DataKeep™

SecurityFirst™
Data-Centric Cyber Solutions

Securely Embrace Cloud Storage for Operational Savings, Infinite Scalability and Ransomware Defense with DataKeep™

Advanced Protection

- Provably secure data protection (FIPS 140-2 certified)
- TLS protection for data in-motion
- Meets regulatory compliance requirements
- Provides Ransomware defense
- Storage spanning across multiple Cloud Service Providers
- Geographic separation of shares for HA and DR

Cost Efficient

- One agent supports multiple server assets
- Supports S3 compatible public or private cloud storage
- Simplifies access to traditional off-line storage
- Highly scalable, no file system or volume block limits

Easy To Use

- Integrates into any existing environment via REST API
- Built-in key management supporting Bring Your Own Key
- Supports existing hardware or software KMIP keystores

Multiple Use Cases

- Data Staging to cloud
- Data Archive to cloud
- Network Backup to cloud

Why Object Storage?

Dramatic improvements in data storage and processing technologies in recent years have fundamentally reshaped entire sectors of the worldwide economy. Today the Digital Economy is valued in excess of $3 trillion dollars amassed since the birth of the Internet approximately 20 years ago. Much of it is fueled by the collection and analysis of so called “Big Data” requiring new, scalable repositories based upon object storage rather than file system technologies.

Object storage technology helps the leaders of this new economy—Facebook, Amazon, Apple and Microsoft—deliver new products and services, but its development also offers disruptive use cases for replacing more traditional low-cost, secondary storage alternatives. Data that was once migrated from random disk to serial tape resources seeking to free-up fast access storage capacity, can now simply be moved to and mounted within a public cloud dramatically simplifying storage management activities.

In addition to massive capacity, forms of cloud-based object storage offer lower overall costs and faster data retrieval possibilities for many non-transactional workloads processing unstructured data on an infrequent basis; yet concerns regarding the security of such data still abound.

Everything is Vulnerable

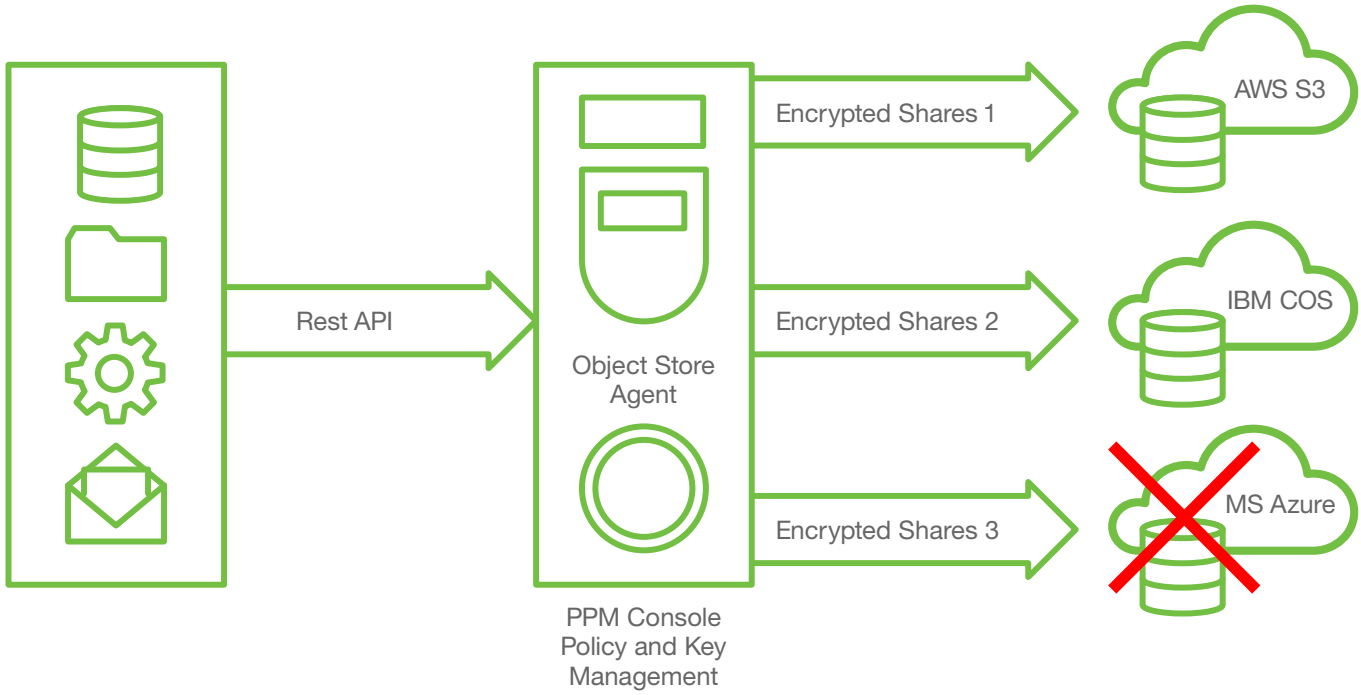
What’s unfortunate about the rise of the Digital Economy is that few (if any) of these new computing breakthroughs were developed with an eye toward security. An industry leader for data cryptology summed the situation up as follows:

“Everything online is hackable. This is true for Equifax's data and the federal Office of Personal Management's data, which was hacked in 2015. If information is on a computer connected to the Internet, it is vulnerable.”[1]

When vulnerabilities are discovered, software or firmware patches and updates are normally developed and distributed, but unfortunately not all are immediately applied. Some are overlooked, some are postponed for a future effort, and some are dismissed due to application compatibility issues.

Consequently, organizations rightly have concerns over using IT capabilities over which they have a more limited degree of insight and control. Cheaper and faster are poor

[1] CQ Researcher, Privacy and the Internet - 2/9/18



DataKeep's Object Store Agent communicates with network assets via a RESTful API, is controlled by a centralized Policy and Provisioning Management console, and encrypts and cryptographically splits data being sent to one or more clouds. Here, even if the share on Azure is compromised, all data is recoverable from the other two (2:3) encrypted components.

excuses for defending cloud storage uses when data breaches occur. Ideally, security teams would prefer to use one data protection solution across all file, volume and object storage resources wherever they reside.

Confidence to use the Cloud

Putting the security of your organization's data in others' hands is generally a bad idea from a data governance standpoint. But there is a way to reap the benefits of cloud-based object storage using an advanced data protection technology. DataKeep,™ which now includes a ground-breaking Object Store Agent, allows anyone to securely store data in the highly scalable, efficient, object storage—whether in a cloud, on-premises or both—leveraging its native resiliency features. Your data is completely in your control, and always private and highly available.

Access is controlled by storage object owner IDs and associated read/write/delete policies. Server security keys are generated and kept by you—not by the storage provider—and can be securely stored in the DataKeep management console or remotely with or without the use of a KMIP compliant hardware or software keystore to give you even more control over data security. Where data is stored, both geographically and/or by cloud providers, is configured by your system administrator.

DataKeep ensures that cloud service providers (CSPs) operate with minimally sufficient metadata including file names and relative sizes. In addition, the data can be allocated across multiple stores, each containing only a fragment of an encrypted file so data falling into the wrong hands is completely useless, and you're not locked into a single CSP.

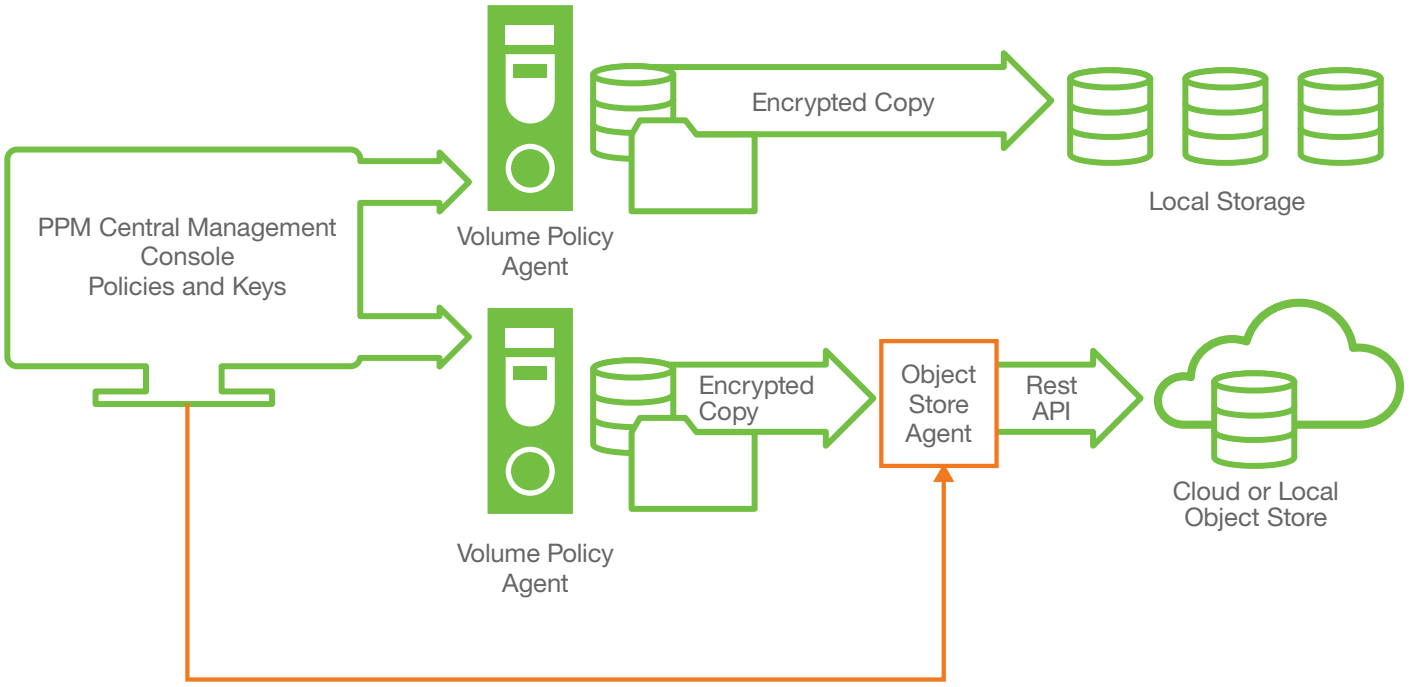
Proven Security

DataKeep ensures your data is provably secure from on-premises resources through to S3 capable cloud storage. Its patented SPxCore™ cryptographic splitting core is an advanced protection algorithm certified as FIPS 140-2 compliant for its combination of encryption, integrity checking, keyed information dispersal and key management.

Data sent through the Object Store Agent is encrypted locally and further protected in-transit using the Transport Layer Security (TLS) protocol. It can be divided into multiple shards stored across one or more cloud service providers in an "M of N" (1:1, 2:3, and 2:4) fashion allowing full restoration from a subset of the original content. The process is operating system agnostic and can protect information sent from Microsoft, AIX, Ubuntu, RedHat and more servers.

Added Protection from Ransomware

Ransomware is one of the fastest growing and successful attacks security teams face and organizations such as the Department of Homeland Security (DHS) have stated that an effective backup/restore solution is your best defense. Studies indicate



DataKeep's Object Store Agent receiving and encrypted version of on-premises data from a File Agent before passing it through to a S3 compatible object storage resource.

that companies are hit every 40 seconds by this type of malware, and 71% of those attacked were infected.[2] The tactic has created another use for object storage in the form of a secure backup, and the real value of cloud data backup is its restoration speed.

For decades, magnetic tape storage had found a role as a near-line and off-line storage alternative for cost reasons, but it could prove a poor choice as a ransomware defense mechanism where time counts most. Tape-based backups are cumbersome, and recoverability of the stored data can suffer from media sagging, magnetic print-through and head/media alignment issues.

DataKeep includes the ability for administrators to copy, move or backup encrypted files or volumes without access to clear-text data and send them through the Object Store Agent where they are re-encrypted and optionally split into multiple shares for added protection. DataKeep's File and Volume agents have the ability to provide scheduled, full, or differential backups – which can be stored locally, or via the Object Store Agent, to any local or cloud-based object storage.

Network backups stored in the cloud can be recovered in minutes to hours depending upon the type of storage selected and are almost always highly available based upon cloud storage service level agreements.

Reduce Overall Storage Costs

DataKeep allows anyone to immediately start protecting data stored in object storage, locally or within the cloud. This results in significantly reduced storage cost, maintenance, and scaling challenges when compared with traditional on-premises primary, backup and archive storage environments. With public cloud object storage, you pay monthly for only the storage you actually use, resulting in 100% storage utilization with no long-term commitments or upfront costs.

Object storage has virtually limitless scale, expanding as you need it from terabytes to petabytes to exabytes, all while converting capital costs into operating costs and eliminating hardware acquisition, deployment, and obsolescence charges.

Your Last Line of Defense

In a layered security model, a data-centric approach is critical to defend against costly data breach disclosures and associated losses. Organizations adding a data-centric solution for security need a compatible technology built around certified industry standards that is easy to deploy, manage, and seamlessly integrate into existing environments. DataKeep offers complete security, privacy and control of data across your enterprise and in the cloud while serving as your last line of defense against a breach.

[2]Kasperky Security Bulletin - 12/8/16

DataKeep Object Store Agent at a Glance

Feature	Description
Software Deployment	Linux RPM based installer provisioned from the PPM Server
Admin Interface	PPM GUI / REST interface and CLI for Object Store Agent itself
API Support	REST – Representational State Transfer
User Authentication	Generated API ID and Key credentials
Admin Authorization	LDAP, AD, or Local
Cache Support	Scales dynamically as required. All data in cache is encrypted
Supported Cloud Storage	IBM SoftLayer Object Storage, Amazon Web Services S3
Data Encryption	AES-256
Server key	Customer Controlled. Stored on PPM or exported via KMIP for storage in hardware or software keystore
Key Management	Built-in simplified key management. Each object has a unique encryption key that is encrypted, split and stored Eliminates the need for bulk hardware keystores Only the server key needs to be secured
Additional Security	Cryptographic splitting (at the bit level) with physical separation of data shares Keyed Information Dispersal Algorithm (IDA)
Fault Tolerance	Standard Cloud: "1:1" (1 share utilizing only object storage data durability) =100% of original data Data Center Outage: "2:3" (3 shares targeted at different sites, sustains loss of 1) =150% of original data CSP Outage: "2:4" (4 shares targeted at different sites, sustains loss of 2) = 200% of original data

DataKeep Object Store Agent Server Requirements

Requirement	Minimum	Recommended
Operating System	RHEL / CentOS 7.2+	
Processor	2 Cores, Intel 2.4 GHz (64-bit), with AES-NI	4+ Cores, Intel 2.66 GHz (64-bit), with AES-NI
Memory	4 GB	8 GB in addition to any required by other applications
Disk space	80 GB	Size according to requirements

About SecurityFirst

SecurityFirst™ specializes in data-centric solutions for protecting an organization's sensitive data – no matter where it resides. We emphasize security at the data layer itself to augment network, hardware and software security to serve as the last line of defense. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure around the globe.

DataKeep, by SecurityFirst, secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption, and event logging combine to complete your data privacy and compliance needs.

SecurityFirst™
Data-Centric Cyber Solutions

For a product demonstration or more information call
1.888.884.7152
securityfirstcorp.com