



# DigitalPersona® Pro Workgroup Software-as-a-Service

Cloud-based security management starting at \$2/month

## DigitalPersona Pro Workgroup SaaS

**DigitalPersona Pro Workgroup** is a cloud-based, Software-as-a-Service (SaaS) solution that helps you centrally manage a variety of security applications from a single web-based console.

- **A single solution for multiple security needs.** You can now control a variety of modules including Disk Encryption, Strong Authentication, Single Sign-On, Email Encryption and more.
- **Hosted Software-as-a-Service.** We keep things running for you, so that you don't have to. No hardware or server investment or maintenance needed, compatible with any existing directory.
- **Affordable fees.** Flexible pay-as-you-go from as little as \$2/ month. No upfront investment or other set-up fees. Only pay for the number of PCs you are managing, and add seats as you need them.
- **Modular deployment.** Choose which modules you need among Disk Encryption, Strong Authentication, etc., and only pay for those. Then, add additional modules when you need it.

## Workgroup SaaS Packages

Modules	Data Protection	Authentication	Ultimate
Centralized management and reporting	✓	✓	✓
Full disk encryption	✓	—	✓
Strong authentication & Single Sign-On (SSO)	—	✓	✓
Secure email and documents	—	—	✓

## Benefits of Cloud-based security management

According to InformationWeek<sup>1</sup>, businesses are primarily adopting SaaS for the improved ease of deployment and lower cost structure. Research firm IDC reported that over a three-year period, SaaS solutions are always more affordable than on-premise options, regardless of the size of the deployment<sup>2</sup>.

Aberdeen Group reports that businesses implementing security as a service instead of deploying traditional on-premise solutions are typically more secure, experiencing fewer security incidents. In addition to being more secure, Software-as-a-Service solutions tend to be less expensive and easier to manage. Businesses using cloud-based solutions had 42% fewer Help Desk calls than users of on-premise solutions<sup>3</sup>.

## Average number of security incidents over the last 12 months

	With on-premise solutions	With cloud-based solutions	Cloud benefit
Data loss or data exposure	11	6	45%
Security-related downtime	11	6	45%
Audit deficiencies	30	2	93%

<sup>1</sup> Businesses get serious about Software-as-a-Service, Information Week, April 14, 2007.

<sup>2</sup> Robert Mahowald, Do Service Providers Deliver Value and Reduce Enterprise Costs?, IDC, 2003.

<sup>3</sup> Web Security in the Cloud: More Secure! Compliant! Less Expensive, Aberdeen Group, May 2010.

**General**

- Centralized management via Cloud-based Web console
  - Centralized log collection and reporting
  - Qualification for operating in FIPS-compliant mode
- 

**Full Disk Encryption**

- Encryption of the entire hard drive, including empty sector, using AES 256-bit encryption
  - Pre-boot authentication
  - Central management of encryption policies (e.g. ON/OFF)
  - One Step Logon (aka Single Sign-On) from pre-boot to Windows/ domain
  - Centralized backup of drive encryption keys
  - IT-assisted recovery (e.g. for forgotten passwords), even with no network or Internet connection
  - Emergency data recovery options (e.g. in case of hardware failure)
  - Centralized collection and reporting of Full Disk Encryption status and event logs
- 

**Strong Authentication and Single Sign-On (SSO)**

- Centrally-managed strong authentication for PC logon
  - Centrally-managed Single Sign-On and/or Strong Authentication into all applications (e.g. Web apps, Windows apps, Terminals, etc.), without modifying existing applications
  - Ability for Administrators to “train” applications for SSO/ strong authentication and deploy data to managed computer
  - Policy-based management, centrally enforced (e.g. Use two-factor authentication)
  - Supported credentials include Windows/domain password, fingerprints, smartcards
  - Windows/ Domain password self-service recovery at PC logon
  - IT-assisted recovery (e.g. for forgotten passwords), even with no network or Internet connection
  - Centralized collection and reporting of Strong Authentication status and event logs
- 

**Secure Email and Documents**

- Digital signature of email messages and documents (Office and PDF)
  - Encryption of email messages and documents (Office and PDF)
  - Policy-based management, centrally enforced
  - Centralized collection of encryption and signature status and event logs
  - Centralized reporting on encryption and signature status and activity
- 

**Requirements****Supported Client and Server Software**

- DigitalPersona Pro Workstation for Workgroup or HP ProtectTools 5.04 or later
- Server software hosted by DigitalPersona

**Client Operating System**

- Windows 7 (32- & 64-bit)
- Windows Vista (32- & 64-bit)
- Windows XP SP3 (32-bit)

**Browsers**

- Internet Explorer 6 or later
- Firefox 2 or later

*Contact DigitalPersona for detailed information on supported fingerprint readers, smartcards, and other authentication methods.*

---