SECURITY SIMPLIFIED: UNDERSTANDING THE BASICS OF DEPLOYING AND MANAGING SECURE ENDPOINTS

By David Schweighofer

With the ranks of mobile and remote workers expanding every day, cost-effective endpoint security is a growing business concern that enterprise IT organizations avoid at their peril. Dell advances enterprise-wide protection with a balanced approach that focuses equally on safeguarding data and preventing unauthorized access.

Related Categories:

Dell Latitude laptops

Security

Visit DELL.COM/PowerSolutions for the complete category index.

In a world where digital information is the key to business and a significant proportion of workers are mobile, data loss is both a worst-case scenario and a daily occurrence. Regardless of whether it is accidental or the result of a security breach, data loss puts organizations at risk of losing market share, damaging shareholder confidence, and incurring compliance fines. Even a single day of downtime can cost thousands of dollars in lost worker productivity, IT administrator time, and data recovery costs.

For many organizations, the risk of business process failures threatens to compromise data security even more than the possibility of an external attack. Securing data on mobile systems can be complex for enterprise IT administrators, which increases the chance that security procedures will be followed improperly or overlooked. Security also can be burdensome and frustrating for end users. Complying with security policies typically requires multiple steps, settings, and actions that can become a barrier to implementation—leading to devastating business consequences.

For these reasons, organizations must protect their IT assets with endpoint security solutions that are simple to deploy and use. By providing a broad choice of world-class security offerings along with deployment and configuration services, Dell can help enterprises secure key data as well as reclaim wasted time and redirect it toward business growth.

UNDERSTANDING REQUIREMENTS FOR ENDPOINT SECURITY

To effectively meet today's endpoint security challenges, enterprise IT departments need a comprehensive approach that addresses three main requirements (see Figure 1):

- **Fast deployment:** Built-in security features such as always-on hard drive encryption help prepare systems for secure operations on delivery.
- **Enhanced protection:** Stringent security technologies for user authentication and access help safeguard precious data and ensure regulation compliance.
- **Smart prevention:** Multiple layers of security help protect valuable assets.

SIMPLIFYING SECURE DEPLOYMENTS

Dell helps simplify mobile security through platforms that are easy to use and manage, including a comprehensive suite of data security options that enable organizations to deploy secure systems direct from the factory. Of course, preventing unauthorized access is equally important. Best practices reach beyond system login procedures to involve facilities

management and human resources processes as well.

> "Dell helps simplify mobile security through platforms that are easy to use and manage."

Encryption provides a first line of defense for data protection

Dell™ systems support several types of encryption. File and folder encryption helps secure data with a digital signature, whether information is in transit over the network or at rest on an internal system—helping minimize the possibility that it will be altered or accessed by unauthorized users either internally or externally. It also helps to secure enterprise data by converting files and text into "cipher text" that can be decoded to its original form only with a valid password or encryption key.

Hardware encryption goes one step further to help ensure data security. Full-disk-encryption hard drives are accessible only through a password, and are designed to work without requiring user intervention or compromising system performance. When unlocked, however, the user interface is easy to use, simple, and transparent.

Dell laptops offer full-disk-encryption hard drives. Dell recently added a 7,200 rpm hard drive option to enhance performance while maintaining a high level of security. Dell also offers an encrypted solid-state drive (SSD) in a range of mobile devices, which combines the durability and reliability of SSDs with strong data protection capabilities.

Protecting sensitive data is a necessary first step to securing enterprise information—but it is not the whole story. By adding multiple access controls, Dell enables organizations to strengthen their authentication processes by implementing multi-factor authentication, which helps ensure that only authorized users get access to valuable information assets. Dell offers a range of authentication technologies, including biometric readers, smart card readers, and contactless smart cards to help support a consistent, cost-effective security strategy for simplifying processes.

Integrated fingerprint readers provide strong authentication

As a result of the strong authentication technology defined by Federal Information Processing Standard (FIPS) 201, a variety of U.S. government employees—including transportation workers and emergency first responders—are using FIPS 201 fingerprint identification technologies as the foundation for biometrically enabled identity credentialing programs.

The Dell Latitude™ E6500 laptop is designed to include an optional FIPS 201–certified fingerprint sensor and Personal Identity Verification (PIV)–compliant smart card reader. Latitude laptops feature the UPEK TouchChip (TCS1) silicon fingerprint sensor, which is designed to meet the demanding FBI fingerprint image quality requirements, fit easily into a tight space, and meet the low-power requirements for laptops.

Many Dell business laptops can be ordered with swipe fingerprint readers. Dell Latitude E-Family laptops and Dell Precision™ mobile workstations offer optional fingerprint readers.

Contactless smart card readers enhance security for mobile employees

Contactless smart cards can be used in various facilities management scenarios—for example, regulating access to company buildings and paying for food at the cafeteria. Dell Latitude E-Family Mainstream and Ultra-Portable laptops offer a radio-frequency identification (RFID)–based contactless smart card reader option. Administrators can enhance security for mobile employees by combining something employees own (a smart card) with something they know (their password) on an identified platform—the Trusted Platform Module (TPM) or Dell ControlVault™ platform.

Embedded smart card readers help make it easy and cost-effective to deploy smart cards for security. Latitude E-Family laptops avoid the requirement for peripheral readers, which occupy a USB port that may be needed for other peripheral devices. Latitude E-Family laptops are the first laptops to offer an embedded contactless smart card reader that supports multiple types of cards.

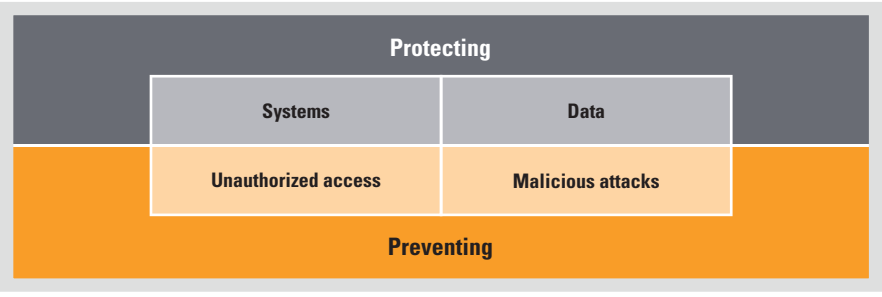

Figure 1. *A comprehensive approach to endpoint security helps protect data and prevent unauthorized access*

Trusted Platform Module software enables secure access to networks

For strong authentication, Dell business clients are often equipped with TPMs. This versatile chip—a microcontroller located on the motherboard of Dell laptops—helps to authenticate a system in an IT infrastructure and stores user credentials such as passwords, digital certificates, and cryptographic keys.

In addition to storage, the chip can securely generate or limit the use of keys for signing and verification as well as encryption and decryption. Capabilities of the TPM include remote attestation, which creates an unalterable summary of the hardware, boot, and host OS configuration to enable a third party to verify that software has not been tampered with. Other capabilities include sealing encrypted data so that it can be decrypted only in the same state.

Dell ControlVault technology dedicates processing power to security

For an additional level of security, Dell ControlVault technology provides a dedicated processor for authentication and certificate storage.[1] Although TPM and ControlVault technologies both store keys and have similar benefits, the ControlVault approach offers additional features designed to improve security. For example, the ControlVault chip can store and execute code using a secure processor—helping protect it from malware attack vectors that typically target RAM or hard drives.

While TPM uses a 160-bit password, ControlVault also supports use of personal authentication methods (such as fingerprint readers, smart cards, and contactless smart cards) to access credentials. The ControlVault chip is designed to store all credential types, allowing a single point of migration and supporting a broad variety of cryptographic algorithms (including Suite B and native error checking and correction). In addition, it supports standard and contactless smart cards, fingerprint readers, and RSA SecurID tokens.

ControlVault helps to protect secure operations by isolating them from the OS environment and memory. Many applications execute their secure operations on the host x86 processor, which exposes it to sniffing of interim values and modification of the final result. Even if the encryption key itself is concealed with another key, the encryption key is still on the hard drive and out in the open. And even if the key is hidden among other data, hackers have programs that can search the hard drive and quickly locate the key.

By sealing off code execution, ControlVault can help protect against these threats. All processing and storage of critical data takes place on a processing and memory chip, which creates a protective boundary. Access to the keys is strictly controlled by an authorization scheme that is designed to prevent any application from accessing the keys without satisfying the authentication requirements set up by the owner or IT manager of a particular ControlVault-protected boundary. In addition, a small memory footprint helps ensure that ControlVault incurs minimal impact on overall system performance.

ControlVault also serves to control access to reference templates. To verify authentication, a reference template—which is created and stored at time of enrollment—must be accessed. Applications usually store this template on the hard drive, thus exposing it to modification, extraction, and copying. ControlVault helps eliminate these threats by allowing applications to store templates inside the ControlVault-protected boundary. Template access is then controlled by an authorization scheme designed to prevent any application from accessing the keys without satisfying the authentication requirements set up by the owner or IT manager of a particular ControlVault-protected boundary.

Dell ControlPoint helps simplify endpoint security management

Authentication is critical to endpoint security—but IT departments must enforce strict rules to strengthen the authentication, which can create complexity for end users. To help simplify using and managing security features, Dell ControlPoint software includes a Security Manager module (see Figure 2).

The ControlPoint platform gathers hardware and security settings within a single intuitive user interface, helping avoid the need to search through multiple control panels for a specific setting. By providing a standardized user interface to access a broad selection of security capabilities, ControlPoint software extends the available authentication offerings and helps simplify management of these options. In addition, the software helps to facilitate implementation and management of multi-factor authentication across multiple devices, including biometrics, smart cards, and contactless smart cards. This combination, when used with preboot authentication and hard drive encryption, provides enterprises with an extra layer of security.

RSA SecurID certification offers strong, cost-effective authentication

The RSA SecurID algorithm is embedded within the Dell ControlVault hardened firmware chip for storage and processing of credentials. RSA SecurID software token seeds are stored within ControlVault, outside the usual attack vector of malicious applications. A one-time RSA password is generated within

> **"ControlVault helps to protect secure operations by isolating them from the OS environment and memory."**

[1] Dell Latitude models E4200, E4300, E6400, E6400 ATG, E6400 XFR, and E6500 as well as Dell Precision models M2400, M4400, and M6400 offer Dell ControlVault and Dell ControlPoint technologies. Other Dell business laptops offer limited versions of these solutions.

Figure 2. *The Dell ControlPoint Security Manager module offers single-view management of security settings, features, and authentication*

the ControlVault chip. Mobile users can conveniently launch the software token from their laptops through Dell ControlPoint Security Manager.

By embedding the RSA SecurID software token within the Dell Latitude ControlVault firmware, the laptop is designed to offer the security of a hardware token combined with the cost-effectiveness and convenience of a software token. This approach helps avoid the need for administrators to replace lost tokens while affording mobile users the convenience of a consolidated device. By linking the two-factor authentication method directly to the laptop, desktop, or workstation, organizations help to ensure that employees are accessing enterprise information only from company computers.

The RSA SecurID software token can be easily licensed and provisioned by organizations with a deployment of Latitude E-Family laptops. Out-of-the-box interoperability with the RSA SecurID Token 4.0 for Windows Desktops allows users or IT administrators simply to install the RSA SecurID Desktop 4.0 application, which is designed to automatically register ControlVault as a token storage device.

ControlPoint Security Manager allows IT professionals to easily access and manage not only RSA SecurID tokens, but also user identification, fingerprint readers, and smart card security technology. The software enables limited access to network resources with a two-factor authenticator linked directly to an enterprise system—meaning that mobile users can use their own mobile device as an authenticator, rather than require an additional dedicated device for two-factor authentication. Integrated two-factor authentication can control access to hundreds of applications, including many from leading virtual private network vendors.

MEETING THE CHALLENGES OF ENDPOINT SECURITY

As the ranks of mobile employees grow, organizations must give resolute focus to protecting IT assets with endpoint security solutions. By understanding how to deploy and use a comprehensive range of endpoint security options, IT organizations can advance enterprise-wide security while enhancing productivity.

Dell endpoint security options start with encryption as a first line of defense for protecting data. In addition, Dell offers FIPS 201–certified fingerprint sensors, PIV-compliant smart card readers, and embedded smart card readers. An embedded contactless smart card in Dell Latitude E-Family laptops supports multiple types of cards. TPM chips offer a security option that helps provide strong authentication, and Dell ControlVault technology offers a dedicated processor for authentication and certificate storage. The RSA SecurID algorithm is embedded within the ControlVault firmware to store and process credentials, and Dell ControlPoint software includes a Security Manager module to help simplify endpoint security management.

Designed to simplify data protection and prevent unauthorized access, the Dell endpoint security options discussed in this article help IT organizations deploy and manage security to facilitate simple and secure data access throughout the enterprise.

David Schweighofer is the worldwide outbound marketing manager for Dell Latitude laptops on the Product Group Marketing team. He has a degree in Marketing and Organization as well as an M.B.A. from the HEC Lausanne business school.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

Dell security solutions:
DELL.COM/Security

Data Protection in a Mobile World:
dell.awakit-webcasts.com/index/webcastsList/series_id/4