F5 ACCESS POLICY MANAGER AND MICROSOFT AZURE ACTIVE DIRECTORY

Applications are everywhere because they are a proven tool to deliver efficiencies to the modern business. Consider how many applications you access in any given day. Then multiply that by the number of people in your organization, and then by every organization in the world, and you can see how vital access to applications is.

Applications can also now live anywhere: in the cloud; in a data center; as a service; on a mobile device. Accessing and using applications can be done from anywhere, at any time. No longer does a user need to be in a specific place, on a specific network to access applications to do their job and be productive. Today's users are able to work from anywhere.

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

CHALLENGES

While organizations migrate their existing applications to the cloud, or are replacing 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 (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.

SECURING AND SIMPLIFYING ACCESS TO APPLICATIONS IN HYBRID ENVIRONMENTS–LIKE AN ORGANIZATION THAT HAS CLOUD-BASED (IAAS) APPLICATIONS AS WELL AS ON-PREMISES OR CUSTOM APPLICATIONS TO WHICH USERS REQUIRE ACCESS–IS A DIFFICULT PUZZLE TO SOLVE.

IDaaS simplifies user application 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. However, hybrid applications (IaaS or on-premises applications) can complicate application authentication and authorization via IDaaS, particularly if they 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. 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.

SOLUTION

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

Microsoft's Azure Active Directory and F5's APM, working in concert, simplify user experience for application access, enabling users to log in once and access all applications from a single location, regardless of where the applications reside—cloud-based (IaaS), as-a-service, or on-premises.

When deployed together, APM enables access security and SSO and extends Azure Active Directory's federation and security capabilities to all applications, including applications that do not support modern authentication and authorization protocols; for instance, applications that leverage header-based or Kerberos. This solves a costly challenge for organizations worldwide and an access nightmare for users, while directly addressing an executive-level risk management concern. As organizations connect APM to Azure Active Directory, organizations can apply advanced security capabilities such as Azure AD Conditional Access and provide end users password-less authentication to all applications.

Migrating or spinning up new applications in the cloud is a time-consuming and costly undertaking. It can be daunting for an organization to migrate all of their existing applications to the cloud, while attempting to launch new SaaS-based applications, and substituting as-a-service solutions for other applications. But, APM, working with Azure Active Directory, can ease on premises application migration to the cloud. Instead of migrating all applications simultaneously, an integrated F5 APM and Azure Active Directory solution enables an organization to take a measured approach to migrating applications to the cloud, delivering cost-savings, allowing them to learn as they migrate, and potentially saving them many headaches. Leveraging the ability of an integrated APM and Azure Active Directory solution to enable user access to applications wherever they may be located allows organizations to take a more systematic approach to application cloud migration.

F5's APM is an identity-aware proxy (IAP), providing authenticated and authorized secure access via Azure Active Directory to specific applications, regardless of their location. F5's APM integrates with Microsoft's Azure Active Directory, which delivers a root of trusted identity. Together, they enable authentication of users and their devices and authorization to the applications they are allowed access. Leveraging powerful context-aware policy management, F5's 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. F5's APM and Microsoft's Azure Active Directory, when deployed together, are powerful allies integrating trusted identity and application within zero-trust architectures.

F5's and Microsoft's Azure Active Directory work seamlessly together to deliver support for modern authentication and authorization protocols such as SAML, OAuth, and OpenID Connect (OIDC). The combined solution enables delegated authentication and authorization capabilities. The configuration of F5 as a service provider or resource server in front of applications providing access to on-premises applications and Azure Active Directory as the authorization server, enables application programming interfaces (APIs), native applications, and mobile applications to delegate authorization functions to a trusted party, eliminating the complexity and cost of implementing discrete systems.