N|DE
Network Defense Essentials

Module 11

Data Security

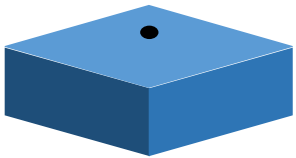
Module Objectives

1. Understanding Data Security and its Importance
2. Understanding the Different Data Security Technologies
3. Understanding the Various Security Controls for Data Encryption
4. Overview of Disk Encryption, File Encryption, and Removable-media Encryption Tools
5. Understanding the Methods and Tools for Data Backup and Retention
6. Understanding the Data Loss Prevention (DLP) and DLP Solutions

Module Flow

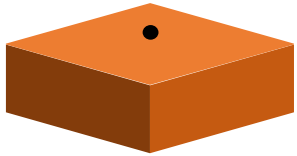
01

Understand Data Security and its Importance



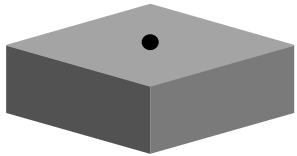
02

Discuss Various Security Controls for Data Encryption



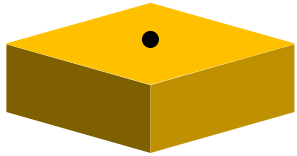
03

Discuss Data Backup and Retention



04

Discuss Data Loss Prevention Concepts



What is Business Critical Data?

- Data is the **heart** of any organization
- Critical data contains information that is important for business operation
- **Identification** and **classification** of business-critical data is the first step in securing an organization's data

Examples of Critical Data

1. Accounting files
2. Databases or any business-related data
3. The operating system files purchased with a computer, CDs, software, etc.
4. Important office documents, spreadsheets, etc.
5. Software downloaded (purchased) from the Internet
6. Contact Information (email address book)

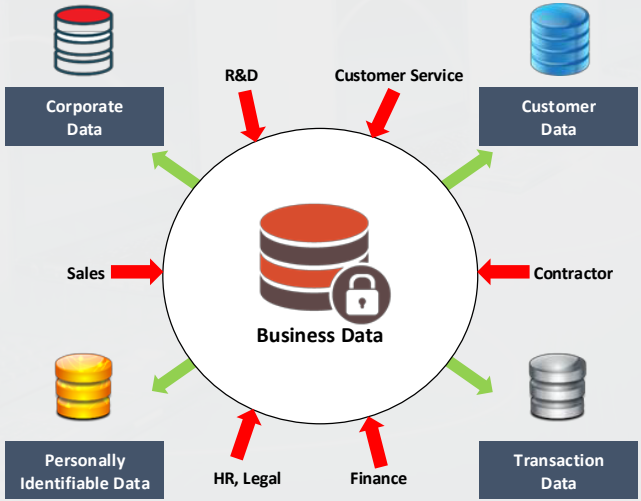
Need for Data Security

- Data is an organization's ultimate asset, which attackers may interested in
- If an organization's data is exposed or lost by any means, it can severely damage **business** and **reputation**

Data Loss Risks in Business Environment

Cause

- Loss/theft of laptops and mobile devices
- Unauthorized data transfer to USB devices
- Improper sensitive data categorization
- Data theft by employees/external parties



Effect

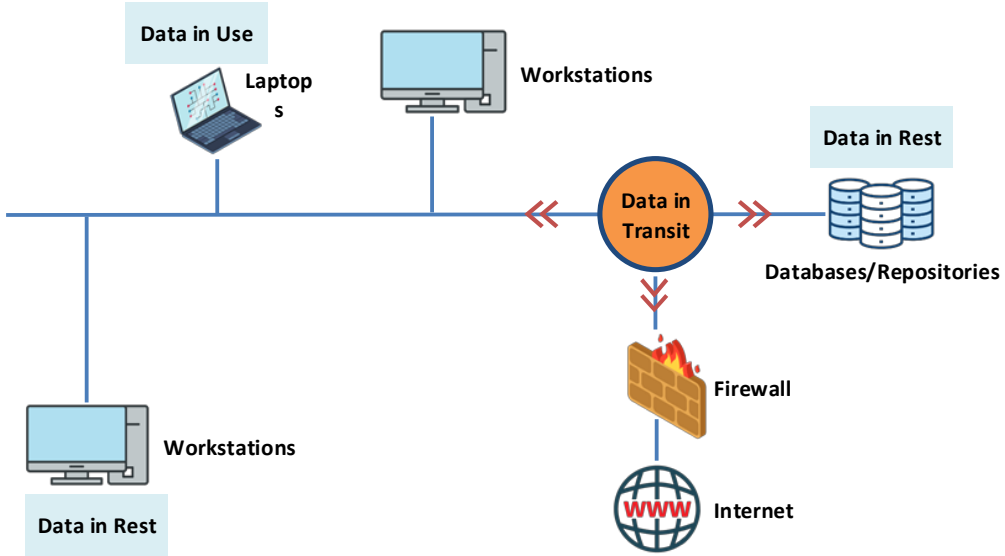
- Brand damage and reputation loss
- Competitive advantage loss
- Loss of customers
- Market share loss
- Shareholder value erosion
- Fines and civil penalties

Data Security

Data security involves the application of various **data security controls** to prevent any intentional or unintentional act of data misuse, data destruction, and data modification

Three Critical States of Data Security

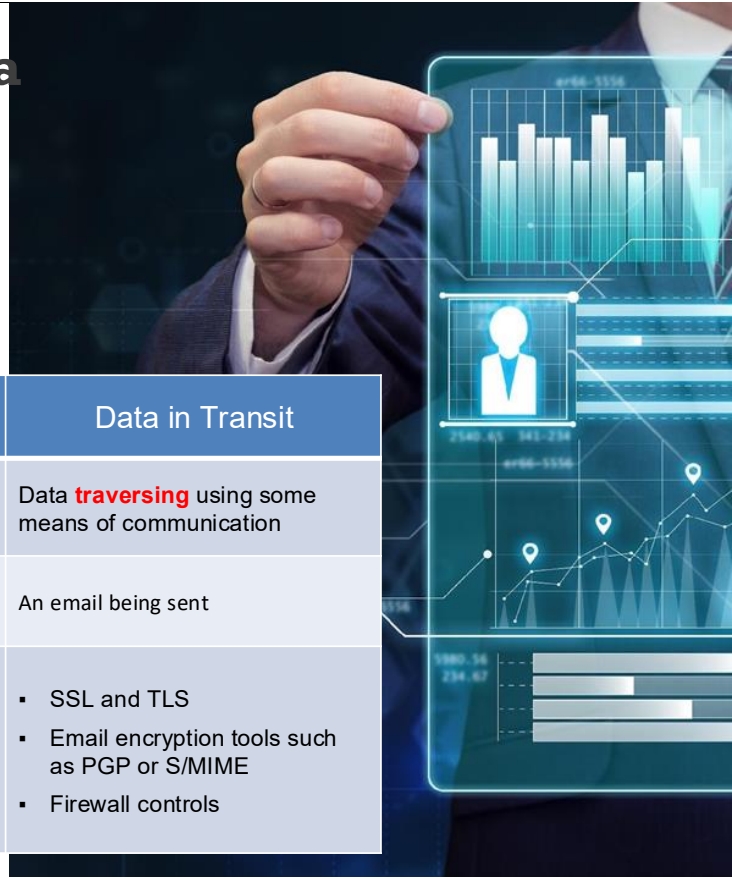
1. Data at Rest
2. Data in Use
3. Data in Transit



Example: “Data at Rest” vs “Data in Use” vs “Data in Transit”

Proper implementation of data security measures are required in **each state** to proactively enhance data security

	Data at Rest	Data in Use	Data in Transit
Description	Inactive data stored in **digitally** at a physical location	Data stored in **memory**	Data **traversing** using some means of communication
Examples	Customer bank balance stored in database	Data stored in RAM	An email being sent
Security Controls	▪ Data encryption ▪ Password protection ▪ Tokenization ▪ Data federation	▪ Authentication techniques ▪ Tight control on this data’s accessibility ▪ Full memory encryption ▪ Strong identity management	▪ SSL and TLS ▪ Email encryption tools such as PGP or S/MIME ▪ Firewall controls



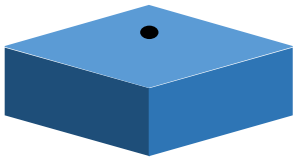
Data Security Technologies

Data Access Control	**Authenticates** and **authorizes** users to access data
Data Encryption	Protecting information by transforming it in such a way that it cannot be read by an unauthorized party
Data Masking	Protecting information by obscuring specific areas of data with **random characters** or **codes**
Data Resilience and Backup	Making a **duplicate** copy of critical data that can be used for restore and recovery purposes when a primary copy is lost or corrupted either accidentally or on purpose
Data Destruction	**Destroying** data, so that it cannot be recovered and used for wrong motives
Data Retention	Storing data securely for **compliance** or business requirements

Module Flow

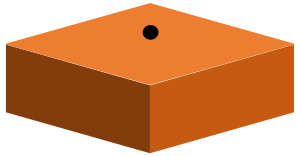
01

Understand Data Security and its Importance



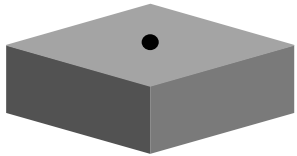
02

Discuss Various Security Controls for Data Encryption



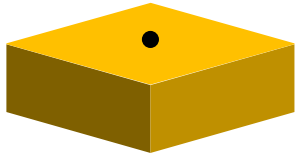
03

Discuss Data Backup and Retention



04

Discuss Data Loss Prevention Concepts



Data Encryption Techniques

Disk Encryption

Full disk encryption is the **encryption of all data** in a disk except the master boot record (MBR)

File-level Encryption

In this type of encryption, the encryption occurs at a **filesystem level**, and in combination with a cryptographic algorithm, the encrypted data will be extremely secure

Removable Media Encryption

Removable media encryption prevents removable media devices such USB flash drives, portable hard disks, digital cameras, smartphones, tablets, etc. from **unauthorized access**

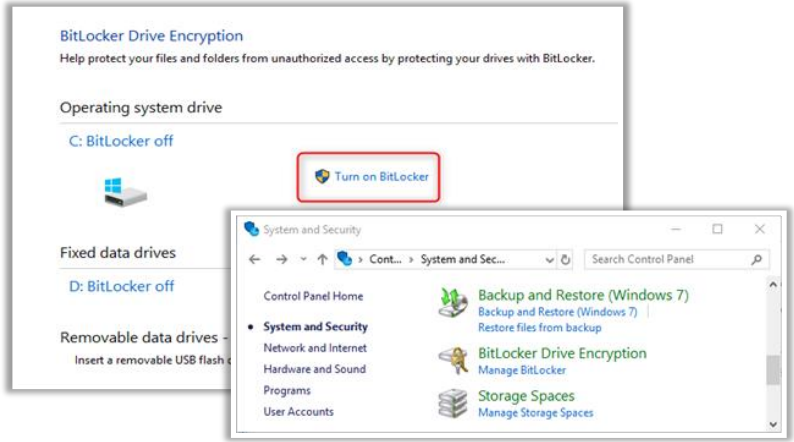
Disk Encryption: Implementing Built-in Disk Encryption for Windows

1. Enabling Device Encryption

- ✓ Go to **Start** → **Settings** → **Update & Security** → **Device Encryption**
- ✓ **Turn on** Device encryption option

2. Enabling Standard BitLocker Encryption

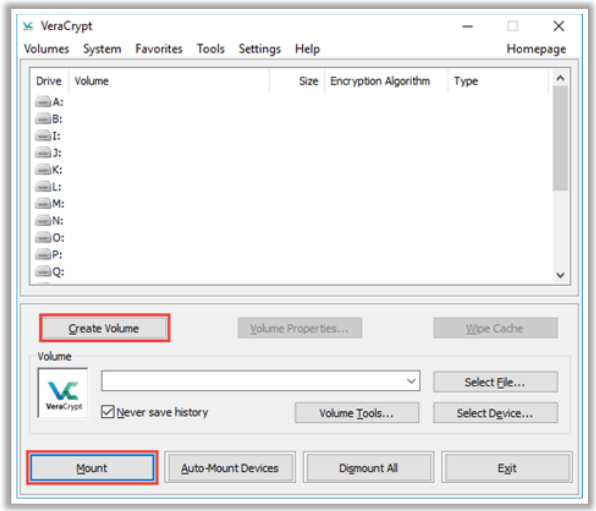
- ✓ Sign in with an Administrator Account. Select the **Start** button, Choose **Control Panel**, and then click **System and Security**
- ✓ Under **BitLocker Drive Encryption**, choose **Manage BitLocker**
- ✓ Select **Turn on BitLocker**



Disk Encryption Tools

VeraCrypt

- VeraCrypt is a software for establishing and maintaining an **on-the-fly-encrypted volume** (data storage device)
- On-the-fly encryption means that **data is automatically encrypted** immediately before it is saved and decrypted immediately after it is loaded, without any user intervention



https://www.veracrypt.fr

BitLocker Drive Encryption
https://docs.microsoft.com

FinalCrypt
https://www.finalcrypt.org

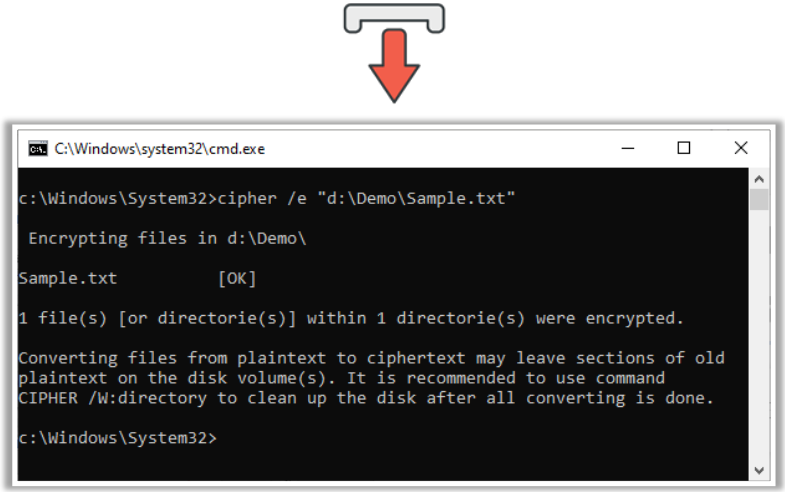
Seqrite Encryption Manager
https://www.seqrite.com

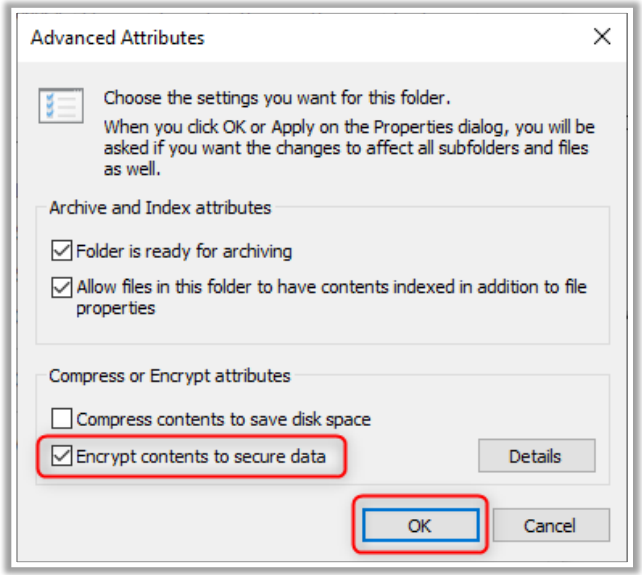
FileVault
https://support.apple.com

Gilisoft Full Disk Encryption
http://www.gilisoft.com

File Level Encryption: Implementing Built-in File System-level Encryption on Windows

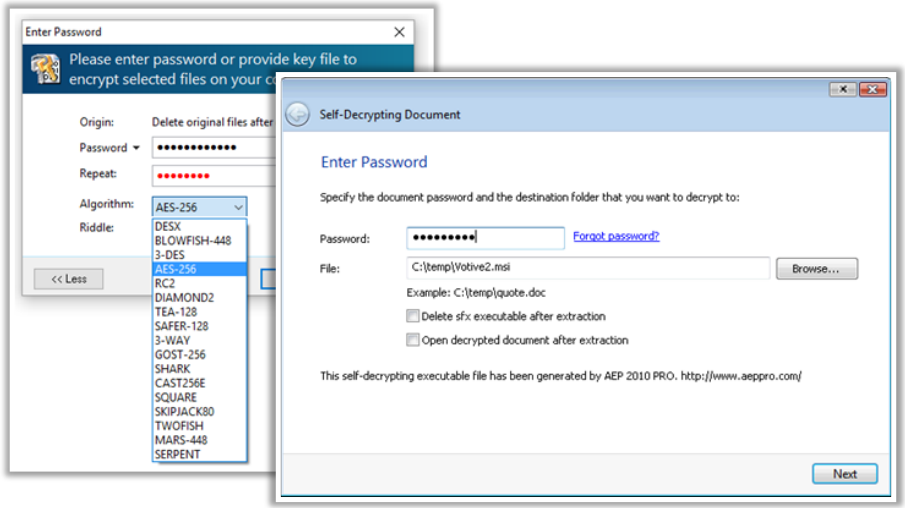
The Encrypting File System (EFS) provides **file system-level encryption** in Windows





File Encryption Tools

Advanced Encryption Package is a file encryption software for Windows 10, 8, and 7. It uses strong and proven algorithms to **protect sensitive documents**



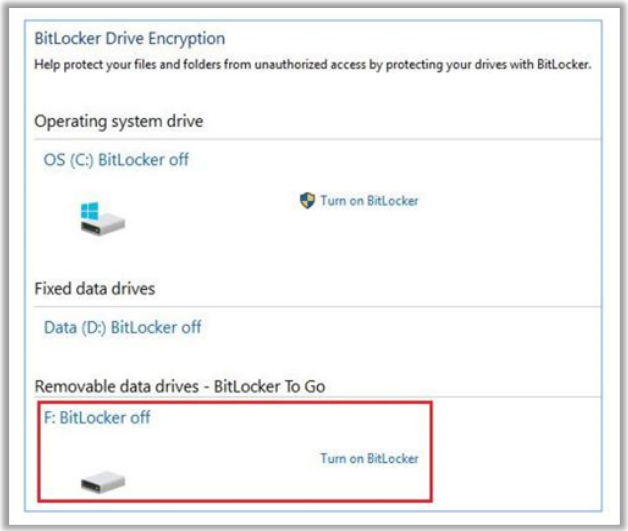
http://www.aeppro.com

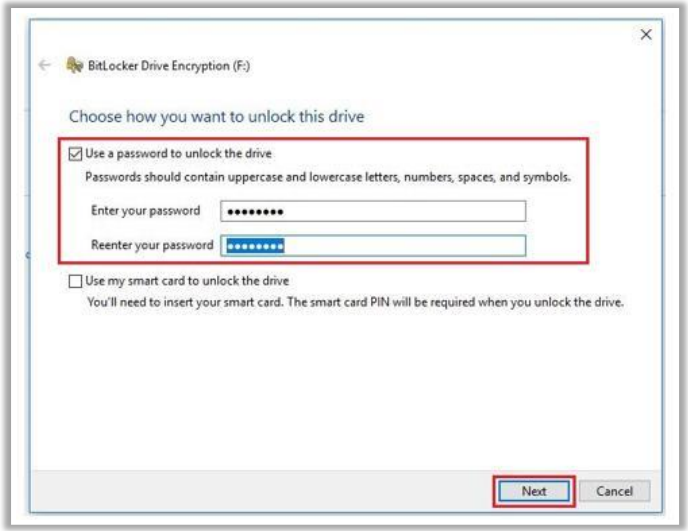
- **AxCrypt** — *https://www.axcrypt.net*
- **idoo File Encryption** — *https://www.idooencryption.com*
- **Cryptomator** — *https://cryptomator.org*
- **Encrypto** — *https://macpaw.com*
- **AES Crypt** — *https://www.aescrypt.com*

Removable Media Encryption: Implementing Removable Media Encryption in Windows

Plug the removable media device into a USB port on your computer

Go to **Start** → **Control Panel** → **System and Security** → **BitLocker Drive Encryption** (Manage BitLocker)

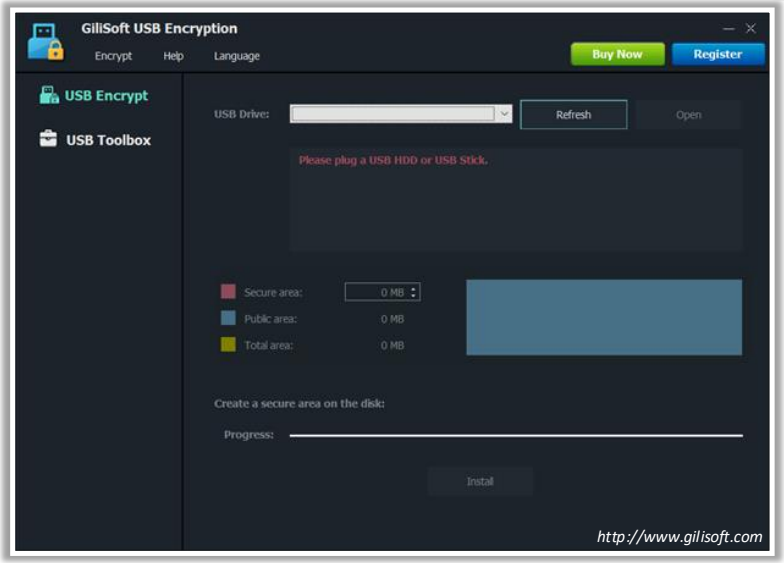




Removable Media Encryption Tools

GiliSoft USB Encryption

- A solution for USB security that supports **encrypting portable storage device** (external drive) and can divide external drive into two parts after encryption: the secure area and public area



idoo USB Encryption
https://www.idooencryption.com

Kakasoft USB Security
https://www.kakasoft.com

Rohos Mini Drive
https://www.rohos.com

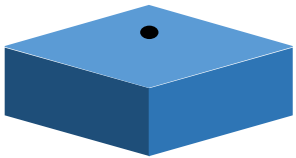
McAfee File & Removable Media Protection
https://www.mcafee.com

MFG's Removable Media Encryption
https://www.managedencryption.co.uk

Module Flow

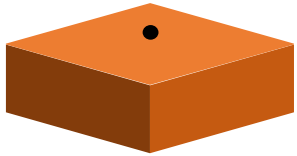
01

Understand Data Security and its Importance



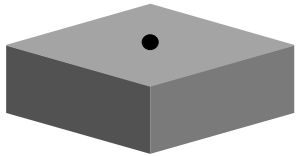
02

Discuss Various Security Controls for Data Encryption



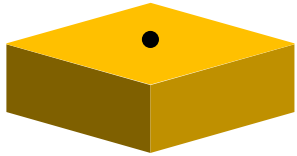
03

Discuss Data Backup and Retention



04

Discuss Data Loss Prevention Concepts



Introduction to Data Backup

Data backup is the process of making a **duplicate copy** of critical data, such as physical (paper) and computer records

It is mainly used for **two purposes**: to reinstate a system to its normal working state after damage, or to recover data and information following data loss or corruption

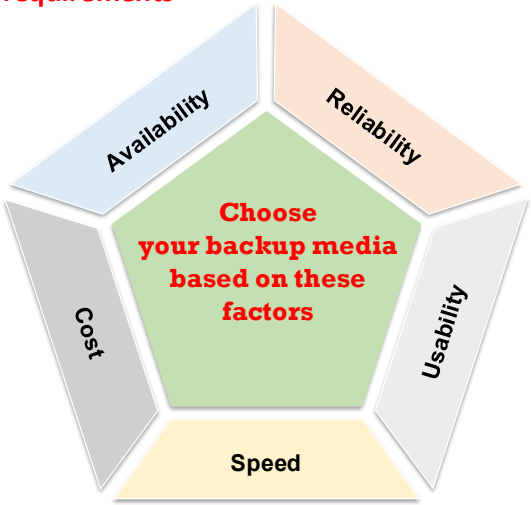
A successful data backup strategy is necessary to **avoid severe damage** to an organization's assets

Data Backup Strategy/Plan

1. Identifying the critical **business data**
2. Selecting the **backup media**
3. Selecting a **backup technology**
4. Selecting the appropriate **RAID levels**
5. Selecting an **appropriate backup** method
6. Selecting the **backup types**
7. Choosing the **right backup** solution
8. Conducting a recovery **drill test**

Selecting the Backup Media

Data backups consume a large amount of storage space. Therefore, select the best backup method to meet the **organization's requirements**



Examples of Data Backup Media Devices

Media	Capacity	Advantages	Disadvantages	Illustrations
Optical disks (CD, DVD, Blu-ray)	~200 GB	▪ Affordable, easy to store and transport	▪ Several manual disk swaps may be required because of the limited data capacity ▪ Recording and verifying a backup is slow	
Portable hard drives/USB flash drives	No limit	▪ Relatively higher storage capacity than optical disks ▪ Ideal for the home or small offices ▪ Faster recording of backups	▪ More expensive than DVD backups ▪ Less recommended for small backups	
Tape drives	No limit	▪ Media for enterprise-level backups ▪ Easy to store and transport	▪ Expensive	

Redundant Array Of Independent Disks (RAID) Technology

01 A method of combining multiple hard drives into a single unit and writing data across several disk drives, offering fault **tolerance** (if one drive fails, the system can continue operating)

02 Placing data on **RAID disks** enables a balanced overlap of input/output (I/O) operations, improving system performance, simplifying storage management, and protecting against data loss

03 RAID represents a portion of computer storage that can divide and replicate data among several drives by working as **secondary storage**

04 RAID has six levels: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10, and RAID 50, to function effectively. All RAID levels depend on the following storage techniques:

Striping **Parity** **Mirroring**

Advantages/Disadvantages of RAID Systems

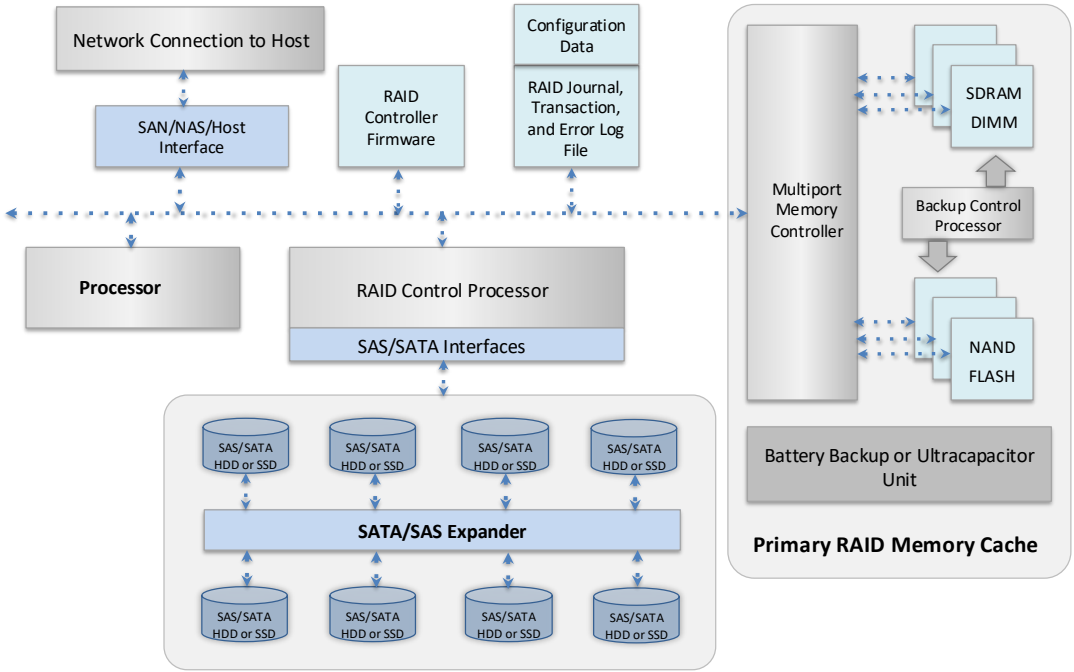
Advantages

- RAID offers hot-swapping or hot plugging, that is, system component replacement (in case a drive fails) without affecting **network functionality**
- RAID supports **disk striping,** resulting in an improved read/write performance as the system completely utilizes the processor speed
- Increased RAID **parity check** prevents a system crash or data loss

Disadvantages

- RAID is not compatible with some **hardware** components and **software** systems, for example, system imaging programs
- RAID data is **lost** if important drives fail one after another, for example, RAID 5, where a drive used exclusively for parity cannot recreate the first drive if a second drive fails too
- RAID cannot protect the data and offer a performance boost for all applications

RAID Storage Architecture



RAID Storage Architecture (Cont'd)

1

RAID Controller

Manages an array of **physical disk drives** and presents them to the computer as logical units

2

IDE, SATA, or SCSI Interface

Internal drives are connected using these **interfaces**; Connection to the server is also through one of these interfaces

3

Multiport Memory Controller

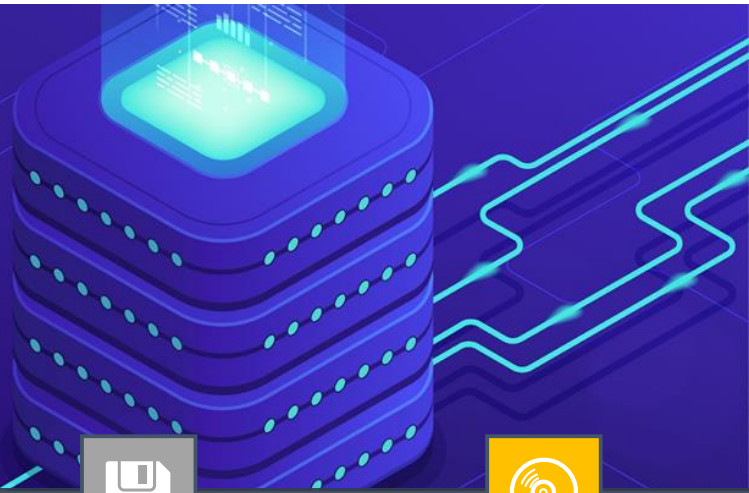
Provides access to a memory bank, and helps achieve a **high efficiency** with random address accesses

4

SDRAM

Dynamic random access memory (DRAM) that is **synchronized** with the CPU clock speed

RAID Storage Architecture (Cont'd)



Primary RAID Memory Cache

- ✓ Cache is used to write the data in **transition**. A RAID system uses a cache to speed up I/O performance on the storage system

nvSRAM

- ✓ nvSRAM is the fastest **nonvolatile RAM** in the industry with 20 ns read and write access time

NAND Flash Memory

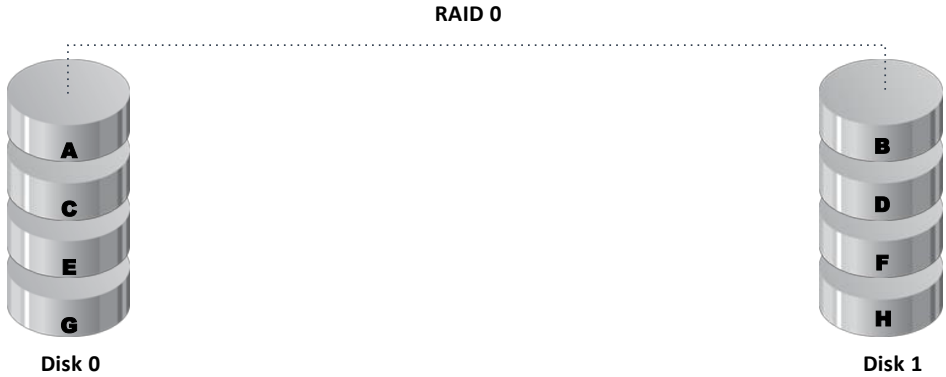
- ✓ Provides a **nonvolatile storage** for the RAID system's primary cache

Disk

- ✓ The hardware presents the RAID to the host system as a single and **large disk**

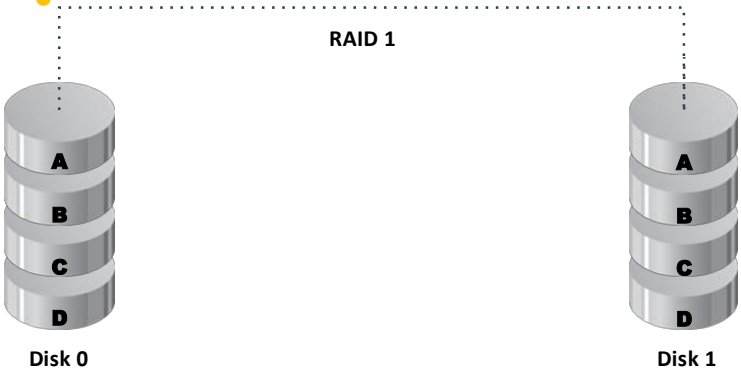
RAID Level 0: Disk Striping

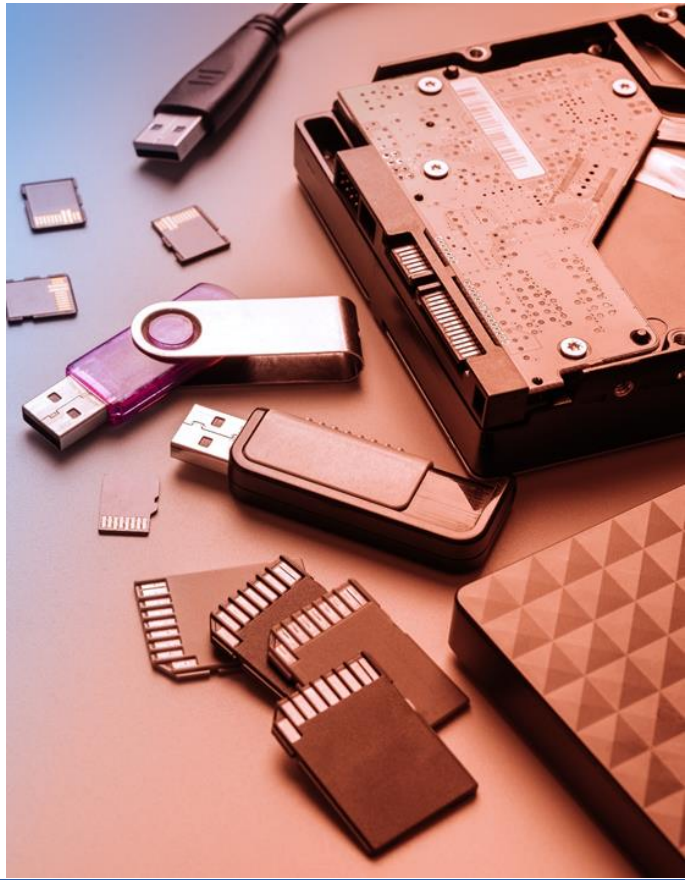
- RAID Level 0 splits data into blocks that are written evenly across **multiple hard drives**
- It improves I/O performance by spreading the **I/O load** across several channels and disk drives
- Data recovery **is not possible** if a drive fails
- It requires a minimum of **two drives**
- It does not provide **data redundancy**



RAID Level 1: Disk Mirroring

- Multiple copies of data are written to **multiple drives** at the same time
- It provides data redundancy by **duplicating the drive data** in multiple drives
- If one drive fails, **data recovery** is possible
- It requires a minimum of **two drives**



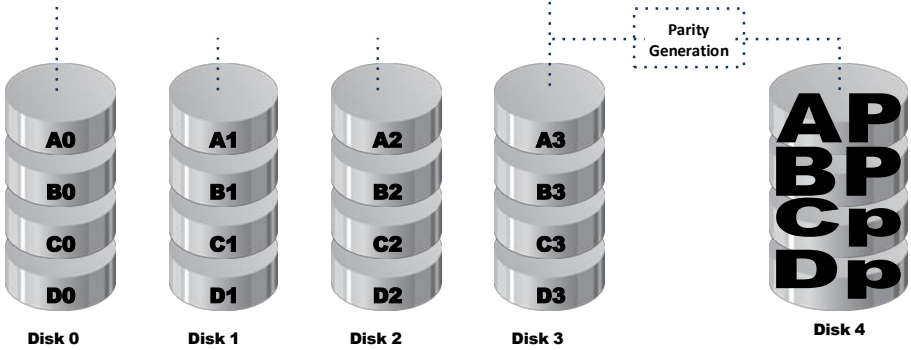


RAID Level 3: Disk Striping with Parity

01 Data is striped at the **byte level** across multiple drives. One drive per set is taken up for parity information

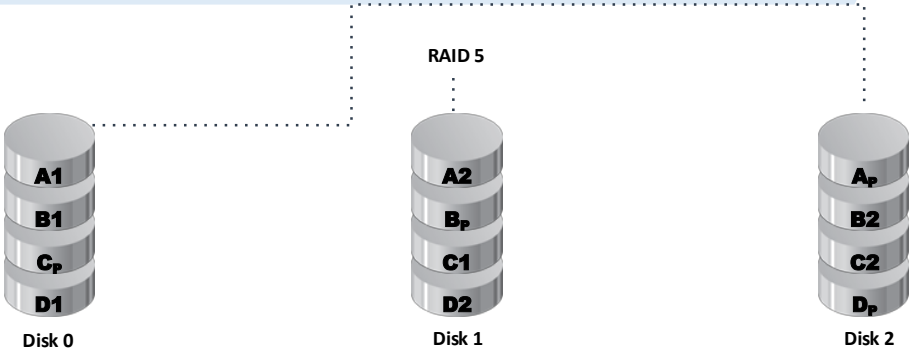
02 If a drive fails, **data recovery and error correction** is possible using the parity drive in the set

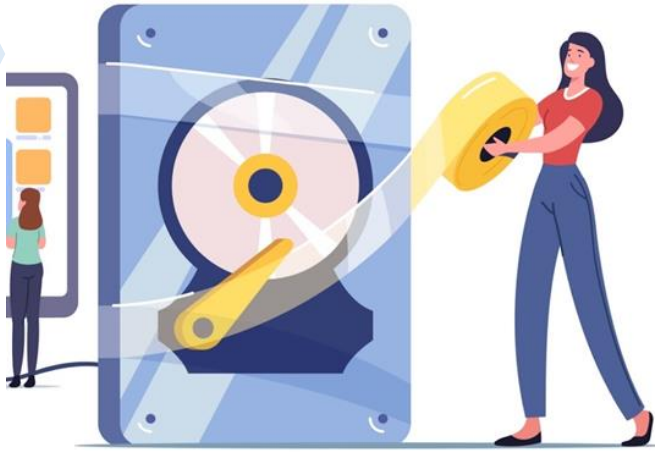
03 The **parity drive** stores the information on multiple drives



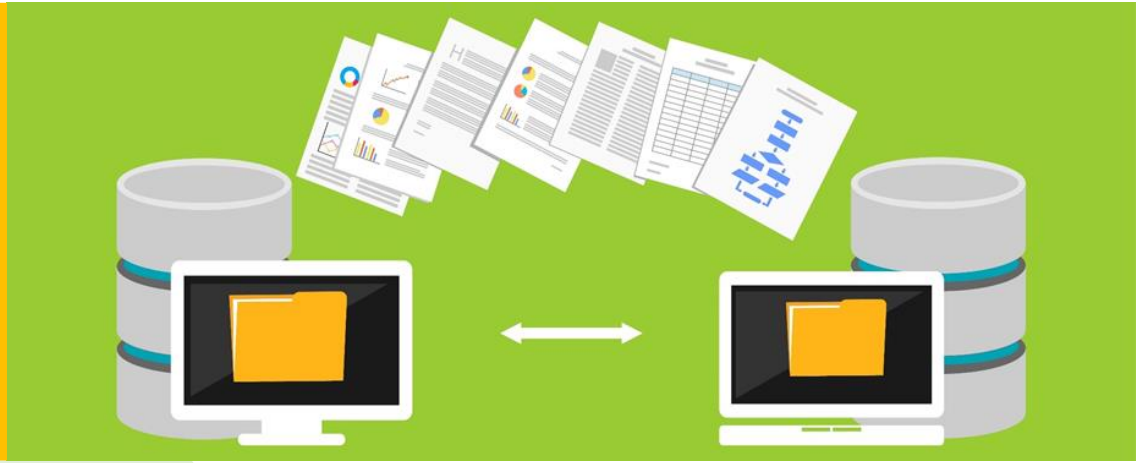
RAID Level 5: Block Interleaved Distributed Parity

1. The data is striped at the byte level across multiple drives, and the parity information is distributed among all the member drives
2. The **data writing** process is slow
3. This level requires a minimum of **three drives** to be set up





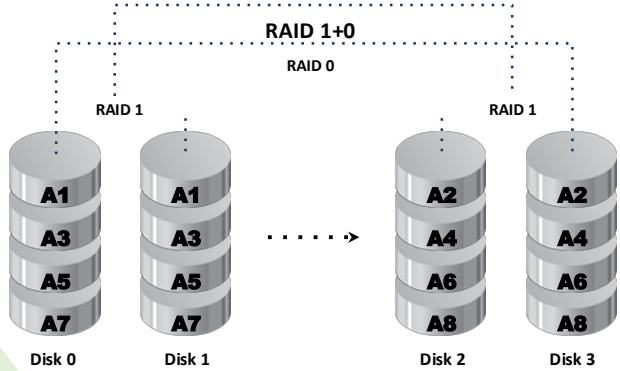
RAID Level 10: Blocks Striped and Mirrored



01 RAID 10 is a combination of RAID 0 (striping volume data) and RAID 1 (disk mirroring), and its implementation requires at least **four drives**

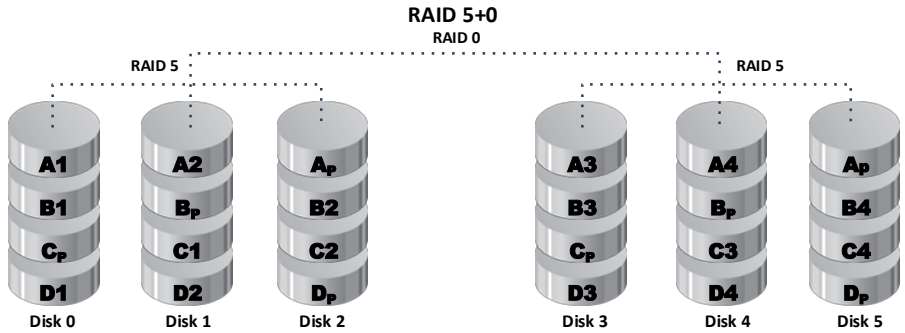
02 It has the same **fault tolerance as RAID level 1**, and the same mirroring overhead as Raid 0

03 It stripes the data across **mirrored pairs**. The mirroring provides redundancy and improves performance. The data striping provides **maximum performance**



RAID Level 50: Mirroring and Striping across Multiple RAID Levels

- RAID 50 is a combination of **RAID 0 striping** and the distributed parity of **RAID 5**
- It is **more fault tolerant** than a RAID 5 but uses twice the parity overhead
- A minimum of **six drives** are required for setup. A drive from each segment can fail and the array will recover. If more than one drive fails in a segment, the array will stop functioning.
- This RAID level offers better reads and writes than a RAID 5 and the highest levels of **redundancy** and **performance**



Storage Area Network (SAN)

A SAN is a specialized, dedicated, and discrete **high-speed network** that connects storage devices (disks, disk arrays, tapes, servers, etc.) with a high speed I/O interconnect (Fiber Channel, SAS, Ethernet, etc.)

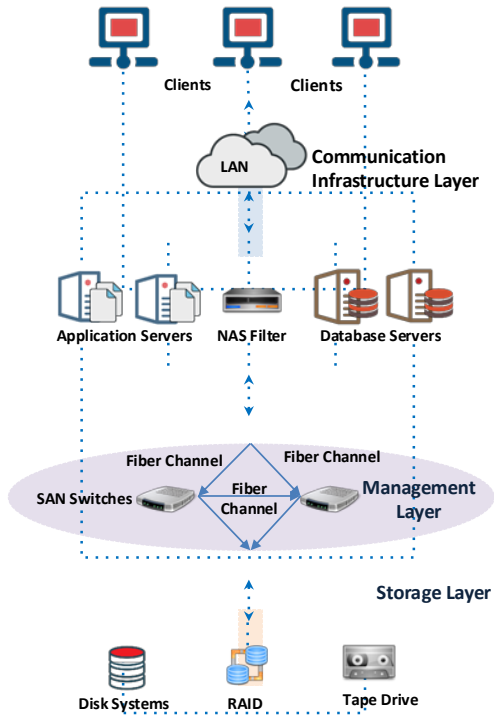
SANs are preferred in large enterprises because of **reliable data transfer** and flexible scalability

A SAN supports **data archival**, backup, restore, transfer, retrieval, migration, and mirroring from one storage device to another

The communication infrastructure layer provides the **physical connections** to the network devices

The management layer **organizes the connections**, storage elements, and computer systems

The storage layer **hosts the storage devices**



Advantages of SAN

- Storage **consolidation**
- Ease of **data sharing**
- **Improved** backup and recovery
- **Reliable and secure** centralized data storage
- **High performance** and low latency

- **LAN-free** and server-free data movement
- LAN-free and **server-free backup**
- Highly available **server clustering**
- **Data integrity** and a decreased load on the LAN
- Disaster **tolerance**

Network Attached Storage (NAS)

- NAS is a **file-based** data storage service and a dedicated computer appliance shared over the network
- NAS is a **high-performance** file server optimized for storing, retrieving, and serving files
- NAS servers contain proprietary or **open-source** operating systems optimized for file serving

Advantages

- Users with different operating systems can **share files** with no compatibility issues
- A NAS can be connected to a LAN using the **plug and play** feature
- Minimal administration required, unlike Unix or NT file servers

Disadvantages

- Applications that use most of the data transfer bandwidth will significantly reduce network performance
- Data transfer is **inefficient** as it uses TCP/IP instead of a specialized data transfer protocol

Selecting an Appropriate Backup Method

❑ Select a backup method based on its **cost** and **ability** according the organization's requirements

Hot Backup (Online)

- ❑ Backup the data when the application, database, or system is **running** and available to users
- ❑ Used when a service level **down time** is not allowed

Advantage:

- ✓ Immediate data backup **switch over** is possible

Disadvantage:

- ✓ Very **expensive**

Cold Backup (Offline)

- ❑ Backup the data when the application, database, or system is **not running** (shutdown) and is not available to users
- ❑ Used when a service level down time is allowed and a **full backup** is required

Advantage:

- ✓ **Least expensive**

Disadvantage:

- ✓ Switching over the data backup requires additional time

Warm Backup (Nearline)

- ❑ A **combination** of both hot and cold backups

Advantages:

- ✓ **Less expensive** than a hot backup
- ✓ Switching over the data backup takes less time than a cold backup but more time than a hot backup

Disadvantage:

- ✓ It is **less accessible** than hot backup

Choosing the Backup Location

Onsite Data Backup

- Storing backup data at **onsite data storage** only

Advantage:

- ✓ Onsite backup data can be easily accessed and **restored**
- ✓ **Less expensive**

Disadvantage:

- ✓ Data loss risk is greater

Offsite Data Backup

- Storing backup data in **remote locations** in fire-proof, indestructible safes

Advantage:

- ✓ Data is secured from **physical security** threats such as fire, floods, etc.

Disadvantage:

- ✓ Problems with a regular **data backup schedule**

Cloud Data Backup

- Storing backup data on storage provided by an **online backup** provider

Advantages:

- ✓ The data is **encrypted** and free from physical security threats
- ✓ Data can be **accessed** from anywhere

Disadvantages:

- ✓ **No direct control** of the backup data
- ✓ **More time** to backup

Types of Backup

Full/Normal Data Backup

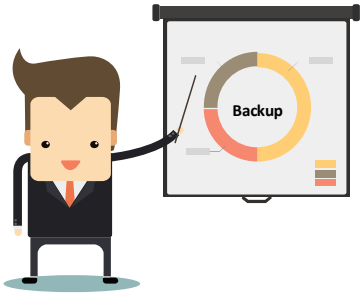
- All system data is **copied** to the backup media

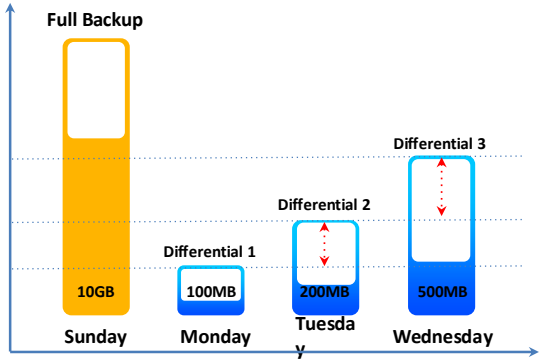
Differential Data Backup

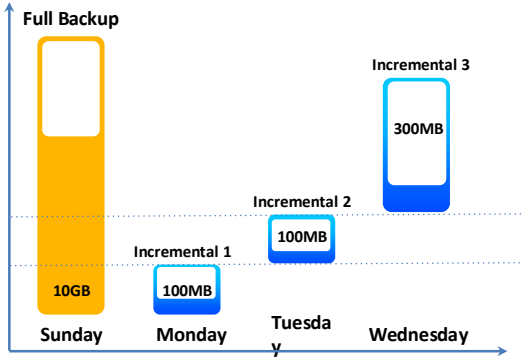
- All data that has been **changed** since the last full backup is copied to the backup media

Incremental Data Backup

- Only files that have been **changed or created** after the last backup are copied to the backup media







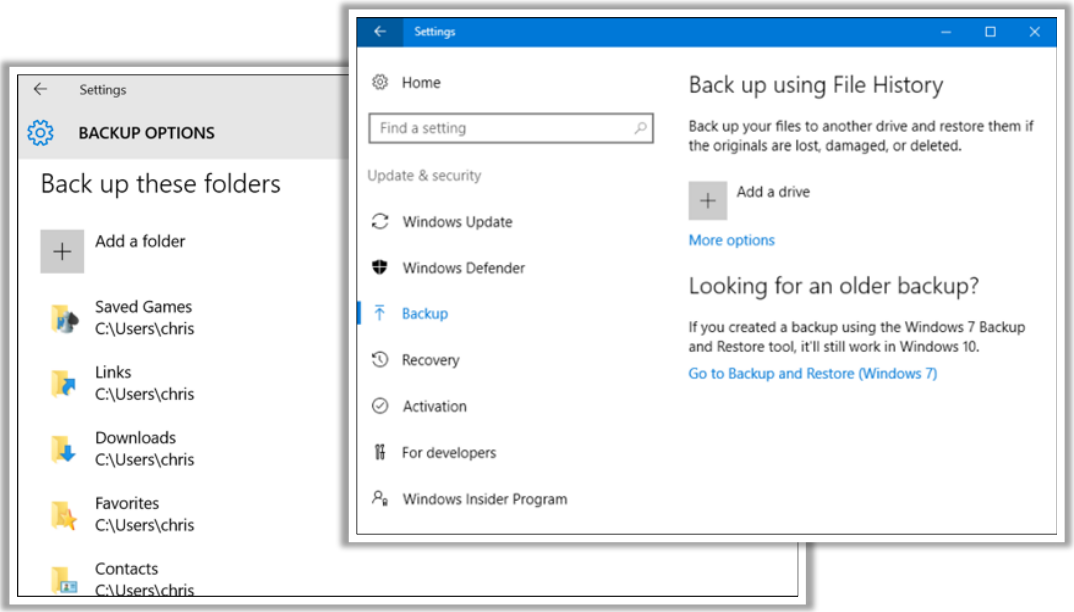
Backup Types: Advantages and Disadvantages

Type	Advantages	Disadvantages
Full Backup	✓ Restoration is fast	✓ Backup process is slow ✓ High storage requirements
Differential Backup	✓ Faster than a full backup ✓ Restoration faster than an incremental backup ✓ Reduced amount of storage than a full backup	✓ Restoring data is slower than a full backup ✓ Slower than an incremental backup
Incremental Backup	✓ Fastest method ✓ Least amount of storage space among other backup types	✓ Slowest restore speed among other backup types

Data Backup Tools

File History Tool

- File History is a **built-In backup tool** in Windows
- It regularly backs up important folders like Desktop, Documents, Downloads, Music, Picture, Videos, and parts of AppData folder



- **Genie Backup Manager Pro**
  https://www.zoolz.com
- **BullGuard Backup**
  https://www.bullguard.com
- **NTI Backup Now EZ**
  https://www.nticorp.com
- **Power2Go 13**
  https://www.cyberlink.com
- **Backup4all**
  https://www.backup4all.com

Data Backup Retention

Data Retention

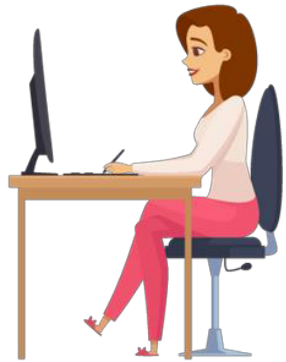
- Data Retention is the process of storing and **maintaining important information** for meeting compliance and business data archival requirements

Data Retention Policy

- Data retention policy is a **set of rules** for preserving and maintaining data for operational or regulatory compliance requirements
- The policy defines the required **retention periods** for different data types, and sets the minimum standards for destroying certain information

Steps for Developing a Data Retention Policy

1. Build a data retention policy development team
2. Understand and determine the applicable legal requirements of the organization
3. Identify and classify the data to be included in data retention policy
4. Develop the data retention policy
5. Ensure that all employees understand the organization's data retention policy



Data Retention Policy Best Practices

01 Create a data retention policy that fulfils **legal** and **business** requirements

02 Justify the **reasons** behind the policy details

03 Start creating a policy with **minimal requirements** and add new requirements as and when required

04 Create a simple policy which is easy for the employees to implement

05 Create different **data retention policies** for different data types, as per their legal and business impacts

06 Retain **customer**, **subscriber**, and **user** information only till they are necessary

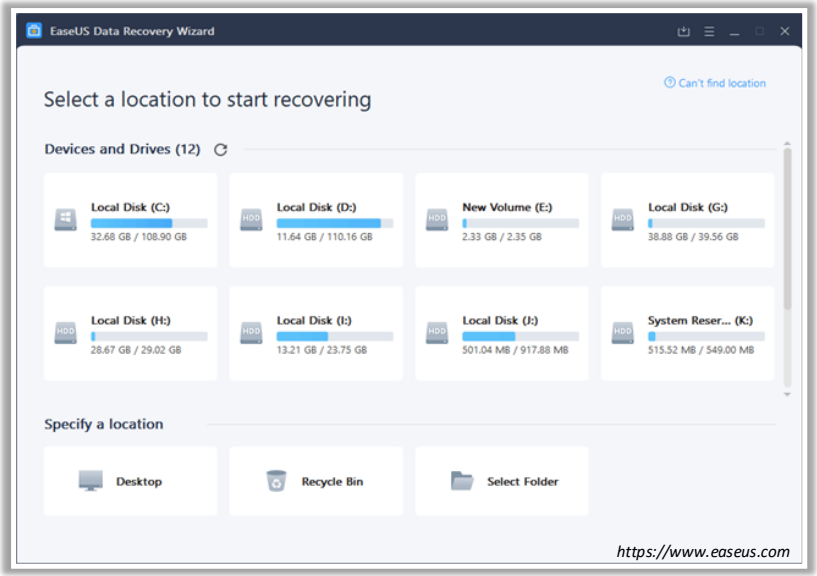
07 Implement **software** to manage the data retention tasks

08 Classify **data** and decide if it should be archived or deleted

Data Recovery Tools

EaseUS Data Recovery Wizard

EaseUS data recovery software can quickly **retrieve lost files** after deletion or emptying the recycle bin

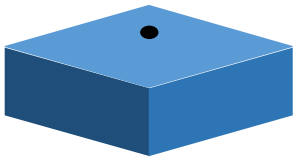


- **Recuva®**
  https://www.ccleaner.com
- **Puran File Recovery**
  http://www.puransoftware.com
- **Glary Undelete**
  https://www.glarysoft.com
- **SoftPerfect File Recovery**
  https://www.softperfect.com
- **Wise Data Recovery**
  https://www.wisecleaner.com

Module Flow

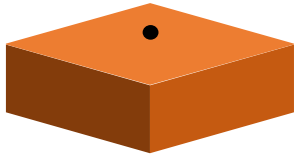
01

Understand Data Security and its Importance



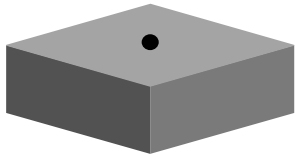
02

Discuss Various Security Controls for Data Encryption



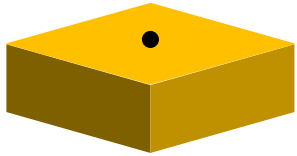
03

Discuss Data Backup and Retention



04

Discuss Data Loss Prevention Concepts



What is Data Loss Prevention?

- Data loss prevention (DLP) includes a set of software products and processes that do not allow users to **send confidential corporate data** outside the organization

- It is used by organizations to:
  - ✓ Discover sources of data leaks
  - ✓ Monitor the sources of data leakage
  - ✓ Protect organization assets and resources
  - ✓ Prevent accidental disclosure of sensitive information to unintended parties
  - ✓ Manage resources with business rules, security policies, and software

Types of Data Loss Prevention (DLP) Solutions

Endpoint DLP

- A solution that **monitors** and **protects PC-based systems** such as tablets, laptops, etc.
- It is used for preventing data leakage through clipboards, removable devices, and sharing applications

Network DLP

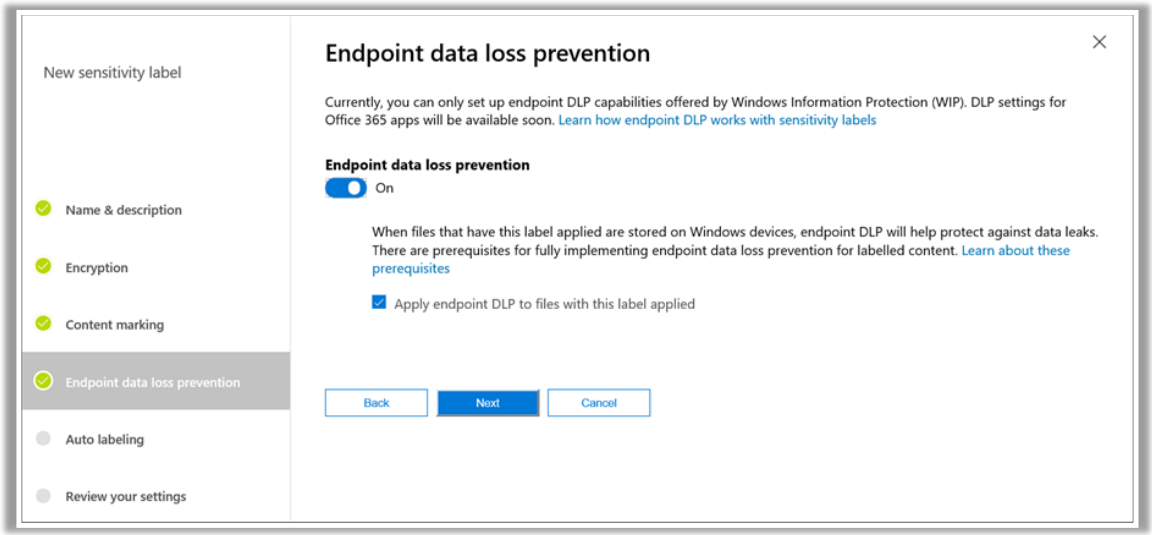
- A solution that **monitors**, **protects**, and **reports all data in transit**
- It is installed at the "perimeter" of an organization's network
- It helps the security professionals in scanning all data moving through the ports and protocols within the organization

Storage DLP

- A solution that **monitors** and **protects data at rest**, that is, the data stored in an organization's data center infrastructure such as file servers, SharePoint, and databases
- It identifies the location where sensitive information is stored and helps users in determining whether it is stored securely

DLP Solution: Windows Information Protection (WIP)

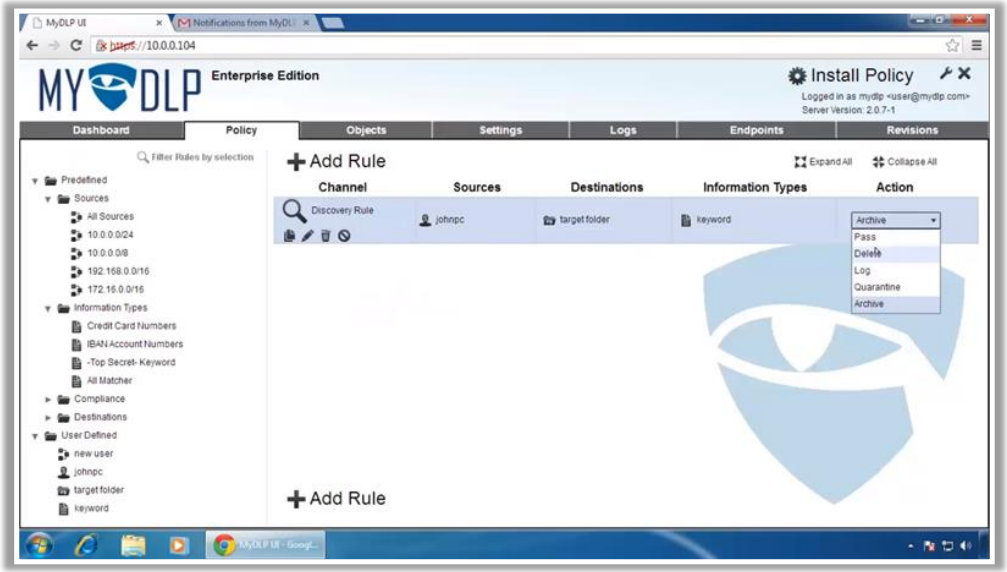
- Windows Information Protection (WIP) has an **endpoint data loss prevention** (DLP) capability that can be helpful in protecting local data at rest on endpoint devices
- WIP can be configured to store business data only on approved devices / within approved applications



DLP Solutions

MyDLP

MyDLP allows the user to monitor, inspect, and **prevent all outgoing confidential data** without any hassle



https://mydlp.com

Symantec Data Loss Prevention
https://www.symantec.com

SecureTrust Data Loss Prevention
https://www.securetrust.com

McAfee Total Protection
https://www.mcafee.com

Check Point Data Loss Prevention
https://www.checkpoint.com

Digital Guardian Endpoint DLP
https://digitalguardian.com

Best Practices for a Successful DLP Implementation

- ✓ Identify the **main objective** of DLP
- ✓ Identify **sensitive data** for protection
- ✓ Evaluate available **DLP vendors**
- ✓ Ensure that the selected DLP product is **compatible** and supports the required data types and data stores of your organization
- ✓ Identify the **roles** and **responsibilities** of individuals for implementing the DLP solution
- ✓ Implement **DLP** with a minimal base to reduce false positives, and enhance the base gradually by identifying sensitive data
- ✓ Enhance the **DLP policies** to support effective DLP operations and eliminate false positives

Module Summary

- This module has discussed data security and its importance
- It has discussed the different data security technologies
- It has also discussed various security controls for data encryption
- It has demonstrated various disk encryption, file encryption, and removable-media encryption tools
- This module has also discussed the methods and tools for data backup and retention
- Finally, this module ended with an overview of the data loss prevention (DLP) and DLP solutions
- In the next module, we will discuss on network traffic monitoring in detail