Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Media Encryption & Port Protection

Comprehensive data protection and control for endpoint removable media

Check Point Media Encryption & Port Protection

YOUR CHALLENGE

Allowing users to use portable media devices such as USB memory sticks, CDs, DVDs, and other devices poses a possible security risk for organizations. Not allowing users to use devices impedes productivity, access to information and resources. However, ensuring that breaches of security and compliance violations do not occur requires monitoring individuals' computers and media devices usage on a wide scale. More and more users are mixing personal files such as music, pictures, and documents with business files such as finance or human resource files on portable media. Evolving risk make it difficult to take the time to educate users on the actions which they may take. Even when a solution is found, having centralized, granular control of media devices poses additional management issues.

PRODUCT DESCRIPTION

The Check Point Media Encryption and Port Protection Software Blade provides centrally enforceable encryption of removable storage media such as USB flash drives, backup hard drives, CDs and DVDs, for maximum data protection. Educating users on when to share and not share corporate data via UserCheck prevents future data sharing mistakes. Port control enables management of all endpoint ports, plus centralized logging of port activity for auditing and compliance.

OUR SOLUTION

To stop incidences of corporate data ending up in the wrong hands via USB storage devices, CDs, DVDs, and other storage media outlets, Check Point Media Encryption encrypts and prevents unauthorized access of storage outlets. With fine grain controls such as limiting read, write, and execute capability of ports on endpoint systems and devices, and separating business and personal data, corporate data remains safe from vulnerabilities. Encryption of device data is done in the background for a transparent end-user experience. Further enhancing a user's experience, users can access encrypted media securely on unmanaged computers with no client installation from both Windows and Mac.

PRODUCT FEATURES

- Encryption using AES 256 bit for maximum protection of data.
- Control access of removable media, devices, and ports down to a granular level. Central management enables central policy administration, enforcement, and logging from a single, user-friendly console.
- Logging and alerts of storage device activity and file movement.
- Keep access to personal data and business data separate.

PRODUCT BENEFITS

- Comprehensive control of endpoint ports and protection of corporate data stored on removable media and devices.
- Transparent end-user experience with automatic data encryption and seamless integration.
- Simplified administration and operation with single agent installation, and centralized policy and management enforcement.
- Actively engages and educates users on Media Encryption policies for business security policy compliance.
- Integration with Check Point Software Blade Architecture for a single-console, centrally-managed endpoint solution.

softwareblades™

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Simple User Experience

- Data read from and written to an encrypted media is done transparently and automatically, without any user interruption.
- Simple access to encrypted media also for external parties and for devices not having the client, based on password access.
- Separate and protect business data from personal data on storage devices.

Granular access rights

- Set granular access policies for users and groups—no access, read only, read write, access to any removable media or only to encrypted media.
- Set granular access policies for encrypted media—starting with access only to device owner, to device owner's group, to other groups or to the entire users in the company.
- Granular control of data—define personal and business applications, and enable separation between encrypted business and non-encrypted personal data.

Protect device port from malicious activity and data loss

- Control what ports are accessible to the user, such as FireWire, Bluetooth, InfraRed, printers, and more. Scan removable storage device for malware before allowing access to the device.

Engage and Educate Users with Integrated Check Point UserCheck™

- Use Check Point UserCheck™ to actively engage and educate users as they access portable media to identify potential policy incidents as they occur and remediate them immediately.

Rigourous Security Certifications

- Check Point's Media Encryption blade has been awarded the rigorous security certifications—including Common Criteria EAL4, FIPS-140-2 and CCTM CESG—thereby enabling compliance with global data privacy rules and regulations.

Central Management

- Integrated endpoint and network security capabilities including centralized logging of data movement and media usage for streamlined compliance and forensic analysis.

Integrated into Check Point Software Blade Architecture

- The Media Encryption and Port Protection Software Blade is integrated into the Software Blade Architecture. Endpoint Security Software Blades from Check Point bring unprecedented flexibility, control and efficiency to the management and deployment of endpoint security.
- Additional Endpoint Security Software Blades: Desktop Firewall and Compliance Check, Antimalware and Program Control, WebCheck Browser Virtualization, Full Disk Encryption, and Remote Access VPN.

SPECIFICATIONS

Client Platform Support

- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64 bit and SP1
- Windows XP Pro (32-bit, SP3 and later)
- Microsoft Vista 32/64 bit
- Mac 10.6/10.7/10.8 – read/write access to encrypted media based on password

CD/DVD Burning Application Integration

- Windows CD/DVD native burning application
- Nero 9 Multimedia Software

Client Language Support

- English
- Japanese
- French
- Italian
- German
- Chinese (simplified)
- Spanish
- Russian

Security Evaluation Certifications

- Common Criteria EAL4
- FIPS 140-2
- CCTM CESG

Ports Controlled

USB, WiFi, Fire Wire, IDE, Bluetooth, PS/2, PCMCIA, SATA, IrDA and SCSI

Devices Controlled

USB flash drives, floppy drives, external hard drives, tape drives, Windows Mobile Smartphones, PDAs, imaging devices, scanners, iPhones, BlackBerrys, tablets, modems, other network access devices, iPods, other digital music devices, printers, CD/DVD drives, keyboard, mouse, digital cameras, wireless network interface cards, biometric devices and smart card readers

Management Platform

See Endpoint Policy Management Software Blade

CONTACT CHECK POINT

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 | www.checkpoint.com

September 18, 2012