Rubrik Encryption at Rest Datasheet

DATA PROTECTION. SIMPLIFIED.

The Rubrik appliance delivers backup, instant recovery, replication, and archival in one, infinitely scalable fabric. Rubrik Converged Data Management powers the appliance, collapsing physically separate hardware and software resources—like backup software, replication, storage, and catalogs—into a single fabric that scales up to thousands of nodes.

Rubrik encrypts user and application data at rest using FIPS 140-2 Level 2 certified self-encrypting drives (SED) as its HDDs and SSDs. The data-at-rest encryption solution is completely turnkey–all SEDs ship completely configured. Rubrik's non-disruptive encryption offering is comprehensive, securing data in a cost-effective manner for all security conscious industries, including the government, financial, legal, and healthcare sectors. Many industries require compliance with rigid data protection policies in order to protect their classified, confidential, or personally identifiable information (PII).

FIPS 140-2 LEVEL 2 DRIVES

Tamper-evident self-encrypting HDDs and SSDs secure your data.

FLEXIBLE KEY MANAGEMENT

Protect keys with the included TPMs or use your existing KMIP 1.0-compliant key management solution.

PROTECT FROM PHYSICAL BREACHES

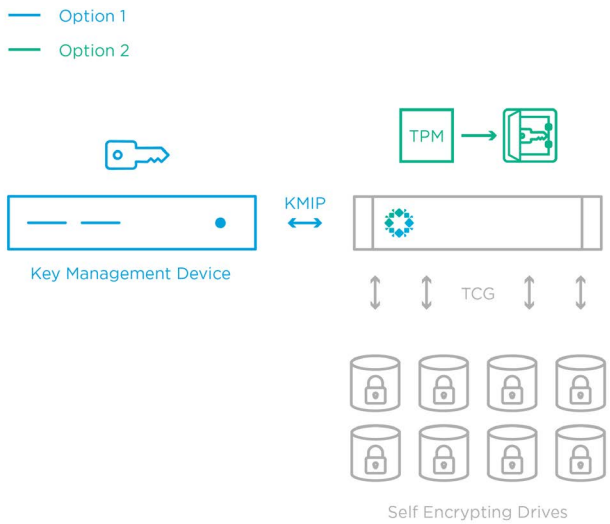
Your data is still secure even if a drive is stolen from your data center.

HOW IT WORKS

Rubrik adds Encryption at Rest while maintaining web-scale performance and speed. Self-encrypting drives provide the additional functionality of automatic data protection without additional intervention. Customers can ensure their data is protected even in the event of a physical theft or breach.

In addition, two key management solution options allow customers great flexibility. For customers who don't use an existing key management solution, cryptographic keys can be protected by the Trusted Platform Modules (TPM) that reside on each Rubrik node. For those who wish to utilize their existing solution, Rubrik supports external key managers using the industry standard Key Management Interface Protocol (KMIP 1.0).

In order to bootup or power cycle, Rubrik retrieves the cryptographic keys protecting its SEDs via its TPMs or key management server. These keys are then used to unlock and mount the drives. Furthermore, these security keys can then be used to instantly and securely delete data on a SED. Rubrik Encryption at Rest enables compliance with the requirements of HIPAA, SOX, PCI DSS, FIPS 140-2, NIST 800-88, and Common Criteria.



> "Rubrik provides comprehensive IT security solutions within their product line to meet Federal standards. Their hardware and software FIPS 140-2 certified encryption solution and secured Brik Operating System (BOS) leave no doubts in the mind of security-conscious organizations that their data is secure."
>
> — VICTOR MARQUEZ, CEO, MARQ SOLUTIONS

DON'T BACKUP. GO FORWARD.

Want to see more? Contact info@rubrik.com for a 15-minute demo. Visit www.rubrik.com and follow @rubrikInc on Twitter.