# Data Encryption with StorMagic & Fornetix

## Why is data security so important at the edge?

The need for data security has never been more important due to the negative impact security breaches can have on an organization — such as point-of-sale malware attacks, leaked credit card payment details, and ransomware attacks. In some cases, these incidents have resulted in hefty fines and financial penalties for the companies involved. Couple that with the need to comply with government regulations such as HIPAA, GDPR, SOX, and PCI DSS, and securing data quickly jumps to the top of most IT departments' to-do lists.

Most large organizations that have enterprise-class datacenters are focused on data security at these locations because there is so much data at risk. However, edge computing locations like retail stores, branch offices, factories, warehouses, and even oil rigs may not get the same level of attention. These smaller locations typically don't have the same levels of physical security — servers are often kept in unsecure rooms or closets, under a desk, or even right in the middle of a factory floor, making it easier to access the data or steal the servers. Data security is often overlooked at the edge, and this is exactly the problem that StorMagic and Fornetix are focused on solving.

## StorMagic SvSAN

StorMagic SvSAN removes the need for a physical SAN in some of the world's most demanding environments by converting the disk, flash and memory of two servers into a virtual SAN. SvSAN coupled with a hypervisor (VMware or Microsoft) and any server hardware creates a hyperconverged solution that is perfect for large organizations with thousands of sites and companies running SME datacenters that require a highly available, two-server solution that is simple, cost-e ective and flexible. SvSAN has the ability to encrypt data as it's written to disk by using military-grade, FIPS 140-2 compliant algorithms and is fully integrated with Fornetix Key Management Server.

## Fornetix Key Orchestration KMS

Fornetix Key Orchestration is an enterprise encryption key management solution that enables a unified approach to data security by deploying and enforcing encryption across an entire organization. This unification allows for centralized storage and control for all encryption keys across all types of environments; whether it's on premise storage, virtualized, or cloud. Through a robust and extensive API and a dedication to industry standards, Fornetix is built on interoperability. When paired with the ability to scale to millions of keys, Key Orchestration ensures seamless integration with organizations today and provides the ability to grow with them in the future.

## What are the benefits of this combined data encryption solution?

**Simple to Use** - 100% software approach that encrypts data before writing to disk and seamlessly integrates with key management servers.
**Cost-Effective** - Eliminates the need for operating system or hypervisor-level encryption. No special self-encrypting disk drives, RAID cards or hardware acceleration cards required.

**Flexible** - Choose to encrypt all or only selected volumes of data, and have rich features like secure erase, rekey and Predictive Storage Caching typically found only in datacenter-class encryption solutions.
**Highly Secure** - Meets the most strenuous security requirements demanded by vertical industries such as healthcare, government, finance, and others. SvSAN Data Encryption is FIPS 140-2 compliant through OpenSSL XTS-AES-256 bit encryption and meets HIPAA, PCI DSS, SOX, and EU GDPR compliance requirements. All data is encrypted on the drives and in-flight between storage caching tiers and high availability clustered servers.

## How Does it Work?

**Step 1: Establish trust relationship between Fornetix KMS and SvSAN**
Using Fornetix Key Orchestration Server user interface, create SvSAN clients so keys can be provided and managed for SvSAN.

**Step 2: Create an encrypted volume or encrypt an existing volume**
When a volume is selected for encryption, SvSAN will request a pair of symmetric 256-bit AES encryption keys to be created and activated from the Fornetix Key Orchestration KMS. Two keys are required as the XTS-AES cipher actually requires a 512-bit key - the two 256-bit keys provided by the KMS are concatenated together to form a 512-bit key. Each volume will have its own pair of encryption keys. For a mirrored volume, the same encryption keys are used for both sides (plexes) of the mirror.

**Step 3: The KMS returns encryption key identifiers to SvSAN**

**Step 4: SvSAN obtains the encryption keys using the identifiers**
The keys are not persistently stored by SvSAN, they only reside in memory for security reasons. If SvSAN is rebooted then the keys need to be retrieved from the KMS.
Inability to retrieve the keys from the KMS will mean that the data is inaccessible.

**Step 5: The keys are used to encrypt/decrypt the data**
When data is written to the volume the XTS-AES cipher uses the keys to encrypt the data which is then written to disk.
When writing data to mirrored volumes, the user data that is synchronously mirrored between the VSAs will also be encrypted.
When data is read from the volume the XTS-AES cipher uses the keys to decrypt the data which is then returned to the application.