SOLUTION OVERVIEW

SIMPLE AND SECURE ACCESS TO LEGACY ENTERPRISE APPLICATIONS

VMWARE WORKSPACE ONE AND F5 BIG-IP

The rapid adoption rate of digital workspace services enables a growing number of users to gain easy access to the most critical enterprise applications—from any device, from anywhere, and at any time. But not all enterprise applications are ready to move into the digital age just yet. While today's users spend much of their time on modern applications, such as Web-based or native mobile applications like Salesforce or Office 365, there is still a need for them to access legacy applications using Kerberos Constrained Delegation (KCD) or header-based authentication.

F5 Networks and VMware have collaborated in order to make these legacy applications accessible to today's workforce in a simple and secure fashion.

Solution Overview

IT departments using legacy applications have a need to provide a secure solution for end-users that enables secure access, while providing customized security policies based on the type of access device. With VMware Workspace ONE™ and F5 BIG-IP® Access Policy Manager® (APM), customers can achieve the following benefits:

Single Sign-On to Legacy Applications

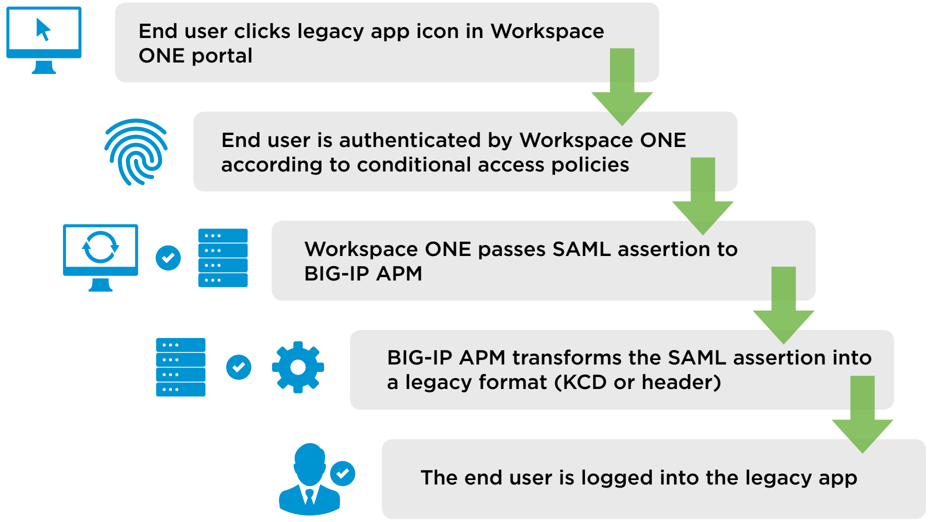
These users do not want to re-enter their credentials (username and password) when switching from a modern-day application to a legacy application. Since many of these legacy applications require authentication methods such as Kerberos, providing a smooth, single sign-on experience to users can be challenging. BIG-IP APM and Workspace ONE make it possible for users to have single sign-on (SSO) access into the most common applications, on- or off-premises.

Powerful policies that reduce risk of unauthorized access and data loss

End-users today have multiple devices whether they be phones, tablets, laptops or desktops running a variety of operating systems.

KEY HIGHLIGHTS

- Single sign-on to legacy applications, for a seamless user experience
- Powerful policies that reduce risk of unauthorized access and data loss
- Integrated multi-factor authentication for increased security



End user clicks legacy app icon in Workspace ONE portal

End user is authenticated by Workspace ONE according to conditional access policies

Workspace ONE passes SAML assertion to BIG-IP APM

BIG-IP APM transforms the SAML assertion into a legacy format (KCD or header)

The end user is logged into the legacy app

These end-users expect that they can be productive on any of those devices, including accessing legacy applications to perform work. This trend requires that organizations have the right controls in place to reduce the risk of unauthorized access and data loss. With Workspace ONE and F5, organizations can enforce access decisions based on a range of conditions from strength of authentication, network, location and device compliance. Additionally, organizations can restrict access from rooted or jailbroken devices.

Integrated multi-factor authentication for increased security

Enterprises today are concerned with the adoption of legacy multi-factor authentication solutions. These solutions are often cumbersome and difficult to use. There is a need for a more modern, low-cost and user-friendly method of strong authentication. Workspace ONE includes VMware Verify, a mobile-push multi-factor authentication solutions that is secure and easy to use. With VMware Verify, organizations can optionally require two-factor authentication when end users access any app, including legacy apps. Two-factor authentication approval is just one swipe away using mobile push notifications.

Summary

For enterprises interested in offering the most seamless single sign-on experience for their users—from cloud and web applications to traditional, on-premises legacy applications—F5 and VMware have the solution. By combining industry leading products from both companies, enterprises can take advantage of the highest scalability, security, and performance while end users enjoy all the benefits of a modern, digital workspace.

For more information on F5 BIG-IP and VMware Identity Manager, visit f5.com/vmware or vmware.com/partners/global-alliances/f5.

About F5

F5 Networks is the global leader in Application Delivery Networking. The company's hardware, software, and virtual solutions help organizations address the relentless growth of voice, data, and video traffic to better support mobile workers and applications—in the data center, the network, and the cloud. F5's extensible architecture provides application optimization, protection for applications and the network, and enhanced application reliability. The world's largest businesses, service providers, government entities, and consumer brands rely on F5's intelligent services framework to deliver and secure their applications and services while ensuring people stay connected. The company is headquartered in Seattle, Washington with offices worldwide. Visit us at https://www.f5.com.

About VMware

VMware is a global leader in cloud infrastructure and business mobility. Built on VMware's industry-leading virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant and more secure. Customers can innovate faster by rapidly developing, automatically delivering and more safely consuming any application. With 2014 revenues of $6 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com