Adaptive Security Manager™
Legacy Application Security Solution

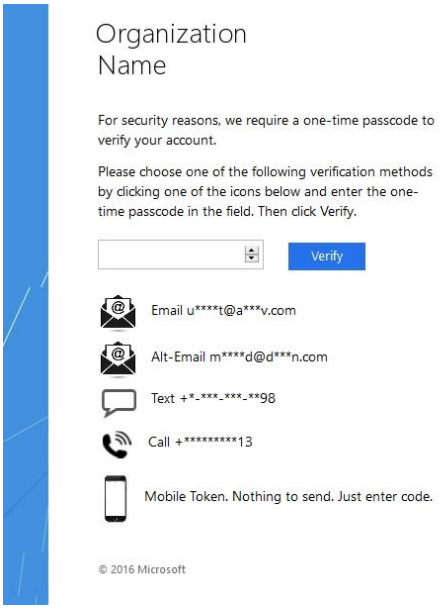
Overview – The Legacy Application Security Problem

Enterprises and organizations of all sizes typically have numerous legacy web services that have no support for modern authentication, Single Sign On (SSO) or Multi-Factor Authentication. These types of legacy applications in many cases cannot be updated and therefore they can dramatically increase an organization's threat attack surface especially if they are Internet facing applications.

To address the Legacy Application Security Problems, aPersona has combined its world-class adaptive multi-factor authentication platform (Adaptive Security Manager) with Microsoft AD FS to provide a complete SSO solution with advanced behavioral multi-factor authentication that enables organizations to easily add an additional and invisible layer of strong authentication to legacy applications with zero changes to the applications.

aPersona's Adaptive Security Manager for Legacy Applications brings the following benefits and features to any legacy application:

- Zero-Tough/Invisible Strong Adaptive Authentication
- Audit and Compliance authentication data on each legacy application.
- Country and Threat actor Filtering
- Flexible adaptive MFA policies to ensure security based on user Security Groups.
- Multiple Identity verification methods including Email, SMS, Voice & Mobile Tokens
- Easy Enterprise Configuration & Management



aPersona's Adaptive Security Manager continuously works behind the scenes to effortlessly bring necessary layers of Single Sign-on and MFA security to Enterprise Legacy Applications.

Setting up and configuring the aPersona Legacy Application Security Solution takes just a few days and there are absolutely no changes required by End Users or by the Legacy Applications themselves.

Contact aPersona for find out more.

For more information or to set up a free trial, go to https://www.apersona.com/contact-us.