Business Brief

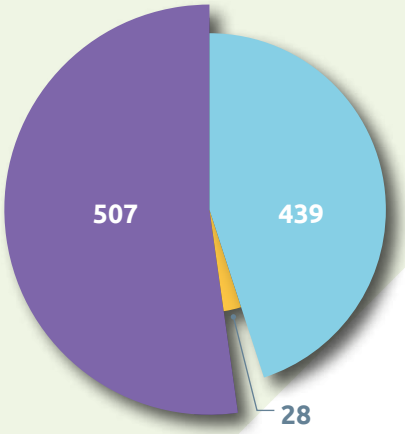
SecureDoc™

Data Security: Encryption Adoption

Encryption is one of the fastest emerging data security options today. Organizations are increasingly adopting it to address the growing concerns of data safety, and data privacy for compliance regulations.

Why? Just look at these stats:

974 Total Breach Incidents[1]

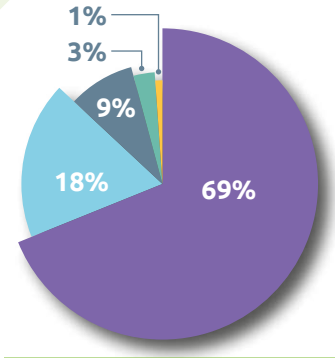


- # of Breaches < Million Records (**45.1%**)
- # of Breaches > Million Records (**2.9%**)
- # of Breaches Unknown Records (**52.0%**)

Data Records Loss Frequency

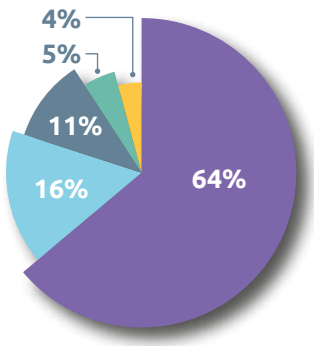
Every Second 35 | Every Minute 2,116 | Every Hour 126,936 | EveryDay 3,046,456

Percentage of Breach Incidents by Source



- Malicious Outsider
- Accidental Loss
- Malicious Insider
- Hackivist
- State Sponsored

Percentage of Breach Incidents by Type



- Identity Theft
- Financial Access
- Account Access
- Existential Data
- Nuisance

The Aftermath of Data Breachers [2]

$4m	Average total cost of data breach
29%	Increase in total cost of data breach since 2013
$158	Increase in total cost of data breach since 2013
15%	Percent increase in per capita cost since 2013

Loss of:

- Financial Record/Health Records
- Tax Information
- Customer Payment Records
- Personally Identifieable Information
- Proprietory Information
- Passwords

Massive Fines
Irreparable Brand Damage
Lost Business

1. Source: BREACHLEVELINDEX.COM January 2016 to June 2016
2. Source: 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute; A survey of 383 companies in 21 countries. $USD

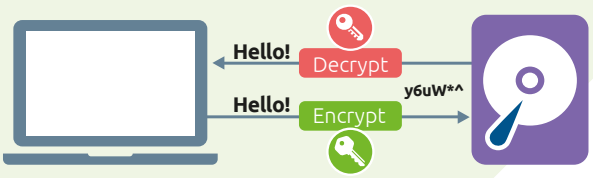
SecureDoc™

Protecting Against Loss

Adopting Encryption

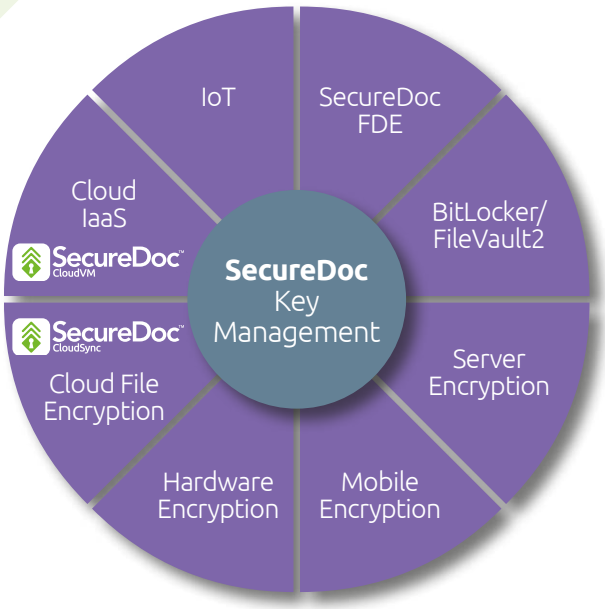
Data Encryption is a time-tested tool that can severely hinder attackers in their goal to steal your data. **Encryption is basically a way of scrambling computer data so it can only be read by the people you want**. Encryption converts data from plaintext to ciphertext, through use of an encryption algorithm which creates an encryption key – Only this key unlocks the data.

Today, sensitive data resides everywhere – On laptops and desktops, USB media, end-user-owned devices, on VMs in the Cloud. The need to control access of endpoints and data, and how data moves, is the number one reason enterprises are adopting full encryption. **However, simply deploying encryption isn't enough. Enterprises need employees to adopt it.**



Encryption and key storage is not hard. Key and Policy Management, getting the right keys to the authorized users and managing the lifecycle of the keys is the challenging part.

Introducing WinMagic's SecureDoc Solution



The Power of Unified Key Management

WinMagic's core offering, secures data at rest by managing how it is encrypted, regardless of where it resides, or on what operating system. SecureDoc provides enterprises a comprehensive data security solution that supports compliance with security and privacy regulations, without increasing IT costs significantly, or compromising end user productivity.

SecureDoc is user-friendly, keeping costs low, while ensuring IT administrators are efficient, and end user experiences are unaffected.

WinMagic's SecureDoc Enterprise Server (SES) provides organizations total control over their data security environment, ensuring maximum security and transparency in the regular work flow. WinMagic's application-aware key management, or Intelligent Key Management, not only manages the keys, but the related policy and configuration for the end point encryption.