DataKeep™

SecurityFirst™ Protecting Critical Data

Complete data security, privacy and control begins with DataKeep™

Highlights

- **Design and administer data access policies with user-defined roles, using individual, group, or application/process level permissions**
- **Leverage integrated, transparent key management that conforms to regulatory requirements with or without an external keystore**
- **Collect and forward detailed activity logs to existing Security Information and Event Management (SIEM) systems**
- **Easily copy, move, backup or restore (full or incremental backup) files for disaster recovery and ransomware mitigation**
- **Single point of data security management for volume level or fine-grained file level data security and access controls**
- **Object store agent for secure on-premises or cloud object storage**

Protecting Data from Creation to Destruction

Organizations face daily challenges from sophisticated cybersecurity attacks, insider threats, and employee errors and omissions. Security lapses, willful data exfiltrations and mistakes can cost millions of dollars to remediate and can detrimentally impact a brand reputation. Customers are growing weary of repeated identity compromises and don't need yet another protection service. What they need is data protection.

The ideal solution must protect data throughout the sensitive data lifecycle, from the point of creation to the point of destruction and not just while the data is in storage. It should layer on top of existing directory services to provide an additional level of access control to define, track, and document who is accessing what and when. It should also fit within budget constraints from both an acquisition and an ongoing maintenance perspective.

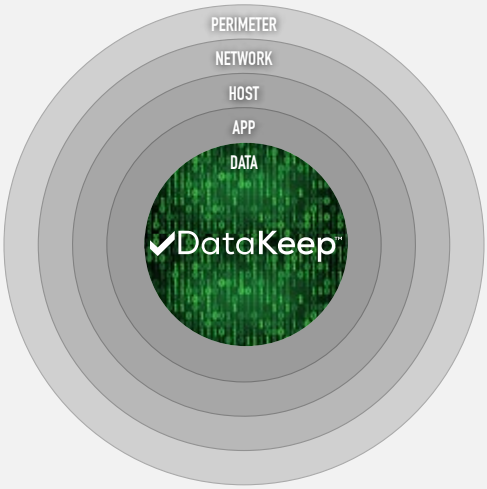
Why DataKeep?

Maintaining control of critical data is the best way to minimize exposure in the event of a breach, and a data-centric management strategy must be employed as part of your layered security model for an additional level of protection against increasing threat profiles.

DataKeep makes protecting data anywhere across your environment, whether on-premises or in the cloud, easier and does not impede on day to day operations. Enhanced features encompass data access management including privileged access, sophisticated encryption, integrated key management, and audit logging and integrated reporting. Together, these create a powerful data protection solution that mitigates unauthorized access and serves as your last line of defense in the event of a breach.

Native copy and move capabilities in the DataKeep File and Volume Agents provides an integrated, cost effective, full or incremental backup and recovery capability with end to end security, low overhead, and no access to decrypted data by the backup system administrators – the only effective mitigation against ransomware.

With DataKeep, organizations can more easily meet compliance, protect their brand, and minimize financial impact and reduce the risks associated with data loss and misuse.



Your Last Line of Defense

Integration of a data level protection product such as DataKeep into your layered security model offers complete security, privacy, and control of data across the enterprise, while serving as a last line of defense against a breach.

DataKeep™ Benefits

Mitigate Risk and Manage Compliance

DataKeep is the next generation of truly secure data-centric protection for organizations looking to protect their digital assets. By implementing DataKeep, organizations can easily manage who, what, when, where and how data is accessed and mitigate risk associated with unauthorized access to data.

Compliance regulations such as Health Insurance Portability and Accountability Act (HIPAA/HITECH) and Payment Card Industry Data Security Standard (PCI DSS) are constantly evolving, applying additional burdens on businesses and organizations. Statewide and global initiatives such as the New York's NYDFS – 23NYCCR 500 and the European Union's General Data Protection Regulation (GDPR) are mandates with strong penalties to ensure data privacy of its citizens.

DataKeep addresses the most stringent compliance requirements, including data that is required to be archived securely over a number of years, across any industry with built-in data protection, data access processes, cryptographic policy enforcement, auditing and reporting capabilities, and integrated key management. By employing encryption that protects data wherever it is created and stored, organizations can avoid associated fines and expensive data breach notification efforts.

Achieve Business Efficiencies

Save time, staff, and budgetary resources through simplified, scalable and affordable data protection that supports all cloud and data center environments, including those across new or existing multi-cloud architectures and the ability to securely take advantage of cost-efficient object storage. Since DataKeep is agile and easy to use, it can scale to easily protect large enterprise environments including those deployed across existing or new multi-cloud architectures.

Thanks to its standards-based interfaces and APIs, it minimizes the constraints on the time, staff and budgetary resources needed to protect all data while avoiding the risk of missing critical data. Native copy capabilities in file and volume agents create an inherent backup/recovery environment and eliminate downtime due to a service provider outage or issue, and even ransomware attacks.

Be in Complete Control

DataKeep offers role-based access control, privileged access management and separation of security vs. administrative duties to prevent any one person or service provider from having complete system control.

With built-in key management capabilities are both simplified and stratified with the ability to incorporate external software or hardware key stores - including Bring Your Own Key (BYOK) capability. DataKeep's key management works transparently and provides organizations with the flexibility they require to stay in control. No unauthorized person can read your data regardless of whether it's stored on-premises or within a public, private or hybrid cloud service.

Protect Anywhere

DataKeep helps to simplify, automate and remove the barriers to protecting data from creation to deletion by combining AES-256 encryption module and

DataKeep™ Benefits

cryptographic splitting for strong data protection that are both FIPS 140-2 certified, with access controls, built-in lifecycle and key management and auditable access logging. It's one solution you can use anywhere and not a solution for one specific problem.

Centralized, Efficient Management

A centralized virtual management console helps you provision, deploy, and manage all instances of the encryption agents across your enterprise. The Management Console can be hosted in the cloud or on-premises. DataKeep agents can be deployed to any virtual or physical server running a supported OS.

RESTful API Enabled

For ease of integration, a RESTful API exposing all management console functions is provided with DataKeep. Large scale deployments can be managed using the API and basic scripting, facilitating significant resource and cost savings.

Role-Based Access Controls

Working with your existing directory services, DataKeep's robust, role-based access controls allow an administrator to define a second layer of data access control policies used to specify which filesystem functions are authorized (read, write, etc.), and the level of data access logging desired based upon user, group, or process. Using a default Least Privileged Access (LPA) approach, DataKeep automatically denies access to all users unless they have been specifically granted permissions. The software works in conjunction with a directory service (e.g., Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory), and the user or group must be granted rights to access and view decrypted data.

Privileged Access Management (PAM)

PAM restrictions can be enforced to prevent system administrators and root users from seeing clear text data so they can still do their jobs without concerns about private data theft. This is especially important when entrusting your data to a cloud service provider.

Strong and Distinct Separation of Duties

By default, DataKeep creates two distinct roles – Product and Security Administrators. The Product Administrator role deploys the software and monitors the general health of the DataKeep system and all deployed agents. This role has no visibility into policy definitions, agent configurations, deployments or policy logs. The Security Administrator roles determines and approves data access rights, manages keys, defines policies, sets logging parameters, and creates the multiple approval process. DataKeep also enables a trusted Public Key Infrastructure (PKI) configuration to provide multi-factor authentication for administrators.

Transparent to the End User

DataKeep agents operate at the kernel level of the protected servers for optimal performance. Encryption is transparently applied during file write operations without any end user interaction or noticeable performance degradation.

DataKeep™ Key Features

Audit Logging

In real time, DataKeep logs all user data access requests as either approved or denied. The reliable eventing capture feature flags data access information that can be forwarded to a Systems Information and Event Management (SIEM) application for analysis. The product supports several standard output formats such as Log Event Extended Format (LEEF), Common Event Format (CEF) and Cloud Auditing Data Federation (CADF) for easy integration. This combination of DataKeep and SIEM products can make it possible to shorten the detection cycle of nefarious activities, reducing the risk of data compromise.

Integrated Key Management

With its transparent, built-in key management capabilities, all phases of key lifecycle stay in your control. Automated key creation, rotation, and revocation/shred conform to industry compliance requirements. Security keys can be stored locally by the DataKeep management console or exported using Key Management Interoperability Protocol (KMIP) or Public-Key Cryptography Standards (PKCS #11) to a compliant external keystore. This approach allows Bring Your Own Key (BYOK) and prevents cloud vendor access.

Volume and File Encryption Agents

DataKeep allows customers to deploy agents that encrypt data at the volume-level or for additional granularity, at file/directory level. The volume encryption agent is a virtual block device that once installed is mounted to look like an attached disk. The file encryption agent works at the file-level based upon fine-grained file or directory level policies. This allows for cryptographic security and access controls based upon User or Group, as well as the ability to encrypt the data in place or limit access via pre-defined applications or processes. DataKeep agents can be deployed to any virtual or physical server running a supported OS.

Either of these agent types also support copy and move of encrypted data and by extension, native backup/recovery as full or incremental copies that can be stored locally or remotely without administrative access to clear text data. And in conjunction with the Object Store Agent, support disaster recovery and ransomware mitigation.

Object Store Encryption Agent

In addition to its massive capacity, cloud-based object storage offers lower overall costs and faster data retrieval possibilities for many non-transactional workloads processing unstructured data. DataKeep's Object Store Agent allows customers to securely leverage the low cost of on-premises or cloud based S3 compatible object storage for infrequently used data, with infinite scalability, and the ability to manage security, encryption keys (including bring your own key), and access controls. Leveraging SecurityFirst's M of N and cryptographic splitting and combined with the native backup/restore of the File and Volume Agents, this can provide the disaster recovery and resilience needed to further mitigate hacks and ransomware attacks.

Always on Data Protection, Powered by SPxCore™

DataKeep assures confidentiality, data privacy and protection against brute force attacks. The SPxCore™ technology combines cryptographic splitting with AES-256 certified encryption and internal key management certified by the National Institute of Standards and Technology (NIST) to be FIPS 140-2 compliant. DataKeep also takes full advantage of the AES-NI hardware acceleration available in most current processors for optimal performance.

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

SecurityFirst™
Protecting Critical Data

For a product demonstration or more information call
1-888-884-7152
securityfirstcorp.com