Flexible, secure solutions to keep unauthorized users out of your data

The status quo of authentication has long been the password, but passwords are widely known by both security professionals and end users to be broken and are considered to be the weakest link of security today. Why? Because end users write down passwords on paper or keep a list of them on their PCs. They choose passwords that are easy to remember or use the same password for access to all of their personal and business systems, and so forth.

When we hear that hackers have gained access to accounts or systems, a likely point of attack was via a user password gained inappropriately. Social Engineering, phishing, Advanced Persistent Threats (APT) and password resets are all used by hackers to gain access to individual's data and business information.

No matter the size of your organization or how much data you have, safeguarding the information stored on your systems is critical. Your first line of defense lies at the endpoint, and having the right authentication solutions in place can greatly strengthen your protection against a security breach. In many cases, this means moving beyond passwords to more advanced authentication measures.

Dell Data Protection | Security Tools

Dell Data Protection | Security Tools (DDP | ST) is an end-to-end software security solution included with all Dell Precision™, Latitude and OptiPlex systems. DDP | ST supports advanced hardware authentication, such as Dell's fully-integrated fingerprint, smart card or contactless smart card reader options. Dell Data Protection | Security Tools can help manage these multiple hardware authentication methods, support pre-OS login with self-encrypting drives, single sign-on (SSO) and manage user credentials and passwords.

In addition, Dell Data Protection | Security Tools provides advanced authentication capabilities to access not only PCs, but any website, SaaS or application. Once users enroll their credentials, DDP | ST allows use of those credentials to logon to the device and perform password replacement. Multifactor policy can be defined as well if required or desired.

Profiles can be set up for each application or website to associate the user's enrolled advanced authentication credentials with the password of that application or service. When the user subsequently accesses that site or application, they are prompted to use their advanced authentication credential instead of typing in the password. This allows the user to choose a stronger, more complex password that they don't need to write down — and in fact, don't even need to know. This significantly raises the level of access security.

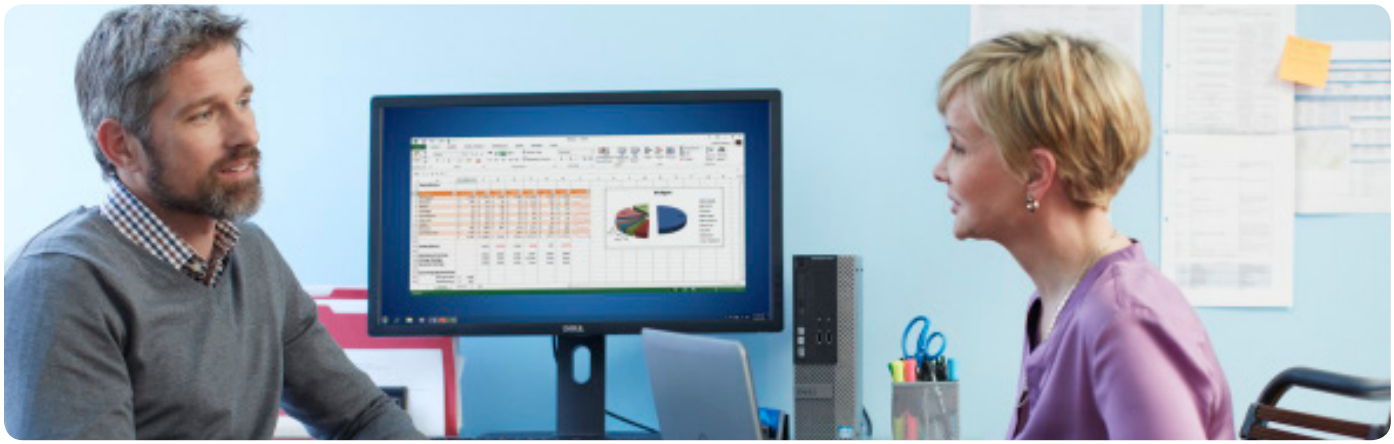
Finally, Dell Data Protection | Security Tools is integrated with the Dell Data Protection remote management console, so you can centrally manage both your authentication and encryption solutions.

Trusted Platform Module (TPM)[1]

For added security, Dell Latitude laptops ship with the only FIPS 140-2 compliant TPM in the industry today. Dell Data Protection | Security Tools stores user credentials in TPM-protected credential stores. It uses TPM to protect the encryption key for user credential containers stored on the system hard drive as well as being used by other Dell Data Protection applications to protect authentication and encryption tokens.

Dell ControlVault™[1] 2.0

Dell ControlVault 2.0, available on select Dell Latitude laptops, offers secure hardware processing and storage for all user credentials — such as user passwords, smart card data or fingerprint data — used during Microsoft Windows preboot.



ControlVault fully isolates a user's credentials from potentially unsecured operating systems and hard drives. The cryptographic secrets which protect the user data, when stored on the PC, are kept in a secure cryptographic co-processor hardware device and are processed inside that device instead of in main memory where viruses can spy on the process. This option helps ensure the ultimate protection, even against sophisticated hackers attempting to gain access to critical systems.

Any OS is inherently difficult to secure from malware, which has become a multi-billion dollar, well-organized industry. Dell ControlVault™ avoids malware by storing and matching credentials in a separate secure process. It is a security subsystem fully isolated from the host OS and associated malware and consists of a local secure memory, integrated fingerprint processing and integrated FIPS 201 contacted and contactless smart card readers.

Dell offers the world's most secure commercial PCs

Dell's advanced authentication solutions, in combination with Dell Data Protection solutions for comprehensive encryption and leading-edge malware prevention help make Dell commercial PCs some of the most secure in the industry. To learn more about Dell Data Protection solutions, visit www.dell.com/dataprotection.

Technical Specifications

Dell Data Protection | Security Tools is pre-installed on all Dell Latitude, OptiPlex, and Dell Precision™ systems.

Operating Systems supported:

- Windows® 7 Enterprise, Professional, and Ultimate
- Windows 8 Enterprise and Pro

Hardware supported:

- Fingerprint readers
- Smart Card readers
- Contactless Smart Card readers

Dell ControlVault™ is available on select Dell Latitude laptops.

Dell FIPS 140-2 compliant TPM is available on select Dell Latitude laptops and select Dell Precision mobile workstations.

Learn more at www.Dell.com/DataProtection

1. Offering may vary by country and by configuration.