Overview

A Myth Busters Guide to Secure Cloud Access

Prevent unwanted access to your digital assets

With F5 and AWS you can enforce zero trust access for users, APIs, and apps—without impacting performance. Secure critical systems and data with stringent authentication and authorization protocols for centralized and consistent protections across AWS and other environments.

Learn more at **f5.com** or find F5 Distributed Cloud Services on **AWS Marketplace**.

Managing access policies across hybrid and multicloud deployments can be complex. To keep systems and data safe, today's businesses need a more secure and centralized approach to preventing unwanted access to cloud, on-premises, and edge environments.

Let's debunk some common industry myths and explore ways to implement more effective access policies across your application estate.

Myth #1

Zero trust is a mindset, not a reality.

Truth: Zero trust methodologies are tangible and improve organizational security postures by employing a never-trust, always-verify approach to privileged user access. F5® BIG-IP® Access Policy Manager® (APM), combined with AWS native identity and access management policies, helps deliver upon zero trust strategies with fine-grained authentication and authorization protocols that prevent unwanted access to data centers, AWS instances, and other cloud services.

Myth #2

User access controls introduce friction.

Truth: Ensuring safe and federated user access can, and should, be a seamless experience. F5 protects user access to AWS and other applications with a frictionless, context-aware and identity-aware approach. Single sign-on (SSO), multi-factor authentication (MFA), geolocation restrictions, and device inspection ensure a secure, user-friendly experience broadly across applications and regions. This eliminates the need to manage independent user accounts in each cloud, regardless of where users or applications are located or hosted.

Myth #3

Access policies can't apply to APIs.

Truth: APIs are a leading vector for cyberattacks and need proper access policies to remain secure. AWS API Gateways bolster protections with flexible and robust access controls that can be applied to an entire API or individual methods within AWS. F5® Distributed Cloud Services further extend these native API defenses with centralized authentication protocols that reduce configuration complexity and enforce zero trust access for API layers in AWS and other environments.

DC 08.2024 | JOB-CODE-1470825575

aws PARTNER