**Explain how your company which depends on local Active Directory authentication service can take advantage of Azure authentication service**.

**Active Directory (AD) authentication**

One such tool you may use to manage people, programs, and other assets inside the company is Active Directory (AD) authentication. When implemented, Active Directory authentication can streamline IT management and improve the company's overall security posture. Find out more about AD authentication, how it functions, and how JumpCloud can assist you in optimizing it.

A Windows-based mechanism called AD authentication is used to authenticate and authorize users, endpoints, and services in Active Directory. Through the AD Group Policy functionality, IT teams may get centralized control over devices and user configurations while streamlining user and rights management using AD authentication.

Authentication in Azure Active Directory (Azure AD) entails more than merely confirming a login and password. Azure AD authentication contains the following elements to increase security and decrease the need for help desk assistance: Resetting a password on your own. Multi-Factor Authentication for Azure AD.

In your web application, RESTful API, and mobile back end, you can sign in users and access data by writing little to no code thanks to Azure App Service's built-in authentication and authorization capabilities.

Step 5 of 7

**Advantages:**

You may build strong security measures with Azure AD to safeguard your data and satisfy compliance requirements. Azure AD offers capabilities like conditional access and multi-factor authentication that can help you secure your data and adhere to industry standards. Azure AD also offers extensive reporting and auditing features, which can assist you in meeting your compliance requirements.

By offering Single Sign-On (SSO) and multi-factor authentication (MFA), which make it simple to manage user identities and access management, Azure AD contributes to increased security. Users that use SSO can log into all of their applications using a single set of credentials. Lowering the number of passwords that users need to remember, can enhance security.

By asking users to verify their identity with a second factor, such as a phone call or text message, MFA adds an extra degree of protection.

By giving you a single spot to manage all of your users and applications, Azure AD helps streamline management. Create and manage user accounts, give permissions, and manage application access using Azure AD. Since password resets are the most common help desk request, Azure AD also offers a self-service password reset tool that can help lower IT support expenses.

Azure AD is a reasonably priced solution that streamlines your IT infrastructure and helps businesses save time and money. Its pay-as-you-go pricing structure for Azure AD. With this price model, you only pay for the services you utilize, which could be a great way to save money when implementing Azure AD.

Azure AD is a cloud-based service. As your business's demands change, Azure AD's great scalability makes it simple to grow your user base. If your company is moving more toward hybrid work, it also implies that Azure AD services will be delivered to your users with good performance wherever they may be. There is no complex virtual private network (VPN) management needed to connect users to the same network as the on-premises AD instance.