McAfee®

Protect what you value.

Proving Compliance with McAfee Total Protection for Data

Proving Compliance with McAfee Total Protection for Data

Since the first wave of regulatory requirements swept across corporations in 2002, companies have spent millions of dollars putting in place processes and technologies to protect the privacy and security of information–and ensure regulatory compliance. According to AMR Research, compliance with Sarbanes-Oxley (SOX), one of the best-known and widest-reaching regulations, will cost companies more than $32.2 billion through 2008. And SOX is just one piece of the regulatory puzzle: AMR estimates that SOX spending accounts for just 20 percent of the total amount companies spend on governance, risk management, and compliance programs.

One of the most common technologies used by companies to protect their information is encryption. By encrypting the data stored on corporate systems–from desktops to laptops to mobile devices–companies feel a sense of security that if the protected systems are stolen or misplaced. Their intellectual property and sensitive customer information will remain safe and secure from unauthorized access.

But simply encrypting this information doesn't help you prove compliance with external regulations or internal controls during a financial audit or legal discovery process. In these cases, you must be able to present irrefutable proof of who, what, where, when, and how your information was protected–or face financial penalties, legal liabilities, brand damage, customer distrust, and more.

So how can you prove that your data was encrypted if it is accidentally lost or misplaced or maliciously stolen? Through comprehensive reporting and auditing capabilities provided by data protection solutions from McAfee®. With endpoint encryption and data loss prevention (DLP) integrated into our award-winning security management system, you gain complete oversight and control over your data security and the ability to provide proof of compliance with government and internal policies–all at your fingertips.

Encryption + Oversight = Secure Data

McAfee Total Protection (ToPS) for Data enables you to not only enforce your internal and external compliance policies but also prove the extent of that enforcement, making audit, legal discovery, and other regulatory processes pain-free and simple. Comprised of ***McAfee Endpoint Encryption***, McAfee Encrypted USB, McAfee Host Data Loss Prevention, and McAfee Device Control–all centrally managed by McAfee ePolicy Orchestrator® (ePO™)–the McAfee ToPS for Data suite brings together network and system threat protection, physical and behavioral controls for sensitive data, and compliance management in a single, integrated solution. So you can prove compliance, not just enforce it.

Encrypt and Protect

Using McAfee encryption solutions, you can encrypt and protect the information stored on all your corporate systems and removable devices. Offering two forms of encryption to protect data from unauthorized access when stored or in transit, ***McAfee Endpoint Encryption*** provides robust, certified, standards-based physical protection for data on every system in your organization. Full-disk encryption helps ensure that information remains secure when stored at-rest on desktops, laptops, tablets, and mobile devices. And using McAfee's patented Persistent Encryption Technology™, you can encrypt specific files and folders and ensure they remain encrypted regardless of where they are saved.

While the movement of easily transportable laptops and other mobile devices–and the data they contain–can be difficult to control, nothing is harder than monitoring pocket-sized USB drives. Offering tremendous storage flexibility and power, these so-called 'thumb' or 'flash' drives are less than three inches long and fit comfortably in someone's pocket or enclosed fist, easily escaping detection. With ***McAfee Encrypted USB***, you can prevent data on these tiny drives from being viewed by unauthorized individuals, either accidentally or maliciously. McAfee's powerful encryption technology and strong access controls ensures that information copied and stored on USB storage devices is protected and can only be read by those authorized to do so.

Monitor and Control

Did you know that more than half the respondents to a McAfee-sponsored survey said they take confidential data out of the workplace on portable systems and storage devices at least once a week? Another 22 percent said they lend their system or mobile device, containing work documents, to colleagues on a regular basis. Each instance is an opportunity for sensitive and confidential data to be lost or stolen–and you must find a way to protect your company from these data loss risks.

McAfee Host Data Loss Prevention (Host DLP) lets you protect data from internal and external data loss threats with comprehensive monitoring, auditing, and control over user behavior across all endpoints. Host-based protection secures data regardless of where users or information go, or whether or not client machines are connected to the corporate network. A key component of McAfee ToPS for Data, McAfee Host DLP lets you monitor and control your critical information–even when the data has been modified from its original form.

To further control how users copy data onto removable media, such as USB drives, MP3 players, CDs, and DVDs, ***McAfee Device Control*** lets you monitor and restrict what data can be copied onto these devices. Using McAfee ePolicy Orchestrator® to deploy the software onto your managed endpoints, you then define the policies that control which content can and cannot be copied onto which removable storage devices. Then, McAfee Device Control automatically enforces these policies, monitors usage, and blocks any unauthorized attempts to use these devices or transfer data in violation of defined policies. And McAfee Device Control even recognizes your data as yours when it has been modified, copied, pasted, compressed, or encrypted–keeping data within your control and giving you peace of mind that it is safe from unauthorized access.

Manage and Audit

Even the most elaborate and wide-ranging security strategy is useless without a comprehensive security management console that lets you implement, enforce, manage, and audit your organization's security policy and all of its components from a single, centralized location. This is where ***McAfee ePolicy Orchestrator*** (ePO) comes in.

McAfee ePO is the most popular and respected security management technology on the market today, deployed at more than 30,000 companies with nearly 54 million desktops and servers under management. An essential component of McAfee ToPS for Data, and the critical piece of the puzzle that enables you to prove–not just enforce–compliance with internal and external policies, McAfee ePO provides central management of all security applications, delivering comprehensive protection and a complete audit trail for all devices and data, including when, where, and how they were encrypted. With McAfee's unique comprehensive and integrated security risk management approach, you can make the most efficient and effective threat protection and compliance management decisions.

Prove Compliance with McAfee Total Protection for Data

Enforcement without proof is useless. All the effort you have spent in addressing regulatory requirements for data privacy could be wasted if you are unable to prove–quickly and resolutely–that your data was properly protected.

With McAfee, you can prove it. Through the integration of McAfee ToPS for Data–including McAfee Endpoint Encryption, McAfee Encrypted USB, McAfee Host DLP, and McAfee Device Control–with the industry-leading McAfee ePO security management system, you can quickly and easily produce a detailed, accurate audit trail and prove compliance with internal policies and external regulations to auditors.

What's more, McAfee can help you prove the integrity as well as the protection of your data in electronic discovery, or eDiscovery, proceedings. Thanks to the integration of McAfee ToPS for Data with McAfee ePO, you can quickly and effectively respond to requests for electronic evidence as a result of legal or regulatory action. With McAfee, you are assured of the complete integrity of the discoverable data and can present a full audit trail to prove the protection to requesting parties.

Product Capability Matrix

ePolicy Orchestrator			
• Centralized management • Comprehensive reporting and auditing • Irrefutable proof of protection			
Endpoint Encryption	**Encrypted USB**	**Host DLP**	**Device Control**
• Powerful full-disk, file, and folder encryption • Strong access control • Synchronized password changes	• Standard, secure USB flash storage • Driverless zero footprint technology • Two-factor authentication • Secure token services	• Control over internal data transfer • Comprehensive device management • Multilayered protection	• Comprehensive device and data management • Granular controls

For more information on McAfee Total Protection (ToPS) for Data or McAfee ePolicy Orchestrator (ePO), visit:

www.mcafee.com or call us at 888.847.8766 - 24 hours a day, seven days a week.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888.847.8766
www.mcafee.com