The world is changing..

- Corporate applications and data are moving to hybrid and cloud environments.

- Organizational assets, resources, and data are being accessed outside the corporate network

- Security perimeter now extends to every access point that hosts, stores, or accesses corporate resources and services
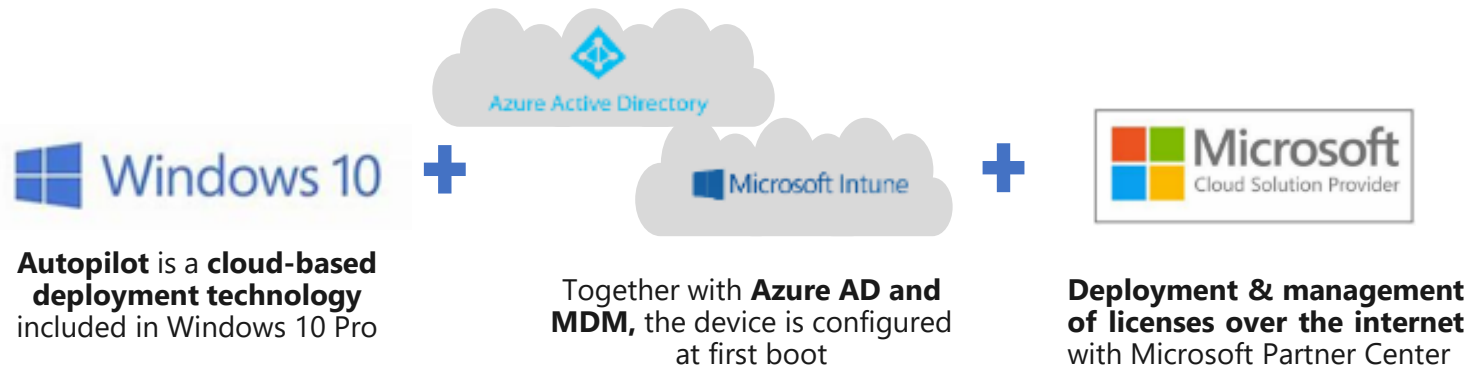
Microsoft

![Microsoft]

Enterprise Mobility + Security and Microsoft Intune

- Microsoft Enterprise Mobility + Security (Microsoft EMS) is intelligent mobility management and security platform.
- EMS helps protect and secure your organization with its products that act to increase security features of Windows 10 and Microsoft 365

What is Windows Autopilot?

A cloud-based deployment technology available in Windows 10 Pro. It enables **deployment & configuration of devices over the internet** through the Microsoft Partner Center. It also requires **Azure Active Directory & MDM** to manage and configure devices via automatic enrollment in these solutions at first boot.
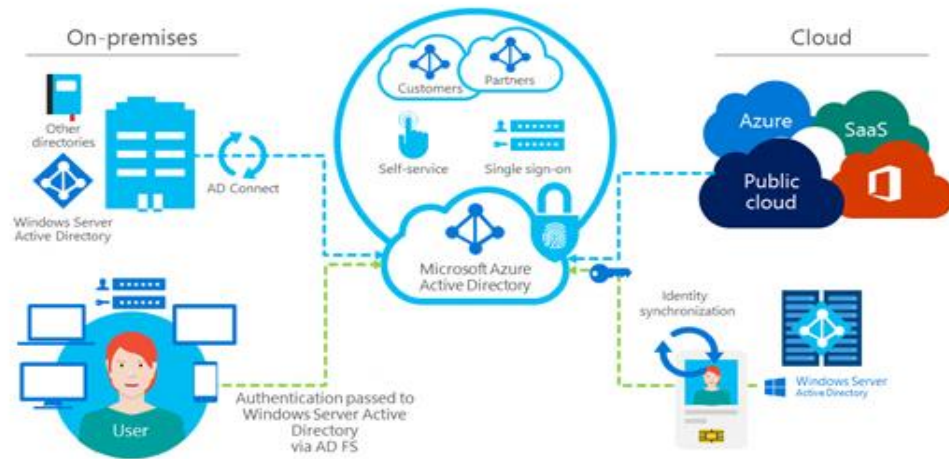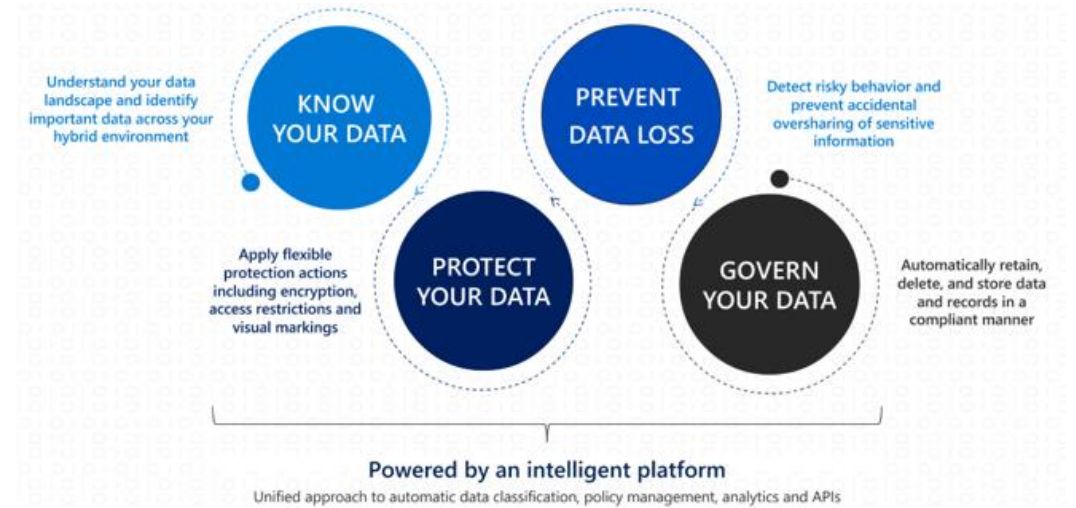
Unbox. Log in. Take off.

Windows 10

Autopilot is a **cloud-based deployment technology** included in Windows 10 Pro

Azure Active Directory

Microsoft Intune

Together with **Azure AD and MDM,** the device is configured at first boot

Microsoft Cloud Solution Provider

Deployment & management of licenses over the internet with Microsoft Partner Center

- Device deployment made simple
- Simplified device management tool
- Secure protection out of the box
- Improved employee satisfaction

VST ECS PHILS., INC. (formerly MSI-ECS Phils., Inc.)

Identity and Access Management

Information Protection

Threat Protection

# Cloud Security
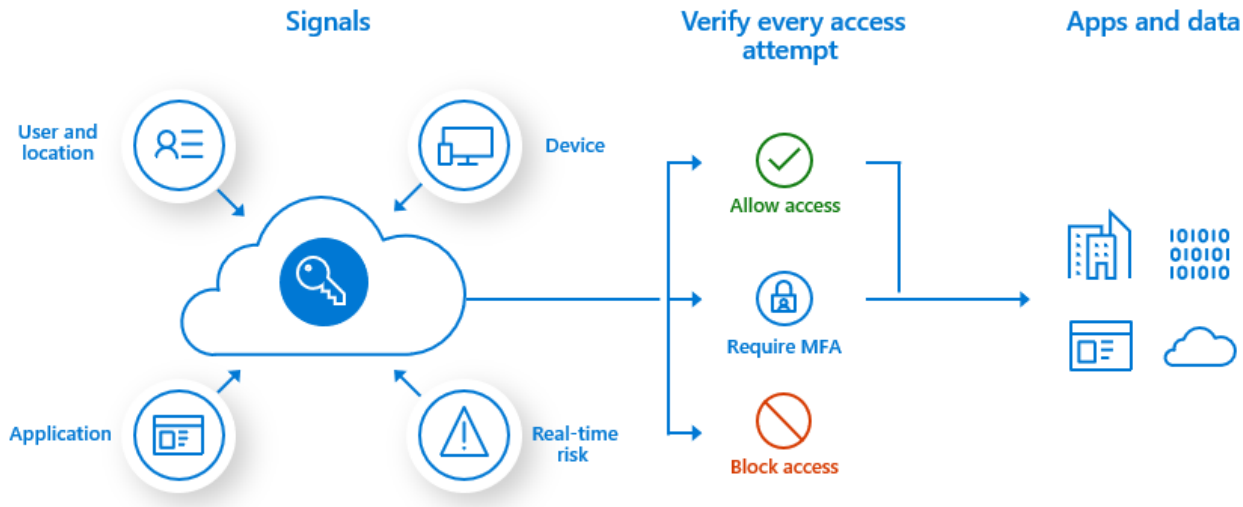
Conditional Access

- Conditional Access is at the heart of the new identity-driven control plane. It spans Microsoft 365 services, including Intune, Microsoft 365, and Windows 10.

- Provides granular access to keep your corporate data secure while allowing users to do their best work from any device and from any location.

- Helps protect sensitive data by evaluating users, devices, apps, location, and assessing the risk before granting access.

Zero Trust Security Model

- Zero Trust teaches us to :

  "never trust, always verify."

- Zero trust is a security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter.
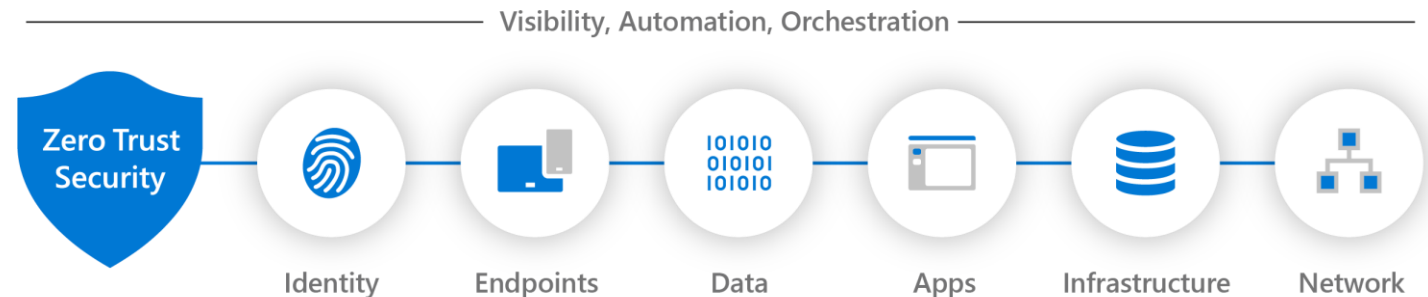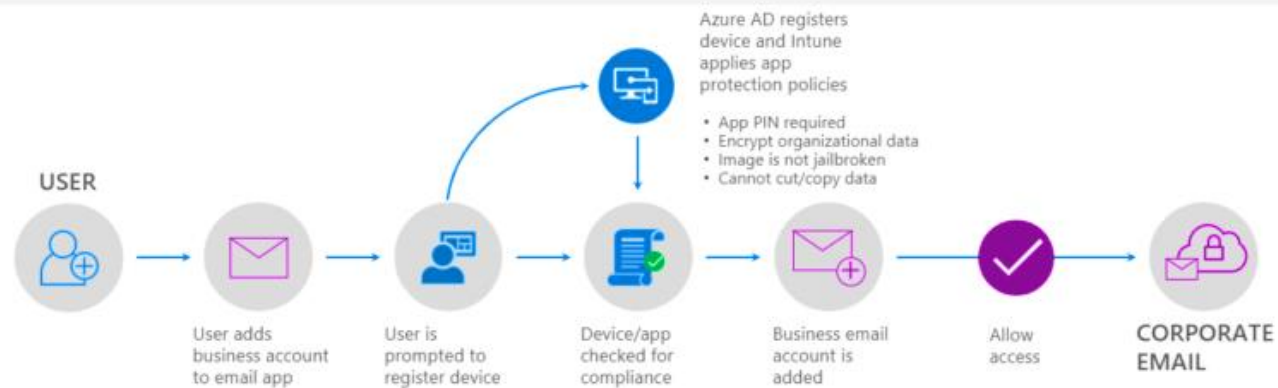
How do we really protect?

Conditional Access

o Secure who can access and how can they access

App Protection Policies

o We can control what users can do of the data in this applications

I want to secure corporate data on personal devices

Azure AD registers device and Intune applies app protection policies

- App PIN required
- Encrypt organizational data
- Image is not jailbroken
- Cannot cut/copy data

USER

User adds business account to email app → User is prompted to register device → Device/app checked for compliance → Business email account is added → Allow access → CORPORATE EMAIL

Microsoft

Company Data: Secured and Protected

Company Managed

- VPN's
- Applications
- Password / PINS

Employee Managed

- Access to E-mail
- Teams
- Protecting applications

Microsoft

Management with Microsoft Intune

Mobile Device Management

Mobile Application Management

PC Management

Intune help organizations provide their employees with access to corporate applications, date and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.