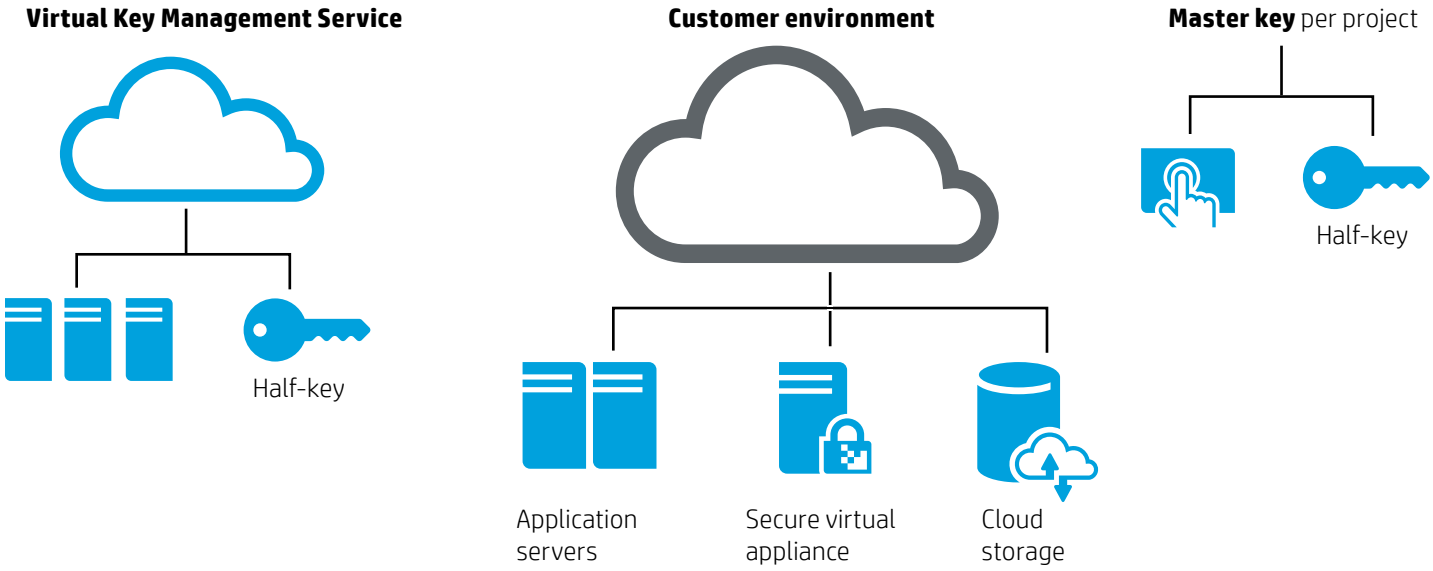
Data sheet

HP Atalla Cloud Encryption

Securing data in the cloud



We are rapidly moving toward a cloud majority world, but the problem of full trust remains unresolved. 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.

Highlights

- Complete data encryption and key management solution
- Easy to automate and integrate
- Scalable and elastic in the cloud

Cloud-hosted key management and encryption with on-premise quality security, using split-key technology

Protecting data in the cloud

Securing data—at rest and in use—is simpler when the data is located within the four walls of a data center. When data is moved to the cloud, it becomes vulnerable to a number of new threats ranging from stolen administrator credentials to new hacking techniques. For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Payment Card Industry Data Security Standard (PCI DSS), Gramm–Leach–Bliley Act, and European Union (EU) Data Protection Directive all require that organizations protect their data at rest and provide defenses against threats.

About HP enterprise security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in its hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, HP Atalla, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

HP Atalla Cloud Encryption uses three core technologies to deliver trust in the cloud:

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

Complete data encryption solution

HP Atalla Cloud Encryption applies the same encryption technology to all of the major business use cases: full disk encryption, database encryption, file system encryption, distributed storage encryption, and even row or column encryption. Whenever an application 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 never 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 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 alternative encryption algorithms as needed.

How it works

With HP Atalla Cloud Encryption, each data object (such as a disk) is stored in a secure virtual appliance and is encrypted using split-key encryption. Each key has two parts:

1. The first part, the master key, is retained by the application owner (you) and is never stored in open form in either your cloud account, or on the Key Management Server.
2. The second part, the project key, is stored on the Key Management Service.

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. However, with HP Atalla Cloud Encryption, both parts of the key are encrypted before and during the startup of the virtual appliance. As a result, the keys are fully encrypted when they are resident in your cloud account.

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 practical—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 attacks 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 you need them to access data stored on your application servers and database servers.

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 makes sure they remain under customer control and are never exposed in storage; and with homomorphic key encryption, even while they are in use.

Key product features

HP Atalla Cloud Encryption includes a virtual appliance or agent that you can install in minutes. Through the intuitive management console, it is easy to encrypt any disk or data storage unit with proven encryption algorithms such as AES-256. After your data is encrypted, it is protected from unauthorized access and other threats.

1. **Easy to automate and integrate**—Time to delivery measured in minutes for a quick and cost-effective security solution.
2. **Complete data encryption solution**—Encrypt the entire data layer including databases, files, and distributed storage, in public, hybrid, and private clouds with keys that are never exposed.
3. **Scalable and elastic**—Application performance is maintained while protecting encryption keys while they are in use in the cloud. It scales up or down easily to deploy virtual encryption resources in your cloud environment as needed.

Homomorphic key encryption: protecting keys in use

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.

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 homomorphically 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 can never be used to access your data.

Cloud database security

HP Atalla Cloud Encryption provides encryption and management of encryption keys that works with major databases, such as Oracle, MySQL, Microsoft® SQL Server, and IBM DB2. Cloud security for databases requires cloud encryption.

HP Atalla Cloud Encryption offerings

Offering	Details	Support options
HP Atalla Cloud Encryption for Amazon Web Services (AWS) per virtual appliance	Deployed into the customer's cloud environment. Price per virtual appliance. Support included in term license, monthly (U.S. only), 1-year and 3-year term licenses; customer data protection is independent of term license renewal.	9x5 Standard 24x7 Support
HP Atalla Cloud Encryption for VMware per virtual appliance	Deployed into the customer's cloud environment. Price per virtual appliance. Support included in term license, monthly (U.S. only), 1-year and 3-year non-renewable term licenses; customer data protection is independent of term license renewal.	9x5 Standard 24x7 Support
HP Atalla Cloud Encryption agent per instance on VMware	Deployed for installation on the application server in the customer's cloud environment. Requires Linux operating system. Price per agent instance on VMware. Support included in term license.	9x5 Standard 24x7 Support
HP Atalla Cloud Encryption agent per instance on Amazon Web Services	Deployed for installation on the application server in the customer's cloud environment. Requires Linux operating system. Price per agent instance on AWS. Support included in term license.	9x5 Standard 24x7 Support

Learn more at
hp.com/go/AtallaCE

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-2725ENW, May 2014