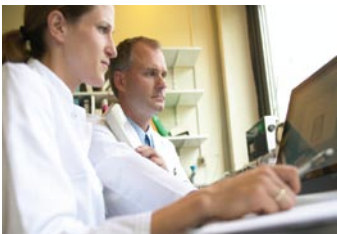


McAfee Network DLP Revolutionizes Electronic Evidence Discovery

The IT staffs of healthcare organizations struggle daily with the challenge of achieving compliance with both the Health Insurance Portability and Accountability Act (HIPAA) and their own internal policies, as well as protecting sensitive data and ensuring appropriate use of the network.



McAfee Network Data Loss Prevention helps organizations minimize litigation support costs through fast, accurate, and complete evidence discovery, thereby improving early case analysis and litigation readiness.

Given the rapid increase of corporate lawsuits, eDiscovery tools are becoming increasingly important within enterprise organizations to help contain costs associated with the identification and correlation of evidence related to each case. **McAfee® Network DLP (Data Loss Prevention)** offers revolutionary capabilities to augment eDiscovery practices and tools at tremendous cost savings, while improving visibility and completeness of evidence, also providing industry-leading data loss prevention (DLP) functionality. This paper will examine the eDiscovery process in detail, as well as the McAfee Network DLP approach to complementing and improving eDiscovery tools and practices, which are summarized as:

- Faster time-to-evidence for data-at-rest through powerful, high-performance crawling and search
- Increased coverage of evidence beyond files and email into network traffic and user activity
- Integrated case management helps keep processes focused, resources aligned, and case progress on track
- Accurate intellectual property detection through concepts and document registration
- Improved early case analysis posture

eDiscovery overview

eDiscovery tools provide a compelling value proposition in that relevant case data can be identified far more quickly—and cost effectively—than if that same data were analyzed by a team of auditors. Use of an eDiscovery tool is normally initiated once a legal team determines that litigation is needed or may happen in the near future, which leads them to focus the eDiscovery tool on the repositories that are most applicable to that case, commonly email, file servers, and laptops.

The eDiscovery tool then connects to these repositories and begins to fetch information. Content is then indexed—much like a search engine would do—and stored in a manner conducive to allowing the system user to perform searches against the data. Once the information has been fetched and indexed, a system user can run simple word queries—or complex compound queries containing keywords, expressions, and meta-parameters—to quickly identify data that is likely to be relevant to the case. This method of automated indexing and fast searching is in stark contrast to the more costly and time-consuming alternative, which involves human intervention on every piece of electronic information.

With eDiscovery tools, a high-confidence set of potential evidence objects is presented to the user as a result of a simple or complex query. This allows the case managers to focus on a smaller set of potential evidence objects, as opposed to manually sifting through and eliminating nonevidence data and other unrelated information from the entire collection of data. By minimizing the amount of data case managers or auditors must manually process—and improving the probability that the evidence they are examining is relevant to the case—case managers and auditors can more quickly identify relevant case evidence. Furthermore, eDiscovery tools can be used to assist in early case analysis, which may allow legal teams to quickly discover evidence that is so compelling that litigation may be avoided, potentially resulting in settlement out of court and the associated savings of time and money.

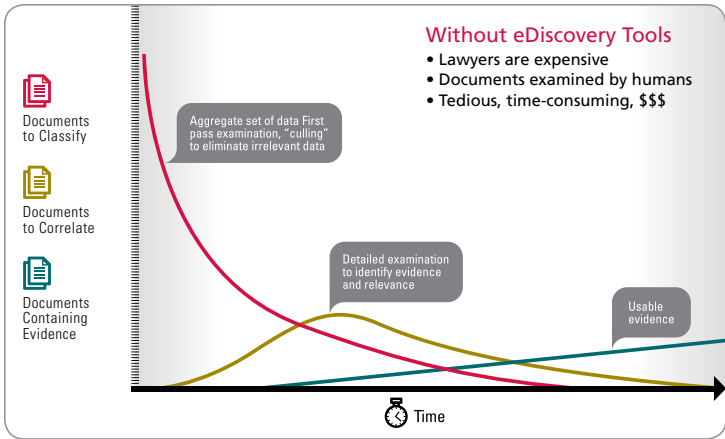


Figure 1. Evidence identification without eDiscovery tools.

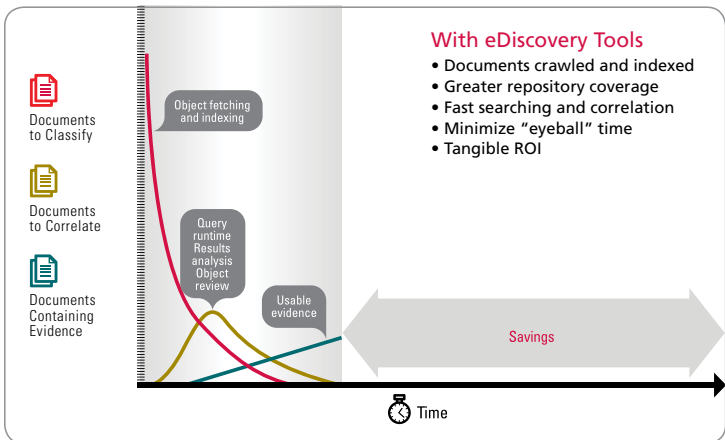


Figure 2. Evidence identification with eDiscovery tools.

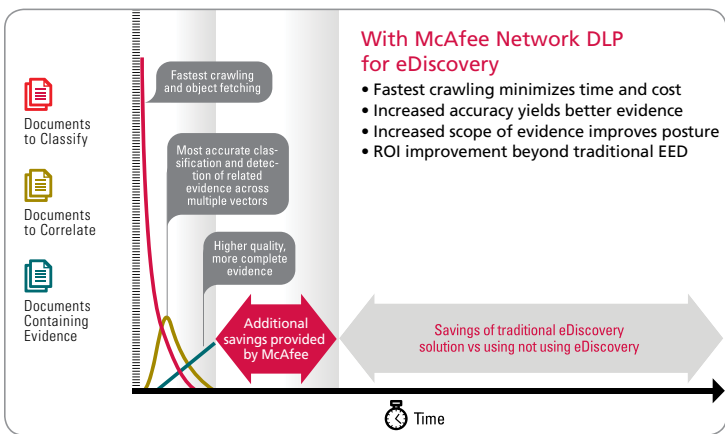


Figure 3. Time and cost savings with McAfee Network DLP for eDiscovery.

Figure 1 and Figure 2 show a comparison of document culling—eliminating irrelevant data—and evidence gathering with and without eDiscovery tools.

Once valid evidence has been identified, eDiscovery tools generally allow the case manager to either copy the evidence to protected storage or assign the information into a case management system that provides its own protected storage. The information copied to protected storage is considered to be forensically-sound assuming the meta information of the original object is preserved, an audit trail of any and all interaction by the system is documented and stored with the object, and the object is stored in such a way to eliminate the possibility of tampering or deletion. Evidence stored in this way and protected in this manner is considered to be viable for use in litigation because it has been protected, secured, and controlled.

Using McAfee Network DLP to Accelerate eDiscovery

McAfee Network DLP provides an industry-leading complement to eDiscovery tools and practices that allows case managers and lawyers minimize the amount of time—and costs—associated with discovering usable evidence and managing information through the case lifecycle. Additionally, McAfee Network DLP provides advantages that traditional eDiscovery tools can not provide, which bring new dimensions of evidence data and accuracy to your cases. All of these capabilities are provided in conjunction with the industry-leading DLP capabilities provided by McAfee Network DLP. With McAfee Network DLP, additional cost savings and case readiness benefits are provided. Figure 3 shows the time—and cost—reduction provided by McAfee Network DLP when used for eDiscovery.

First, McAfee Network DLP Discover provides the industry’s highest performance and accuracy for data at rest crawling, indexing, and analysis. McAfee Network DLP Discover crawls your network and quickly identifies content that is of interest to you, using the extensible and flexible McAfee Network DLP classification engine. With McAfee Network DLP Discover not only can you identify compliance data and the proliferation of your company intellectual property, but you can also create rules to proactively identify case data, or use the intuitive search interface to identify such contents in information that has already been crawled. McAfee Network DLP Discover provides comprehensive coverage of file servers, workstations, laptops, and other repositories, that help you isolate case evidence quickly.

Second, McAfee Network DLP Monitor examines and indexes all content entering or leaving the corporate network. Similar to McAfee Network DLP Discover, McAfee Network DLP Monitor can be configured using rules to generate incidents when certain types of information with a configured context are found leaving the network.

Solution Overview McAfee Network Data Loss Prevention Revolutionizes Electronic Evidence Discovery

Also like McAfee Network DLP Discover, McAfee Network DLP Monitor indexes all information and allows you to perform searches using content or context parameters, which are helpful in investigating user activity, identifying content usage behaviors, or understanding business process. From an eDiscovery perspective, McAfee Network DLP Monitor adds new dimensions of usable evidence, which encompass web transactions, webmail, instant messenger transactions, or data from other applications (such as FTP or P2P) that traditional eDiscovery tools can not provide. With McAfee Network DLP Monitor, your scope of evidence is increased beyond files and email into network traffic and user activity.

Third, McAfee Network DLP Manager provides aggregation of incident data and unified searches across McAfee Network DLP appliances. McAfee Network DLP Manager also provides a robust built-in case management system that can be leveraged by case owners and content managers for litigation scenarios to keep relevant case data in order or escalate items for review by a team of auditors. Data retained in a case can be from multiple vectors—including data-in-motion, data-at-rest, and data-in-use, and is forensically sound and digitally signed for protection.

Real-world examples

Consider the following real-world examples where eDiscovery has provided a tangible cost reduction and impact in the area of case readiness. In each example, McAfee Network DLP can provide additional value above and beyond what is provided by traditional eDiscovery products and tools.

Intellectual property litigation

Sensitive information assets are critical to the success of today's business. Intellectual property (IP)—the backbone of your current and future product strategy—is one of the most valuable assets to your organization. In situations where IP is compromised intentionally, or a competitor is found to be using patented IP, litigation generally follows to put an end to the misuse of protected information, which could compromise your business, strategy, brand—and even financial posture.

With traditional eDiscovery tools, you can scour the network looking for evidence of the existence of intellectual property to determine where it could have been sourced from and scour many thousands of email boxes to understand how it may have left the company. However, traditional eDiscovery tools don't cover the entire gamut of ways that IP could have been compromised. Traditional eDiscovery tools leave many questions unanswered, including:

- Could the information have left via an instant messenger conversation?
- Could the information have left while an employee was off the corporate network?

Furthermore, traditional eDiscovery tools may not provide the performance—or accuracy—that you need for early case assessment or even for trial. McAfee Network DLP helps improve your posture, saves you time and money, and increases accuracy for IP litigation:

- Comprehensive coverage of all ports and protocols at the network perimeter
- Endpoint protection to ensure consistency when the user is on or off the corporate network
- Increased accuracy in evidence discovery through document registration and hierarchical classification

Harassment

Today's litigious corporate environment brings about new strains for IT and information security professionals, particularly as it relates to code of ethical business conduct and appropriate behavior amongst employees, as well as with business partners and customers. A single instance of harassment or discrimination can damage an organization deeply and impact productivity, worker satisfaction, public perception, and may bring tremendous financial implication. Traditional eDiscovery tools provide ample coverage for email conversations, but leave many other items undiscovered, including:

- Did the harassment happen over some other channel, such as instant messaging conversations?
- Did the harassment include public defamation, perhaps through blog sites or bulletin boards?
- Could the harasser have left evidence outside of email that could support the case?

Solution Overview McAfee Network Data Loss Prevention Revolutionizes Electronic Evidence Discovery

McAfee Network DLP provides comprehensive detection and analysis of content in motion or at rest on your network—not just email or files. By providing coverage for other risk vectors such as instant messenger conversations and blog postings, McAfee Network DLP provides a more complete view of evidence compared to using traditional eDiscovery tools alone. With McAfee Network DLP, you can:

- Gain a better view of all pieces of evidence in motion or at rest on your network
- Identify areas of harassment that would not have been visible to you otherwise
- Streamline case workflow and improve litigation readiness

Summary

McAfee Network DLP provides a number of benefits to you and your organization for eDiscovery by providing powerful complements to existing eDiscovery tools. By using McAfee Network DLP to accelerate and improve your eDiscovery processes, customers can quickly realize cost savings and time savings due to the powerful, high-performance crawling and search capabilities. Additionally, evidence is more complete, as you are no longer limited to simply files and email, but can look into user behavior, network application traffic, and more. Evidence analysis is improved by leveraging the powerful concept-based classification engine of McAfee Network DLP and document registration. Case management for litigation and evidence review is streamlined and operationalized through the McAfee Network DLP case management framework. All of these benefits combined help provide cost savings, time savings, and most importantly, improved litigation posture.

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.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. It delivers proactive and proven solutions and services that secure systems and networks around the world, allowing users to browse and shop the web securely. With its unmatched security expertise and commitment to innovation, McAfee empowers home users, businesses, the public sector, and service providers by enabling them to comply with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

www.mcafee.com



McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2009 McAfee, Inc. All rights reserved.
5518bfr_dp_dlp_a_ediscovery_0109