

Raising the Bar on Mobile Workforce Security with Integrated Data Protection and Strong Authentication



July 2011

Increasingly mobile workforce poses new threats to businesses

The growing adoption of laptops and other portable devices is changing the foundation of traveling and telecommuting. Laptops have overtaken desktops as the computer of choice for business users. By 2012, Forrester estimates that mobile PC usage will increase from 32% to 43%¹.

As a result, notebooks and netbooks have grown to occupy two roles within the organization:

- They are repository of confidential data, including business plans and customer information.
- They are the access point through which users log on – including remotely – to business resources such as networks, shared drives and enterprise applications.

While endpoint protection has been traditionally associated with solutions like antivirus and firewalls, these technologies don't adequately protect data against theft, loss or unauthorized access.

New needs and solutions pose new IT management challenges

IT managers have responded to the new security threats by adopting solutions aimed at protecting data stored on portable computers and securing access to enterprise systems. According to a recent study by Aberdeen Group, as many as 76% of best-in-class organizations are investing or considering hard drive encryption solutions to more effectively protect data in case notebooks are lost or stolen². More than half

¹ *The Costs and Challenges Associated with Supporting Today's Information Workers*, Forrester Consulting, 2009.

² *Full Disk Encryption on the Rise*. Aberdeen Group, 2009.

of best-in-class firms have deployed authentication methods that go beyond username and passwords.

Adopting new technologies, however, is often not a simple task, especially when an organization is looking at more than one solution to provide the type of comprehensive protection mobile workers need.

Challenges include:

- High out-of-pocket and management costs due to deploying and maintaining multiple management systems.
- Compatibility issues that may arise if some of the selected applications do not peacefully coexist on managed computers.
- Increased support costs due to the difficulties experienced by end users in dealing with many different systems to accomplish different operations (e.g. unlocking the PC, logging on to the VPN, etc.).

Integrated solutions help achieve comprehensive security and lower IT costs

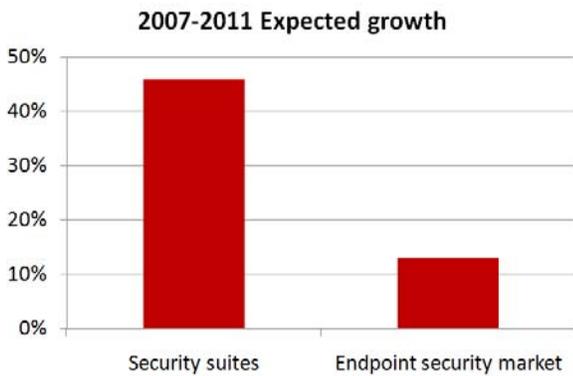
Solutions that integrate data protection and strong authentication help solve the security challenges organizations face while lowering the administrative burdens and costs often associated with multiple, independent solutions.

Integrated suites can help organizations achieve high security and compliance with internal and external mandates while also providing:

- Lower out-of-pocket costs
- Simplified management - thanks to a single administrative interface or console
- No compatibility issues among different security applications

- Single agent on managed clients
- Streamlined user experience, which often results in lower support costs

The growth of security suites is dramatically outpacing the expansion of the overall endpoint security market³. This reflects how appealing and valuable security suites are for businesses.



Aberdeen Group reports similar findings. Best-in-class organizations that adopt strong authentication methods are 31% more likely to use comprehensive solutions that provide an infrastructure capable of dealing with multiple applications and credentials⁴.

Gartner reports this trend is likely to affect security software providers, as they will optimize their offering to follow customers' interest and needs for comprehensive security suites⁵.

Mobile security brings a high ROI

The Return on Investment (ROI) for data protection and access management solutions primarily comes from two areas:

- Reduction in potential liabilities in the case of security breaches, for example if a notebook is lost
- Direct cost savings that translate into lower recurring operating expenses

Market studies show that solutions such as full disk encryption protect intellectual property and other sensitive information if a computer is lost or stolen. According to Aberdeen Group, companies lose at least 4.7% of their computers every year⁶ and The Ponemon Group says each of them carries IP worth almost \$6,000⁷.

Using alternative authentication methods instead of usernames and passwords can help reduce the volume of password-related Help Desk calls by as much as 70%^{8,9}. This can provide significant savings; Gartner estimates that password calls can consume upwards of 30% of companies' support resources at a cost of \$17 per call¹⁰.

In addition, Datamonitor and Microsoft show that efficient management of strong authentication can

³ *Strategies for Endpoint Security*, InfoWorld, 2009.

⁴ *Strong User Authentication: Best-in-Class Performance at Assuring Identities*. Aberdeen Group, 2008.

⁵ *Magic Quadrant for Mobile Data Protection*, Gartner, 2008.

⁶ *Laptop Lost or Stolen? Five Questions to Ask and Answer*. Aberdeen Group, 2010.

⁷ *The Cost of a Lost Laptop*. The Ponemon Institute, 2009.

⁸ *Toolkit: Evaluating Enterprise Options for Managing Passwords*, Gartner, November 2006.

⁹ *Applications at Their Fingertips*, Federal Computer Week, August 2004.

¹⁰ *Id.* at 8.

help organizations lower the costs of user authentication by as much as 90%¹¹.

Together, these potential cost saving items can enable a company with 1,000 users to save as much as \$340,000 in IT-related costs per year:

Cost saving item	Potential savings
Savings in value of lost Intellectual Property	\$ 275,937
Savings in password-related Help Desk calls	\$ 54,275
Savings in IT costs by adopting efficient management of authentication	\$ 10,745
Total potential cost savings	\$ 340,957

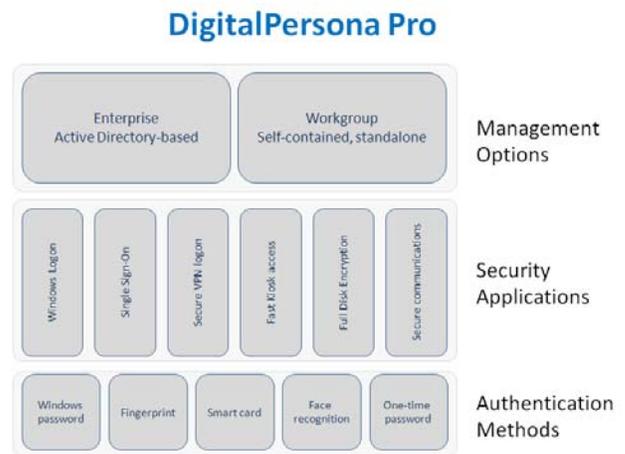
In addition to the direct cost savings, data protection and strong authentication solutions may reduce an organization’s exposure to liabilities that arise from security breaches. Aberdeen Group estimates that each security breach may cost up to \$640,000 in legal costs, lost revenues, etc. Just a handful of security breaches could generate costs adding up to millions of dollars.

Best-in-class organizations using data protection solutions such as full disk encryption have been able to reduce the number of breach exposure incidents experienced in the last twelve months by 84%¹². Similarly, more than half of the best-in-class companies that use strong authentication reduced the number of security breaches over the last year and 80% reduced the number of human errors related to security.

The solution: DigitalPersona® Pro

DigitalPersona Pro provides small businesses and enterprises with a powerful, flexible solution for integrated data protection and strong authentication. This centrally-managed suite of security applications

guards business information against unauthorized access. It protects data and controls access to computers and applications. With Full Disk Encryption, Two-factor VPN Authentication, Single Sign-On, Digital Signature and more, DigitalPersona Pro enables businesses to increase security and achieve compliance while reducing operating costs. It provides support for a variety of authentication credentials and offers flexible management options to adapt to your needs and requirements.



Key benefits of DigitalPersona Pro include:

- One solution to centrally manage multiple security applications and provide comprehensive security for the mobile workforce. You can deploy the entire solution or choose which configuration and applications fit your immediate needs.
- Full disk encryption with pre-boot authentication and BIOS-level integration¹³.
- Strong authentication with a variety of credentials, including fingerprint, face recognition, smart cards, one-time (OTP) tokens and smartphones. DigitalPersona Pro

¹¹ The ROI for Enterprise Smart Cards, Datamonitor and Microsoft.

¹² Id at 2.

¹³ Available on select computers.

takes advantage of fingerprint readers that are built into notebooks or attached as peripherals and supports a wide range of smart cards and OTP devices.

- Two-Factor VPN authentication for secure remote access. DigitalPersona Pro supports all RADIUS-based Virtual Private Networks, such as Cisco, Juniper, Check Point and others.
- Single Sign-On to all enterprise applications, including Citrix, Web apps, Windows applications, legacy green-screen terminals, and more.
- Powerful emergency access recovery to securely “rescue” users who are locked out of their PCs, even when a network connection is not available.
- Ability to roam users’ credentials across computers and across applications, providing consistent strong authentication without per-machine setup.
- Support for shared workstations, such as financial institutions, police vehicles and kiosks in hospitals.
- Flexible deployment options that include a cloud-based Software-as-a-Service solution, as well as Active Directory-based one.
- High security with FIPS 140-2 compliant encryption for sensitive user data.
- High Return on Investment and low Total Cost of Ownership with savings over 50% in out-of-pocket costs over individual solutions.

DigitalPersona’s award-winning technology has been used worldwide by thousands of companies and more than 100 million users for security and compliance. Customers range from small businesses to the US Department of Defense, from hospitals to banks.

DigitalPersona also powers HP ProtectTools, the security suite preloaded by Hewlett-Packard on millions of business notebooks and desktops every year. Now you can use DigitalPersona Pro to centrally manage HP ProtectTools-enabled computers or any mixed environment of HP ProtectTools and DigitalPersona Pro client software.

Questions? Contact us!

For more information about DigitalPersona Pro, visit www.digitalpersona.com or contact us at:

- Email: sales@digitalpersona.com
- North America contact: +1-650-474-4000
- EMEA contact: +44-203-286-4004

Free trials are available.

About DigitalPersona

DigitalPersona, Inc. is a global provider of authentication and endpoint protection solutions that make security simple, practical and affordable for businesses of all sizes. The company helps enterprises, government agencies, custom application developers and independent software vendors to efficiently address growing security, compliance and fraud-prevention demands. DigitalPersona’s award-winning technology is offered by market-leading computer manufacturers and solution providers around the world.

Disclaimer

THE INFORMATION IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED TO BE ANYTHING OTHER THAN THE

EDUCATED OPINION OF THE AUTHOR. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT DIGITALPERSONA MAKES NO CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS, OR ADEQUACY OF THE INFORMATION. THIS INFORMATION SHOULD NOT BE RELIED UPON AS LEGAL ADVICE. DIGITALPERSONA SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS OR COMPLIANCE WITH ANY LEGAL REQUIREMENTS.

© 2011 DigitalPersona, Inc. All rights reserved. DigitalPersona, is a trademark of DigitalPersona, Inc. registered in the U.S. and other countries. All other brand and product names are trademarks or registered trademarks of their respective owners.