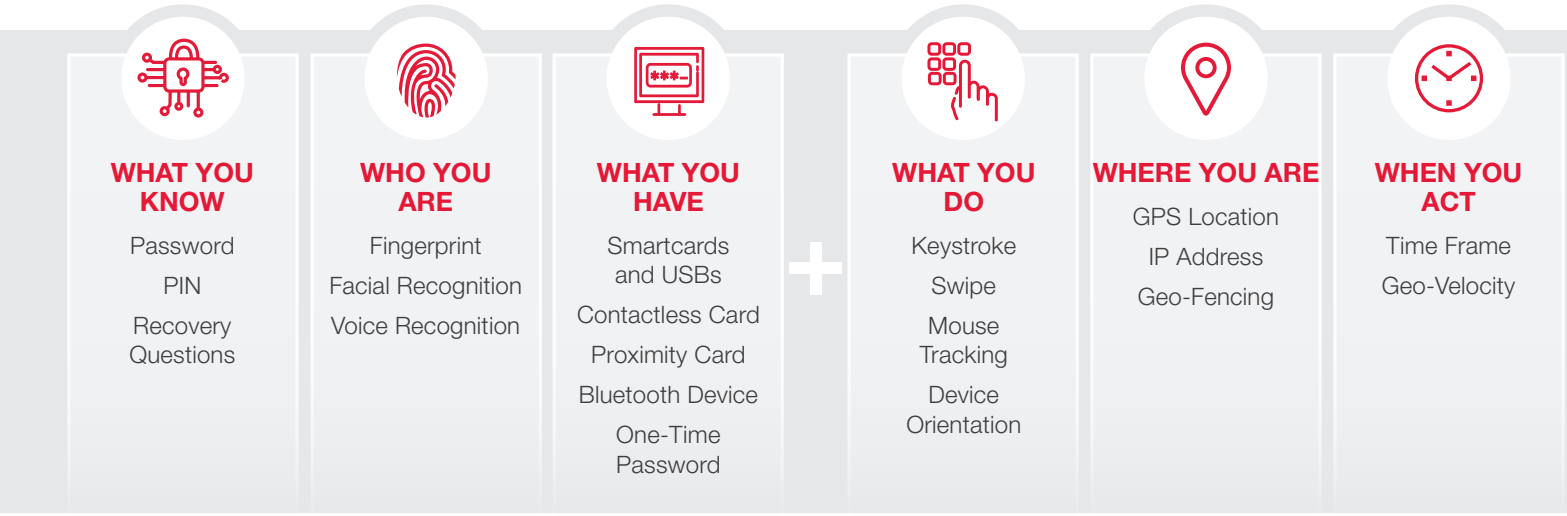
# DigitalPersona® Premium Data Sheet

## Overview

DigitalPersona's Composite Authentication transforms the way IT executives protect the integrity of the digital organization by going beyond traditional two-factor and multi-factor authentication. DigitalPersona Premium builds on the fast and secure Windows Logon and VPN access found in DigitalPersona Altus, adding advanced integration options to secure all applications, systems and networks. Additional client and server components included in Premium are SSO (SAML), Access Management API and Password Manager modules. Premium offers the ability to deploy the optimal set of authentication factors for every user, application, device and network – moment by moment. It accomplishes this while uniquely serving IT through unparalleled ease of integration and ongoing maintenance.

digitalPersona®
A CROSSMATCH® Solution

**COMPOSITE AUTHENTICATION:** The Right Mix of Factors, Moment by Moment




Full protection requires organizations to eliminate their dependence on the ability of humans to adhere to complex authentication policies. Only DigitalPersona offers a human-proofed solution that delivers the right level of security through the broadest possible selection of authentication factors – from a completely frictionless user experience to one that delivers the strongest protection available in the industry.

# Key Benefits

### CLOSES EVERY GAP

In addition to the traditional set of authentication factors – what you have, are and know – DigitalPersona offers authentication for the contextual risk factors of time, velocity, location and behavior. The latter cover what you do, where you are and when you act, allowing you to precisely match your risk exposure to the optimal security posture for your organization.

### COMPLETE COVERAGE

Complete coverage is finally possible. DigitalPersona supports ALL your applications, including web, cloud, Windows, mobile, VDI and VPN. DigitalPersona goes beyond contemporary applications to include even legacy mainframe apps, which continue to play a vital role in many organization's computing environments. And with DigitalPersona, ALL your constituencies are covered – employees, customers, vendors and partners.

### HUMAN-PROOFED

DigitalPersona's widest array of authentication factors eliminate both the reliance and burden on users enabling organizations to lead with strong authentication postures without fear of compromise due to lack of user compliance. The range of authentication options means you're never forced down a predetermined path. With this unprecedented freedom of choice, organizations can balance usability and protection based on specific security goals.

### RAPID ADAPTABILITY

With DigitalPersona, you can leverage your existing IT infrastructure and deploy more quickly than other solutions in the market today. Organizations are typically up and running in days – not weeks or months. DigitalPersona also provides native support for Active Directory, Azure AD and Office 365, enabling you to leverage your existing Microsoft expertise. Administration is simplified: no proprietary tools are needed to learn, manage or administer the system.

You can implement with minimal disruption, total staffing flexibility and both lower up-front and ongoing overhead costs. DigitalPersona's extensible architecture also provides peace of mind. DigitalPersona offers "future-proofing" and is designed to easily accommodate new authentication factors as they emerge.

# Premium Key Components

## CLIENT MODULES

| | |
|---|---|
| **Composite Windows Logon** | • Provides fast and secure device logon<br>• Includes behavioral and contextual risk-based policies |
| **Altus Client**<br>**Altus Console with Enrollment, Policy Engine, and Core Components** | • Connects to Altus server for enrollment, authentication and policy enforcement<br>• Provides tools for user enrollment |
| **Altus Mobile Enrollment Client** | • Offers strong attended enrollment on a Windows mobile platform to onboard users in disconnected mode |
| **Altus Password Manager** | • Enforces strong MFA for Windows, web and legacy apps<br>• MFA unlocks username/password to fill in authentication forms<br>• Includes password randomization and self-serve reset |
| **Altus SAML SSO Portal** | • Allows for app integration using SAML protocol<br>• Provides browser-based SSO Portal for accessing SAML enabled apps |
| **Altus Access Management API** | • MFA authentication SDK for custom app integration<br>• Native SDK – interfaces include C, Java and .NET<br>• Web services interface – for integration with web apps<br>• Eliminates the need for password-based authentication |

## SERVER MODULES

| | |
|---|---|
| **Altus Server**<br>**Policy Engine and DB (AD or LDS)** | • Creates, distributes, and enforces MFA policies<br>• Acts as a central repository for user credentials |
| **Altus RADIUS VPN Extension** | • Provides two-factor authentication for remote access |
| **Altus SAML Identity Provider** | • Allows users to authenticate at an identity provider (IdP) and then access apps without additional authentication |

# Premium Integration Options

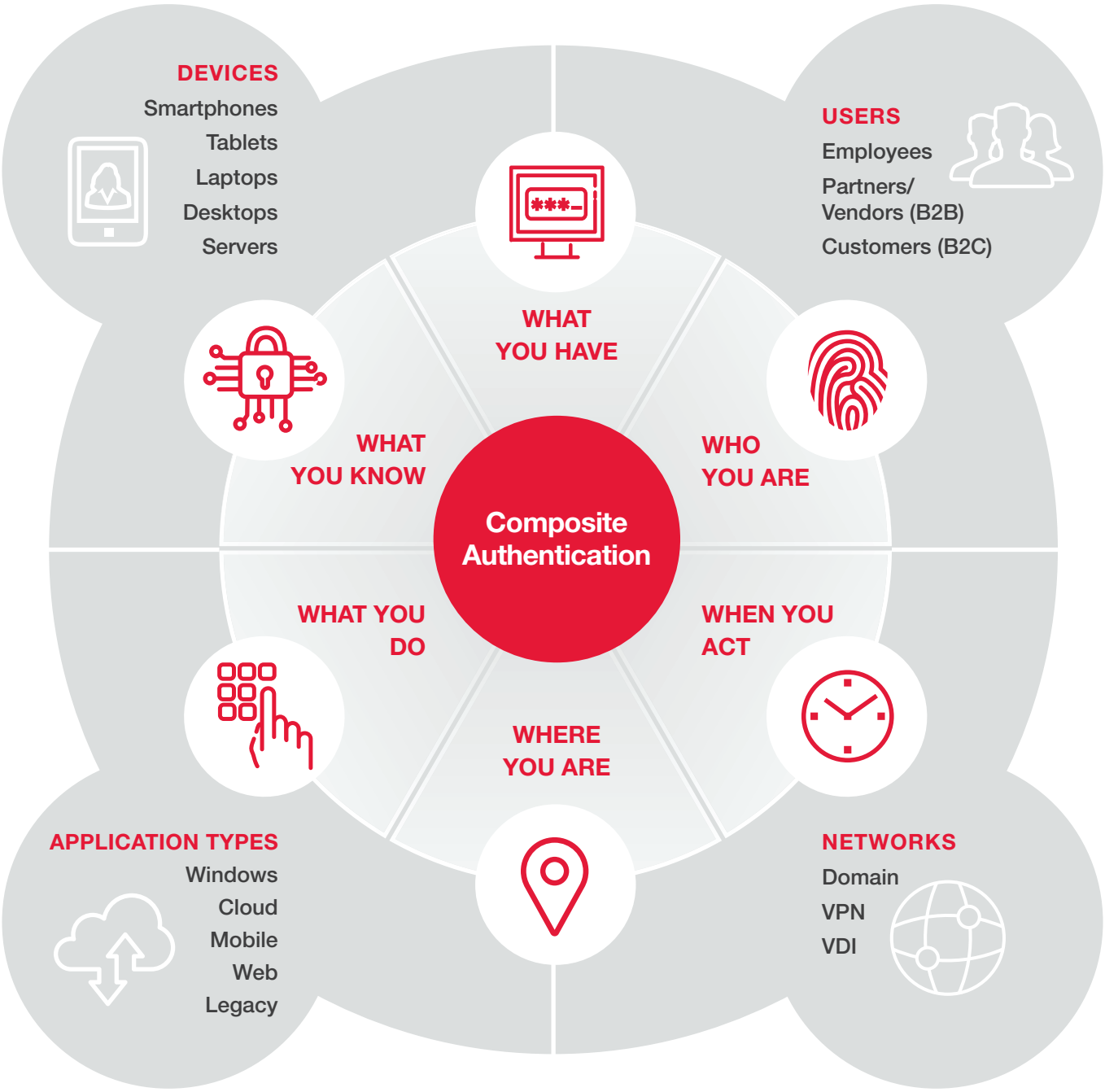
A rich array of integration options – from native integration to SAML to our own industry-leading password manager – help ensure all applications are covered.

| SSO (SAML) | Access Management API | Password Manager | Windows Logon |
|---|---|---|---|
| • Integration of SAML enabled applications<br>• SSO application portal on both Window and mobile platforms<br>• Customers option to remove all passwords | • Comprehensive DigitalPersona API management enables tightly integrated implementation<br>• Full scalability across on-premise and cloud services | • Secure and convenient authentication application overlay<br>• Allows customers to quickly provision apps without modifying source code | • Out of the box integration with Windows logon<br>• Includes all factors including contextual and risk-based<br>• Up to 3-FA, any combination |

WEB CLOUD MOBILE SERVER WINDOWS

# DigitalPersona Composite Authentication

The most complete way to optimize security for every app, every user, every time. DigitalPersona's Composite Authentication transforms authentication and provides entirely new levels of protection ensuring the digital identity of employees, customers, and partners as well as protecting access to networks, applications and data.



# Premium Features and Specifications

| | |
|---|---|
| **Centralized Management** | Active Directory – Set security policies for domain users and groups using Group Policy Objects (GPOs) |
| **Web Administration Console** | Administer Altus LDS and AD users with the Altus LDS backend infrastructure |
| **Composite Authentication for Windows Logon** | **Authentication Factors:**<br>**Know:** Windows password, PIN, recovery questions<br>**Have:** OTP, contactless cards (HID iCLASS memory cards, MIFARE Classic 1k, 4k and mini memory cards), smart cards (PKCS11 and CSP-compatible), proximity cards (HID 125 kHz) and Bluetooth devices<br>**Are:** Fingerprint, face, voice<br>**Do:** Keystroke, swipe, mouse-tracking, device orientation<br>**Where:** GPS location, IP address, Geo-fencing<br>**When:** Time frame, Geo-velocity |
| **SSO (Single Sign-On)** | **Password Manager** – Provides Single Sign-On and enforces strong authentication without modifying underlying applications<br>**SAML** – Federated identity SSO, SSO application portal accessible from Windows PC, Mac, and mobile devices |
| **Per Application Authentication Policy** | **Per Application Policy** – Adds additional authentication credential to specific applications |
| **Fast Kiosk Access** | **Shared-User Workstation ("Kiosk") Logon Control:** Enforce advanced authentication policies for shared workstations (such as walk-up kiosks) where people use their individual credentials to unlock Windows and log into applications. Support for multiple kiosk environments under Citrix/RDP |
| **Self-Service Password Recovery** | If users forget their passwords, they can access their PC by answering a set of predefined questions (this can be customized and centrally managed by IT) |
| **Reports** | Generate, view and schedule preconfigured activity and status reports for users and applications from a centralized location |
| **Client Software Operating System** | Windows 10, Windows 8.1 (desktop mode), Windows 7 (32- and 64-bit), Windows Embedded Standard 2009 (requires .NET 4.5), Windows Server 2008 and 2012 and Linux (select thin clients) |
| **Server Software Operating System** | Windows Server 2012 and 2012 R2, Windows Server 2008 R2 (64-bit) |
| **Mobile** | SSO application portal accessible from mobile device. Mobile Access SDK for mobile app integration using: Web Services from iOS and Android native wrapper over Web Services on Android mobile devices |
| **Browsers** | Internet Explorer versions 8-11, Chrome latest version, Firefox |
| **VDI (Virtual Desktop Infrastructure)** | XenApp (server) 6.5, XenDesktop 6.2 and 7, Receiver and Online Plug-In 11 and 12, VMWare View and VMWare Horizon |

# About Crossmatch

Crossmatch® solutions solve security and identity management challenges for hundreds of millions of users around the world. Our proven DigitalPersona® Composite Authentication solution is designed to provide the optimal set of authentication factors to meet today's unique risk requirements and afford complete enterprise authentication coverage. Crossmatch identity management solutions include trusted biometric identity management hardware and software that deliver the highest quality and performance required for critical applications. Our solutions support the financial, retail, commercial, government, law enforcement and military markets. With 300 employees and customers in more than 80 countries, Crossmatch sets the standard for innovation and reliability. Learn more: **www.crossmatch.com**

**Crossmatch**

3950 RCA Boulevard, Suite 5001

Palm Beach Gardens, FL 33410

USA

Tel: +1 561 622 1650

Fax: +1 561 622 9939

**www.crossmatch.com**