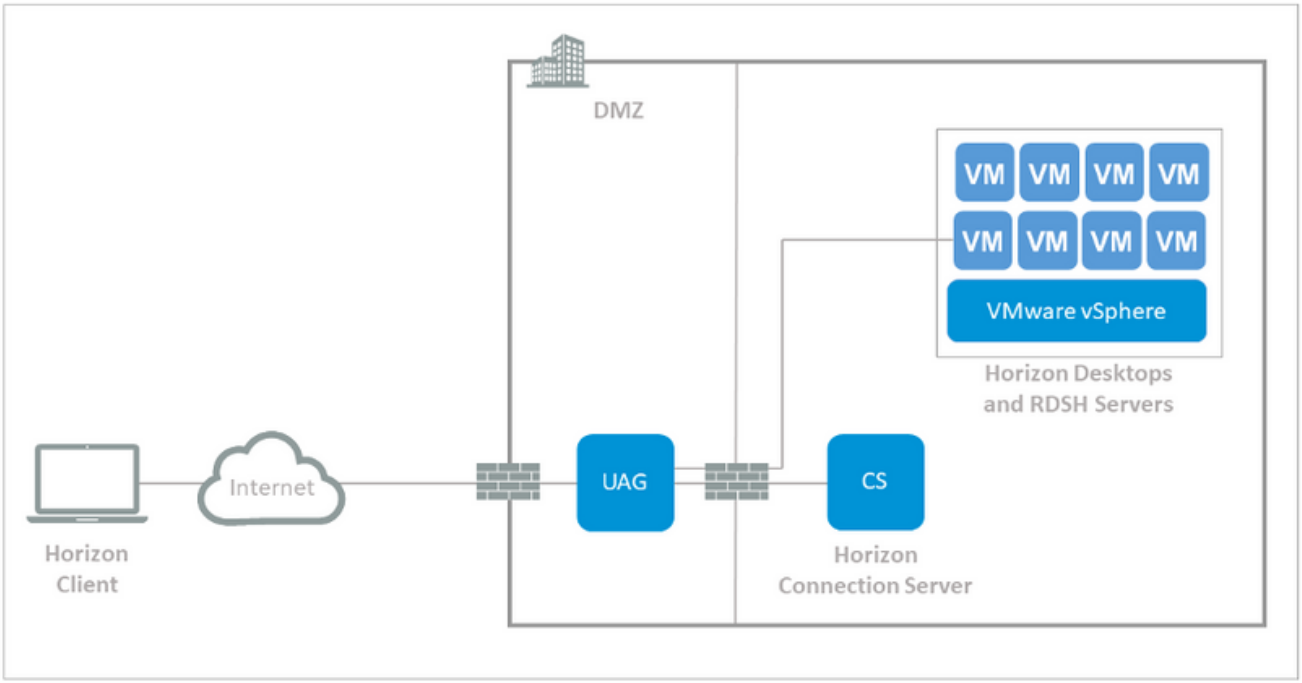
TraitWare - VMWare Horizon Use Case

Introduction

TraitWare protects VMWare Horizon environments by providing simple, secure Passwordless Multi-Factor Authentication (MFA) for end users. TraitWare accomplishes this by integrating with the VMWare Unified Access Gateway (UAG) within the Horizon deployment. The VMWare UAG allows secure remote access to a VMWare Horizon environment by users from inside and outside of the corporate network. The goal of the end customer was to enable MFA and Passwordless authentication for users inside the office, remote users, Horizon clients, and web clients.

Figure 1. Standard VMWare Horizon Configuration



VMWare Horizon - Customer Overview

The customer is a medium-sized Federal Credit Union, subject to the rules and regulations of the financial industry. The customer chose to use VMWare Horizon's VDI solution to reduce the risk of data exfiltration, to apply consistent security policies to Windows 10 desktops, and to simplify the procurement of workforce hardware.

TraitWare integrated into the VMWare UAG using the SAML 2.0 standard. When a user signs into the Horizon Client or web browser, the request is forwarded to TraitWare for authentication. TraitWare presents the user with a QR code using the TraitWare app on the user's mobile device and the user is signed into Horizon in 3 touches! The user is never required to enter a username, password or One Time Passcode (OTP). The user employs biometric authentication, a secure token, and a complex OTP - by merely opening an app and scanning a QR code.

Figure 2. TraitWare-enabled Horizon environment