Microsoft

CIO's guide to Azure Active Directory

Identity and Access Management as a Service boosts organizational effectiveness

Executive summary

Being an effective Chief Information Officer (CIO) in a modern, global business world is not simply about managing an efficient department that delivers on its service level agreement (SLA); increasingly, your function is to be the driver and enabler of current and future revenue streams. You must be a proactive provider, who can anticipate the company's long-term direction. You also work as a peer with your senior leadership colleagues to open up new avenues to growth and make a quantifiable contribution to the organization's mission. Microsoft Azure Active Directory, the Identity and Access Management as a Service (IDaaS) component of the Enterprise Mobility and Security Suite, accelerates the rate at which you can achieve this ambition. It gives secure and productive access to the applications your users need to do their jobs, both now and in the future.

Azure Active Directory extends your on-premises directories into the cloud, providing a truly global identity and access management solution that delivers effective, secure and modern IT services. It releases you from the constraints of on-premises directory services to provide global reach and secure user access to vital data. It also integrates line-of-business apps into multidevice, multiplatform environments that deliver fully realized IT agility, while controlling costs and enforcing security.

This guide explains how to make Azure Active Directory a central part of your IT strategy. You will review the priorities of your CIO peers and consider how they plan, or have already have embarked on, this innovative strategic direction. Having read this white paper, you will appreciate how updating and modernizing your identity and access management services better prepares your organization for the next wave of IT modernization. This proactive approach ensures that your organization remains at the forefront of technology and maximizes the flexibility and cost reduction benefits of cloud-enabled identity and access management.

Identifying the challenges that CIOs face today

Information Technology (IT) is a major contributor to the rate of change within the world. IT not only enables change in almost any endeavor to take place more quickly, but also accelerates the development of the very technologies which, in turn, generate further change. Consequently, the role of CIO within most organizations has been transformed, from that of primarily providing a supporting service, to being an integral and essential part of how a company delivers value to its customers.

"There is nothing permanent except change."

Heraclitus (c. 535-475 BC)

Forrester recently completed a survey[1] of 1,087 business decision makers and influencers around the world to identify the top technology management organizational priorities for enterprise customers who are dealing with rapid rates of change. Figure 1 shows the top five findings from this study, which all point to the need to respond effectively to this challenge.

Technology Management Priorities

Base: Security Technology Purchase Influencers

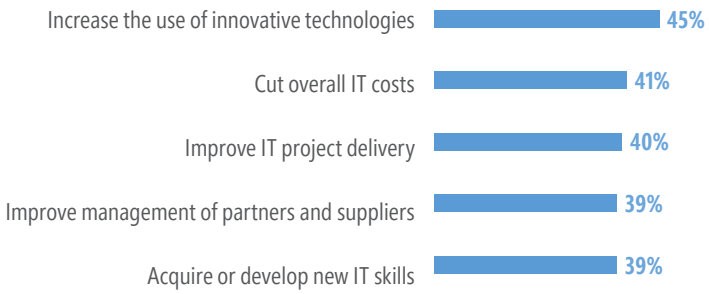

Figure 1: Top technology management priorities for CIOs

Increase the use of innovative technologies

In today's business world, a CIO needs to be so much more than a technologist. You must have a keen appreciation of how to use technology to empower your business and be able to add value incrementally in all areas of operation. You have to respond to customer needs and show return on investment within weeks, not years. You appreciate that securing the business is a factor in all areas of IT operations and you will need additional security capabilities that are as agile as your new services.

Cut overall IT costs

Today's ever-growing IT expenditure is driven by a range of factors that increase risk and keep costs high. These factors include:

- The rising cost and availability of specific expertise.
- The number of discrete services you are developing and managing.
- The cost of securing these separate systems.

[1] Forrester Data Business Technographics® Global Priorities & Journey Survey 2016

- The cost of compliance associated with these services.
- The manual processes associated with outdated approaches.

To address these challenges, you need to investigate emerging cloud solutions, architectures and IT patterns that give you back control and reduce costs, while still generating growth and protecting the company.

Improve IT project delivery

Today, you no longer have the luxury of taking the time to stop and plan multiyear projects to evolve your IT infrastructure. Technology that you may have identified as being of value at the scoping phase might have been completely superseded by the time you arrive at the implementation phase. Increasingly, you need greater IT agility, where the approach is to focus on incremental steps, gain quick wins and reap business benefit—then repeat until you have evolved your IT architecture to a modern, configurable, low maintenance, secure, and auditable system.

Improve management of partners and suppliers

Modern companies thrive by successfully utilizing a partner ecosystem and supply chain that helps the company to expand quickly and address new business opportunities without having to recruit new employees. Secure collaboration with your organization's partners and suppliers is key to running a successful and productive business, while at the same time reducing risk. The rapid changes in your partner and suppliers' businesses now require a more flexible and fluid way to maintain secure access to the resources that encourage effective collaboration.

Acquire or develop new IT skills

Your company workforce is changing rapidly in line with global trends. More than ever, IT departments need to respond instantly to customer demands. End users in your company expect you to offer services that are up-to-date and have similar usage patterns to the modern mobile applications with which they have become very familiar and take for granted. Within your department, it is becoming increasingly harder to find talented staff who are interested in working on what is perceived as legacy infrastructure.

Aim

The aim of this paper is to explain how Microsoft Azure Active Directory can address the top five CIO priorities identified in the recent Forrester study. This paper also shows how Azure Active Directory (AD) can help with other challenges that affect modern IT environments.

Answering CIO challenges with Azure Active Directory

Azure AD is Microsoft's Identity and Access Management as a Service (IDaaS) offering for organizations of all sizes. Companies without on-premises Active Directory can use it as their main identity and access management resource; those with Active Directory or other directories already deployed can connect their current infrastructure and

synchronize identity attributes into the cloud. Any app that you deploy can then connect to your instance of Azure AD for secure single sign-on and use that information to boost employee productivity, enhance partner working, build customer relations, and maximize sales.

Figure 2 shows the relative importance of being able to stream identity information throughout an organization. More than half of CIOs reported that this ability was a high priority for adoption.

Streamlining Employee Identity and Access Management to Applications, Systems, and Data Across the Organization

Sample Size = 2,320

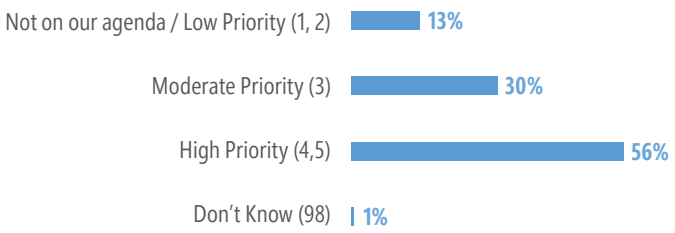

Figure 2: Priority levels for streaming employee identities across organizations

Increase the use of innovative technology

The proliferation of Software as a Service (SaaS) applications of all types offers organizations a range of innovative new technologies that can enhance productivity. However, this growth also brings the challenge of easily providing these new technologies to your end users in ways with which they will most benefit. Ninety percent of CIOs report that upgrading or simplifying the user experience is a key concern; usefully, Azure AD addresses this issue by enabling timely and controlled application roll-outs across your user community. "Keeping it simple" is the key mantra for making life easier for your users—the following Azure AD features contribute towards this goal:

- **Single sign-on to cloud and on-premises apps from one screen.** Azure AD offloads the complexity of maintaining multiple app accounts—users connect to all their productivity apps with just one authentication dialog.
  The result: less time spent logging on and greater output from your workforce.
- **End user application launcher and self-service portal (MyApps) available for every platform.** In addition to the MyApps feature on the Windows and Windows Phone platforms, users have access to thousands of productivity apps on Apple and Google platforms.
  The result: greater flexibility for your workforce, particularly in BYOD environments.
- **Application SSO seamlessly integrated with Office 365.** Single sign-on to all of your cloud and on-premises applications is available directly within Office 365.

Risks from Employee-Provisioned Applications are a concern for 81% of organizations [2]

The result: employees have all of their applications at their fingertips, making them easier to use and increasing productivity.

- **Cloud App Discovery.** Identify the risk related to employee provisioned application—sometimes called "shadow IT". See the later section in this paper for further discussion of this topic.

Cut overall IT costs

Self-service capabilities in Azure Active Directory also provide new approaches for simplifying the user experience and reducing overall IT costs. A key benefit with Azure Active Directory is the control it passes back to your users, while also reducing the load on your helpdesk. Unnecessary time spent on the phone talking to helpdesk personnel is entirely unproductive, so this single change can have immediate and quantifiable financial effects on your organization. In a cloud-enabled world where disruptive technologies and business models pop up with increasing regularity, having a modern IT environment is a competitive necessity. The following features provide compelling returns on investment:

- **Self-service password reset, change and unlock for both on-premises and the cloud.** Password resets, changing passwords, and unlocking accounts together consume by far the largest proportion of helpdesk time. Using Azure Active Directory, users now reset their own passwords, change those passwords when prompted or unlock accounts—all without a single helpdesk call.
  The result: more productive users and a helpdesk able to concentrate on the real technical issues.

- **Self-service application addition.** With this feature, managers no longer have to contact the IT department to obtain and publish applications. If a department head finds an off-the-shelf application that meets a specific business need, they can purchase it, put it onto the company portal, and make it available for installation by staff in that department.
  The result: fewer reasons for departments to operate a shadow IT function and reduced costs from application rollout.

- **Self-service group management.** Self-service group management helps users to create and add themselves to groups, again without intervention from the IT department. You delegate group management powers to departments and users to ensure that group creation is driven by the people who need those groups the most—the users.
  The result: greater group manageability at lower cost.

- **Self-service application access management.** Departments use self-service application access management to control who can and who cannot access their applications. Most powerful of all is the ability to use identity attributes to control that access; for example, you configure settings so that only users who have the value for the department field set to "Human Resources" can access the company HR app. If they move to another business unit, changing the department field value instantly removes access to the HR apps but grants access to the new department's apps.
  The result: reduced costs and consistent control over access to company applications.

91% of Security Technology Decision Makers believe that the adoption of an as-a-service security offering is important or very important to support a large number of mobile and remote users [2]

- **Compatibility with all platforms supporting BYOD.** Use Azure AD to lower the cost of integrating non-Windows platforms and users' own devices (BYOD). Through device registration, users enjoy the benefits of BYOD while retaining control of their own devices. The result: users gain the flexibility of working with the device they know best and non-Windows platforms are securely integrated within your identity environment.

Improve IT project delivery

In pre-cloud days, it was standard practice for organizations to look at replacing their infrastructure every three to five years. Today, SaaS productivity applications, such as Microsoft Office 365, are fast to deploy; yet critical applications, such as ERP, might remain on-premises for longer. Azure AD provides your hybrid infrastructure with several options to remove or reduce the size and consequent cost of your next infrastructure refresh cycle, while still providing access to existing on-premises applications.

- **Azure AD Application Proxy.** Azure AD Application Proxy hugely simplifies the process of publishing internal applications on the Internet and provides secure remote access to those applications. Application Proxy now supports Remote Desktop, and complex network and non-Windows applications using Kerberos over Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO), in addition to custom domain names, conditional access policies and Windows Intune Network Device Enrolment Service (NDES). This support is particularly useful for Intune and System Center Configuration Management (SCCM) deployments.
  The result: you can make almost anything you publish inside your network available to your mobile users and office-based staff around the world.

- **Azure Active Directory Domain Services.** You use Azure Active Directory Domain Services to migrate your existing on-premises directory-aware applications to Azure without having to worry about identity requirements.
  The result: there is no need to deploy domain controllers as Azure virtual machines, or use a VPN connection to connect to your identity infrastructure.

- **Azure Active Directory Connect.** You use the Azure AD Connect tool to integrate your on-premises identity system—such as Windows Server Active Directory with Azure Active Directory—and connect your users to Office 365, Azure and thousands of SaaS applications published through Azure. This tool enhances productivity by creating a common identity for your users to access on-premises and cloud-based resources.
  The result: simpler identity management, greater accessibility, and increased productivity.

- **Azure Active Directory Connect Health.** You use Azure Active Directory Connect Health to monitor your on-premises identity infrastructure and check the synchronization services available through Azure AD Connect. You can view alerts, system performance, usage patterns, and configuration settings, ensuring a consistent connection to Microsoft Azure, Office 365, and much more.
  The result: a more reliable on-premises Active Directory and better connectivity to Microsoft Azure Active Directory.

- **Azure Active Directory Join.** As Azure Active Directory extends your on-premises Active Directory to the cloud, Azure Active Directory Join provides the ability for Windows 10 client computers to join a domain, either one entirely hosted in Azure, or one that uses a hybrid architecture. Additionally, Azure Active Directory Join supports self-provisioning of corporate devices, signing-on with organizational accounts, and SSO access to cloud-based and on-premises resources.
  The result: better integration with your identity store and easier access to productivity resources wherever they are stored.

Improve management of employees, partners and suppliers

Your organization will benefit from a single, unified and consistent view of all the users who need to access your organization's applications. This view should include not only employees and contractors, but also individuals from other companies, such as supply chain partners. Azure AD provides the interconnection to popular HR applications and simplifies the process of giving secure access to individuals outside your organization through the following features:

63% of security Technology decision makers have deployed or plan to deploy a B2B Federated Single Sign on solution for partner access in the next 12 months [2]

- **HR App integration.** Azure AD interacts with a large and increasing range of applications that fully integrate with this cloud-based identity store. For example, when you onboard a new employee into Workday, Azure AD makes it simple to automate the provisioning of that user, and grants them access to the key resources that they need for their role. This approach provides a true cloud-based and modern human resources service that seamlessly connects to your company. When users leave the company, the same automation can ensure efficient de-provisioning.
  The result: easier user management and improved security.

- **Azure Active Directory B2B collaboration.** You use Azure Active Directory B2B collaboration to access your corporate applications using identities that represent partner organizations. You generate the required federation relationships, and then grant permissions to access resources on your network to specific users from each partner. If an individual leaves the partner company, access is automatically revoked. Additionally, if the partnership agreement is terminated, nobody from that company can connect.
  The result: better partner integration with no requirement to manage external accounts.

- **Dynamic membership groups.** Dynamic membership groups use identity attributes to assign users to groups. Rather than a manager specifically needing to request membership for an employee or that employee having to add themselves to a group, changing a user's attribute in Azure AD is enough to automatically add them to a specific group. For example, if you have a department group called Marketing, you would set up a rule so that, if a user's department field value is equal to "Marketing", then that user is added to the Marketing group without further intervention. Similarly, if that user changes to another team within the company, they are immediately removed from the Marketing group.
  The result: accurate and automatic control of group memberships across multiple groups, reflecting a modern and dynamic approach to IT.

- **Provisioning and de-provisioning.** Azure AD automates the process of provisioning and de-provisioning users. Any changes to user accounts, attributes or group membership results in automated provisioning of those accounts or dynamic de-provisioning of access to resources.
  The result: more accurate control over your user base, a tighter security profile, and faster access for your users.
- **Company branding.** Azure AD accepts a range of company branding options, starting with the initial SSO logon page. Instead of generic colors or imagery, you can put a picture of your company headquarters where users enter their user name and password. This feature provides a strong corporate identity that gently welcomes employees back to their organization.
  The result: your organization presents a unified and modern appearance to the world that engenders confidence in customers, suppliers, partners, and employees.
- **Azure AD B2C.** Azure AD B2C provides a toolkit that helps your developers to identity-enable consumer-facing applications quickly and easily, and without writing additional code. This toolkit consists of a secure, standards-based platform and a rich set of extensible policies that simplify the process of designing, creating, deploying, and supporting identity-enabled applications that engage with your customers—all without requiring custom code or on-premises account storage.
  The result: developers can release applications more quickly and customers can purchase your products more easily.

A consumer IAM solution is something that 71% of security technology decision makers have, want to expand or are considering implementing [2]

Acquire or develop new IT skills

As CIO, you are committed not just to keeping your current IT environment up to date, but also to providing users with new capabilities that ensure your organization stays competitive. As this paper has highlighted, these Azure AD capabilities can enhance your current service lineup or generate new and exciting opportunities to engage better with customers.

But what of the effects on your staff? Implementing a cloud-based IDaaS solution with the advanced security and protection capabilities of Azure AD gives your team the opportunity to work with the latest IT architectures and technology. Gartner's Magic Quadrant (MQ) analysis of Identity and Access Management as a Service for 2016 named Microsoft as a leader, and the company with the most complete vision, in this space. By adopting Azure AD, your IT department will be working with visionary methods and implementations that are pioneering changes within the identity and security arena.

Giving your team the opportunity to work with these technologies will ensure that they stay current with the latest industry developments and remain fulfilled in their roles. Importantly, developing your people and equipping them with the latest technological skills in this way not only improves employee loyalty, but also demonstrates that you have the leadership skills for further advancement within your organization.

Going beyond the top five concerns

You doubtless have additional concerns over and above those covered in this paper so far—such as security, shadow IT, and auditing and reporting facilities. The identity and access management features of Microsoft's cloud-based services help protect business and personal information from unauthorized access. However, legitimate users take advantage of the simple and easy-to-use features that provide stronger authentication and access controls. In particular, Azure AD has several options that provide greater security and visibility to simplify meeting audit controls and objectives, without the penalty of reduced productivity. This final section discusses these features.

Improve your security position

No self-respecting CIO would ever play fast and loose with security. But security always comes at a cost—and that cost is often usability. Striking the balance between security and usability is a growing problem. Your organization needs to have a good grasp of identity and access management principles to achieve the right level of protection without hampering productivity.

88% of the polled security technology decision makers implemented changes to their strategy and observed impact in their business as a result of security breaches occuring in the past 12 months [2]

The vast majority of security breaches take place when attackers steal a user's identity. This theft could be through passwords revealed in third-party breaches, or through sophisticated phishing attacks. Regardless of how a security breach starts, attackers then look for opportunities to expand their reach across the organization. Users who hold on to unnecessary or uncontrolled privileges expose the organization to these external, as well as internal, attacks. The following features in Azure AD help guard against these intrusions:

- **Multi-Factor Authentication (MFA).** Azure MFA helps protect access to data and applications while meeting your users' demands for a simple sign-in process. Azure MFA delivers strong authentication with a range of verification options, such as a phone call, a text message or a mobile app notification—allowing users to select the method they prefer.
  The result: better security without additional complexity for users.

81% of security technology decision makers in the forrester survey are interested in or have implemented Multifactor authentication [2]

- **Advanced security reports and alerts.** Advanced security reports and alerts protect your environment by employing machine-based learning that helps you gain new insights into improving your access security and respond more rapidly to potential threats. This feature works by monitoring user activity and flagging anomalies and patterns of inconsistent access.
  The result: greater levels of data and access protection without having to wade through vast amounts of error logs.

- **Automatic password rollover for group accounts.** Group accounts for social media services ensure that multiple users can update newsfeeds on social media platforms. However, the very nature of these accounts makes them potential targets for attackers—a defamatory tweet or Facebook post could have huge consequences, even affecting stock valuations of the company. With automatic password rollover, you can set and change social media account passwords for multiple users on platforms such as Facebook, Twitter, and LinkedIn. The account password is stored

in encrypted form in Azure AD—the user does not know the password itself. Every time the password needs changing, that process is handled automatically, using a randomly generated strong password.
The result: greater ease of use for your social media team and reduced risk of account compromise for your company.

- **Conditional Access.** You use Azure Active Directory Conditional Access to control who can access applications and data, even in BYOD environments. This means you can give all your registered users access to most content but only allow devices that are compliant with company policy to access specific resources. Finally, you can entirely disallow access from lost, stolen, or non-compliant devices.
The result: user-owned devices can be integrated into your security environment without creating additional risk to your organization.

- **Privileged Identity Management (PIM).** You can use PIM in Azure AD to manage, control and monitor privileged identities (such as administrators for Office 365 Exchange or SharePoint Online) and discover what these individuals are up to. This monitoring is necessary in case a user account with privileged access is compromised; an attacker who has those privileges would impact the organization's overall cloud security. With PIM, you can enable "just-in-time" privileged access to Azure AD and connected applications, and generate reports on when administrators use their privileges.
The result: better control and monitoring of what your administrators are doing.

- **Azure Active Directory Identity Protection.** Azure Active Directory Identity Protection provides a consolidated view of suspicious sign-in activity and potential vulnerabilities. It generates notifications, recommends remediation, and applies risk-based policies to help protect your business. The service works by detecting suspicious activities for user and privileged (admin) identities, based on activities such as brute force attacks, leaked credentials, sign-ins from unfamiliar locations, and infected devices—protecting against these activities in real time. More importantly, it calculates a user risk severity level, based on these suspicious activities. You can then configure risk-based policies that automatically protect your user identities from future threats.
The result: you can have confidence that your identities are being properly protected.

51 % of security technology decision makers have already implemented or expanding a PIM solution and 19% are planning to in the next 12 months [2]

43% of surveyed security technolgy decision makers estimate that their sensitive data was compromised at least once in the past 12 months [2]

Address shadow IT

Shadow IT can be a pernicious threat, as it comes into the category of "unknown unknowns"—if you don't know which applications are using your organization's data and where that data resides, you won't know who has access and whether that access is appropriate. Shadow IT can also be utilized as an attack vector by cyber criminals who introduce unregulated applications into your environment. It is therefore essential to provide consistency across applications and, should a user's identity be compromised, proactively prevent the compromised identity from being abused.

Industry studies have found that many departments and individuals within your company are probably using one or more unregulated SaaS applications. Azure AD helps address the issue of unauthorized applications in the following way:

- **Cloud App Discovery.** Cloud App Discovery in Azure AD helps you identify the applications that your company is using, often undetected. Use this feature to bring these rogue apps under IT management so they are made available through a single cloud-accessible company portal.
  The result: employees don't have to look elsewhere for the applications they need to do their jobs and managers don't have to run a shadow IT department.

Meet reporting and audit requirements

Finally, Azure AD gives you the capability to meet demanding reporting and auditing requirements, ensuring the appropriate amount of security granularity at the right level. Azure AD includes several options that simplify meeting audit controls and objectives, without the penalty of reduced productivity. The features that provide this capability are as follows:

- **Advanced security reports.** As previously mentioned, advanced security reporting includes anomaly reports, which identify activities that are considered out of the ordinary. Azure AD makes you aware of these types of activity and helps you determine whether or not an event is suspicious.
  The result: even non-standard attacks will show up in your security reports.
- **Usage reports.** Usage reports generate information on what your users are doing, such as changing their passwords, and logging on or logging off, along with their IP address, location, client device, and application usage.
  The result: you can keep track of user activities globally to identify how they are using Azure AD and the applications that you publish.
- **Reporting Application Programming Interface (API).** Azure AD includes a fully-featured Reporting API that consists of a set of REST APIs. You use REST APIs to access and display data in Azure AD reports through a variety of tools and programming languages, including C# and PowerShell. You then return this data in a number of formats, such as Extensible Markup Language (XML), JavaScript Object Notation (JSON), and text.
  The result: your developers can customize their reports and ensure that they deliver the right information from backroom to boardroom.

Risk-based or Context-based authentication is an IAM Service that 69% of surveyed security technolgy decision makers already have or plan to adopt in the next 12 months [2]

Summary

There is no denying the importance and the challenging nature of the CIO's role in the modern business world. Microsoft Azure Active Directory is one of the key cloud solutions that will help you achieve your goals and successfully deploy important IT initiatives during. With Azure AD, you will drive growth, empower users, cut costs and maintain appropriate levels of security within your organization, while making a positive contribution to overall growth at a strategic level.

Next steps

To find out more about how Microsoft Azure Active Directory can help your organization to continue to grow in a global marketplace, go to microsoft.com/identity and click "**Try Now**". It could be the best executive decision you make today.

[2] Forrester Data Business Technographics® Global Global Security Survey 2015