



Check Point Endpoint Security Full Disk Encryption

Detailed product overview for Windows and Linux

Contents

How secure is my data?	3
How effective is startup-screen password protection?	4
What is the best way to protect data at rest?	5
Encryption schemes	5
File/folder encryption	5
Full-disk encryption	6
How does Check Point Full Disk Encryption protect my data?	7
What happens during installation?	7
Are there any changes to the PC startup procedure?	7
Does Check Point Full Disk Encryption affect normal PC operations?	8
Can Check Point Full Disk Encryption protect data transfers to external devices? ...	8
How do I deploy and manage Check Point Full Disk Encryption?	8
Establishing security parameters	9
Choose an encryption algorithm	9
Select an authentication method	9
Administrator access	10
Deploying the software	10
Image check	11
Tool setup	11
Pilot deployment	11
Full deployment.....	11
Managing and administering security policies	11
Long-term support and maintenance	12
Establishing a help desk	12
Resetting locked user accounts and passwords	12
Allowing temporary access to PCs.....	12
Change management	13
Imaging and forensics tools.....	13
Data recovery.....	13
Hard disk maintenance and problem prevention	14
Data backup	14
Reviewing Check Point Full Disk Encryption system logs	14
Is Check Point Full Disk Encryption right for my application?	15
Is my data important? Is it sensitive? Is it completely secure?	15

How secure is my data?

How important is your company's data? Unless you can answer, "not at all," you need to ask the next question: Exactly how secure is my data?

In times past, securing sensitive company data was a simple matter of locking doors, hiring guards, and issuing employee IDs. In today's high-tech world, sensitive data travels outside of company walls with alarming frequency—most often on mobile devices such as notebook personal computers (PCs). And as more company data travels, the greater the risk of loss or theft that can result in damaging legal and financial repercussions.

All notebook PCs can be password protected by means of their operating system (OS) login screens, but such protection can be easily defeated. The most effective way to truly protect data at rest on a PC hard disk drive is to encrypt it—that is, to scramble the data so that it cannot be deciphered and read by an unauthorized user. Of the two major types of data security—*file/folder encryption* and *full-disk encryption*—only full-disk encryption eliminates the possibility of human error and ensures that all the data on a disk is protected.

Check Point Endpoint Security Full Disk Encryption™, based on market-leading Pointsec® technology, is designed to provide comprehensive security for data at rest, especially on notebook PCs. It is designed to be easy to set up, deploy, administer, manage, and support and will easily scale to meet the needs of any size enterprise or government agency. Check Point Full Disk Encryption (FDE) is also fully compliant with current privacy and security legislation to satisfy regulatory requirements.

This document will familiarize you with Check Point FDE and specifically answer four major questions:

- How effective is startup-screen password protection?
- What is the best way to protect data at rest?
- How does Check Point FDE protect my data?
- How do I deploy and manage Check Point FDE?

These questions, taken together, will help you to answer a larger question: Is Check Point FDE right for my application?

How effective is startup-screen password protection?

Any PC operating system, such as Microsoft Windows, Mac OS X, or Linux, can be configured for password protection at startup, but such protection is easily defeated. To understand its basic vulnerability, consider the system startup sequence for a PC running Microsoft Windows OS (see Figure 1).

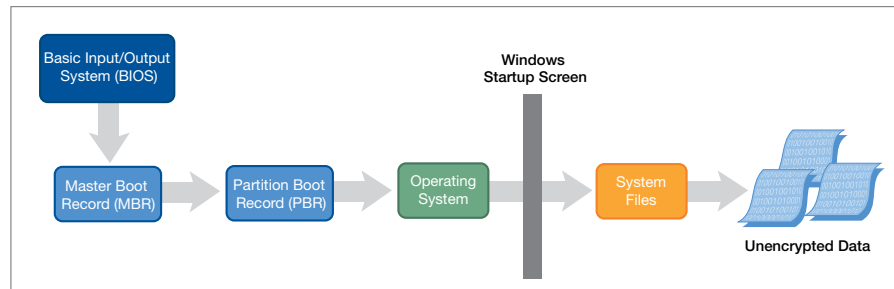


Figure 1: Microsoft Windows startup sequence

The startup sequence consists of five steps:

1. The *basic input/output system* (BIOS) loads the *master boot record* (MBR)
2. The master boot record loads the active *partition boot record* (PBR)
3. The active PBR loads and starts the operating system (OS), which displays the blue Windows startup screen and accesses the system files, including the password files
4. The user *authenticates* by selecting a user name (for multiple-user installations) and/or entering a password at the startup screen
5. Windows validates the user and continues the startup process, displaying the desktop and starting any applications

Although the Windows authentication process can prevent unauthorized people from using the computer, it does **not** protect the data from access. Hackers can easily bypass the Windows authentication process, for example, by booting the PC from a Windows PE or Linux Live CD. Also they could physically remove the hard disk and mount it as a *slave* (or secondary) drive on a different computer. In summary, Windows authentication attempts to prevent unauthorized use of the system but stops short of protecting the information stored on the system.

Some PC BIOS programs allow the creation of a *BIOS password*, however, the level of security provided is similar to that of Windows authentication, and is just as easily defeated. BIOS passwords may prevent unauthorized users from accessing the OS and, in some cases, may even prevent the hard drive from starting by using a *BIOS hard drive password*, but even this defense can be defeated by determined hackers.

What is the best way to protect data at rest?

Because startup password protection is so easily defeated, it is necessary to provide a higher level of security for data at rest on a PC hard disk. The best way is to encrypt the data—that is, to scramble the data on the disk such that it can only be unscrambled and read by an authorized user. Encryption renders data unreadable to unauthorized users—even when disks are slaved to hacker computers or computer security is otherwise compromised. Only authorized users can access the key that enables *decryption* of the data.

Many data encryption products exist in the marketplace, but not all products use the same approach or are equally effective.

Encryption schemes

PC data encryption products typically use either of two schemes:

- File/folder encryption—encrypts only data located in specified files, folders, and/or disk partitions
- Full-disk encryption—encrypts the **entire hard disk** including the OS, system files, and all data

File/folder encryption schemes are inexpensive and plentiful and can provide a useful means of protecting data under certain circumstances. However, full-disk encryption schemes are far more secure, easier to manage, and fully compliant with current privacy and data security laws and regulations.

File/folder encryption

File/folder encryption schemes selectively encrypt data in specified files, folders, and/or disk partitions. As a result, they protect only certain sections of the disk (see Figure 2). The unencrypted sections of the disk remain vulnerable to access by unauthorized users.

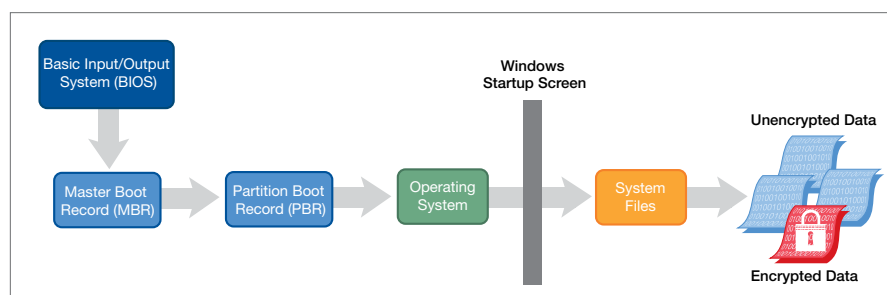


Figure 2: File/folder encryption scheme

When installing and setting up a file/folder encryption scheme, users typically specify which file types, folders, and/or disk partitions to encrypt. When the encryption program is running, any data created or saved as a specified file type, or moved to a specified folder or partition, is automatically encrypted. However, because such programs encrypt data selectively, they suffer from two major drawbacks: the user-dependent nature of the file/folder scheme and their inability to guarantee protection of critical files—such as OS and password files.

User dependence

Unfortunately, file/folder encryption schemes rely on users to ensure that sensitive data is protected. Consequently, these solutions are **user-dependent** and inherently subject to human error. Such errors can involve failing to store data in a secure file type, neglecting to move sensitive data to an encrypted folder, accidentally copying the data to an unencrypted folder, or incidentally generating an unencrypted residual copy of the data (for example, a temporary file) in the normal course of using the PC. A few file/folder encryption solutions attempt to enforce security policy through automatic identification of the type of data being stored. However, these solutions are easily bypassed by careless users and determined hackers.

In addition, relying on end users to secure data is inherently **unenforceable**. Therefore, its use constitutes a weak defense against lawsuits filed in response to the loss or theft of confidential information. As a result, file/folder encryption schemes do not comply with current privacy and security legislation, and they leave businesses that use them vulnerable to costly legal battles and excessive damage control operations in the event of data loss or theft. File/folder encryption schemes **cannot guarantee** that sensitive user data has been encrypted.

Lack of guaranteed protection for critical files

To ensure data security, it is also necessary to protect certain files that may provide access to the data—especially the OS and system files, as well as any files containing application user passwords. If such files are not explicitly included in the list of files to be encrypted when setting up a file/folder encryption scheme, they are vulnerable to compromise by unauthorized users—often resulting in devastating outcomes. For example, an unauthorized user who is able to obtain the local password for a VPN client could gain access to the associated VPN network, possibly disrupting company-wide operations.

Full-disk encryption

Unlike file/folder schemes, full-disk encryption protects an **entire PC hard disk**—including the OS and system files. Once a disk is fully encrypted, a dedicated driver encrypts and decrypts data on the fly, completely transparent to authorized PC users. Because the encryption/decryption operations are automatic and continuous, full-disk encryption schemes are inherently user independent and completely **enforceable**, making them fully compliant with current computer privacy and security legislation. Full-disk encryption also eliminates the problem of unencrypted residual data because **all data is encrypted**—even temporary files. This removes the administrative burden of being forced to determine which files and folders require protection, and renders a slave hard disk completely unreadable to an unauthorized user.

Check Point FDE provides complete protection for data at rest on a PC disk. Sensitive data is fully protected no matter where it resides on a hard disk, and the security system is fully enforceable, enabling compliance with current privacy and data security legislation.

How does Check Point FDE protect my data?

In order to protect your data, Check Point FDE changes the way in which your data is accessed and processed.

What happens during installation?

It is easy to install Check Point FDE on new laptops and PCs as well as those already in use. Deploying Check Point FDE on existing PCs can be accomplished by pushing it out with software distribution systems, initiated by different types of scripts, or started by an end user working on a PC as a silent (noninteractive) installation. Check Point FDE can also be incorporated into a *standard operating environment* and used with different types of hard-drive imaging products to simplify deployment on new PCs. When first installed, Check Point FDE installs an encryption/decryption driver that acts as a filter between the operating system and the hard disk to ensure that all data stored on or retrieved from the disk is encrypted or decrypted on the fly. During the last part of installation, Check Point FDE automatically starts the hard-disk encryption process. This process encrypts data at about 20 to 30 GB/hour and is completely fault tolerant—that is, immune to power loss or computer shutdown. If the computer loses power or shuts down during its initial encryption, Check Point FDE simply resumes encryption when the computer is next turned on. The initial encryption process works entirely in the background so that users can run other applications and continue to use their computers.

Are there any changes to the PC startup procedure?

Check Point FDE adds a layer of authentication to the startup process by installing its own access control module between the MBR and the active PBR (see Figure 3).

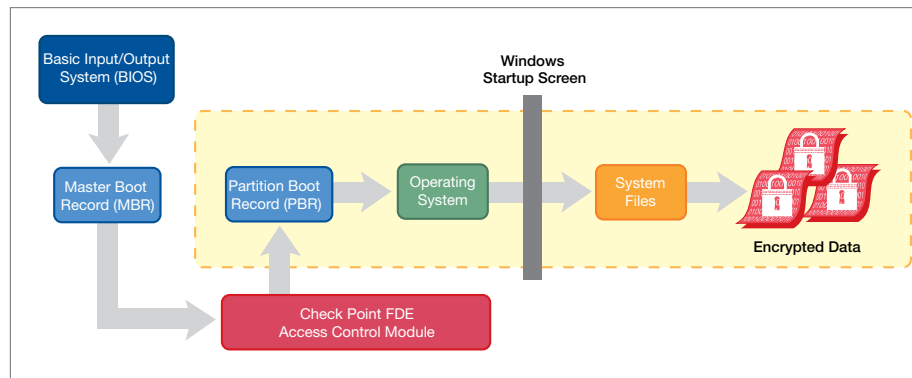


Figure 3: Preboot environment with Check Point FDE installed

After the MBR loads, Check Point FDE requests user authentication by displaying its access control screen. The normal startup sequence of booting the OS and displaying the Windows startup screen will proceed **only** after users have satisfied all Check Point FDE authentication requirements. Utilizing the *Windows integrated login (WIL)* feature presents users with a single login screen if this better suits the organization's needs.

Does Check Point FDE affect normal PC operations?

Each time users start their computers and successfully authenticate at the access control screen, Check Point FDE automatically installs its encryption/decryption driver between the OS and the disk driver (see Figure 4).

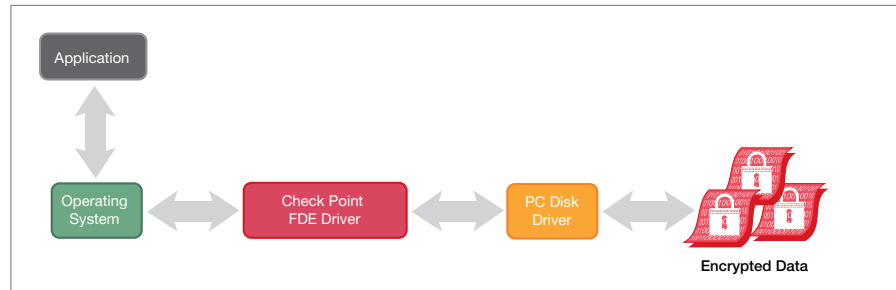


Figure 4: Check Point FDE driver location

Thereafter, the encryption/decryption driver runs in the background, automatically encrypting and decrypting data as it is stored on and retrieved from the disk. Check Point FDE remains **transparent** to all other computer applications, including system operations such as disk defragmentation.

Can Check Point FDE protect data transfers to external devices?

Data transfers external to the protected PC, such as backing up data on an external hard drive, are performed by applications that operate at the system level. As noted above, the Check Point FDE driver encrypts data transferred between the OS and the PC disk driver. Consequently, data transferred to an external drive or other removable medium, such as a USB memory stick, is not encrypted during transfer. Therefore, it is possible for an authenticated user to create and store unencrypted copies of data on an external device.

If leakage of unencrypted data concerns your enterprise, Check Point also offers a solution for this potential problem. Check Point Endpoint Security Media Encryption prevents unauthorized copying of sensitive information from laptop and desktop PCs through a flexible combination of port control, content filtering, and removable media encryption.

How do I deploy and manage Check Point FDE?

Check Point FDE is easy to deploy for any company, large or small.

Doing so involves four basic operations:

- Establishing security parameters
- Deploying the software
- Managing and administering security policies
- Ensuring long-term support and maintenance

Establishing security parameters

Prior to deploying Check Point FDE, administrators may configure their own security policies by choosing among options—such as the type of encryption algorithm and authentication methods to be used. Check Point FDE makes it easy to modify security policy at any time, but most customers do not change their policies more than once per year.

Choose an encryption algorithm

Check Point FDE can be configured to use any of four encryption algorithms: AES, Blowfish, CAST, or 3DES. The choice of algorithm is typically influenced by overall effectiveness and prevailing government policy. In recent years, many national governments have established specific rules regarding types of encryption algorithms legally allowed for use within their borders—and rules can vary from country to country.

Select an authentication method

User authentication is local to the device (PC), so the user can authenticate even when the PC is not connected to a network. Check Point FDE can be configured to use any of three authentication methods: *password*, *certificate-based SmartCard*, and/or *dynamic token*. Any of these methods can be deployed at the same time for different users. Regardless of the authentication methods used, Check Point FDE is designed to allow administrator access to protected data at all times.

Password authentication

Password authentication is the most commonly used method. To gain access to a computer and its data, users simply enter a username and password, which Check Point FDE then checks against the login information stored in its secure system area. Password rules can be set and enforced by system administrators.

Certificate-based SmartCards

A SmartCard is one type of token. SmartCard tokens provide an added level of security, relative to password-only protection, because they require something the users possess (tokens) in addition to something they know (passwords to unlock the certificate). This is often referred to as strong or *two-factor authentication*. The user must authenticate to Check Point using the certificate information stored on the SmartCard.

Dynamic tokens

Dynamic (or one-time password) tokens are similar to certificate tokens in that they require authentication based on something the users possess, as well as something they know. Administrators can choose dynamic tokens requiring either *synchronous* or *asynchronous* one-time passwords.

Synchronous one-time passwords are most commonly used for remote access, for example, when a remote access server (also known as a VPN gateway) sends an authentication request to a one-time password server. The server authenticates users and then replies to the remote access server. Because the use of synchronous one-time passwords requires a connection to a remote password server, it cannot be used with offline applications.

Asynchronous (or challenge-response) one-time passwords do not require a one-time password server to authenticate users. This makes them suitable for use with PCs that utilize offline data security applications, such as access to laptops protected with full-disk encryption. Check Point FDE supports the X9.9 standard for asynchronous one-time passwords.

Administrator access

Regardless of authentication method, Check Point FDE allows administrators—as well as other privileged users—to access any protected PC at any time using unique personal credentials. Consequently, it is unnecessary for administrators to maintain a list of passwords for all the users in a system—or even to know user passwords. By not requiring administrators to know user passwords, Check Point FDE simplifies system administration while providing an added level of security because there are no central password files that can be stolen in the event of a security breach. In addition, by giving administrators access to every protected PC, it is easy to recover PC data when authorized users leave the organization.

Deploying the software

Check Point FDE is easy to deploy regardless of company size or number of PCs (seats) to be protected. Deployment is typically accomplished in four phases (see Figure 5):

- Image check
- Tool setup
- Pilot deployment
- Full deployment

A major milestone in the deployment process lies between Steps 3 and 4, when an evaluation of the pilot deployment is required to determine whether the system is ready for full deployment.

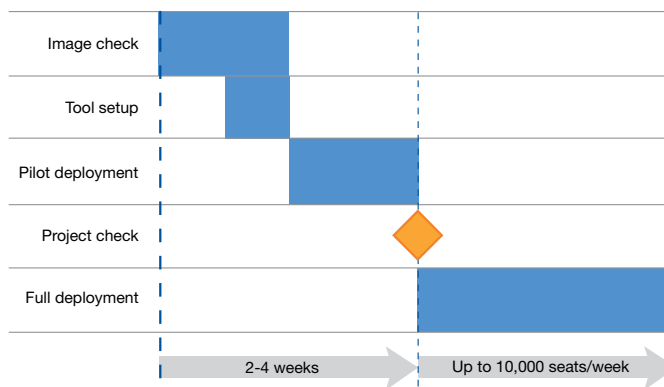


Figure 5: Check Point FDE deployment phases

The first three deployment phases can be completed in as little as two to four weeks. The length of the fourth phase depends on the number of PCs to be protected and can often be completed at a rate of up to 10,000 seats per week.

Image check

In the image check phase, Check Point-trained personnel evaluate the client systems to ensure that no compatibility issues will arise during deployment of Check Point FDE. In a typical installation, the images are small and well defined, and this phase is completed quickly.

Tool setup

The tool setup phase involves installation of the tools necessary to administer Check Point FDE—for example, tools that deliver security policies to end users. In addition, Check Point personnel set up the company-specific help system and train the help-desk personnel to handle common requests, such as resetting passwords.

Pilot deployment

In the pilot deployment phase, Check Point FDE is deployed for a trial run on a sample of company notebook PCs. A typical pilot phase will involve 100 to 500 PCs. Executive-level users are often engaged for the pilot phase because their PCs are most likely to contain sensitive information, and executive satisfaction with the product facilitates acceptance by the rest of the company during full deployment.

At the end of the pilot phase, Check Point personnel meet with the customer to evaluate the pilot program and determine if the customer is ready for full product deployment.

Full deployment

The full deployment phase involves complete deployment of Check Point FDE across the company. As noted above, Check Point FDE is easy to deploy regardless of the number of seats involved and can be installed at a rate of up to 10,000 seats per week.

Managing and administering security policies

Check Point FDE allows the administrator to establish and manage security policies through either the *enterprise workplace* (EW) or *management infrastructure* (MI) modes. Both modes allow the administrator to quickly and easily modify security policies but vary how policy changes are communicated to individual users.

EW mode stores security policy information in a file-based security profile that resides on the company network. To change a security policy, administrators simply change any associated security-profile files. When users are connected to the network, their local Check Point FDE agents periodically check network-security policy files to see if any changes have been made and then retrieve and institute any changes affecting users. Consequently, administrators can manage security policy by broadcasting changes from a single set of centrally located files, rather than making changes on individual PCs. If preferable, administrators can still push changes remotely to individual PCs.

The MI solution mode is similar to the EW mode in function. However, security policies are maintained in a database rather than from a set of centrally located files. As a result, the MI solution mode can be managed over the Internet by means of a connection-point Web server.

In addition, the MI solution mode can leverage Microsoft Active Directory information (e.g., users, computers, and organizational units) to simplify deployment of multiple policy settings across groups of users.

Long-term support and maintenance

To be effective as a means of protecting data, any encryption program must be easy to administer and manage. With Check Point FDE, a single administrator can easily manage thousands of PCs. The major issues involved in such operations include establishing a help desk for tasks such as remote password resets, imaging and forensics, data recovery, and making the data on a hard disk temporarily accessible to external technicians.

Establishing a help desk

Check Point FDE provides simple, yet powerful tools for maintaining a help desk to support its implementation. The help desk is operated by means of a Web-based tool and is scalable to support thousands of users. In addition, Check Point FDE includes an integrated application program interface (API) that serves as a self-help tool. The API can even be configured to use voice recognition as a means of user authentication.

One of the most common tasks for help-desk personnel is to provide access to computers if authorized users forget their passwords. To handle this situation, Check Point FDE allows users to gain access to their computers by means of a verbal challenge-and-response sequence that can be communicated over the phone between users and help-desk technicians. In this way, users can access their systems and reset their passwords even if their PCs are not connected to the company network or the Internet.

Resetting locked user accounts and passwords

Check Point FDE provides a simple yet secure process to unlock user accounts and reset passwords without revealing administrator passwords to users or user passwords to administrators. When users forget their passwords or fail to authenticate after a predetermined number of attempts, their accounts will be locked. The account lock can be configured in one of three ways: temporary lockout, automatic unlock after a preconfigured number of minutes, or remain locked until the user receives assistance from an administrator or help-desk staff member. Check Point is not involved in unlocking accounts or resetting passwords. The unlocking process is simple and secure for end users, and help-desk staff members are not required to have network connections. The entire process can be completed in less than five minutes.

Allowing temporary access to PCs

Different types of users may need temporary access to end user PCs. For example, service engineers may need to install new applications or OS patches, or consultants may need to use PCs for a limited time. Check Point FDE includes the following temporary access features.

One-time logon

One-time logon allows an end user, service engineer, or any other person to boot the PC only once. The user selects “one-time logon” in the Check Point FDE preboot environment and then must follow the same challenge-and-response procedure described above for password changes to gain one-time access.

After the PC is turned off, the procedure must be repeated if access is needed again. This procedure can also be used when SmartCards or challenge-response tokens are required for preboot authentication.

Service user account

Temporary service user accounts can be created, for example, by service engineers who need to reboot PCs multiple times in order to install multiple applications or OS patches. If user accounts are created with the account type set to “service,” the accounts will automatically be locked and require a remote password change session to be activated. Service accounts allow service engineers to boot PCs as many times as needed and remain valid until other authorized users lock the service accounts.

Change management

Check Point FDE software updates can be performed without end user interaction, and all configuration changes are transparent to end users.

Configuration changes after installation

Configuration changes can be implemented using either the local administration program installed on end user PCs or by using the central administration tools over a network connection. This includes the addition and removal of user, administrator, and help-desk accounts.

Software updates

Software updates can be installed remotely by administrators and require restart on local PCs.

Imaging and forensics tools

Imaging and forensics tools may be used by authorized personnel. If unauthorized users attempt to create full-disk images of disks encrypted by Check Point FDE, the images will be encrypted and therefore useless to hackers. Check Point FDE also supports the Microsoft OSD imaging process based on WinPE or WinRE.

Data recovery

When the Windows OS crashes or the hard drive fails, it may be necessary to recover data from the hard drive. Common data recovery scenarios are described below:

Hard drive is readable but Windows does not boot

Because Check Point FDE does not modify the MBR, users are still able to authenticate—then Check Point FDE software can redirect to a bootable floppy or, for example, to a WinPE CD. The floppy or CD can then be used to mount the Windows file system and extract files from the unbootable hard drive. This allows data recovery in minutes, instead of the many hours required to complete a full-disk decryption.

Windows needs to be reinstalled

Windows can be reinstalled at any time with Check Point FDE software. Because the hard disk MBR is not modified, there is no need to perform more steps in a Windows reinstallation process.

For example, in a dual-partition system with the OS installed on the *C: drive* and the data on the *D: drive*, the OS can be reloaded and re-encrypted while keeping the *D: drive* partition intact and accessible.

Hard drive is not readable at all

If a hard drive is not readable at all, there may be a serious logical or physical failure. The first step in working with such a disk is to try to create a full drive clone using some type of sector-by-sector backup tool. If there is a physical failure, the hard drive must first be repaired by a forensics expert. Once the encrypted information is available on a hard disk allowing access without physical problems, Check Point FDE can be removed using a Check Point FDE recovery floppy. A Check Point FDE recovery floppy is generic and can be created using any PC on which Check Point FDE has been installed, or alternately sent as an image from any help desk. To remove Check Point FDE software, two Check Point administrators (with privileges to remove Check Point FDE) are needed to unlock the Check Point FDE recovery file that would have been created during the installation process. This forces a separation of duties, ensuring that no single user account can be used to remove Check Point FDE.

Hard disk maintenance and problem prevention

Check Point FDE runs beneath the OS and, therefore, will not interfere with the OS, applications, antivirus software, or maintenance applications. To prevent or repair minor hard disk problems, users can perform a standard check disk or disk defragmentation with no problems.

Data backup

As stated above, Check Point FDE does not interfere with applications running on the OS. If data needs to be transferred from a problem PC to a new PC, this can be accomplished utilizing standard CDs, DVDs, USB drives, network connections, etc.

Reviewing Check Point FDE system logs

All security systems must maintain an audit trail. The Check Point FDE system log is an encrypted and tamperproof audit trail. The system log tracks all types of events, including failed authentication attempts and information about users and administrators from remote help sessions. The log file is automatically transferred to the Check Point FDE central recovery directory, allowing Check Point system administrators to view and export log files from all network-attached PCs protected by Check Point FDE. System administrators can select event types to view and, when viewing log files using the central log tool, can select which PC log files to read from. The Check Point FDE log file is written by default in clear (unencrypted) text to the EventViewer—enabling harvesting and aggregation with popular third-party log tools (this feature can also be disabled).

Is Check Point FDE right for my application?

Check Point FDE uses a full-disk encryption scheme to provide comprehensive protection for data at rest, especially on notebook PCs. As this document shows, Check Point FDE is easy to set up, deploy, administer, manage, and support. Check Point FDE is easily scalable for any size organization and is fully compliant with all current privacy and security legislation.

Is my data important? Is it sensitive?

Is it completely secure?

If the answer to this last question is anything other than a confident “yes,” it’s time to contact your Check Point representative.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is the leader in securing the Internet. Check Point offers total security solutions featuring a unified gateway, single endpoint agent, and single management architecture, customized to fit customers' dynamic business needs. We are unique in this offering as a result of our leadership and innovation in the enterprise firewall, personal firewall/endpoint, data security, and VPN markets. The pure focus of Check Point is on information security. Through its NGX platform, Check Point delivers a unified security architecture to protect business communications and resources, including corporate networks and applications, remote employees, branch offices, and partner extranets. The company also offers market-leading endpoint and data security solutions with Check Point Endpoint Security products, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point award-winning ZoneAlarm solutions protect millions of consumer PCs from hackers, spyware, and identity theft. Check Point solutions are sold, integrated, and serviced by a network of Check Point partners around the world, and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.