 256-bit key. Multiple blocks are chained using Cipher-Block Chaining (CBC), and the Encrypted Salt-Sector Initialization Vector (ESSIV) scheme is used to counter fingerprinting attacks. It is also possible to configure the system to use alternate encryption algorithms as needed. The solution can encrypt several different types of data dynamically:

- Disk volumes: It can be exposed to applications as NFS disks or as Windows® shares (CIFS volumes).
- Disk volumes configured as a SAN: HP Atalla Cloud Encryption supports the iSCSI protocol for exposing these volumes. This is a common way to configure storage for database servers.
- Distributed storage: It is where applications normally write the whole file into a Web service, and benefit from extremely high durability. Porticor supports the most popular implementation, Amazon Simple Storage Service (S3), and can integrate with other implementations.

Beyond encryption, HP Atalla Cloud Encryption features additional technologies to reinforce the security of your data:

- Digital signing to help ensure data has not been altered.
- Patented data dispersion and deconstruction technology to help ensure distributed storage data objects are difficult to find in the cloud.
- Logging and alerting on data-related events to support auditing and compliance with regulations.

Managing the encryption keys in the cloud

To encrypt data, HP Atalla Cloud Encryption performs the encryption algorithm on both the plain text and the secret key to obtain the cipher text: C = EK(P). The best practice is to generate as many different random keys as possible—e.g., one key per disk volume or object—and to store them securely. You should never store the key next to the encrypted data, since it would be vulnerable to the same attack as the data. This is a dilemma in the cloud: ideally, you do not want to store your keys in the cloud with your data, but of course, you need them to access data stored on your application servers and database servers.

To address this issue, some security vendors require installation of a physical key management server in your data center as a pre-requisite. Other security vendors ask you to "trust" them and use their Key Management Service. This approach violates the principle—and the compliance requirement—of keeping the keys under your own control.

HP Atalla Cloud Encryption running the Porticor engine is the only system available that offers the convenience of cloud-based hosted key management without sacrificing trust. Breakthrough split-key encryption technology protects keys and helps them remain under customer control and are seldom exposed in storage, and with homomorphic key encryption—even while they are in use.

Like your private bank's safe deposit box in the cloud

The split-key encryption of HP Atalla Cloud Encryption is similar to the traditional practice used to protect private safe deposit boxes at banks around the world. Each safe deposit box has two keys: the customer holds one, while the other is kept by the bank. Neither the customer nor the banker can open the safe on their own; both keys are needed at the same time.

The HP Atalla Cloud Encryption key management solution also requires two keys. Each data object (such as a disk or file) is encrypted with a unique key that is split in two. The first part—the Master Key—is common to all data objects in the application. It remains the sole possession of the application owner and is unknown to HP. The second part is different for each data object and is stored by the Key Management Service. When the application accesses the data store, the engine uses both parts of the key to dynamically encrypt and decrypt the data.

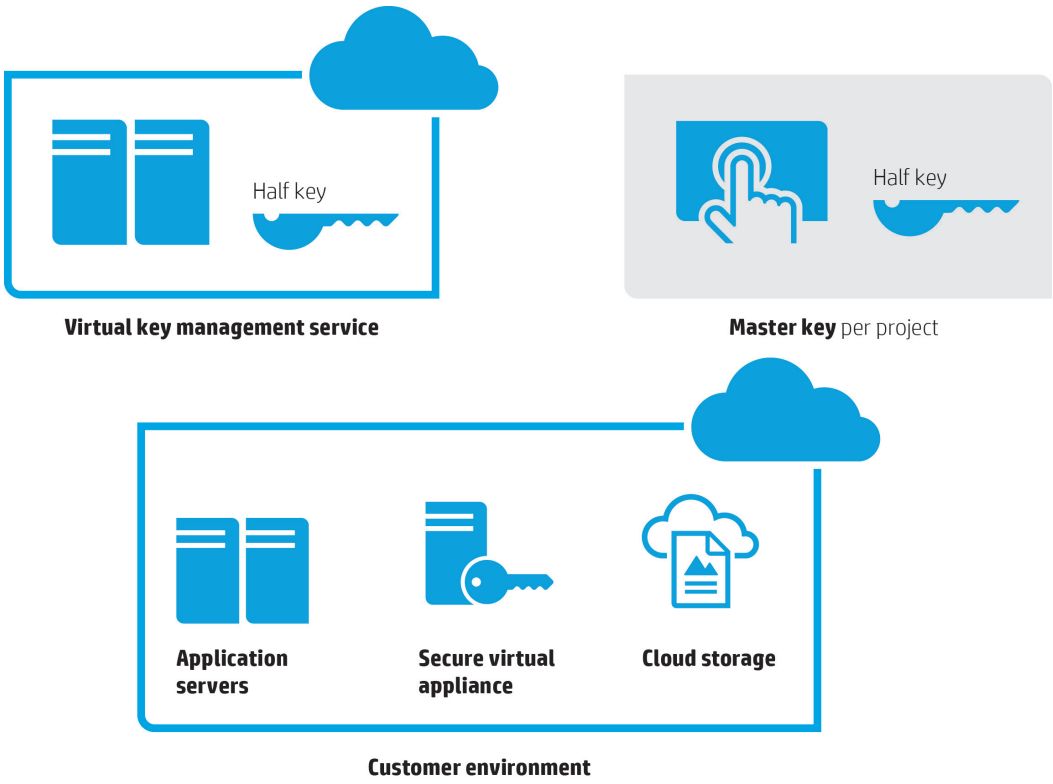
Whenever you create a new project (application), you generate a single Master Key and back it up securely on your own premises. The Master Key is used by the secure virtual appliance, which resides in your own cloud, but it is never transferred to the Key Management Service of HP Atalla Cloud Encryption. When you encrypt a disk volume or an Amazon S3 object, it receives a new key that is a mathematical combination of the Master Key and a unique random key created by the secure virtual appliance and stored in an encrypted form in the Key Management Service.

So for each application or project, you only have to keep track of one Master Key. For every disk or data storage object used by the application, the secure virtual appliance generates the second half of the key, and stores it in the Key Management Service after further encryption with an RSA private key.

Just like the bank, you have one key, HP Atalla Cloud Encryption keeps the other—both are required to access the data. To retrieve the data encryption key (e.g., when the secure virtual appliance is restarted), the appliance combines the Master Key with the second key (the "banker" key) to obtain a key that can actually decrypt an object.

When you no longer require ongoing access to a data object, you can use the management interface (or API) to "lock" the object. The key is then erased, and only the "banker" part is retained (encrypted) in the secure virtual Key Management Service. The object is still protected by both the Master Key and the "banker" key. When the key is needed again for reactivation of the volume, it can be fetched from the secure virtual Key Management Service.

Figure 1. Patent-pending split-key management technology



Homomorphic key encryption: protecting keys in use

HP Atalla Cloud Encryption running the Porticor engine is the only solution that keeps your data and encryption keys safe at all times—even when they are in use in the cloud. Homomorphic encryption is a technique that enables mathematical operations to be performed on encrypted data. Patent-pending technology implements homomorphic techniques for combining and splitting encryption keys. It enables the secure virtual appliance to give the application access to the data store without ever exposing the Master Keys in an unencrypted state.

As explained above, with HP Atalla Cloud Encryption, each data object is encrypted with a key that has two parts: the Master Key and the second ("banker") key. When the application needs to access the data store, the secure virtual appliance combines both parts of the key in a mathematical operation. Ordinarily, this would require both parts of the key to be exposed (unencrypted). However, with HP Atalla Cloud Encryption, both parts of the key are encrypted before and during their use in the virtual appliance. As a result, the keys are fully encrypted when they are resident in your cloud account. The solution similarly encrypts the Master Key differently for each instance of the secure virtual appliance. So even if your cloud account is breached or attacked, and the encrypted Master Key is stolen, it cannot be used to access your data.

With fully homomorphic encryption, all mathematical operations can be performed on encrypted data, but since it requires an enormous amount of computational resources, it isn't yet feasible for a real-world system. With partially homomorphic encryption, only select mathematical operations are supported, dramatically reducing the computational overhead. Partially homomorphic encryption is used in a patent pending implementation so that the most critical link in the encryption of data in the cloud—the Master Key—is also encrypted and protected. At the same time, you benefit from fast, reliable performance for your business-critical applications.

Understanding threats in the cloud

In order to manage and mitigate risk, you need to understand it. Threats to cloud security are widely publicized and they are real.[4] But with HP Atalla Cloud Encryption, you get a level of data protection that resolves the competing concerns over control of encryption keys while realizing the benefits of the cloud.

All data encryption systems, both in the cloud or in a physical data center, share a common vulnerability—they need to use the encryption keys. When the keys are in use, they can, hypothetically, be stolen. HP Atalla Cloud Encryption takes numerous known precautions, and leverages new ones, to mitigate this risk.

HP Atalla Cloud Encryption appliances are designed for security. The disks seldom contain the encryption keys and the memory (where the encryption keys are stored) is inaccessible—even to HP Atalla Cloud Encryption agents and the Porticor engine. Nevertheless, in the unlikely event that a secure virtual appliance is breached and the encryption key is stolen, only the one stochastically dependent data object that is in memory at that time is exposed. In order to access the rest of your data storage, the thief would need the enterprise's project Master Key. Thanks to homomorphic key encryption, the Master Key cannot be stolen and used. As a result, the breach of a single object cannot lead to a breach of your entire system. This is a level of protection that most traditional on-premise encryption solutions cannot offer.

Conclusion: HP Atalla Cloud Encryption

Data encryption is critical to protecting the security of data at rest in the cloud. But when it comes to the cloud, encrypting the data is only the beginning—managing and protecting the encryption keys effectively is vital. An effective data encryption solution must include:

1. Robust, fast, yet easy-to-use data encryption
2. Reliable, cloud-based key management that is cost-effective, but trustworthy
3. Key encryption technologies to protect your encryption keys as well as your data—both in storage and in use

Learn more at
hp.com/go/AtallaCE

[4] HP Cloud—public cloud security research, November 2013, go.hpcloud.com/security-survey

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-2726ENW, May 2014