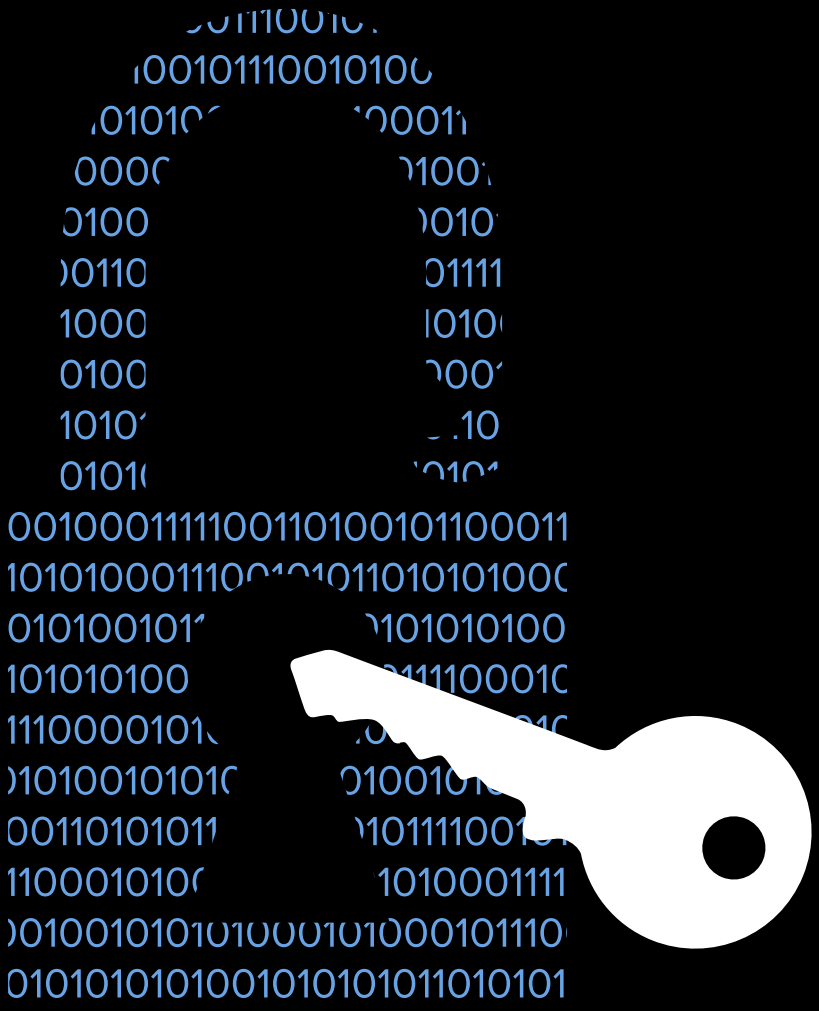
THE ENCRYPTION GUIDE



Townsend SECURITY

THE ENCRYPTION COMPANY

“Encryption and key management can’t become ubiquitous the way they need to be without being easy and affordable. That’s a fundamental fact.”

- Patrick Townsend, Founder & CEO of Townsend Security

Contents

Introduction

Encryption *Must* be a Part of the Solution

Data security today is a major problem. Security professionals, administrators, and executives know this because highly publicized data breaches occur on what seems to be a monthly, if not weekly, basis, and lesser-publicized data breaches happen nearly every day. Loss of customer trust, huge payouts in fines, damage to reputation, and business leaders losing their jobs are just some of the consequences associated with a data breach.

Most high profile data breaches result in a lot of finger pointing with little discussion about what actually went wrong, and how other companies can prevent suffering a similar fate. Unfortunately, it is often revealed that some of the largest data breaches could have been prevented had the organization used proper encryption and encryption key management where it was needed.

Unencrypted sensitive data is a dangerous reality for most businesses. It's an issue complicated by the fact that sensitive data is typically processed and stored in many disparate, fragmented locations so that administrators and business leaders alike aren't certain where their data is, if they're handling unknown sensitive data, which data should be encrypted, or know if their data is being encrypted at all.

In this eBook designed for IT professionals and executives, we will discuss how critical encryption is to your business continuity, how a solid encryption plan can help protect your business in the event of a data breach, and encryption best practices that will ensure your data security plan is effective and defensible, and keep you and your customers safe.

While encryption is only a component of a holistic security solution that should also include people, process, and other technologies, it is a mission critical component of the solution.

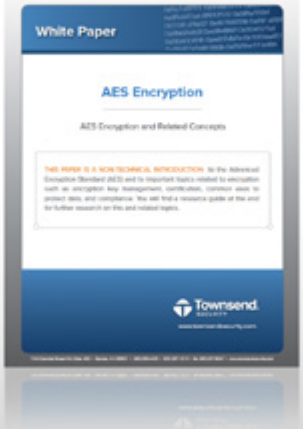
What is Encryption?

A Non-Technical Overview

Encryption is a means of encoding data such as words, numbers, and images, using mathematical algorithms in order to make that data undecipherable to unauthorized viewers. Over the past several decades encryption has evolved and changed to meet the demands of evolving technology. Today the encryption algorithm accepted as the highest standard is the Advanced Encryption Standard (AES). AES is a formal encryption method adopted by the National Institute of Standards and Technology (NIST) of the US Government, and is accepted worldwide.

In the process of encrypting data, an encryption key is created that allows users to encrypt and decrypt the data when it needs to be accessed. The encryption key must be protected in order to prevent access to the data from malicious or unauthorized users. Encryption key management is essential to a successful encryption solution, and it is often required or strongly recommended by most industry regulations.

White Paper
AES Encryption &
Related Concepts



Download Now

THE ENCRYPTION COMPANY

Know When to Encrypt

Knowing when you need to encrypt data is a critical step in developing a holistic security plan. Today the strongest driving factor for companies to encrypt data is to meet compliance regulations. However, many compliance regulations only address the bare minimum security needs, and a poor execution of these requirements may not help you in the event of a data breach.

With the ongoing increase in corporate data breaches and identity theft, many businesses choose to encrypt sensitive data primarily in order to help protect themselves in the event of a breach. This strategy often helps a company meet or exceed compliance regulations as well.

Encrypt to Protect Yourself in the Event of a Data Breach

The number one reason many companies are concerned about a data breach is cost. The average cost of a data breach in 2013 was $5.4 million(1). The cost of a breach not only includes penalty fines but extends far beyond and includes the cost of:

- **Brand damage**
- **Litigation**
- **Credit monitoring**
- **Lost customers**
- **Bad publicity**
- **Forensic investigations**
- **Yearly audits**
- **Lost jobs**

These, as well as the resignation of company executives, are consistent outcomes of a data breach.

Risk mitigation is a huge motivator for many companies to encrypt sensitive data. Under several industry regulations such as PCI-DSS and HIPAA/HITECH, if a data breach occurs, but the lost data is encrypted using standard encryption methods and encryption key management best practices are in place, an organization does not have to report the breach. Therefore breach notification can be avoided and no financial loss or brand damage incurred.

Encrypt to Meet Compliance

Many organizations decide to encrypt sensitive data because their industry requires it, or because they have recently failed a security audit and must comply within a set timeframe. When deciding to encrypt sensitive data you must first ask yourself these questions:

- **What kind of data do I process or collect?**
- **Where is my data located?**
- **Which industry regulations do I fall under?**
- **What do those regulations say about data security and encryption?**

White Paper
Meet the Challeneges of PCI-DSS

Download Now

The regulations outlined below are the most common industry data security regulations. All of these require encryption to protect customer and consumer data.

WHAT REGULATIONS DO I FALL UNDER?	
PCI DSS	If you take or process credit card information, you fall under PCI DSS standards. This means that you must encrypt credit card information when it is at rest or in motion and protect encryption keys in accordance with Section 3.
HIPAA/HITECH	If your company operates in the medical sector—which is any organization defined as a Covered Entity within the HIPAA/HITECH act—you and your business associates fall under HIPAA/HITECH data security regulations. The HITECH act of 2009 strengthened HIPAA regulations tremendously by referring to the National Institute of Standards and Technology (NIST) for both encryption standards, best practices of encryption key management, and the collection of system logs. The Omnibus Rule, which became effective in March 2013, expanded the Health and Human Services (HHS) Security Rule to include "business associates" under covered entities that must comply with HIPAA/HITECH data security regulations. Business associates includes patient safety organizations (PSOs), health information organizations (HIOs) and subcontractors.
GLBA-FFIEC	The Gramm-Leach-Bliley Act and Federal Financial Institutions Examination Council regulate data security in the financial sector. Under these regulations the financial industry is defined broadly and includes banks, credit unions, trust companies, insurance companies, and brokerage firms, but also covers credit reporting agencies and other financial institutions.
Sarbanes-Oxley (SOX)	Any publicly traded company in the United States falls under SOX.
Federal & State Laws	Currently 46 out of 50 states have data privacy regulations requiring organizations to report data breaches involving personally identifiable information. Many organizations are unaware of their own state's data privacy laws, or assume those laws do not apply to them, when in fact they almost always do.

Know What to Encrypt

Each regulation mentioned in the previous section outlines the types of data that need to be encrypted. In general, data that needs to be encrypted is personally identifiable information (PII) that identifies a person's financial, cardholder, or health information, and is often information that can be used to commit theft or fraud. With the vast amount of personal information that gets collected by credit card, health, financial, and commerce organizations, today information such as email addresses, usernames, and passwords are considered PII by some regulations and state data privacy laws, and must also be encrypted.

Knowing what regulations your organization falls under will inform you to what you should encrypt.

WHAT DATA SHOULD I ENCRYPT?	
PCI DSS	Primary Account Numbers (PAN)
HIPAA/HITECH	Health organizations and business associates should protect Protected Health Information (PHI) as defined by the latest HIPAA/HITECH Act rules. This includes Personally Identifiable Information (PII) as well as patient treatment information.
GLBA-FFIEC	If operating a financial institution you should protect nonpublic personal information (NPI) of a customer or consumer. GLBA defines NPI broadly and may include names, addresses, phone numbers, and social security numbers.
Sarbanes-Oxley (SOX)	Publicly traded organizations must protect sensitive data related to financial reporting. SOX also provides clear guidance around encryption key management.
Federal & State Laws	Many states require breach notification if an individual's first name (or first letter of the first name) and last name are exposed in conjunction with their social security number, health information, or cardholder information, and neither pieces of data are encrypted. Breach notification is also required if an individual's email address is exposed in conjunction with a password or security question, and this data is unencrypted.

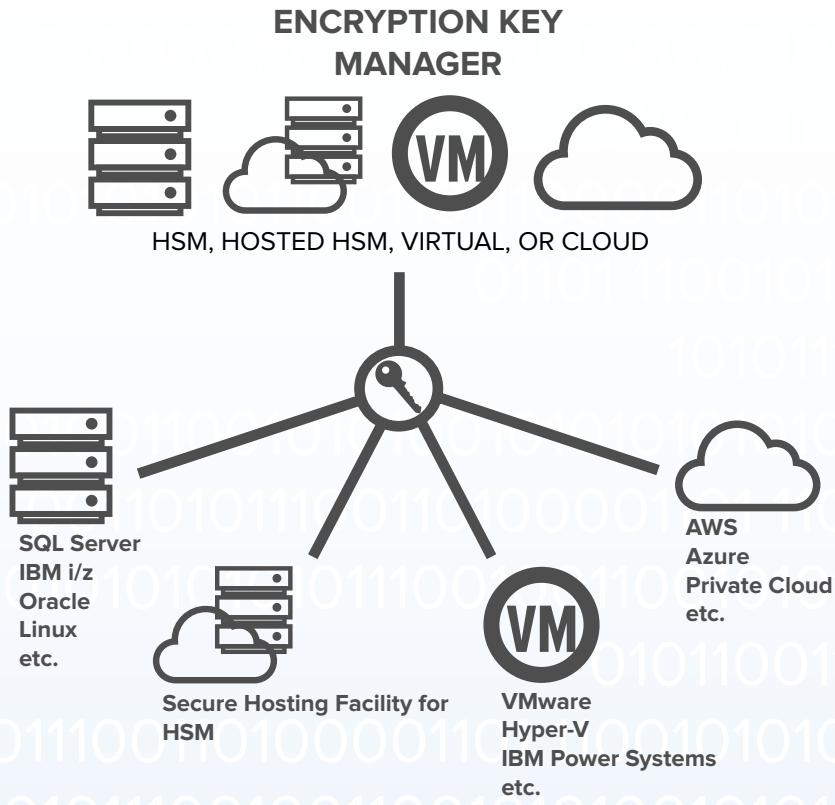
Know Where to Encrypt

Locating sensitive data is a critical first step to creating a holistic security solution. Many IT administrators know that this step can be the most difficult, especially in larger enterprises where each department uses different methods and means of handling and storing data. Luckily, today solutions exist that centralize the encryption process across the company in a consistent and affordable way, regardless of where the data is located.

You can encrypt your data through one holistic solution even if your data is located on physical servers, virtual servers, hosted servers, or in the cloud. Depending on your vendor, an encryption key manager can support encryption and key management for data anywhere. Key managers themselves can be hardware, virtual appliances, or cloud instances.

Webinar:
Encryption & Key Management Everywhere Your Data is

Watch Now



Encryption Best Practices

A successful encryption solution relies on how well you implement best practices around people, process, and technology. A poorly executed encryption project can leave you vulnerable. Encryption solutions that tend to fail are do-it-yourself or "in-house" encryption projects that cut corners, have no certifications, and fail to encrypt all sensitive data and protect encryption keys. In a study of the certification program, NIST found nearly 50 percent of software vendors had errors in their encryption solutions. It isn't easy to get encryption right. A certificate of validation from NIST is your assurance that AES encryption does what it is supposed to do. Every time.

In order to have a successful encryption solution you must utilize industry standard encryption methodologies, encryption key management, use NIST validated solutions, and follow administrative and technological best practices such as dual control and separation of duties. Here's why:

Standards-Based Encryption

Selecting the right encryption technology to protect data at rest is important. Some encryption technologies, such as DES, do not provide enough security now that computers have become so powerful. Other encryption technologies are secure today, but will soon not meet the minimal requirement for security due to technological advancements. Triple DES falls into this category. Other encryption technologies are secure, but do not satisfy federal and international standards. Twofish and Blowfish are examples of this type of encryption technology.

One encryption technology meets all of the requirements for strength, longevity, and regulatory approval – the Advanced Encryption Standard (AES). AES has been adopted by the federal government as an approved encryption technology under the

FIPS-197 standard. AES is accepted by the Health Insurance Portability and Accountability Act (HIPAA), and is accepted by all credit card issuers for data security including Visa, Mastercard, Discover, American Express, JCB, and others. AES has also been incorporated into Pretty Good Privacy (PGP) encryption which is used by banks, insurance companies, benefits providers, and most major financial institutions for securing data in motion.

Selecting a data security solution based on AES is a safe and wise decision. It provides the best encryption security, the best regulatory coverage, and the best position for future development.

Encryption Key Management

The protection of encryption keys, also called encryption key management, is critical to successful encryption. In fact, it is so crucial that most industry compliance regulations require or strongly recommend the use of an encryption key manager.

When you encrypt sensitive data, a key is used to “lock” the data on encryption and also created to “unlock” the data on decryption by authorized users. If that key is stored on the same server as your encrypted data, then any hacker or malicious intruder will be able to decrypt and access plaintext data resulting in a data breach. In order to prevent this you must store encryption keys in a separate location away from the encrypted data in a hardware security module (HSM), virtual appliance, or cloud key manager—dedicated key servers that store and manage encryption keys for data in databases, virtual systems, or the cloud.

Encryption Key management

Not protecting your encryption keys is a lot like leaving your house in the morning and taping your key to the front door. It would be easy to find your key there, but you're practically inviting an unwanted intruder.

Using key management best practices is fundamental to preventing unauthorized access to encryption keys. In order to have effective encryption you must securely separate the data being encrypted from the keys performing that data encryption. An encryption key manager enables a secure channel between the encryption keys and wherever that data may reside. Technology has evolved to enable stronger management so that companies no longer need to leave their encryption keys vulnerable to attackers.

If you do experience a breach of encrypted sensitive data, and you have secured your encryption keys away from the compromised data, many compliance regulations will consider that data "safe," and you may be able to avoid breach notification.

eBook:
ENCRYPTION KEY MANAGEMENT SIMPLIFIED

Download Now

THE
ENCRYPTION
COMPANY

Certifications

Using NIST validated AES encryption and FIPS 140-2 compliant key management is critical to ensuring that your security solution will stand up to scrutiny in the event of a data breach. These certifications are difficult to acquire and are only given to encryption and key management systems that have been heavily tested against government standards. Using trusted third-party systems is typically the easiest way to acquire and implement this technology. Many industry regulations require that your security solutions have these certifications.

NIST Validated AES Encryption - The National Institute of Standards and Technology (NIST) established AES as the highest standard for encryption in 2001. AES supports nine modes of encryption, and NIST defines three key sizes for encryption: 128-bit, 192-bit, and 256-bit keys. Any encryption that you use to protect data at rest should be AES standard encryption. When encrypting data in motion, use industry standard encryption such as PGP.

FIPS 140-2 Compliant Key Management - The highest standard for encryption key management is the Federal Information Processing Standard (FIPS) 140-2 issued by NIST. A key management hardware security module (HSM) with NIST FIPS 140-2 compliance will offer the highest level of security for your company.

About Townsend Security

Townsend Security is a leading provider of encryption and key management systems for over 20 years. We help each and every one of our customers achieve industry standard data protection and meet compliance regulations in less time and at an affordable price. Townsend Security provides companies with cost-effective, easy-to-use, NIST validated AES encryption and FIPS 140-2 compliant encryption key management solutions to help our customers meet evolving compliance requirements and protect sensitive information.

Web: www.townsendsecurity.com/partners
Email: info@townsendsecurity.com
Phone: (800) 357-1019 or (360) 359-4400
Twitter: @townsendsecure

Townsend® SECURITY