

Combating the Insider Risk to Data

McAfee® Data Protection solutions



According to Forrester Research, more than 65 percent of enterprises surveyed realize employee behavior is a significant threat to corporate security.

Forrester Research
 "Client Security Purchases
 Miss the Mark"
 April 4, 2008

The headlines about external threats to corporate data are frightening—and unrelenting. We've all read about hackers and cybercriminals stealing valuable confidential customer information by penetrating corporate networks from far-flung locations. Customers are expressing outrage at the public disclosure of their sensitive and private information as a result of these external attacks—and spending hundreds of hours restoring their precious identities. Companies are paying millions of dollars in penalties for regulatory noncompliance as well as suffering the long-term consequences of lost customer confidence and a tarnished brand.

While external threats continue to capture the lion's share of newspaper and online headlines, the bigger risk to data security actually exists within corporations' own four walls: employees who unwittingly expose the company's sensitive data and intellectual property to the public. Whether it's a researcher who accidentally sends a new product formula to hundreds of partners, or a junior member of the finance team who unknowingly exposes the company's unannounced financial results to the public, or even a hard-working, loyal employee who takes home his laptop or a USB drive for the weekend to get work done—and accidentally leaves it on the subway as he runs to greet his children at the end of a long workweek—the internal risk that can lead to data loss are real.

For example:

- In 2007, an official with the Dutch Foreign Ministry accidentally left a USB stick containing unencrypted confidential information—building maps, security codes, account information and more—in a rental car.¹
- A laptop stolen from the home of a U.S. Department of Veterans' Affairs employee contained the Social Security numbers and birth dates for nearly 27 million veterans and their spouses. None of the information was encrypted.²
- More recently, the Harris County (Texas) Hospital District admitted that an administrator, eager to catch up on work over the weekend, lost an unencrypted USB flash drive containing medical and financial records of 1,200 patients with AIDS, HIV, and other medical conditions.³
- And Countrywide Financial Corporation (now part of Bank of America) is still recovering from the theft and sale of personal information—including Social Security numbers—of nearly two million mortgage applicants, by a former employee in August, 2008.⁴

¹ The Inside Threat: A Data Loss Disaster, McAfee Corporation, February 2007, p. 10.

² Ibid., p. 12.

³ Network World. "Technology Executive Alert", Linda Musthaler, November 3, 2008.

⁴ Absolute Software, Laptop Security blog, "Countrywide Financial Insider Breaches 2 Million," August 11, 2008.

Protecting your vital information requires new technologies and strategies

Industry observers agree that, to protect themselves against the insider threat to data, companies must implement a comprehensive security strategy that includes both technological and social methods. For example, enterprises must deploy technology to address the protection of information assets as well as create a training and awareness program to ensure that employees act appropriately when interacting with intellectual property and other sensitive company information.

Before you can protect your information assets, you must know what information needs protecting. If you are like most companies, however, you don't completely know:

- **What** data you have
- **Where** it resides
- **Who** is accessing your data
- **When** users are accessing it
- **How** users are accessing it

Unfortunately, identifying your data—before a security incident—isn't easy. You need a comprehensive, proactive, and adaptive solution that automates data protection, enabling you to define the critical information assets you know need to be protected—and discover or learn what must be added.

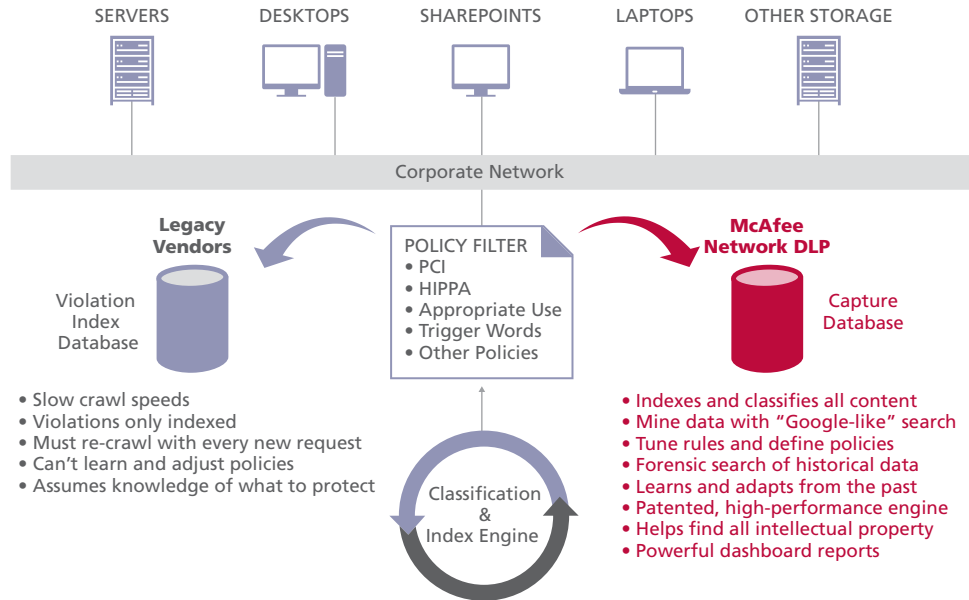
With McAfee Data Protection solutions, you can quickly determine **what** data needs to be secured, **when** you need to protect it, **who** is sending it out of the company, **how** sensitive is the data, and **where** it is stored. So you can reduce operational costs, decrease risk, and let your information become the lifeblood of your business again.

Protecting your vital information with McAfee Data Protection solutions

McAfee Data Protection solutions let you secure the data you know you need to protect—as well as automate the discovery and understanding of the data you don't know—to create a comprehensive solution that guards against the risk posed by insiders. By securing all your information—from the data center to the network endpoints—you protect it through all phases of its lifecycle—at rest, in motion, and in use—and ensure its confidentiality and integrity.

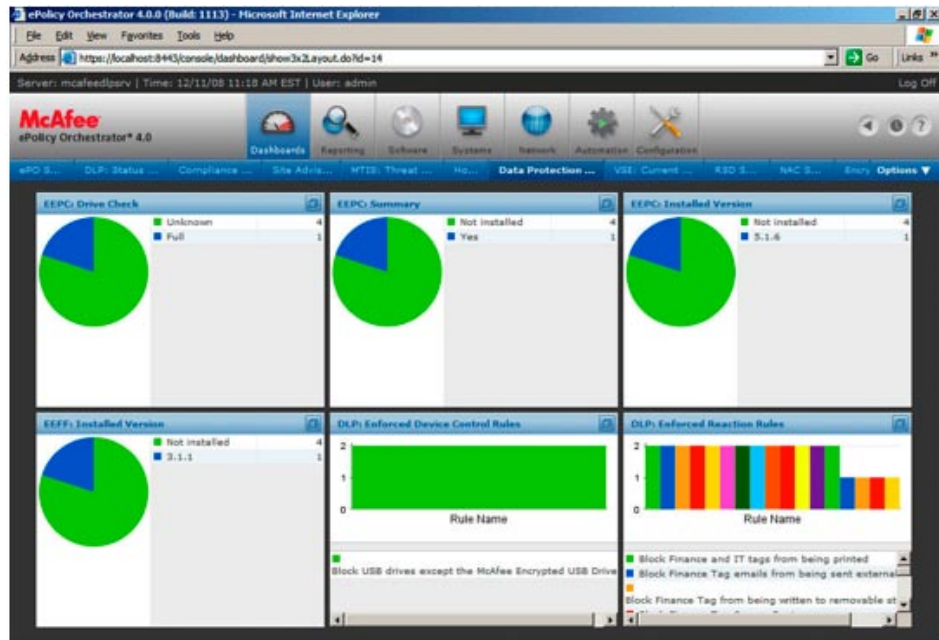
Within its data protection solutions, McAfee implements unique learning technologies to capture and index all content—whether or not a security rule was violated—enabling you to automate and accelerate the understanding of your most vital information. McAfee's "Google-like" learning capabilities allow you to mine the knowledge of your corporate information at rest, in motion, and in use, adapting and tuning protection to your specific requirements, and storing this information in a capture database. Once you have created the database, you can review all content, so you can understand your data, who is using it, how it is being used, where it is stored, and where it is going in your environment. With this technology, the process of identifying—and protecting—your sensitive data is reduced from months to just days.

Solution Brief Combating the Insider Risk to Data



McAfee Network Data Loss Prevention includes unique "Google-like" learning capabilities

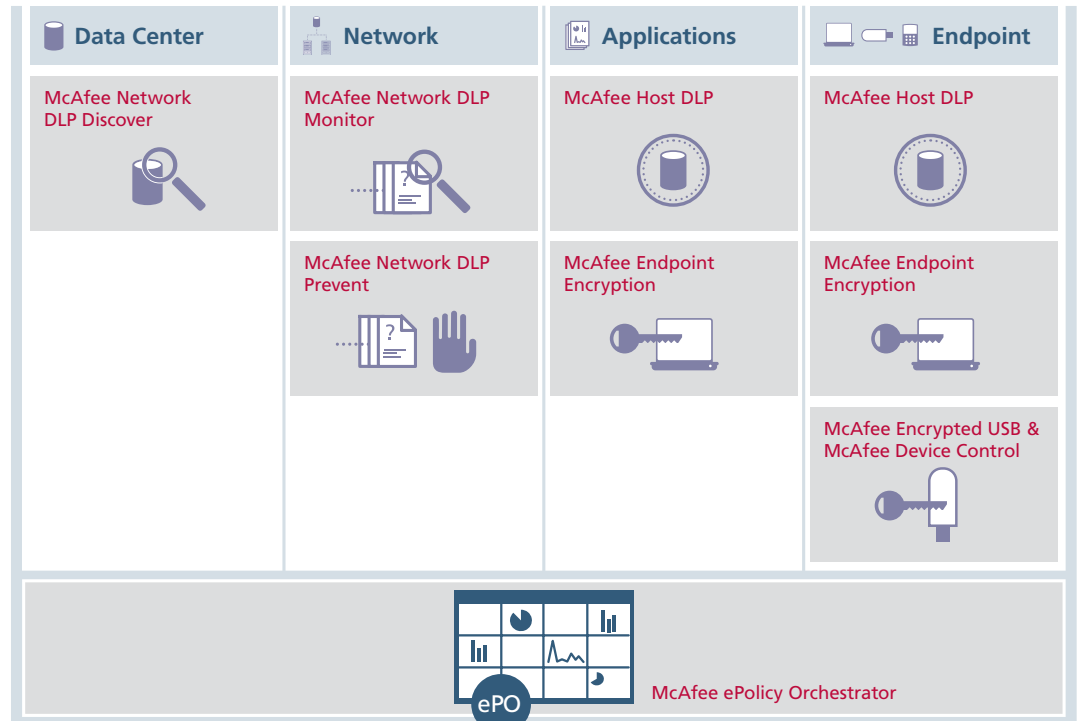
Integration with McAfee ePolicy Orchestrator® (ePO™) automates the process of monitoring, reporting, and responding to incidents, thereby further optimizing your security processes and infrastructure. This reduces overall costs by speeding the response to security incidents and shortening the time required to complete a data security audit.



The McAfee ePolicy Orchestrator Console automates incident monitoring, reporting, and mediation.

McAfee's Data Protection solutions: protecting from the data center to the network

McAfee Data Protection solutions are comprised of McAfee Network DLP Discover, McAfee Network DLP Monitor, McAfee Network DLP Prevent, McAfee Host DLP, McAfee Endpoint Encryption, McAfee Device Control, and McAfee Encrypted USB. They give you a clear roadmap to protecting your enterprise against data loss.



McAfee Data Protection solutions

Data Center

The roadmap to information assurance begins in the data center. You need to locate your data (in other words, what servers contain what content) and classify this information according to business purpose and its relationships to other content. Using **McAfee Network Data Discovery**, you can explore your data center and all the data sources across your network, helping you to discover the data you know—and what you don't know—classify it, and automate the process of understanding the business relationships between your data that will help accelerate your path to protection.

Network

After you have located and classified your data, you need to identify and track the issues within your organization that cause data loss. How can you prevent data from leaking out of your network? Are your email and web channels secure? Can you block unauthorized users? With **McAfee Network DLP Monitor**, you can gather, track, and report on the data-in-motion across your entire network, thereby understanding what and how information travels between your users and other organizations and uncovering threats to your data. Once these threats are understood, you can create rules using **McAfee Network DLP Prevent** to block inbound and outbound communications that violate your policy and put data at risk. In this way, you can actively protect your data against employee behavior and actions that unwittingly, unknowingly, or carelessly expose your company's information.

Applications

Now that you have analyzed and uncovered threats to the data in your network and put into place rules to prevent data loss through network communications—such as email, IM, and web—you must understand how users interact with enterprise applications to uncover additional threats to data privacy and integrity. Learning what your employees do with data helps you better understand how to protect your sensitive information. Can you prevent activities that would expose confidential data? Are you able to lock down sensitive data stored on shared workgroup servers? With **McAfee Host DLP**, you can monitor how your users work with your business applications and protect your data against risky behavior. When you add **McAfee Endpoint Encryption** to the equation, you gain the ability to encrypt files and folders on your workgroup servers to protect critical information—even when the data has been modified from its original form.

Endpoints

Once you have protected your information in the data center, on the network, and in your enterprise applications, you must protect against data loss via laptops and removable media, such as USB drives, MP3 players, CDs, and DVDs. **McAfee Endpoint Encryption** enables you to encrypt entire laptops and mobile devices, making them unusable in the event of loss. Using **McAfee Host DLP**, you can monitor how your users interact with and store data at the endpoints—and enforce policies to protect your data. **McAfee Device Control** lets you monitor and restrict what data can be copied onto these removable devices, enabling you to define and enforce policies that control which content can and cannot be copied onto which removable storage devices, monitors its usage, and blocks any unauthorized attempts to use these devices or transfer data in violation of defined policies. Finally, with **McAfee Encrypted USB**, you can provide encrypted mobile storage, coupled with strong authentication to protect against unauthorized data access in the case of accidental loss or misplacement of USB storage devices.

Conclusion

Protecting your organization against internal data threats is not just about protecting the sensitive information you know could put your company at risk if exposed. It's also about discovering those hidden data sources that you don't even know exist and have not secured. Staying on top of your organization's changing network and managing your data loss strategy is critical, but it is also time-consuming and costly. And it takes you away from adding real value to the bottom line, which is especially important during an uncertain economy.

With McAfee Data Protection solutions, you can protect the data you know you need to protect—and discover the data you don't know—with a comprehensive solution that secures your organization against insider threats. Reduce the overall time and cost of security by proactively mitigating the risk of insider breaches. Prevent employees from engaging in risky behavior by implementing technologies and policies that take the data they need and the workflow they use into account. Protect your organization before your data is compromised.

For more information about McAfee Data Protection solutions, please visit www.mcafee.com, or call us at 888.847.8766, 24 hours a day, seven days a week.

