Course Conclusion

Vlad Catrinescu

Microsoft MVP

@vladcatrinescu   https://VladTalksTech.com

Security in the Cloud Is a Partnership

The cloud provider operates and secures

– **The base infrastructure**
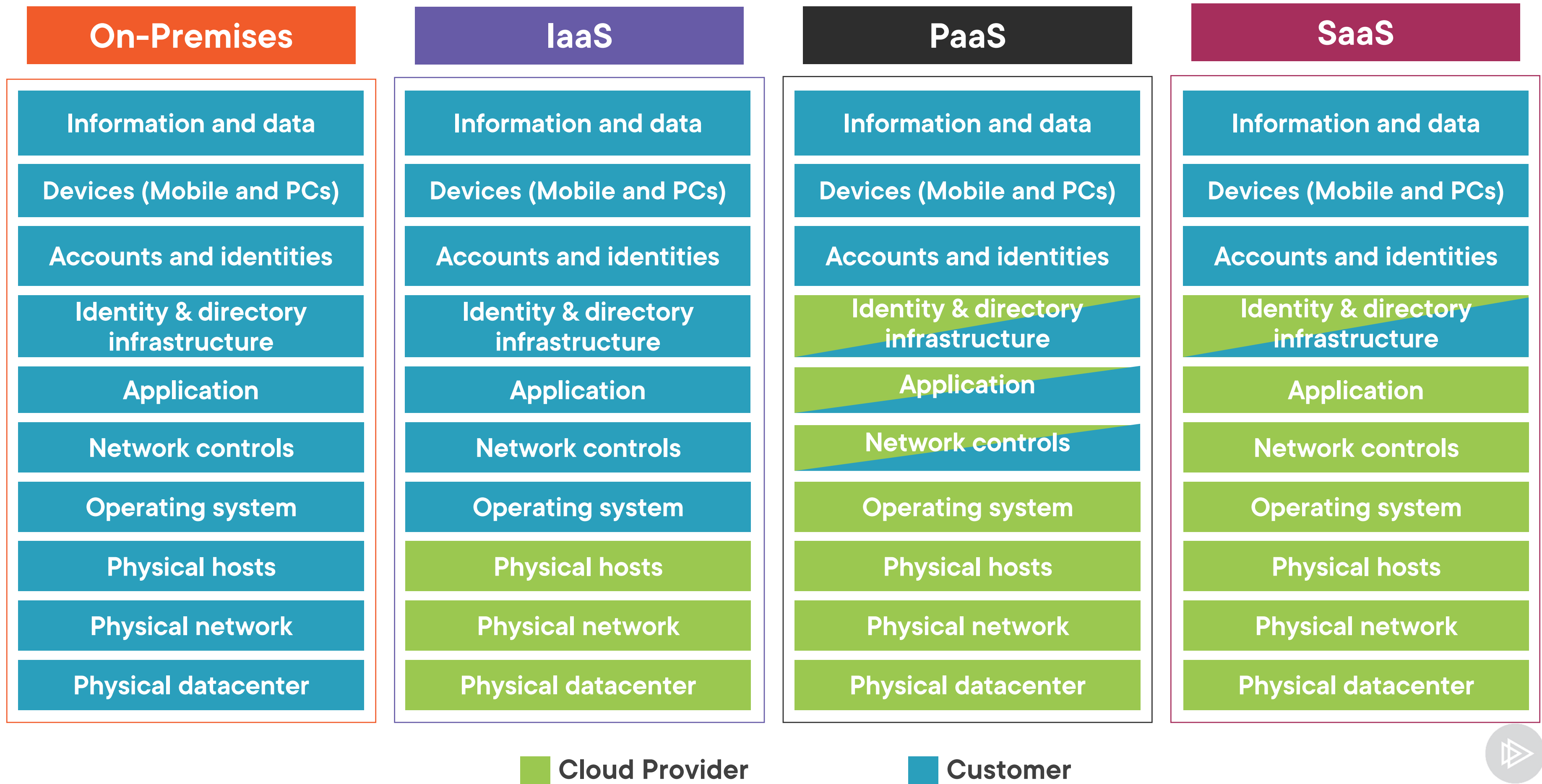
– **Host operating system layers**

You control and secure

– **Identities**

– **Additional application settings (ex: MFA)**

The responsibilities and controls for the security of applications and networks vary by the service type

Who Secures What? – The Shared Responsibility Model

On-Premises	IaaS	PaaS	SaaS
Information and data	Information and data	Information and data	Information and data
Devices (Mobile and PCs)	Devices (Mobile and PCs)	Devices (Mobile and PCs)	Devices (Mobile and PCs)
Accounts and identities	Accounts and identities	Accounts and identities	Accounts and identities
Identity & directory infrastructure	Identity & directory infrastructure	Identity & directory infrastructure	Identity & directory infrastructure
Application	Application	Application	Application
Network controls	Network controls	Network controls	Network controls
Operating system	Operating system	Operating system	Operating system
Physical hosts	Physical hosts	Physical hosts	Physical hosts
Physical network	Physical network	Physical network	Physical network
Physical datacenter	Physical datacenter	Physical datacenter	Physical datacenter

Cloud Provider   Customer

Zero Trust Guiding Principles

Verify Explicitly

Least Privileged Access

Assume Breach
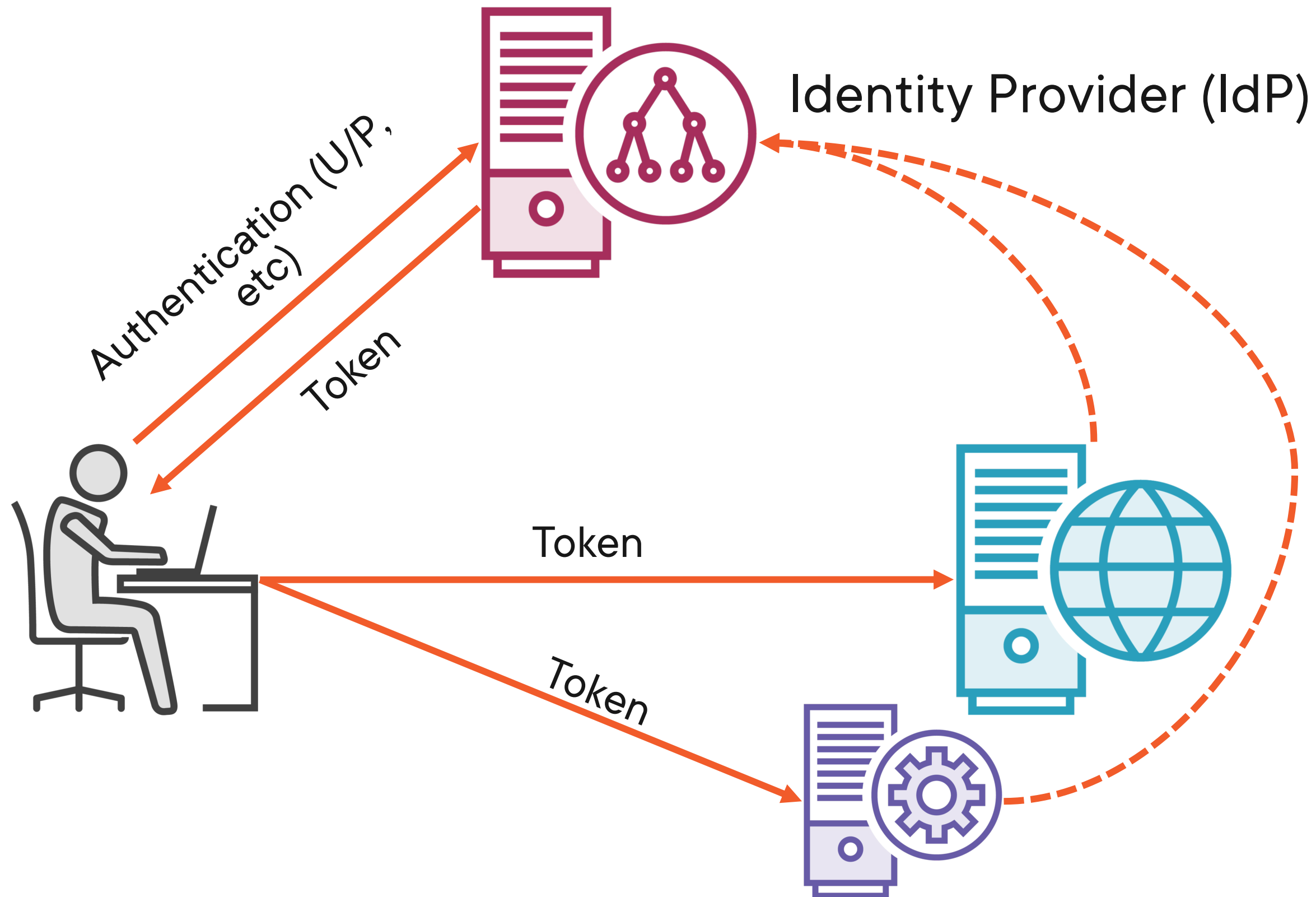
Authentication and Authorization

Authentication
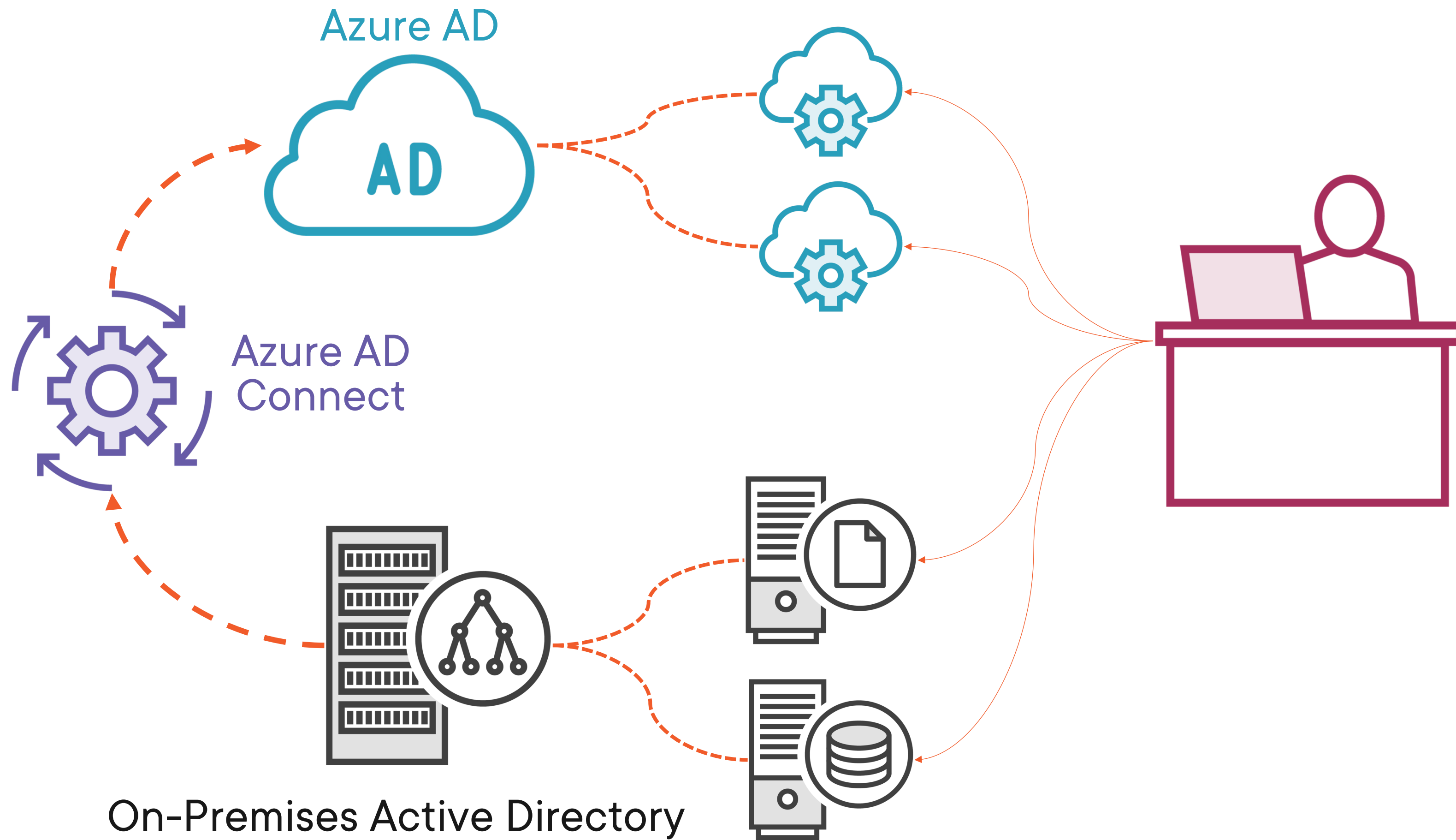Confirms users are who they say they are

Authorization
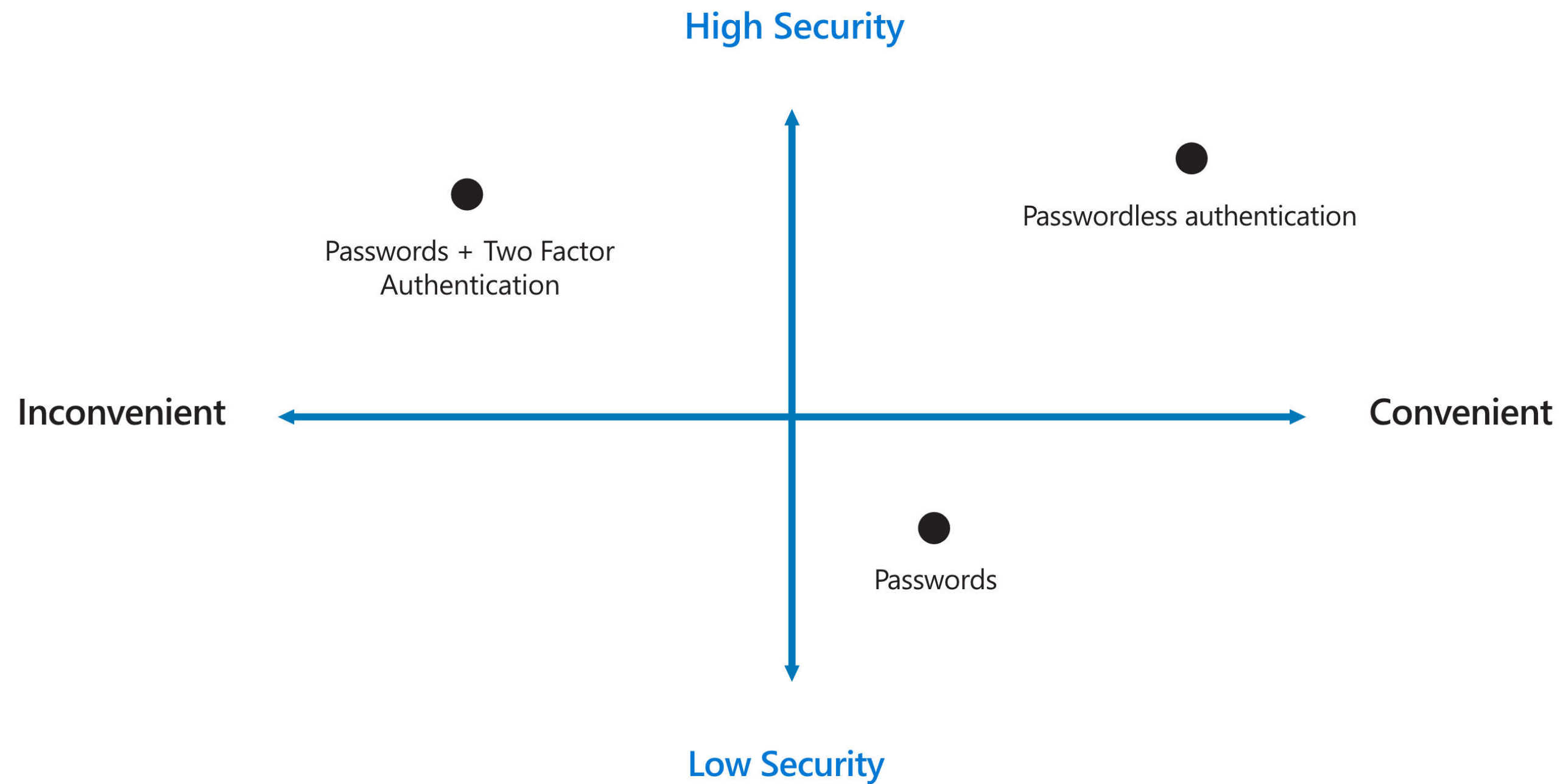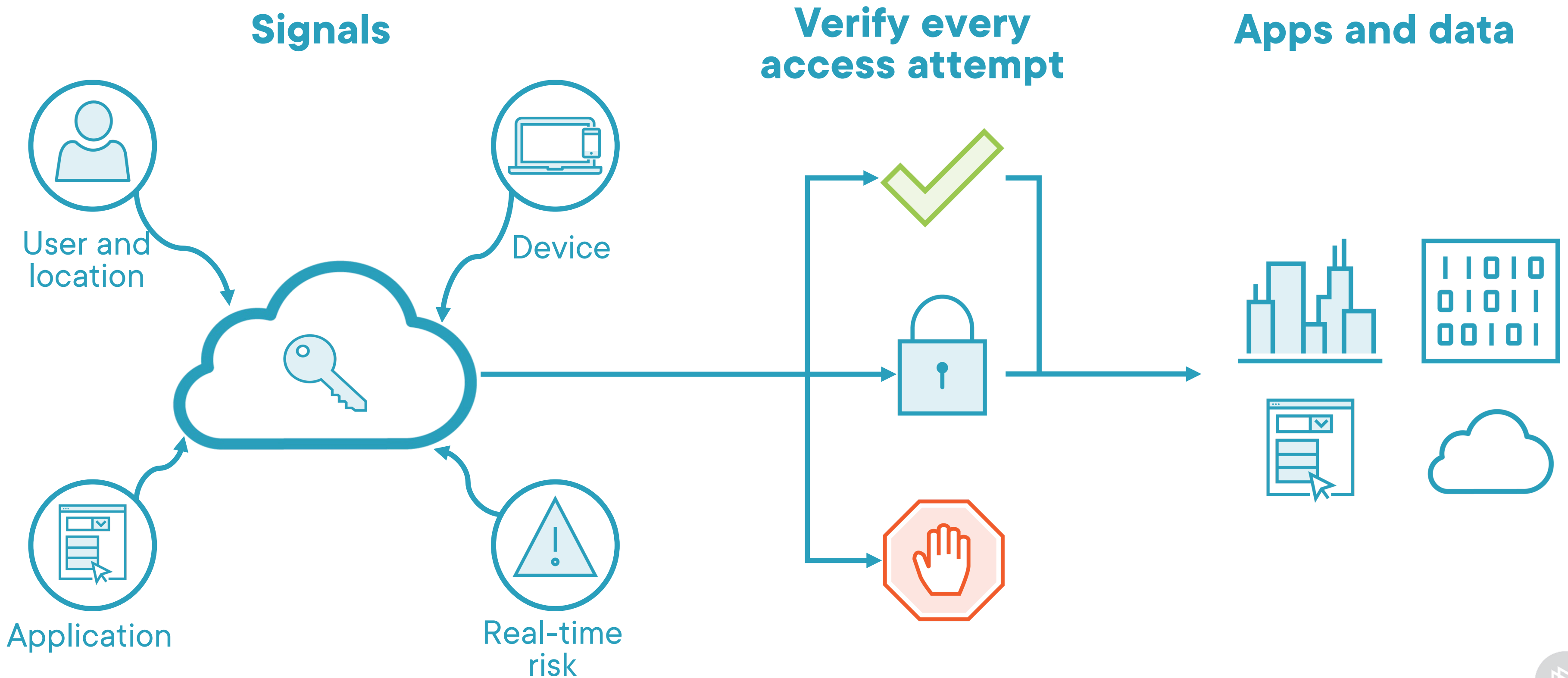Checks if users are allowed to access a resource

Modern Authentication

Identity Provider (IdP)

Authentication (U/P, etc)

Token

Token

Token

Hybrid Identities – High Level

Azure AD

AD

Azure AD
Connect

On-Premises Active Directory

Passwordless as Positioned by Microsoft

High Security

● Passwords + Two Factor
Authentication

● Passwordless authentication

Inconvenient ←———————————→ **Convenient**

● Passwords

Low Security

Azure AD Conditional Access

Signals

User and location

Device

Application

Real-time risk

Verify every access attempt

Apps and data

Set of Security Tools

SIEM | **Security Incident and Event Management**

SOAR | **Security Orchestration Automated Response**

XDR | **Extended Detection and Response**

Microsoft 365 Defender

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Microsoft Sentinel Functionality
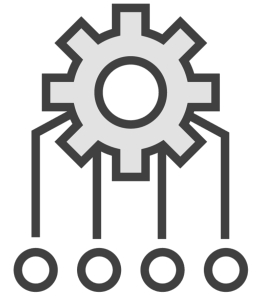
Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft
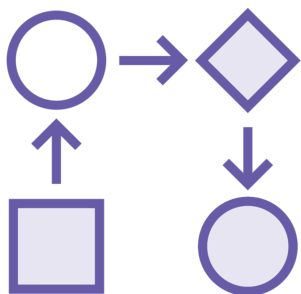
Respond to incidents rapidly with built-in orchestration and automation of common security tasks

Compliance in the Cloud

Overall compliance score

Your compliance score: 75%
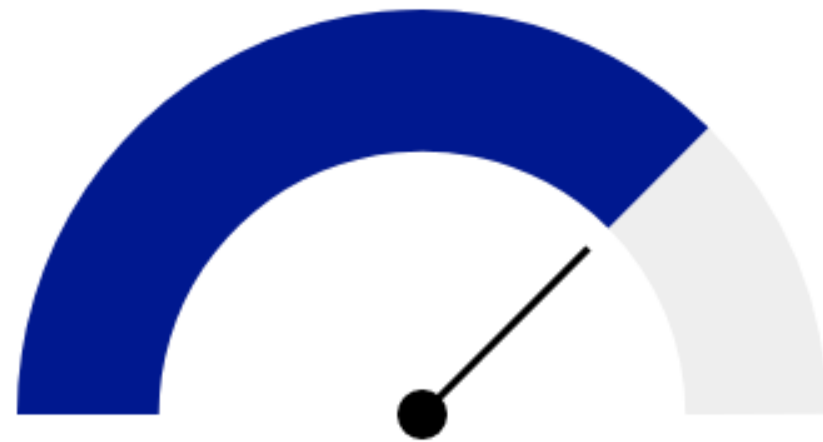
12159/16167 points achieved

Your points achieved ⓘ
0/ 4008

Microsoft managed points achieved ⓘ
12159/ 12159

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Security in the cloud is a partnership
- **So is compliance!**

Part of the requirements will be done by Microsoft
- **Documentation in the Service Trust Portal**

A lot of it depends on you

Microsoft's Six Key Privacy Principles

Control

We will put you in control of your privacy with easy-to-use tools and clear choices.

Transparency

We will be transparent about data collection and use so you can make informed decisions.

Security

We will protect the data you entrust to us through strong security and encryption.

Strong legal protections

We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

No content-based targeting

We will not use your email, chat, files or other personal content to target ads to you.

Benefits to you

When we do collect data, we will use it to benefit you and to make your experiences better.

Service Trust Portal

The Service Trust Portal is a single location where you can find audit reports, Pen Tests, Security Assessments, and more information on how Microsoft manages security, privacy and compliance.

https://servicetrust.microsoft.com/

Microsoft Purview Products in This Course

Microsoft Purview Compliance Manager

Microsoft Purview Information Protection

Microsoft Purview Data Loss Prevention

Microsoft Purview Insider Risk Management

Microsoft Purview eDiscovery

Microsoft Purview Audit

Get Microsoft 365 Certified!

Microsoft 365 Certified: Fundamentals

Prove that you understand the options available in Microsoft 365 and the benefits of adopting cloud services, the Software as a Service (SaaS) cloud model and implementing Microsoft 365 cloud service.

Exam MS-900

https://docs.microsoft.com/en-us/learn/certifications/exams/ms-900

Check out the certification path on Pluralsight!

The Security, Compliance, and Identity Certification Portfolio

Exam SC-900

Exam SC-200

Exam SC-300

Exam SC-400

Microsoft Certified: Security, Compliance, and Identity Fundamentals

Audience is everyone who wants to familiarize with fundamentals of security, compliance, and identity

    – **Microsoft 365 & Azure!**

Check out the certification path on Pluralsight!

Follow me on Pluralsight!

https://app.pluralsight.com/profile/author/vlad-catrinescu

Thank You!

Twitter®: @vladcatrinescu

LinkedIn®: http://ca.linkedin.com/in/vladcatrinescu

Blog: https://VladTalksTech.com

YouTube®: https://spvlad.com/YouTube