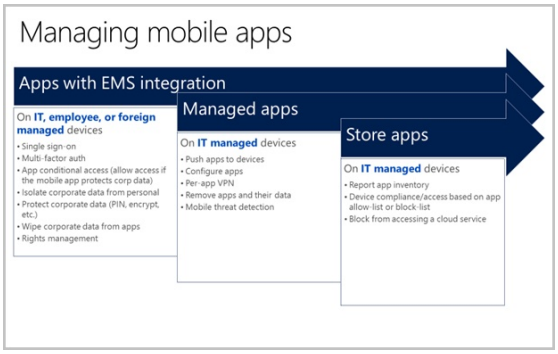
Microsoft Intune is an MDM and MAM provider for your devices. Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices are used, including mobile phones, tablets, and laptops. You can also configure specific policies to control applications. For example, you can prevent emails from being sent to people outside your organization. Intune also allows people in your organization to use their personal devices for school or work. On personal devices, Intune helps make sure your organ

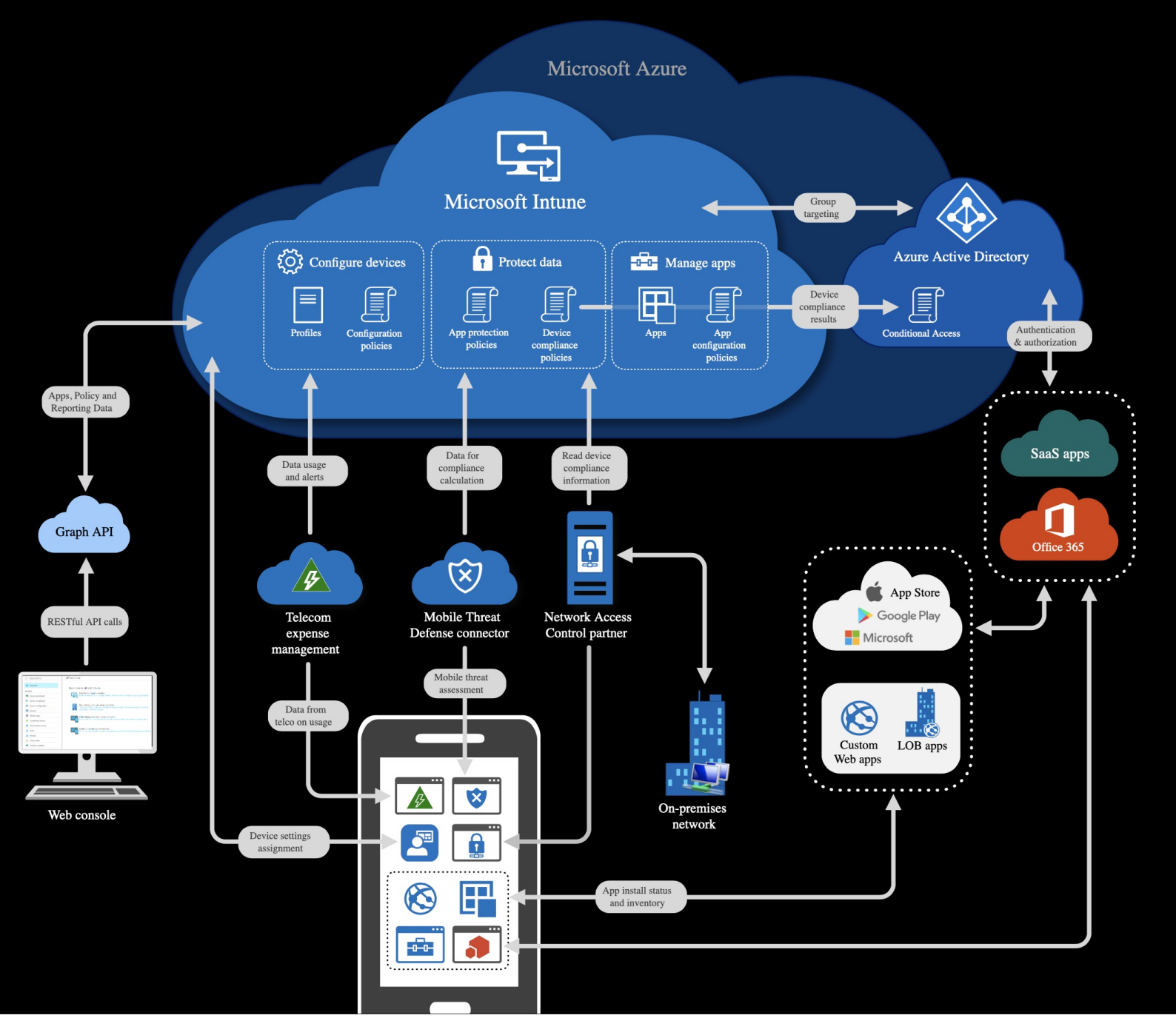


Intune is part of Microsoft's Enterprise Mobility + Security (EMS) suite. Intune integrates with Azure Active Directory (Azure AD) to control who has access, and what they can access. It also integrates with Azure Information Protection for data protection. It can be used with the Microsoft 365 suite of products. For example, you can deploy Microsoft Teams, OneNote, and other Microsoft 365 apps to devices. This feature enables people in your organization to be productive on all of their devices, while keeping your organization's information protected with policies you create.

In Intune, you manage devices using an approach that's right for you. For organization-owned devices, you may want full control on the devices, including settings, features, and security. In this approach, devices and users of these devices "enroll" in Intune. Once enrolled, they receive your rules and settings through policies configured in Intune. For example, you can set password and PIN requirements, create a VPN connection, set up threat protection, and more.

- Choose to be 100% cloud with Intune, or be co-managed with Configuration Manager and Intune.
- Set rules and configure settings on personal and organization-owned devices to access data and networks.
- Deploy and authenticate apps on devices -- on-premises and mobile.
- Protect your company information by controlling the way users access and share information.
- Be sure devices and apps are compliant with your security requirements.

For personal devices, or bring-your-own devices (BYOD), users may not want their organization administrators to have full control. In this approach, give users options. For example, users enroll their devices if they want full access to your organization resources. Or, if these users only want access to email or Microsoft Teams, then use app protection policies that require multi-factor authentication (MFA) to use these apps.


Microsoft Azure
Microsoft Intune
Group targeting
Azure Active Directory
Configure devices
Profiles
Configuration policies
Protect data
App protection policies
Device compliance policies
Manage apps
Apps
App configuration policies
Device compliance results
Conditional Access
Authentication & authorization
Apps, Policy and Reporting Data
Graph API
RESTful API calls
Web console
Data usage and alerts
Data for compliance calculation
Read device compliance information
Telecom expense management
Mobile Threat Defense connector
Network Access Control partner
Mobile threat assessment
Data from telco on usage
Device settings assignment
On-premises network
SaaS apps
Office 365
App Store
Google Play
Microsoft
Custom Web apps
LOB apps
App install status and inventory