Extend Access Management Through Azure Active Directory

Applications are a proven tool to deliver efficiencies to the modern business, and there's an obvious trend of larger companies deploying more apps over time. According to Okta, companies have increased their total app usage by 68% in the past four years, which underscores the vital need for seamless and secure application access.[1]

KEY BENEFITS

Enhance User Productivity
Enable users to access all necessary apps without frustration—even those not supporting modern authentication such as SAML, OpenID Connect (OIDC) and Open Authorization (OAuth).

Increase App Security
Obfuscating individual application authZ/N from the user means users have fewer passwords to remember and a reduced threat surface for attackers.

Reduce Costs
Quickly and easily deploy and manage access through the guided configuration, which reduces management overhead and cost.

Now, applications can live anywhere: in the cloud, in a data center, as a service, or on a mobile device. No longer does a user need to be in a specific place and on a specific network to access applications and be productive. Today's users can work from anywhere.

That's great for user and corporate productivity. But how can organizations ensure quick, easy, and secure access to applications that can reside anywhere and be accessed from anywhere, at any time?

The Challenge

While organizations migrate their existing applications to the cloud—or replace them with SaaS applications—there are still many applications that cannot be moved to the cloud or easily replaced. Securing and simplifying access to applications in hybrid environments—like an organization that has cloud-based Infrastructure as a Service (IaaS) applications as well as on-premises or custom applications to which users require access—is a difficult puzzle to solve. It's also a costly one. Plus, it can negatively affect the user experience, especially if users are forced to authenticate numerous times to gain application access. To solve this problem, many organizations are moving to cloud-based Identity as a Service (IDaaS) solutions.

IDaaS solutions, like Microsoft Azure Active Directory (Azure AD), simplify user access to cloud-based and as-a-Service applications, and can add another layer of protection against the scourge of security issues such as credential theft and abuse. However, hybrid applications (IaaS or on-premises applications) can complicate application authentication and authorization via IDaaS, particularly if those apps don't support the modern authentication and authorization standards and protocols leveraged by IDaaS solutions.

ORGANIZATIONS NEED A SOLUTION THAT SECURES, SIMPLIFIES, AND CENTRALIZES ACCESS TO ALL APPLICATIONS, REGARDLESS OF WHERE THEY RESIDE AND WHETHER OR NOT THEY SUPPORT MODERN AUTHENTICATION AND AUTHORIZATION METHODS.

Organizations need a solution that secures, simplifies, and centralizes access to all applications, regardless of where they reside and whether or not they support modern authentication and authorization methods. Application access must be seamless, secure, and simple. It must include extending access to applications unable to support today's single sign-on (SSO) protocols, while leveraging existing, well-known directory services to deliver Zero Trust application access and a safe, effortless access experience.

The Solution

F5® BIG-IP® Access Policy Manager® (APM) securely and simply integrates with Azure AD to expand application SSO, streamline deployment and management of application access, and enhance security and the user experience. BIG-IP APM federates user identity, authentication, and authorization, bridging the identity gap between cloud-based IaaS, SaaS, and on-premises applications.

THIS APPLICATION-LEVEL ACCESS CONTROL ALLOWS REQUESTS FOR APPLICATION ACCESS TO BE REVIEWED, AUTHORIZED, OR TERMINATED BASED ON PRESCRIPTIVE POLICIES.

Azure AD delivers a root of trusted identity, and together with the F5 APM Identity Aware Proxy, they enable user and device authentication with authorization to the applications users are allowed access. Leveraging powerful, context-aware policy management, BIG-IP APM extends granular application access control to Microsoft's Azure Active Directory users. This application-level access control allows requests for application access to be reviewed, authorized, or terminated based on prescriptive policies.

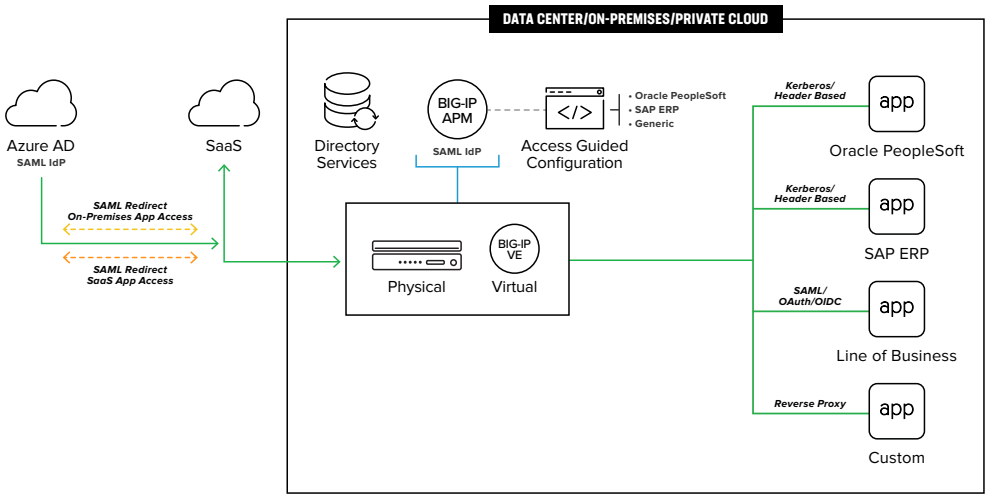

Figure 1: F5 BIG-IP APM and Azure AD work seamlessly together to deliver support for modern authentication and authorization protocols such as SAML, OIDC, and OAuth.

A BETTER USER EXPERIENCE

Together, BIG-IP APM and Azure AD simplify application access and deliver a better user experience by centralizing application access. The combined solution enables users to log in once and access all appropriate applications they are authorized to access—no matter where those applications are hosted—from a single location. This reduces frustration and enables users to be more productive.

THE COMBINED SOLUTION ENABLES USERS TO LOG IN ONCE AND ACCESS ALL APPROPRIATE APPLICATIONS THEY ARE AUTHORIZED TO ACCESS—NO MATTER WHERE THOSE APPLICATIONS ARE HOSTED—FROM A SINGLE LOCATION.

ENHANCED SECURITY

Centralizing user authentication to applications diminishes an organization's threat landscape, including scenarios such as credential stuffing or unauthorized access after a phishing attack. By focusing security controls in one place with the combined F5 and Microsoft solution, multi-factor authentication (MFA) options can be presented to the user when applicable and device security posture can be analyzed on a per-request basis through context-aware policies. This is particularly important for classic and custom applications that previously could not or would not support these types of security controls.

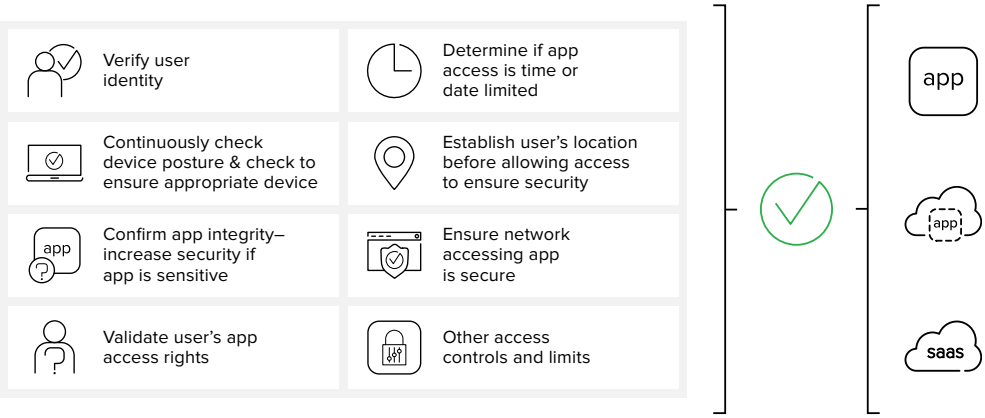

Figure 2: Context-aware policies enforce conditional app access.

DECREASED MANAGEMENT OVERHEAD AND COMPLEXITY

With a single interface for policy control across all apps, the Access Guided Configuration (AGC) for BIG-IP APM centralizes authentication, simplifies deployment and management of application access, and eases the administrative experience. AGC also enables Azure AD administrators to quickly onboard and manage classic, mission-critical applications such as SAP ERP and Oracle PeopleSoft. Since each of these classic apps requires its own access configuration, administrators traditionally had to separately configure access to their SAP applications, their Oracle applications, and every other classic or custom app—often even creating unique configurations from one version to the next.

AGC DRASTICALLY REDUCES CONFIGURATION COMPLEXITY WHEN COMPARED TO OTHER SOLUTIONS.

Using AGC, the administrator can provide basic information across a straightforward, easy-to-navigate series of inputs. This capability in AGC drastically reduces configuration complexity when compared to other solutions. Once the guided process is complete and the administrator has clicked the “deploy” button, the application is available to the appropriate users.

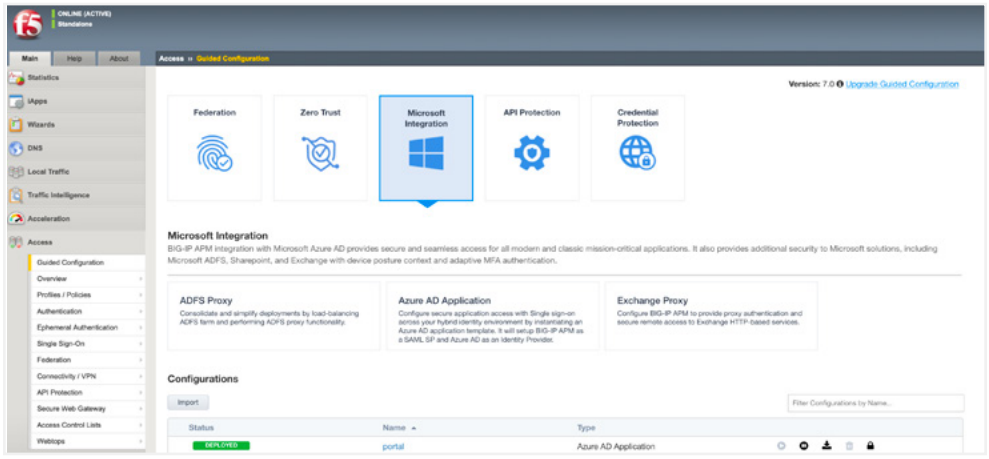

Figure 3: F5 BIG-IP APM offers AGC to greatly ease the process of onboarding and managing classic and custom apps, including SAP ERP and Oracle PeopleSoft.

Conclusion

With today’s applications located on premises and across private and public clouds, enterprises need a solution that secures, simplifies, and centralizes access to all of their applications—cloud native, SaaS, classic, and custom. They also need to extend access to applications unable to support today’s SSO protocols and MFA, while delivering Zero Trust application access and an effortless user experience. Using BIG-IP APM and Microsoft Azure AD together, organizations can ensure seamless, trusted access to all of their applications—dramatically improving the experience for both users and administrators.

To learn more, explore F5 Access Control and Authorization solutions or contact your F5 representative.

[1] Okta 2019 Business @ Work report, found at https://www.okta.com/businesses-at-work/2019

OV-300SP | JOB-CODE-605386732