Safeguarding Data in the Cloud

Porticor® Virtual Private Data™ (VPD™) combines state of the art data encryption with patented homomorphic split-key management to offer the most secure, cost-effective solution for safeguarding data in the cloud. Easy to install and use, Porticor VPD provides a complete solution for the entire data layer, and solves the biggest challenge of cloud data encryption – safe storage of the keys.

Data in the cloud: The opportunity and the risk

Hosting applications in the cloud is an opportunity to increase agility and control costs. But it can also put information about your business, your employees and your customers at risk. Data at rest – information stored on a disk or other media – is usually considered secure when it is located within the four walls of a data center. But once it is moved to the cloud, an inherently public space, it becomes more vulnerable to threats, ranging from stolen administrator credentials to hackers and competitors. In addition, recent legislation gives government agencies the ability to access data from cloud providers without the consent of the owner.

Your Data, Your Responsibility

In Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) clouds, protecting data at rest is your responsibility. To meet privacy obligations to your customers and employees, and to comply with regulatory standards such as PCI DSS, HIPAA and SOX, you must securely encrypt cloud-based data, while keeping operational overhead to a minimum.

Cloud Provider Security Responsibilities:

Physical Security
Virtualization Security
Host OS Security

Customer Security Responsibilities:

Encryption
Key Management
Application Security

From Installation to Encryption in Minutes

Porticor Virtual Private Data includes a virtual appliance or agent that you can install in minutes. Through the intuitive management console, it's easy to encrypt any disk or data storage unit with proven encryption algorithms such as AES-256. Once your data is encrypted, it is safe from hackers, unauthorized access, competitors and other threats.

Disk	Size (GB)	🔒 / 🔓	Network Storage	⚙	⚡	❌
sdf	3	Available for secure use	NFS File System use it	Lock		
sdg	2	Available for secure use	Windows Share use it	Lock		
sdh	5	Available for secure use	Windows Share use it	Lock		
sdi	1	Available for secure use	iSCSI Target use it	Lock		
sd...	[number]			Create new		

The Porticor Advantage

- Highest degree of data privacy

- Protection from hackers and competitors

- Compliance with standards: SOX, SOC2, HIPAA, PCI DSS, GLBA

- Fully cloud-based, dynamic and elastic

- Quick, cost-effective operations

- Easy automation and integration

- Amazon AWS official solution provider

"Porticor's service and knowledge of the Amazon platform has been top notch. As we have examined multi-tenant environments, Porticor has been valuable for my team and has alleviated security concerns."

Steve McAtee
Senior Director of Architecture, IT
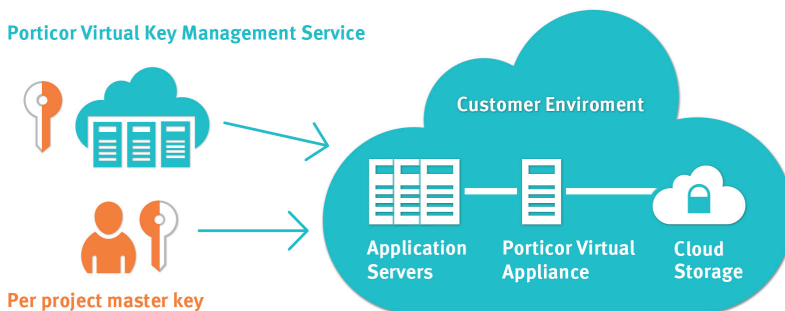Risk Management and Security
McGladrey & Pullen

Trusted, Cloud-Based Key Encryption

Porticor® patented Virtual Key Management™ solves the biggest challenge for data encryption in the cloud – storing the keys. Every time an application accesses the data store, it needs to use the encryption keys. This puts the keys at risk in two places: when they are in storage, and when they are in use. Porticor's key management features breakthrough split-key encryption technology that increases security by an order of magnitude, and is built for homomorphic[1] key encryption which protects keys even when they are in use in the cloud. Porticor VPD is the only system available that offers the convenience of cloud-based hosted key management without sacrificing trust.

Homomorphic Split-Key Encryption

With Porticor, each disk or file is encrypted with a unique key that is split in two. The first part - the master key - remains in your possession and is not even known to Porticor. The second part is stored by the Porticor Key Management Service. As the application accesses the data store, Porticor uses both parts of the key to dynamically encrypt and decrypt the data. When your master key is in the cloud, it is homomorphically[1] encrypted – even when in use – so that it can never be hacked or stolen.

Product Highlights

- Complete data layer encryption
- Support for public, private and hybrid clouds
- Patented split-key encryption technology
- Secure, cloud-based key management
- Patented Homomorphic key encryption
- 5 minute installation and setup
- API for automation and integration
- High performance
- Scalable and elastic

Porticor Virtual Key Management Service

Per project master key

Customer Enviroment

Application Servers

Porticor Virtual Appliance

Cloud Storage

"Porticor enabled us to bring our business data securely to public clouds, and reduces our effort dramatically - we were very impressed with the Porticor vision and execution."

888 Holdings

Protection for All of Your Cloud Data

Only Porticor encrypts the entire data layer including virtual disks, databases, files, distributed storage and more. Porticor is suitable for public, hybrid and private clouds offered as Infrastructure as a Service and Platform as a Service.

High Performance with Unlimited Elasticity

Porticor Virtual Private data is scalable and elastic. The virtual appliance has virtually no impact on application performance or latency. You can create as many Porticor appliances or agents as you need.

Robust API for Automation and Integration

With our secure, cloud-based API, you can rapidly integrate Porticor into your automated environment. The API controls all of the functions of the virtual appliance as well as the Virtual Key Management service to support integration with your existing cloud deployment.