ENABLE VSAN ENCRYPTION WITH HYTRUST KEYCONTROL

Top 5 Reasons to Enable vSAN Encryption

01
Satisfy regulatory compliance mandates

02
Easy implementation with your existing VMware investment

03
Secure your sensitive data; avoid a data breach

04
Reduce your liability; protect your reputation

05
Encryption is required for sensitive government data

HyTrust KeyControl Features

- FIPS 140-2 Level 1 Validated
- FIPS 140-2 Level 3 Validation via HSM
- VMware Ready Validated
- Rapid rollout and easy to use
- Leverages existing vSAN functionality. No additional VMware modules to install
- Encrypt and still enjoy vSAN deduplication and compression

Who is HyTrust?

- Founded in 2007
- Backed by VMware and In-Q-Tel
- 40 granted and pending patents
- Data protection for federal agencies, global banks, insurers, and healthcare providers

Compliance Mandates That Call for Encryption

- NIST
- DISA
- FISMA
- FedRAMP
- PCI DSS
- HIPAA
- PCI

Gartner statistics:

- 2,216 confirmed data breaches
- 2,216 confirmed data breaches and 53,000+ incidents in 2017.
- $3.86 million - average cost of a data breach globally, up 6.4% from last year.
- Through 2020, driven by the increasing risk of a data breach, more than 50% of enterprises will purchase enterprise-wide encryption products, which is a significant increase from fewer than 20% today.

vSAN encryption with HyTrust KeyControl protects against data breaches. Don’t become a statistic!

To learn more, visit www.carahsoft.com/hytrust