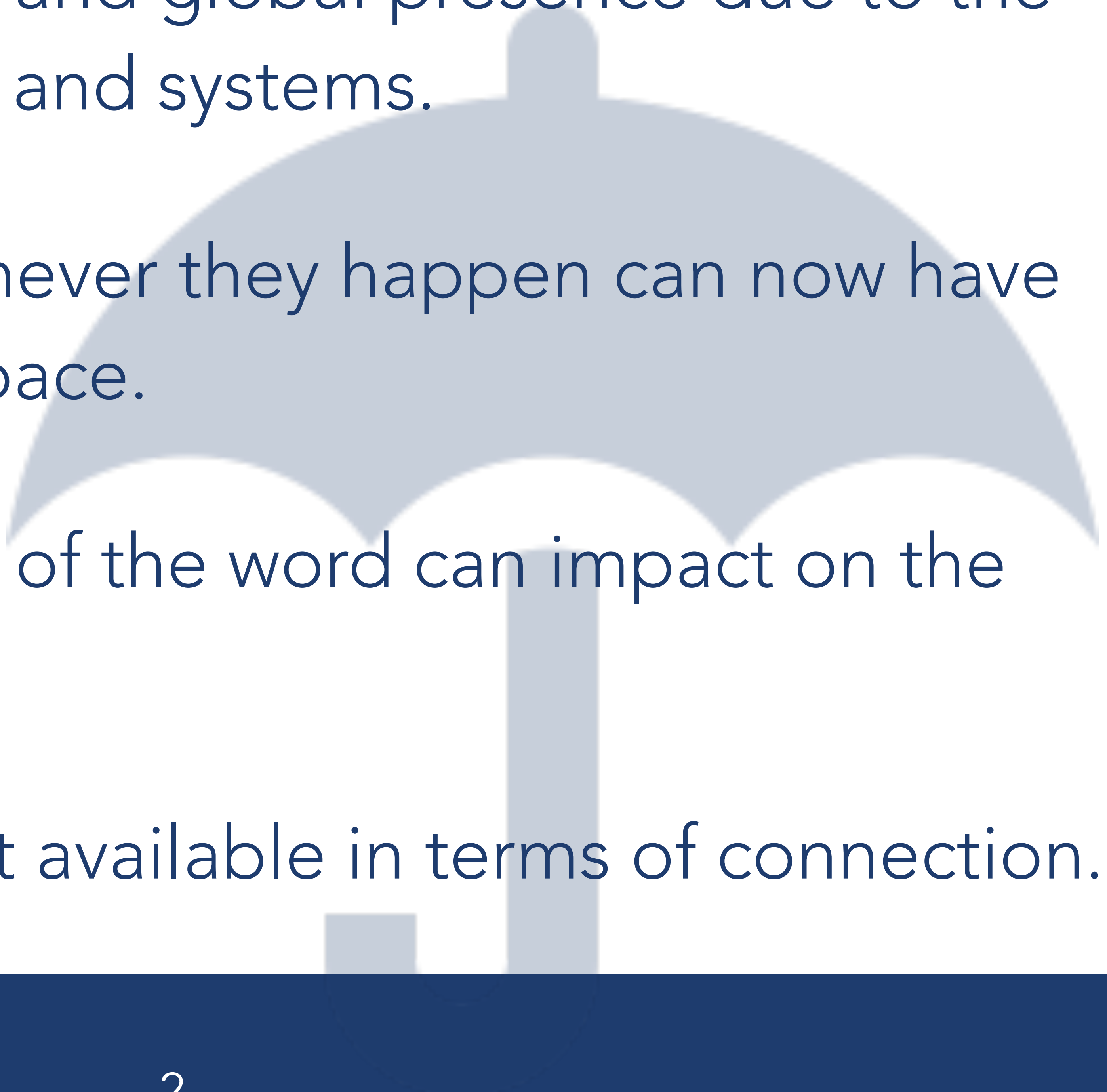
ENTERPRISE CYBER SECURITY

BUSINESS CONTINUITY MANAGEMENT

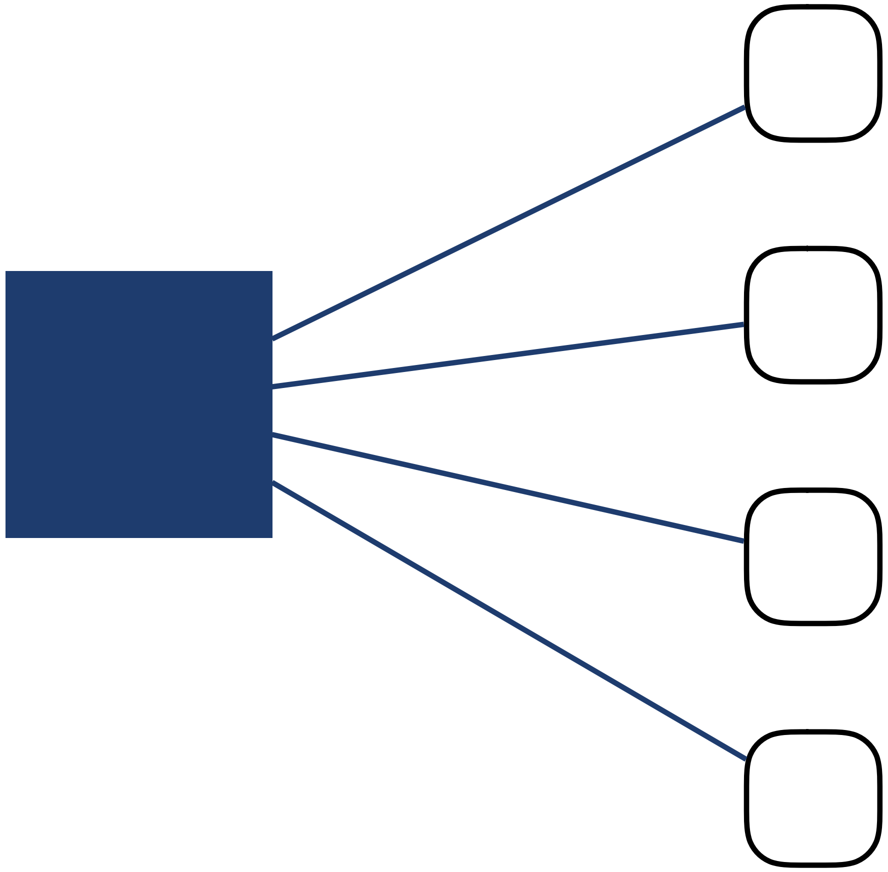
University of Glasgow

CONTINUITY

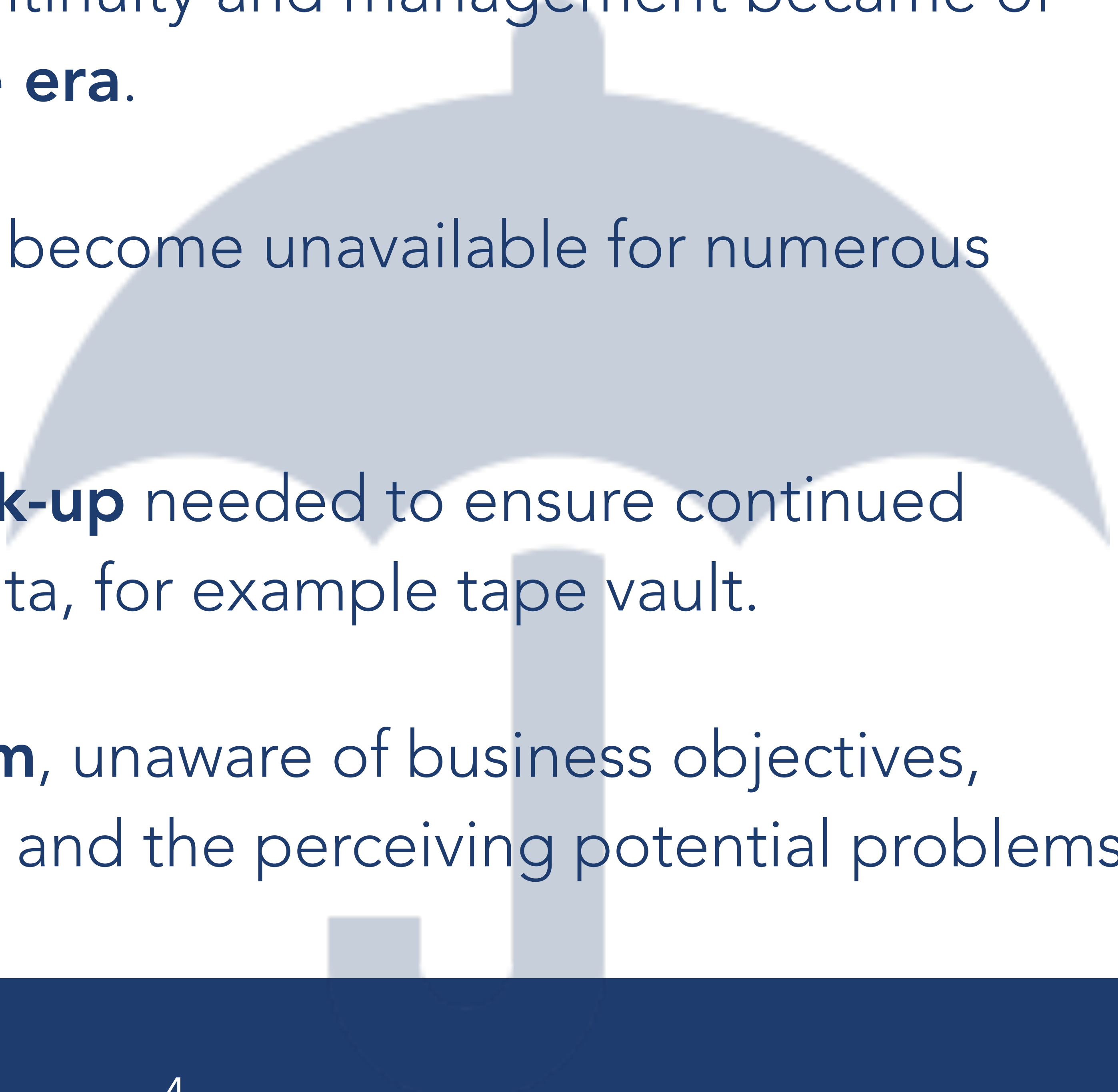
- companies have local and global presence due to the power of cyber space and systems.
- natural disasters whenever they happen can now have an impact on cyber space.
- failure in another part of the word can impact on the system right here.
- information keeping it available in terms of connection.



MAINFRAME ERA (1950S-70S)



PRE-HISTORY



- reality is that business continuity and management became of interest in the **mainframe era**.
- central system that could become unavailable for numerous reasons.
- **periodic copies and back-up** needed to ensure continued access and integrity of data, for example tape vault.
- **dedicated technical team**, unaware of business objectives, focused on a single room and the perceiving potential problems.

PRE-HISTORY

- notion of **disaster recovery** came from the logic of bringing system back online.
- recall though such elements are part of a **larger system** that is working towards some goal.
- recovery and continuity could be managed by **technical teams**, but it is debatable if this is optimal.

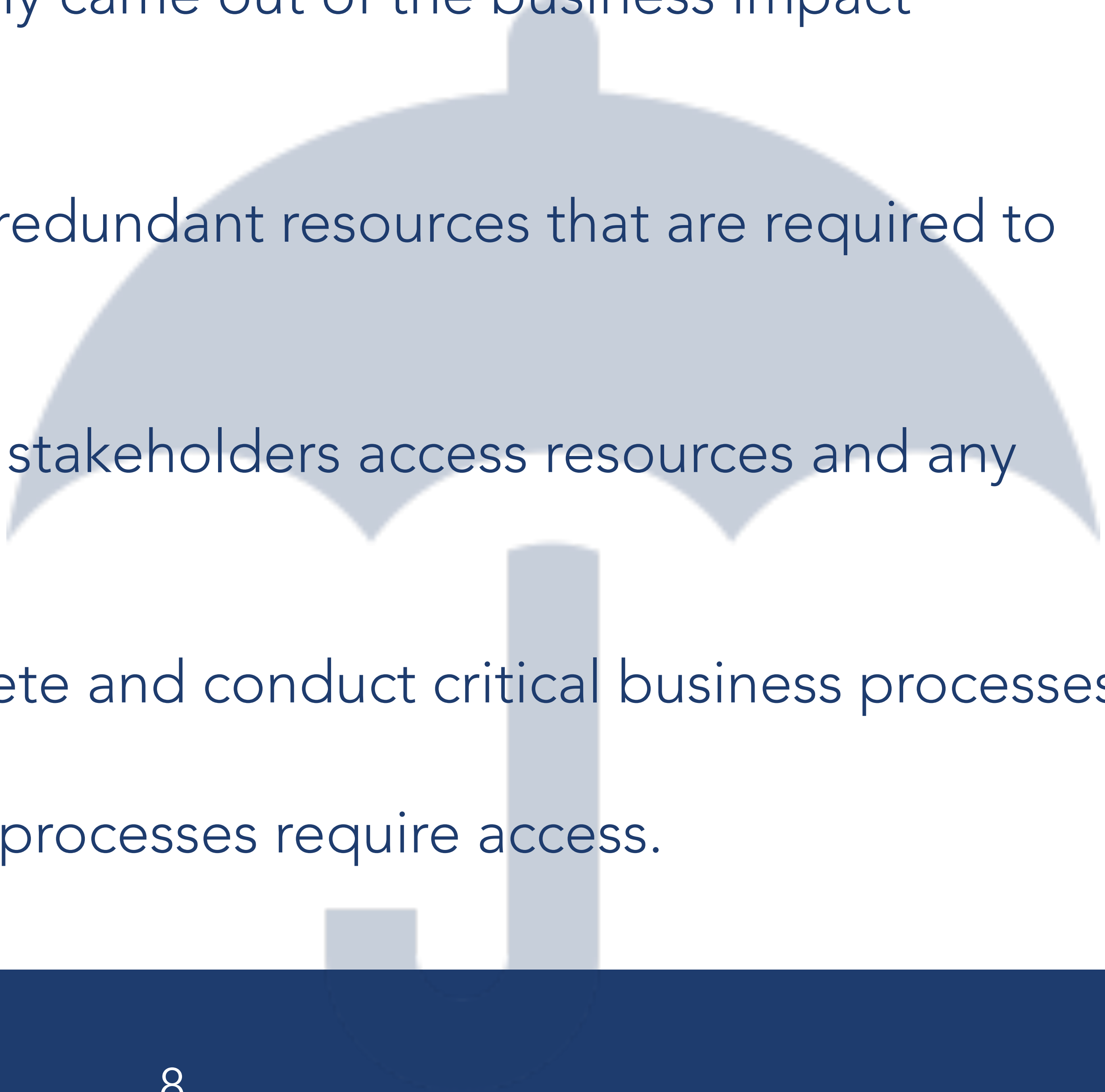
STRATEGY

RECOVERY REQUIREMENTS

- business impact analysis will have informed **critical processes** and the **window of recovery**.
- need to consider other recovery requirements that an enterprise will need consider.

RECOVERY REQUIREMENTS

- **time** requirements essentially came out of the business impact analysis.
- **utilisation** or occupancy of redundant resources that are required to continue processes.
- **geography** in terms of how stakeholders access resources and any additional requirements.
- **facilities** required to complete and conduct critical business processes.
- **assets** that critical business processes require access.



CONTINGENCIES

- **balance** between the expense and risk appetite of the enterprise.
- can guarantee access to cyber systems such as **mainframe** applications if they are under control.
- **external** parties becomes challenges, SLAs can be used as guarantees.
- consider the balance of the system and the needs of continuation.

CONTINGENCIES

- internal
- external
- mutually assured
- reactive

INTERNAL

- in-house provision of redundancy is traditionally the most expensive, but the least risk option.

- unfettered access to redundant resources and can conduct tests.

- consider the expense of provisioning redundant infrastructure and hardware within an enterprise.

- expense of maintaining and securing such elements is non-trivial and could create problems.

EXTERNAL

- redundant resources and **sold several times over**, consider cloud computing.
- **minimises costs** and potentially reduces specific security concerns from some perspectives.
- **warm vs cold** start recovery redundant options for large enterprises.
- **unforeseen costs** associated with time and resource allowances associated with contracts.

MUTUALLY ASSURED

- enterprises can enter into agreements to support one another during crisis moments.

- complexities ensure that such agreements should be formalised by parties.

- reduces costs associated with maintaining redundant resources in terms of equipment and staff.

- displaced activity could impact on the supporting enterprise, compromising their critical processes.

REACTIVE

- alternative is to react to issues when they occur, this may be possible for some situations.

- purchase of the off-the-shelf components and resources.

- consider the complexity and expense in purchase off-the-shelf resources and how useful.

RESTORATION

- areas of restoration can often only be determined once incidents occur.
- planning in advance can reduce the impact an incident could have on an enterprise.
- considering the critical processes and what may need to deployed elsewhere.

SALVAGE

- coupled with restoration, salvage of existing elements may be the most efficient method to continue critical processes.

- involve process of segregating and quarantining hardware rapidly.

- terminating communications or shutting authentication procedures or specific transactions.

DATA

DATA

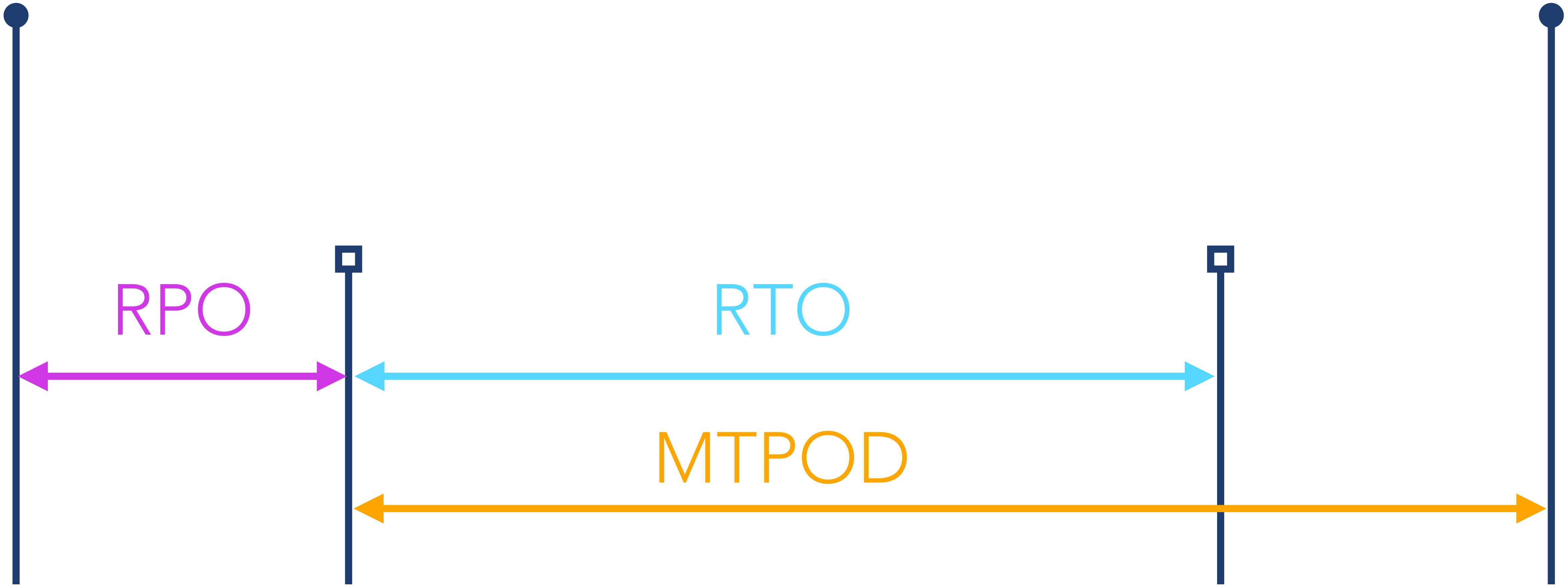
- recovery is not just about duplicating data for the purposes of back-up.
- the aim is to recovery from failure and keeping the critical processes flowing.
- also need to consider the process of archive in specific situations and these may be mandated by specific regulations.
- core question when duplicating data is why the data is being duplicated.

INFLUENCE FACTORS

- recall RPO, the window of data loss the enterprise is willing to sustain.
- recall RTO, the window of recovery time to bring an organisation back online.
- availability of data is crucial, enterprises will lose when it is not available.
- reliable systems are not necessarily available system.
- need to understand the **value** of data to justify the cost of duplication.

UNDERSTANDING RTO, RPO AND MTPOD

UNDERSTANDING RTO, RPO AND MTPOD



INFLUENCE FACTORS

- recall RPO, the window of data loss the enterprise is willing to sustain.
- recall RTO, the window of recovery time to bring an organisation back online.
- availability of data is crucial, enterprises will lose when it is not available.
- reliable systems are not necessarily available system.
- need to understand the **value** of data to justify the cost of duplication.

BACKUP STRATEGIES

- there are many different back-up strategies that enterprise may decide to use.

- enterprises could agree a contract with an **external** provider to duplicate data.

- data could be duplicated to **tape**, supporting cheap duplication and numerous locations.

- transfer data to **disks** to ensure efficient duplication and retrieval of data.

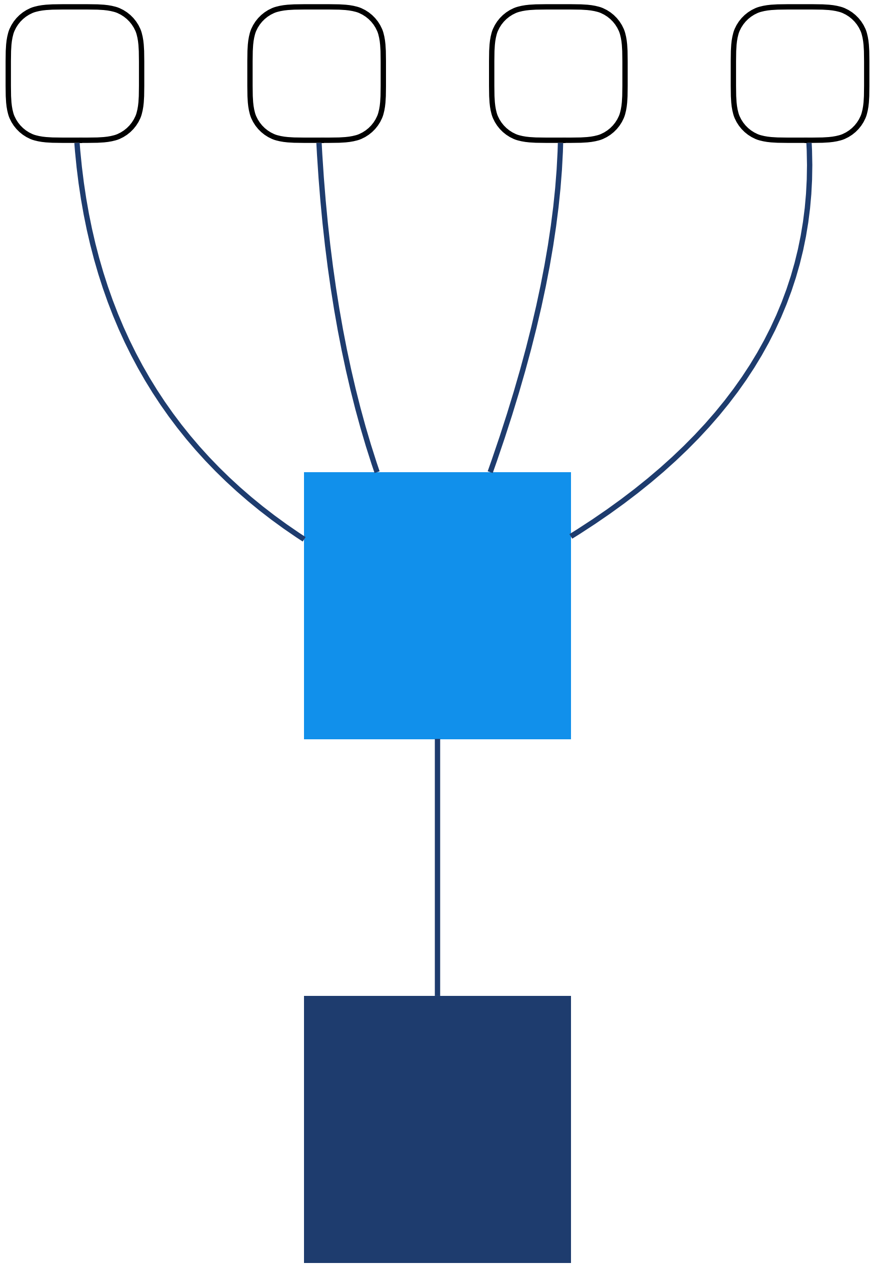
EXTERNAL

- enterprise could enter into agreement with an external partner to duplicate and archive data.
- SLAs can be agreed to ensure partnering organisations actual meeting back-up requirements.
- concern is that the enterprise is entrusting its business to an external force.
- external parter may have more experience at securing data as well as ensuring compliance standards.

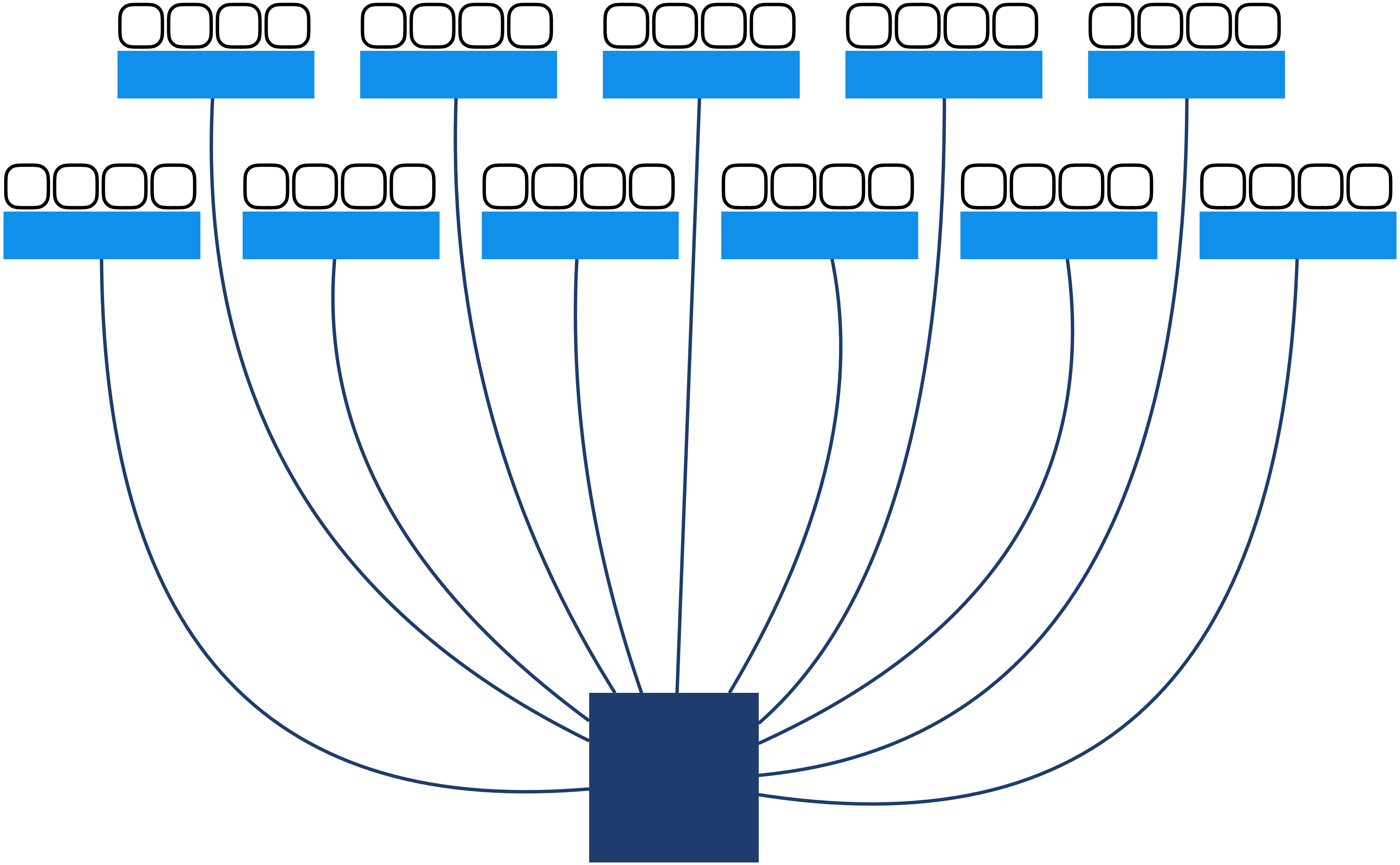
TAPE

- incredibly inexpensive to manage and store data on tapes.
- can be managed in multiple locations, format is easily moved around and administrators should be familiar with it.
- expense of production elements, increasingly complex routines and the reliability of the process.
- window of duplication as well as the long-term archival issues associated with it.

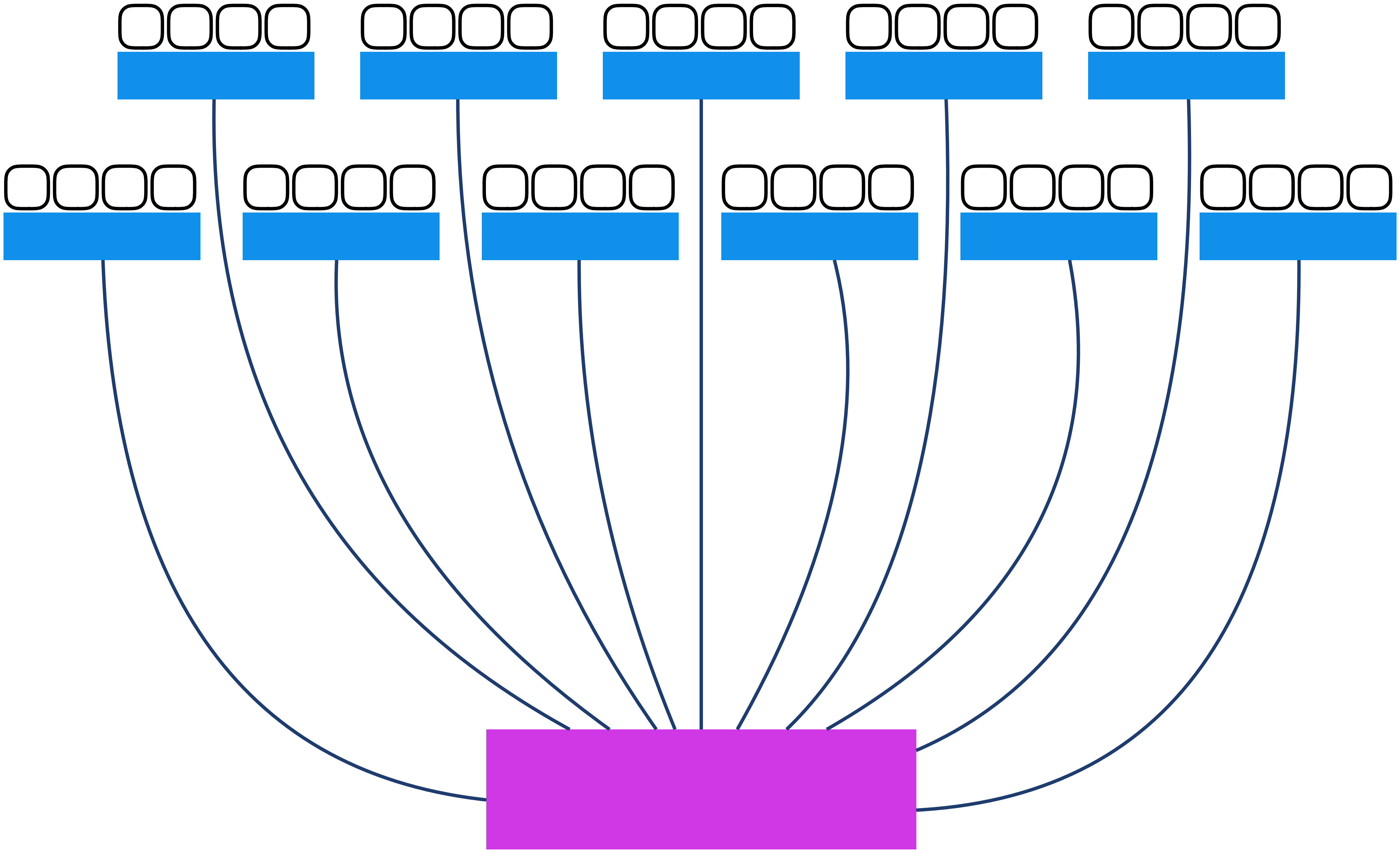
TAPE



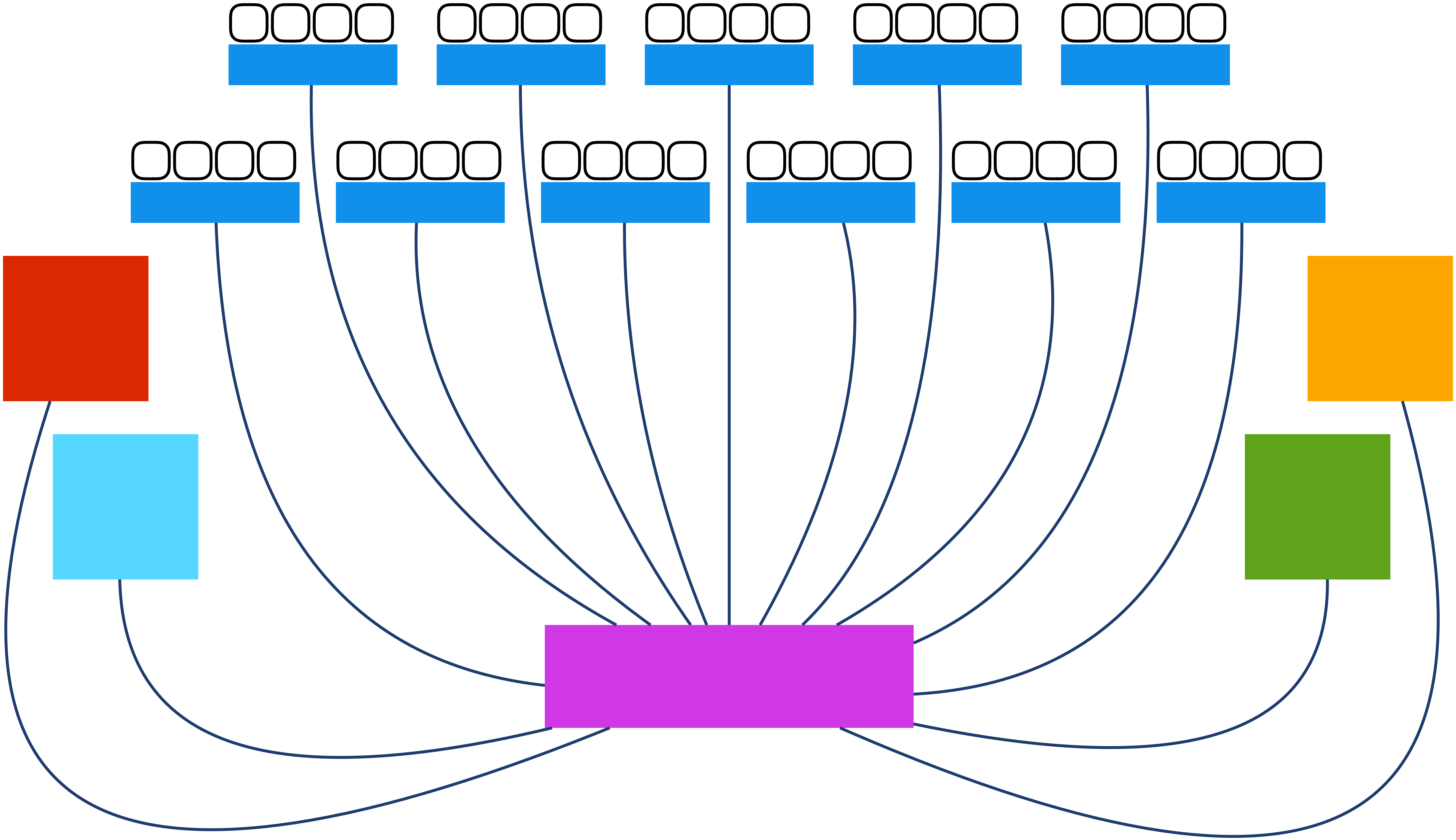
TAPE VS CLOUD COMPUTING



VIRTUAL TAPE LIBRARY

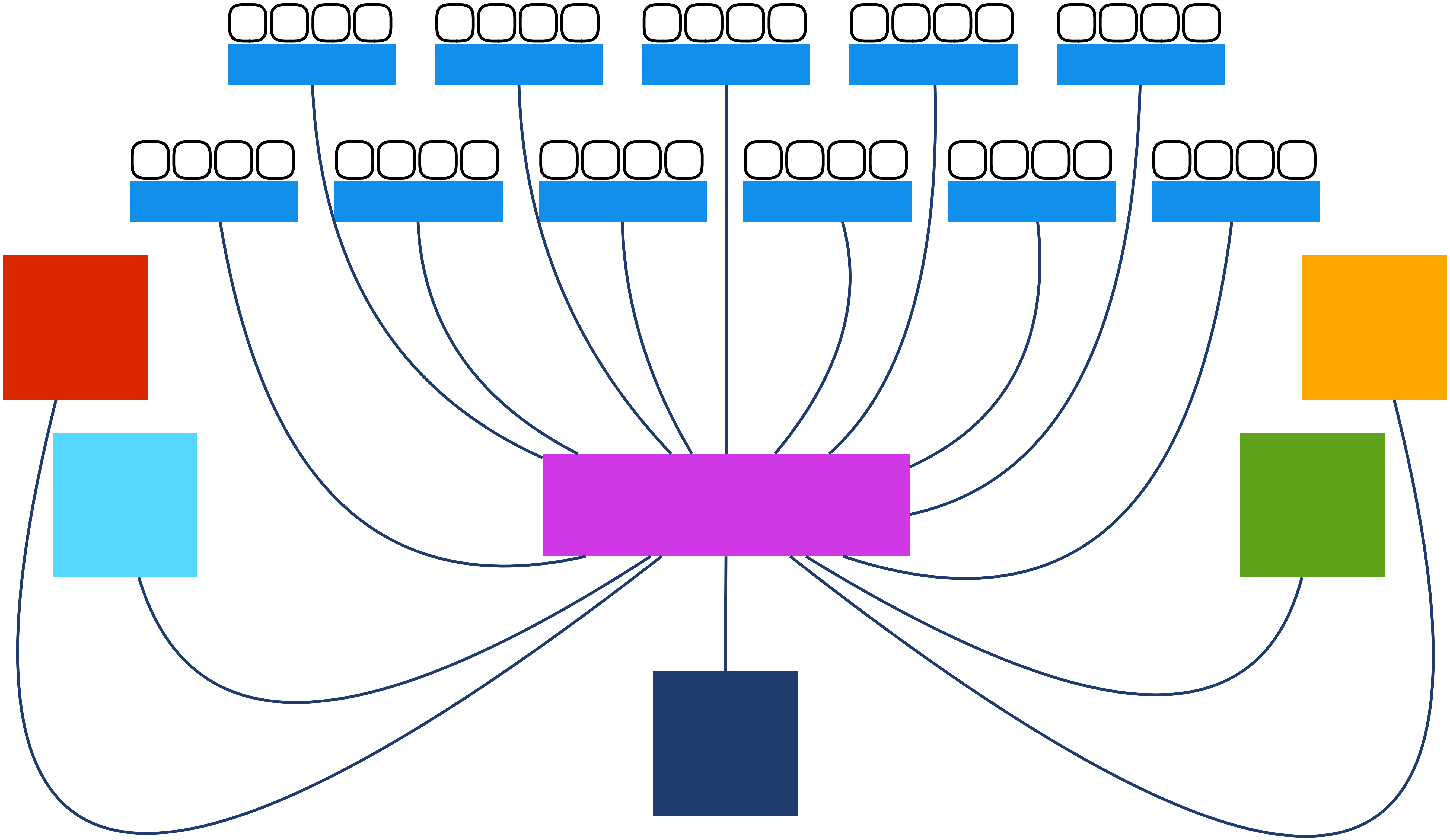


VIRTUAL TAPE LIBRARY



DDT

DDT



DISK TO DISK

- more expensive than tape, but typically offer better performance in terms of backup and restore.
- hard disks are often cheap and can be used for the purposes of backup.
- typically have improved efficiency in terms of back-up and restore.
- approaches include virtual tape libraries, content-addressable storage and continuous data protection.

VIRTUAL TAPE LIBRARY (VTL)

- virtual tape libraries afford tape methodologies with fast, inexpensive disks.
- improves back-up and restore of data in terms of continuity.
- physical tapes can still be used to back-up the virtual tape library.
- concerns surround the use physical disks that need to flow of energy and are typically not removable.

CONTENT-ADDRESSABLE STORAGE (CAS)

- high-speed storage of fixed-sized archival data based on **content rather than location**.

- content-addressed storage means changing the content can actually **change the location** of data.

- content-addressed storage is ideal for **long-term storage** of content that needs to be retrieved easily.

- useful approach for **complying** with standards such as Sarbanes-Oxley and HIPAA.

CONTINUOUS DATA PROTECTION (CDP)

- continuous data protection effectively generates a new version of a file for every alteration.

- can recover from a particular version of a file, rather than from the last available back-up.

- can adopt a different strategy to back-up, rather than every write, may just create a copy over a particular window, known as **near continuous**.

- there are some concerns associated with continuous data protection.

PROBLEMS WITH DATA BACKUP

DATA DEDUPLICATION

DATA DEDUPLICATION

- data deduplication is process of **reducing redundant data**.
- consider the problem of **compression** and how to reduce and archive data.
- considerable redundant could be consume space and energy at **rest** on disks.
- not only the storage, consider the communication **bandwidth** expense in transporting all the data.

DATA DEDUPLICATION

- many different way to consider data duplication could be in terms of but can consider in terms of **files** or **blocks**.
- files could have different filenames, but essentially represent the **same binary data**.
- files could be different, but contain similar **patterns** or blocks of binary data.
- instead of repeatedly storing the same files or patterns, **store original and point the others to it**.

DATA DEDUPLICATION

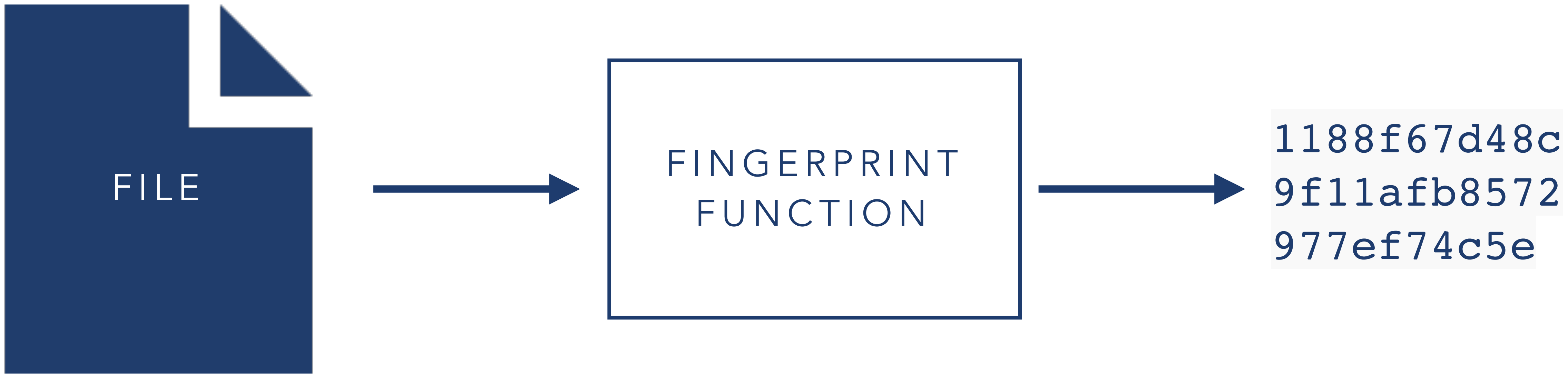
- process essentially requires **fingerprinting** data using a one-way hash function.

- **store** all the fingerprints for the files within the system.

- **process** now is compute hash or rather, produce fingerprint.

- **compare** fingerprint, if present store as pointer to existing data, if not add fingerprint to store.

FINGERPRINTING



FILE

FINGERPRINT FUNCTION

```
1188f67d48c
9f11afb8572
977ef74c5e
```

DATA DEDUPLICATION

- process essentially requires **fingerprinting** data using a one-way hash function.

- **store** all the fingerprints for the files within the system.

- **process** now is compute hash or rather, produce fingerprint.

- **compare** fingerprint, if present store as pointer to existing data, if not add fingerprint to store.

DATA DEDUPLICATION

- process **reduces** the need to store lots of redundant data.
- ensures enterprise is **not storing lots of duplicates** of data on its systems.
- more importantly, **reduces the expense in transmitting** all the data between the different parts of the system.
- need to consider where the **process will actually occur**.

SOURCE VS TARGET

- **source-based deduplication** occurs on the client or source device before transmission.
- requires **source device to communicate** with the server to determine if the data is already exists.
- **target-based deduplication** occurs on the actual server coordinating storage.
- efficiencies can be made without making any significant alterations to the source device.

CYBER SECURITY AND PRIVACY

CYBER SECURITY AND PRIVACY

- concerns surrounding the **cyber security and privacy** of such an approach.
- potential for attackers to gain **insight** into the data being stored by enterprises and employees in cloud computing.
- consider two specific attacks, that is **identifying a specific file** and determine **existence of a file**.
- consider the potential as well from an implementation perspective of attackers stealing the **fingerprint**.

SPECIFIC FILE

- need to determine the **ownership** or **existence** of a specific file.
- consider an **indecent image** of child pornography or even a celebrity image.
- Alice can use **deduplication** to see if a specific file exists on a given service.
- Alice could obtain a court order to demand the cloud service provider reveal the **identity** of the owner, Bob.

SALARY ATTACK

- consider the number of **standard letters** that an enterprise generates and dispatches.

- standard letters have **small alterations** - consider PIN reminder letters, pay or medical letters.

- Alice could brute-force **generate** such letters altering the specifics of determine the existence of it.

- reasonable attack if the alterations are relatively restricted, becomes difficult if they are varied.

SOLUTIONS

SOLUTIONS

- enterprises and employees could **encrypt data** to prevent it from being deduplicated.
- concerns from cloud service providers that it makes it difficult to **benefit** from the nature of the cloud.
- ignore small files and instead **focus on larger files** that would still result in efficiency savings.
- consider the reality that keeping **rarer files private** is arguably more important than common files.