



Sponsored by DigitalPersona

Controlling Access, Authentication and Data on the End Point: A Review of DigitalPersona Pro 5.1 for Enterprises

July 2011

A SANS Whitepaper

Written by: Jim D. Hietala

DigitalPersona Pro Features and Components *PAGE 2*

Overview of DigitalPersona Pro 5.1 for Enterprise *PAGE 4*

Disk Encryption *PAGE 5*

Strong Authentication *PAGE 6*

Single Sign-On *PAGE 7*

Centralized Management *PAGE 9*

Use Case Examples *PAGE 12*

Executive Summary

With security breaches almost constantly in the news, senior managers are challenging their IT staffs to solve security problems before their organizations end up in the headlines. Security breaches are perpetrated by a wide variety of external and internal sources, including hackers, targeted attackers, and profit-motivated cybercriminals, as well as through mundane everyday occurrences, such as missing laptops and thumb drives.

As a result of all these threats against today's open networks, compliance requirements have emerged that include requirements around access, authentication and protection of sensitive data on end points. HIPAA, SOX, GLB, PCI DSS, and multiple state, federal and international laws and regulations make it clear that access must be strictly controlled and monitored for compliance. Data at rest on devices should be encrypted as a final protection against sensitive data exposure and (in many cases) liability.

To address these compliance and privacy issues, organizations have responded by adding layers of controls and integrating them with varied results. Now, those organizations realize that making security simpler is the ultimate strategy for ensuring end user adoption of new security measures and meeting multiple, overlapping regulatory requirements.

DigitalPersona Pro for enterprise end point security streamlines a mix of important, integrated capabilities aimed at these problems, including strong biometrics and other multifactor authentication to uniquely identify users, encryption to ensure confidentiality for data even if devices are lost or stolen, and single sign-on to ease the access process for legitimate end users.¹ This paper is a review of DigitalPersona Pro, its integrated approach, and its features and efficiencies in these areas.

Overall, the product was easy to setup, use and manage from a local administrator console, all while providing centralized administration. DigitalPersona Pro modules work together to provide an ease of use that makes this a strong choice for large organizations with complex user access requirements.

¹ <http://www.digitalpersona.com/enterprise/overview>

DigitalPersona Pro Features and Components

The DigitalPersona Pro software provides an integrated approach to a number of end point security and compliance requirements:

- Strong authentication of users
- Encryption of data stored on devices
- Single sign-on to enterprise applications
- Communications encryption and digital signing of documents and e-mail

There are obvious advantages of having these functions integrated, versus operating these functions as multiple standalone components. Benefits include simpler management with fewer security consoles, reduced interoperability issues, and the possibility of reducing the number of support vendors with which an organization has to interact.

The DigitalPersona approach allows for management of the above functions using familiar Windows mechanisms (Active Directory and Group Policy Objects) and familiar security and authentication constructs from Windows. As a result, managing the DigitalPersona Pro software will be very natural for Windows shops.

This collection of functionality in an integrated end point security suite seems well suited to enterprises in which strong authentication is becoming a requirement—as is encryption of data in end points. In these environments, single sign-on (SSO) provides a convenience that makes enhanced security more palatable to end users because they no longer have to remember multiple passwords to their many accounts. Security is, at the same time, enhanced because more powerful authentication mechanisms (such as tokens, one-time passwords, and even their computer location or their cell phone devices) can be used as secondary authentication factors.

DigitalPersona Pro Enterprise 5.1 includes numerous components reviewed for this paper, as well as some capabilities that were not reviewed. (Note: Hewlett-Packard (HP) is an OEM partner of DigitalPersona's, and the HP ProtectTools are functionally equivalent to the DigitalPersona software.) DigitalPersona Pro 5.1 product components include:

Pro Enterprise Server — This is the central configuration and management tool for installation of the DigitalPersona Pro Workstation and HP's ProtectTools software. Pro Enterprise Server is installed on a domain controller. Client systems automatically connect to the server software.

Pro Workstation — This is the workstation software module. It includes a dashboard for local access to installed security applications and an administrative console on which the local administrator can preconfigure applications. The local console can be disabled through a Group Policy Object setting in Active Directory.

DigitalPersona Pro Features and Components (CONTINUED)

Credential Manager and Password Manager — These provide strong/multifactor authentication and SSO to Windows systems and applications, websites and other programs.

Drive Encryption for DigitalPersona Pro — This disk encryption capability allows for encryption of any nonremovable hard drives.

DigitalPersona Defender VPN module — This component provides authentication capabilities to RADIUS-based VPNs using OATH-compliant One Time Password (OTP) tokens. Hardware tokens or smartphone tokens can be supported as well.

DigitalPersona Privacy Manager Pro — This provides digital signature capabilities for Outlook e-mail, Office documents, and Windows Live Messenger instant messages, coupled with password or biometric authentication.

DigitalPersona Defender Security Server — This provides strong authentication services (supporting soft and hard tokens) and support for Radius client requests and Defender clients.

Administration Tools — This is a set of software applications for administering additional features of DigitalPersona Pro for enterprise that may be installed separately from the server.

Overview of DigitalPersona Pro 5.1 for Enterprise

The setup used for this review consisted of DigitalPersona Pro Workstation software, a Windows 2003 Domain controller, and a Windows 7 test client. The DigitalPersona Pro Server central management software was also tested using a web interface on a sample network. Additional equipment included the U.are.U 4500 fingerprint reader from DigitalPersona (used to provide biometric authentication capabilities).

Pro Workstation Local Administrator Console

Software installation was straightforward, and the documentation did a good job of describing installation and configuration of the various components. The local administrative console, shown in Figure 1, was easy to use and presented information logically.



Figure 1. DigitalPersona Pro Local Administrative Console

The local administrative console provides designated business users and local administrators with quick access to the basic features they require to interact with the software. These include managing passwords and logins to enterprise applications, controlling local backup and restore for DigitalPersona configuration data, enrolling user credentials, and managing the encryption capabilities.

Once installation and configuration were complete, I ran a variety of functionality tests, which included logging onto the client machine with administrative and non-administrative user IDs and enrolling different fingers/fingerprints to different user IDs. Using the software was very straightforward, and although not tested, it was easy to see how deployment and settings could be pushed out from a central location without user intervention once policies are set.

This product review focused on the three key security capabilities that organizations usually struggle to manage separately: disk encryption, strong authentication, SSO and centralized management capabilities using Group Policy Objects and Windows Directory Services.

Disk Encryption

Using DigitalPersona's local administrator console, disk encryption was simple to set up and configure using the setup wizard. The product documentation recommends using a drive health check via CHKDSK or a third-party program before activating the encryption process. While this is not difficult for relatively technical users, asking average end users to run CHKDSK on their computers before encrypting would probably meet with resistance. So, installation of the package, at least where it is being used to perform disk encryption, would be best handled by support staff.

After verifying the hard disk, setting up the disk encryption functionality was simple. Setup required selecting the drives to be encrypted and supplying a USB port and device on which to store a recovery encryption key. Figure 2 shows these configuration settings.

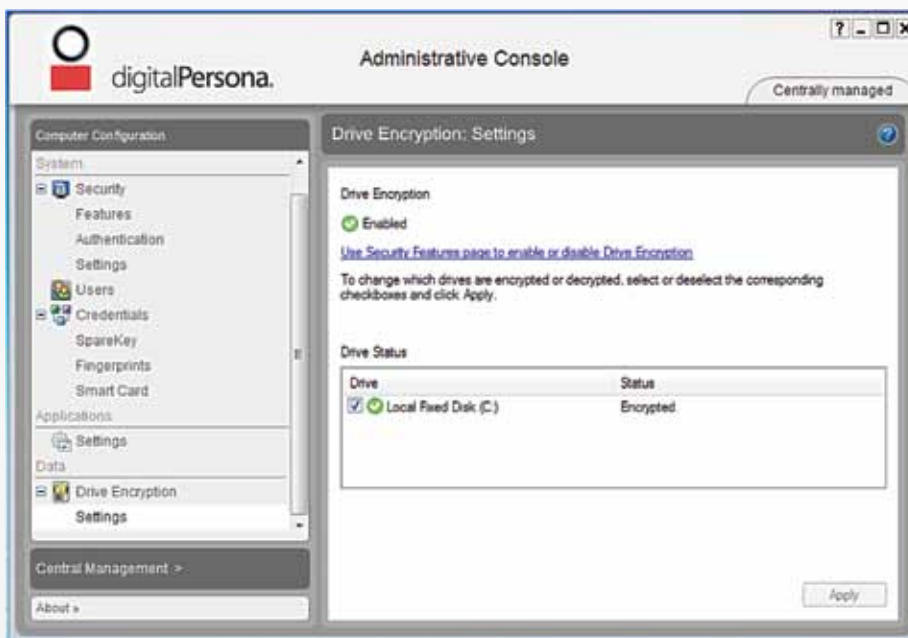


Figure 2. Encryption Configuration Settings

User Experience

Once provided with these essentials, and after a required reboot, the software proceeded to transparently and rapidly encrypt files as a background task without disrupting PC operations.

After drive encryption is enabled, users must log in (pre-boot) from the Drive Encryption login screen, shown Figure 3.

Users can log in using their Windows password, Java Card PIN, or fingerprint using an attached fingerprint reader. Passwords from Trusted Platform Modules (TPMs) are also supported by the software for TPM-enabled systems.



Figure 3. Pre-Boot Login Screen

Strong Authentication

This review also looked at how DigitalPersona's local and central management server modules allow specific authentication options to be applied to users and groups of users. This also was easy to set up and deploy using the central manager, as shown in Figure 4.

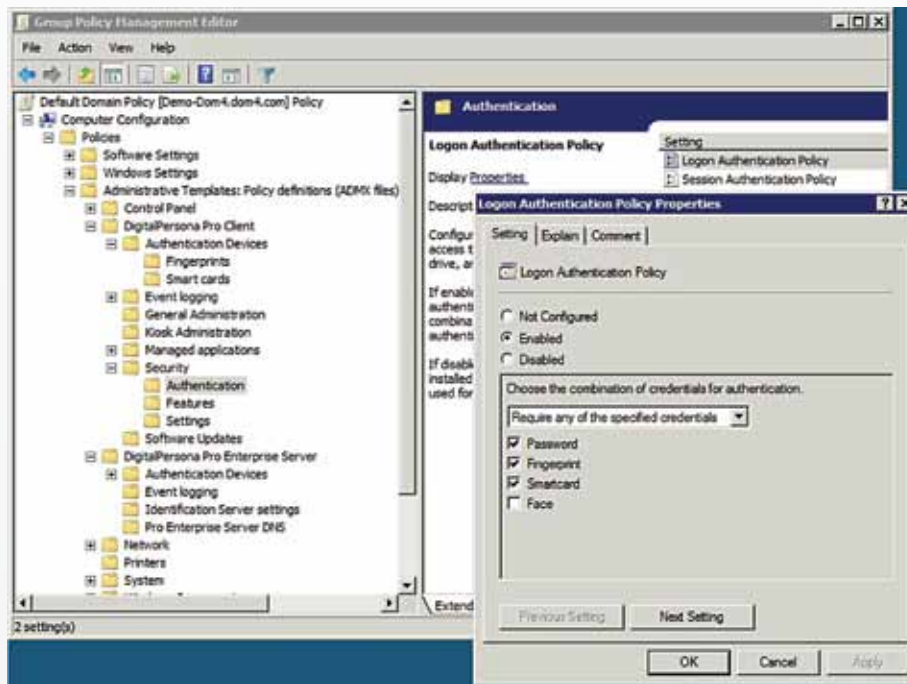


Figure 4. Authentication Options Menu

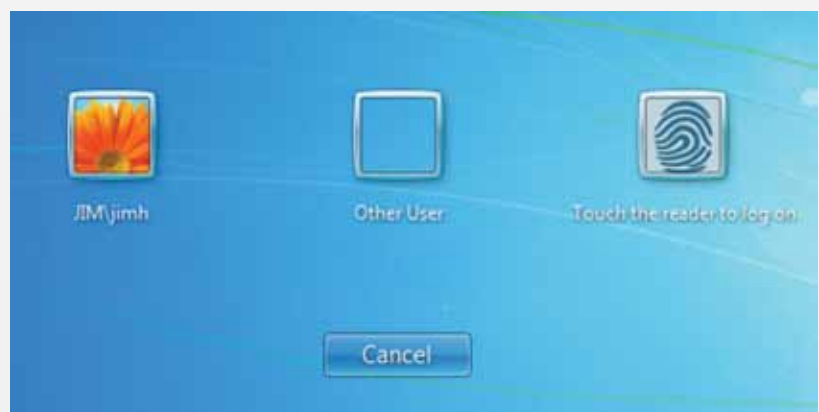
DigitalPersona Pro's local administrator console provides numerous options to set up multifactor authentication on devices, including the use of fingerprints and fingerprint readers, facial recognition, smart cards, and OATH-compliant one-time passwords.

This review focused on using fingerprints as a second authentication factor. This required enrolling fingerprints as a biometric credential. DigitalPersona provides several methods for achieving this: user self-enrollment, an Active Directory Users and Computers snap-in, or the Attended Enrollment tool. Fingerprint self-enrollment was simple using the local console. Attended enrollment allows for a supervisor to be granted authority to enroll groups of users.

Once user fingerprints are enrolled, using this capability is quite easy. Figure 5 shows the login interface with a fingerprint reader enabled and a user enrolled.

Figure 5. Login Interface with Fingerprint Authentication

For users and IT staff with multiple logins (for example a regular user login, a domain administrative login, and other administrative account logins), the fingerprint reader can save time and make life easier.



Single Sign-On

To simplify end point user access to multiple applications, DigitalPersona also has a function called Password Manager, which is a bit of a misnomer and sells the provided capability short. While it does manage passwords, Password Manager also provides single sign-on into multiple enterprise or web applications.

The Password Manager software has configuration options for changing passwords, including allowing users to invoke password changes, password change intervals, and password format restrictions. From a single sign-on (SSO) perspective, the product provides administrators with access to logon field attributes so that they can customize or adapt the automatic logon to the needs of the enterprises applications.

Password Manager did a good job of automatically identifying fields in websites and programs during this review. Also, having the ability to create and manage logon scripts manually (which DigitalPersona provides) is a very good idea, because many enterprise legacy applications require some adaptation to work properly with single sign-on.

The software includes a Field Catalog. This is a reusable repository for logon fields and attributes that can be helpful in building new managed logons for applications using -sed fields. With the ability to manage large numbers of end points running the DigitalPersona software through the use of Group Policy Objects, it is then easy to deploy new managed logon scripts for new applications to many end points simply and quickly. Using Group Policy Management, administrators can establish group policies and create and distribute managed logons to specific applications. Once established, administrators download managed logons to client devices as soon as they are created or at refresh intervals based on their policy.

In this review, the single sign-on capability was configured to access two different applications, which was a straightforward process. Figure 6 shows the configuration menu for using the Password Manager capability.

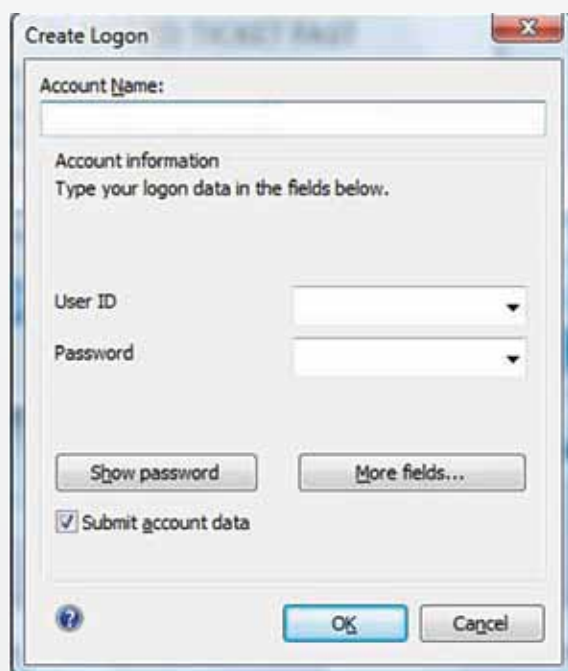


Figure 6. Password Manager Configuration Menu

Single Sign-On (CONTINUED)

When the single sign-on capability is married to a fingerprint reader, a single swipe of a finger can log the user into all of the user's designated applications. See Figure 7.

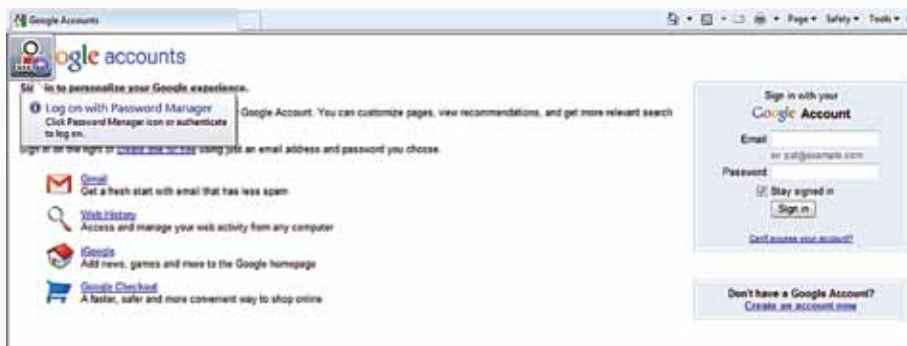


Figure 7. DigitalPersona Password Manager Setup for Access Only Via Fingerprint

The user can only log on to the applications by using the registered credential, in this case a fingerprint. The small icon displayed at the top left of the screen gives the user one click (single sign-on) access to their applications based on the policy already set up in the Password Manager software. Alternately, the software can be configured to allow automatic sign in to enterprise applications without any additional steps.

A beneficial byproduct of using the Password Manager is improved use of very strong passwords for enterprise applications. Rather than having users use common words with meaning to them in their passwords, which may be more susceptible to dictionary and man-in-the-middle authentication attacks, users can create very strong, complex passwords without fear of forgetting them and without resorting to writing them down.

The DigitalPersona software can be configured to take this a step further and allow the software to autogenerate a randomized password for the user. To the extent that IT staff can enforce policies around the use of complex passwords in conjunction with DigitalPersona Pro, they will have raised the bar for attackers and improved the organization's security posture. Coupling a biometric authentication capability such as a fingerprint reader with SSO is a great thing!

Centralized Management

DigitalPersona Pro leverages the Windows security infrastructure to support its management capabilities. DigitalPersona Pro's management console runs on domain controllers, and the management server can be located by Domain Name Service. Security policies can be deployed as Group Policy Objects, one of many tight integration areas with Windows security in DigitalPersona. For example, encryption keys are stored in Active Directory, which ensures that critical encryption keys are automatically backed up securely.

This integration with Active Directory leverages the existing database of user data in Active Directory instead of requiring the introduction of a separate user database. It also allows for integration with tools that are familiar to Windows shops, including Group Policy Management for settings, configurations, and policy creating.

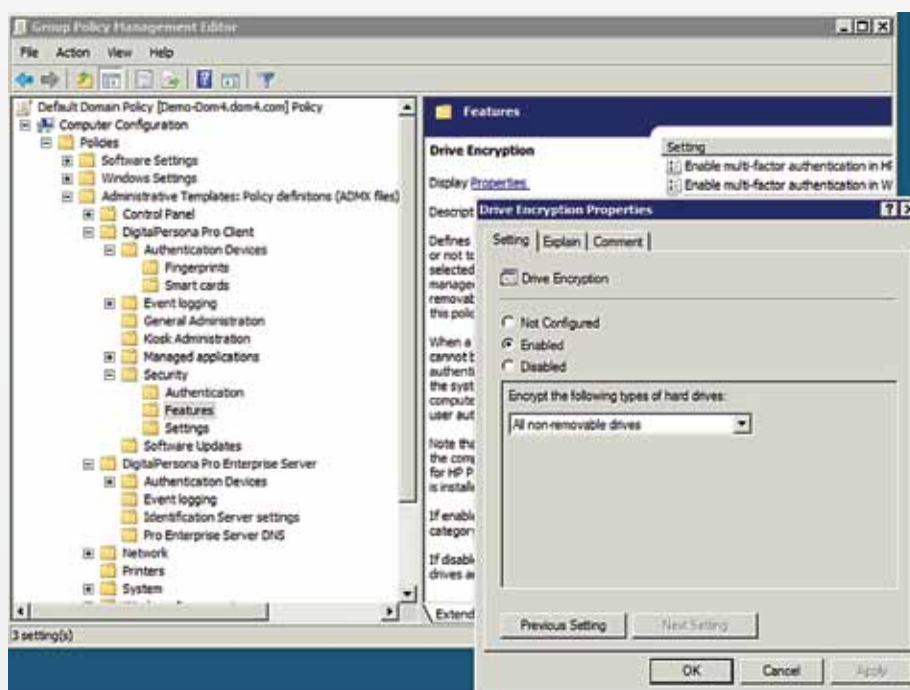
Setting up the central management console requires running an Active Directory schema extension wizard (using schema administrator privileges) to add the extensions used by DigitalPersona Pro Server to provide central management capabilities. Although not required, this step — and the installation of the server software itself — usually take place before installation of any client software.

Centralized system management is achieved through the use of Group Policy Management Editor and DigitalPersona ADUC (Active Directory Users and Computers) snap-ins. The Group Policy Management Editor allows numerous security policies that relate to the operation of the DigitalPersona client software to be easily created and deployed to user devices, leveraging the Active Directory group structures, which are typically already in place.

Centralized Deployment

Using DigitalPersona Pro's central management system, policies that enable drive encryption for all users, or groups of users, can be created and deployed from this interface, as shown in Figure 8.

Figure 8. Group Policy Management Editor with Drive Encryption Menu



Centralized Administration

The Active Directory Users and Computers capability allows administrators or help desk staff to do some critical administrative functions when required. First, in the event that a user gets locked out of his or her system (for example if the threshold for failed fingerprint attempts has been reached), this module can provide an emergency complex password that can be used to unlock the system and regain access. Second, the software allows a recovery code to be created in case a user or an administrator needs to recover access to an encrypted PC. Figure 9 shows the recovery function.



Figure 9. DigitalPersona Recovery Menu

Leveraging Group Policy Objects and Windows management makes the DigitalPersona software easy to deploy centrally in large, complex environments. Policy distribution via Group Policy Objects supports updates to security policies, configuration settings, and things like adding managed logons through the Group Policy Management Editor.

Centralized Reporting

Additionally, DigitalPersona Pro provides for central audit collection and central reporting, which is important for compliance and audit purposes. Figure 10 shows the menu of reports available in the product.



Figure 10. DigitalPersona Report Options

An example report that identifies the status of encryption on the end point device and which drives have encryption enabled is provided in Figure 11.

digitalPersona Reporter			
Disk Encryption Status			
Computer name	Status	Encryption method	Date and time
QA_Vista_32Bit	C: Not Encrypted D: Not Encrypted G: Not Encrypted H: Encrypted	Software encryption	04/21/11 01:12
QA_Vista_32Bit	C: Not Encrypted D: Not Encrypted G: Not Encrypted H: Encrypted	Software encryption	04/21/11 01:12
QA_Vista_32Bit	C: Not Encrypted D: Not Encrypted G: Not Encrypted H: Encrypted	Software encryption	04/21/11 01:12
QA_Vista_32Bit	C: Not Encrypted D: Not Encrypted G: Not Encrypted H: Encrypted	Software encryption	04/21/11 01:19
QA_Vista_32Bit	C: Not Encrypted D: Not Encrypted G: Not Encrypted H: Encrypted	Software encryption	04/21/11 01:19
QA_Vista_32Bit	C: Not Encrypted D: Not Encrypted G: Not Encrypted H: Encrypted	Software encryption	04/21/11 01:19

Figure 11. Encryption Status Report

Use Case Examples

Two use cases in the health care and law enforcement sectors are provided below, although many more industries are being subject to their own specific regulatory requirements. These use cases identify the importance of using access, authentication and encryption together, holistically, to solve specific industry-related problems.

Health Care Settings and Mobile, Ubiquitous SSO

Clinical health settings represent an industry-specific use case where the capabilities of DigitalPersona Pro would be helpful for security, compliance and convenience. Hospitals are populated with doctors, nurses, and other clinicians requiring fast access to desired information about patient health, insurance and ability to pay.

Historically, users in these clinical environments have had little patience with complex security procedures interfering with their mobility and the speed in which they often work. In many health care environments, prior to regulatory enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule², it was common to use shared logins among doctors, nurses and other clinical and support staff for workstation access. As a result, numerous security breaches have occurred in the health care community (87 breaches classified as medical between 1-1-11 and 6-16-11, according to DatalossDB.org).³ With more active enforcement of regulations, IT staffs in hospitals have been challenged to meet the objectives of enforcing individual logins while providing a more streamlined login experience for clinicians.

In health care organizations, the combination of capabilities offered by DigitalPersona Pro makes a great deal of sense. For example:

- Disk encryption for workstations helps address a HIPAA requirement for encryption of electronically protected health information that might get downloaded to or stored on an end point system.
- Strong authentication in the form of biometrics, whether through fingerprint reader technology or the other forms of strong authentication supported by DigitalPersona, helps ensure that the individual login requirements in HIPAA are achieved.
- Finally, the single sign-on functionality further simplifies login, which is critical for adoption by this demanding user community.

² www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

³ [http://datalossdb.org/search?direction=desc&order=reported_date&org_type\[\]=Med](http://datalossdb.org/search?direction=desc&order=reported_date&org_type[]=Med)

Law Enforcement

Modern law enforcement agencies require remote access to databases and criminal justice information systems in order to perform their duties while on patrol and in the field. Due to the sensitive nature of the information being accessed about citizens in these systems, encrypting data on the local system is mandatory, as is strong authentication. Law enforcement agencies accessing criminal justice information systems have strict requirements for positive identification of users accessing this information.

For this user community, easing access through a streamlined login process is also highly desirable. For law enforcement IT staff, the DigitalPersona integrated solution delivers encryption, strong authentication and single sign-on to enterprise applications in a single package that can be centrally managed. Through its variety of SSO authentication options, the system also enables the mobility and ease of use that law enforcement personnel need to be effective in the field.

Despite the obvious differences in the type of data and end users, there are commonalities between these use cases. In both examples, the data being accessed is highly sensitive and regulated. Both groups of end users could also be characterized as being demanding and intolerant of technology barriers to getting their jobs done, so SSO greatly benefits the adoption of new technology, including strong multifactor authentication such as biometrics.

Many other industries and groups of end users who use data and applications share these characteristics. Other similar use cases can be found in the financial services, legal, IT services, government, judicial, and other sectors that interact with personal, financial, medical, online account, and other data that is now being usurped by criminals for financial gain.

Summary

The DigitalPersona Pro software was easy to install and set up, and it is equally easy for an end user to interact with. DigitalPersona's integrated approach provides needed access, authentication, encryption and compliance capabilities in a single package. The combining of these capabilities seems natural for certain verticals and use cases, including health care, law enforcement, financial services and others with regulatory requirements to protect access to critical data. Ultimately, all organizations processing data and accessing systems they don't want made public will benefit from more integrated approaches such as DigitalPersona's.

To really achieve widespread adoption and use, security products have to offer ease of use that is (at a minimum) no worse than the prior experience or, ideally, offers an improvement by converging disparate functions, improving visibility, and making access easy on end users. DigitalPersona has achieved this with easy-to-use authentication (in this case, biometrics) and SSO to simplify the user login experience across multiple applications from multiple devices. For large complex organizations, managing multiple access and authentication requirements, DigitalPersona leverages commonly-used Windows directory and user services for easier administration.

DigitalPersona Pro provides a strong option for environments needing more than one of these capabilities (strong authentication, disk encryption and single sign-on) deployed on end points.

About the Author

Jim Hietala, CISSP, GSEC, is a frequent speaker at industry conferences. He has written several research whitepapers and participated in several webcasts for SANS. He has also published numerous articles on information security, risk management, and compliance topics in publications including CSO, The ISSA Journal, Bank Accounting & Finance, Risk Factor, SC Magazine, and others. Jim sits on the advisory board for the Open Security Foundation. He contributed to the Cloud Security Alliance's version 2.1 guidance and is active in the development of standards and best practices in the IT security industry.

SANS would like to thank its sponsor:

