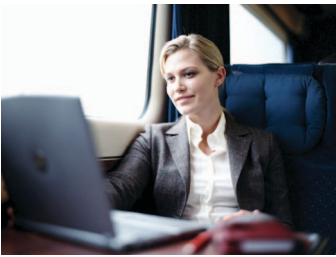


McAfee Removable Media Security

Strong data security that supports mobility and productivity

An increasingly mobile workforce requires ready access to the company information they need to stay productive, regardless of where or how they work. Portability of both access and data is critical to day-to-day operations, but this convenience brings increased risk to your company's most sensitive information assets, such as intellectual property and regulated data. How do you balance the need for anywhere, anytime access with the need to protect your organization against intentional or accidental exposure of sensitive data?



"We evaluate a security solution's success by how much it saves us from spending on crisis management if we lose sensitive data. With McAfee, we're investing in risk-cost avoidance for the long haul."

Randy Yates
Director of Information Security
Memorial Hermann Medical Center

At McAfee, we relentlessly tackle the complex security challenges faced by organizations that want users to benefit from the flexibility offered by removable media devices. We provide unique solutions built on our proven encryption, user-friendly authentication, content analysis, and behavior control capabilities. Our solutions provide the most comprehensive approach available to protect sensitive data on removable media—without interfering with users' need to get work done.

A Virtual Tether

Although employees may leave the physical office at 5:00 p.m., today's fast paced business environment requires them to have anytime, anywhere access to corporate data and business applications. The physical tether to the desk is easily controlled, but the evolution of business has also made that tether virtual—one that is more difficult to control because it needs to be able to work over public networks and from foreign access points. One of the most popular mobile productivity devices today is high-capacity, removable USB media storage. Users often have multiple USB devices, and multiple access points that enable them to use the information on these devices. This means there are many different possible points where a trusted, secure environment is required. It also means that measures must be taken to ensure that these devices and access points do not become leaky sieves for sensitive corporate data.

Regulated and Sensitive Information Requires Persistent Protection

There are many different types of sensitive information. Constantly evolving privacy regulations in the U.S., the European Union, and other countries or regions govern usage policies over structured customer information and certain financial data. Industry-specific regulations, such as Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and European Union Data Retention Directive affect how certain types of information related to financial transactions, citizen health, and communications must be handled to ensure compliance. All of these regulations require enforcement to be persistent and provable, regardless of whether the information stays within corporate walls or travels freely with users. Knowledge workers in research-driven industries such as pharmaceuticals, biotechnology, high technology, chemicals, energy, and others, are constantly generating and manipulating high-value intellectual property that, if unwittingly exposed, could put revenue and operations at significant risk. This information is the lifeblood of an organization and requires persistent protection regardless of how users—from executives to authorized insiders—access it. However, with the expanding technologies and

Solution Advantages

- Help enforce regulatory compliance mandates persistently
- Protect all types of data, including high-value intellectual property
- Control user behavior with removable media devices intelligently and transparently
- Enable everyday user behavior while protecting users against potentially risky behaviors
- Enforce portable encryption on many types of removable media
- Get support for many different software and hardware authentication methods, including enforcement of multiple factors
- Create fully portable, managed, secure business application environments capable of running on any access point

options available for portable, removable storage, the challenge of securing this environment properly to meet regulatory and business requirements has become increasingly complex. This is exactly the type of problem that the security experts at McAfee are committed to help customers solve.

Comprehensive Solutions for Removable Media Security

McAfee offers comprehensive solutions for enabling productive use of removable media storage devices without compromising security. The McAfee solutions include:

- Intelligent and transparent location, action, and content-driven monitoring and control over how removable media devices are used
- Multiple industry-standard, flexible options for strong encryption and authentication—both software- and hardware-based
- Support for creating completely portable, secure, and managed business application environments on convenient USB devices

McAfee Removable Media Security Products

McAfee Device Control

McAfee® Device Control protects critical data from coming into and leaving the company through removable media such as USB drives, iPods, Bluetooth devices, recordable CDs and DVDs. It provides tools to monitor and control data transfers from desktops and laptops—regardless of where users and confidential data go, even when they are not connected to the corporate network. With granular control, companies can specify which devices can and cannot be used, define what data can and cannot be copied onto allowed devices, and restrict users from copying data from specific locations and from certain applications.

McAfee Endpoint Encryption for Removable Media

McAfee Endpoint Encryption for Removable Media protects information saved on common, off-the-shelf removable storage devices with strong encryption. The solution is device- and vendor-independent and allows the encrypted device to be used on any machine without installing any software or requiring administrator privileges. The solution permits editing and saving of encrypted files which maintains the portability, flexibility, and ease of use that business professionals demand from these devices. The same device can be enabled with encrypted space for business use and unprotected space for personal use. It also fully integrates with McAfee Device Control to provide enforcement of user, group, or company policies that define which information must be in protected, encrypted space on removable devices.

McAfee Encrypted USB Devices

McAfee Encrypted USB devices are high-performance removable storage devices with built-in hardware-based encryption and authentication available in a wide variety of flash and hard drive capacities. These devices expand on the capabilities offered by McAfee Endpoint Encryption for Removable Media to offer specialized authentication methods, such as integrated support for one-time passwords, biometrics, and HSPD-12-compliant CAC and PIV smart cards. These devices also provide the ability to create customized, managed, portable, and secure business application environments that run directly from the device. This way, persistent security is maintained for all data and interactions, regardless of the user access point. These devices also provide the option for a complete virus and malware threat detection and removal environment powered by proven McAfee anti-virus technology.

Product Capabilities

McAfee Device Control

- Built on powerful, proven McAfee Host Data Loss Prevention (DLP) product technology
- Regulates how users copy data to USB storage devices, iPods, recordable CDs and DVDs, Bluetooth and IrDA devices, imaging devices, COM and LPT ports, and more
- Protects all data, formats, and derivatives even when data is modified, copied, pasted, compressed, or encrypted
- Includes a flexible classification engine with expression and term assistants to enable you to easily identify data for protection by physical location, application type, creator, or content
- Integrates with McAfee Endpoint Encryption for Removable Media to force encryption onto supported devices by policy to protect identified types of sensitive information
- Enables you to quickly and easily configure, deploy, and update policies and agents throughout your environment from McAfee ePolicy Orchestrator® (McAfee ePO™) software for seamless, centralized management integrated with other McAfee endpoint security solutions
- Sets device and data policies and registers collections of documents for control by user, group, or department
- Specifies which devices can and cannot be used by any device parameter, including product ID, vendor ID, serial numbers, device class, device name, and more
- Supports auditing and compliance needs with detailed user- and device-level logging
- Gathers incident details, such as device, time stamp, data evidence, and more for prompt and proper response, investigation, and audit

McAfee Endpoint Encryption for Removable Media

- Enables creation of encrypted, protected space on removable USB storage devices; the amount of encrypted versus user space is determined by policy
- Hardware independent, so any USB device capable of operating system mountable and accessible storage can be encrypted using industry-standard, FIPS-validated, and AES 256-bit encryption
- Truly portable, so no special software is required to access encrypted space, even when you use the device on another machine that does not have McAfee software
- Integrates with McAfee Device Control to enforce encryption policies for devices based on specific workgroups, content types, locations, or applications. If policies require encryption on a device to use specific data, Endpoint Encryption for Removable Media will add and manage that encryption.
- Data remains in encrypted space on the removable device; sensitive information does not remain on a user's desktop or laptop after it is used
- Provides multiple options for recovery of encrypted data, including PKI certificates and challenge questions, whether user-driven or administrator-driven
- Centrally managed and administered by McAfee ePO software for seamless integration with other McAfee endpoint security solutions (available mid-2010)

McAfee Encrypted USB Devices

- High-performance storage devices with built-in hardware-based, industry-standard, FIPS-validated, and with AES 256-bit encryption in a wide range of flash and hard disk capacities
- Supports multiple authentication methods and factors including passwords, biometrics, PKI certificates, HSPD-12-compliant CAC and PIV smart cards, and one-time password authenticators
- Credentials and keys are securely stored on the USB device in protected space and never leave the device. There is also an option to store additional certificates and other credentials such as soft one-time password tokens on the device
- Multiple options for data recovery if a user is not able to provide their original credentials
- Zero footprint and complete independence from the operating system environment with no special software installation—all you need is a free USB port

- You manage the installation of important business applications directly onto the secure devices, creating a reusable, portable, completely secure working environment for users that they can run anywhere they go
- Optional integrated McAfee anti-virus and malware threat detection and prevention environment on the devices
- Centrally managed authentication and usage policies via McAfee ePO software for seamless integration with other McAfee endpoint security solutions (not currently available on all models)
- All devices are compact and portable, made of tamper-evident, dustproof, and waterproof enclosures with easy-to-read status indicators and no requirement for external power sources

Seamless Integration Increases Your Security Posture While Reducing Costs

Centralized management and proof of compliance with McAfee ePO software

Most components of the McAfee removable media security solutions are centrally deployed and managed by the award-winning McAfee ePO software environment. Deploying and managing removable storage devices across an enterprise can be extremely complex and expensive for an organization. Centralized management with the McAfee ePO platform enables corporations to overcome these challenges and manage how removable media devices are used on enterprise-wide scale—all from a single console, improving security posture while reducing ongoing administrative costs. McAfee ePO's integrated monitoring, reporting, and auditing capabilities enable you to quickly prove compliance with external regulations and internal governance policies, further driving down costs by simplifying the ongoing audit process.

Interoperability ensures end-to-end security

Our removable media security solutions provide seamless interoperability with the other components of the McAfee Total Protection for Data security suite—end-to-end physical and behavioral controls to protect all of your data at the endpoint regardless of how it is accessed, stored, used, or transported. McAfee Total Protection for Endpoint expands on these capabilities to tackle evolving Internet threats with industry-leading anti-spyware, anti-malware, anti-phishing, host intrusion prevention, anti-spam, and firewall capabilities. It also includes a powerful adaptive anti-virus engine that uses McAfee Artemis technology to leverage the intelligence of millions of McAfee user endpoints worldwide for accelerated time to protection. McAfee network data loss prevention solutions and email and web security appliances extend protection for data into the network with complete monitoring and control over electronic communications regardless of protocol or location.

For more information about our removable media security solutions, please visit www.mcafee.com, or call us at 888.847.8766, 24 hours a day, seven days a week.

