CHECK POINT ENDPOINT SECURITY FULL DISK ENCRYPTION

ENDPOINT SECURITY FULL DISK ENCRYPTION

Benefits

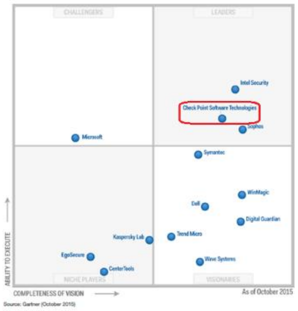
- Transparent security for all information on endpoint hard drives.
- Strong data recovery and emergency access procedures.
- Central management offers great ROI and optimal protection.
- Flexible deployment, simple to operate and monitor.

Features

- Protects data from unauthorized access if computers are lost, stolen or left in other vulnerable states.
- Multi-user preboot environment supports advanced security; Network Authorized Preboot Bypass, OPAL Self-Encrypting Drives, smart cards, TPM, touch interfaces, custom graphics.
- Manage online and offline endpoints.

Recognition

- A leader in Gartner's Mobile Data Protection Magic Quadrant for over 14 consecutive years.



Source: Gartner (October 2015)

OVERVIEW

Users store sensitive company data on their devices and carry it with them wherever they go. Outsiders can easily obtain this valuable information through lost or stolen laptops which can result in legal and financial repercussions.

SOLUTION

Check Point Full Disk Encryption (FDE) provides transparent security for all information on all endpoint drives, including user data, operating system files and temporary and erased files. For maximum data protection, multi-factor pre-boot authentication ensures a user's identity before the operating system loads, while encryption prevents data loss from theft.

FULLY INTEGRATED SOLUTION FOR ENDPOINTS

To complement the Full Disk Encryption solution, we offer additional data security components, as part of our Endpoint Security suite:

- **Media Encryption & Port Protection** - Secures removable media devices and enables restricting or blocking physical ports.
- **Capsule Docs** - Protects documents wherever they go and prevents unintentional data leaks.
- **Remote Access VPN** - Provides secure access to corporate resources when traveling or working remotely.

Media Encryption & Port Protection

Capsule Docs (Document Security)

Remote Access VPN

Check Point provides the most comprehensive solution for securing endpoint devices, leveraging our data protection offering together with advanced threat prevention and access control solutions.

Uncompromised Security

We use the strongest encryption algorithms standards, including XTS-AES and AES-CBC. Our CryptoCore encryption engine was officially certified to be compliant with the strict FIPS (Federal Information Processing Standards) 140-2 guidelines. TPM (Trusted Platform Module) and Network Authorized Preboot Bypass (Unlock On LAN) are also supported.

Secure Preboot Environment, Seamless End User Experience

Preboot authentication ensures that only authorized users are allowed to access the endpoint. The preboot environment loads prior to the operating system and securely authenticates the user and verifies their identity. We provide an excellent user experience with Single Sign On for preboot/operating system login and support multi-factor authentication, such as smart cards and dynamic tokens for enhanced security. Lockout settings can be configured to prevent brute-force attacks, for example to lock the user account after a set number of failed login attempts have been reached.

Excellent Remote Help and Recovery Capabilities

We provide a cryptographically safe challenge response remote help mechanism, allowing secure key exchange for locked users. Remote password changes and one-time logon options are available for users who may have forgotten their passwords or lost their access tokens. Administrators can have one-time access to the computer. We also offer a Self Help Remote Help Portal which lowers the TCO of the product, by reducing number of supporting IT operations staff. For recovery scenarios we ensure that data stays accessible and secure using the Drive Slaving Utility or recovery decryption.

Portable Security

Our solution offers a consistent user experience with a familiar look and feel and supports multiple languages, within the operating system and in the pre-boot environment, across both Windows and macOS. We are compatible with most hardware configurations and support any Windows or Mac machine, including ATM and POS devices. We have a very close cooperation with the major PC vendors, which allows us to verify and officially certify that our solution runs successfully on top of their latest hardware and BIOS/UEFI versions.

Unified Central Management

The Full Disk Encryption solution is centrally managed using our Endpoint Security Management server, enabling central policy administration, enforcement and logging from a single, user-friendly console. Endpoint Security Software Blades from Check Point bring unprecedented flexibility, control and efficiency to the management and deployment of endpoint security. Choose from a variety of Software Blades to deploy only the protection you need, with the freedom to increase security at any time from a single central management console.

Flexible Deployment Options

Our solution supports various types of environments with different connectivity behaviors. The Offline Mode (similar to the legacy EW Mode) is suitable for environments where clients have regular connectivity to the server and are being managed by it. The Offline Mode is suitable for environments where there is minimal or no connectivity, including embedded systems such as ATMs, where the client gets configuration data from specific network shares or local folders instead of communicating with the Endpoint Security Management server. This mode allows organizations to use their own infrastructure to gather recovery data and logs.

For more information, visit www.checkpoint.com/products-solutions/endpoint-security.

CONTACT US

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 | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com