SEC-202: Secure Start-Up

Lecture 3 – Infrastructure Security

Instructed By:

Dr. Charnon Pattiyanon

Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer Engineering (AICE) Program

Class Agenda

- Asset Inventory
- Network Security
- Container Security
- Secure Remote Access
- Availability and Backups
- Physical Security

The Foundation – Asset Inventory

- **The Golden Rule:** You cannot protect what you can't see.
- **The Problem:** Most companies rely on a spreadsheet to track laptops. This is obsolete the moment it is saved.

- **Modern Inventory:**
  - Hardware: Laptops, Servers, Routers.
  - Software: Installed apps, SaaS subscriptions.
  - Data: Where does PII live?
- **Automated Discovery:** Using tools that scan the network (Nmap, Rumble/runZero) to find "**ghost**" devices.

The Shared Responsibility Model

“I use AWS, so I am secure”

- **Reality:**
  - The Provider (AWS/Azure/GCP): Secures the Cloud (Compute, Storage, Database, Networking, Global Infrastructure).
  - The Customer (You): Secures what is **IN** the Cloud (Data, Identity, OS patching, Network configuration).
- **Takeaway:** If you leave an S3 bucket open to the public, that is your fault, not Amazon's.

The Shared Responsibility Model

Data of TrueMove H users leaked online

PUBLISHED : 15 APR 2018 AT 05:00
NEWSPAPER SECTION: NEWS WRITER: SUCHIT LEESA-NGUANSUK AND KOMSAN TORTERMVASANA

Add as a preferred source on Google

The personal data of around 46,000 TrueMove H users was leaked into Amazon Web Services' cloud storage, leading the National Broadcasting and Telecommunications Commission to call in the company for questioning. (Photo by Narupon Hinshiranan)

MainPassengerID	PassengerType	ReservationID	Title	FirstName	SurName	DateOfBirth	MobileNo	PassportNo	PassportExpDate
0	"Adult"	"JT1008"	"Mr."	[redacted]		"1996-03-28 00:00:00"			
0	"Adult"	"JT1009"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1001"	"Ms."			"1988-10-29 00:00:00"			
0	"Adult"	"SL1002"	"Ms."			"1988-10-29 00:00:00"			
0	"Adult"	"SL1003"	"Mr."			"1986-10-30 00:00:00"			
0	"Adult"	"SL1004"	"Ms."			"1988-10-29 00:00:00"			
0	"Adult"	"SL1005"	"Mr."			"1990-03-28 00:00:00"			
0	"Adult"	"SL1006"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1007"	"Mr."			"1988-06-07 00:00:00"			
324054	"Child"	"SL1007"	"Mstr."			"2002-08-07 00:00:00"			
324054	"Infant"	"SL1007"	"Mstr."			"2012-06-06 00:00:00"			
0	"Adult"	"SL1008"	"Mr."			"1996-03-28 00:00:00"			
324057	"Adult"	"SL1008"	"Mr."			"1996-03-28 00:00:00"			
324057	"Child"	"SL1008"	"Mstr."			"2011-12-05 00:00:00"			
0	"Adult"	"SL1009"	"Mr."			"1977-06-03 00:00:00"			
0	"Adult"	"SL1010"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1011"	"Ms."			"1988-10-29 00:00:00"			
0	"Adult"	"SL1012"	"Mr."			"1990-03-28 00:00:00"			
0	"Adult"	"SL1013"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1014"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1015"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1016"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1017"	"Mr."			"1990-03-28 00:00:00"			
0	"Adult"	"SL1018"	"Mr."			"1984-02-03 00:00:00"			
0	"Adult"	"SL1019"	"Mr."			"1996-03-28 00:00:00"			
0	"Adult"	"SL1020"	"Mr."			"1996-03-28 00:00:00"			
324071	"Child"	"SL1020"	"Mstr."			"2011-12-05 00:00:00"			
324071	"Infant"	"SL1020"	"Mstr."			"2013-03-28 00:00:00"			
0	"Adult"	"SL1021"	"Mr."			"1996-03-28 00:00:00"			
324074	"Child"	"SL1021"	"Mstr."			"2011-12-05 00:00:00"			

Tens of millions of records belonging to passengers of two airline companies owned by Lion Air have been exposed and exchanged on forums.

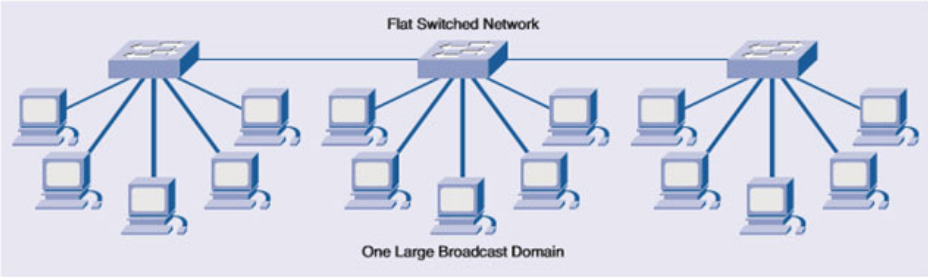
Data belonging to passengers of two airline companies owned by Lion Air have been exposed and exchanged on forums.

The information was left exposed online on an unsecured Amazon bucket, the records were stored in two databases in a directory containing backup files mostly for Malindo Air and Thai Lion Air. The most recent backup, dated May 25, is named 'PaymentGateway.'

The directory was created in May 2019, the databases included respectively 21 million records and 14 million records. It seems that data was circulating on exchange forums since August 10.

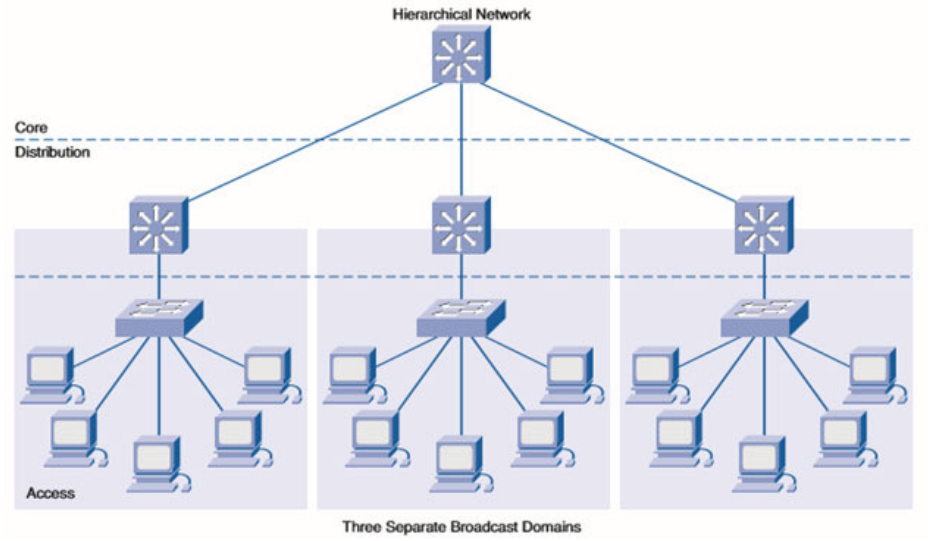
The directory also included a backup file for the Batik Air that is owned by Lion Air. Leaked records include passenger and reservation IDs, physical addresses, phone numbers, email addresses, names, dates of birth, phone numbers, passport numbers, and passport expiration dates.

Network Segmentation



- **Flat Networks (Bad):** Everyone is on the same Wi-Fi.

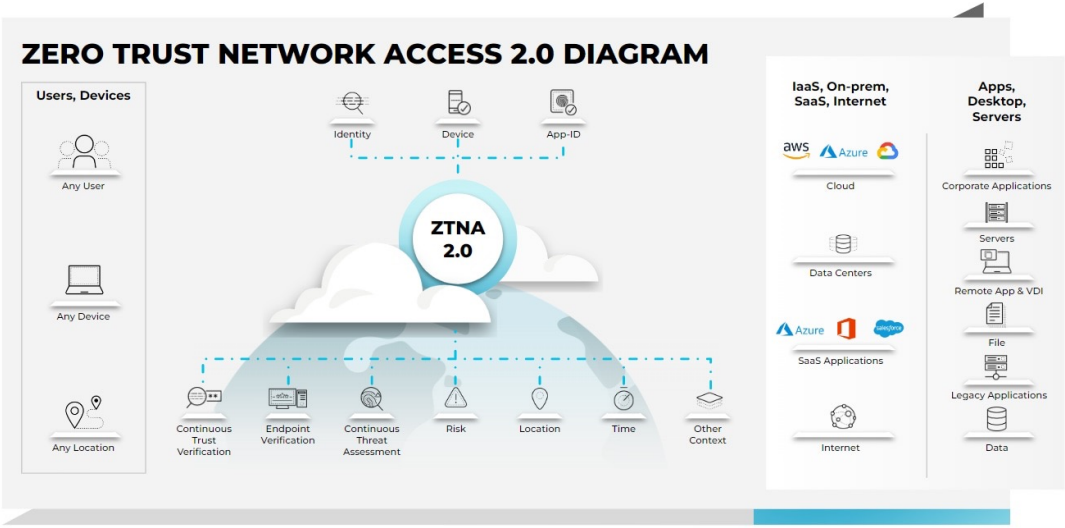
  If a receptionist gets a virus, it can spread to the CEO's laptop and the Production Database.



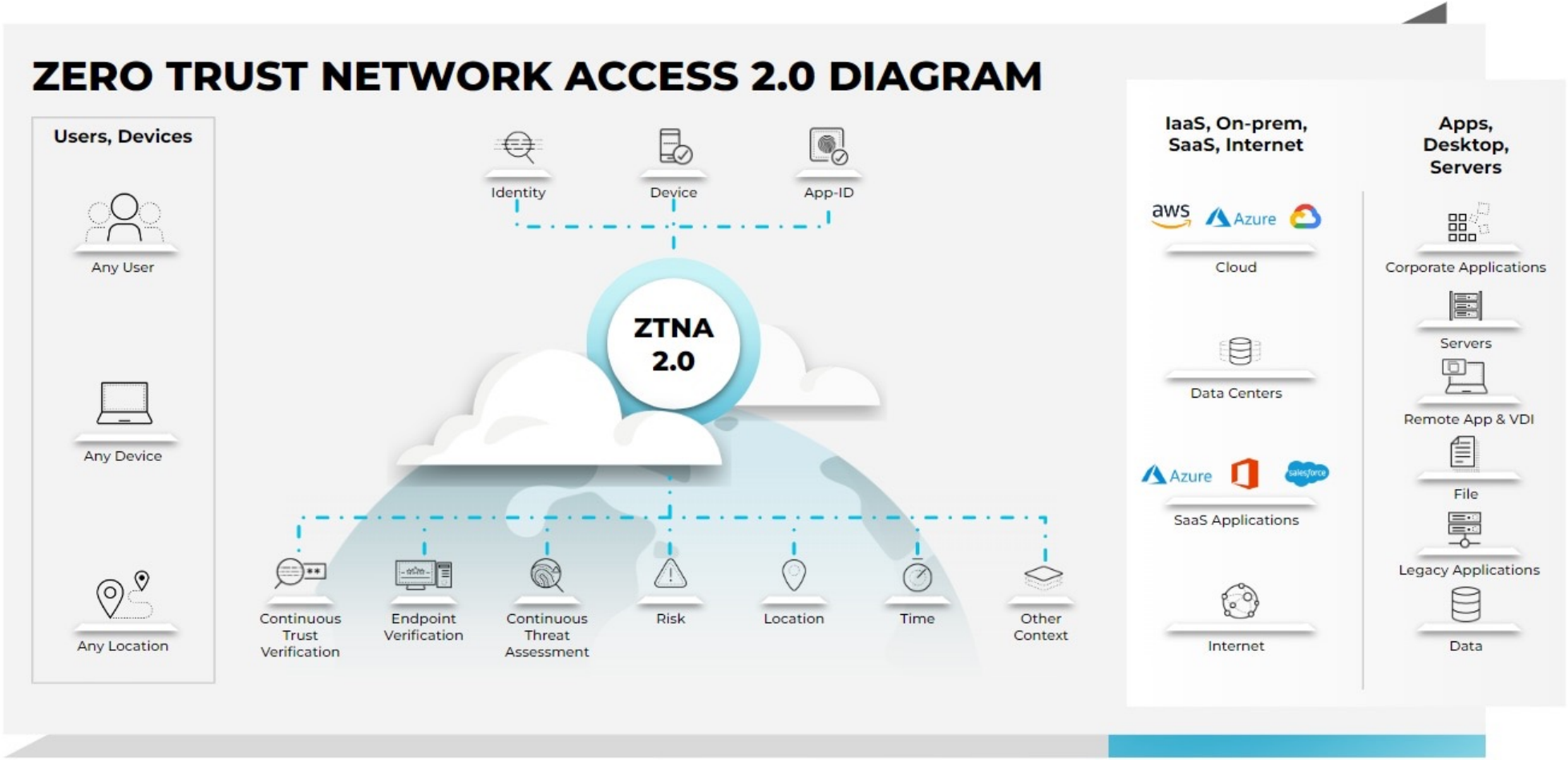
- **Segmented Networks (Good):** Using VLANs (Virtual Local Area Networks) and Subnets to build internal walls.
  - Example: The "Guest Wi-Fi" should dump traffic straight to the internet, never touching the internal office printer or server.

Network Segmentation

- **Zero Trust Network Access (ZTNA):** The modern evolution—segmenting down to the specific application, not just the network zone.
- With ZTNA, access is established after the user has been authenticated to the ZTNA service. The ZTNA service then provisions access to the application on the user's behalf through a secure, encrypted tunnel. This provides an added layer of protection for corporate applications and services by shielding otherwise publicly visible IP addresses.



Network Segmentation

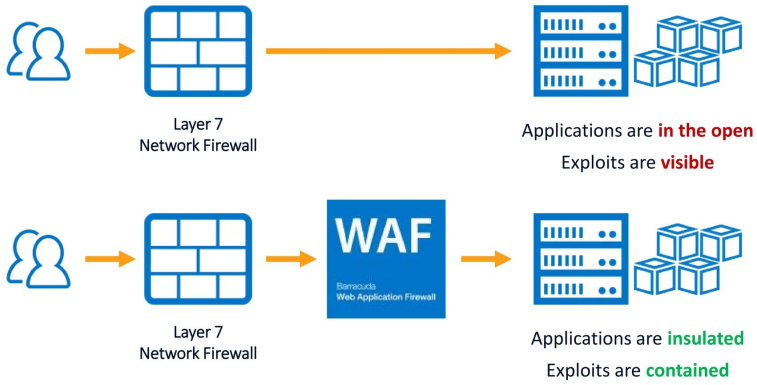


Firewalls – Network vs. Application

Network Firewall (Layer 3/4):

- The "Bouncer" at the door.
- Checks IP Addresses and Ports.
  (e.g., "Block all traffic from North Korea").

WAF Extends Your Network Security Posture



Web Application Firewall / WAF (Layer 7):

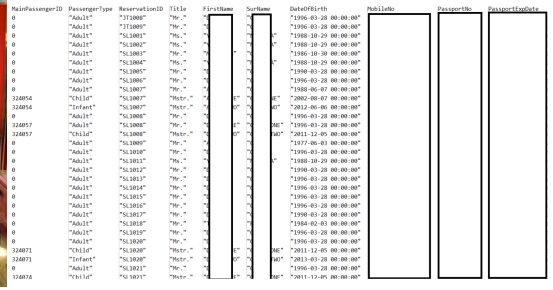
- The "Translator."
- Inspects the actual conversation (HTTP traffic).
- Blocks attacks like SQL Injection or Cross-Site Scripting (XSS) that a normal firewall would miss.

PARAMETER	WAF	NETWORK FIREWALL
Philosophy	A **Web Application Firewall (WAF)** is a network security firewall solution that protects web applications from HTTP/S and web application-based security vulnerabilities.	**Network Firewall** is a device which controls access to secured LAN network to protect it from unauthorized access. Firewall acts as a filter which blocks incoming non-legitimate traffic from entering the LAN network and cause attacks.
OSI Layer coverage	Layer 7	Layer 3 - 4
Modes of operation	• Active Inspection • Passive mode	• Transparent mode • Routed mode
DDOS Protection	Application Layer	Basic level only at Network Layer
Target objects protection	Protects HTTP/HTTPs based servers and Applications placed in Internet facing Zones of Network Firewall	Protection of user and organizational IT assets including applications, Servers and management.
Placement in Network	Close to Web/Internet Facing Applications	On Perimeter of Network (Commonly Internet)
Web Application protection	All-encompassing, including complete coverage of application layer	Minimal
Access Control	Not possible	Possible
Algorithms	• Signature based • Anomaly detection • Heuristics	• Packet filtering • Stateful/stateless inspection • Proxy
Related attacks protection	• SQL injection attacks • cross-site scripting (XSS) attacks • DDoS attacks.	• Attack from less secured zones. • Unauthorised users accessing private networks
		https://ipwithease.com

Cloud Security Posture Management (CSPM)

Data of TrueMove H users leaked online

The personal data of around 46,000 TrueMove H users was leaked into Amazon Web Services' cloud storage, lea
National Broadcasting and Telecommunications Commission to call in the company for questioning. (Photo by N
Hinshiranan)



Tens of millions of records belonging to passengers of two airline companies owned by Lion Air have been exposed and exchanged on forums.

Data belonging to passengers of two airline companies owned by Lion Air have been exposed and exchanged on forums.

The information was left exposed online on an unsecured Amazon bucket, the records were stored in two databases in a directory containing backup files mostly for Malindo Air and Thai Lion Air. The most recent backup, dated May 25, is named 'PaymentGateway.'

The directory was created in May 2019, the databases included respectively 21 million records and 14 million records. It seems that data was circulating on exchange forums since August 10.

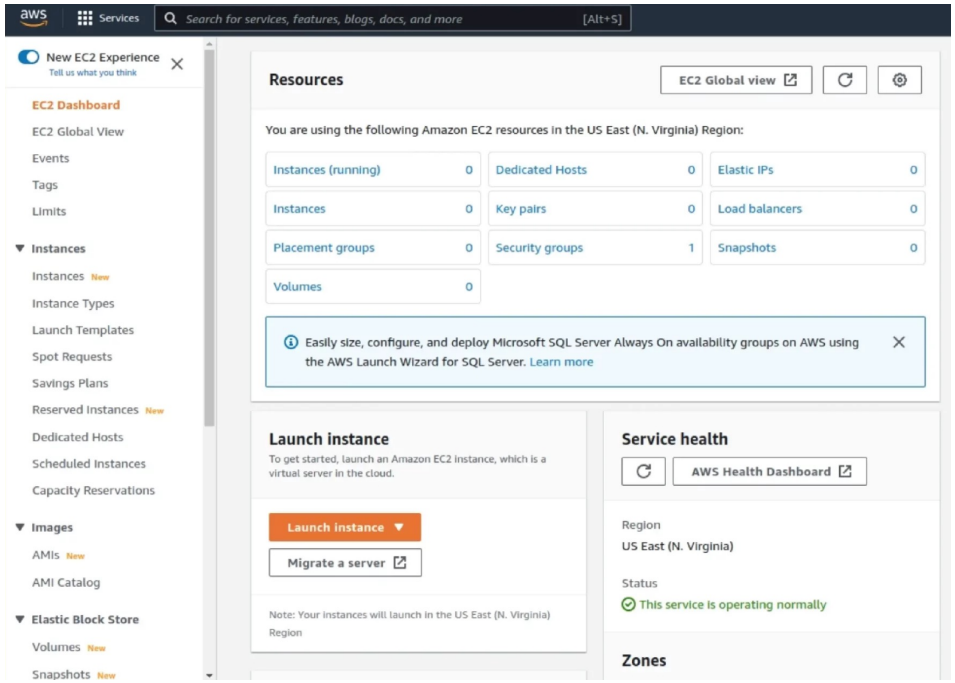
The directory also included a backup file for the Batik Air that is owned by Lion Air. Leaked records include passenger and reservation IDs, physical addresses, phone numbers, email addresses, names, dates of birth, phone numbers, passport numbers, and passport expiration dates.

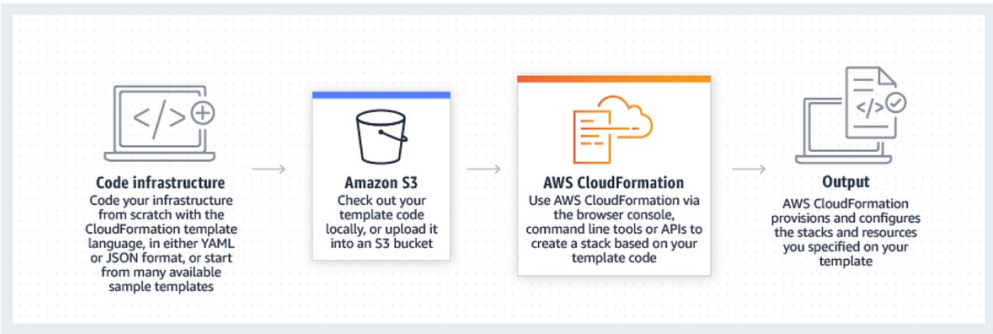
- **The Solution (CSPM):**
  - Automated tools (like Wiz, Orca, Prisma) that continuously scan your cloud account against best practices (CIS Benchmarks).
  - **Alert:** "You have a root account without MFA enabled."

Orca Security · Wiz · Prisma Cloud by Palo Alto Networks · CloudGuard Check Point · sysdig Secure · Lacework FortiCNAPP

- **The Risk:** Misconfiguration is the #1 cause of cloud breaches. (e.g., leaving a database password in a public field).

Infrastructure as Code (IaC) Security






```
Resources:
  #Let's take care of the VPC
  #https://docs.aws.amazon.com/AWSCloudFormation/
  VPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: '10.0.0.0/16'
      EnableDnsSupport: true
      EnableDnsHostnames: true
      InstanceTenancy: default
```

Security Benefit: You can scan the *code* for security flaws before the server is ever built. "Fixing it in the blueprint phase."

Old Way:

Clicking buttons in the AWS Console to launch a server. (Hard to repeat, hard to audit).

New Way:

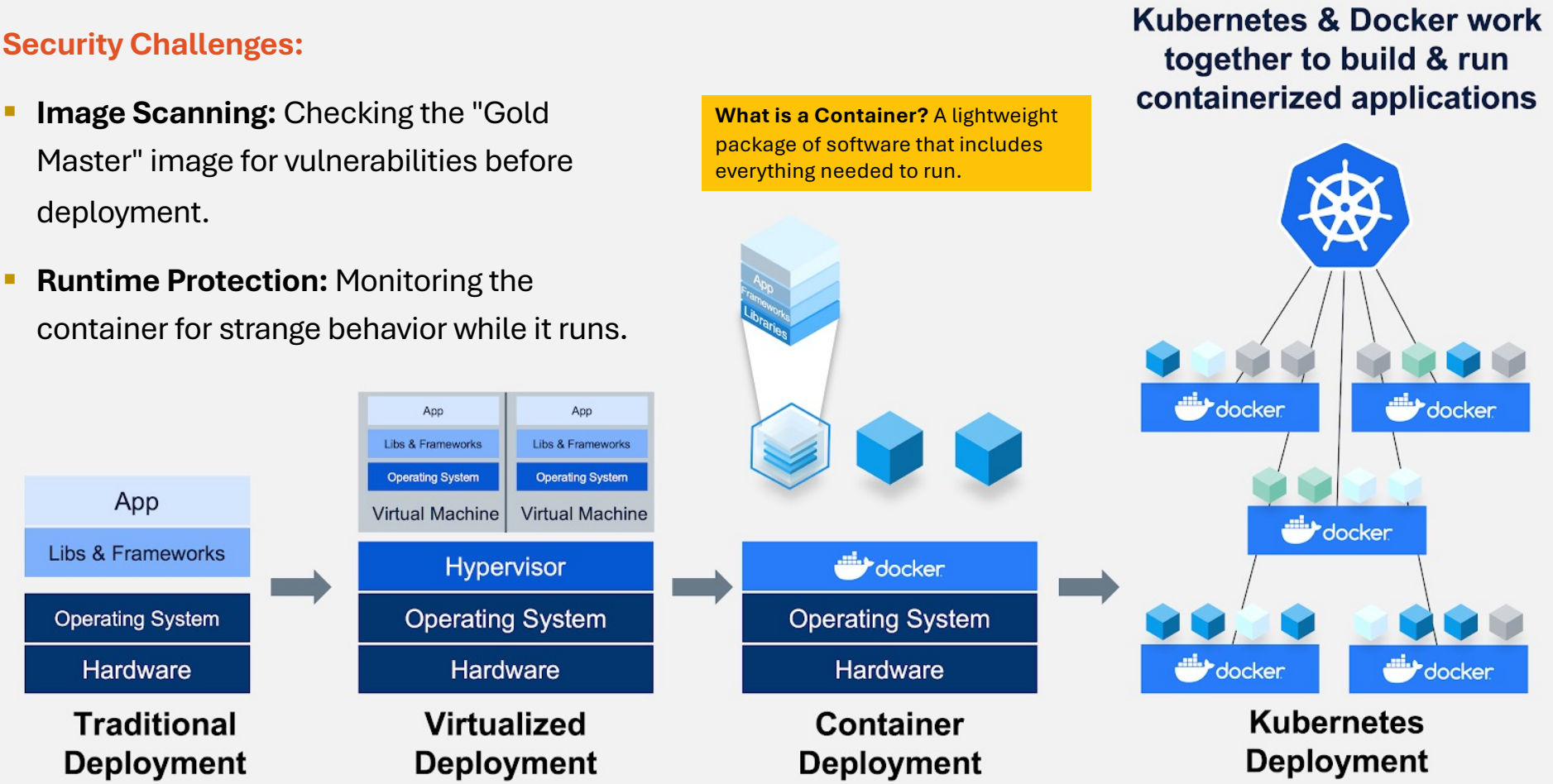
Writing code (Terraform, CloudFormation) to define the infrastructure.

Container Security (Docker & Kubernetes)

Security Challenges:

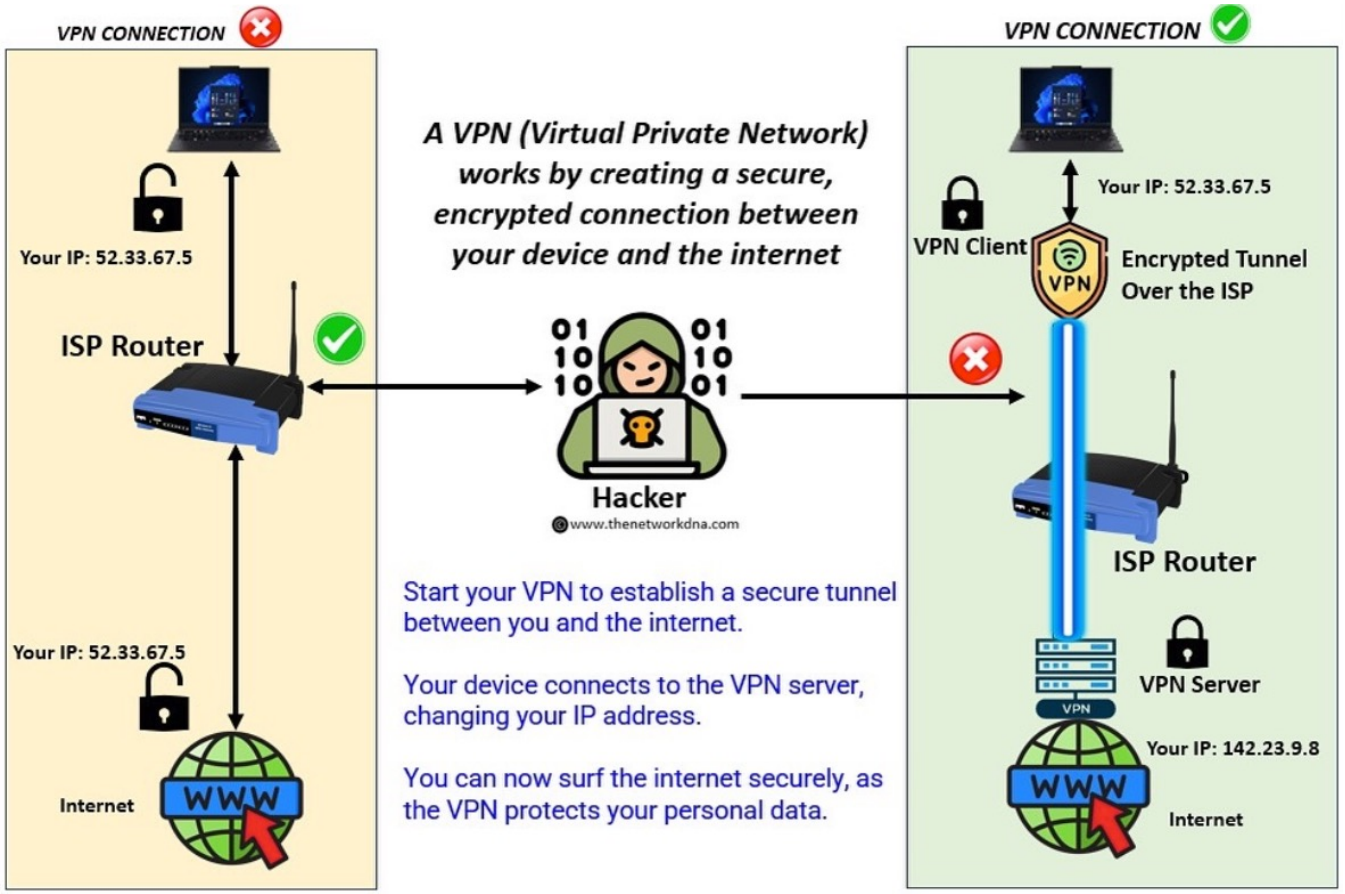
- **Image Scanning:** Checking the "Gold Master" image for vulnerabilities before deployment.
- **Runtime Protection:** Monitoring the container for strange behavior while it runs.

What is a Container? A lightweight package of software that includes everything needed to run.

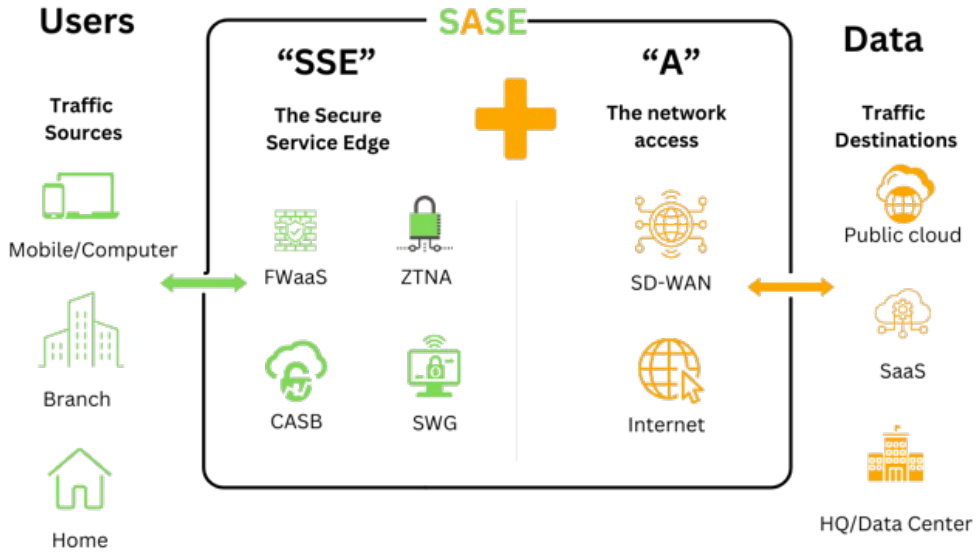


Secure Remote Access (VPN vs. SASE)

- **Legacy VPN:**
  - Tunneling a user into the corporate network.
  - **Risk:** Once connected, they often have broad access ("lateral movement").



Secure Remote Access (VPN vs. SASE)

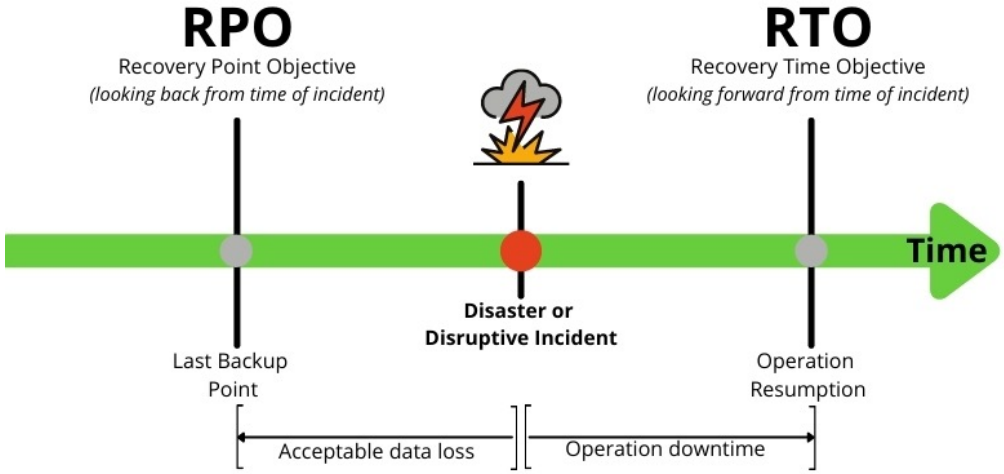


- **SASE (Secure Access Service Edge):**
  - A cloud-native approach.
  - The user connects to the SASE cloud, which applies security policies (SWG, CASB) before connecting them to the specific app they need.

Availability and Backups

- **Definition:** Backup vs. Availability
  - Availability ensures data is accessible;
  - Backup is a copy for recovery.
- **Why it Matters:** Protection against hardware failure, cyberattacks, accidental deletion, and natural disasters.
- **Goal:** Maintain business continuity and minimize data loss.

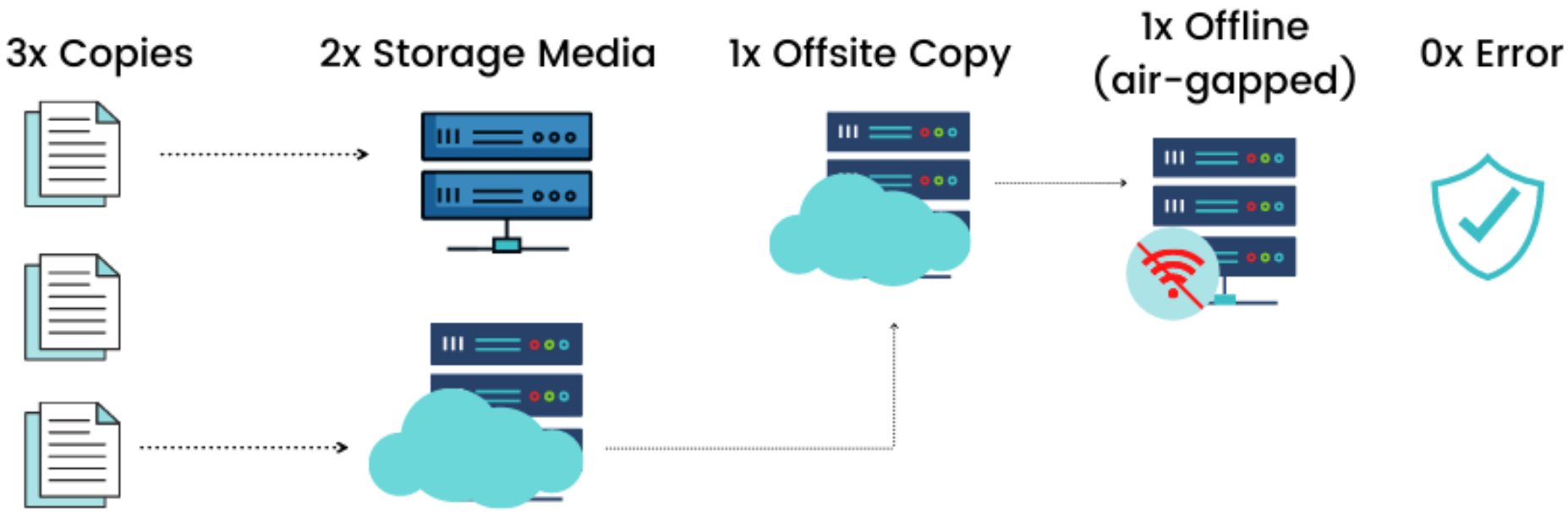
RPO (Recovery Point Objective): How much data can you afford to lose? (e.g., 1 hour, 1 day).



RTO (Recovery Time Objective): How long can you afford to be offline?

Availability and Backups

- **The 3-2-1 Backup Rule (Best Practice)**



3: Keep at least **three** copies of your data.

2: Store on **two** different types of media.

1: Keep **one** copy off-site (cloud or remote location).

Availability and Backups

- **Types of Backups**
  - **Full Backup:** Complete copy of all data (High storage space).
  - **Incremental Backup:** Only backs up data changed since the last backup (Lowest storage space).
  - **Differential Backup:** Backs up data changed since the last full backup (Moderate storage space).
  - **Hot vs. Cold:**
    Hot (system active) vs. Cold (system offline).

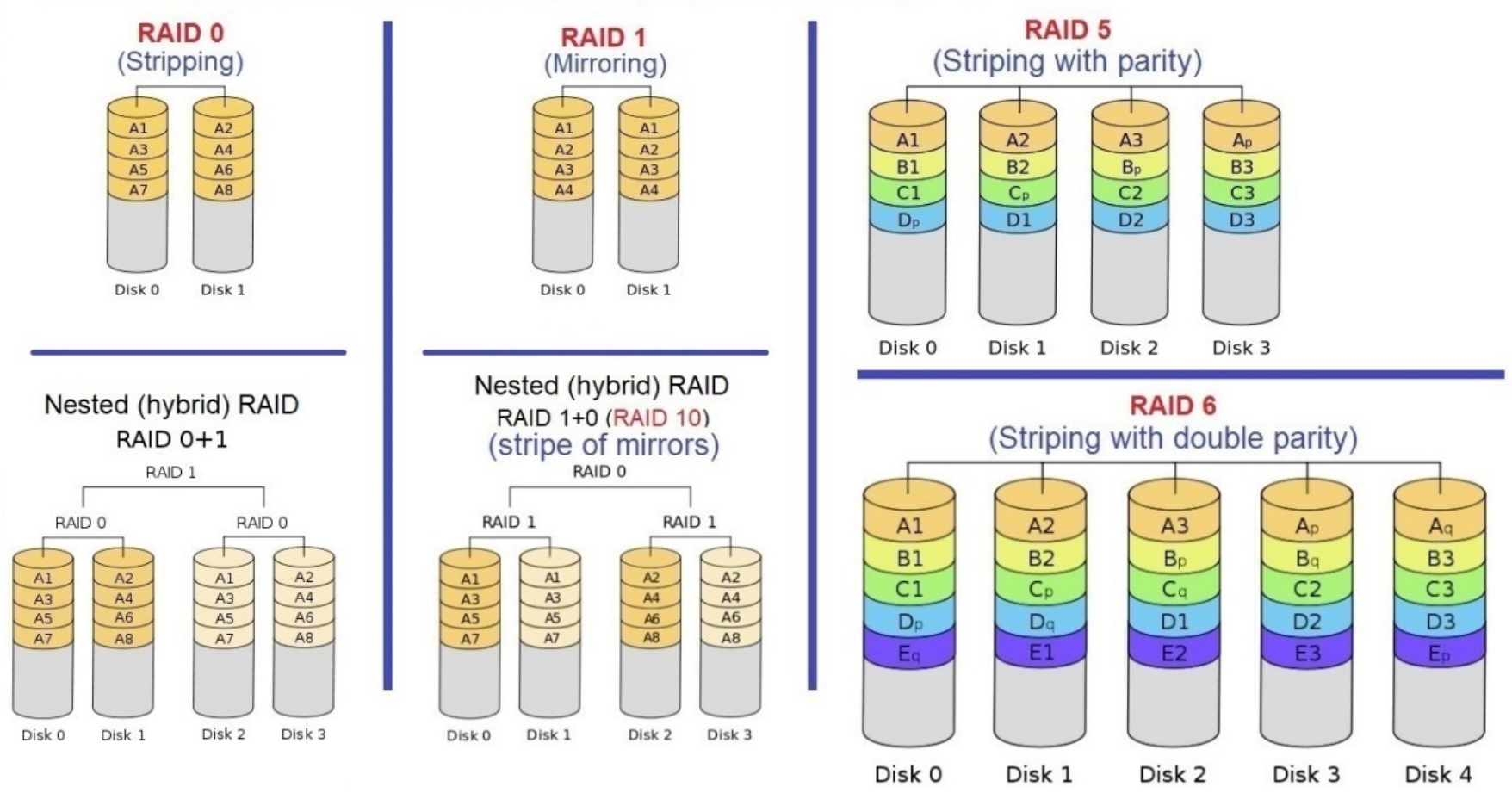
- **Storage Solutions**
  - **Local Storage** (NAS, USB drives).

  - **Cloud Storage** (Secure, scalable).

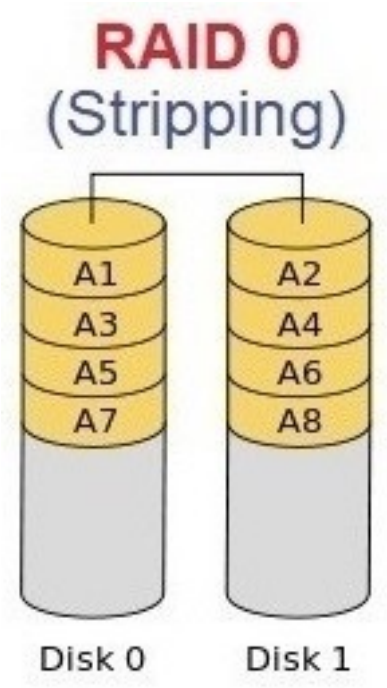
  - **Hybrid Solutions** (Local for speed, Cloud for security).

Availability and Backups

RAID (Redundant Array of Independent Disks)



Availability and Backups



- **RAID 0 (striping): High Performance**
  - **RAID 0** offers the fastest read/write speeds and maximum availability of raw storage capacity.
  - Although **RAID** is typically associated with data redundancy, **RAID 0** does not provide any. However, it does provide the best performance of any **RAID** level.
  - It achieves this by breaking up data into smaller Blocks and storing it on separate disks.
  - Min. Drives Required: **2**

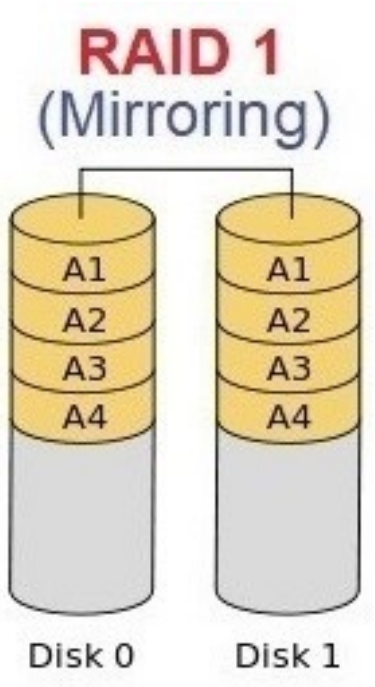
Advantages of RAID 0

- RAID 0 offers great performance, both in read and write operations.
- There is no overhead caused by parity controls.
- All storage capacity is used; there is no overhead.
- The technology is easy to implement.

Disadvantages of RAID 0

- RAID 0 is not fault-tolerant. If one drive fails, all data in the RAID 0 array are lost.
- It should not be used for mission-critical systems

Availability and Backups



- **RAID 1 (mirroring): Solid Data Protection**
  - **RAID 1** is an excellent option when data Protection and Redundancy is your primary goal.
  - This **RAID** type stores your data on one disk and then keeps a separate copy of that data on each of the available remaining disks.
  - This means that if one disk goes down, you still have your data ready to go.
  - Min. Drives Required: **2**

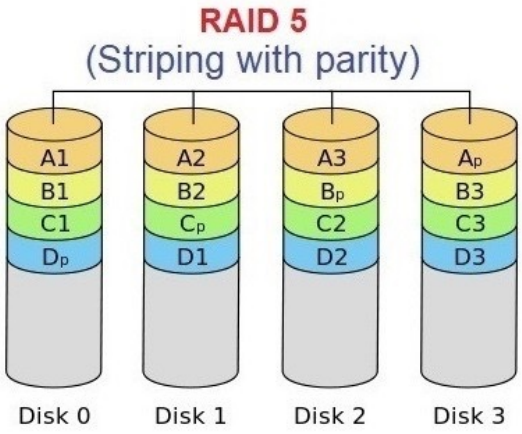
Advantages of RAID 1

- RAID 1 offers excellent read speed and a write-speed that is comparable to that of a single drive.
- In case a drive fails, data do not have to be "rebuild",
  they just have to be "copied" to the replacement drive.
- RAID 1 is a very simple technology.

Disadvantages of RAID 1

- The main disadvantage is that **the effective storage capacity is only half of the total drive capacity** because all data get written twice.
- Software RAID 1 solutions do not always allow a hot swap of a failed drive. That means the failed drive can only be replaced after powering down the computer it is attached to.
- For servers that are used simultaneously by many people, this may not be acceptable. Such systems typically use hardware controllers that do support hot swapping.

Availability and Backups



- **RAID 5 (Striping with Parity): Balanced Data Protection and Speed**
  - Requiring a **RAID** system of **three drives at least but** can work with up to **16 drives**. **RAID 5** offers the best of both worlds, balancing *Performance* and *Redundancy*.
  - It does this by splitting data into Blocks across all available drives and creating distributed **parity**, where data calculations are stored across the drives so that any one drive may fail, and the data — or parity — on the other drives can reconstitute what was lost on the failed drive.
  - Min. Drives Required: **3**

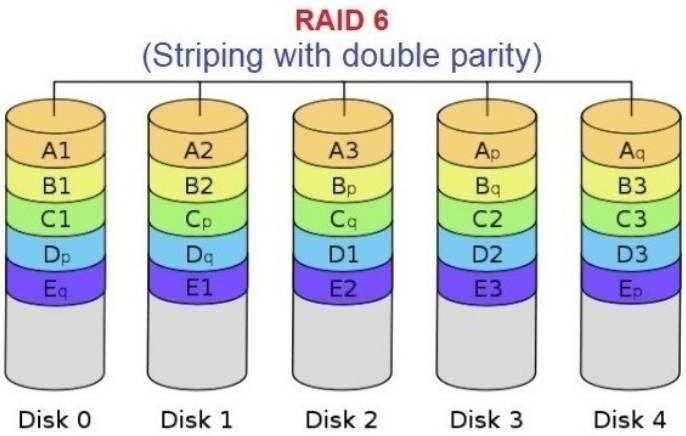
Advantages of RAID 5

- Read data transactions are very fast while write data transactions are somewhat slower (due to the parity that has to be calculated).
- If a drive fails, you still have access to all data, even while the failed drive is being replaced and the storage controller rebuilds the data on the new drive.

Disadvantages of RAID 5

- Drive failures have an effect on throughput, although this is still acceptable.
- This is complex technology. If one of the disks in an array using 4TB disks fails and is replaced, restoring the data (the rebuild time) may take a day or longer, depending on the load on the array and the speed of the controller. If another disk goes bad during that time, data are lost forever.

Availability and Backups

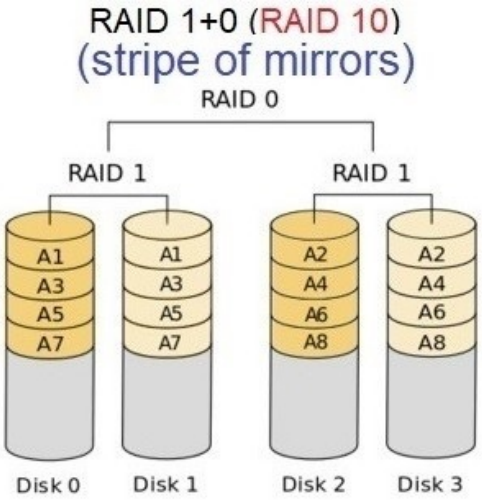


- **RAID 6 (Striping with Double Parity): Balanced Data Protection and Speed**
  - Like with **RAID 5**, read data transactions are very fast.
  - If two drives fail, you still have access to all data, even while the failed drives are being replaced. So, **RAID 6** is more secure than **RAID 5**.
  - Min. Drives Required: **4**

Disadvantages of RAID 5

- Write data transactions are slower than RAID 5 due to the additional parity data that have to be calculated. In one report I read the write performance was **20% lower**.
- Drive failures have an effect on throughput, although this is still acceptable.
- This is complex technology. Rebuilding an array in which one drive failed can take a long time.

Availability and Backups



- **RAID 10 (combining mirroring and striping): High Reliability and Performance**
  - **RAID 10** nests at least **two RAID 1** sets within a **RAID 0** configuration.
    This blends performance with potentially higher fault tolerance.
    Mirroring lends additional Redundancy, which means that you can retain your data *even if you lose up to half your disks* — provided your mirrored copy does not fail.
  - This is why businesses and other professional teams use **RAID 10** where uptime and availability are critical for intense workflows.
  - Min. Drives Required: **4**

Advantages of RAID 10

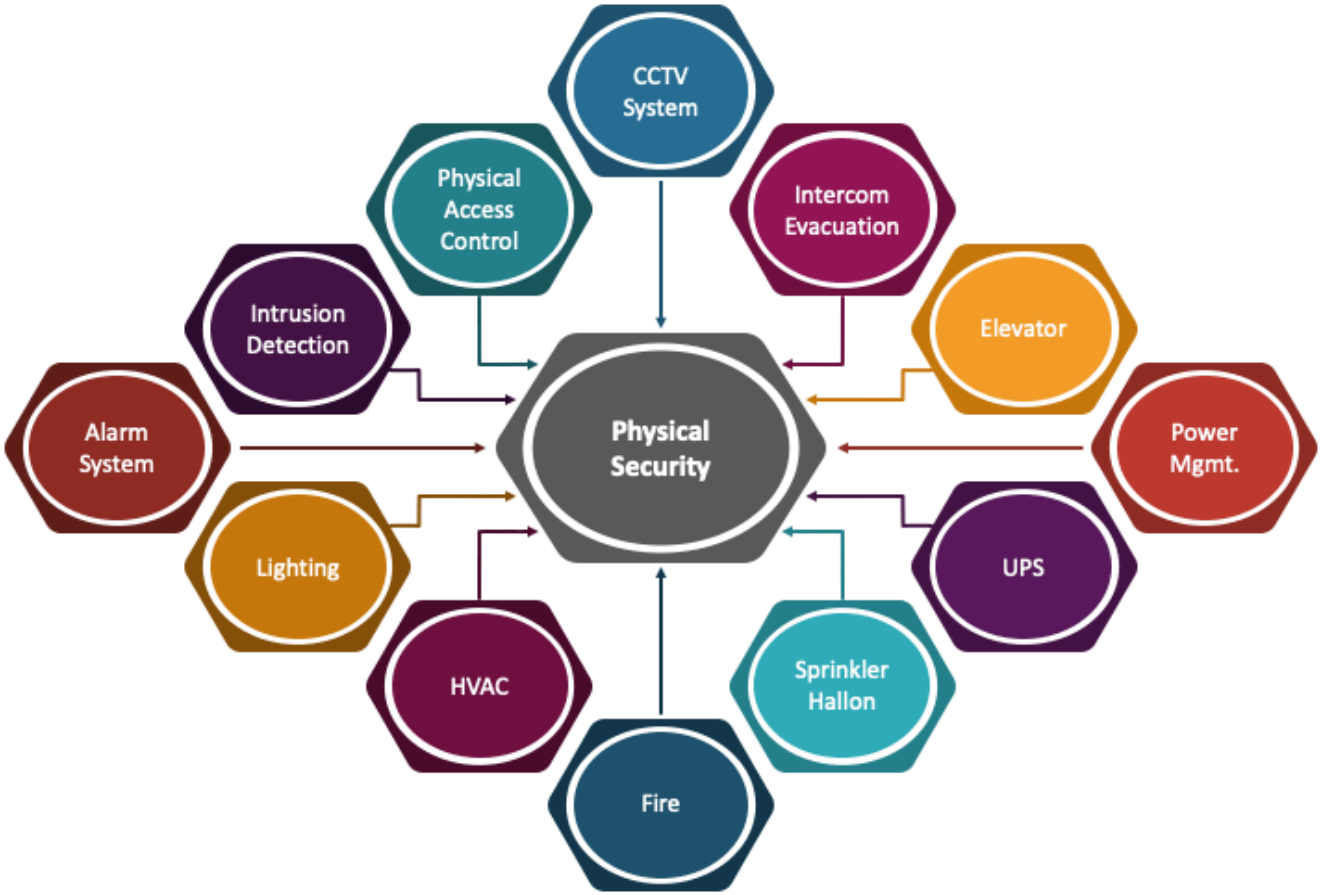
- If something goes wrong with one of the disks in a RAID 10 configuration, the Rebuild time is very fast since all that is needed is copying all the data from the surviving mirror to a new drive. This can take as little as 30 minutes for drives of 1 TB.

Disadvantages of RAID 5

- Half of the storage capacity goes to mirroring, so compared to large RAID 5 or RAID 6 arrays, this is an expensive way to have redundancy.

Physical Security

- **It Still Matters:** If I can steal the server, I own the data.
- **Controls:**
  - **Access Control:** Badges and Logs.
  - **Environmental:** Fire suppression (Gas, not water!), Humidity control, UPS (Battery backups).
- **The "Evil Maid" Attack:** If an attacker has physical access to a laptop for 5 minutes, they can compromise it via USB.

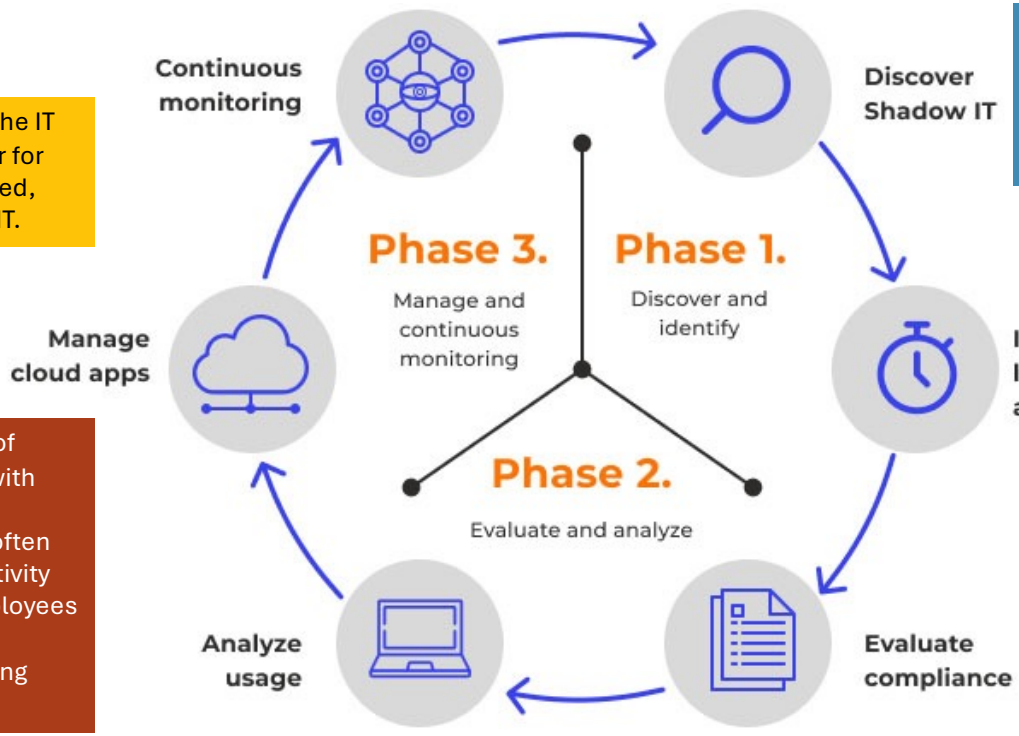


Physical Security - The 5 D's Framework

Shadow IT Strategy

- A comprehensive Shadow IT strategy focuses on **discovering**, **assessing**, and **managing**, **rather than merely prohibiting**, **unauthorized applications and hardware** to mitigate risks like data leaks and compliance breaches.

Proactive Procurement: Streamline the IT procurement process to make it faster for employees to obtain the tools they need, reducing the motivation to go around IT.



Visibility & Discovery: Utilize tools like CASBs, SaaS Management Platforms (SMPs), and network monitoring to identify unauthorized cloud services and devices, creating a "continuous signal" of new tools.

Risk Assessment & Management: Categorize unsanctioned applications based on their risk level (e.g., data security, compliance). Implement, in some cases, automated actions to block high-risk applications, while sanctioning or providing safer alternatives for others.

Collaboration & Education: Instead of simply prohibiting tools, collaborate with departments to understand the "why" behind their use of shadow IT, which often stems from a desire for better productivity or specific functionality. Educate employees on data security risks, such as using unapproved cloud storage or messaging apps for sensitive information.

Policy & Governance: Create clear, flexible policies that define acceptable use of technology. These policies should educate employees on the risks of Shadow IT while providing clear, fast pathways to request and approve new software.

End of the Lecture

Please do not hesitate to ask any questions to free your curiosity,

If you have any further questions after the class, please contact me via email (charnon@cmkl.ac.th).