SEC-202: Secure Start-Up

Lecture 2 – Identity and Endpoint Security

Instructed By:

Dr. Charnon Pattiyanon

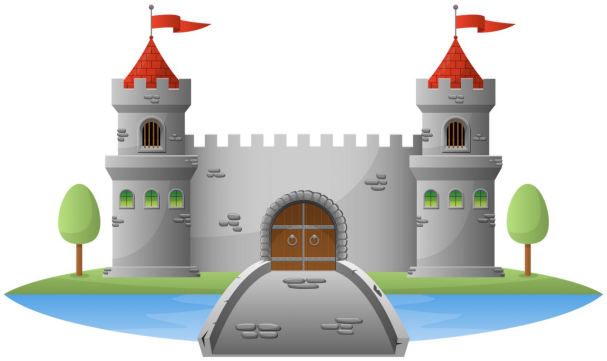
Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer Engineering (AICE) Program

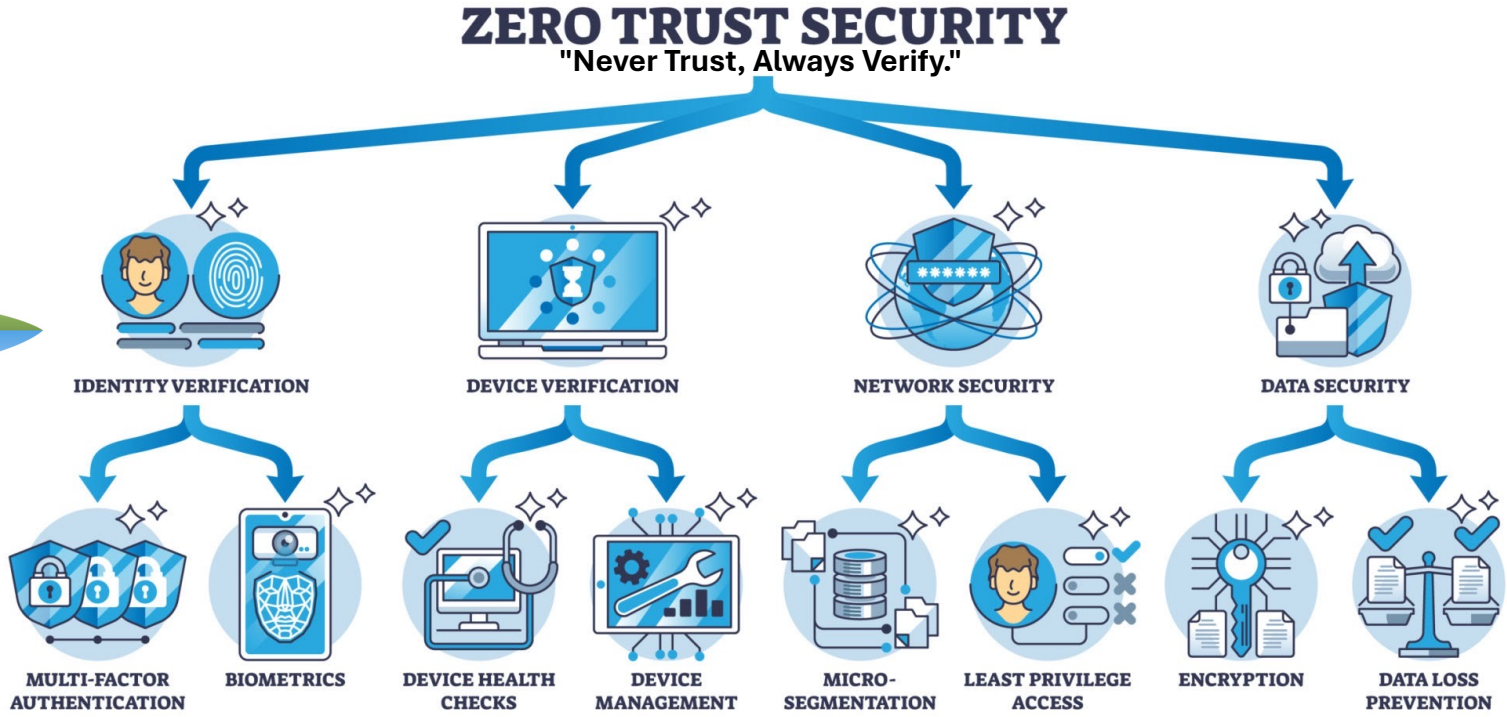
Class Agenda

- Identity is the New Perimeter (Zero Trust)
- Identity and Access Management Core Concepts
- The Password Problem
- Multi-Factor Authentication (MFA) Deep Dive
- Single Sign-On (SSO)
- The Principle of Least Privilege (PoLP)
- Endpoint Protection – EDR vs. Legacy Anti-Virus
- Mobile Device Management (MDM) and Browser Security
- Secrets Management and Offboarding

Identity is the New Perimeter (Zero Trust)



- **The "Castle & Moat" is Dead:**
  - Traditional security relied on a firewall (the moat) to protect the office (the castle).
  - **Problem:** If an attacker gets inside the castle (phishing), they can move freely. Also, users are now working from coffee shops and homes, outside the castle walls.



We don't trust you just because you are on the office Wi-Fi. We verify every request based on:

Identity: Who are you?

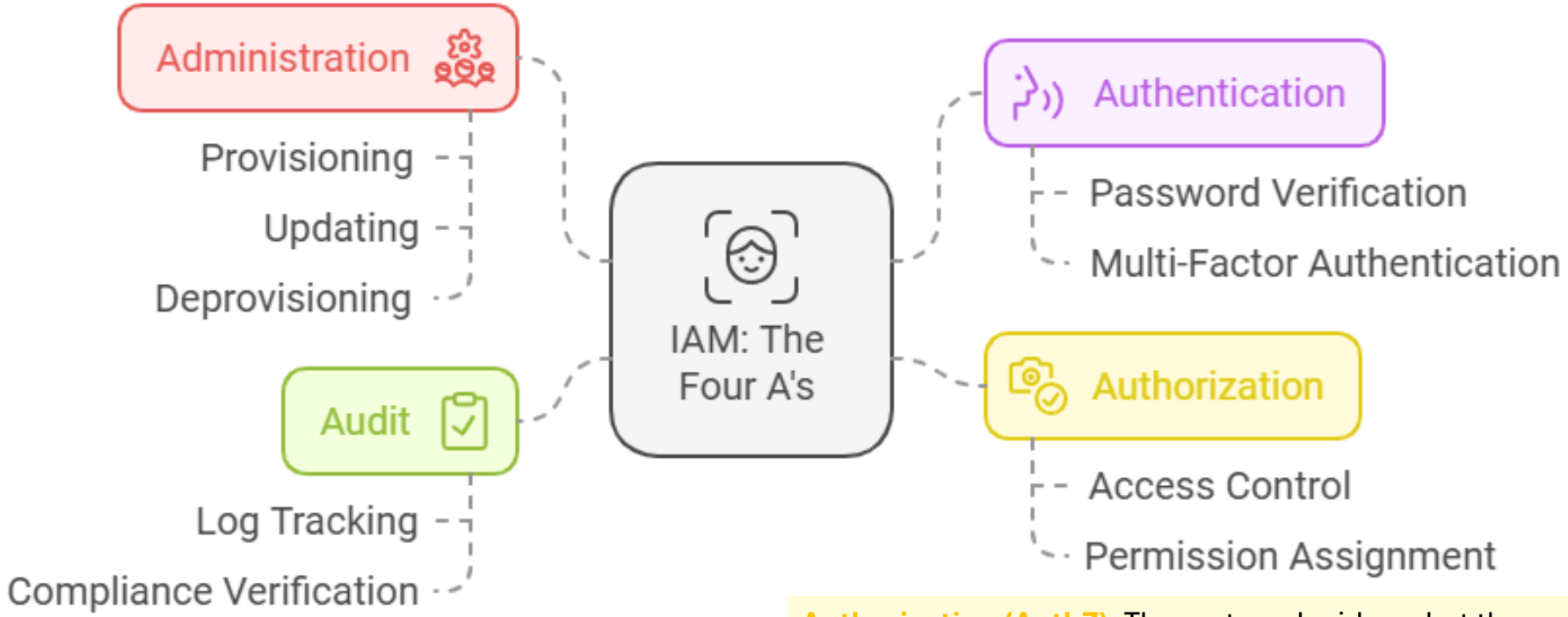
Device Health: Is your laptop patched?

Context: Are you logging in from an unusual location?

Identity and Access Management – Core Concepts

Identification: The user claims an identity (e.g., typing `user@company.com`).

Authentication (AuthN): The user proves they are who they say they are (e.g., Password, FaceID).



Accounting: The system logs the activity for future audits.

Authorization (AuthZ): The system decides what the user is allowed to do (e.g., Read-Only access vs. Admin access).

Identification & Authentication

The Password Problem

- **Why Humans Fail:**
  - We crave convenience. We choose "Password123" or "Summer2024!".
  - **Reuse:** We use the same password for Netflix and our Bank.

- **Credential Stuffing:**
  - Attackers take a leaked database from a low-security site (e.g., a fitness forum) and try those same email/ password combos on high-value targets (e.g., Corporate Email).

- **Modern Password Policy (NIST Guidelines):**
  - **Do:** Use long passphrases (e.g., `Correct-Horse-Battery-Staple`).
  - **Don't:** Force rotation every 90 days (it makes people choose weaker passwords).
  - **Don't:** Rely on complexity rules (e.g., Pa$$w0rd is easy to guess but "complex").

Multi-Factor Authentication (MFA) Deep Dive

Something You Know
(Password, PIN, ...)

Something You Have
(Keys, Badges, Tokens, Cards, ...)

Something You Are
(Biometric, Retina Patterns, ...)

Something You Do
(Handwriting, ...)

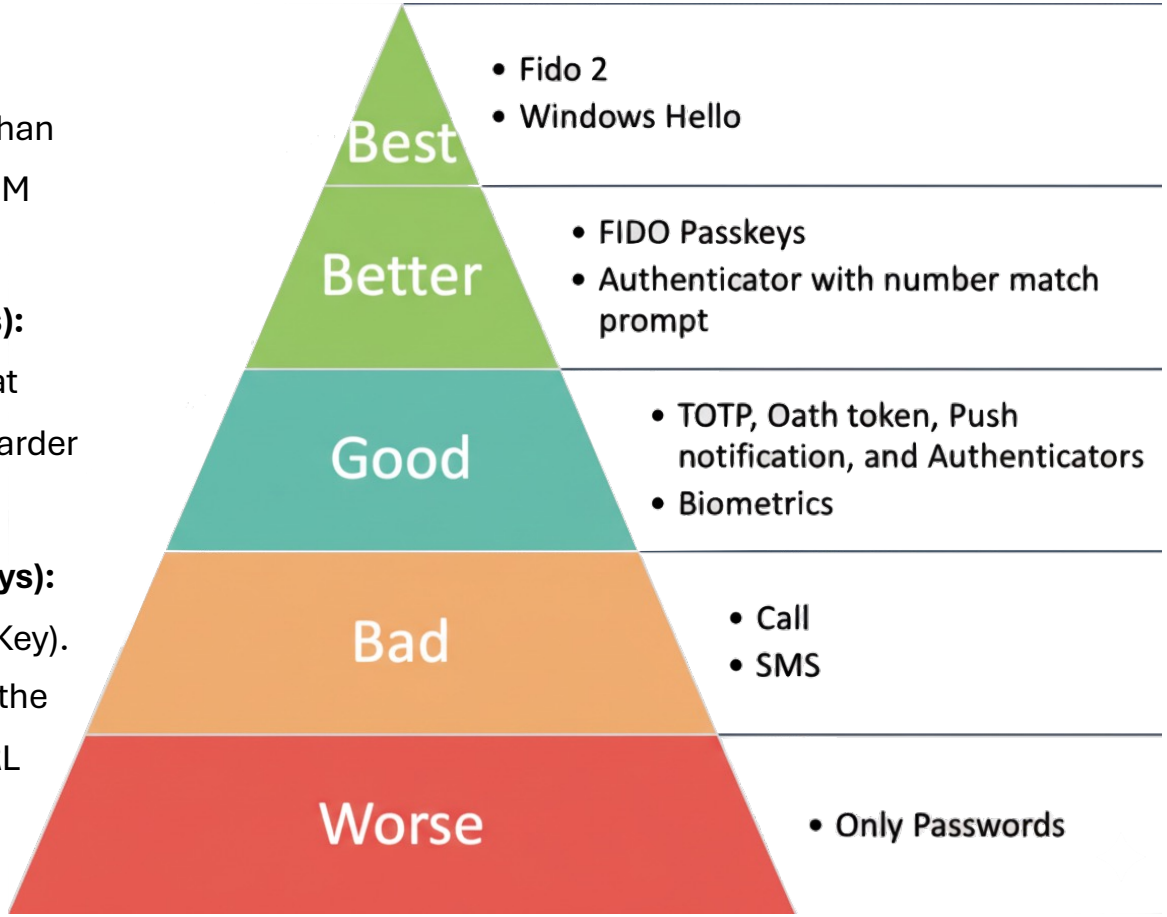
Where You Are

Where you are?

- ❑ does not verify identity, ***unless only one person can enter that location.***
- ❑ could ***reduce*** the number of possible identities.
- ❑ but should rather be thought of as ***access restriction***, than an authentication mechanism

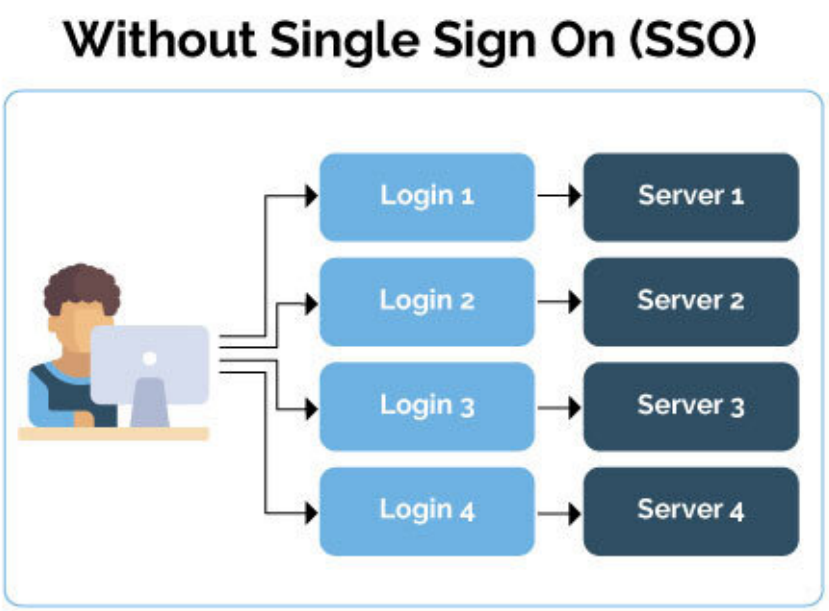
Multi-Factor Authentication (MFA) Deep Dive

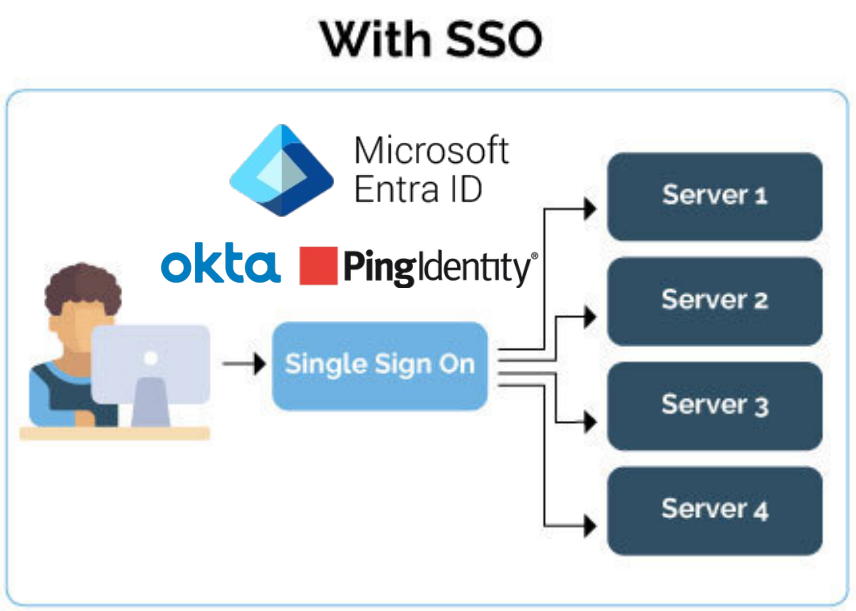
- **MFA Hierarchy of Safety:**
  - **Good (SMS/Email):** Better than nothing, but vulnerable to SIM Swapping and interception.
  - **Better (Authenticator Apps):** Generates a code (TOTP) that rotates every 30 seconds. Harder to hack.
  - **Best (FIDO2 / Hardware Keys):** Physical USB keys (like YubiKey). Phishing-resistant because the key verifies the website's URL before unlocking.



Single Sign-On (SSO)

The Concept of SSO: One "Master Key" (Identity Provider) unlocks all doors (SaaS Apps).

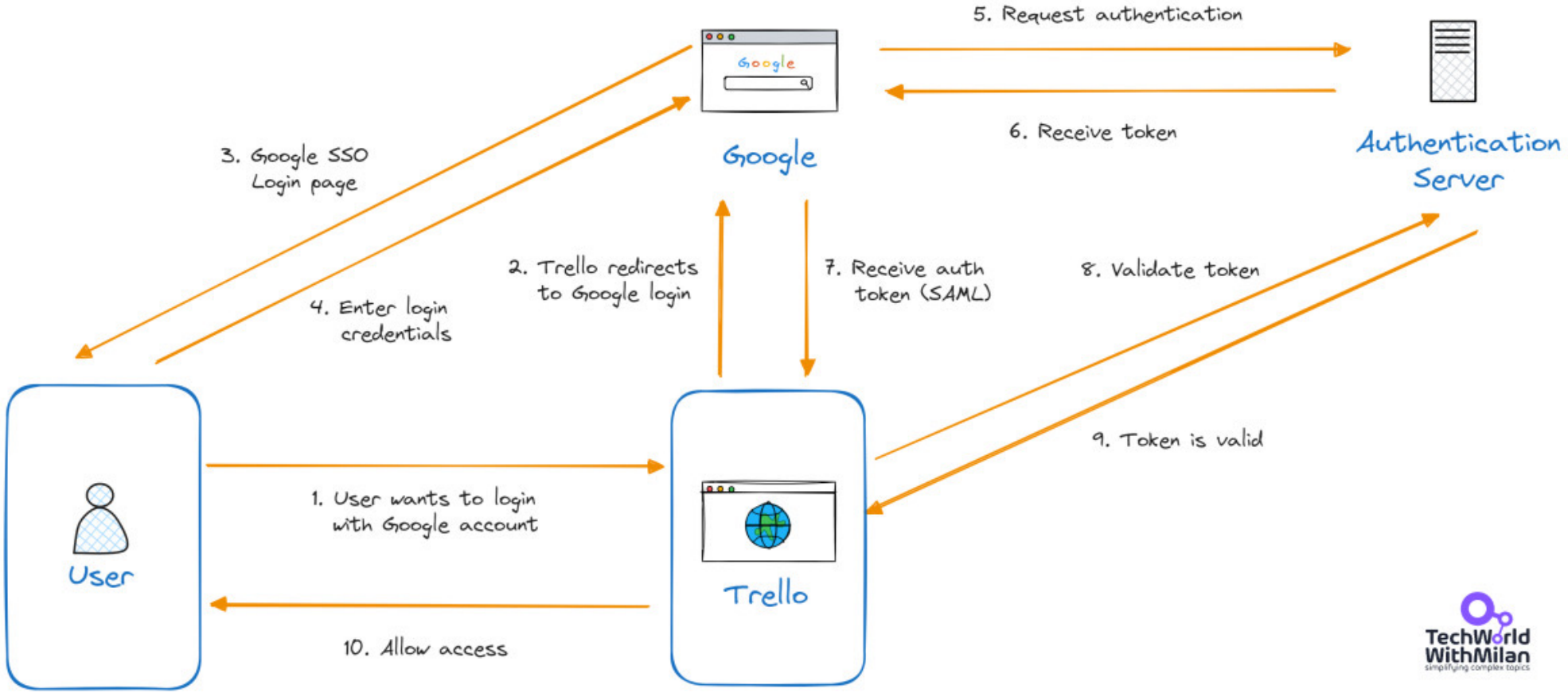


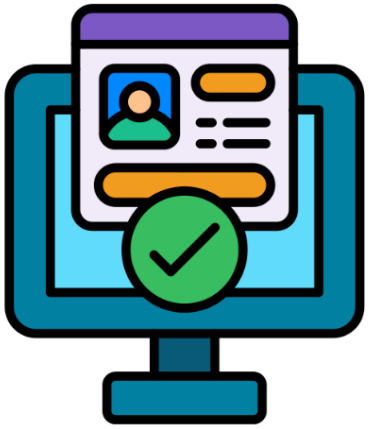


- **Benefits:**
  - **User Experience:** Log in once, access everything.
  - **Security:** IT has a single "Kill Switch." If an employee leaves, disabling their Okta account instantly locks them out of Slack, Salesforce, Zoom, and Email.

- **Risks:** It is a Single Point of Failure. If the SSO admin account is breached, the attacker owns the company.

Single Sign-On (SSO) – How Does It Work?





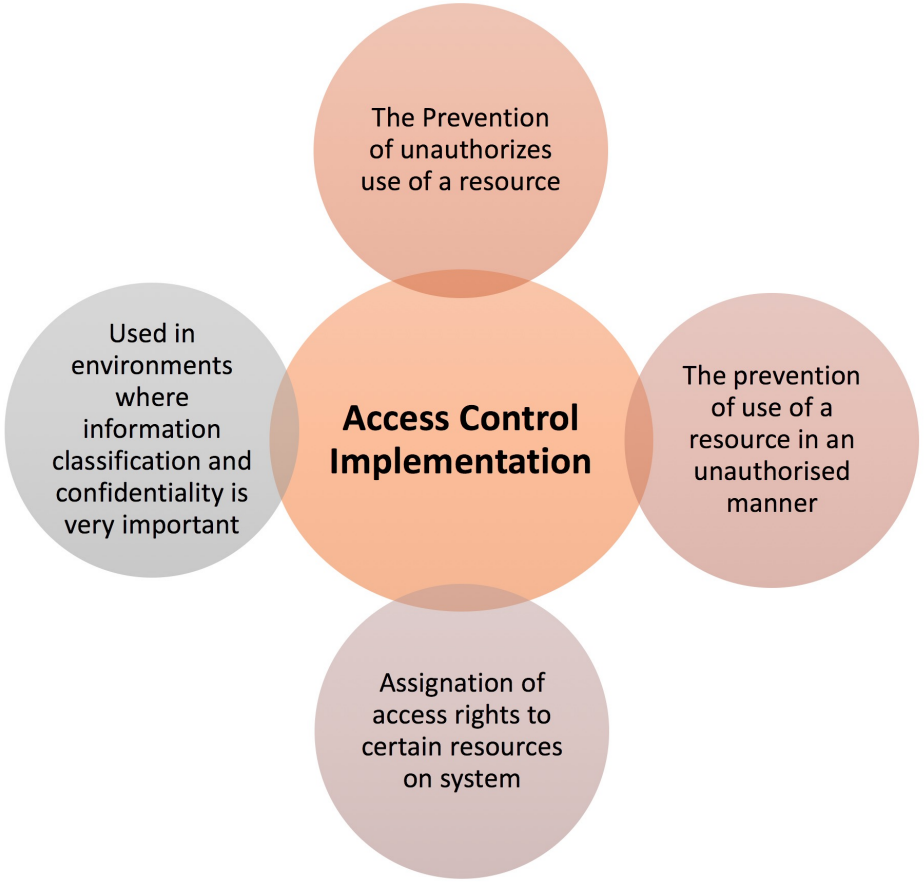
Authorization & Access Control

The Principle of Least Privilege (PoLP)

- **Definition:** A user, program, or process should have only the bare minimum privileges necessary to perform its function.
- **Standard vs. Admin:**
  - Day-to-day work (email, browsing) should never be done as a Local Administrator.
  - Why? If you click a malicious link as an Admin, the malware gets Admin rights too.
- **Just-In-Time (JIT) Access:**
  - Instead of giving someone "Permanent Admin" rights, give them "Admin for 2 hours" to fix a specific issue, then automatically revoke it.

Access Control

- Access control is the heart of security.
- **Definitions:**
  - The ability to allow only authorized users, programs, or processes to access resources.
  - The granting or denying, according to a particular security model, of certain permissions to access a resource.
  - An entire set of procedures performed by hardware, software, and administrators, to monitor access, identify users requesting access, record access attempts, and grand or deny access based on pre-established rules.



Access Control Tools and Methods

- **Access Control Matrix**
  - An access control matrix is a matrix ($M_{S,O}$) whose rows are subjects and columns are object.

    An element $m_{s_i,o_j} \in M_{S,O} \subseteq P$ is the set of permissions that a subject $s_i \in S$ is authorized to access an object $o_j \in O$.
  - Disadvantages: In a large system, the matrix will be enormous in size and mostly sparse.

	O_1	O_2	O_3	O_4	O_5	O_6
S_1	Y	Y	Y	Y	Y	N
S_2	N	N	Y	N	Y	N
S_3	N	N	N	N	N	Y

Access Control Tools and Methods

- **Access Control Matrix**
  - An access control matrix is a matrix ($M_{S,O}$) whose rows are subjects and columns are objects.
  - **Let's try this together:**
    - Suppose the private key file for S_1 is object O_1, i.e., only S_1 can read,
    - Suppose the public key file for S_1 is object O_2, i.e., all subjects can read, and only S_1 can write.
    - Suppose all subjects can read and write object O_3.
    - ***What is the access control matrix?***

	O_1	O_2	O_3
S_1	?	?	?
S_2	?	?	?
S_3	?	?	?

Access Control Tools and Methods

- **Access Control Matrix**
  - An access control matrix is a matrix ($M_{S,O}$) whose rows are subjects and columns are objects.
  - **Let's try this together:**
    - Suppose the private key file for S_1 is object O_1, i.e., only S_1 can read,
    - Suppose the public key file for S_1 is object O_2, i.e., all subjects can read, and only S_1 can write.
    - Suppose all subjects can read and write object O_3.
    - ***What is the access control matrix?***

	O_1	O_2	O_3
S_1	R	RW	RW
S_2	-	R	RW
S_3	-	R	RW

Access Control Tools and Methods

- **Access Control Matrix:**
  - **Secrecy:** Does this protection state ensure secrecy of S_1's private key in O_1?
  - **Integrity:** Does this access control matrix ensure the integrity of S_1's public key in O_2?
  - **Trust Processes:** Does it matter if we don't trust some of S_1's processes?

	O_1	O_2	O_3
S_1	R	RW	RW
S_2	-	R	RW
S_3	-	R	RW

	O_1	O_2	O_3
S_1	R	RW	-
S_2	-	R	RW
S_3	-	R	RW

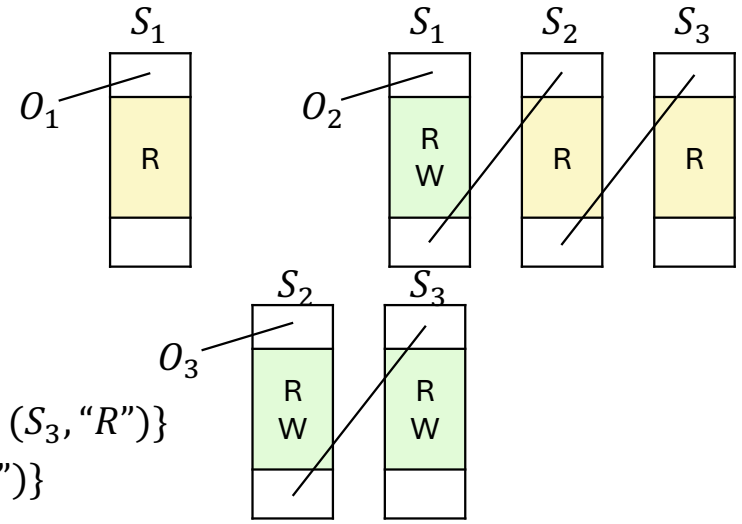
- Non-malicious process should not leak the private key by writing it to O_3.
- A potentially malicious process may contain a **Trojan horse** that can write the private key to O_3.

- **Least Privilege** – Limit permissions to those required only.
- For instance, restrict privilege of the subject S_1 to prevent leaks.

Access Control Tools and Methods

- **Access Control List**
  - An access control list is a set $\{A_o | o \in O\}$, i.e., one element of **object**. The elements of the list are the pair (s, p) of **subject** s who has **permission** p to that object.

	O_1	O_2	O_3
S_1	R	RW	-
S_2	-	R	RW
S_3	-	R	RW

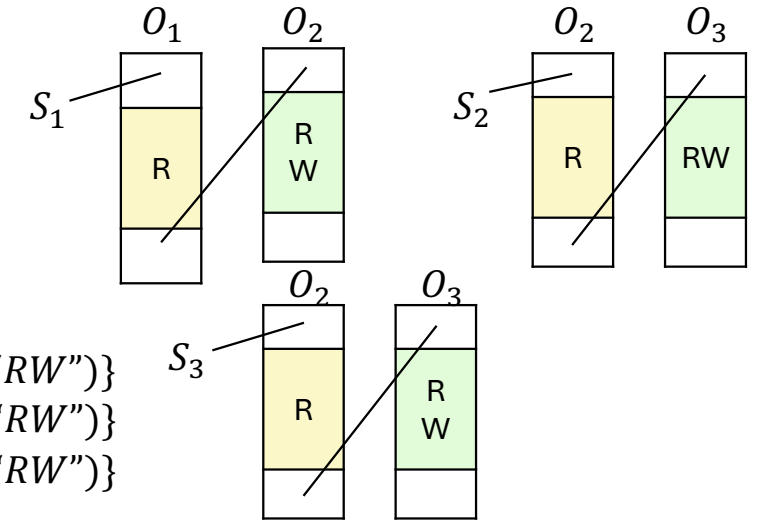


$$A_{O_1} = \{(S_1, "R")\}$$
$$A_{O_2} = \{(S_1, "RW"), (S_2, "R"), (S_3, "R")\}$$
$$A_{O_3} = \{(S_2, "RW"), (S_3, "RW")\}$$

Access Control Tools and Methods

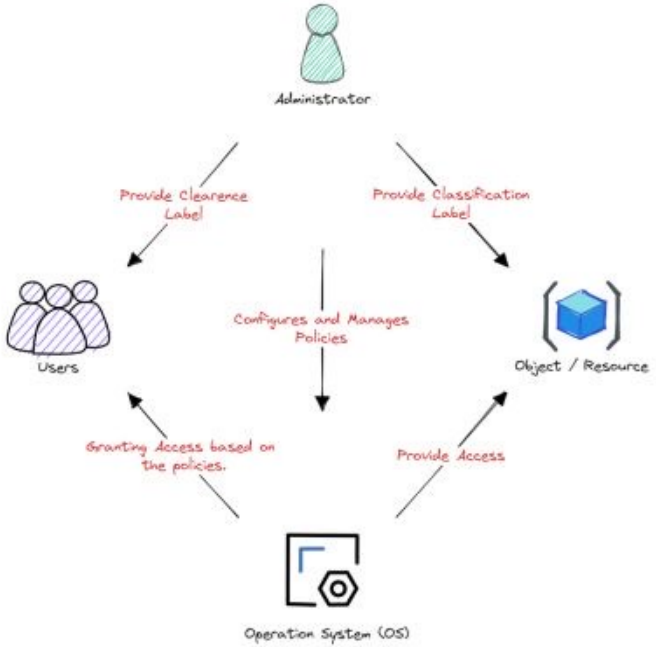
- **Capability List**
  - A capability list is a set $\{A_s \mid s \in S\}$, i.e., one element of **subject**. A capability can be thought of as a pair (o, p) where o is the name of an **object** and p is a set of **permissions**.

	O_1	O_2	O_3
S_1	R	RW	-
S_2	-	R	RW
S_3	-	R	RW



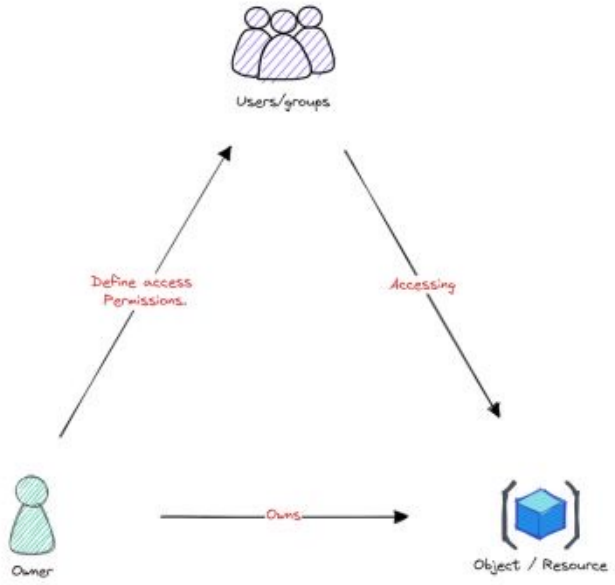
$$A_{S_1} = \{(O_1, "R"), (O_2, "RW")\}$$
$$A_{S_2} = \{(O_2, "R"), (O_3, "RW")\}$$
$$A_{S_3} = \{(O_2, "R"), (O_3, "RW")\}$$

Access Control Policy Models



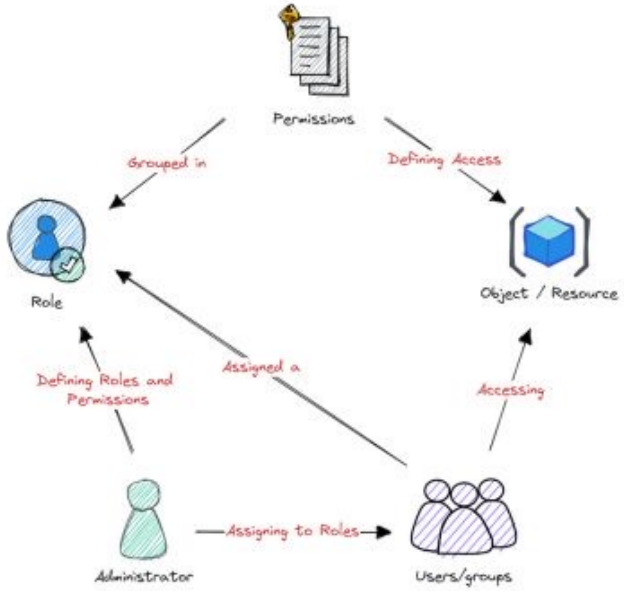
Mandatory Access Control (MAC)

- MAC is a model where access to resources is controlled by the system and is based on predefined security rules.
- MAC has a centralized control structure, with a single entity responsible for setting and enforcing access rules.
- MAC has limited flexibility, as access rules are set by the system and cannot be modified by users.
- MAC typically has a higher overhead, as the system must enforce access rules and ensure they are not violated.



Discretionary Access Control (DAC)

- DAC is a model where access to resources is controlled by the owner of the resource, who assigns permissions to users.
- DAC has a decentralized control structure, with individual resource owners responsible for setting and enforcing access rules.
- DAC offers more flexibility, as resource owners can assign permissions based on their own discretion.
- DAC has lower overhead, as the burden of setting and enforcing access rules falls on resource owners.



Role-Based Access Control (RBAC)

- RBAC is a model where access to resources is determined by the role an individual holds within an organization.
- RBAC can have either a centralized or decentralized control structure, depending on the organization's security needs.
- RBAC offers the most flexibility, as access rights can be assigned and modified based on the roles and responsibilities within an organization.
- RBAC overhead depends on the level of centralization, with centralized systems having higher overhead and decentralized systems having lower overhead.

Endpoint Security

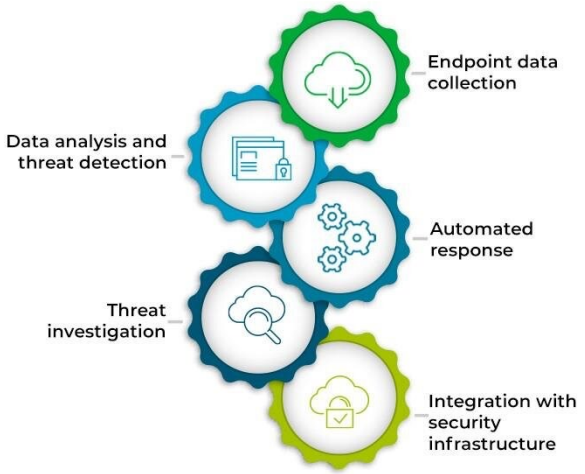
Endpoint Detection & Response, Antivirus, Mobile Device Management,

Browser Security, Secrets Management, Off-boarding Processes

Legacy Antivirus vs. Endpoint Detection and Response (EDR)

McAfee™ · KASPERSKY SECURITY · Avira · eset · Avast · Norton by Symantec

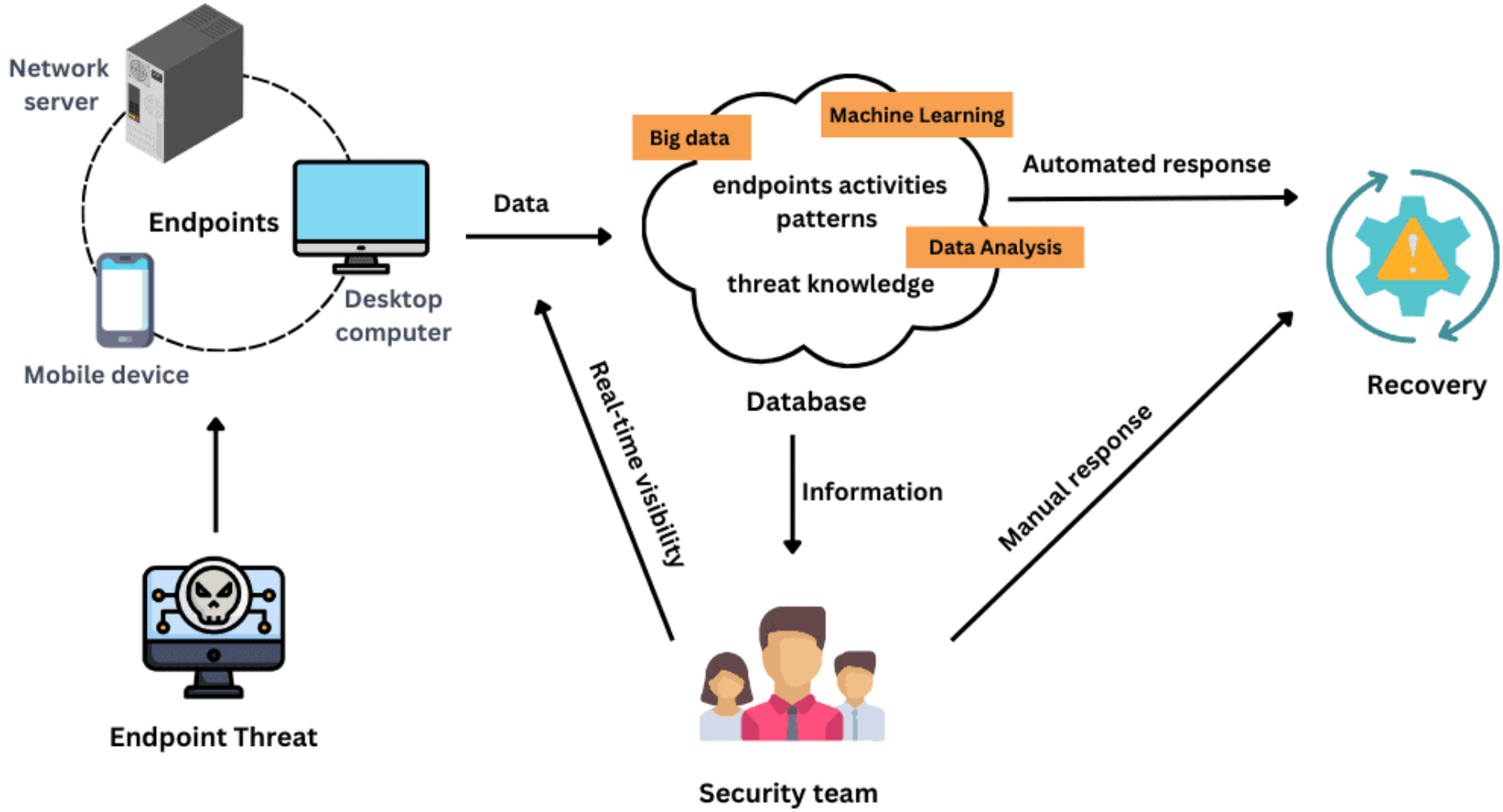
- **Legacy Antivirus**
  - Works like a "**Wanted Poster**" (Signatures).
  - It scans files against a list of known bad viruses.
  - **Fail:** It cannot stop new (zero-day) viruses or attacks that don't use files (fileless malware).



cisco SECURE · paloalto NETWORKS · SentinelOne™ · FORTINET · CROWDSTRIKE

- **Endpoint Detection and Response (EDR)**
  - Works like a "**CCTV Camera**" (Behavioral).
  - It watches what programs do.
  - **Example:** If Microsoft Word tries to open PowerShell and download a file, EDR blocks it because that is suspicious behavior, even if the file itself looks clean.

How Does Endpoint Detection and Response Work?



Mobile Device Management (MDM)

- **The BYOD (Bring Your Own Device) Challenge:**
  - Employees want to use their personal iPhones for work email.
  - **Risk:** What happens if they lose the phone or leave the company?
- **The Solution (MDM):**
  - **Containerization:** Creates a "walled garden" (Work Profile) on the phone. Personal apps (Photos, WhatsApp) cannot touch Work apps (Outlook, Teams).
  - **Remote Wipe:** IT can delete the "Work Profile" without deleting the user's personal photos.

How Does Mobile Device Management (MDM) Work

Microsoft Intune

Features and benefits

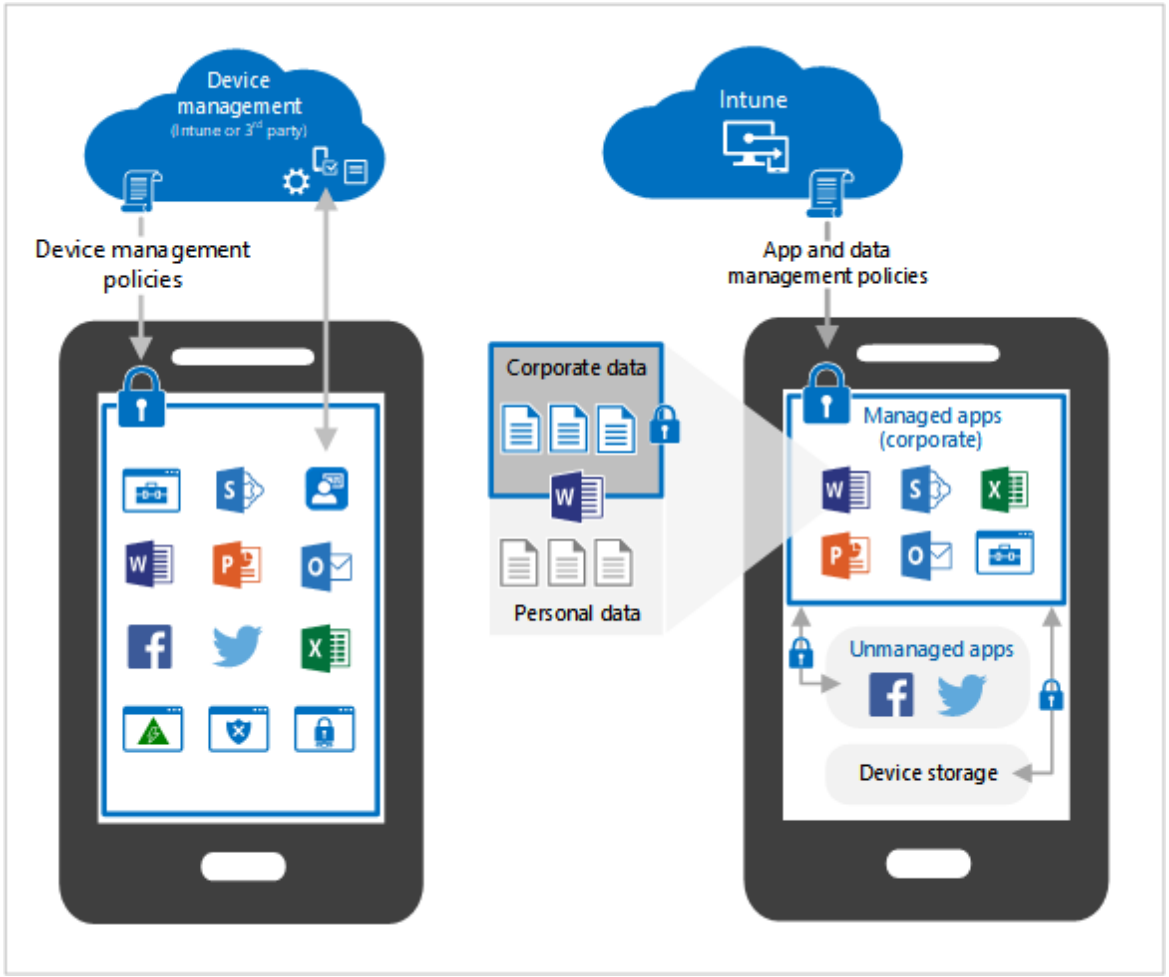
- Manage devices from a central console
- Deploy and update software
- Configure settings
- Enforce policies
- Monitor with data and reports
- Remote administration
- Maintain networks of common OS
- Optimize devices for business use
- Automate policy management
- Cloud-attach on-prem Configuration Manager

Mobile Device Management

- Enroll user devices
- Push apps on devices
- Restrict devices to a specific OS
- Block personal devices
- Remove data from lost or stolen devices
- Security and protection

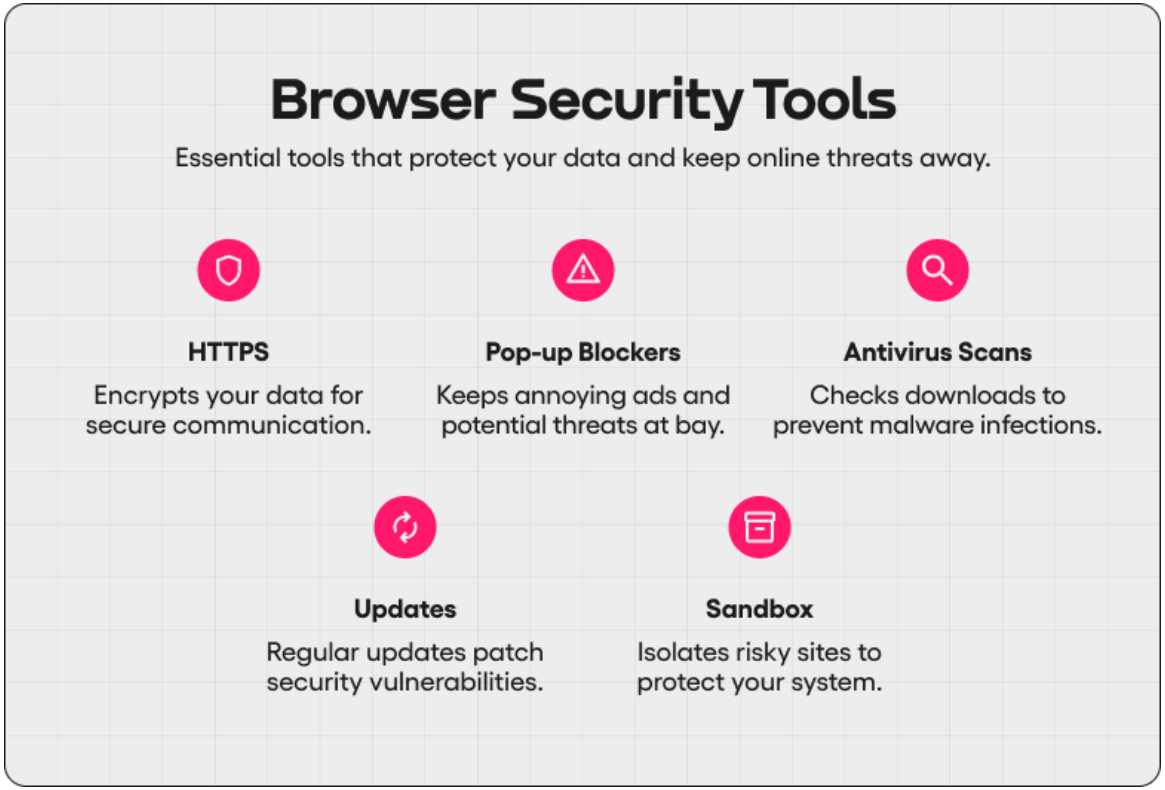
Mobile Application Management

- Allow personal devices to access org resources
- Prompt users to authenticate
- Remove data from lost or stolen devices
- Security and protection



Browsers Security

- **The Browser is the New OS:** Most employees spend **90%** of their day in Chrome or Edge.
- **Attack Vectors:**
  - **Malicious Extensions:** Free PDF converters that secretly read your email.
  - **Drive-by Downloads:** Malware that downloads just by visiting a site.
- **Controls:**
  - Enforcing "Managed Browsers" where IT controls which extensions are allowed.
  - Disabling "Save Password" in the browser (forcing use of a Password Manager).

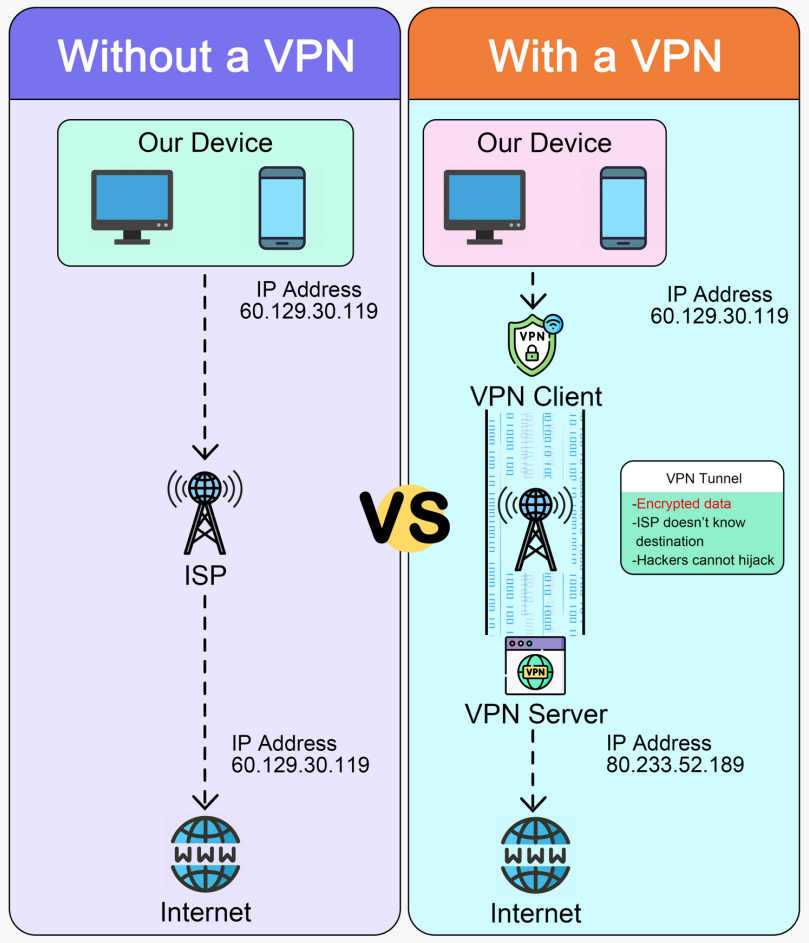


Browsers Security – How Does It Work?

6 Browser Security Best Practices

Advanced Techniques and Tools for Browsers Security/Privacy

- A **virtual private network**, or **VPN**, is an encrypted connection over the internet from a device to a network. It prevents unauthorized people from eavesdropping on traffic and ensures that sensitive personal or professional data is safely transmitted over the internet.
- This can be specifically helpful while accessing websites that monitor user behavior or avoiding targeted ads based on browsing history.
- Besides, a VPN can protect against cyber threats on unsecured public Wi-Fi networks. It masks the user's IP address, ensuring safer and more private browsing.

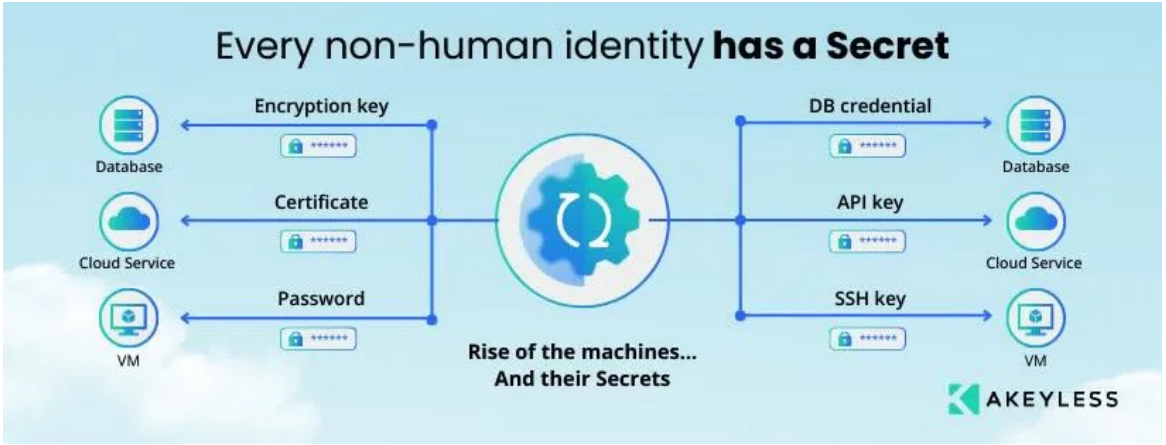


Advanced Techniques and Tools for Browsers Security/Privacy

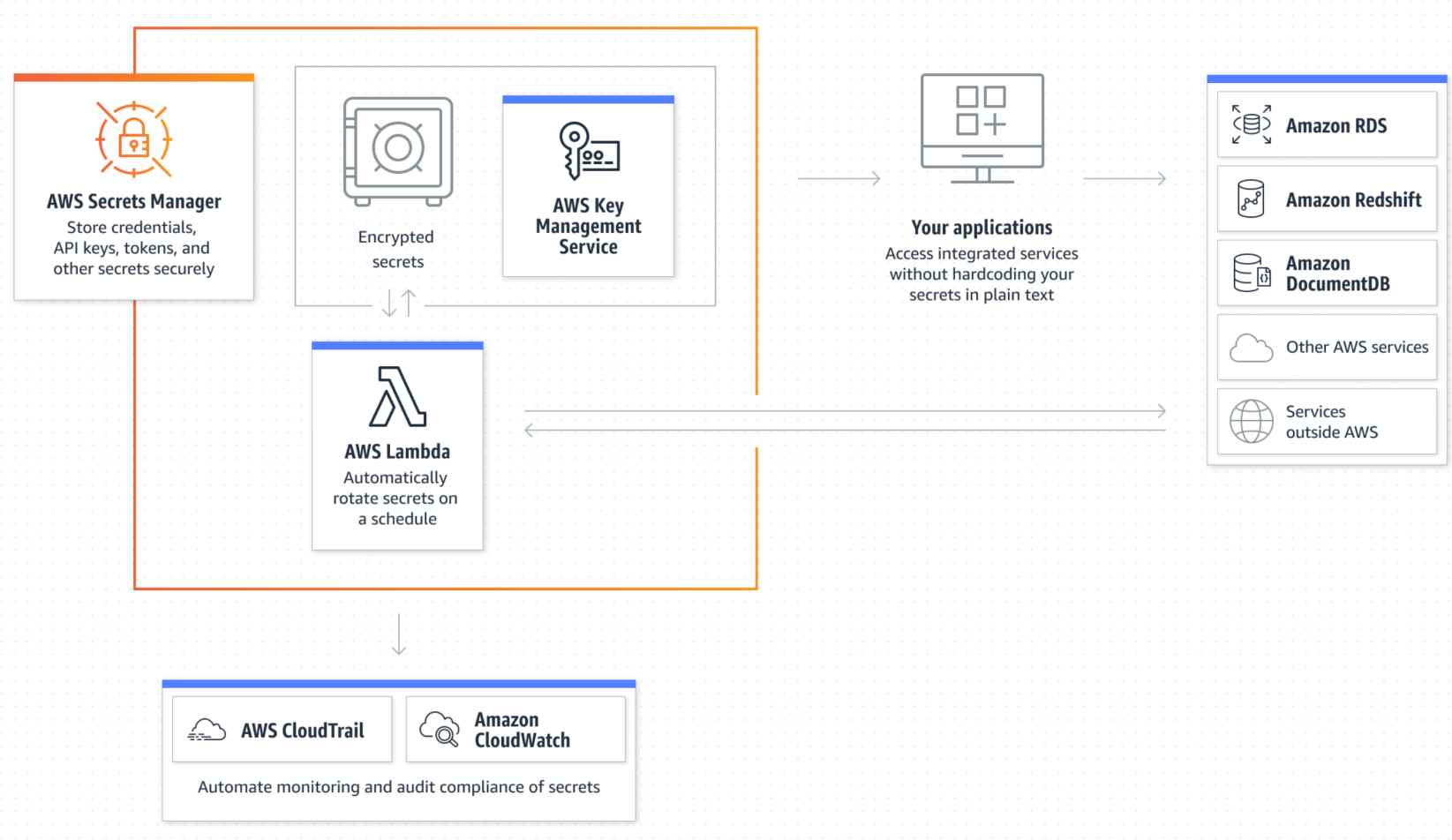
- Several websites track user activities through cookies and other data collection techniques.
- **Privacy-focused browser extensions** can limit this tracking and ensure that personal and professional data remain safe.
- Use free-of-cost browser extensions, such as:
  - **Privacy Badger:** Blocks hidden trackers
  - **HTTPS Everywhere:** Ensures secure, encrypted connections
  - **DuckDuckGo Privacy Essentials:** Prevent websites from collecting browsing data
  - **ClearURLs:** Removes tracking elements from links
  - **Cookie AutoDelete:** Automatically clears unnecessary cookies after leaving a website
- Installing and keeping these extensions updated to enhance online privacy and security.

Secrets Management

- **The Hidden Identity Risk:**
  - It's not just humans who have identities; applications do too (API Keys).
  - **The Mistake:** Developers hardcoding AWS Keys or API tokens directly into the source code (e.g., uploading them to GitHub).
- **The Solution:**
  - Use a **Secrets Manager** (e.g., AWS Secrets Manager, HashiCorp Vault).
  - The app requests the key at runtime (when it starts), keeps it in memory, and never writes it to a file.



Secrets Management – How Does It Work?



Offboarding – The Most Dangerous Time

- **The "Zombie Account" Risk:** An employee leaves, but their account remains active. An attacker finds it 6 months later. What will happen?
- **The Golden Process:**
  1. **HR Trigger:** HR system notifies IT before the exit interview.
  2. **Revoke Access:** Kill SSO session, disable VPN, reset shared passwords.
  3. **Recover Assets:** Wipe mobile data, lock the laptop, retrieve physical keys.
  4. **Transfer Data:** Move their files to their manager (don't just delete them).

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).