Azure Active Directory

OXFORD COMPUTER GROUP

Azure Active Directory (Azure AD) is the backbone of identity security within all of Microsoft's cloud offerings. This is the security endpoint that allows for authentication and authorization for Microsoft services, as well as any modern application that is integrated with Azure AD.

How does Azure AD provide that security endpoint for the entire range of Microsoft's Azure services? With a plethora of infrastructure and cloud solutions

Azure identities work with...

Storage

- Azure Storage security comes with a comprehensive set of security capabilities, including the ability to restrict permissions based on your identities and groups in Azure
- Utilizing the pre-defined, granular RBAC functionality constrains access to a "need to know" and "least-privileged" security model

Virtual Machines

- The key to security in any virtualized environment is controlling authentication and access to the virtual resources. In Azure, this is accomplished by using Azure policies along with RBAC
- While Azure policies are driven by what a particular user or resource does, RBAC manages security based on who that user or resource is

Databases (i.e. SQL, Cosmos, etc.)

- Security is a foundational requirement that can be fulfilled by leveraging your Azure AD identities and groups, originating in the cloud or on-premises, within Azure database workloads
- Privileged Identity Management (PIM), Conditional Access, and Multi-Factor Authentication (MFA) can all be layered into database access

Networking

- A strong and dynamic identity management system will position an enterprise with Azure AD well for managing Azure Networking components
- With Azure Role-Based Access Control (RBAC), you can easily leverage existing identities in your cloud directory for access ranging from full administration to monitoring

...and we've only scratched the surface of Azure workloads.

Other Microsoft cloud technologies enabling identity and security

Multi-Factor Authentication

- Azure MFA relies on a phone or other device to provide a second authentication token, helping to reduce the success of phishing attacks
- MFA can be configured to secure the authentication of an Azure AD user upon log-on of any modern app that utilizes SAML, OAuth, or OpenID Connect.
- PIM utilizes MFA to protect administrative users during their Just-In-Time 'step-up' authentication

Access Reviews

- Azure AD Access Reviews enable organizations to efficiently manage group memberships, access to applications, and privileged role assignments.
- With Access Reviews, you can attest the membership of the group, including all users or guest user membership. You can also attest to access to an application that is federated with Azure AD

Privileged Identity Management

- Securing privileged identities (administrators) is a key component of IT security (least-privileged access)
- Just-In-Time elevation to administrative capability for only the time required, and Just-Enough permissions grants just the proper level of access for the role actor
- Eliminates shared admin accounts for better auditing

Azure Active Directory:

Enabling Identity & Security Across the Enterprise

OXFORD COMPUTER GROUP

Passwordless Authentication

- Windows Hello for Business is a step on the road to passwordless authentication
- Biometric information (fingerprint, face, etc.) are used to authenticate the user
- Windows 10 will add the ability to use FIDO2 authentication tokens to provide authentication with a hard token (Fall 2018)
- Intranet authentication may be performed without password using the Multi-Factor Authentication token devices

Domain Join

Azure Domain Join provides several benefits:

- True single-sign on for all apps provisioned through Azure
- Ability to automatically enroll in Device Management
- Doesn't require connectivity to AD Domain (on-premises)
- Identifies devices as 'known' or 'trusted' to the organization, allowing Conditional Access to manage access on the computer to data and apps

Intune

- Managing security on end-user devices is a core requirement that can be managed in a straightforward manner with the security controls native to the Azure deployment
- Identities in Azure permits Intune to distribute apps based on group membership, configure restrictions based on group membership, deliver certificates to provide strong authentication, and restrict access to content and applications using Conditional Access
- With a strong identity foundation in Azure AD managed by a strong identity management platform, makes Intune manageable and auditable.

Office 365 Data Loss Prevention, Azure Information Protection (AIP), and Cloud App Security

These three components are tightly related and protect data in differet ways:

- Office 365 DLP can stop data from going out through Exchange
- AIP can encrypt, classify, and enforce usage restrictions on that data
- Cloud App Security is the investigation of where that data is going and where it is being leveraged in an environment

With Azure AD, content can be shared securly with users, customers, and partners.

Data Classification

AIP provides a data classification taxonomy. Classification may:

- Start with new data and pickup older data as it's referenced
- Be set by the user or automatically by AIP
- Be used to set encryption and useage rights
- Be used to restrict where data may travel with using Cloud App Security
- Be used to restrict where data may be sent in Exchang Online

Leveraging a strong identity management solution that keeps identities in the cloud accurate and consistent is key to leveraging any of these Azure solutions.

Why choose Oxford Computer Group?

For over a decade, we have specialized in Microsoft identity solutions. We have an excellent track record, having won the Microsoft Partner of the Year award seven times, including the inaugural Enterprise Mobility Partner of the Year award in 2015.

We conduct strategic reviews for customers in all areas of industry and across the globe. We assess architectures and processes, and make recommendations designed to support strategic objectives.

To accelerate deployment, we use our proven methodology, best practices, and a unique library of code developed during 900+ projects.

Get in touch!

877-862-1617

info@oxfordcomputergroup.com

www.oxfordcomputergroup.com