WEEK 3
IDENTITY & ACCESS MANAGEMENT

Taha Yiğit ALKAN

Agenda

- Identity, Access, Security
- Azure Active Directory
- Authentication vs Authorization
- Azure AD Conditional Access
- Multi-Factor Authentication
- Paswordless
- Role-Based Access Control
- Microsoft Defender for Cloud

IDENTITY, ACCESS, SECURITY

Virtual Machines, Scale Sets, Virtual Desktops, Web Apps, Functions

“Identity”

“representation of a person, application or a device”

Scott Duffy

Identity

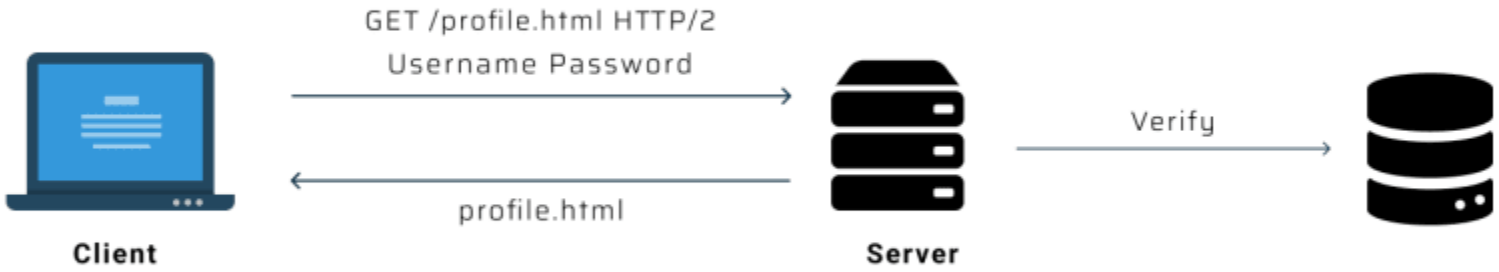
Examples

- Taha Yiğit ALKAN
- 20195175002
- yigitalkan@akdeniz.edu.tr
- Student Information System
- Laser Printer – Computer Engineering
- Headphones

Requires to prove

- Password
- Secret key
- Certificate

Client Server Model



Source: *https://dev.to/ratneshjain40/beginners-guide-to-authentication-and-authorization-in-client-server-model-express-js-and-passport-n46*

Hacks

- Storing password in “plain text”
- Using a simple reversible hash algorithm (MD5)
- Using salt
- Not enforcing password change policies
- Not enforcing password complexity policies

Active Directory

"A database and set of services that connect users with the network resources they need to get their work done"

https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx

Azure Active Directory

It is redesigned version of Active Directory

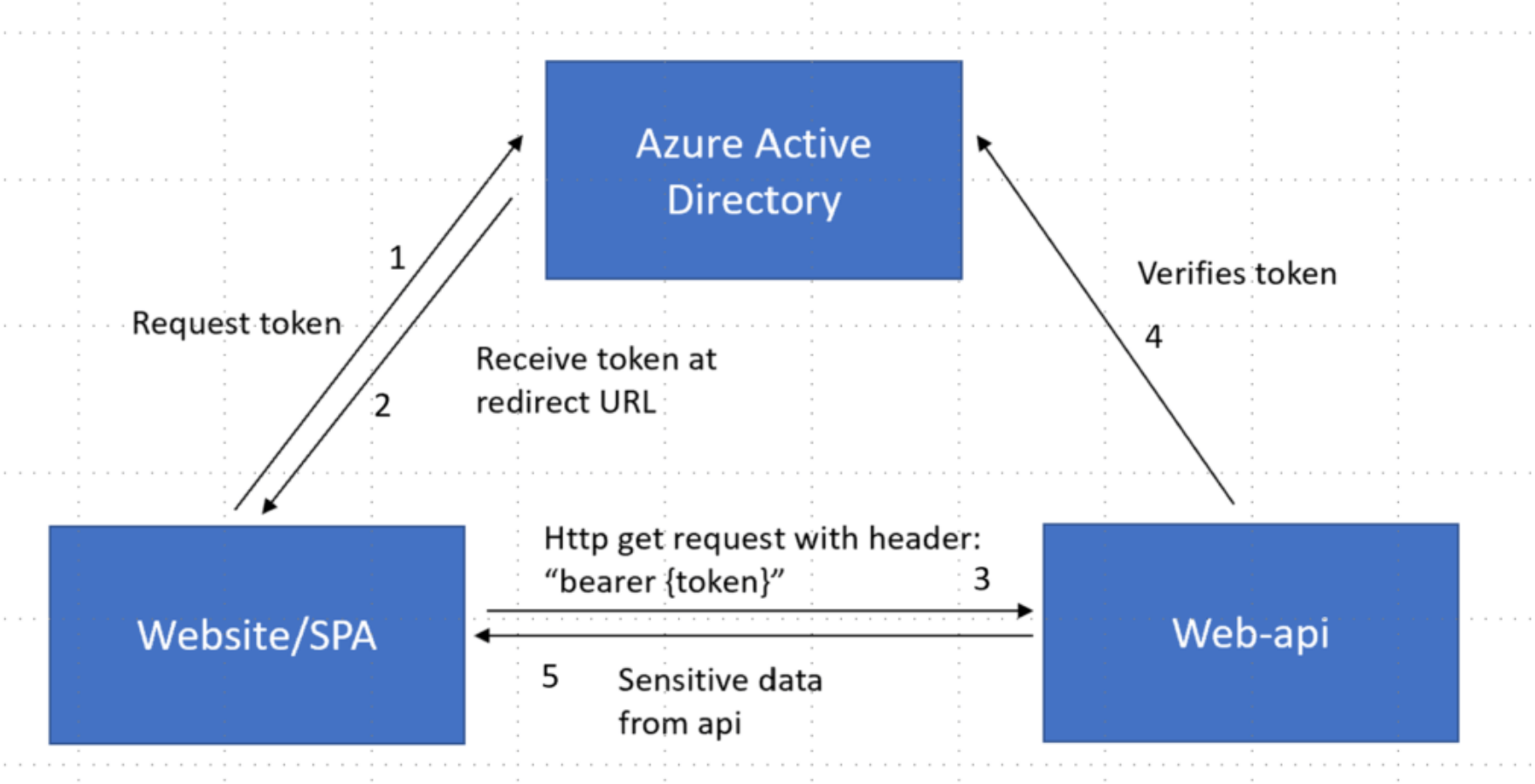
Works differently

Has more features and functionalities

E.g., Traditional Ad does not work with Internet protocols (SAML, OpenID, WS Federation)

AZURE AD PROVIDES “IDENTITY AS A SERVICE”

AAD Model



https://www.luminis.eu/blog/using-azure-active-directory-for-your-web-apps-thoughts-from-a-software-developer/

Benefits of Azure AD

- Security
- Reduced development time
- Support
- More features
- Centralized administration
- Single Sign-On
- Integration with other Azure services

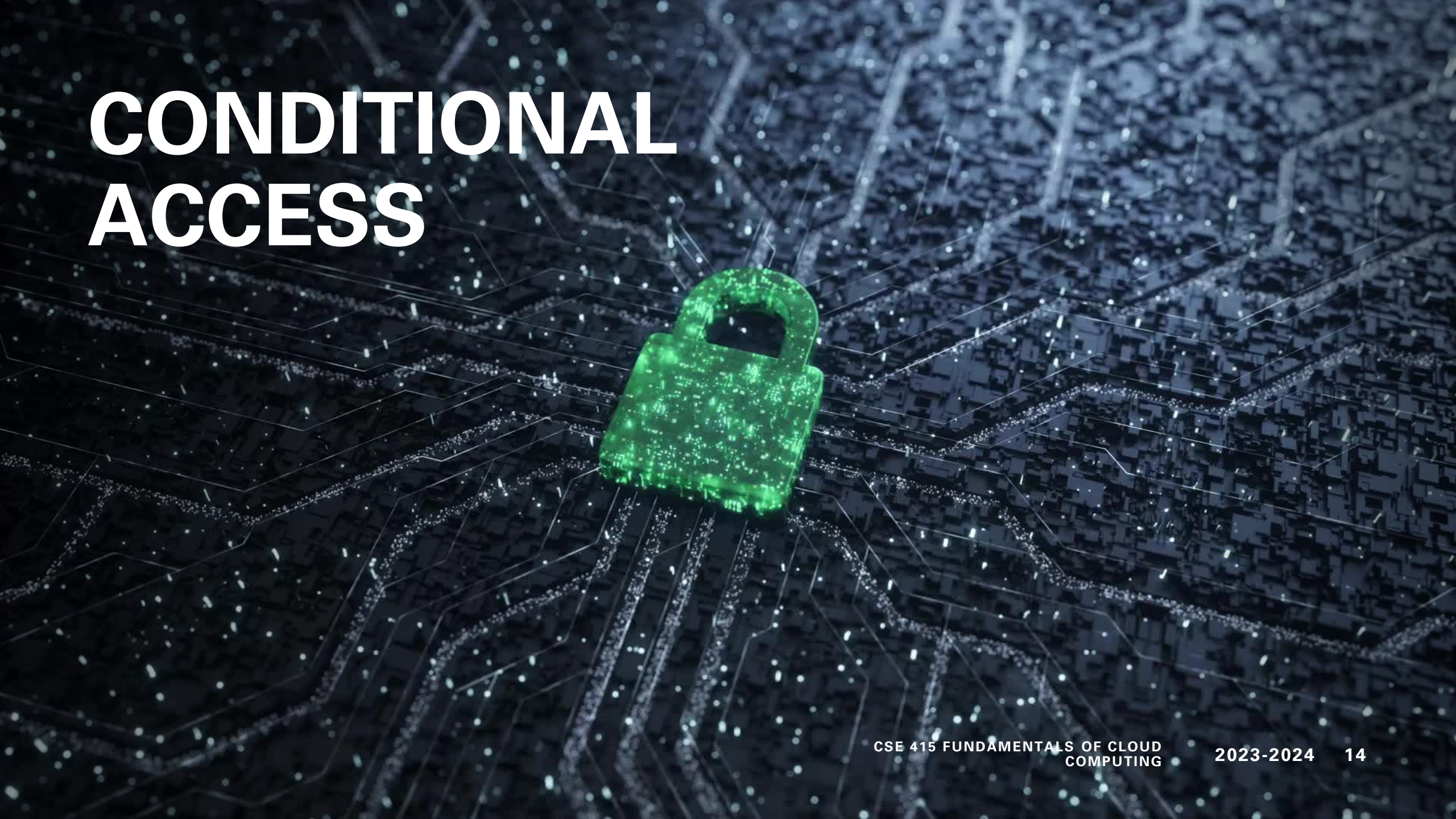
Authentication

- Verifying who a user is

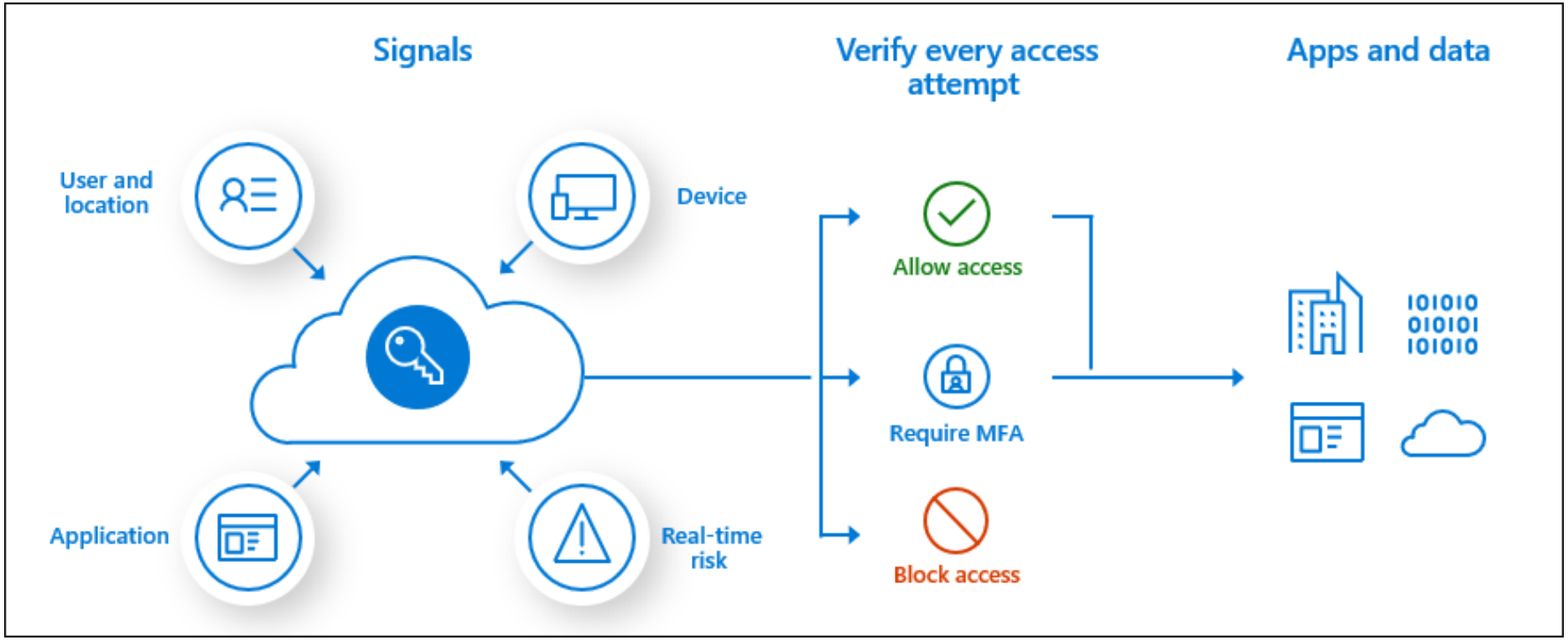
Authorization

- Verifying what they have access to

CONDITIONAL ACCESS



Conditional Access



https://www.mshowto.org/azure-ad-conditional-access-ve-named-locations-yapilandirmalari.html

MFA (Multi-Factor Authentication)

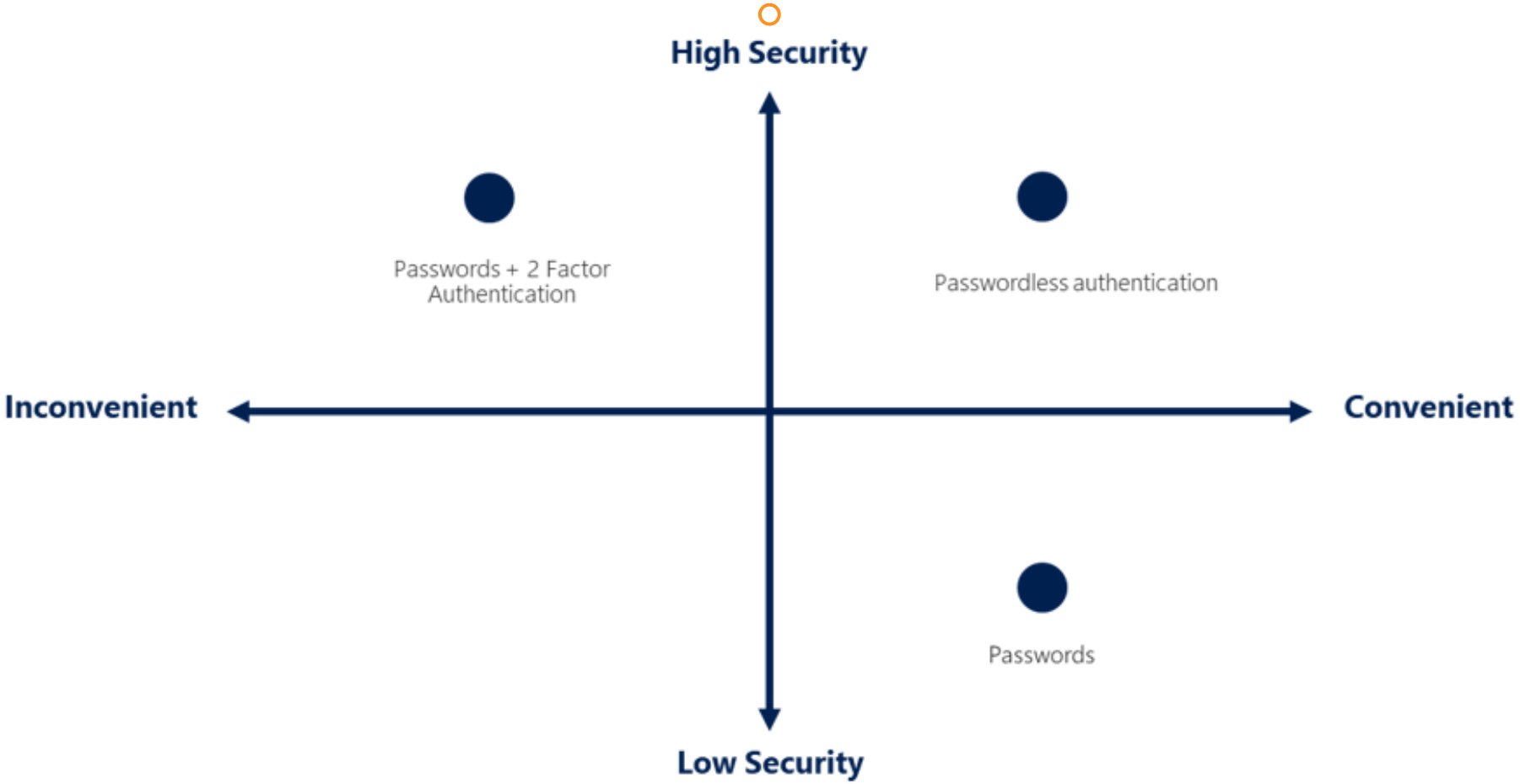
Require 2 or more pieces of evidence (factors) in order to login

- Something you **know**
- Something you **have**
- Something you **are**

Azure AD Provides

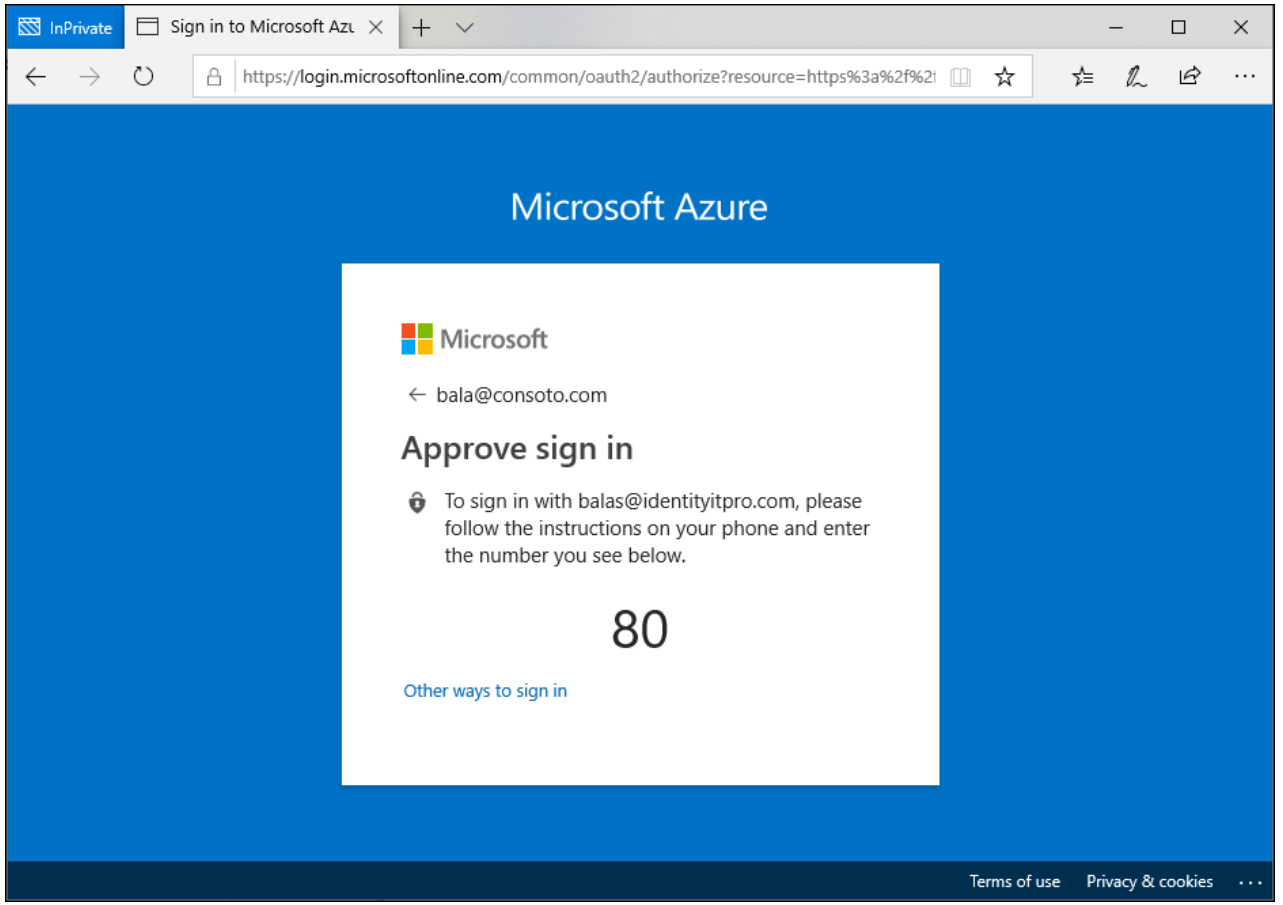
- SMS
- Email
- Authenticator
- Phone call

Passwordless



https://news.microsoft.com/apac/2020/06/02/going-passwordless-for-smarter-and-better-protection/

Microsoft Authenticator



https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

Role-Based Access Control (RBAC)

- Create roles that represent the common tasks of the job
- Assign granular permissions to that role
- Assign users to that role

- Reader, Contributor, Owner

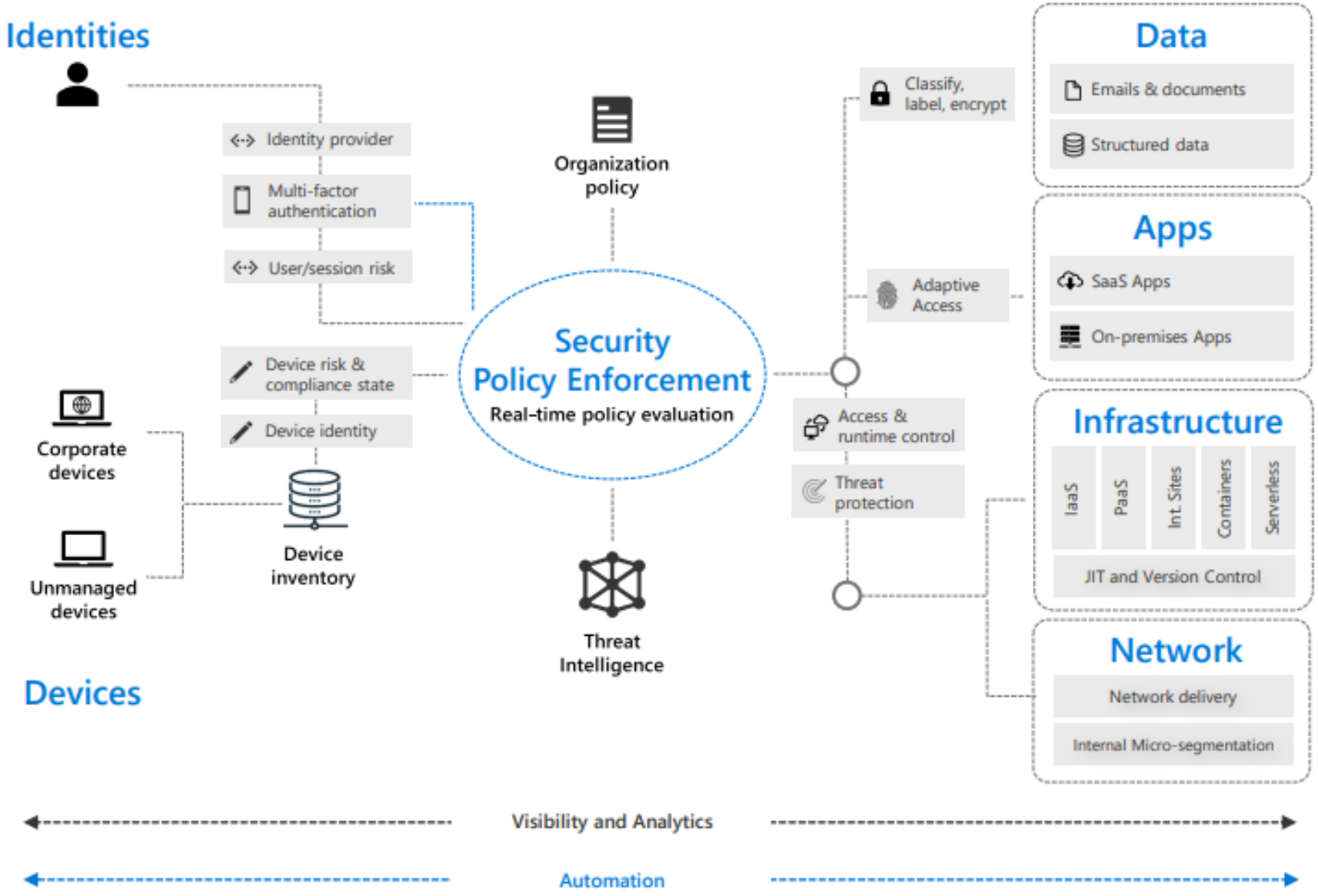
Zero Trust Methodology

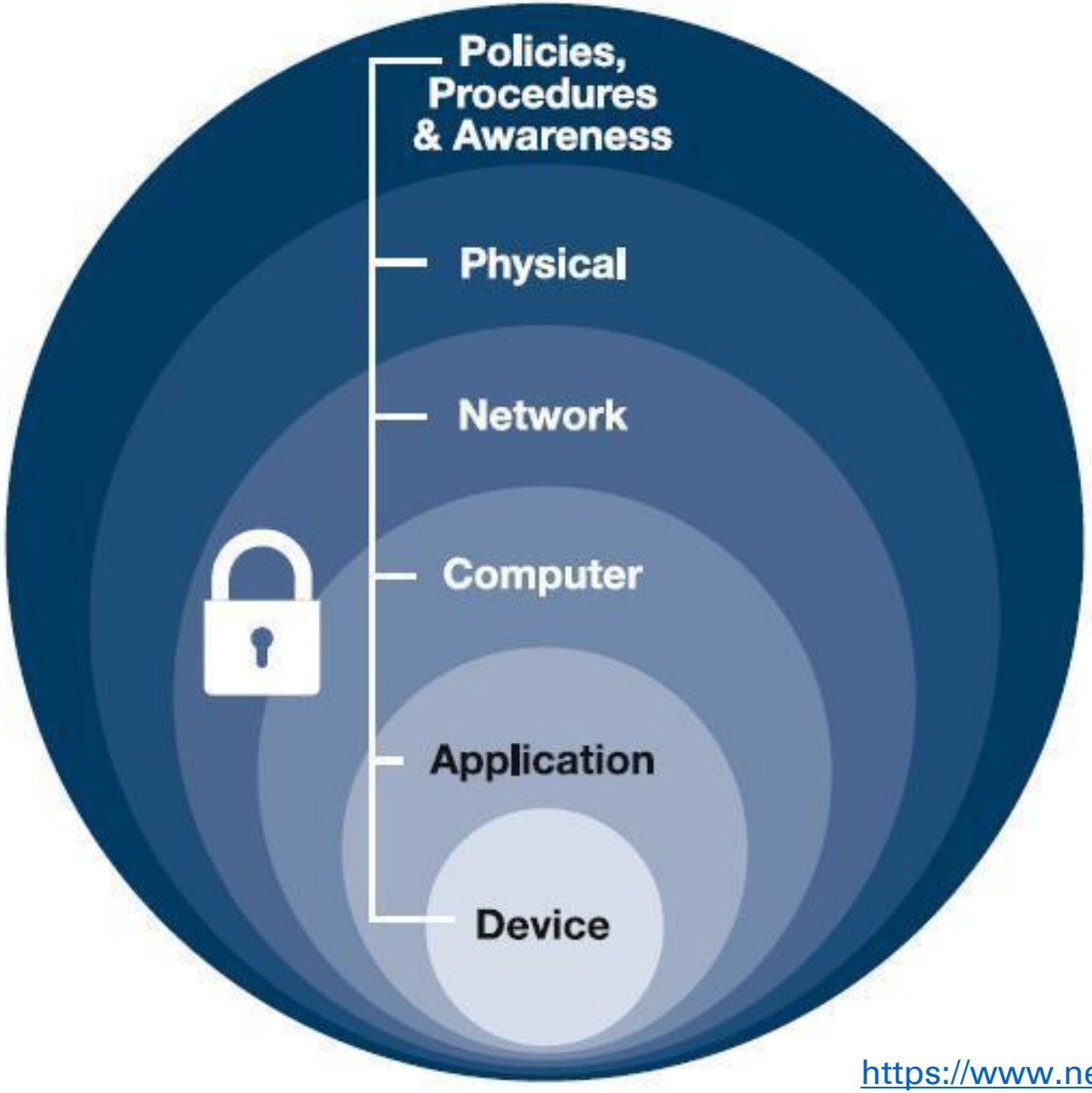
Don’t assume everything behind the firewall is safe!

Zero Trust Principles

1. Verify explicitly
2. Use least privileged access
3. Assume breach

JUST-IN-TIME(JIT)
JUST-ENOUGH-ACCESS(JAC)


Identities
Identity provider
Multi-factor authentication
User/session risk
Device risk & compliance state
Device identity
Corporate devices
Unmanaged devices
Device inventory
Devices
Organization policy
Security Policy Enforcement
Real-time policy evaluation
Threat Intelligence
Classify, label, encrypt
Adaptive Access
Access & runtime control
Threat protection
Data
Emails & documents
Structured data
Apps
SaaS Apps
On-premises Apps
Infrastructure
IaaS
PaaS
Int. Sites
Containers
Serverless
JIT and Version Control
Network
Network delivery
Internal Micro-segmentation
Visibility and Analytics
Automation



https://www.networkaccess.com/defense-in-depth/

Defense in Depth

Security Layers

- Data (virtual network endpoint)
- Application (API Management)
- Compute (Limit RDP access)
- Network (NSG, subnets, deny by default)
- Perimeter (DDoS, firewalls)
- Identity & Access (Azure AD)
- Physical (Door locks and key cards)

Defense in Depth

Identity & Access	Apps & Data Security	Network Security	Threat Protection	Security Management
Role-based access	Encryption	DDOS Protection	Antimalware	Log Management
Multifactor Authentication	Confidential Computing	NG Firewall	AI-Based Detection and Response	Security Posture Assessment
Central Identity Management	Key Management	Web App Firewall	Cloud Workload Protection	Policy and Governance
Identity Protection	Certificate Management	Private Connections	SQL Threat Protection	Regulatory Compliance
Privileged Identity Management	Information Protection	Network Segmentation	IoT Security	SIEM

Microsoft Defender For Cloud

- https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

THANK YOU

Taha Yiğit ALKAN
yigitalkan@akdeniz.edu.tr