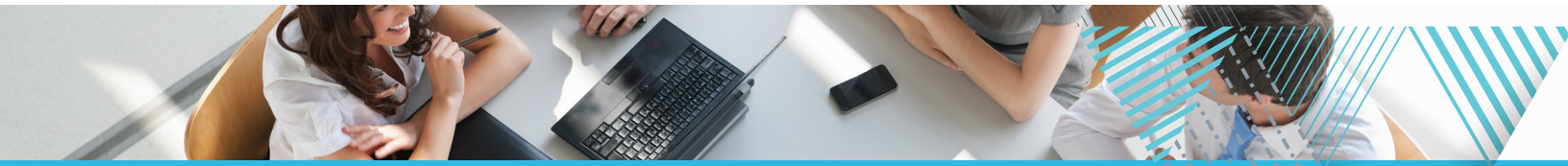

LEVERAGE THE MOST ADVANCED MICROSOFT TECHNOLOGIES

Avaleris works closely with clients from multiple industries and sectors to customize Security, Hybrid Identity and Access Management solutions that will empower their users, improve their business agility, and strengthen their cybersecurity posture.

Our intimate knowledge of the following Microsoft technologies will ensure that you are making well informed decisions:

ACTIVE DIRECTORY

Active Directory (AD) is a Windows OS directory service that facilitates working with interconnected, complex, and different network resources in a unified manner. It forms the foundation of authentication used for identity and access management.

AZURE AD PREMIUM

Azure Active Directory Premium is a cloud-based identity and access technology that supports single sign-on to thousands of cloud apps, which includes self-serve password reset and multi-factor authentication. Using Azure AD Connect, the technology integrates with on-premises directories to provide a common identity in a hybrid environment. Azure AD Premium enables powerful access control and includes a number of robust security features.

ACTIVE DIRECTORY FEDERATION SERVICES (AD FS)

AD FS is a standards-based authentication service from Microsoft that enables single sign-on. It is often used as a component of a larger on-premises, hybrid, or cloud identity architecture. Advanced Federation configurations allow organizations to trust partner organizations' identities.

MICROSOFT ADVANCED THREAT ANALYTICS (ATA)

Advanced Threat Analytics is an intrusion detection solution (IDS) specifically built for Active Directory. It uses machine learning and behavior analytics to detect abnormal behaviors in the Active Directory, alerting users of possible breaches and threats. This technology allows our clients to detect intrusions in real time before significant damage can occur.

AZURE ACTIVE DIRECTORY B2B COLLABORATION

Azure Active Directory (Azure AD) B2B collaboration enables organizations to partner more effectively with others by inviting trusted external users to access certain internal resources. As with all Azure AD products, access can be secured, altered, and revoked as required. In industries where collaboration is a fundamental requirement, this tool greatly improves efficiency and communication between organizations.

AZURE ACTIVE DIRECTORY B2C

A key advancement for online service delivery applications, Azure Active Directory B2C enables organizations to connect with consumers in a highly scalable way. Organizations using Azure AD B2C can offer external users the ability to sign in to services using social accounts with all authentications and account information managed securely in the cloud.

AZURE ACTIVE DIRECTORY IDENTITY PROTECTION

Azure Active Directory Identity Protection is a feature of the Azure AD Premium that provides a consolidated view into risk events and potentially vulnerable corporate identities. It uses a number of factors to determine user risk levels and enables risk-based conditional access policies and other security policies.

AZURE INFORMATION PROTECTION (FORMERLY RMS)

Azure Information Protection (formerly RMS) protects emails, documents, and sensitive data inside the company and once it leaves company walls. Using manual and automatic classification, organizations can encrypt sensitive data and define usage rights, tracking what happens to documents when they are used inside the organization or shared with external users.

MICROSOFT CLOUD APPLICATION SECURITY (CAS)

Cloud Application Security (CAS) enables IT teams to take control of the shadow IT phenomenon. It also secures corporate resources by discovering cloud apps used in their network, assessing risk, and controlling data sharing. This is a powerful tool for data loss prevention and threat protection.

MICROSOFT ENTERPRISE MOBILITY + SECURITY (EMS)

Enterprise Mobility + Security is a digital transformation tool that combines the latest and most powerful Microsoft technologies for identity & access management, enterprise mobility, and identity driven security. It allows organizations to effectively and securely control identity and access to the cloud, manage mobile devices and apps, protect information, and virtualize desktops.

MICROSOFT IDENTITY MANAGER (MIM), FORMERLY FIM

Microsoft Identity Manager (MIM) simplifies on-premises identity management and enables IT teams to cut costs by introducing automations, workflow rules, and self-service capabilities. This technology also automatically prepares active directory identities for synchronization to the cloud in hybrid scenarios.

MICROSOFT INTUNE

Microsoft Intune provides mobile applications management and mobile device management, enabling BYOD scenarios, access to industry and in-house applications, MFA, and conditional access for added security.

OFFICE 365

Office 365 enables organizational productivity from anywhere. It offers a comprehensive set of Microsoft Office tools available in the cloud and optimized for collaboration, availability, and security.

WINDOWS 10 SECURITY

Windows 10 features a number of security layers that protect your organization using a flexible framework of technologies. These technologies include Windows Hello and credential guard, Bitlocker, Trusted Platform Module, and Windows Defender. Windows 10 features support biometric authentication and the ability to join directly with Azure AD.

Microsoft Partner

Microsoft

Gold Cloud Productivity
Gold Identity and Access
Gold Cloud Platform
Gold Enterprise Mobility Management

1-844-996-9695 • info@avaleris.com • **www.avaleris.com**

OTTAWA • CALGARY • TORONTO • NEW YORK