SecurityFirst™
Data-Centric Cyber Solutions

DataKeep™

Complete data security, privacy and control begins with DataKeep™

Highlights

- Design and administer data access policies with user-defined roles at the individual and group levels
- Leverage integrated, transparent key management that conforms to regulatory requirements
- Avoid data breach reporting activities
- Collect and forward detailed activity logs to existing Security Information and Event Management (SIEM) systems

Protecting Data from Creation to Destruction

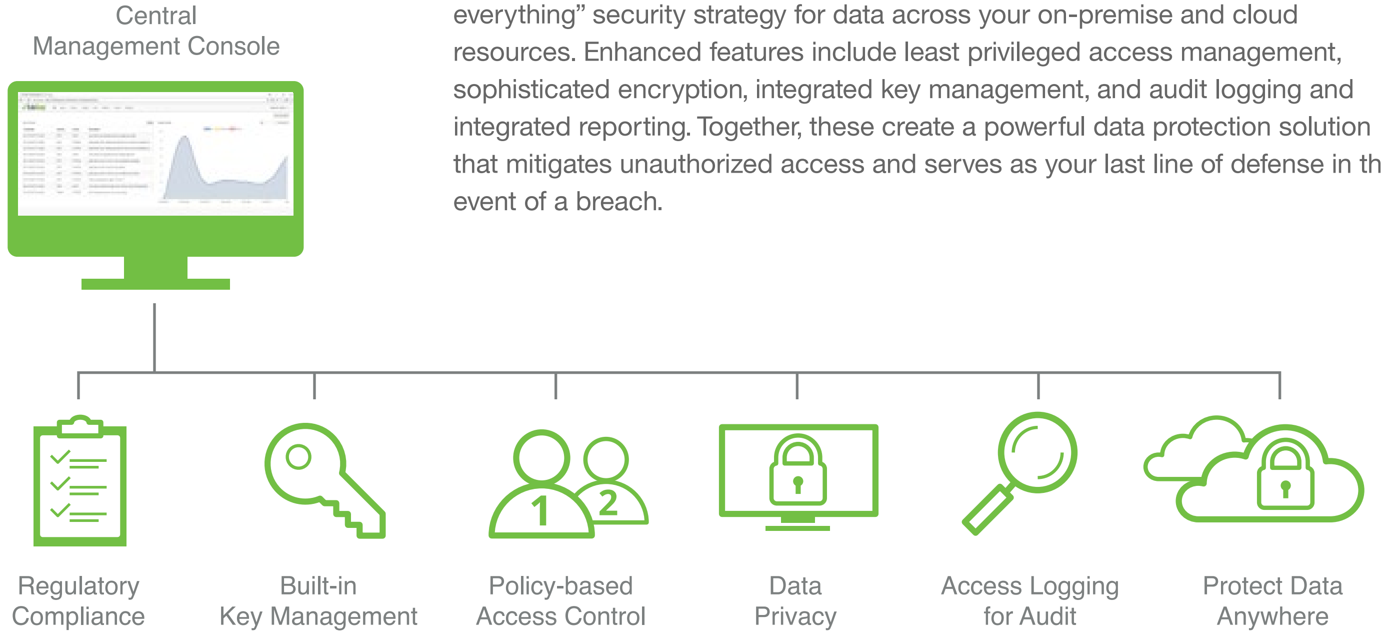
Organizations face daily challenges from sophisticated cybersecurity attacks, insider threats, and employee errors and omissions. Security lapses, willful data exfiltrations and mistakes can cost millions of dollars to remediate and can detrimentally impact a brand reputation. Customers are growing weary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

The ideal solution must protect data across the sensitive data lifecycle, from the point of creation to the point of destruction and not just while the data is in storage. It will 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 will 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 a last line of defense.

DataKeep is an enterprise-class solution that makes it easier to adopt a "protect everything" security strategy for data across your on-premise and cloud resources. Enhanced features include least privileged access management, 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.



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 the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS) are constantly evolving, applying additional burden on businesses and organizations. Forty-eight states have also now defined their own requirements for controlling personally identifiable information (PII). The European Union's General Data Protection Requirement (GDPR) will have a global impact as it adds considerable regulations and financial penalties starting May 2018.

DataKeep addresses the most stringent compliance requirements across all industries 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's 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. 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.

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.

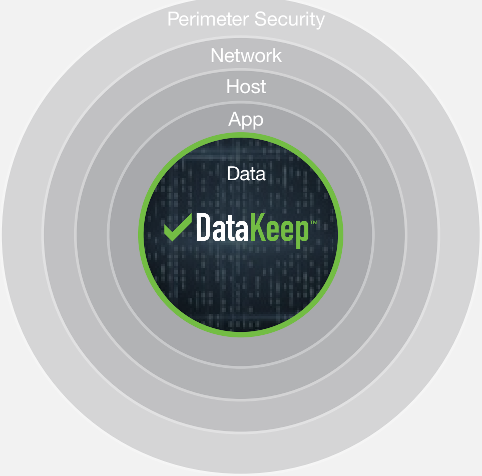
With built-in key management, capabilities are both simplified and stratified with the ability to incorporate external software or hardware key stores. DataKeep's key management works transparently and provides organizations with the flexibility they require to stay in control. No unauthorized person can read your data regardless of whether it's stored on-premises or within some cloud service.

Protect Everything

DataKeep helps to simplify, automate and remove the barriers to protecting data from creation to deletion, by combining an AES-256 certified encryption module and cryptographic splitting for strong data protection that are both FIPS 140-2 compliant, with access controls, built-in lifecycle and key management and auditable access logging. It's one solution you can use everywhere and not a solution for one specific problem.

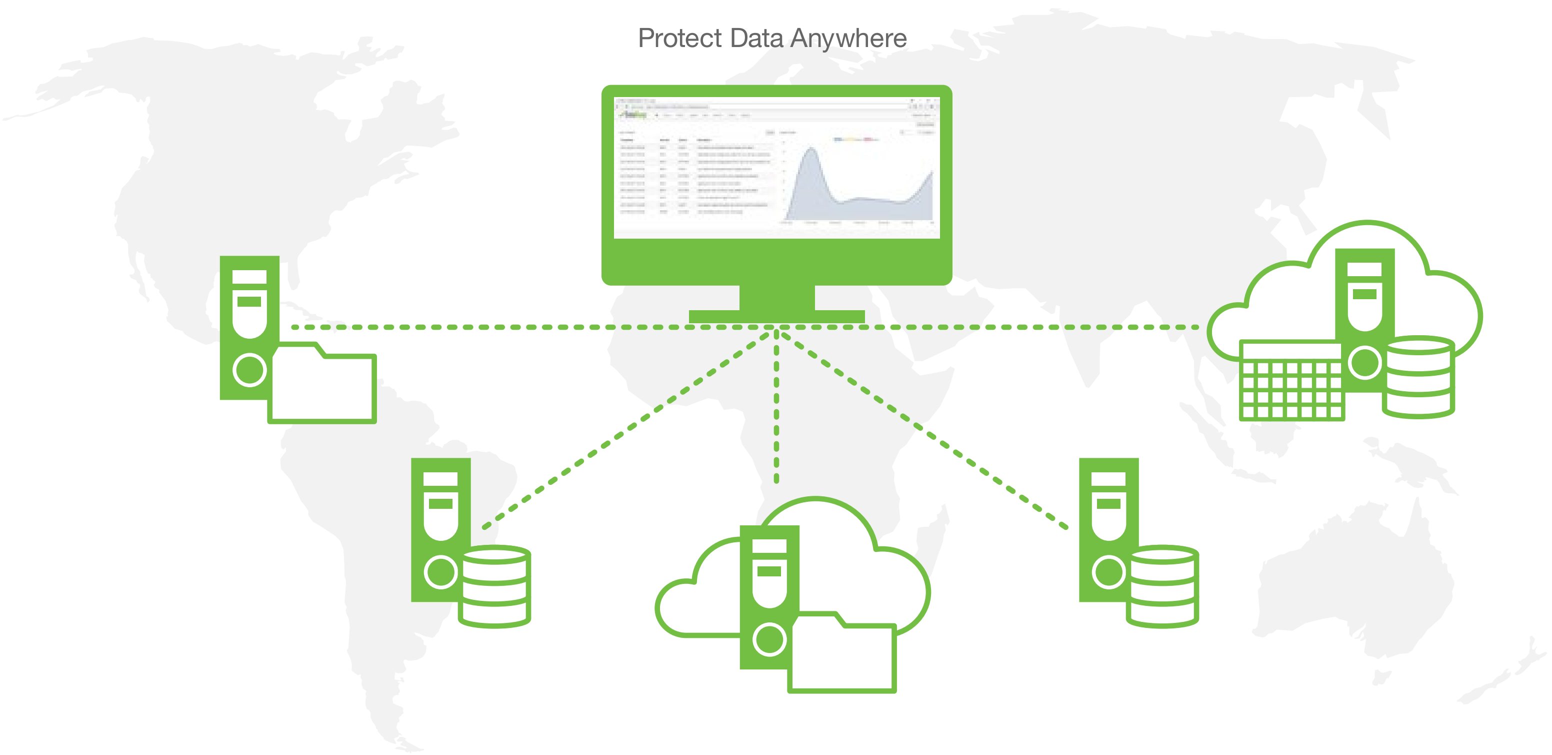
Superior Data-Centric Security with DataKeep

Network-centric security measures are important, but at the end of the day, they do nothing to protect your organization's most valuable asset — the data — when a breach occurs. A data-centric approach introduces a last line of defense to protect sensitive and private data against any possible loss when all other security measures fail.



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

DataKeep™ Key Features



Protect Data Anywhere

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 operating system (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.

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

DataKeep™ Key Features

forwarded to Systems Information and Event Management (SIEM) 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 on nefarious activities, reducing the risk of data compromise.

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.

Volume and File Level Encryption

DataKeep allows customers to deploy agents that encrypt data at the volume-level or for additional granularity, at file-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.

DataKeep agents can be deployed to any virtual or physical server running a supported operating system (OS).

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.

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 an open solution 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 while serving as your last line of defense against a breach.

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.

About SecurityFirst

SecurityFirst provides innovative and affordable software solutions that protect one of the world's most valuable assets – digital data. SecurityFirst specializes in data-centric cyber solutions that provide cryptographic splitting across a range of security options for robust data security and policy-defined access controls – all intended to meet the growing mandate for data privacy.

SecurityFirst™
Data-Centric Cyber Solutions

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

securityfirstcorp.com