CONNECT MORE APPS TO MICROSOFT AZURE ACTIVE DIRECTORY (AZURE AD) WITH PINGACCESS
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>03</td>
</tr>
<tr>
<td>ENSURE ACCESS WHILE MITIGATING RISK</td>
<td>04</td>
</tr>
<tr>
<td>WHY YOUR WAM WON’T WORK</td>
<td>04</td>
</tr>
<tr>
<td>SUPPORTING MOBILITY WITH MICROSOFT AZURE AD</td>
<td>05</td>
</tr>
<tr>
<td>CONNECT ON-PREMISES APPS WITH APPLICATION PROXY</td>
<td>06</td>
</tr>
<tr>
<td>CONNECT TO EVEN MORE APPS USING PINGACCESS</td>
<td>07</td>
</tr>
<tr>
<td>PINGACCESS SUPPORTS YOUR DIGITAL TRANSFORMATION</td>
<td>09</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>09</td>
</tr>
</tbody>
</table>
INTRODUCTION

Mobility has evolved significantly since its humble beginnings. Once defined as simply providing and supporting company smartphones, mobility today is seen as a strategic business enabler.

There’s no denying the enterprise landscape has changed. Your users want and need to work without boundaries. They've experienced the freedom of SaaS apps and want this same accessibility to all of the apps they work with. To support them, you must ensure all your users have instant access to the applications and data they need to get the job done, at any time and from any location. But access is about much more than convenience.

According to Apperian's 2016 Executive Enterprise Mobility Report, “Custom apps save people time, improve productivity, make employees’ work easier, and in some instances create revenue-producing opportunities and a competitive advantage.” In fact, improved business processes and improved productivity are the top two benefits of enterprise mobility, as cited by 53% of their respondents.

But embracing a mobile-first, cloud-first world doesn’t come without its challenges. Enterprises face new security risks and vulnerabilities as they adopt cloud and mobile technology. The average number of applications per enterprise is growing, but most of them are not enterprise-ready. And the budget to support digital transformation isn’t growing proportionately to the need.

CONSIDER THE FACTS:

- Of the average 935 apps per enterprise, 94.6% of them are not enterprise ready
- 77% of respondents are now adopting private cloud (up from 63% last year), driving the use of hybrid cloud environments to 71%
- Gartner predicts that 2016 global IT spending will remain flat year-over-year

Despite these realities, standing still isn’t an option. Mobility is the new normal, and you need to find new ways to support it. Further, the benefits to your enterprise of adopting cloud technology far outweigh the potential downsides.

In this paper, we’ll demonstrate how you can use an identity-based architecture to support enterprise mobility. You’ll learn how using Microsoft Azure Active Directory (Azure AD) with Application Proxy provides the access you need to both cloud and on-premises applications. You’ll discover how PingAccess extends your access to even more on-premises applications using standards-based access management. By the end, you’ll have gained a deeper understanding of how an identity strategy centered on Microsoft Azure AD and PingAccess enables you to provide the secure and seamless access and freedom your users expect and demand.
ENSURE ACCESS WHILE MITIGATING RISK

When it comes to enterprise mobility, you must balance your need for data protection with your users’ need for seamless access. A successful mobility strategy will embrace the following principles:

- Deliver seamless and secure access to all applications, while protecting against threats.
- Maximize productivity by allowing employees to work without borders.
- Connect everything in your enterprise, from cloud to mobile, to on-premises technologies and web apps.

These are tricky to accomplish when you have apps that reside in the cloud, while other mission-critical apps are still on-premises where your existing infrastructure and current IAM likely are. Add to that a mobile workforce using a mix of managed and unmanaged devices, and connecting everything with policy and governance oversight can feel like an unsolvable puzzle.

WHY YOUR WAM WON’T WORK

Historically, organizations relied on firewalls and invested heavily in WAM-based products to protect and allow access to applications. This worked fine for web apps, but legacy WAM solutions pre-date mobile and cloud. They weren’t built to extend beyond the firewall, and they rely on outdated and proprietary tokens and protocols.

You can try to rework your WAM system to address your enterprise mobility challenges, but it’s prohibitively costly, laborious and inefficient at best. Plus, it offers no intelligent protection mechanisms and only limited support for the rich level of access users demand today. In an interconnected world where users are location-independent, you must modernize your access management to address governance and security needs.
Identity can be thought of as the new perimeter in today’s virtual, mobile and software-defined world. As the core of enterprise mobility, identity goes way beyond protecting your data with a firewall and outdated passwords to protecting data everywhere that it’s used.

Azure Active Directory (Azure AD) is Microsoft’s multi-tenant cloud-based directory and identity management service. It provides an easy-to-use solution to give employees and business partners single sign-on (SSO) access to thousands of cloud-based SaaS applications like Office365, Salesforce.com, Box and ServiceNow.

Built for ease of use, Azure AD delivers advanced identity protection through security reports, audits and alerts. It offers adaptive conditional access policies based on device health, user location and risk level, as well as machine learning backed intelligence. And if you’re an application developer, Azure AD lets you focus on building your application by making it fast and simple to integrate with a world-class identity management solution.

IDaaS is already a staple of enterprise identity strategy. And more and more enterprises are looking to Azure AD as their single identity source. Each day, there are 1.3 billion user authentications against Azure AD. This number will only get larger as more enterprises move identities to the cloud.

**IDENTITY AS THE CORE OF ENTERPRISE MOBILITY**

*Figure 1. Microsoft Azure Active Directory acts as the core of enterprise mobility bridging the gap between cloud and on-premises applications and resources.*
As enterprises increasingly rely on Azure Active Directory, they want the ability to authenticate users and provide single sign-on to cloud and SaaS apps, but still need access to on-premises apps. Azure AD Application Proxy helps you support your mobile workforce by publishing on-premises applications to be accessed over the internet.

Providing access to on-premises applications has traditionally involved setting up virtual private networks (VPNs), demilitarized zones (DMZs) or on-premises reverse proxies. Not only are these solutions complex and hard to secure, they are costly to set up and manage.

Azure AD Application Proxy provides SSO and secure remote access for web applications hosted on-premises. This can include SharePoint sites, Outlook Web Access or any other line-of-business web applications you have. These on-premises web applications are integrated with Azure AD, allowing end users to access your on-premises applications the same way they access Office 365 and other integrated SaaS apps. You don’t need to change the network infrastructure or require VPN to provide this solution for your users.

With Azure AD Application Proxy you can access different types of internal applications:
- Web applications that use Integrated Windows Authentication for authentication
- Web applications that use form-based access
- Web APIs that you want to expose to rich applications on different devices
- Applications hosted behind a Remote Desktop Gateway

Application Proxy works by installing a slim Windows Server service called a connector inside your network. When users access applications remotely, they connect to the published endpoint. Users authenticate in Azure AD and then are routed through the connector to the on-premises application as shown in Figure 2.
There are a whole host of legacy on-premises applications that aren’t easily accessible via Microsoft Azure AD, even with Azure AD Application Proxy. These apps typically use HTTP header-based authentication brokered through a legacy WAM system. PingAccess working with Azure AD Application Proxy can help integrate these apps with the Azure AD control plane. These apps would need to be significantly modified to allow a secure, seamless connection. Unless you use Azure AD with PingAccess.

If you want to provide SSO to a broader spectrum of on-premises applications through Azure AD, PingAccess can serve as the gateway to those mission-critical legacy applications. PingAccess integrates with Azure AD Application Proxy, so you can use a single, Azure AD-connected identity to access on-premises web apps. PingAccess allows the provision of SSO and secure remote access to header-based, on-premises web applications from any device in any location through Azure AD, without the need for VPN.

**HOW IT WORKS**

PingAccess is a software component that installs quickly and easily on-premises. It can also be installed in an IaaS environment to protect legacy applications hosted in popular cloud environments like Azure and AWS. PingAccess extends the reach of Azure AD Application Proxy to provide SSO and access to a host of on-premises web applications through a process called HTTP header injection.

As users request resources protected by PingAccess, Azure AD Application Proxy routes those requests to the PingAccess server. PingAccess then needs to check if an SSO session is active or not. If a session is not active, PingAccess redirects back to Azure AD for user authentication. Azure AD returns an OpenID Connect (OIDC) token to PingAccess. PingAccess uses the OIDC token containing claims and user attributes and places the appropriate attributes in the HTTP request header that the application can leverage for managing access.
This last step shows the real power and benefit of PingAccess. Organizations can SSO-enable legacy, on-premises applications without heavyweight or time-consuming modifications to these applications. This method utilizes the latest standards in identity, allowing secure access to web applications that many times pre-date these standards.

Here's another quick view of how this flow works:

Authentication and Access Flow Use Case
1. User makes application request (attempts to access on prem app) and Azure AD Application Proxy routes request to PingAccess.
2. PingAccess checks for existence of active web session.
3. PingAccess redirects to Azure AD for SSO authentication. User signs on via Azure AD. Since the user would’ve already signed on, they’ll get SSO. Azure AD will issue a token for PingAccess.
4. Browser is redirected back to PingAccess with OIDC token which PingAccess validates.
5. PingAccess session is created and access is granted.
6. Application request is forwarded to the protected application with identity information in HTTP request header.

This approach to providing Azure AD-based authentication and SSO for on-premises enterprise applications has been proven to work very well for a wide variety of web applications running on Apache, IBM, NGINX and many other web servers. It provides instant, secure access for users from any device and any location without cumbersome VPN connections. In addition, many applications can be connected rapidly with no changes required.
PINGACCESS SUPPORTS YOUR DIGITAL TRANSFORMATION

PingAccess for Azure AD is a critical step toward connecting all users to all applications with SSO and secure remote access, and delivering on productivity, one-identity and do-more-with-less goals. It also puts you squarely on the path of digital transformation.

PingAccess is a proven enterprise solution for WAM modernization and migration, advanced contextual access management, and migrating your enterprise apps to the cloud without security concerns.

CONCLUSION

Microsoft Azure AD plus PingAccess enables enterprise mobility, enhances user productivity, and ensures secure remote access to legacy on-premises applications, all without the need for VPN.

Based 100% on open standards, it gives your enterprise the power to move applications to the cloud and gain increased security without additional risk. By employing Microsoft Azure AD plus Ping Access as part of an identity-centric strategy, you'll simultaneously mitigate the risks of cloud and mobile migration, while enabling—even accelerating—your digital transformation.

To learn more, visit pingidentity.com