SOLUTION OVERVIEW

F5 BIG-IP APM and Azure Active Directory Conditional Access

Integrating F5 BIG-IP APM's Identity Aware Proxy (IAP) with Azure AD Conditional Access enables fine-grained, adaptable, zero trust access to any application, regardless of location and authentication method, with continuous monitoring and verification.

KEY BENEFITS

Secures wherever, whenever productivity
Empowers users to be productive wherever and whenever through simple, seamless access to cloud-based and custom/classic apps if policy conditions are met and upheld.

Diminishes app access risk
Leverages real-time and calculated risk detection with Azure Active Directory Identity Protection to substantially mitigate access risks.

Simplifies user experience (UX)
Centralizes user authentication, alleviating separate user authentication methods for cloud-based apps and classic/custom applications.

Streamlines administrative experience
Leverages a single, easy-to-use interface to onboard apps and define Azure AD Conditional Access policies through BIG-IP APM's Access Guided Configuration (AGC).

Work from Anywhere Plus Hybrid Access = A Security Nightmare

Corporate users have always required anywhere, anytime access to applications, whether they're working from home, at a coffee shop, or on the go. And while the supporting technology has been available for decades, it has been cumbersome to use and implement.

Many organizations now want to allow corporate users to work from anywhere at all times to enable a better work-life balance—from alleviating lengthy commute times to permitting people to reside wherever they want. Technological advances and the drive for digital transformation have paved the way for this new hybrid work world where employees can be productive from anywhere, and organizations can cut costs by consolidating or even closing physical locations.

With corporate users more readily able and approved to work from anywhere, organizations and their security teams face increasing pressure to balance the need for stringent remote access security with a seamless user experience. Corporate resources can be hosted in the cloud as native cloud apps or as a service, on-premises in a data center, or in a private cloud. The fact that corporate resources, and particularly applications, can be hosted just about anywhere has sealed the fate of the tried-and-true network perimeter.

However, many mission-critical applications—like classic and custom applications—are not cloud migratable. Many of these apps do not or cannot support modern authentication standards and protocols such as Secure Access Markup Language (SAML) or OIDC / OAuth. They probably can't support identity federation and single sign-on (SSO) access or multi-factor authentication (MFA), either. As a result, your organization will need to manage multiple user authentication methods, while corporate users must remember numerous credentials and use various forms of authentication to access the applications they need to be productive. It's a complicated, confusing experience for users, a huge headache for SecOps and admins, and a source of rapidly rising support costs for your organization.

APPLICATIONS AND USER ACCESS TO THEM WILL NEED TO REMAIN HYBRID FOR SOME TIME, CREATING A "PERFECT STORM" FOR ACCESS AND SECURITY, WHILE POSING A SECURITY NIGHTMARE FOR SECOPS TEAMS.

For these reasons, applications and user access will need to remain hybrid for a while with some apps in the public cloud as native cloud or SaaS apps, and other apps on-premises, in a data center, or in a private cloud. This creates a "perfect storm" for access and security, while posing a security nightmare for SecOps teams.

As many organizations begin to explore and deploy a zero trust architecture across all their applications and data, regardless of where they reside, this perfect storm creates a dangerous access and security situation that isn't easy to address. Hybrid access is going to be the new norm.

Today's organizations need a way to enable simple, secure corporate user access to all applications, regardless of where they're hosted. This would improve user experience, prevent security catastrophes, and decrease SecOps and admin headaches.

Enhancing and Extending Zero Trust Application Access

BIG-IP APM INTEGRATES WITH AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS TO ENABLE EVEN GREATER GRANULAR ZERO TRUST APPLICATION ACCESS.

F5® BIG-IP® Access Policy Manager® (APM) is a secure, highly-scalable access management proxy solution that enables centralized global access control for users, devices, applications, and APIs. Azure Active Directory (AD) is Microsoft's widely deployed, comprehensive, cloud-based identity and access management platform.

Together, BIG-IP APM and Azure Active Directory empower simple, seamless, secure access to all applications, regardless of where they're hosted or where the user is located. BIG-IP APM and Azure Active Directory combine to significantly improve your user experience and drastically reduce application and data access security risks. Users can securely access all applications they're authorized to access, whether the application supports modern authentication standards and protocols or classic authentication methods, such as Kerberos or header-based methods.

BIG-IP APM and Azure Active Directory also address a major challenge for organizations exploring or deploying a zero trust architecture: that is, how to ensure zero trust access to any application, regardless of its location or authentication method. Deployed together, BIG-IP APM and Azure Active Directory ensure zero trust application access, through BIG-IP APM's identity- and context-aware per-application request access policies and its continuous monitoring of user device security and context-related parameters, including location, network condition, and more.

BIG-IP APM also integrates with Azure Active Directory Conditional Access to enable even more granular zero trust application access. Azure Active Directory Conditional Access is a tool that Azure Active Directory uses to bring signals together to help make decisions and enforce organizational policies, and it applies the appropriate access controls when necessary to keep your organization secure. When making a policy decision, there are several common signals that Azure Active Directory Conditional Access can consider, including:

- User or group membership targeted to specific users and groups, allowing fine-grained access control
- IP location information, to create and use trusted IP address ranges when making policy decisions
- Devices from specific platforms or those marked with a specific state

KEY FEATURES

Continuous monitoring and assessment
Continuously monitor and assess device security integrity, user identity, and adherence to role-based access control (RBAC) and attribute-based access control (ABAC).

Enhances zero trust application access
Protect assets by applying additional, new access controls as needed to ensure even greater granular application and data security.

Identifies and mitigates login risks
Integrates with Azure Active Directory Identity Protection to identify risky sign-in behaviors, forcing password changes or MFA, or blocking access.

Trusted IP address ranges
IP location information allows you to create and use trusted IP address ranges when making policy decisions.

- Specific application access attempts
- Real-time and calculated risk detection that integrates with Azure Active Directory Identity Protection to identify risky sign-in behavior, force password changes or MFA, or block access until manual action is taken
- Real time monitoring and control of user application access and sessions by Microsoft Defender for Cloud Apps

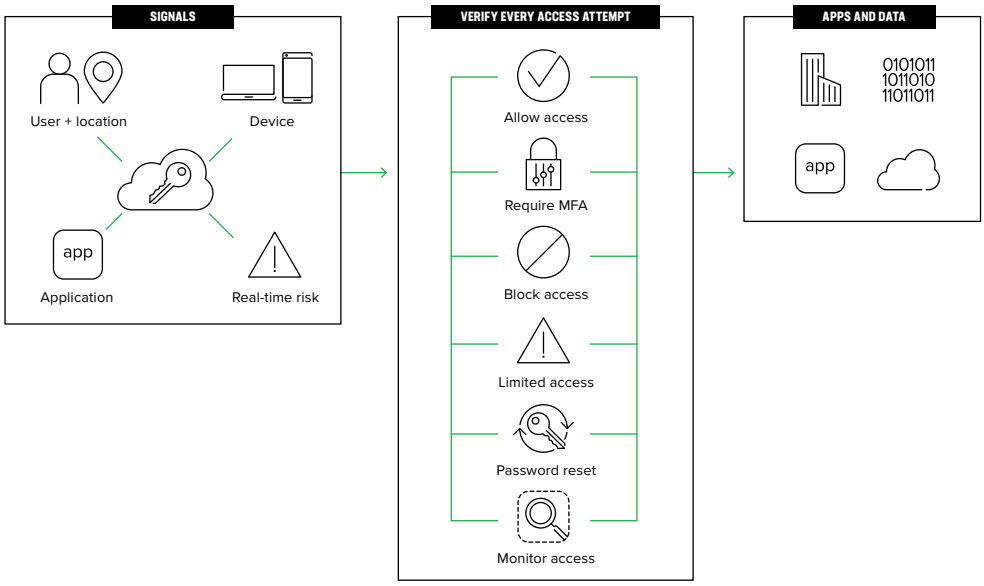

Figure 1: Azure Active Directory Conditional Access

Based on those signals, a decision is made to either allow, grant, or block user access. Combining BIG-IP APM and Azure AD Conditional Access extends the signals gathered by Azure AD Conditional Access to be applied to access for web and SaaS applications, and legacy and custom applications typically found on-premises, in a data center, or private cloud.

By integrating BIG-IP APM and Azure Active Directory, your organization can:

- **Continuously monitor and assess** user devices to ensure they meet a minimum bar of security, user identity, and user application access based on context, location, and other security parameters
- **Leverage a single and easy-to-use interface to onboard your legacy apps**, as well as deploy Azure AD Conditional Access policies leveraging BIG-IP APM's Access Guided Configuration (AGC)

- **Empower users to be productive wherever and whenever** with simple and seamless access to cloud-based and custom/classic apps if conditions and policies set by their administrator in either or both BIG-IP APM and Azure AD Conditional Access are met and upheld
- **Centralize user authentication**, alleviating the need for separate authentication methods for cloud-based apps and other methods for classic/custom applications
- **Protect your assets** by applying additional, appropriate access controls when needed to keep applications and data secure—granting user access only on a per-app request basis

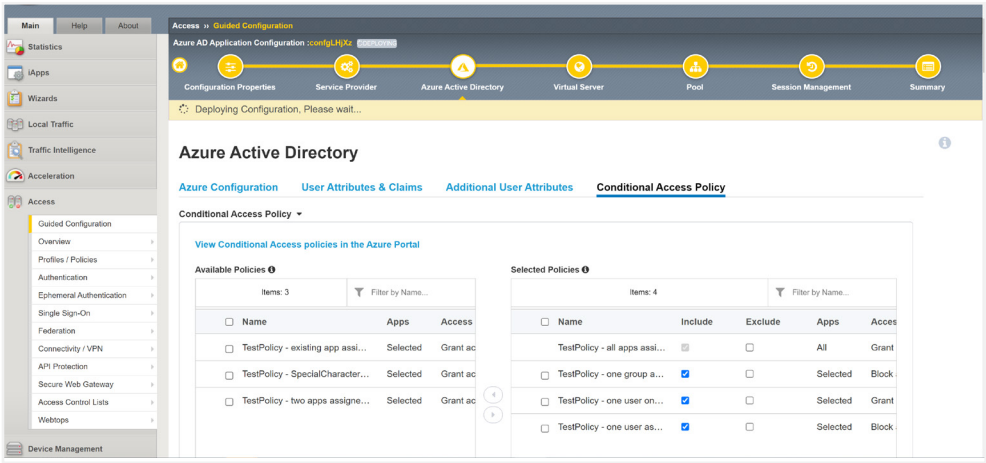

Figure 2: Integrating Azure Active Directory Conditional Access with BIG-IP APM in the Access Guided Configuration (AGC) enhances zero trust app access and streamlines administration.

Conclusion

F5 and Microsoft continue to deliver best-of-breed, integrated solutions for adopting and adapting zero trust across all your applications.

Integrating BIG-IP Access Policy Manager and Azure Active Directory, including Azure AD Conditional Access, solves the challenges and relieves the headaches posed by today's work from anywhere and hybrid business environment. Together, they not only enable secure access to any app hosted anywhere, but also ensure, extend, and enhance zero trust application access.

Learn how F5 products and solutions can help you to achieve your goals. Contact F5.