

# The Challenges of One Size Fits All Encryption



## INTRODUCTION

Encryption has become one of the most important tools in the information security arsenal, providing an effective approach to reducing the risk of data loss and therefore avoiding the costs associated with a large breach.

The traditional approach to implementing encryption has been to deploy a single encryption technology throughout the enterprise, regardless of the type of user or the nature of the data to be protected.

However, in the face of an increasingly complex regulatory landscape, an expanding ecosystem of storage devices, and the threat from highly sophisticated external, (or worse, insider) attacks, many enterprises are experiencing significant challenges trying to deploy a single encryption technology strategy for all data and systems. The simple fact is that this approach no longer protects what's important to your organization in a way that is manageable and scalable.

## THE CHALLENGES OF ONE SIZE FITS ALL ENCRYPTION

For many years sector-based encryption, also known as Full Disk Encryption (FDE), has been the standard approach to protecting data on personal computers. However, simply relying on FDE alone for encryption across the enterprise has exposed limitations and introduced management challenges that are now forcing organizations to look for a more flexible strategy to protect sensitive information.

While FDE provides many benefits, it also forces changes in the ways users operate and the ways in which systems are administered. In instances where users share systems, or where they handle especially sensitive information such as healthcare data, financial information or highly proprietary intellectual property, FDE alone is unlikely to offer enough flexibility to meet security best practices and adequately reduce the risk to your organization.

Relying only on FDE introduces a number of problems, including:

- Impact on end-users who are required to learn a new process for pre-boot authentication – often stalling or even derailing successful roll-out of widespread encryption
- The requirement to allow administrators – especially contractors in IT service roles – to have full decryption rights to a system in order to perform administrative tasks- potentially exposing sensitive information
- The inability to segregate access between users - so all users sharing the same system can see all data

## CREDANT SOLUTIONS

*CREDANT data security solutions ensure that encryption and security requirements are consistently and efficiently enforced—regardless of where the data resides.*

### ONLY CREDANT ENABLES ORGANIZATIONS TO:

- Encrypt and secure data across multiple endpoints from a common management platform
- Create automatic audit trails that offer proof of end-to-end data security
- Provide a transparent end-user interface that supports user productivity while keeping data safe
- Choose from full-disk encryption (FDE), device-specific encryption, or a combination of both
- Integrate management for Windows® BitLocker™

CREDANT data security solutions provide centrally managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:

- Prove that data stored on lost or stolen devices is encrypted.
- Prevent data from leaving the organization unprotected on removable media.
- Safeguard data from unwarranted access, thus reducing risk of internal breaches.

## The Challenges of One Size Fits All Encryption

- › Additional workload in updating the operating system as a result of the need to pass credentials to the pre-boot environment before work is performed – introducing additional administration burden and slowing down the implementation of potentially critical updates
- › Gaps in coverage or inability to protect the increasing quantities on sensitive data on removable media
- › Inability to integrate emerging standards such as Opal (for self-encrypting drives) and Microsoft BitLocker for Windows 7 into a broader encryption strategy

While legacy full disk encryption provides a good baseline for many devices, these issues may make it totally unsuitable for some systems. Because FDE is device-centric, encrypting only the local hard drive, it does not protect data transferred to removable media or external drives like those commonly used for quick backups. Thus, a more flexible approach to protecting sensitive data is required. This is the primary reason that FDE solutions are rarely, if ever, deployed successfully across the entire enterprise infrastructure.

### A BETTER SOLUTION— FLEXIBLE, SECURE ENCRYPTION

The most effective approach to protecting sensitive data will therefore use the right encryption method for the type of system and data to be secured.

Such an approach must be able to combine the management of FDE, policy-based encryption, removable media protection, and utilize new, self-encrypting drive technologies, all within the same set of management tools. This will enable your organization to deploy the right tools to protect systems in the most effective manner.

- › FDE primarily for supported single-user systems where it causes the least end-user and administrative impact and where less sensitive information is held

- › Policy-based encryption where systems cannot support FDE, are shared, or where highly sensitive data resides that must remain protected at all times even from illicit insider access
- › Removable media encryption to protect against one of the most common sources of breach
- › Management of Self-Encrypting Drives (SED's) to utilize this high-performance hardware based technology

### HOW CREDANT CAN HELP

CREDANT provides a single set of management tools to enable your organization to select, deploy and centrally manage the most appropriate encryption technology to meet your security needs.

As a solution partner focused on securing highly sensitive data, CREDANT provides a single set of management tools for:

- › Integrated management for BitLocker
- › Full Disk Encryption for Windows and Mac OS/X
- › Policy-based Encryption to protect highly sensitive data based on user role
- › Enterprise management of Self-Encrypting Drives
- › Highly secure, easy to use, yet robust encryption for removable media
- › Hand-held device encryption and encryption management
- › Centralized compliance reporting

This unique breadth of coverage helps ensure that data remains protected wherever it resides, that the risk of a significant breach is dramatically reduced, and that your organization has the ability to deploy the most appropriate encryption technology to meet your needs today and in the future.