HID DigitalPersona® SSO for Microsoft® Office 365

Strong Multi-Factor Authentication

HID®

IMAGINE A WORLD

Where...
Passwords are nearly impossible to hack
People can't share credentials
Users can't pretend to be someone else

Where authentication is more...
Secure Complete Human-Proof Adaptable

That world is here.
Welcome to DigitalPersona®

Introduction

Securing the IT environment from data breaches and other unauthorized access has risen to board-level concern for most organizations. In this solution brief, we will look at the challenges and obstacles surrounding the implementation of strong authentication for organizations of all sizes. The primary focus will be on multi-factor authentication for Microsoft® Office 365™ and its impact to the organization. We will also introduce a promising new solution to the multi-factor conundrum — DigitalPersona® Single Sign-On for Microsoft® Office 365™.

The Challenge

Reeling from continued security breaches due to compromised static passwords; commercial, government, and academic institutions are actively searching for authentication alternatives. In response, a broad array of new approaches to authentication have flooded the market—including 2-factor (2FA), multi-factor (MFA), biometric, contextual and behavioral solutions.

Despite this, most organizations still have not found an acceptable substitute, and they continue to use passwords despite their serious shortcomings. There are many reasons why the authentication practices have not advanced faster. The most common barriers to adopting strong authentication include:

Limited Authentication Methods

Most 2-factor and multi-factor solutions on the market still use a password as one of the credentials. Given the insecurity of passwords, the inconvenience they cause for end users and the cost of resetting them, authentication solutions that still incorporate them have only taken a small step forward. Indeed, combining a weak factor with a stronger factor does not add much to the security provided.

In addition, being limited to just two static factors does not allow security policies to incorporate the notion of risk into authentication transactions. Not all authentication events pose the same risk and therefore need different levels of identity assurance. For a risk to be considered during authentication it must be measured using contextual markers, such as user behavior, time of day, geolocation, network address and device, to name a few.

Unfortunately, few authentication solutions incorporate contextual or behavioral awareness and even if they do, there aren't a sufficient number of factors to elevate authentication security for high-risk transactions.

Finally, different industries and individual organizations have varying security needs and are subject to differing compliance mandates. For government agencies, the use of smart card and biometric factors may be a requirement and some organizations still require the use of a hardware token.

Also, consider the use case where a user forgets or misplaces an authentication factor. In this scenario, the solution should be capable of providing alternative backup authentication methods not possible with only two factors. The bottom line is that every industry or organization has different security goals, use cases, architectures and compliance mandates that need to be supported by a wide choice of authentication factors that satisfy all use cases.

Complexity

The cost and complexity of deploying multi-factor authentication is a major barrier and most available solutions do not deliver a seamless and user-friendly experience. A report from Vormetric found: :

- Across nearly all geographies, “complexity” was the number one barrier to adopting data security tools and techniques more widely, selected by 57 percent of respondents.
- Complex deployments also typically require significant staffing requirements, and the “lack of staff to manage” came in as the second highest barrier, albeit a distant second at 38 percentage of respondents.

The major contributing factor to IT complexity has been the explosion of new endpoints, systems, and applications flooding into the IT ecosystem. This is exacerbated by the fact that organizations tend to add new technologies faster than they retire legacy ones. This is especially true for small-to-medium businesses where the old mantra “if it isn’t broken, don’t fix it” is alive and well. The result is that the security posture of companies is increasingly fragmented, or worse yet, hopelessly out of date.

Because this diverse mix of endpoints, systems and applications does not share common security interfaces; authentication practices in most organizations have devolved into a series of siloed point solutions that have organically evolved over time, each solving the security challenge of the moment but unable to extend to new technology implementations or security threats. This represents an unwelcome layering of security complexity over infrastructure complexity, compounding the IT challenge.

Single Sign-On (SSO) has inspired hope that it could bring relief by allowing users to authenticate once and subsequently access all their applications without further authentication burden. However, because of its requirement for a single user authentication it has also become an attractive target, an authentication single point of failure, if you will. When we consider the fact that SSO requires a user login — and username and password are still the most common credentials in use; we see that we are back to square one.

Implementing 2FA or MFA promises to alleviate the SSO password exposure, but none of the available solutions on the market are able to extend their authentication security to the rest of legacy IT assets. Introducing yet a new technology to the crush of all the other security management protocols is disruptive and cumbersome, promoting a continued fragmentation of IT security.

Incomplete Coverage

Multi-factor authentication vendors often talk about ease of use, ease of deployment and complete coverage, but they constrain their examples to a subset of IT systems. Because of the surge in cloud adoption, the focus has been principally on cloud and SSO applications. But what about your mainframe, client and server logon, desktop client applications, VDI and VPN? So now that you have your cloud secured with MFA, what about all these other IT assets?

Customers are left to adopt a multiplicity of authentication protocols for each use case. Therefore, many organizations continue to use antiquated and insecure authentication, mainly passwords, and data breaches continue to occur with such alarming frequency. Locking the front door but leaving all your windows open does not make for a viable security posture. And, without a unified authentication solution, it is difficult, if not impossible to get a complete record of all access activity which is vital for compliance purposes.

MFA for Microsoft® Office 365

Microsoft provides multi-factor authentication for Office 365. It is acknowledged as being serviceable and provides enhanced access security to the Office 365 SSO portal — a critical need when you consider the sensitive data commonly stored in Office 365 apps. The challenge is that MFA for Office 365 does not extend to many common applications and systems in the data center. This includes Microsoft desktop applications such as Outlook®, Skype™ for Business, Word®, Excel®, PowerPoint® and OneDrive® for Business.

The fundamental issue is that many client applications are solely designed to use traditional username/password authentication. They cannot be secured with Microsoft's multi-factor authentication. To get around this issue, Microsoft introduced App Passwords, allowing users to bypass multi-factor authentication and continue to use their application. The unfortunate result is that users now need to manage multiple app passwords, frustrating the promise of single sign-on convenience. To illustrate the end user impact of this approach, imagine a plausible scenario where each user has over twenty app passwords and are required by IT policy to change them on a recurring basis. Worse yet, with app passwords, users need to change them on all their devices. To remedy this security management headache, Microsoft implemented a system whereby when users change their main password, all their app passwords get a new "Date Created" stamp, without actually changing them! With this approach, the usability of app passwords may have improved, but it resulted in a troubling security dilemma – client applications and peripheral devices now have perpetual passwords.

Even with the questionable stopgap solution that app passwords represent for some rich clients, there are still many applications and systems for which neither Microsoft MFA nor app passwords provide access security, such as mainframe, server, VPN, VDI, and of course, Windows logon. All these assets are left to be secured separately, if at all, resulting in serious security gaps. To cope with the heterogeneous IT environment, organizations have implemented multiple-point solutions, each needing to be separately managed, presenting users with a confusing array of interfaces and disparate workflows. Many times, the access security defaults to the lowly password. And with such a patchwork of authentication systems, organizations do not have visibility into who is accessing what and when.

A Better Approach to Access Security is Needed

The historic approach to access security is no longer viable . Organizations cannot afford to throw yet another point product at each new app and each new IT system, adding complexity, jeopardizing security, frustrating end users and increasing the burden on already stretched IT staff. We need to take a holistic approach to access security.

This means that all IT assets must be secured — including web, SSO, mainframe, client and server logon, desktop client applications, VDI and VPN. All actors must be secured — including employees, partners, suppliers and vendors. The solution must be integrated to provide common administrative and user interfaces and provide visibility to the entire authentication landscape through a single lens. A unified authentication security approach will not only protect Office 365, but provide security coverage across the entire organization.

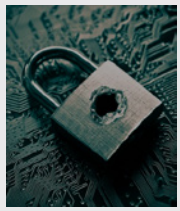
The DigitalPersona® Solution Multi-factor Authentication

DigitalPersona® SSO for Office 365 is part of the DigitalPersona family of solutions. It transforms the way IT executives protect the integrity of the digital organization by providing a comprehensive, integrated authentication solution that secures disparate applications and systems. Customers can finally secure all their IT assets, including Microsoft Office 365, using a common identity store with administrative and end user interfaces.

DigitalPersona SSO for Office 365

DigitalPersona SSO for Office 365 allows customers to be able to replace the weak "password only" logon with strong multi-factor authentication. It offers a rich set of authentication factors and flexible deployment options. Whether you have a cloud only Azure deployment or have configured an on-premise Active Directory infrastructure, there is a convenient DigitalPersona deployment option available for you. If you want to extend authentication beyond Office 365 to all your digital assets, you can use the same platform, the same authentication factors and the same authentication database to do so. One solution protects your entire organization.

BEYOND MFA: CLOSE EVERY GAP

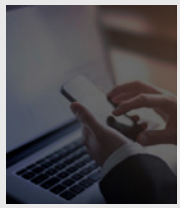


DigitalPersona closes the gaps in today's user authentication solutions. In addition to the traditional set of authentication factors — what you have, are and know — it offers authentication for contextual risk factors of time, velocity, location and behavior. These factors cover what you do, where you are, and when you act. Now you can choose the right level of protection for every application, every user and every system.

COMPLETE COVERAGE

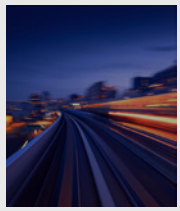
Complete coverage is finally possible. DigitalPersona supports ALL applications, including web, cloud, windows, mobile, VDI and VPN. However, DigitalPersona goes beyond these contemporary applications to include even legacy mainframe apps that continue to play a vital role in many organization's computing environments. And, with DigitalPersona, all constituencies are covered — not only your employees, but also your customers, vendors and partners.

HUMAN-PROOFED



Eliminate the reliance as well as the burden on users — so that you can lead with strong authentication postures without fear of compromise due to lack of cooperation. Strengthen your compliance profile with an irrefutable proof-of-presence, while lowering administration costs with an IT-friendly architecture.

RAPID ADAPTABILITY



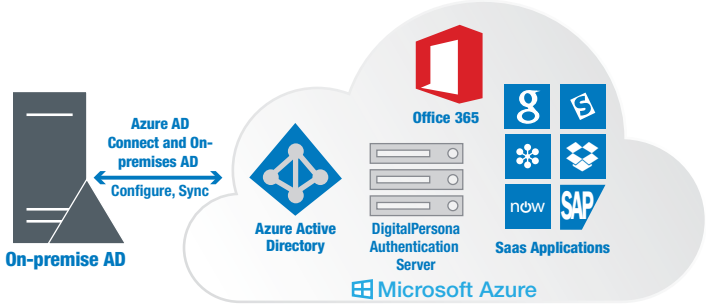
Deploy quickly, with minimal disruption and without forcing YOUR systems to adapt to OUR product. Integrate with your existing IT infrastructure using current IT tools and resources and achieve staffing flexibility and lower up-front and ongoing overhead costs — all while gaining peace of mind with a future-proofed architecture.

DigitalPersona® Adapts to Your Existing Environment

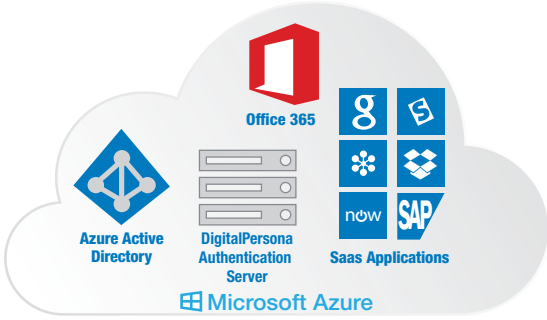
DigitalPersona Hosted in the Azure Cloud

For customers that have opted for a cloud-based Azure model, with (1) or without (2) an on-premise Active Directory, DigitalPersona® SSO for Office 365 fits like a glove. It can be hosted in an Azure instance to provide multi-factor authentication or Office 365 apps as well as the extended set of SaaS apps supported by Azure.

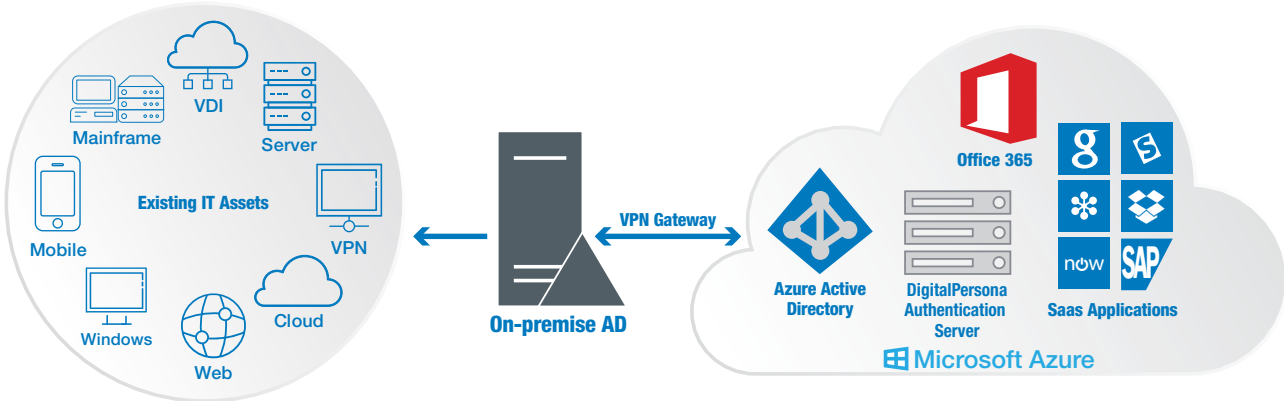
1) DigitalPersona Server Hosted in Azure, On-Premise AD



2) DigitalPersona Server Hosted in Azure, No On-Premise AD



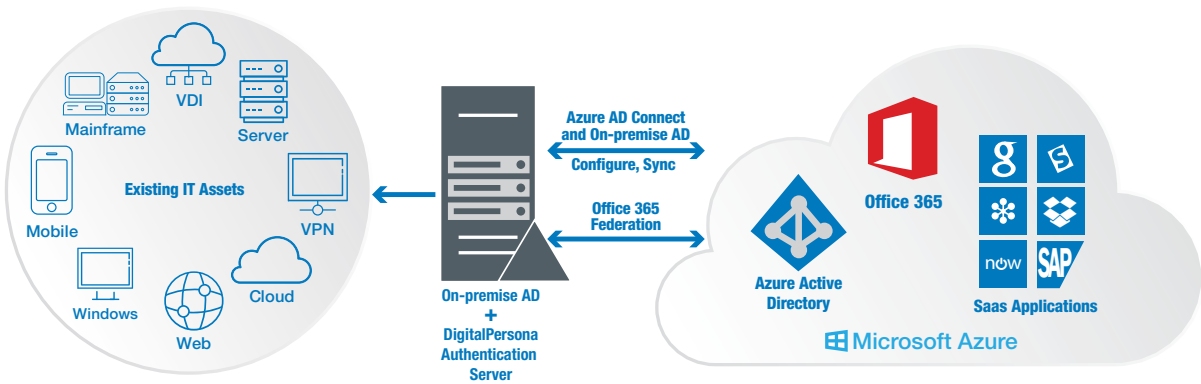
3) DigitalPersona Server Hosted in Azure with Full Application Coverage



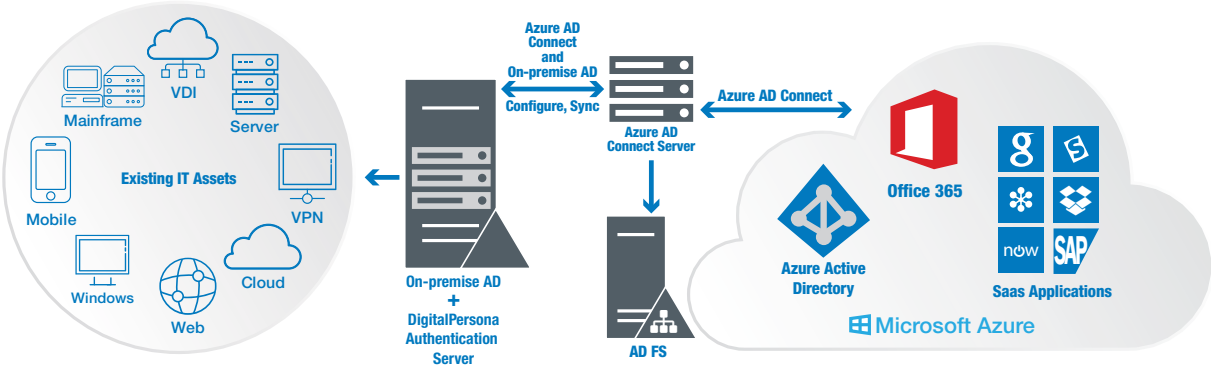
DigitalPersona® Server On-Premise Deployment Options

Customers have the option to install the DigitalPersona® Server on-premise to provide composite authentication protection for Azure SaaS applications. DigitalPersona supports customer configurations using either (4) Office 365 Federation or (5) Microsoft Active Directory Federation Services (AD FS). In either case, DigitalPersona can be extended to provide full application protection with the addition of an endpoint client.

4) On-Premise Server Deployment, Office 365 Federation



5) On-Premise Server Deployment, Micorsoft AD FS



DigitalPersona® SSO for Office 365 sets organizations free from the tyranny of siloed security solutions. With one platform, DigitalPersona not only protects your Office 365 SaaS environment, but can easily be extended to protect every application, every user and every system, moment by moment. Contact us to find out more and arrange a free trial.

North America: +1 512 776 9000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 5081 1650

2019-07-05-iams-digitalpersona-sso-office-365-br-en PLT-04487

An ASSA ABLOY Group brand

ASSA ABLOY

hidglobal.com