FORNETIX

Secure Data Protection Platform
Solution Brief

RACKTOP

SEAGATE | GOVERNMENT SOLUTIONS

» HIGHLIGHT

Bringing Unmatched Encryption Management to Cost-Effective, Secure Data Storage

The Secure Data Protection Platform (SDP2) enables encryption for data-at-rest with zero impact on performance.

Replace traditional NAS data storage in both physical and virtual environments with a drop-in solution that is easy to implement and maintain. Eliminate the complexity of disparate tools by creating a simple, unified, and secure data protection solution. Data is shared securely using common protocols (SMB, NFS, iSCSI) and is protected via orchestrated versioning, replication, retention, and disposition capabilities.

SDP2 is ideal for organizations that must protect their sensitive data against unauthorized disclosures.

» TECHNOLOGY THAT GROWS WITH YOUR ORGANIZATION THROUGH A HIGHLY SCALABLE ARCHITECTURE

- Platform can scale from a few terabytes to multiple petabytes per node
- Option for hybrid storage to take advantage of SSD speed and HDD economy
- A single BrickStor can service thousands of users and virtual machines
- Manage multiple BrickStors across data centers with a unified user interface
- Fornetix® VaultCore™ supports lifecycle of tens of millions of keys

» GUARD YOUR DATA WITH CYBER RESPONSE WORKFLOW INTEGRATION

- Cyber response workflow operations can be executed through RESTful services
- Allows outside applications such as Splunk to execute changes and actions
- Allows the SDP2 to be responsive to cyber threats by aligning storage services and key management automation with security monitoring and response.

» MEET ORGANIZATION-SPECIFIC SECURITY REQUIREMENTS WITH A POLICY ENGINE

- Policy-driven architecture ensures consistent and compliant behaviors
- Settings are applied automatically based on use-case and data protection policy
- Policy can be configured to replicate snapshots efficiently
- VaultCore applies access controls according to NIST 800-57
- Fine-tune key management behavior based on operational need
- Can integrate with an HSM to provide additional security

» ACHIEVE TRANSPARENCY THROUGH AUDITING & TRACKING SERVICES

- BrickStor and VaultCore logs are compliant with Common Event Format (CEF)
- Easy integration with Elastic Search, Splunk, HPE ArcSight, and IBM Qradar
- CEF integration and audit workflows allow users to monitor and execute response plans

» ENSURE RELIABILITY WITH HIGH AVAILABILITY & REDUNDANCY

- BrickStor and VaultCore support high-availability deployments
- Solution can provide for offsite disaster recovery
- Clustering for storage and VaultCore appliances while maintaining replication

» FLEXIBLE DEPLOYMENT OPTIONS BEND TO YOUR ENVIRONMENT

- Entire SDP2 platform can be self-contained in one location or distributed
- Centralized key management appliances with distributed storage
- Data replicated securely between branch sites and main office for backup and archive

» TECHNICAL OVERVIEW

RackTop®, Seagate Government Solutions® (SGS), and Fornetix have developed a strategic relationship to combat external and insider cybersecurity threats. The result is a platform that provides the U.S. government, civilian agencies, military agencies, and contractors with a powerful combination of Fornetix advanced encryption key management and RackTop's high-performance storage using Seagate FIPS 140-2 certified drives. The integrated solution makes it easier to dynamically manage and re-key drives without compromising data security, a traditionally cumbersome and difficult process.

The software-based platform running on common x86 hardware allows for easy customizations to meet future requirements or unique deployment options. Seagate's self-encrypting FIPS drives offer security assurance enhancements to increase trust levels. The Fornetix VaultCore appliance creates, manages, and makes available the encryption keys used to control drive-level security. BrickStor acts as a client to VaultCore and uses standards-based security protocols to communicate with each drive. Security operations indirectly invoked by authorized end-user entities are authenticated using credentials stored in the key manager. VaultCore implements policy evaluation and mandatory access controls on BrickStor clients to ensure only the correct keys associated with BrickStor are provided. BrickStor exposes stored data using standard file protocols NFS and SMB while authenticating with Microsoft® Active Directory™.

The SDP2 solution combines the following systems:

Fornetix VaultCore — A highly-secure key manager appliance that is compliant with the Key Management Interoperability Protocol (KMIP), PKCS#11, and Common Event Format logging

RackTop BrickStor TI-3202E — Unified shared storage, BrickStorOS, and myRack™ Manager software supporting NFS and SMB

Seagate OneStor™ — 12GBs SAS enclosure with dual I/O controllers and SAS self-encrypting FIPS HDDs or SSDs