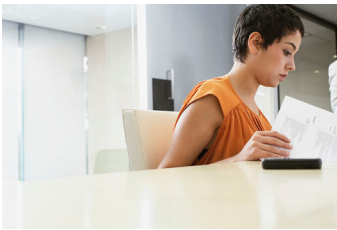


Regulated Data Protection

Maintaining productivity under stringent regulatory scrutiny



The *Unsecured Economies* survey revealed that 800 companies lost a combined \$4.6 billion worth of intellectual property in 2008 alone and spent approximately \$600 million repairing damage from data breaches. Based on these numbers, McAfee projects that companies worldwide lost more than \$1 trillion in 2008.

Unsecured Economies/Protecting Vital Information*

Highlights of Massachusetts Data Privacy Law

Defines "personal information" as a combination of a resident's first and last name connected to one of the following: a driver's license number, a credit card number, or a Social Security number

- Requires measures that restrict access to personal information and files on a need-to-know basis
- Requires unique identifications plus private passwords to each individual with computer access
- Requires encryption of all personal information records and files transmitted across all public networks
- Requires current firewall protection and operating system security patches
- Requires up-to-date system security agent software (including malware protection) and security patches

Regulations on data privacy are getting increasingly prescriptive, creating a staggering, potentially business-breaking burden on both IT and security staff and end users. Businesses of all sizes must ensure that all their users remain productive while achieving escalating expectations of compliance. McAfee has the only end-to-end integrated controls that protect regulated data while allowing users to perform their jobs. Our complete solutions save you time, money, and stress by optimizing critical controls and centralizing processes, including encryption, management, monitoring, auditing, and reporting.

Regulations regarding sensitive data, both within the United States and globally, continue to evolve. Initially, most regulations were open to interpretation and provided minimal penalties. Recent events mark a change in the regulatory climate.

The Massachusetts Data Privacy Law (201CMR 17.00), passed early in 2009, is among the most prescriptive to date. It mandates security programs with stringent controls for any business, individual, or organization handling personal information. Unlike many data regulations, it defines clear actions, such as extensive encryption wherever customer data is transmitted or stored and use of up-to-date system security and firewalls.

Older laws are also receiving new emphasis. For example, HIPAA investigations are on the rise, with stiff penalties and even jail time for violators, including a recent \$2.25 million dollar fine against the CVS/pharmacy.¹ Happily, there are incentives for compliance as well as penalties for noncompliance. The American Economic Reinvestment and Recovery Act requires the implementation of HIPAA privacy guidelines as a condition to receiving funding to upgrade healthcare IT systems.

As regulations become more detailed and more heavily enforced, companies start to experience more confusion and pay higher costs, since regulations are starting to conflict. "Safe Harbor" laws helped initially with privacy law conflicts between the U.S. and the European Union,² but both regions are raising the ante. New U.S. e-discovery requirements are in direct conflict with new E.U. rules blocking release of private information.³ The patchwork and overlap of laws like these make it even more important to have an infrastructure that can adapt to constant change.

McAfee Can Help

McAfee understands what it takes to protect regulated data, your reputation, and competitive edge while ensuring regulatory compliance. Whether your sensitive information consists of customer and employee data, intellectual property, or legal and financial records, McAfee can help. We can help you locate your sensitive data, assess your risk, and implement effective policies where they will do the most good: on endpoints and mobile devices and throughout your network.

* <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>

1. www.hhs.gov/news/press/2009pres/02/20090218a.html

2. www.export.gov/safeharbor/eg_main_018236.asp

3. www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202426918666

Through end-to-end integration, our tools work together to reduce risky events, including accidental misuse, malicious activities, and malware that targets your sensitive data. We also take the tedium out of the user experience, management, audit, and reporting, so you and your entire user community can remain productive.

Beyond the Fear Factor: What It Means for You

Once you've recovered from the mere shock of such demanding regulations, the real challenge is finding a balance between implementing and maintaining the broad range of required controls and ensuring your IT team and your business are still able to operate efficiently and profitably.

Increasing security controls must not burden users or obstruct legitimate activities, or users and business managers will revolt.

This task isn't simple. Let's face it, today's corporate networks are truly virtual as employees access corporate information from anywhere at any time, taking advantage of laptops, smartphones, and removable storage devices. Security controls are a must to ensure that trusted employees can gain access to networked resources without fear of leaking corporate data. But users can't be assigned installation and update processes or hobbled by complex authentications or approval hurdles. If they have to deal with extra process, they want it to be seamless with their existing security experience.

Initially, many companies responded to the regulatory environment by adding data controls in a "piecemeal" approach. Many companies started and stopped with full-disk encryption of a few high-risk laptops. They had little incentive to invest in a coherent, integrated plan with corresponding administrative overhead. Every new control added manual, redundant, recurring management and auditing tasks.

Even stopgap controls are not enough. Newer regulations require that you not only have more extensive controls, but that you can prove to auditors and regulators that your security controls function automatically and meet requirements continuously, as users and policies change. With the prospect of more intense scrutiny, you need to find an efficient path to implement rigorous controls and adapt them as regulations change.

For business to function competitively, IT must enable controls while remaining efficient—and getting the rest of their work done. Efficiency requires a broader, company-wide view of security controls.

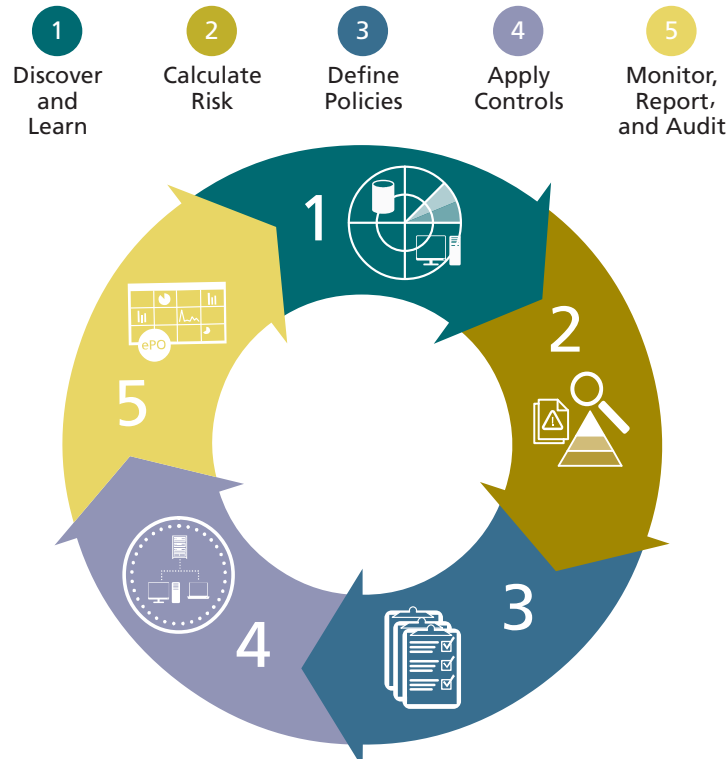
Starting Point: McAfee Data Protection Solutions

When it comes to data protection, there are many ways to mitigate risk. McAfee® Data Protection Solutions offer the flexibility to tailor security controls and protection to fit your organization's needs, structure, and budget. Best of all, you can choose to start where your risk is the most immediate.

Our solutions factor proven best practices into a five-step process. This approach allows you to see how your data is being used, and then implements the least intrusive and most effective security controls to protect it. Our integrated management streamlines tasks throughout the process, so you get greater compliance with less effort.

"Simply receiving notice of an investigation requires firms and individuals to incur the costs of retaining counsel and allocating time, energy, and resources to preparation."

Sarah Cortes
IT Compliance Advisor Blog⁴



Scoping the Problem

No company knows where all their data is, so they unknowingly underestimate their data loss risk. The reality is that most organizations don't even realize that they store so much sensitive data in so many places. McAfee has you covered with data discovery capabilities on your hosts and across your network. These not only enable you to find your sensitive data, but also catalog and understand it so you can assign appropriate risk levels—and act to protect it.

McAfee Network DLP Discover automates the process of understanding your information, including how it is used and accessed. This solution encompasses your network and data center to help you discover, understand, and classify your data according to your security priorities and policies. McAfee Host Data Loss Prevention offers options for crawling local drives on systems; discovering data based on file types, tags, categories, and dates; and even exploring files encrypted with McAfee Endpoint Encryption. Once you identify and understand your data and its legitimate use, it is easier to define and evolve policies to protect it.

Confronting Accidental Exposure from System Loss, Theft, or Physical Compromise

For most companies, the greatest compliance risk today comes from end users who accidentally expose data by losing devices or leaving them unprotected. As the mobility of today's workforce increases, it is more important than ever to give your users freedom without allowing them to become a liability. The threat not only lies with laptops, but also with a variety of wireless technologies such as smartphones, USB storage, and other portable devices, along with mistakes in transmissions across the network.

Regulated Data Defined

So what exactly is regulated data? It depends on the industry. Many regulations focus on personally identifiable information on individuals, such as Social Security numbers, addresses, or credit card numbers. It also can be computer access protection data (such as passwords) or protected patient health information (treatment records, diagnoses), or financial statements and other privileged corporate data. The unifying factor with regulated data is that it can be fairly easily recognized and reused: it has a specific number and pattern of characters or typical labels and terms.

Extensive Encryption Options

McAfee Endpoint Encryption provides multiple options to protect data from accidental exposure due to loss, theft, or compromise of devices—whether within or outside of corporate walls. To protect lost or stolen laptops and desktops, McAfee Endpoint Encryption for PC provides robust encryption and access control with two- and three-factor preboot authentication. McAfee Endpoint Encryption for Virtual Disks stretches security across virtual environments, including shared platforms, networks, and devices. It also defines and encrypts personal virtual disks that are fully portable and easily controlled.

McAfee Endpoint Encryption for Files and Folders protects against data being exposed beyond trusted workgroups that share servers and desktops. And McAfee Endpoint Encryption for Mobile secures smartphones and mobile devices by preventing unauthorized use or access to data on the devices. This option lets you encrypt standard applications including contacts, calendar, tasks, and emails that can contain sensitive, regulated data.

Rigorous Control over USB Devices

Since USB devices are ubiquitous, they merit extra attention. McAfee makes sure you can use them safely with integrated usage controls that address three particularly tough problems: enabling the legitimate use of removable USB storage devices; monitoring which devices are “good” and “bad,” and what users have them; and automatically guiding users on how to make good decisions with sensitive information. Yet we still stay out of their way when they are doing legitimate tasks.

McAfee Device Control transparently and seamlessly manages user behaviors with removable storage devices, letting you monitor and restrict what data can be copied to mobile devices. You can define what devices they can use and specify in detail which content can and cannot be copied to particular removable storage devices. Device Control does the rest, automatically monitoring usage and blocking any attempts to use devices or transfer data in violation of the policies you have set, even when data is modified, copied, pasted, compressed, or encrypted. Device Control allows legitimate business activities to proceed without disruption.

For safe use of USB devices, McAfee Endpoint Encryption for Removable Media can create managed encrypted space on your users’ personal or other unprotected devices. This locker makes it possible to guard sensitive corporate information for transport or future use, without inhibiting personal use.

For the ultimate convenience and control, you can provide approved USB devices with built-in encryption, multiple authentication factors, and even support for customized secure application environments. They are centrally managed with full data back-up and come in a range of sizes and authentication options, including biometric. McAfee Encrypted USB reliably encrypts storage for all information, and can secure a fully mobile business application environment, wherever your active users need it.

Protection Against Unintentional Mistakes and Intentional Malware

Although any user can inadvertently leak information, most really want to do the right thing, while remaining productive and effective in their jobs. It is important that the business of your business does not turn users into data sieves. McAfee Host Data Loss Prevention makes sure your users’ actions on their desktops and laptops do not put data at risk.

It provides full visibility and the control to protect your most critical data. You can easily monitor events in real time, apply centrally managed security policies, and generate detailed forensics—all without affecting your daily business activities. Host-based protection secures data regardless of where users and information travel, or whether or not client machines are connected to the corporate network.

Everyday electronic communications can also accidentally expose sensitive regulated data. Gateway controls can reduce and even squelch this risk across your network. Together, McAfee Network DLP Prevent, McAfee Email Gateway (formerly IronMail), and McAfee Web Gateway (formerly Webwasher) provide you with the controls you need and the confidence to allow information to flow securely. These solutions allow you to actively block, quarantine, or simply monitor outbound transmission of sensitive and regulated data.

Let's face facts--not all data loss is unintentional. Endless malware and malicious attacks deliberately try to steal data. McAfee leads the field in providing end-to-end, continuous protection against such threats. For instance, in one simple solution, McAfee Total Protection (ToPS) for Endpoint combines anti-virus, anti-spyware, anti-spam, web security, host intrusion prevention, network access control, and policy auditing.

In addition to endpoint and network controls, governance, risk, and compliance solutions from McAfee can help you understand your risk, manage vulnerabilities, and enforce policies end to end with options like dynamic whitelisting and application trust technology.

Simplified, Optimized, Unified Management

Increasing regulations on data privacy generate new requirements, more detailed controls, and different guidelines. They demand more audits, increased monitoring, and more rigorous management. Such tasks can be complicated and daunting, not to mention costly and time consuming. When you add a new control, do you also have to add a new agent, management environment, and maintenance program? Each new regulation heightens the need for integrated management, deployment, and administration of security and compliance products.

McAfee ePolicy Orchestrator® (ePO™ software) streamlines and simplifies these tasks by centralizing administration and improving consistency and control. This powerful system works across products to integrate and automate processes. With McAfee ePO software, even large deployments become manageable. A single agent simplifies installation and minimizes client compatibility issues, then simplifies maintenance so security does not weigh on end-user productivity.

A single, unified management console makes it easy for administrators to track systems, monitor changes, and define and distribute policy updates to the right users. From an audit perspective, separate products look like one. Data can be examined and documented more easily. Automated reporting further reduces the effort of proving compliance. The result is lower costs and greater control. In simple terms, you spend less time managing security and more time running your business. In fact, customer surveys show ePO users spend 36 percent less time and manage security with 22 percent fewer staff than customers without ePO.

Conclusion

Regardless of your industry, your data inevitably will come under regulatory scrutiny—from the state, the federal government, and international organizations. Your challenge is to find a balance between implementing the required controls cost effectively and ensuring your IT team and your business are still able to operate efficiently and profitably. Despite today's climate of heightened security for regulated data, you expect your users to maintain—and even exceed—their current level of productivity.

The answer is a comprehensive solution from a single vendor: McAfee. We can provide the layers of controls needed to address evolving regulations, as well as the integrated reports and audits to prove compliance. We give you the flexibility to meet ever-changing threats with the innovation and integration necessary to protect your data, all while driving down both operational and compliance costs. With McAfee protecting your sensitive data, you can focus on your business and not the business of data protection. Learn more at www.mcafee.com.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

