

Introduction to Cybersecurity

Chapter 7

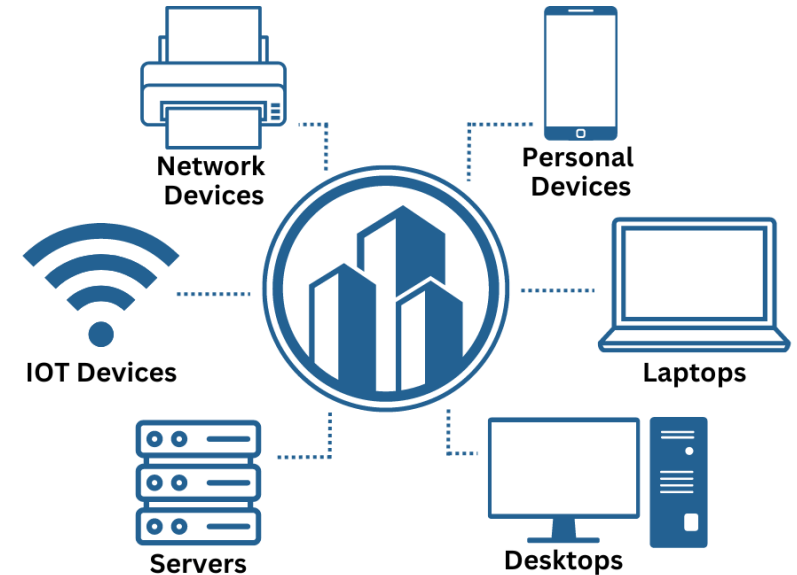
Endpoint Security

Chapter Outline

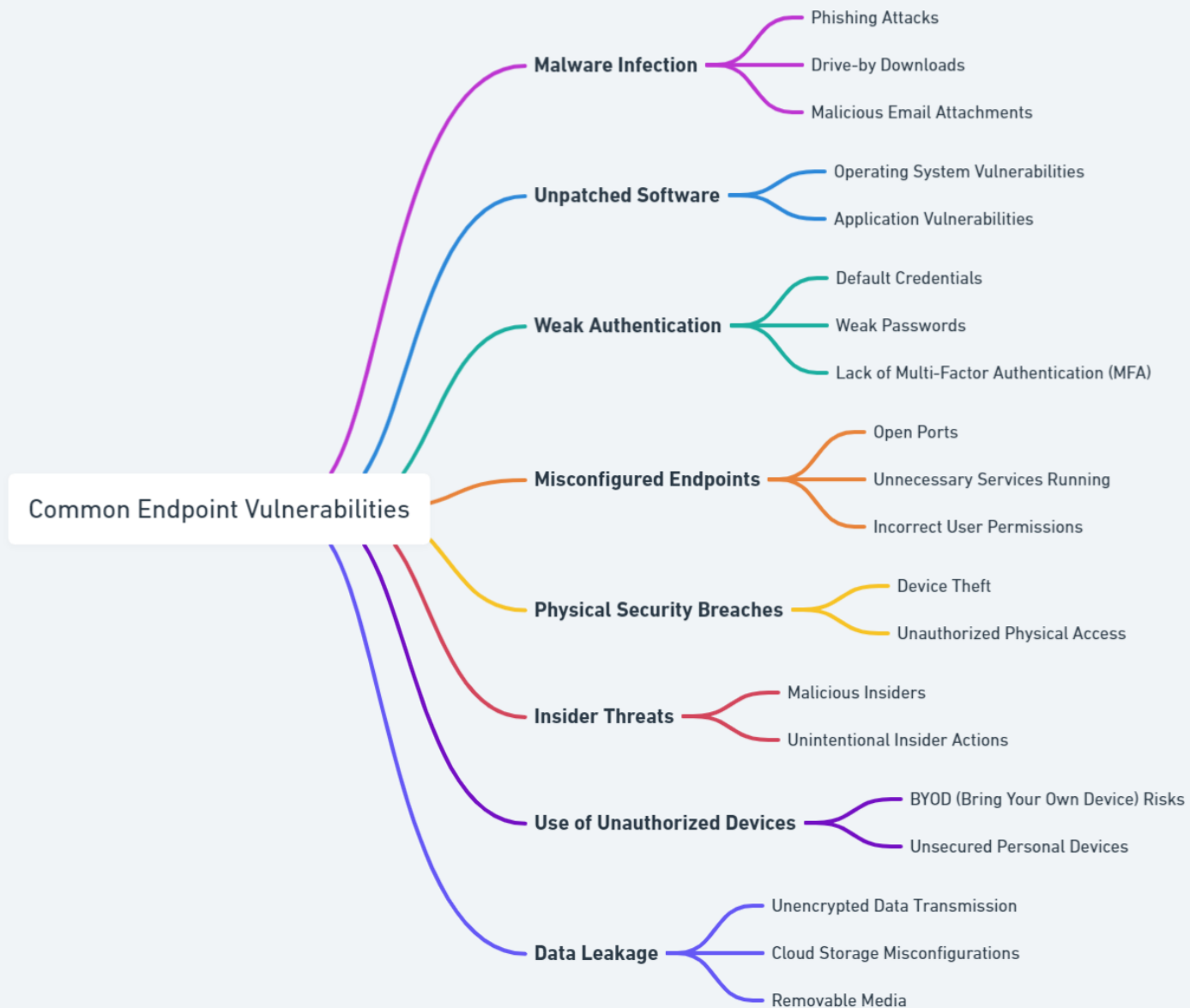
- What is endpoint security and why is it essential?
- Key tools: UEM, EDR, DLP, NGFW
- Techniques for hardening endpoints
- How to apply fault tolerance and redundancy
- Best practices for backup and power protection

Endpoint Security

- **Endpoint:** Hardware device that is an end point of a wired or wireless network connection
- 70%+ of cyberattacks begin at the endpoint
- Laptops, phones, tablets, and servers = everyday tools and attack surfaces
- End users = most frequent targets of phishing and malware
- Endpoint security is the frontline of defense for any organization



Threat to Endpoints



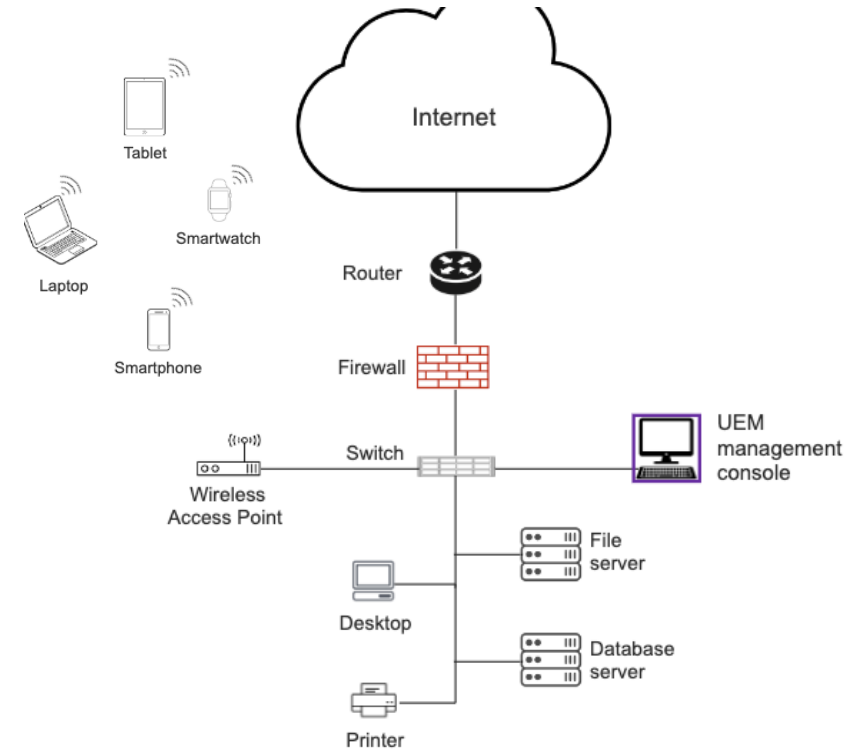
Endpoint Security

Unified endpoint management (UEM): collection of software tools for monitoring, managing, and securing endpoints from a single management console

- Enables the management of endpoints, regardless of the operating system or device type
- Has the capability to install firmware and software updates, apply security policies, patch management, and remotely remove all applications and data from lost or compromised

• Benefits

- Improves endpoint security and reduces attack surface
- Streamlines IT operations and reduces management overhead
- Supports remote/hybrid workforce securely
- Enables BYOD policies while maintaining control
- Helps ensure regulatory compliance



N-able N-central UEM tool

Dashboard: Monitoring

+ Add device | Refreshed 9:51:07 AM

Devices

17

Problem devices

8

Daily safety check problems

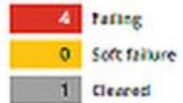
3

24x7 check problems

7

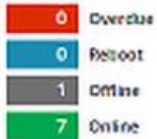
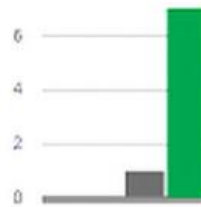
Problem servers

With one or more failing checks



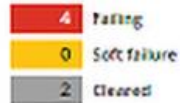
Server status

All clients and sizes



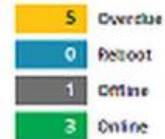
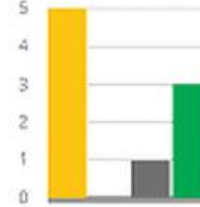
Problem workstations

With one or more failing checks



Workstation status

All clients and sizes



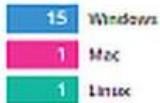
Device types

All clients and sizes



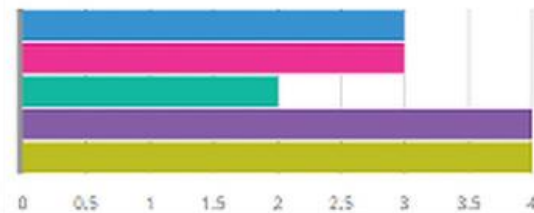
Devices by main OS

All clients and sizes



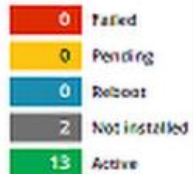
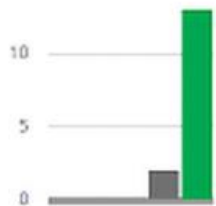
Last reboot time

All servers and workstations



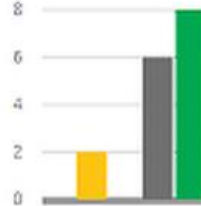
Patch Management install status

All servers and workstations



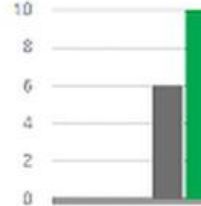
Managed Antivirus install status

All servers and workstations



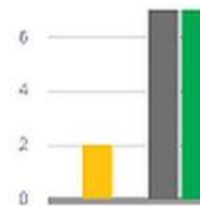
Backup install status

All servers and workstations



Web Protection install status

All servers and workstations



Ivanti Neurons UEM



Endpoint security/protection

- **Endpoint protection:** set of technologies used to protect an endpoint against various attack types
 - **Antivirus and anti-malware software** to prevent and remove malicious programs
 - **Next-Generation Firewalls (NGFW)** to detect and block a network attack
 - Host-based int **HIDS/HIPS** to secure endpoints from external threats
 - **Data Loss Prevention (DLP)** systems to protect sensitive data from unauthorized access or breaches
 - **Endpoint Detection and Response (EDR)** to monitor and analyze endpoint activities for threats



EDR

EDR is an endpoint security solution that combines endpoint monitoring and log analysis capabilities with contextual information from correlated network events to detect and respond to security incidents at an endpoint

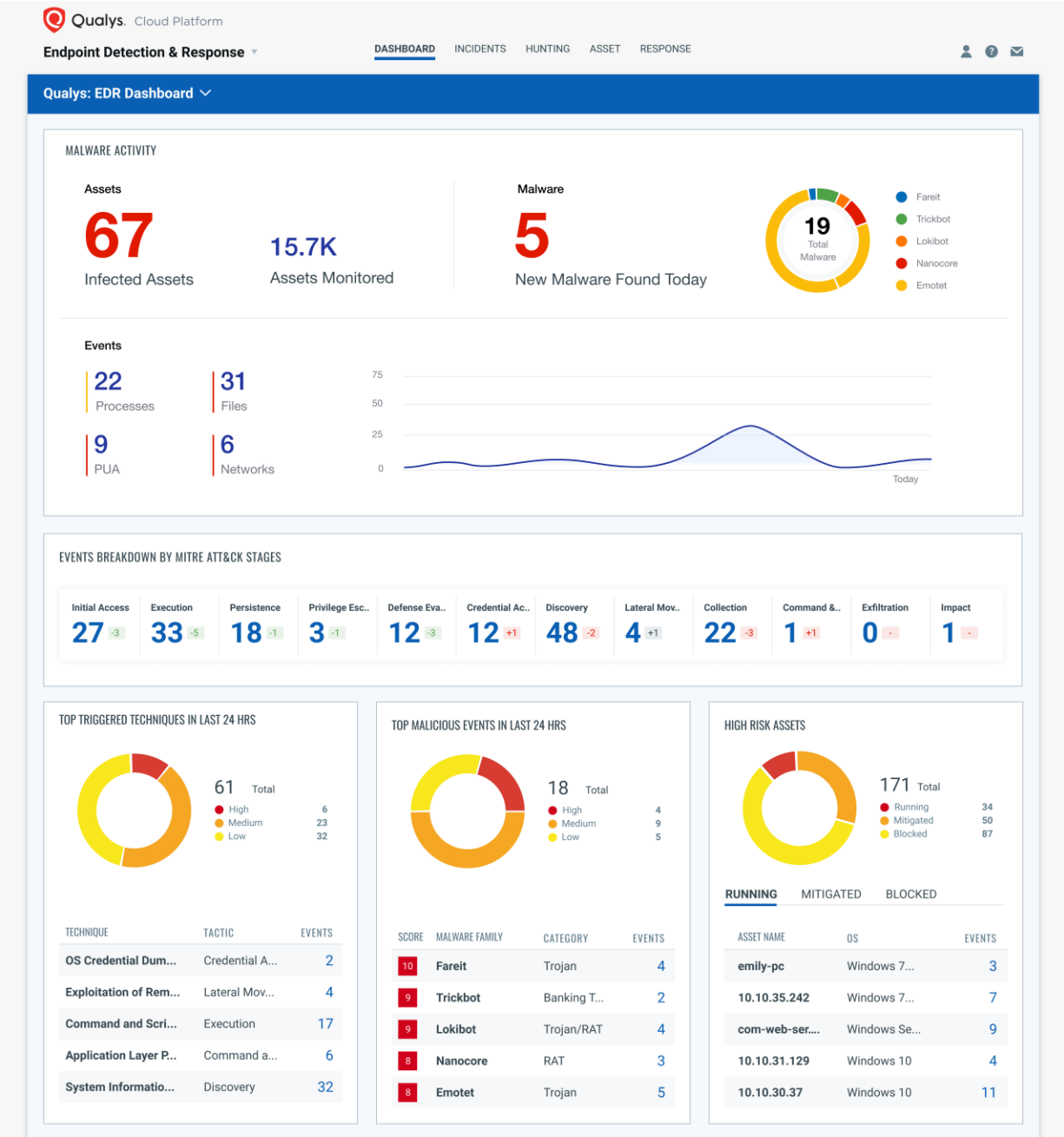
Core Capabilities of EDR:

- Real-time monitoring of endpoint behavior
- Threat detection using behavioral analysis and signatures
- Automated response (e.g., isolating an infected device)
- Threat hunting to proactively search for indicators of compromise (IoCs)
- Forensics & investigation with detailed event timelines and data logs
- Integration with SIEM/SOAR platforms for broader incident response

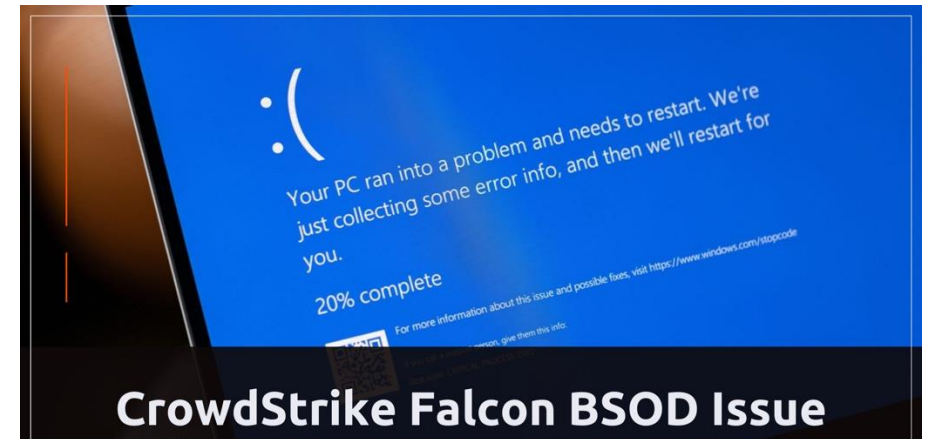
Why EDR Matters:

- Helps detect advanced threats like zero-day malware and fileless attacks
- Enables faster incident containment and remediation
- Reduces the dwell time of attackers on the network

Qualys EDR provides visibility and monitoring of malicious activity on endpoints



- CrowdStrike Falcon is a leading **EDR platform** known for advanced threat detection and response
- Approximately 8.5 million Windows devices were affected
- 3500 flights cancelled in USA
- Fortune 500 companies incurring an estimated \$5.4 billion in losses
- A recent **CrowdStrike Falcon sensor** update caused Windows systems to crash with a Blue Screen of Death (BSOD)

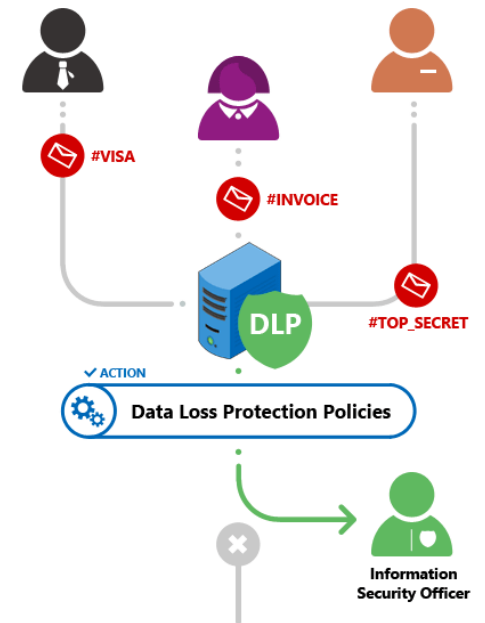


Data Loss Prevention (DLP)

DLP is a data security technology that detects potential data breach incidents in a timely manner and prevents them by monitoring data in use (endpoints), in-motion (network traffic), and at-rest (data storage)

Main goal:

- Monitor endpoint to detect policy violations, and take protective actions
 - Prevents an employee from sending an email containing a customer's SSN
- Ensure an organization is in compliance with laws and regulations that govern the use of personal, financial, and medical information of the organization's customers
 - HIPAA, PCI-DSS, GPDR



Symantec Data Loss Prevention (DLP) policies describing the types of data that are monitored and protected to ensure compliance with various laws and regulations.

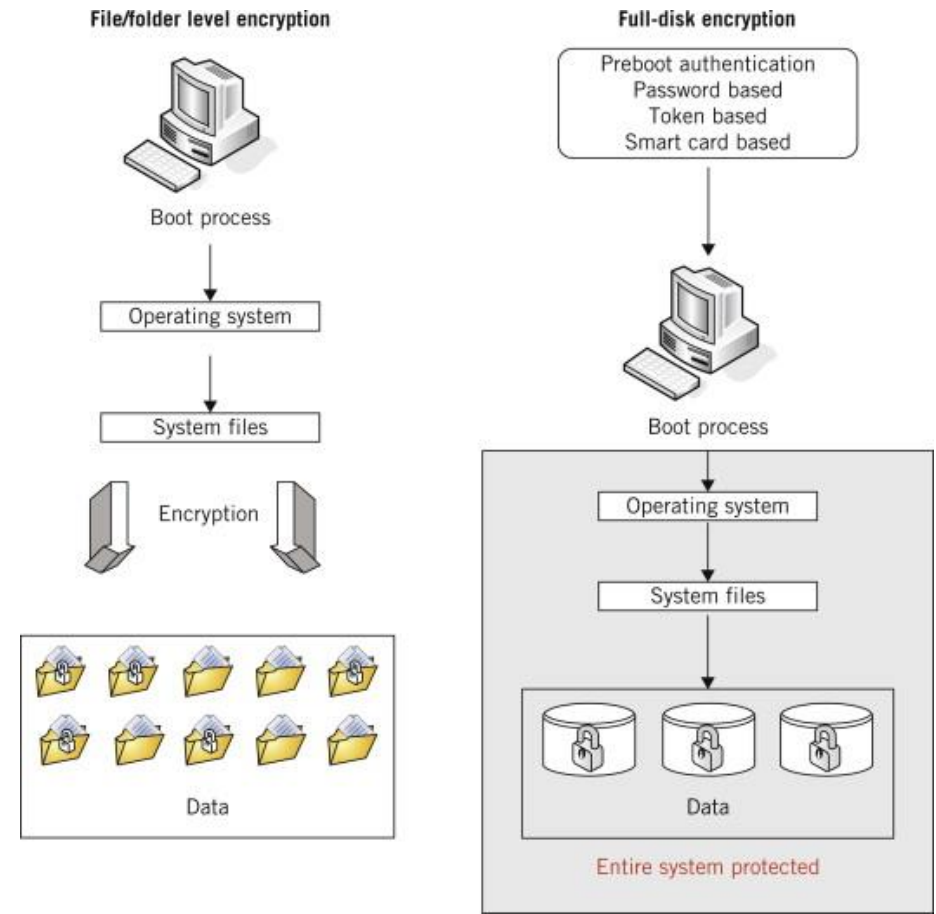
Symantec Data Loss Prevention				
Home Incidents Manage System				
Manage > Policies > Policy List				
<div> <div> New Import Export Download </div> <div> Policies Data Profiles Discover Scanning </div> <div> Suspend Delete Clone Assign Group </div> </div>				
Showing 1 to 22 of 22 entries				
<input type="checkbox"/>	Status	Name	Description	Policy Group
<input type="checkbox"/>		Americas PII (DCM)	This policy detects Personally Identifiable Information from within the Americas Region.	Personally Identifiable Info
<input type="checkbox"/>		APJ PII (DCM)	This policy detects Personally Identifiable Information from within the Asia Pacific & Japan Regions.	Personally Identifiable Info
<input type="checkbox"/>		Classification compliance	Classification compliance	Classification
<input type="checkbox"/>		Credit Card Data	This policy detects any credit card info leaving the organization	Confidential Data Protection
<input type="checkbox"/>		DCS - Legal Hold	DCS - Legal Hold	Classification
<input type="checkbox"/>		DCS Policy - Do not Archive	DCS Policy - Do not Archive	Classification
<input type="checkbox"/>		Design Documents (DCM)	This policy detects various types of design documents such as CAD/CAM at risk of exposure.	Intellectual Property Policies
<input type="checkbox"/>		Digital Rights Management	Digital Rights Management	Classification
<input type="checkbox"/>		Email Quarantine	Policy for use with Email Quarantine use case	Default Policy Group
<input type="checkbox"/>		EMEA PII (DCM)	This policy detects Personally Identifiable Information from within the Europe, Middle East and Africa Regions.	Personally Identifiable Info
<input type="checkbox"/>		HIPAA and HITECH (including PHI)	This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy may also be used for organizations which are not subject to HIPAA but want to control PHI data. Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for PHI.	Regulatory Compliance
<input type="checkbox"/>		Information Centric Tagging (DCM)	Information Centric Tagging (DCM)	Classification
<input type="checkbox"/>		Intellectual Property (IDM)	Intellectual Property (IDM)	Intellectual Property Policies
<input type="checkbox"/>		International Data Identifiers (DCM)	International Data Identifiers (DCM)	Personally Identifiable Info
<input type="checkbox"/>		Medicaid Cases (VML)		Confidential Data Protection

DCS: Data Center Security
DCM: Described Content Matching
Computer-aided design (CAD)
Computer-aided manufacturing (CAM)
IDM: Identity management

Credit: Broadcom Inc

Endpoint Hardening

- Hardening an endpoint includes measures to protect data stored at an endpoint
 - Disk encryption can be used to provide data confidentiality and data protection from unauthorized access
 - File Vault for Mac or BitLocker for Windows
- Full disk encryption (FDE): secure drive data using encryption
- Self-encrypting drive (SED) is an HDD or SSD with encryption circuitry built into the drive



Endpoint hardening like this is a fundamental step in safeguarding against data breaches and unauthorized access.

Redundancy and Fault Tolerance

- **Fault tolerance:** ability of a system to continue operating despite failures or malfunctions in one or more of its components
- **Redundancy:** Inclusion of extra components, such as duplicate or mirrored data, so that a system can continue to work even if individual components fail
- Single point of failure
 - Any component whose failure results in the failure of an entire system
 - Single points of failure are often overlooked until a disaster occurs
- Remove single points of failure with
 - RAID (disk)
 - Failover clustering (server)
 - UPS and generators (power)

Single Point of Failure

Best Practices to Avoid SPOF

- Implement redundancy (e.g., multiple load balancers, failover routers)
- Use high-availability (HA) architectures
- Set up automatic failover mechanisms
- Regularly test fault tolerance and disaster recovery plans

Application Clients (End Users)



Internet Router



Load Balancer



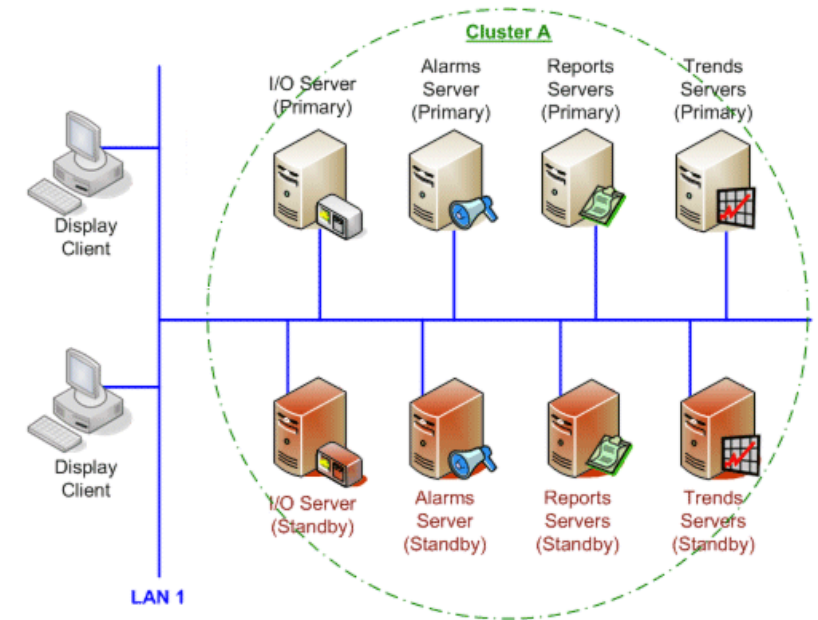
Application Servers



Single Point of Failure (SPOF)

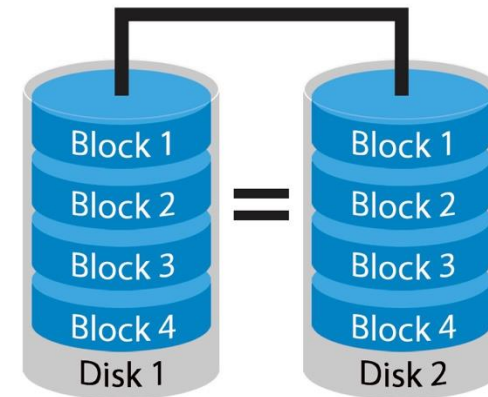
Managing Redundancy

- Redundancy establishes a straight copy of an entire system, ready to take over if original system fails
- Can be applied almost anywhere in a network, from hard disks to network cables
- It's a way of achieving fault tolerance
- Redundancy should be added to:
 - Critical servers (file server, login server)
 - Business-critical functions (e.g. database server, web server)
 - Any component that must always run
- Two general redundancy categories:
 - Disk-level
 - Server-level



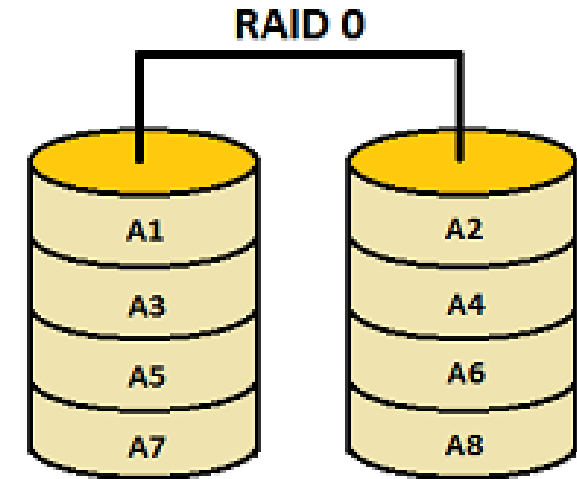
Redundancy at the Disk level

- To protect the server from catastrophic disk failure, disk drives on most network servers support one of the RAID techniques (Redundant Array of Inexpensive Disks)
 - Purpose of RAID is to achieve data redundancy to reduce data loss and, in a lot of cases, improve performance
 - Allows storing data across multiple hard drives
- **Why RAID?**
 - Protects data from disk failure
 - Disk performance improvement
 - Provides data security
- **Several levels RAID schemes:**
 - Commonly used are RAID 0, RAID 1, RAID 5
 - Rarely used: RAID 2, 3, 4, 6, 10, 50



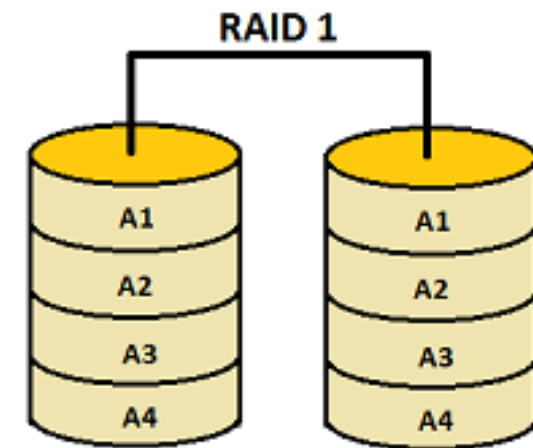
RAID 0

- RAID 0 is based on data **striping**
- Stream of data is divided into multiple segments or blocks
- Each of those blocks is stored on different disks
- Data reading simultaneously from all the disks and join them together to reconstruct the entire data stream
- Implementation requires minimum 2 disk
- No data protection (no redundancy)
- 100% capacity utilization
- Used to store temporary files
- **Advantage:** Easy implementation, fast data access (two disk controllers)
- **Disadvantage:** No redundancy/duplication of data, If one of the disks fails, the entire data is lost



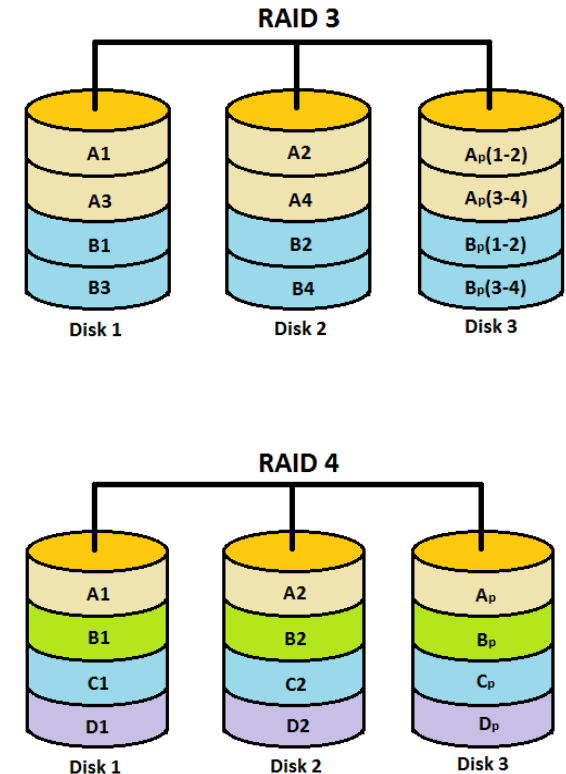
RAID 1

- Also called "**mirroring**" as it copies data onto two disk drives simultaneously
- Every disk in the array has a mirror disk that contains the same data
- Data can be read from either disk but is written on both disks
- Can handle single drive failure
- Minimum number of drive needed is 2
- 50% capacity utilization
- Used to store crucial information, bank data, family photo
- **Advantages:**
 - Data can be recovered in case of disk failure
 - Increased performance for read operation
- **Disadvantages:**
 - Slow write performance
 - Space is wasted by duplicating data which increases the cost per unit memory



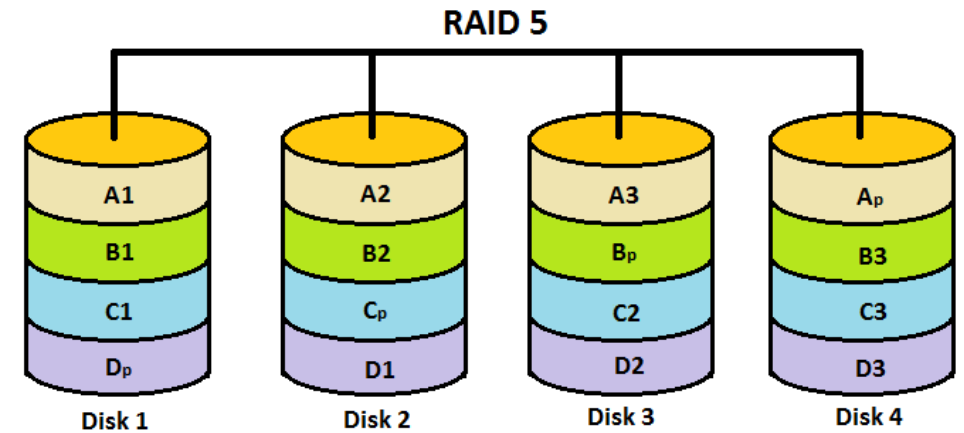
RAID 2, RAID 3, RAID 4

- These levels do exist but are not that common
- Based on data stripping
- **RAID 3:** uses byte-level stripping along with parity
 - One dedicated drive is used to store the parity information
 - In case of any drive failure the parity is restored using this extra drive
- **RAID 2:** uses bit-level data stripping
- **RAID 4:** uses block level stripping



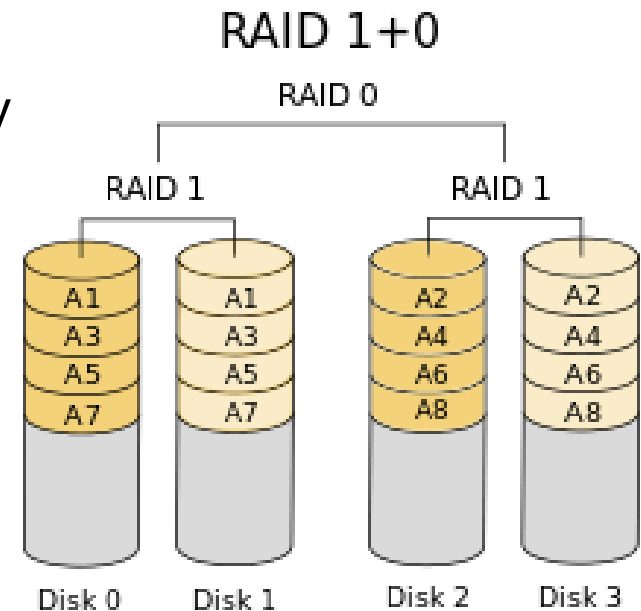
RAID 5

- Also called '**disk stripping with parity**'
- Uses block-level stripping but the **parity information is distributed over all the disks** instead of storing them in a dedicated disk
- Can handle single drive failure
 - Single disk failure data can be recovered with the help of distributed parity
 - Disk failure recovery may take longer time as parity has to be calculated from all available drives
- Minimum number of drive : 3
- Ideal for file and application servers that have a limited number of data drives



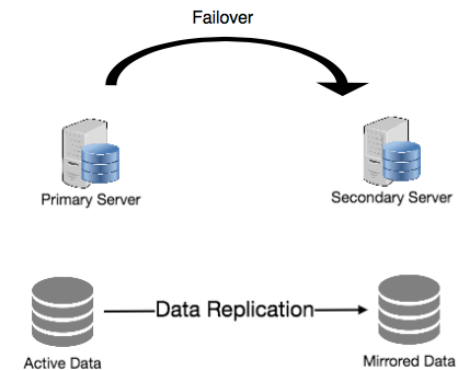
RAID 10

- RAID 10, also known as RAID 1+0, is a RAID configuration that **combines disk mirroring(1) and disk striping (0)** to protect data
 - Needs at least 4 hard drives
 - Disk utilization is 50%
 - Provides excellent fault tolerance and it has 100% redundancy
 - Data recovery is fast: not relied on parity
-
- **RAID is no substitute for back-ups!**
 - Back-up will come in handy if all drives fail

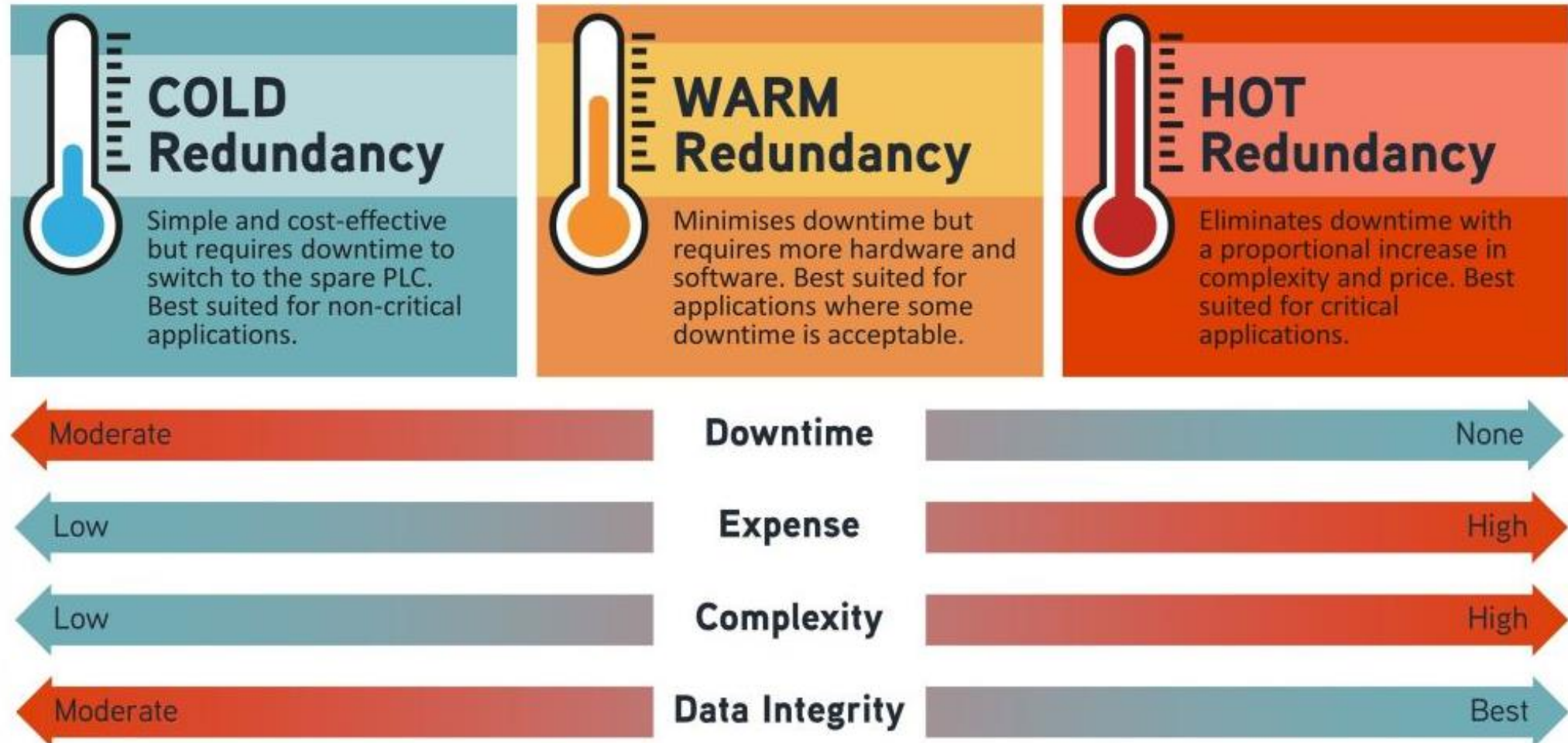


Redundancy at the Server Level

- Fault tolerant solutions
 - Use multiple servers (e.g. multiple DNS, DHCP servers)
- **Hot redundancy:**
 - Duplicate hardware, software, and data
 - Data is kept in sync with the primary server to allow for immediate failover
 - Failover is a process of switching servers (automatic or manual)
 - Cannot experience an outage for even a brief moment
 - Best for critical applications
- **Warm redundancy:**
 - Duplicate hardware and software
 - Data on the redundant hardware is not kept in sync with the primary server
 - Time and response are important but a momentary outage is still acceptable
 - Synchronization of data is needed before failover



Cold, warm, and hot redundancy: Which one is right for you?



Protecting Data with Backups

- Backup: Process of copying data stored on a computer and saving an exact duplicate of the data on another storage device
 - May include operating systems, user files, applications, and data on hard disk
 - Doesn't provide real-time protection
 - Provide protection against a greater set of problems, including failed drives, device theft, fire










Backup Platforms

- Two types of backup platforms
- **Local backup**
 - Copying data to an onsite device
 - Storage such as CD/DVD, tapes, external HD
 - Have a limited lifespan, should be replaced time to time
 - Not safe from natural disaster, security incidents, technical failures
 - IT staff will need to manage local backup
- **Cloud Backup:**
 - Copying data to an offsite server, usually hosted by a service provider
 - Storage is readily available
 - Backups are easy to configure (fully automated backups)
 - Cloud provider typically takes care of management
 - Usually slower, depends on cloud service and internet provider limits



Which backup solution is better?

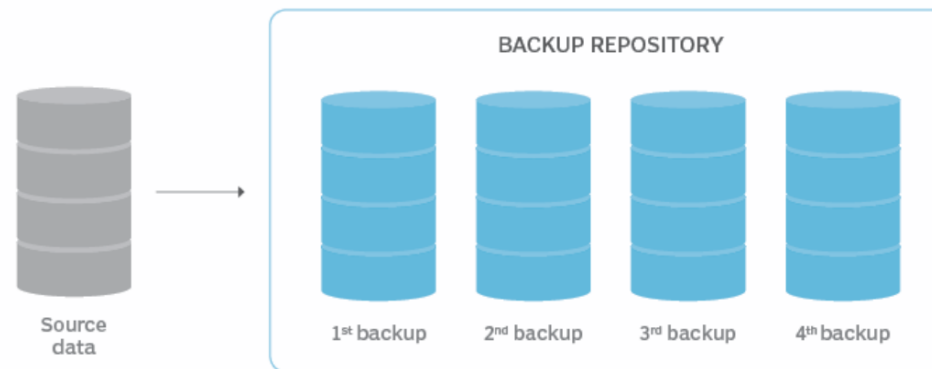
CONSIDERATIONS	CLOUD BACKUP	LOCAL BACKUP
What it is 	The process of copying data over a network to an off-site server, typically hosted by a service provider.	The process of copying data to an on-site device, typically disk-based hardware managed by backup software.
Cost 	While backing up a small amount of data to the cloud is cheap, costs can escalate quickly over time as volumes grow.	On-premises hardware, especially a disk-based product, gets expensive. Disks also need to be replaced, at a faster rate than tapes.
Scalability 	Cloud backups are easy to scale and there is essentially no storage limit, but be careful of cost as space increases.	In adding to a traditional backup setup, an organization needs to be wary of space, cost and the process of actually installing it.
Accessibility 	Cloud backups are easy to access when you're connected to the internet. However, getting lots of data out of the cloud can take a long time.	On-premises hardware is easily accessible, unless there's a disaster at that site. Speed varies, with disk among the faster techs and tape among the slower.
Security 	Increasingly less of a concern, end-to-end security will be a key feature in any top cloud backup product.	Top local backup products will have security features, but they are still susceptible to a cyberattack or a disaster at the primary site.
Management 	The cloud provider typically takes care of management, which is especially helpful for businesses that don't have the resources.	IT staff will need to manage local backup. An organization may prefer its own management versus outsourcing it to a provider.
Recovery 	Failing over to a cloud disaster recovery platform is a straightforward process, but actually recovering data out of the cloud can be burdensome.	It depends. If there's a disaster at the primary site, local backup probably won't be an option. For less catastrophic events, recovery can be quick.

Types of Data Backup

Three types of backup: Normal (Full), Differential, and Incremental

1. Normal (Full)

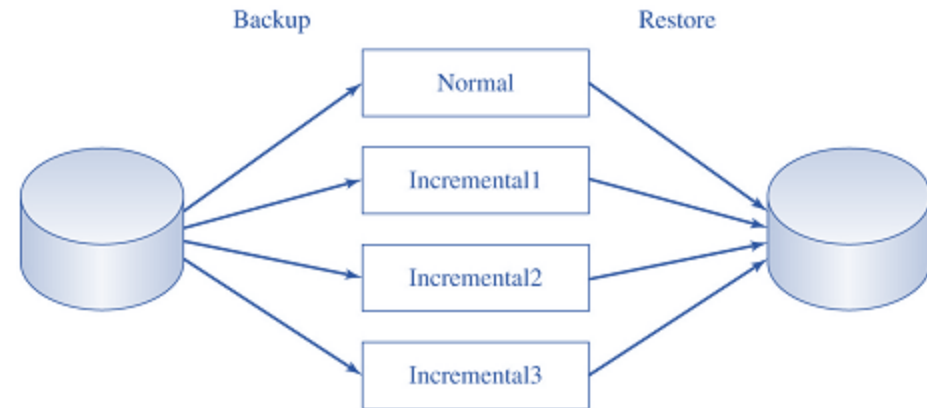
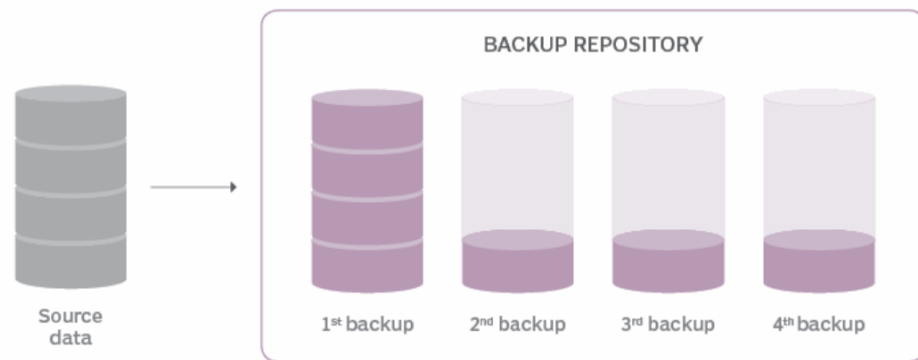
- Backs up all data whether or not data has changed since last backup
- Typically used for first backup and periodically to back up all data
- Backup duration is slow, restoration is fast
- Typically scheduled for off-peak time, weekends, because of time required
- Overloads storage space



Types of Data Backup

2. Incremental

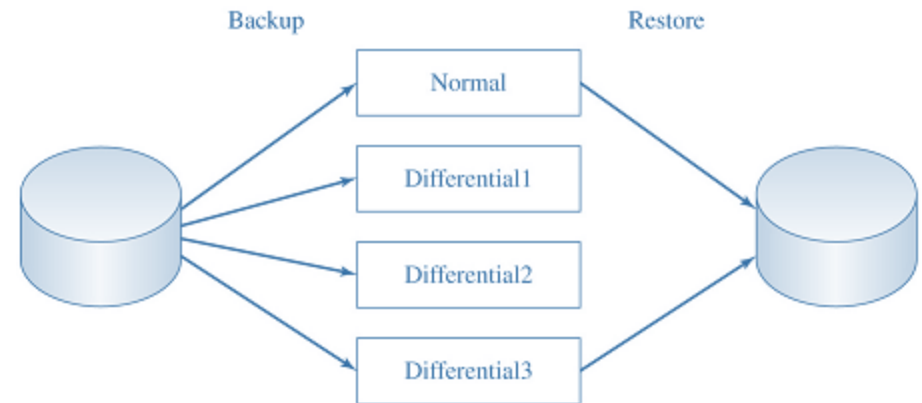
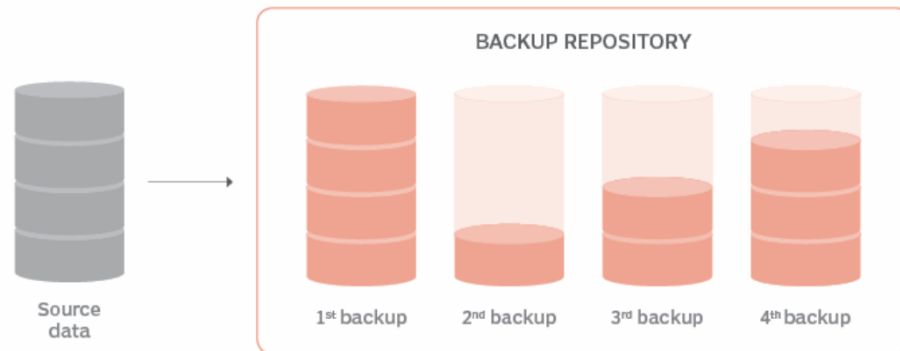
- Backs up changed data
- Scans the last full backup and proceeds with the backup of new data only
- Restoration requires full backup and all incremental backups
- Backup is fast, restoration is slow
- Good choice for companies with large amounts of strategic data, for example, weekly use of full backups, followed by a daily incremental routine



Types of Data Backup

3. Differential Backups

- Same basic structure as an incremental backup: it involves making copies only of new files or of files that underwent some kind of change
- Restoration requires a full backup and most recent differential backup only
- Backup is fast, restoration is fast

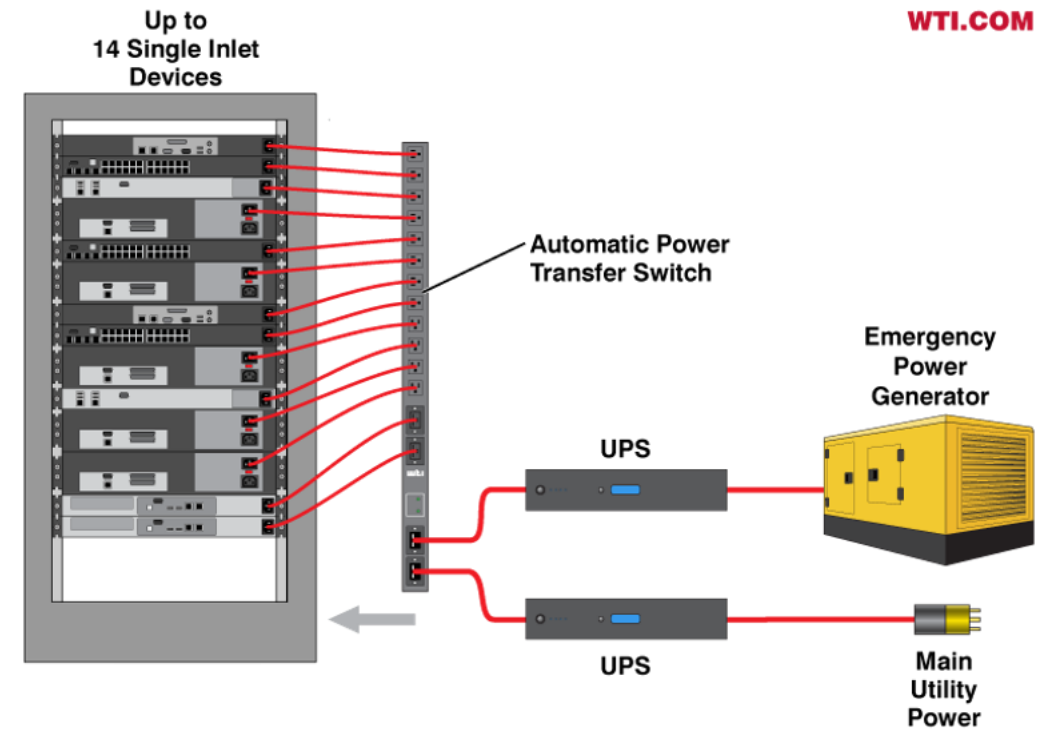


Difference Between Full, Differential and Incremental Backups

	Full	Incremental	Differential
Storage Space	High	Low	Medium to High
Backup Speed	Slowest	Fastest	Fast
Restoration Speed	Fastest	Slowest	Fast
Media Required for Recovery	Most recent backup only	Most recent full backup & all incremental backups since full backup	Most recent full backup & most recent differential backup
Duplication	Stores a lot of duplicate files	No duplicate files	Stores duplicate files

Power Redundancies

- Used to minimize system downtime in case of power failure
- UPS
 - Provides short-term fault tolerance for power
 - Can protect against power fluctuations
- Generators provide long-term fault tolerance for power
- Automatic Transfer Switches can prevent downtime by instantly switching to back-up/emergency power when the primary power source is interrupted



[What is a Redundant Power Supply and How Does It Work?](#)

Summary

- What is endpoint security and why is it essential?
- Key tools: UEM, EDR, DLP, NGFW
- Techniques for hardening endpoints
- How to apply fault tolerance and redundancy
- Best practices for backup and power protection