An Integrated and Cost-Effective Solution for Access Control and Data Encryption

A Frost & Sullivan White Paper
Prepared by Robert Ayoub, CISSP
Global Program Director—Information Security
Executive Summary ........................................................................................................... 4

Why Does Your Business Need Enterprise Class Access and Data Security Solutions? ................................................................. 5

The Changing Threat Landscape ....................................................................................... 5

Compliance and Regulatory Requirements ........................................................................ 6

Privacy and Confidentiality .............................................................................................. 6

Challenges in Implementing Traditional Access Control and Data Encryption Solutions ........................................................................ 7

Cost of Ownership ............................................................................................................ 7

Level Complexity ............................................................................................................. 8

Lack of Flexibility ............................................................................................................. 8

Better Authentication: Increased Security and Operational Efficiency ......................... 8

The DigitalPersona Solution ........................................................................................... 9

Ease of Deployment ......................................................................................................... 9

Straightforward Pricing .................................................................................................. 9

A Complete Solution ...................................................................................................... 10

How DigitalPersona Addresses Industry Best Practices ............................................. 10

Cost Effective ................................................................................................................ 10

Ease of Integration ........................................................................................................ 11

Flexibility ....................................................................................................................... 11

Conclusions .................................................................................................................... 11
EXECUTIVE SUMMARY

The modern organization finds itself in a precarious situation. Security is necessary, but implementing an effective balance among strength, usability and manageability can be very difficult. Too much security, and end-users will revolt or compromise security solutions, accidentally or intentionally. Too little security, and organizations increase the risk that their data, applications or networks will be breached.

In order to address the risk, organizations have significantly increased their spending on information security solutions. The growth of mobile devices is exposing data to ever-greater threats as the notebook computer is now the point of access for an employees’ “digital life.” This unprecedented access to the corporate network from outside the corporate walls is driving significant spending on solutions to keep data secure. Figure 1 below illustrates the growth occurring in spending on endpoint security products. Even with the global recession, organizations still devoted significant portions of their budgets to endpoint security and authentication solutions. Frost & Sullivan does not see a slowdown in this spending in the near term.

Enterprise Spending on Endpoint Security and Authentication Solutions

Unfortunately, despite increased spending on endpoint security and authentication solutions, many professionals still believe organizations are at a high risk of attack from insiders, viruses, and phishing threats. This has left many organizations struggling to understand what else can be done.

Traditional endpoint security solutions usually include a mix of anti-virus, anti-spyware, and personal firewall capabilities. These products are ubiquitous in the modern enterprise; however, Frost & Sullivan believes that two key components are missing from the majority of endpoint security deployments. One is irrefutable verification of identity, and the second is security of data itself.
One of the key weaknesses in most security solutions today is the lack of identity awareness. The vast majority of devices and applications only require a username and password for entry, and many studies have shown the inherent weaknesses of the username/password combination.

The second weakness with most endpoint security solutions is the lack of a data security component. As employees continue to be more mobile and data flows to smartphones, laptops, and tablets, the need to protect an organization's data is paramount.

This white paper will examine the changing threat landscape and discuss the wide variety of solutions that are necessary to keep employees safe. This paper will discuss the challenges associated with many identity, authentication and data security solutions on the market today—price, scalability, and complexity. Finally, this paper will look at the DigitalPersona solution, a solution that Frost & Sullivan believes provides an effective, standards-based solution for small and medium enterprises while maintaining enterprise class features and functionality.

**WHY DOES YOUR BUSINESS NEED ENTERPRISE CLASS ACCESS AND DATA SECURITY SOLUTIONS?**

**The Changing Threat Landscape**

Cybercriminals are more sophisticated than ever before. As evidenced by the January 2010 attacks on Google, even the largest companies still fall prey to attack. Despite increased spending on information security products, more successful breaches are occurring every year. This makes the obvious point that existing controls have not adequately addressed the modern threat. The 2010 Verizon Data Breach Investigation Report gives a sobering illustration of this fact. In reviewing hundreds of live incidents, Verizon found that misuse of privileges (48 percent of breaches), hacking (40 percent of breaches), and malware (38 percent of breaches) were the top attack vectors.¹

Some organizations may not believe they are attractive targets to criminals. As it turns out, all the major attack vectors today are just as likely to impact an organization with 100 users as they are to organizations with thousands of users. Verizon's 2010 Incident Report also looked at size of organizations reporting breaches and found that 50 percent of breaches occurred at businesses with less than 1,000 employees, and more than 75 percent occurred at organizations with less than 10,000 employees.² This goes against traditional thinking that small businesses don't have valuable information or are “just not worth it” to criminals. Adding to the challenge is the reality that small and mid-sized businesses do not always have the personnel, money, or time to devote to managing security systems full time.

On top of all these technical challenges, businesses of all sizes have tightened budgets to contend with, making them do even more with fewer resources.

---

¹ 2010 Verizon Data Breach Investigation Report
² 2010 Verizon Data Breach Investigation Report
**Compliance and Regulatory Requirements**

Whether mandated by industry or geography, there are few businesses that are not affected by regulatory or industry directives. The requirements for data and client security are similar regardless of company size. As a result, even the smallest companies find the need to adhere to the alphabet soup of regulations. Notable samples of global regulations are listed below.

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Objective</th>
<th>Regulated Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>Protect patient personal health information (PHI) and personal identifiable information (PII) from misuse and improper disclosure</td>
<td>Any organization in the healthcare field, including but not limited to: clinics, hospitals, doctor’s offices, healthcare facilities in schools, pharmacies, insurers, and pharmaceutical companies</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standards (PCI-DSS)</td>
<td>Protect the private information of credit card account holders (account number, name, service code, and expiration date) from unauthorized disclosure</td>
<td>Physical and online retailers, merchants, and payment card processors and clearinghouses</td>
</tr>
<tr>
<td>Sarbanes-Oxley Act (SOX)</td>
<td>Protect non-public financial data and intellectual property (IP) from improper disclosure</td>
<td>All companies publicly traded in the U.S.</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Financial Modernization Act (GLBA)</td>
<td>Protect the security and confidentiality of client non-public personal information</td>
<td>Financial services firms, including banks, financial institutions, insurers, and security brokers</td>
</tr>
<tr>
<td>State data notification and privacy laws. Notable examples: California SB 1386 and Massachusetts Data Protection Law 201 CMR 17.00</td>
<td>Protect personal identifiable information (PII) as defined by the state</td>
<td>Organizations conducting business with customers in a covered state</td>
</tr>
<tr>
<td>Basel II</td>
<td>Protect non-public financial data and intellectual property (IP) from improper disclosure</td>
<td>Global financial services organizations, specifically internationally active banks</td>
</tr>
<tr>
<td>CJIS Security Policy</td>
<td>Protect data in the FBI Criminal Justice Information System</td>
<td>State and local government agencies accessing the FBI Criminal Justice Information System</td>
</tr>
</tbody>
</table>

**Privacy and Confidentiality**

Customers have become increasingly concerned with privacy and confidentiality. Many public security breaches have led to loss of customer trust and loss of business. In fact, the 2008 (ISC)2 Global Information Security Workforce Survey illustrates how privacy and
confidentiality concerns are ranked by information security professionals. Figure 2 below clearly indicates that concerns around privacy, confidentiality, and data loss are key pain points for modern organizations, with a majority of information security professionals ranking each of the below areas as high or top priority for the organization.3

**High or Top Priority Concerns Ranked by Information Security Professionals**

![Image of bar chart showing priority ratings for different concerns]

**Figure 2—Information security professionals’ rankings of top concerns**

**CHALLENGES IN IMPLEMENTING TRADITIONAL ACCESS CONTROL AND DATA ENCRYPTION SOLUTIONS**

As companies start to address their access control and data encryption challenges, they immediately look for industry standard solutions. Unfortunately, many organizations quickly realize that there are a number of significant challenges with most authentication and data access solutions on the market. Some of the key challenges include:

**Cost of Ownership**

Most enterprise solutions are designed for large enterprises with full dedicated information security departments. The products are expensive and often require expensive maintenance agreements and consulting engagements just to implement. Frost & Sullivan tracks numerous segments within the information security market and finds that list prices for data security solutions typically range from $50 to $70 per user. Disk encryption solutions are even more expensive, typically ranging from $70 to $120 per user. While many vendors offer volume discounts, most mid-tier businesses often find themselves paying close to list prices. Only the largest organizations have the volume that is necessary to get significant discounts. On top of the per-user costs, the maintenance and consulting costs make most solutions prohibitive for many organizations.

---

3 2008 (ISC)2 Global Information Security Workforce Study
**Level of Complexity**

Traditional access control and encryption solutions are complex. Often these solutions have their own independent management consoles and require specialized training to deploy and use. In environments with sufficient resources, this overhead is less of a challenge. In many mid-sized businesses, the IT and security departments are often one in the same, and there is rarely enough personnel to dedicate resources to managing new solutions. Adding complex solutions increases the likelihood of increased user difficulties and increased help desk costs. With many industry reports citing help desk costs at $175 per incident, a solution that minimizes complexity has direct positive impact on the bottom line.

**Lack of Flexibility**

Traditional access control and encryption solutions lack flexibility—in deployment options and in the security provided. Most traditional solutions focus on solving one single problem. While these solutions are often very good at solving one key pain point, an organization facing today’s challenging economic and regulatory environment needs solutions that can solve a multitude of problems in a cost-effective way. One size does not always fit all groups or users within an organization, and organizations need a solution that can manage different authentication or data security policies to address the unique needs of different groups or employees.

**BETTER AUTHENTICATION: INCREASED SECURITY AND OPERATIONAL EFFICIENCY**

There should be no doubt that better authentication provides increased security for the organization, both for access control and data security purposes. Frost & Sullivan also believes that better authentication is fast becoming a necessary component of increased operational efficiency. The factors listed below illustrate some of the key trends that are driving this need:

- The number of application-level passwords continues to increase, along with controls that force users to change the passwords constantly. This is driving an increased need for managing all of those passwords. As the number of passwords each user has to deal with explodes, help desk costs increase due to password reset requests and users looking for shortcuts, such as using the same passwords across multiple systems in order to keep up.

- Compliance rules such as HIPAA and PCI are beginning to mandate stronger security around the access of sensitive data, requiring organizations to implement strong authentication and encryption in order to be compliant. Compliance mandates are not based on the size of the business, meaning all organizations must address these mandates.

- Most information security controls are not identity-aware; they still rely on some combination of username and password. Ultimately, even security solutions that should be strong in theory (such as disk encryption) could be easily circumvented if a weak
administrative password was used. Even more disturbing is that many information security solutions rely on the controls provided by the operating system—again, a username and password combination. Even though simple to implement, there are numerous industry studies pointing to the weaknesses of this combination. Recent reports of the Gawker breach illustrate just how many users continue to use the same password across accounts or use weak passwords.

• Economic conditions have forced IT decision-makers to ensure that investments made in their business provide future-proofing of the environment as well as provide a simple way to leverage new technologies like biometrics, smart cards and other credentials to simplify operations and reduce costs.

• There are multiple advantages to having a single authentication framework for multiple security applications. It allows users to enroll their credentials only once, there is no risk of incompatibility, there is no need to carry around different smart cards/tokens/credentials to accomplish different tasks, and the same authentication management system can be used for different credentials and applied to different user groups if "one size doesn’t fit all."

• Ultimately, improved data access control and authentication lowers the risk to the organization. It removes the challenges posed by a compromised password and provides a significant deterrent to hacking or the misuse of privileges.

THE DIGITALPERSONA SOLUTION

DigitalPersona offers a standards-based data security and access control solution for enterprises of all sizes. The solution is easy to install and administer, and offers a significant price advantage over many solutions on the market. Some of the key features of the DigitalPersona solution are listed below:

Ease of Deployment

DigitalPersona products make it easy for small or mid-sized businesses to deploy a solution in line with their existing infrastructure. DigitalPersona Pro is designed to integrate directly into Active Directory, eliminating the need for a separate console and speeding up the learning curve. Small businesses have the option of purchasing DigitalPersona Pro Workgroup, which provides a standalone deployment of the solution that does not require any IT infrastructure, while still providing centralized management. Both deployment methods provide similar functionality, while allowing customers the flexibility of choosing the best option for their organization.

Straightforward Pricing

DigitalPersona offers straightforward, per-computer pricing that includes all the products offered by DigitalPersona. Instead of paying and maintaining multiple vendor relationships, an organization can simply pay one flat price for the entire suite of solutions provided. DigitalPersona Pro’s modular structure and pricing also allows companies looking to solve
just one specific security problem (e.g., strong authentication) to only deploy the modules they are most interested in, and then expend the solution over time as their needs evolve. This allows organizations to purchase a solution based on the precise needs of the organization at a certain period in time.

**A Complete Solution**

An enterprise deploying DigitalPersona can offer its users strong authentication integrated into Disk Encryption (with BIOS integration), Single Sign-On (for all enterprise applications), Two-Factor RADIUS authentication, digital signature, and other solutions. This integration helps simplify the deployment of access control and data encryption. This leads to more content users and lower total cost of ownership.

![Management Options](image)

**Security Applications**

- Full Disk Encryption
- Email Encryption
- Windows Password

**Authentication Methods**

- Self-Contained, for Small Businesses
- Enterprise Single Sign On (SSO)
- Document Encryption
- Fingerprint

**Figure 3**—DigitalPersona offers a completely integrated, centrally managed solution suite.

**HOW DIGITALPERSONA ADDRESSES INDUSTRY BEST PRACTICES**

Frost & Sullivan believes the DigitalPersona solution addresses many challenges inherent in traditional, enterprise-focused access control and encryption solutions.

**Cost-Effective**

The DigitalPersona solution is very cost-effective when compared to purchasing and installing solutions from a variety of vendors. As illustrated in Figure 4, this can result in more than 50 percent savings on a per-user basis.
Ease of Integration

The DigitalPersona solution allows for easy integration into the existing organizational IT infrastructure. The two deployment options offered by DigitalPersona allow organizations the ability to deploy the solution based on the existing network configuration. By integrating directly into an organization’s existing Active Directory configuration, DigitalPersona Pro provides administrators with a predefined management console that is familiar and operates just like other Active Directory consoles. For organizations that do not have Active Directory or customers that don’t want to take advantage of that integration, DigitalPersona Pro Workgroup offers a standalone console that is likewise easy to deploy and use, including in small businesses or departments within larger corporations.

Flexibility

DigitalPersona is focused on offering a flexible solution for customers that can address the wide spectrum of authentication and encryption needs required by the organization. This allows the organization to provide the appropriate level of security to different users and groups within the organization. The DigitalPersona solution also gives organizations the ability to future-proof their businesses by providing all data security solutions as part of the license, requiring only a checkbox for deployment.

CONCLUSIONS

There is no doubt that the increased mobility of the workforce and the continued evolution of the threat landscape will continue to drive the need for increased access control and encryption by all organizations. Unfortunately, many solutions around access control and data encryption are targeted at the large enterprise. These solutions are highly effective, but tend to be complex and expensive. Frost & Sullivan believes that DigitalPersona’s solution offers the mid-sized enterprises and small businesses an effective alternative to large solutions that is integrated, easy to deploy and flexible, as needed.
ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company’s TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 35 offices on six continents. For more information about Frost & Sullivan’s Growth Partnership Services, visit http://www.frost.com.

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041