



## Endpoint Security

*Check Point Endpoint Security is total endpoint protection for enterprises.*

# Check Point Endpoint Security Media Encryption

*Prevents data leakage and encrypts removable media*

## YOUR CHALLENGE

The staggering number of USB and other plug-and-play-enabled ports on laptops and PCs has driven the potential for serious data leakage occurring within your enterprise. These ports allow users to extract any data in an instant by connecting common storage devices like USB flash drives, iPods, or Bluetooth devices to company computers—effectively making all enterprise computers vulnerable to this data leakage threat. Most users only intend to download music or digital photos onto their work PCs from their personal storage devices. However, the capability to copy huge amounts of sensitive enterprise data from corporate PCs onto these personal devices places your organization at considerable risk of undetected data leaks.

Couple all that with the shrinking size of plug-and-play storage and a booming market for personal electronics like music players and digital cameras, and an entirely new category of threats to your most sensitive information has emerged. Not only are your chances of data loss increasing, you probably have no way to detect or track these devices on your network—even if you have fully educated users about your formal security policy.

## OUR SOLUTION

Check Point Endpoint Security Media Encryption™ addresses the internal threat from unauthorized copying of enterprise data to personal storage devices through a powerful combination of port management, content filtering, centralized auditing and management of storage devices, and optional media encryption. Check Point Endpoint Security Media Encryption plugs these potential leak points and provides a comprehensive audit-reporting capability of how data files move on and off these devices, giving enterprises complete control of their security policies.

## PRODUCT DESCRIPTION

Check Point Endpoint Security Media Encryption™ offers complete port and storage device management, preventing unauthorized copying of sensitive information from enterprise desktops and laptops through port control, content filtering, and optional media encryption.

## PRODUCT FEATURES

- Content control function
- Role-based policy enforcement
- Three-dimensional auditing
- Optional removable media encryption
- FIPS-certified AES 128/256-bit algorithm for optional transparent media encryption
- Fully MSI-enabled installer

## PRODUCT BENEFITS

- Deploys quickly, which meets compliance objectives and conserves resources
- Controls input and output on all connection ports
- Centrally manages devices individually by type, brand, or model
- Scales to meet the needs of any size enterprise or government agency
- Provides complete audit of device usage
- Operates 100 percent transparently with Windows 2000/2003 Active Directory and Novell eDirectory
- Maintains high productivity because the application runs transparently to users



Check Point Endpoint Security Media Encryption is centrally managed, so the solution can be deployed easily across all endpoints, and policy settings can be updated, as business needs change. This fine level of granularity over policy settings keeps enterprises in control, allowing them to optimize security while minimizing the effect on user work patterns and IT operational costs.

**COMPLETE FLEXIBILITY**

Check Point Endpoint Security Media Encryption offers total flexibility to enable the management of USB plug-and-play devices. By operating 100 percent transparently with Active Directory or eDirectory, roaming user security policies are associated with existing users and groups to enable role-based access throughout the organization.

**UNIQUE WHITELIST AND BLACKLIST FUNCTIONALITY**

Check Point Endpoint Security Media Encryption has an exclusive design that offers both whitelist and blacklist management of USB removable media. This capability enables organizations to enforce the use of authorized

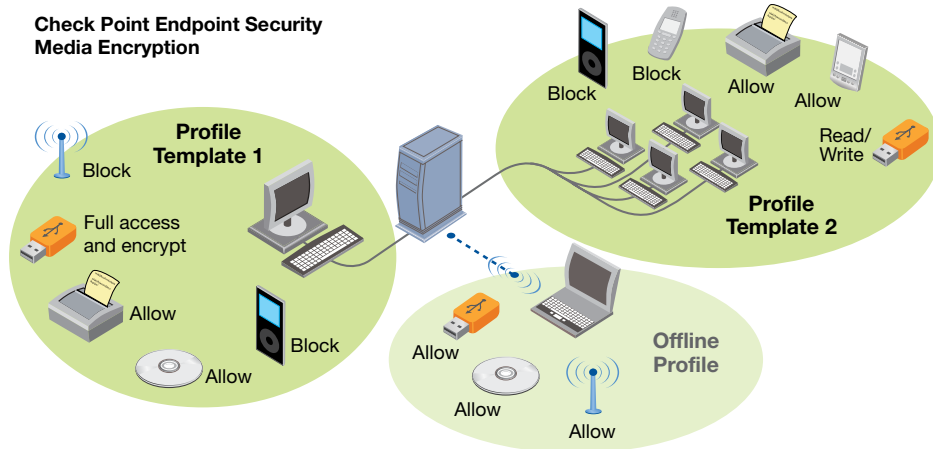
media across the enterprise, while offering the flexibility of enabling unapproved devices to be used without introducing unwanted or malicious files and reducing the risk of data loss.

**TRANSPARENT REMOVABLE MEDIA ENCRYPTION**

Check Point Endpoint Security Media Encryption is the market leader in device security that offers transparent access to encrypted removable media, while also offering the ability to control which employees can share data internally. Check Point Endpoint Security Media Encryption enables full read/write encryption capability off the network without the need to install any third-party software, while enforcing a content and virus scan when data is returned to ensure network integrity is maintained at all times.

**COMPREHENSIVE AUDIT CAPABILITIES**

Check Point Endpoint Security Media Encryption provides extensive audit capability that extends beyond the boundaries of workstation control. Unique to the market, this three-dimensional audit trail enables network administrators to track data movement to and from removable media, wherever devices are used.



SYSTEM REQUIREMENTS	
Windows	
Windows 2000 (SP4)	
Windows 2003	
Windows XP (SP1+)	
Windows Explorer (5.5+)	
Novell Client v4.91+	

**CONTACT CHECK POINT**

**Worldwide Headquarters**

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-575-9256 | 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

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, 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, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, 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.