HP ProtectTools Client Security Solutions Manageability for Customers with Limited IT Resources

Security challenges

Data protection on lost or stolen client devices is a growing concern among IT managers and business executives. The data stored on a PC or client device are often significantly more valuable to a business than the asset itself, and the loss, theft or unwanted disclosure of that data can be very damaging. Recent government regulations and mandates such as HIPAA, Sarbanes-Oxley, and international regulations focus on data protection and privacy; this legislation has a strong impact on organizational storage policies, especially for PC devices that are susceptible to loss or theft.

These laws are complex, however, one thing is invariably clear: the unauthorized disclosure of data can be damaging, with some regulations demanding substantial fines for the business and potentially for custodial sentences for offending parties. Many IT managers and business executives seeking to mitigate risks in this area are looking for solutions that increase protection around data and help provide compliance.

Beyond seeking security solutions for the PC devices, customers with limited IT resources will require manageability solutions to meet their security needs.

To begin, there are several simple guidelines that can assist with security manageability decisions:

1. There's no single vendor that provides all the solutions, and there is no single solution that fits all needs.
2. Each environment will have its own unique requirements, and these requirements form unique customer or usability scenarios.
3. All manageability should be done securely, but not all security attributes should be made manageable.

Security made easy

Providing protection for your business that is easy to use and easy to implement is top of mind as HP designs its products. Since there are many excellent security solutions available, it is HP's strategy to collaborate with and utilize the offerings of security software market leaders to provide customers with client security and security manageability solutions faster and more efficiently.

The purpose of this whitepaper is to provide information regarding HP's Client Security and Client Security Manageability strategy in conjunction with key security companies and their capabilities as they apply to common usability scenarios. Throughout this paper, HP's key collaborators will be identified and discussed as they provide client security manageability solutions to support offerings on HP's desktops, notebooks, tablets and workstations.

Additional materials are available for review and are listed in the "For More Information" section at the end of this paper. These include:

- **HP Brochure for customers with limited IT resources** – Provides you with an overview of HP's client security software and its manageability collaborators.
- **Vendor Data Sheets** - This vendor-specific collateral provides information on the HP security collaborator and its offering. Each company has been validated and provides security manageability solutions to HP ProtectTools.
- **Vendor Whitepapers** - These vendor whitepapers provide extended information on their offerings as they apply to client security manageability solutions for HP ProtectTools.

Client device security

Businesses trying to implement client device security from various sources face a number of choices on solutions that may not always work well together. Security solutions can also be difficult to deploy and use. If a technology is difficult to use, most users will avoid it, which further complicates the task of making client devices more secure. HP's strategy is to build security into the product from the ground up, rather than have you bolt on ad-hoc solutions after the fact.

HP ProtectTools security software suite, Figure 1, addresses these challenges. With an intuitively designed GUI interface, HP ProtectTools Security Manager permits easy setup and control of various HP software modules to provide important client security features. New features can easily be added by installing and utilizing new modules, meeting the ever-changing security needs of businesses and giving you an all-in-one security solution that is easy to use. And, since all security software offered within the HP ProtectTools suite has been extensively tested, you can be sure that each module will function seamlessly and effortlessly. HP ProtectTools security software suite is preinstalled in most business notebooks and desktops and is available as an after market option in select business desktops and workstations.

HP ProtectTools modules that can be installed as needed by the end user or IT administrator include:

- Drive Encryption for HP ProtectTools
- Device Access Manager for HP ProtectTools
- Credential Manager for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools

HP ProtectTools client device security modules feature a number of critical capabilities based on a variety of technologies:

- Trusted Platform Module (TPM), or embedded security chip designed to the Trusted Computing Group (TCG) standard, is available on a range of HP commercial products. This security chip provides the basic hardware capability to be able to help prevent subversion of key security features by software attacks on the platform.
- Personal Secure Drive (PSD) utilizes the TPM to provide an encrypted hard drive partition. PSD can be as large as the entire hard drive (less 5GB for operating systems requirements) and automatically encrypts any data stored on it.
- Notebook computers have been configured with smart card readers or biometric fingerprint sensors. Desktop and Workstation computers can utilize biometric fingerprint readers or smart card keyboards (sold separately).
- Credential Manager serves a dual purpose in that it is a personal password vault that makes accessing protected information more secure and convenient. Users won't need to remember multiple user names or passwords for their various protected websites, applications, and network resources. Additionally, Credential Manager provides the capability to strengthen access control for authenticating identity on a PC. The End User or IT administrator can define and implement combinations of different security technologies to create multi-factor authentication. These factors include smart cards, biometric readers, tokens, passwords, etc.
- Device Access Manager allows selective restriction of information storing and printing, based on user profiles or external storage devices.

- BIOS Configuration allows convenient access to the BIOS security and configuration settings to take advantage of built-in BIOS security features.
- DriveLock can be synchronized with the power-on password and protects the data on the hard drive, even if it is removed by an unauthorized user.
- TPM Enhanced DriveLock (available on notebooks) uses the embedded security chip to generate an extremely strong password that locks the hard drive.

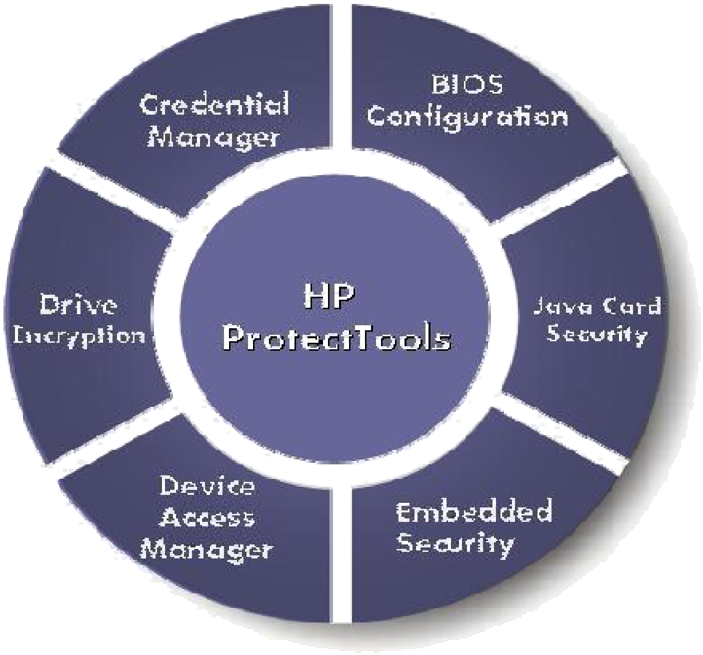


Figure 1- HP ProtectTools Client Security

Security manageability challenges

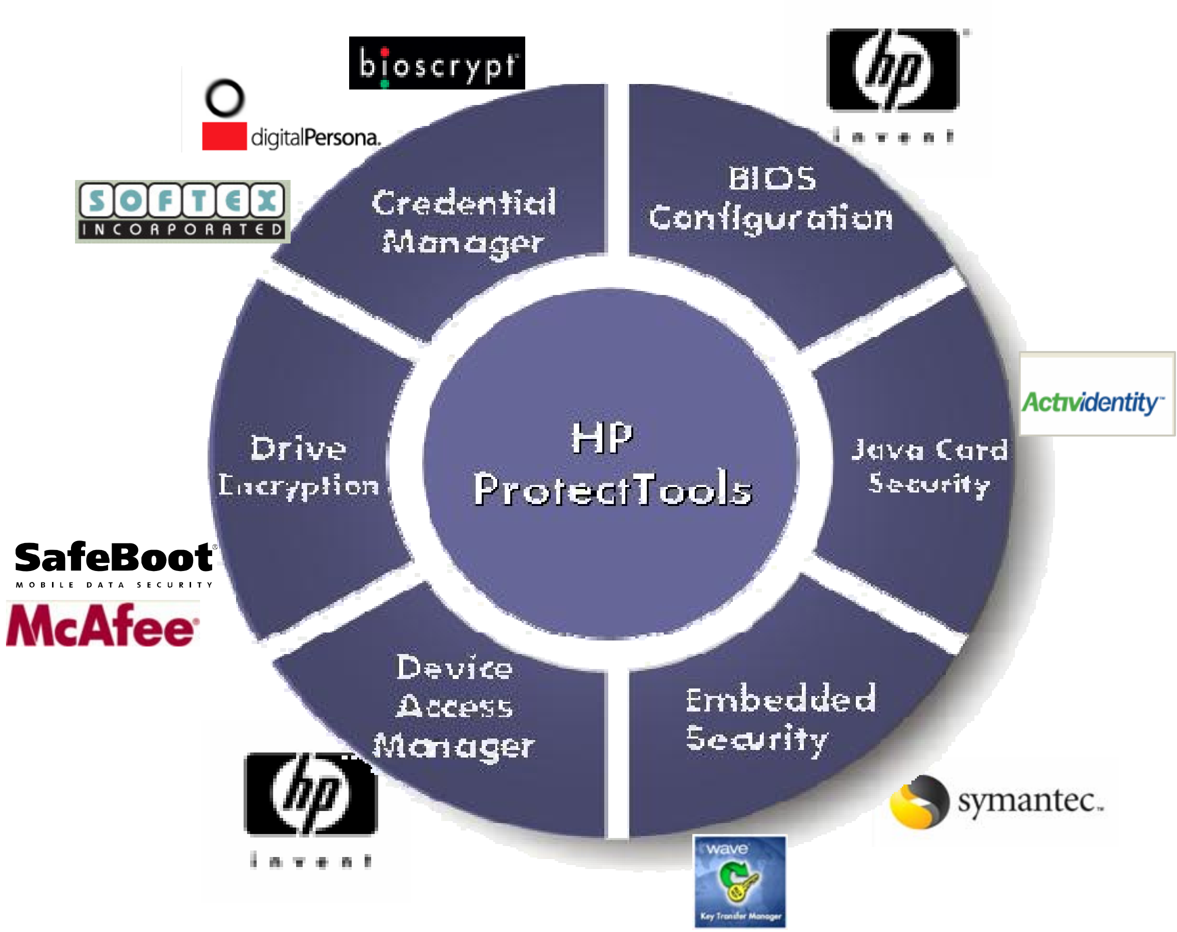
IT systems developers struggle to provide a unified interface for their security infrastructures that includes authentication, data encryption, single sign-on, policy management, administration and auditing. Businesses focused on improving their levels of security are looking to address the manageability of these critical security issues, including:

- Secure and accessible credential information for each user and secure access to all services, regardless of network connectivity or server load
- Management of increasingly disparate applications, each with a proprietary authentication mechanism, directory and usage limits
- Ability to address differing enterprise security requirements across multiple organizations, whether federally mandated or management-directed
- Enterprise-level vs. client-level deployment through an IT administrator for HP platforms

Security manageability for the customer with limited IT resources

You want your IT staff focusing on business-critical projects, not touching every PC when enabling security. As part of an ongoing effort to strengthen PC security and make it remotely manageable, HP in conjunction with key security companies is offering new applications that deliver enterprise-class IT security solutions, Figure 2, that extend HP ProtectTools features, adding manageability, remote configuration and serviceability. HP's security vendors have independently tested their remote manageability software on both HP and non-HP platforms which can provide you with consistent protection if you have a mixed-vendor computing environment.

Figure 2- Enterprise IT Manageability for HP ProtectTools



Full Volume Data Encryption

McAfee Endpoint Encryption, formerly SafeBoot Drive Encryption, offers a data security solution that protects data, devices and networks against the risks associated with loss, theft, and unauthorized access, any time and anywhere. McAfee is a leading vendor for powerful encryption and strong access control technologies that seamlessly integrate with existing enterprise systems, and has collaborated with HP to develop Drive Encryption for HP ProtectTools. McAfee's centralized management capabilities provide you with operational efficiency and a low total cost of ownership.

McAfee’s offering ensures you can:

- **Centralize your security management**: From a single, centralized console, implement and enforce mandatory, company-wide security policies that control data encryption and user authentication
- **Prove compliance with less effort**: Generate detailed reports to demonstrate compliance with internal and regulatory privacy requirements to auditors, senior management, and other stakeholders; ensure your brand image and reputation are constantly protected
- **Seamlessly integrate with existing infrastructure**: Synchronize this solution with Active Directory, LDAP, PKI, and others; supports all Microsoft ® Windows ® OS (full 32- and 64-bit Vista support), common languages, and various keyboards; next to that, endpoint encryption supports automatic language detection in preboot based on Microsoft Windows language settings

Selectively disable USB devices on HP notebooks, desktops and workstations

In today’s open office environments, anyone can walk up to a PC, insert a USB drive or other removable media, and copy any information from the PC or the company’s network to which it is connected. To protect the data, HP engineers have designed and developed Device Access Manager for HP ProtectTools and its manageable version, **Enterprise Device Manager**. By default, Device Access Manager for HP ProtectTools allows users to access all devices, but if device control is needed, Device Access Manager creates access policies for individual users or classes of users. Enterprise Device Manager is available in Europe through the Consulting & Integration team in the United Kingdom. If you are outside of Europe, please contact your HP representative for more details.

This level of configurability enables new client usage models that, for example, allow an auditor to view sensitive financial information while protecting it from copy or removal from the business by denying access to removable storage devices or printers.

HP ProtectTools Device Manager is the manageable version of Device Access Manager that is intended for domain environments and allows device policies to be created, configured, deployed and managed centrally through Active Directory. It is compatible with most widely used versions of Microsoft Windows software

This software allows IT administrators to permit viewing of sensitive data while preventing those data from being copied or printed to external media.

There are two configurations, simple and advanced.

The simple configuration lets users choose common options with a single selection:

- Limit access to all USB devices to administrators only
- Limit access to removable media to administrators and power users only
- Limit access to optical drives to administrators and backup operators
- Limit access to serial and parallel ports to administrators and power users only

With the more powerful advanced configuration, policies can easily be created by the IT administrator to support complex security requirements and business processes.

Multifactor authentication

Passwords can sometimes be haphazardly guarded by your employees, and your Help-Desk costs could be increasing because employees have forgotten their passwords. To more efficiently and securely access your computer systems, HP offers an automated password vault as a standard feature on HP notebooks and many desktops, and is also offered as an option on select desktop and workstation configurations. Credential Manager for HP ProtectTools provides single sign-on capabilities to store user names and passwords in a protected location for secured websites, applications and network resources within the enterprise realm. Storage of user credentials and automatic submission of user names and passwords when required eliminate the need for username and password memorization which encourages users to create stronger, more complex passwords.

In addition to single sign on, Credential Manager also provides strong multifactor authentication support. Various security methods or factors can be combined to provide multi-factor authentication. These factors include user passwords, biometric fingerprint readers, TPM embedded security chips, smart cards, USB tokens and virtual tokens. IT security policies can define the appropriate authentication method for all users, including password alternatives when logging on to Microsoft Windows. Multiple authentication methods can be used in any combination when assigning access privileges to applications and services.

Additionally, Credential Manager addresses:

- Security problems from compromised passwords caused by limited ability to memorize long passwords
- Call volume to Help Desks concerning forgotten passwords, enabling businesses to reduce costs
- Strong multifactor authentication for more secure application credentials and automated application credential management
- Increased productivity from better access to applications through elimination of password problems
- Improved compliance with government and industry regulations such as HIPAA, Sarbanes-Oxley, Graham-Leach-Bliley Act and other international government regulations and industry requirements

For manageability of Credential Manager for HP ProtectTools, there are several key collaborators that could be utilized. These choices include Bioscrypt, DigitalPersona and Softex, just to name a few. Their manageability offerings work seamlessly with Credential Manager.

Biometrics

To help your IT staff provide centralized management control of single sign-on to all of the PCs in your environment, HP recommends Bioscrypt's award winning [1] Verisoft Single Sign On. Working together, the HP ProtectTools Security Manager and Bioscrypt's VeriSoft Single Sign On create a modular, unified approach to configuring and integrating security policies, authentication methods and enterprise applications.

Key features of the HP/Bioscrypt solution:

- Extension of Credential Manager for customers with managed IT infrastructures
- Identity access control
- Integrated back-end for Fingerprint authentication, Multifactor authentication policies, Enterprise single sign-on

- Manages users via existing LDAP Directory Servers including Microsoft Active Directory and Sun Microsystems iPlanet/SunOne Directory Server
- Scalable deployment solution
- Leverages organizations' investment in Active Directory
- Multi-device support
- Creates access policies using any combination of biometrics, smart cards, tokens, certificates, etc.
- Integrated event logging provides a more secure and non-refutable audit trail
- Supports multi-vendor environments

[1] Bioscrypt VeriSoft v2.0 awarded Best Buy for Biometric Tools by SC Magazine, October 2, 2007

digitalPersona.

DigitalPersona is a leading provider of biometric authentication solutions for enterprise networks. DigitalPersona products improve network security, assist with regulatory compliance and reduce IT support costs within organizations of all sizes.

DigitalPersona Pro offers multiple offerings including:

- DigitalPersona Pro Workstation Software (no hardware): Software may be purchased when using Digital Persona approved third-party hardware.

- DigitalPersona Pro Workstation Package: Fingerprint Authentication for Secure Sign-On; scalable to hundreds of thousands of users. Includes both hardware and software.

- DigitalPersona Pro Server Software: Integrates into Active Directory to provide domain-wide more secure sign-on control and password management for networked DigitalPersona Pro Workstations.

- DigitalPersona Pro SBS Solution: Targeted at the Microsoft Small Business Server 2003 R2 users, DigitalPersona Pro SBS provides a more secure sign-on and password management for businesses with up to 75 users.

SOFTEX INCORPORATED

Softex Incorporated offers OmniPass Enterprise Edition-a strong authentication and identity management solution that is more secure, scalable, easy to deploy, lowering total cost of ownership of passwords.

OmniPass Enterprise Edition allows OmniPass Client and Mobile Edition software users to connect more securely into the enterprise. It is a cost-effective, server-based back end that offers enterprise-wide identity management that is easily deployed and managed by the IT department. Passwords can be completely eliminated from the enterprise and network access, e-mail and VPN access, and data are completely secured.

The software provides organizations a well integrated, strong authentication and identity management system that ties easily into their existing infrastructure.

- Support for Active Directory
- Support for Active Directory Application Mode (ADAM)
- Support Novell Modular Authentication Services (NMAS)
- Standard Microsoft Management Console (MMC) console plug-in

Key Features include:

- Standard MMC for managing user accounts and settings
- Choice of centralized or remote enrollment for user authentication devices (e.g. fingerprint enrollment or smart card enrollment)
- Support for multi-device and multifactor authentication including biometrics, smart card s, TPM support and hardware tokens
- Encrypted file sharing in the enterprise. OmniPass Enterprise Edition allows encryption keys for each user to be stored in the Active Directory, allowing any user in the domain to more securely share encrypted data with other users without any key management or transfer.
- Integrated License Management to simplify the procedure of auditing and tracking
- Enterprise-level event logging. This allows for authentication, encryption and most other user operations to be logged into the Active Directory or the ADAM server. It allows IT staff to produce an audit trail of user operations to help comply with governmental regulations such as HIPAA, Sarbanes-Oxley, and Gramm-Leech-Bliley Act.
- Multi-language support
- Supports Windows 2000, XP and Server 2003

Smart Cards for strengthened security

Utilization of smart cards ensures multi-factor authentication in that it requires the user to have the card and a PIN. Smart cards are as easy and can be as secure as using a bank card. HP offers Java Card Security for HP ProtectTools, which was co-developed with ActivIdentity. They provide manageability of smart cards with HP's Java Card being their standard smart card.

ActivIdentity

ActivIdentity (formerly ActivCard) is the trusted provider of digital identity assurance solutions for the more secure issuance, management and use of single secure digital identities. The company's solutions include large-scale enterprise access card systems, more secure remote access, single sign-on, and multi-channel identification and verification. More than 15 million users and 4,000 customers worldwide rely on solutions from ActivIdentity.

If you are seeking to prevent unauthorized access to information and IT resources, ActivIdentity **Strong Authentication** Solutions enable proof of identity through multifactor authentication with smart cards, USB tokens, one-time password tokens, soft tokens, biometrics, or a combination of these.

With ActivIdentity Strong Authentication solutions, organizations can establish proof of identity before granting users access to IT systems and information across their IT infrastructure.

ActivIdentity solutions provide Strong Authentication for:

- **Remote Access** – Remote access is the most vulnerable entry point to IT resources, since it is open to attacks originating outside the organization's physical perimeter. ActivIdentity solutions enable strong authentication for a wide variety of remote applications. This issue is even more crucial in the case of mobile users with laptops that can be easily lost or stolen.

- **Workstation and Network Access** – Within the perimeter of the organization, strong authentication allows enterprises to ensure that only authorized users access wired or wireless networks. ActivIdentity solutions enable more secure access to leading operating systems and networks including Windows, UNIX®, Novell, Thin Clients, Wireless Networks and Pre-Boot Login.
- **Application Access** – Once users are connected and authenticated to the network, they need to access enterprise applications that often require their own authentication method, typically passwords. ActivIdentity strong authentication solutions provide a range of methods to strengthen user authentication for specific business applications.

Embedded security establishes a trusted computing environment

Trusted computing platforms from HP (business desktops, notebooks and workstations) feature the Trusted Platform Module (TPM) embedded security chip and supporting software that help strengthen your access control with stronger authentication by tying it to your password. The TPM security feature is being validated for many applications and a growing number of third party security solutions on the market today. HP enables trusted computing security solutions that deliver greater value and trouble-free deployment with leading third-party software solutions, to provide the enterprise with end-to-end security today and into the future.

The TPM is a small piece of silicon affixed in a device. It more securely stores digital keys, certificates and passwords and is more difficult to attack virtually or physically[2]. Stated more simply, the TPM embedded security establishes a trusted computing environment by offering capabilities to:

- Authentication to the platform and the infrastructure
- Protect user credentials and other secrets

HP platforms are delivered with the TPM in a hidden and/or disabled [3] state, allowing opt-in decision by the IT organization or end-. Prior to using the TPM, the user or IT organization must "take ownership" of the TPM, establishing owner and user level passwords in the process. In a centrally managed environment, the process must be extended across the entire infrastructure.

Deployment of the TPM includes initialization, inventory, back-up and restore capabilities, and manageability. This allows the IT administrator to monitor TPM inventory, change the TPM owner/user password, back up TPM keys for disaster recovery, and in general, manage the TPM.

[2] Trusted Computing Group white paper, Embedded Systems and Trusted Computing Security, https://www.trustedcomputinggroup.org/groups/tpm/

[3]Some governments require the TPM to be disabled for shipment into their country.

Certified under RSA Secured Partner program

TPM embedded security chip-enabled PCs, based on open Trusted Computing Group architecture, have been certified under the RSA Secured Partner Program. Specifically, Embedded Security for HP ProtectTools has been designed to enhance the RSA SecurID solution, enabling use of RSA software tokens within the RSA SecurID infrastructure. By using the TPM embedded security chip, customers are no longer limited to RSA hardware token - a credit card sized device that generates one-time use passwords - and are instead able to use the software version. The combination of these complementary solutions from HP and RSA Security generates real benefits in terms of reduced deployment complexity and cost for many types of users without compromising overall security of the RSA SecurID solution.

Set up, initialize and maintain embedded security remotely

For multi-vendor PC environments, security infrastructure software may already be installed. Typical software deployed could include HP Software's Client Automation, Symantec, Wave's Embassy Trust Suite or others. Information on each of these systems is detailed below:

Remote initialization and inventorying of TPMs

HP's Business Technology Optimization software, **Client Automation**, and **HP Client Manager** for Symantec 6.1 SP1, provide the ability to set up, initialize and maintain embedded security remotely on HP computers that include the TPM embedded security chip. IT administrators can use these consoles to enable and take control of a client TPM remotely, yet still meet the Trusted Computing Group (TCG) requirement. HP Client Automation – Starter and HP Client Manager for Symantec products are offered free of charge.

HP has access to TPM deployment scripts that can be customized. Requests for these scripts should be made to the HP representative. With the end user present (per TCG specification), the remote system script enables and takes ownership of the client TPM chip. If the end user leaves the business or forgets the password (which is set and known only by that user), an emergency recovery archive and emergency recovery token are created, giving administrators the ability to recover data by a password reset token file. TPM backup keys can be stored locally or on an external device.

HP and Symantec have a longstanding and unique partnership that extends beyond sales and marketing to include joint development and technology sharing. By combining hardware and software management, HP and Symantec have established the industry benchmark for reducing the total cost of owning and managing desktops, notebooks, workstations, handhelds, and servers.

Beyond the security capabilities available through HP Client Manager, Symantec offers a comprehensive set of security solutions that can be implemented on top of **HP Client Manager** or independently. HP Client Manager and Symantec security solutions share the same infrastructure so it is a simple procedure to implement additional security capabilities on an existing solution.

Several Symantec products can provide remote manageability of security. For more information on individual products, please refer to:
http://www.altiris.com/upload/altiris_security_offerings_for_hp_24apr07.doc

Centralized storage of keys

Wave's EMBASSY Trust Suite (ETS) client software family has been thoroughly tested for use on HP business desktop and notebook PCs with the TPM embedded security chip that integrates the core elements of trust into the subsystem.

When used in conjunction with Wave Systems' EMBASSY Trust Suite, Embedded Security for HP ProtectTools software enables more secure and seamless file storage and business transactions. The combined solution from Wave Systems and HP provides stronger PC security that is easy to administer and use by IT staff and end users alike.

Wave Systems' Document Manager also uses the TPM chip to provide more secure storage and management capabilities for file-, folder- and drive-level encryption, enhancing the native functionality of the HP solution. This solution easily integrates file encryption into Microsoft Office applications and Microsoft Windows Explorer and will work on most HP commercial notebooks and desktops.

Wave Technologies Key Transfer Manager (KTM) solution allows centralized storage of keys with centralized archiving and the ability to restore/transfer keys.

Simplified remote access to BIOS settings

The HP Software **Client Automation** simplifies the integration of HP business computers with popular industry system management tools including Microsoft Systems Management Server, IBM Tivoli software and HP Business Technology Optimization software, as well as custom-developed management applications. HP Client Automation and HP Client Manager for Symantec access on clients to request in-depth client inventory, receive health status information and manage system BIOS settings by communicating directly with client computers, all from a central console. Specific to security, HP Client Automation and HP Client Manager for Symantec can set BIOS security options on collections of computers with a single task.

HP Client Automation and HP Client Manager for Symantec also provide a rich set of customizable reporting tools to display the exact information needed to manage client computers. Combined, these capabilities enable greater efficiencies and lower IT costs. Both of these software packages are offered at no charge.

Several Symantec products can provide remote manageability of security. For more information on individual products, please refer to:
http://www.altiris.com/upload/altiris_security_offerings_for_hp_24apr07.doc

Protecting local storage with DriveLock

One way an unauthorized user could bypass strong user authentication is to remove the hard drive from a secured system and insert it into an unsecured system. By using the primary hard drive from a secured system as a secondary hard drive on an unsecured system, virtually all data on an unprotected hard drive becomes accessible.

HP business notebooks and desktops enable a hard drive security feature called DriveLock. When enabled, it locks the hard drive with a password. At power-on, the user is prompted for the DriveLock password. The hard drive is accessible only after the correct DriveLock password is entered.

For ease of use, DriveLock does not require the user to remember another password if it is integrated with a power-on password. Both passwords will be the same, so only a single password is required to unlock the system as well as the hard drive. The DriveLock password is stored inside the hard drive itself and cannot be read; it can only be used for authentication. In practical terms, this means that an unauthorized user does not have any means to read the DriveLock password; the correct password must be entered in order to unlock the hard drive. A hard drive protected with a DriveLock password stays protected even if removed from one system and inserted into another.

DriveLock is enabled in BIOS setup by selecting DriveLock Passwords from the Security menu. Before enabling DriveLock, the user will be prompted to create a master password and a user password.

DriveLock requires physical presence, and therefore **cannot** be activated remotely.

TPM Enhanced DriveLock

Enhanced DriveLock adds an additional level of security to the computer without sacrificing usability for the authorized user. Enhanced DriveLock ties pre-boot authentication and the TPM embedded security chip to DriveLock by automatically using a TPM-generated, 32-character DriveLock user password. This enhanced DriveLock user password is a random number and is not stored anywhere.

At pre-boot, the user must be successfully authenticated by the TPM in order for the 32-character Enhanced DriveLock password to be automatically entered and the boot process to continue.

For an authorized user, the login process is completely transparent. However, unauthorized access is now even more difficult due to the randomly generated DriveLock user password.

Enhanced DriveLock protection can be enabled through BIOS setup in the Security menu. It can also be enabled in the BIOS Configuration for HP ProtectTools module in the Security section.

Activating TPM Enhanced DriveLock requires physical presence so it **cannot** be activated remotely.

For more information

HP

1. HP ProtectTools security software suite web ordering http://h30094.www3.hp.com/product.asp?sku=3461276&pagemode=ca
2. Security Website www.hp.com/products/security
3. Notebook Security http://www.hp.com/sbso/solutions/pc_expertise/professional_innovations/protecttools.html
4. Desktop Security http://www.hp.com/sbso/solutions/pc_expertise/great-desktops/index.html
5. Brochure for customers with limited IT resources: http://h71028.www7.hp.com/ERC/downloads/5983-2058EN.pdf

Drive Encryption for HP ProtectTools

SafeBoot or McAfee

1. General website: http://www.safeboot.com/
2. Fact Sheet: http://www.safeboot.com/products/endpointencryption/

Device Access Manager for HP ProtectTools

HP

HP ProtectTools Device Manager

1. General website: www.hp.com/hps/security/products
2. Fact Sheet: http://h71028.www7.hp.com/ERC/downloads/4AA1-1372EEE.pdf

Multifactor Authentication

Bioscrypt

1. General website http://www.bioscrypt.com
2. White Paper VeriSoft Single Sign On: http://www.bioscrypt.com/products/verisoft_sso

DigitalPersona

1. General website http://www.digitalpersona.com/
2. Fact Sheet: http://www.digitalpersona.com/products/business.php

Softex Incorporated

1. General website http://www.softexinc.com/main.asp

ActivIdentity

1. Website http://www.actividentity.com/solutions/technology/sa__overview.php
2. Technology Brief on ActivIdentity solutions for Device and Credential Management http://www.actividentity.com/solutions/docs/briefs/AI_device_credential_management_L.pdf

Client Manager and TPM

HP

1. General Security Website: www.hp.com/products/security
2. White Paper: HP Client Manager 6.1 www.altiris.com/Products/HPClientManager.aspx

Symantec

1. General website: www.altiris.com
2. Website on HP/Symantec collaboration http://www.hp-altiris.com/
3. White Paper: HP/Symantec security offerings http://www.altiris.com/upload/altiris_security_offerings_for_hp_24apr07.doc

Wave

1. General website: www.wave.com
2. White Paper Embassy Trust Suite: http://www.wave.com/products/ets.html
3. White Paper Key Transfer Manager: http://www.wave.com/products/ktm.html

4AA1-8478ENW, March 2008