SOLUTION OVERVIEW

Cisco Duo and F5 BIG-IP APM: Partners for Anywhere, Anytime Zero Trust Access

Today many companies just like yours are embracing a work-from-anywhere policy. And that requires secure, verified workforce access from anywhere and by any device without introducing unnecessary complexity—complexity that can frustrate users and make it harder for them to effectively and efficiently do their jobs.

KEY BENEFITS

Enhance secure application access
Access to any application is secured via multi-factor authentication (MFA) and single sign-on (SSO).

Reduce costs and mistakes
Eliminates redundant tasks and limits human errors.

Meet compliance requirements
Secures application and resource access for highly regulated businesses.

KEY FEATURES

Seamless zero trust experience
Ensures secure zero trust application access to all apps for all users.

Simple, protected SSO
Simplifies access to any app, regardless of location or authentication, and is especially beneficial in hybrid application environments.

Dynamic, adaptive, and customizable access control policies
Create and apply policies across applications and environments for uniform or custom application access and security.

Today, Trust-But-Verify Security Isn't Good Enough

The ability for employees to work from anywhere helps drive workforce diversification. But it also means different types of devices will likely be used to access corporate resources, like applications, data, and more.

It's vital that your organization rapidly deploys and scales trust-based access to all applications, regardless of where they're located—cloud or on-premises. This needs to happen no matter which authentication method applications support, modern or classic. Point being, only the right authorized users, with trusted, verified devices should be able to access the resources they need to be productive.

The concept of network perimeter security and its "castle and moat" approach worked for many years because users, their devices, and resources, including applications and data, were typically housed within a corporate network. The organization provided endpoints to users and managed those endpoints. The corporate network was protected by firewalls and other perimeter security devices, ensuring intruders were locked out of the castle walls and its protected resources.

Users who were trusted and had the appropriate credentials, usually a username and password, were allowed inside the walls. And once a user was trusted and allowed entry, they'd be able to reach any resources they were authorized to access. This castle and moat security approach followed the motto "trust, but verify."

Then came the cloud and cloud applications.

Organizations quickly realized the cloud was safe and secure. They also realized the cloud and apps in the cloud, like SaaS and native cloud apps, helped alleviate the costs they'd incurred for years for servers and storage as they built protected data centers within the network perimeters.

The shift to remote work also accelerated the use of cloud applications, because users needed to work from anywhere and access authorized resources anytime to be able to do their work.

The double whammy of cloud migration and the sudden, expansive growth of the remote workforce meant the death knell for the castle and moat security approach. Users are using devices not provided or managed by their organization (think bring your own device, or BYOD) to access authorized resources located virtually anywhere. Today's organizations can't assume that just because a user is within the perimeter, they can be trusted, and their device deemed secure. Trust but verify-based security isn't good enough anymore.

What Does Zero Trust Mean for Your Organization?

Today, organizations are making the switch to zero trust security. Zero trust eliminates the idea of a trusted network inside a defined perimeter. It shifts the secure perimeter to anywhere from which access is requested. Then comes the decision point. Should the user be granted access? How much?

Zero trust questions the assumption of trust each time access is requested. It also requires the implementation of least-privilege access. Organizations need to scrutinize access to applications and resources wherever they're located as much as possible.

IT'S VITAL THAT YOUR ORGANIZATION RAPIDLY DEPLOYS AND SCALES TRUST-BASED ACCESS TO ALL APPLICATIONS, REGARDLESS OF WHERE THEY'RE LOCATED—CLOUD OR ON-PREMISES. THIS NEEDS TO HAPPEN NO MATTER WHICH AUTHENTICATION METHOD YOUR ORGANIZATION SUPPORTS, MODERN OR CLASSIC.

User identity, access context, and visibility are fundamental control points for a zero trust environment. Visibility informs policy. And the intelligence and insight that flow from visibility drive informed access policy decisions across an organization. Trust is continuously verified by reassessing device posture and user identity as determined by the organization.

NEVER TRUST, ALWAYS VERIFY

Organizations should assume attackers are already lurking on their network, just waiting for the right moment or trigger to launch an attack. This may seem grim, but it aligns with what today's security priorities require. The new security mantra is "never trust, always verify."

That means never trust users, even if they've been authorized and granted access to a resource. Always verify user identity, device security and integrity, location, and other contextual parameters for each application they try to access. And monitor context continually until the user closes the app.

"Continuously monitor" should actually be a part of the zero trust motto. A root of trusted identity is imperative. The user's identity, as determined by the organization, must constantly be reasserted. Trust is verified by continuous reassessment of device posture and integrity. If a user's device fails posture and integrity checks, the user's resource access must be halted immediately.

Hybrid environments—where applications and resources are available in the cloud, on-premises, or anywhere in between—will be commonplace for some time. You have to manage secure access for hybrid environments by validating and protecting access to all applications and networks, including those you don't own or manage, like SaaS and the public cloud.

HOW THE F5 AND CISCO DUO PARTNERSHIP MAKES ZERO TRUST EASIER—ON EVERYONE

F5 and Duo (now part of Cisco) are partnering to bring your organization and users a seamless zero trust approach for anywhere, anytime application and resource access.

Duo verifies user identity and establishes trust through easy and secure multi-factor authentication (MFA) with the broadest range of multi-factor options available. Duo's MFA options include mobile push, biometrics, security keys, one-time passwords (OTP), and more. Duo protects against stolen credentials, phishing, and other identity-based attacks. Through its secure MFA, Duo ensures access to applications and resources is only granted to trusted individuals and devices.

F5, through its BIG-IP Access Policy Manager (APM) full-proxy application access gateway, delivers secure application access services to apps and resources located anywhere—in the public cloud as cloud-native or SaaS apps, in a private cloud, on-premises, or in a data center. F5 and BIG-IP APM empower organizations to embrace the infrastructure they choose or need without sacrificing speed and control.

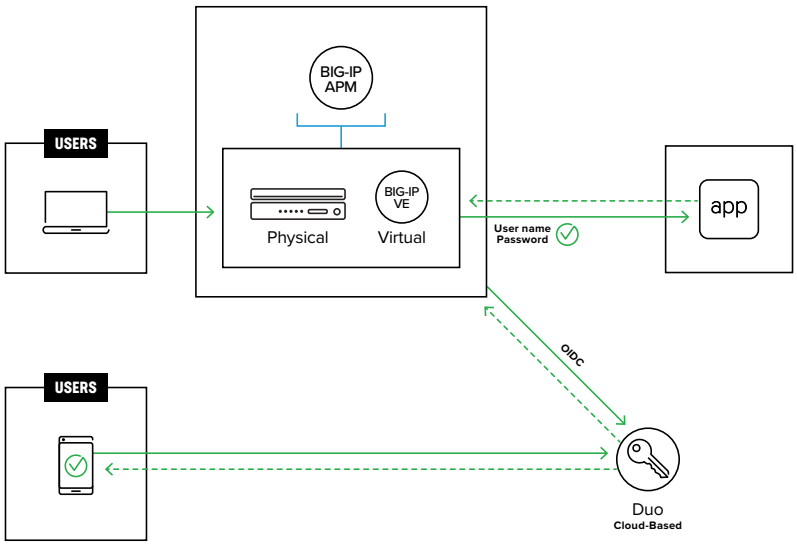
WHEN DEPLOYED TOGETHER, DUO AND F5 BIG-IP APM HELP ORGANIZATIONS DEPLOY AND ATTAIN ZERO TRUST PROTECTION FOR THEIR WORKFORCE AND RESOURCES.

When deployed together, Duo and F5 BIG-IP APM help organizations deploy and attain zero trust protection for their workforce and resources. The joint solution enables organizations to easily deploy a seamless, robust zero trust experience for all users, regardless of location or type of user (employee, contractor, vendor, and so on).

Access to any application, regardless of where it's located or form of authentication, is simple and protected via single sign-on (SSO). SSO is especially beneficial in hybrid application environments, enhancing the user experience by decreasing logins, and credentials needed, to a single set. Dynamic, adaptive, and customized access control policies can be created and applied across applications and environments, ensuring either uniform or customized application access and security, whichever an organization requires.

This solution also lets you reduce user enrollment and remediation costs by removing redundant tasks, as well as limiting opportunities for human error. Deploying the joint F5 BIG-IP APM and Duo solution also helps your organizations to meet industry and government compliance requirements for secure application and resource access in highly regulated industries, including healthcare, financial services, education, and government.

Figure 1: F5 BIG-IP APM configures and supports Duo multi-function authentication (MFA) through the OIDC authentication protocol.



USE DUO AND F5'S ADAPTIVE ACCESS POLICIES TO QUICKLY DETERMINE AND ENFORCE THE RIGHT LEVEL OF AUTHENTICATION AND ACCESS FOR EACH UNIQUE USE CASE.

Conclusion

Now, adopting and deploying a zero trust approach to security for your organization doesn't require a complete retooling of your infrastructure. To be successful, zero trust initiatives should start with solutions that can augment, work with, and support your hybrid environment without ripping and replacing existing investments.

F5 and Duo enable your organization to quickly and easily leverage their strengths individually and collectively. You can utilize Duo and F5's adaptive access policies to quickly determine and enforce the right level of authentication and access for each unique use case.

Together, F5 and Duo deliver context-based access controls so only the right users are able to access the right applications and resources at the right time, with the right device, with the right configuration, and from the right place.

Learn more about the Duo and F5 BIG-IP APM integration