CHECK POINT ENDPOINT SECURITY MEDIA ENCRYPTION & PORT PROTECTION

ENDPOINT SECURITY MEDIA ENCRYPTION & PORT PROTECTION

Benefits

- Comprehensive control of endpoint ports and protection of corporate data stored on removable media devices.
- Transparent end-user experience with automatic data encryption and seamless integration. Actively engages and educates users on Media Encryption policies.
- Central management offers great ROI and optimal protection.

Features

- Protects data from unauthorized access if devices are lost or stolen.
- Blocks specific ports based on policy.

Recognition

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

OVERVIEW

Removable media devices, such as thumb drives, provide a convenient mechanism for sharing files across devices. Yet, copying business data to such devices may pose a security risk, as these devices may get into the wrong hands. Our computers have many ports, such as USB and Bluetooth, allowing us to connect various devices. Sometimes we need to allow connecting only specific devices.

SOLUTION

Check Point Media Encryption and Port Protection (MEPP) provides centrally enforceable encryption of removable media devices such as flash drives, external drives and CDs/DVDs, for maximum data protection. UserCheck messages prevent future data sharing mistakes and educate users on when to share and not share corporate data. Port control enables management of all endpoint ports, plus centralized logging of port activity for auditing and compliance.

FULLY INTEGRATED ENDPOINT SOLUTION

To complement the Media Encryption and Port Protection solution, we offer additional data security components, as part of our Endpoint Security suite:

- **Full Disk Encryption** - provides transparent security for all information on all endpoint drives, including user data, operating system files and temporary and erased files.
- **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.

Full Disk Encryption

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

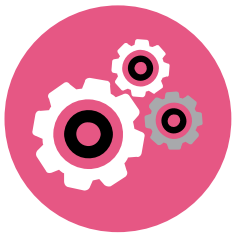
Our CryptoCore encryption engine was officially certified to be compliant with the strict FIPS (Federal Information Processing Standards) 140-2 guidelines. We use the strongest encryption algorithm standards, including AES 256, for maximum protection. Security administrators can define the users and groups who have access to encrypted devices and their access permissions; no access, read-only or read-write. Devices can be scanned before allowing access, using the Check Point Anti-Malware Software Blade as well as 3rd party vendors. Devices can also be locked after a number of failed password attempts.

Excellent End User Experience

Data on removable media is automatically encrypted providing a seamless end user experience. Business and personal data are isolated on separate partitions. When users access portable media Check Point UserCheck™ actively engages and educates users to identify potential policy incidents as they occur and to remediate them immediately. Encrypted devices are also available using a password without the need for an agent. Our remote help technology recovers lost user passwords using a challenge-response exchange. We can require reauthorization to access encrypted devices when unauthorized changes have been made.

Enhanced Monitoring Capabilities

Complete audit logs of user, device and file activity is available, satisfying regulatory compliance and facilitating forensics investigations. Security administrators can identify the types of devices used in the organization and who is using the devices. With this information administrators can fine-tune their media encryption and port protection policy accordingly. If a device has been compromised, then access to specific users and devices can be removed to lock down the compromised device.



Highly Customoziable Policy

Control access to devices and ports down to a very granular level. You can create and endpoint security policy that is based on port type (USB, Bluetooth, etc.), device type, brand, size or ID. Define the file types allowed on a device, business or personal, and our solution enforces your policy. The policy is communicated to users with our unique UserCheck message, educating them when the policy is applied.

Unified Central Management

Our Media Encryption and Port Protection solution is centrally managed using our Endpoint Security Management server. 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. Central management enables unified policy administration, enforcement, and logging from a single user-friendly console.

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

