SANS Review: McAfee's Total Protection for Data

SANS ANALYST PROGRAM

SANS Review: McAfee's Total Protection for Data

A SANS Whitepaper – June 2009

Written by Dave Shackleford

Executive Summary – Data Protection in Review

Ninety major breaches last year resulted in 285 million records being used in criminal activity, according to Verizon's 2009 Data Breach Report.[1] With breach reports like these, data protection has now become a central focus in IT environments. Resulting regulatory requirements, along with concerns over negative publicity (and its associated costs), have spawned a market for data-centric protections. So now, in addition to their traditional network security focus, organizations are looking more closely at where their critical data resides, how it's used, how it leaves the protected network, and how to protect sensitive and regulated data throughout its lifecycle.

However, when it comes to managing data at its source, organizations face a key challenge: How can they apply policy to their data in motion, data at rest, and data in use in any unified manner? As organizations lay out their data protection roadmaps to accomplish these goals, they need policies and procedures that evolve as new technologies and regulations dictate.

Over the past several years, the market for data protection tools evolved in fragments—starting with encryption thanks to Payment Card Industry and state privacy requirements. Host-based data fingerprinting and detection/prevention software followed, along with data-centric network-based monitoring and analysis. Now, the challenge is bringing these capabilities together to work and be managed in tandem—a challenge McAfee's Data Protection suite, Total Protection for Data, addresses robustly in Phase I integration of several acquired data protection components including SafeBoot (encryption), Reconnex (network policies) and others. Full integration into its overall centralized management framework, ePO (ePolicy Orchestrator), is scheduled for the next release, according to product managers.

- **Data in Motion:** Data moving across the network. Network-based tools that can "sniff" traffic are used for detection and prevention.
- **Data at Rest:** Data that is stored in various file types and databases. Host-based protections ranging from encryption to localized detection and prevention agents address security for this data.
- **Data in Use:** Data that is currently being accessed by applications and users. This data may require both host-based and network-based tools and techniques to adequately monitor and protect.

[1] www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

In this document, we describe the results of our review of a broad range of features and functions within McAfee's Total Protection for Data suite. This includes McAfee's Phase I integration of host (Host DLP v3.0) and network (Network DLP—Discover, Manager, Monitor, and Prevent—v8.5) data protection tools and management dashboards, along with McAfee's host-based full disk, file/folder and device control encryption (Endpoint Encryption (EE) for PC v5.1.8 and EE for Files and Folder v3.1.3).

Each of these products met or exceeded review objectives in all categories. Furthermore, McAfee has made strong headway in integrating management among the products, starting with its Host DLP integration into the ePO framework. Some of the grades the products received reflect elements that are prioritized and planned for integration in McAfee's next release, but which aren't integrated in the versions in this review.

Overall Report Card: Total Protection for Data by McAfee

Category	Products	Score
DLP	Network DLP (NDLP)	A
	Host DLP (HDLP)	A
Endpoint Encryption	Endpoint Encryption (EE) for PCs	A
	Endpoint Encryption for Files and Folders (EEFF)	A
Integration	HDLP Integration with ePO	A
	NDLP Integration with ePO	A
	EE Integration with ePO	B

In the following pages, we include more detailed report cards for DLP, encryption, and dashboard integration, with descriptions of review results for both the EE and DLP toolsets. Preceding the report cards is a description of review requirements and methodology.

Requirements

Data protection tools need to include fast, deep and accurate content identification for a variety of use scenarios that involve data at rest, data in use and data in motion. Policy creation and tuning must be flexible and intuitive for monitoring, discovering and taking appropriate action on critical data traversing the network—on data at rest or in use on the host, and as it attempts to leave the host on removable media, via e-mail or by other means. Any data protection toolkit should also include broad environmental coverage (network and host platforms, integration with directory services and e-mail platforms, and auxiliary functions like encryption.) While there are myriad requirements to consider, they essentially fall into the following five categories:

Discovery and Capture: Both host and network discovery tools should be capable of discovering sensitive content stored on key systems across the enterprise, a critical first step many organizations still need to take—and one that large enterprises cannot reasonably conduct without leveraging automated tools.

Monitoring: Data in use and in motion should be monitored at line-speed as it traverses network links. Monitoring of data on critical applications and systems, including storage devices, should be comprehensive, port agnostic and flexible enough to change policy on the fly when needed.

Alerting and Prevention: Host and network tools should be able to match detected events to policies, which then tie into an incident response (alerting and blocking specific actions). Workflow/alerting should involve specified participants from affected business units (Compliance, Human Resources, Legal, Help Desk, etc.). The system should also be self-learning, that is able to discover and alert on "unknown" or unclassified data types.

Encryption: Deployed encryption models should be flexibly and easily created and enforced for a variety of uses, such as file, folder, e-mail and full disk encryption as well as copying data to USB devices and other removable media.

Compliance: Policies and reports should be available out of the box, with the ability to easily modify these for internal compliance standards and changing regulations.

See our accompanying **Data Protection Requirements Worksheet**, which can be used to create individually tailored lists of requirements based on organizational needs and rank vendor ability to meet those requirements.

Methodology

The following McAfee products were included in the review:

- Endpoint Encryption (EE) for PC version 5.1.8
- EE for Files and Folders version 3.1.3 (V3.2 now available but was not yet released at time of review)
- Host DLP version 3.0
- Network DLP (Discover, Manager, Monitor, and Prevent) version 8.5
- Integration of these into the ePolicy Orchestrator version 4.0 (version 4.5 available soon)

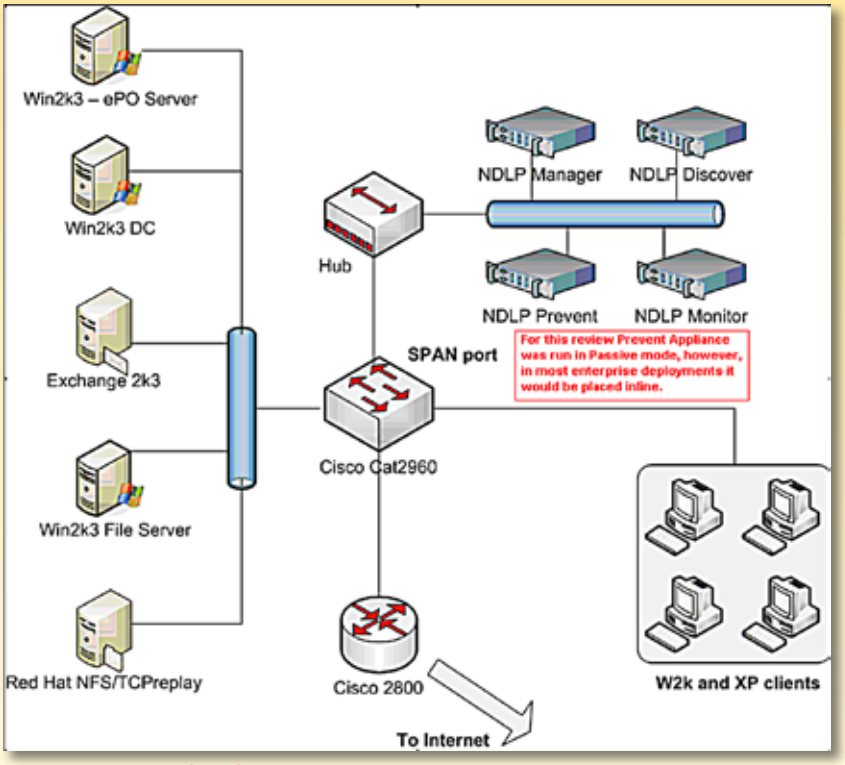

Figure 1: Review Lab Architecture

For this product review, a number of separate products and components were installed and configured. In the lab, the following systems were configured as illustrated in Figure 1:

- One Windows 2003 Server Domain Controller
- One Windows 2003 Server running Exchange Server 2003
- One Windows 2003 Server acting as a file server
- One Cisco 2960 switch with a span port activated, connected to a hub
- One Cisco 2800 connected to the Internet
- One Red Hat Linux Enterprise server running NFS and TCPreplay
- Four Windows workstations (two each of XP and Windows 2000)
- One Windows Server 2003 system running ePolicy Orchestrator (ePO)

The data formats used for testing included Microsoft Office documents and spreadsheets, text files, e-mail content, and PDF documents. Sensitive data types of interest included Social Security numbers, payment card data, customer lists, board meeting minutes, pharmaceutical formulas, tax information, and other intellectual property.

The product review methodology, at a high level, involved the following:

1. Installing and configuring the products, including integration with Active Directory and an e-mail server, as well as pointing components and agents to the ePO and the McAfee network DLP management platform.
2. Creating host and network DLP policies to implement within the test network and on workstations and servers.
3. Conducting network and host content discovery, capture and fingerprinting.
4. Testing modification of data on endpoints and attempting to remove data to external media, create screen captures, and so on.
5. Testing network data leakage detection by sending data across the network using TCPreplay and preconfigured PCAP files, as well as custom e-mails, file transfers and other such transmissions.
6. Testing encryption capabilities by defining policies for handling certain documents and data types and then moving the files to removable media or transmitting them via e-mail to determine whether encryption was properly maintained.

In this review, we refer to our accompanying **Data Protection Requirements Worksheet's** severity level ratings as we set up scores for features and functions. Priorities are described as follows:

Priority 1: Essential, critical features that must be considered for all organizations when evaluating DLP solutions.

Priority 2: Important features that deserve attention, but may not be deemed as critical depending on the organization.

Priority 3: Interesting features that may be worthy of focus and attention.

Assigned grades in this review are subjective. They are based on the reviewer's experience with the products, interviews with McAfee product managers, and discussions with information security professionals working with data protection tools in enterprise situations. Grades were assigned as follows:

A = Product met or exceeded expectations.

B = Product met all requirements with some exceptions.

C = Product met most requirements but was deficient in many.

D = Product met some requirements but was deficient in most.

SANS Review of McAfee Endpoint Encryption for PC (v5.1.8) and for Files and Folders (v3.1.3)

McAfee's Endpoint Encryption for PC (EEPC) and for Files and Folders (EEFF) allow for policy-based application and device control that can maintain persistent file and folder encryption across a variety of states—including sensitive files being transferred onto USB devices. EE for removable media is integrated into McAfee's central management platform, e Policy Orchestrator (ePO). McAfee plans to offer central management for third party, hardware-based Encrypted USBs and hard disk drives through ePO in the future.

Although not reviewed in this paper, the suite also includes encryption, as well as data and device management tools for protecting mobile devices using the Windows Mobile and Symbian platforms, with support for additional platforms planned for the future.

Key features reviewed in the EEEF and EEPC products include disabling system ports, defining what applications are trusted/untrusted (and what the applications are allowed to do on each system), and maintaining "persistent encryption" as data moves from the system via e-mail, removable media or other transmission method. Other features of note include:

- Complete encapsulation of the operating system on a user's system, replacing all login and system access functions.
- A central management console that keeps a running directory of users, systems, policies and other objects.
- Support for multiple two-factor authentication types like smart cards and hardware tokens.

EEEF extends this level of protection to files and folders on systems, allowing extremely granular policies to be established and maintained for different file types, system types and specific users.

The EEPC products were reviewed by first installing the Endpoint Encryption Manager, EE Server, and Object Directory on a Windows 2003 Server and then creating install packages with a variety of password, audit, and file/folder policies enabled. For both products, the review process consisted of the following:

- Selecting a "Password Only" token option after installation of the management components. Then selecting the default Program Files list and creating a variety of user and machine groups.
- Creating user-based policies that restrict several applications and logging attempts to use those applications.
- Creating machine groups and adding user groups to them. For EEFF, this included creation of several classes of encryption keys and policies including automatic encryption for Word documents and data copied to USB drives, user and group policies, etc.
- Generating and copying install packages to a USB for deployment to PCs.

After installation, policies were tested for each individual machine and found to work as specified without exception. All encrypted data remained encrypted while moving from the systems to devices. The user experience was easy, and users could not decrypt data that they had no rights to view.

Report Card: McAfee End Point Encryption for PC 5.1.8 and Files/Folders 3.1.3

Feature	Priority	Comments	Grade
Installation, Setup and Deployment	1	Deployment of the EE products was straightforward. There are several components that need to be installed—the EE Manager, Object Directory, and communications components. These are simple to install and manage. Users, Machines, and Machine Groups are all then easily created and modified. Finally, an installation package for clients is created, which can then be installed from removable media or via ePO, SMS or other software distribution tools.	A
Platform Support	1	EE products support Windows 2000, XP, Vista (32/64 bit), and Windows Server 2003. Mac OSX and Linux support are on the current McAfee DLP product roadmap, but not available at the time of this review.	B
User Transparency and Friendliness	2	The level of user transparency for the EE line is magnificent. Encryption and decryption of disk, files and folders had minimal impact on performance. Enforcement of policies and policy updates is performed seamlessly in the background without any user interaction required. As an option, a system tray icon can be made visible, allowing the user to perform some simple actions at the administrator's discretion.	A
Identity Management	1	LDAP, Active Directory, and other user identity repositories are supported. The product was specifically tested with Active Directory and integrated with no issues. All user management is performed at the repository level, and rules then propagate to the EE Management Server.	A
Centralized Administration and Role-Based Access	2	Administration and creation of agents are handled through a single console called the Endpoint Encryption Manager. Within this console, packages were generated with specific user and machine policies, token-based and other types of authentication configured, and deployment options set. Multiple administrator accounts were created, each with a variety of roles and permissions that were assigned according to business unit, machine groups, and so on.	A
Algorithm Support	2	FIPS 140-1/140-2 algorithms are supported, including AES and RC5 with strong key lengths (256-bit and up).	A
Key Management	1	Keys are not stored in plaintext on the server side and can be generated on the client and server. Authentication is required to access keys, and all key transfer communication is encrypted. This was observed by watching the traffic with a sniffer while managing and updating keys with clients.	A
Recovery Capabilities	1	Password and token recovery and resets were simple to perform, and "recovery administrators" can be created that don't have any additional privileges (great for Help Desk and Support teams that don't need full access). The software was robust, maintaining the encrypted state even after sudden power loss. One interesting feature is a challenge-response password reset option for users who forget passwords, which also allows users with lost tokens or smart cards to temporarily become "password-only users" at the local machine.	A
Security and Auditing	1	The EE products do not provide any sort of "master key." Only the keys used to encrypt data can decrypt the data. This provides an additional level of protection against any one administrator having the ability to access all encrypted data with a single key. Separation of duties was achieved by assigning specific roles for different administrators: "encryption administrators" or "user and machine administrators." In this way, certain administrators can be responsible for key management and encryption control, while others control user, group and machine administration. All boot and logon events are logged centrally, and audit trails can be exported in a number of formats.	A

SANS Review of McAfee Host and Network Data Protection

McAfee's Host DLP 3.0 and Network DLP 8.5 products cover a wide variety of different data protection use cases.

McAfee has integrated its agent-based **Host DLP (HDLP)** into the ePolicy Orchestrator (ePO) console with a robust Policy Manager that centers on several key areas. First, a number of tags and tagging rules are created. These are the foundation of HDLP and are used to classify content and define rules that identify content on systems on which agents are installed. Tagging rules can be based on applications, specific content patterns or locations. The classification methods provided are flexible, including regular expressions, dictionaries and registered documents. Users can also apply manual tags to files not covered by existing rules. Files being copied from sensitive shares can be tagged, and new files generated by applications can be tagged on the fly.

Protection rules are then created to define the actions taken when violations are found. A variety of applications and system types (including printers) can be included in these rules. To help locate applications that contain critical content, there are several major categories that define applications that edit content, archive content, and so on. Whitelists for applications and data can be created, and other rules for controlling the clipboard, screen capture, and device controls are also easily defined.

Host-based policies were then initiated through ePO and tested on workstations in various ways, including attempts to take screenshots or to copy protected information to removable media. All such attempts were successfully blocked and reported per policy requirements.

McAfee's **Network DLP (NDLP)** suite includes Discover (identifies sensitive data in the environment); Monitor (scans the network for sensitive data movement); Prevent (integrates with Web Proxies and Mail Transfer Agents to block sensitive content leakage); and Manager (manages all network DLP functions, policies and alerts). Once these products were installed in the test lab, data discovery was initiated to determine whether the NDLP platform could locate sensitive data at rest on the NFS and SMB file shares. Numerous document types were included (e.g., XLS, DOC, and PDF), and the DLP tools found and identified them accurately without advance knowledge of what or where they were.

Network traffic was then generated with SMTP and other applications, and sensitive data within the applications were all discovered and identified through the NDLP Monitor. Prevention rules were then tested with Microsoft Exchange. Sensitive e-mails were successfully blocked, and various types and methods of notifications were sent in accordance with pre-set policy. The Case Management system and workflow within the NDLP Manager was leveraged with multiple users and various roles. From a forensics standpoint, this tool is valuable because evidence was gathered and attached to cases. Case data, searches and reports history and other critical data are stored and indexed for examination and chain of custody if needed.

Report Card: McAfee Host DLP 3.0 and Network DLP 8.5

Feature	Priority	Comments	Grade
Installation and Initial Configuration	2	Installation of NDLP appliances was simple and intuitive—as close to "plug and play" as possible. Installation of HDLP was also simple. Documentation is excellent. Configuration of out-of-the-box policies is easy.	A
Integration with Directory Services and MTA (Mail Transfer Agent)	1	Integration with Microsoft Active Directory and Exchange servers was seamless and fast due to readily accessible configuration options within the NDLP and ePO consoles.	A
Data Discovery, Retention, and Archived Search	1	NDLP supports three scan modes: Registration (fingerprinting a repository's files), Discover (finding previously-fingerprinted files), and Inventory (generating a full listing of files, whether they are fingerprinted or not). Both CIFS and NFS network shares were reviewed using simple authentication via directory credentials. Scheduling scans and tying scans to existing rules and policies was simple. Performing searches based on violations and content types was also easy and flexible. HDLP discovery crawls each endpoint looking for sensitive content (regular expressions, dictionaries, content form registered document) and/or previously tagged files. Detected content files can be quarantined or encrypted using Endpoint Encryption products. Rules and policies based on the tags were easily created and monitored for violations. Events are then easily monitored within the ePO console, which archives and indexes event data with full search capabilities suitable for forensics, compliance or incident drill down.	A
Policy and Rule Creation and Management	1	Within NDLP, standard policies (known as Electronic Risk Modules) are installed by default and have a wide variety of flexible rules assigned to them. Compliance-specific policies are also available, and custom policies can be created easily by cloning an existing policy. NDLP rules are flexible and use standard Boolean and Regex-like syntax. Rules can also be tuned rapidly as dictated by logged events to refine and eliminate false positive and false negative behavior on the fly. Rule exceptions are also simple to add. For HDLP, classification rules are used to define sensitive categories according to regular expression, dictionaries, and registered documents. Tagging rules are used to tag files copied from sensitive location, or files generated by sensitive applications. Protection rules are then created to determine particular actions taken when data is transferred or transmitted. These rules are robust and use flexible syntax for tying data to specific applications, file servers, network shares, printers and unique content patterns. Finally, device rules are used to specify external devices like USB drives with a large variety of unique identifier data. Loading HDLP rules and policies into ePO was simple.	A
Detection of Data in Motion, at Rest, and in Use	1	The NDLP and HDLP products capably detected every attempt at sensitive data removal, modification, or transmission. Sensitive data in motion and use was successfully detected and logged in a variety of situations, including data sent in e-mail traffic, sent as e-mail attachments, processed within applications on hosts, and transferred to USB drives and CDs (CD-R). Attempts to capture screenshots and numerous other file manipulations were all successfully detected and logged.	A

Report Card: McAfee Host DLP 3.0 and Network DLP 8.5 *(CONTINUED)*

Feature	Priority	Comments	Grade
Incident Workflow and Management	1	The NDLP console is a robust, built-in case creation and management system that allows multiple incidents to be assigned for data at rest, in use and in motion. The only downside is that ePO does not directly manage the cases. It is only a minor inconvenience to launch the NDLP management console from within ePO and manage cases from all products there. Full case management integration is on McAfee's roadmap for next release.	A-
Centralized Management and Role-based Access	2	All events and systems could be managed from within ePO 4.0. Some of the NDLP functions within ePO launch a separate NDLP management console, but this is a minimal issue. Numerous roles can be assigned, including administrator, reviewer, agent administrator, auditor, and so on. Roles can be assigned to any user within the organization, and audit trails for user actions within the console are maintained.	A-
Reporting	2	A variety of reports that offer many options and chart types are available within the ePO console and NDLP manager.	A
Product Security	2	The NDLP appliances are purpose-built, locked-down devices that have only specific ports and services running. The McAfee host-based agents are also protected from user tampering and disabling.	A
Compliance	2	Although a wide variety of reports for compliance are available in the product, they are primarily focused on U.S.-based compliance. International regulatory compliance features are on the roadmap for next release, including content analysis and pattern matching in multiple languages, international compliance templates and reports, and additional languages for the user interface.	B

SANS Review: NDLP, HDLP, and Endpoint Encryption Integration Data Protection

With their latest developments and acquisitions in encryption, host and network DLP, McAfee has begun the integration to allow users to monitor and manage their critical data at use, data at rest, and data in motion within one framework. In this review, several critical first stages of this integration were in place, while others are on the product roadmap for next release.

One of the primary areas of focus for McAfee is consolidating management consoles into its ePO product, which would allow a simple, well-known interface to be leveraged for all policy and rule creation, package creation, event and incident management and reporting. Today, McAfee's integrated deployment, auditing and reporting for data discovery, monitoring, prevention, endpoint protection, device control and encryption can all be handled from within ePO. McAfee aims to provide automated correlation, central policy configuration and management from ePO in its next release.

Current integration of the Endpoint Encryption products with Host DLP is strong, allowing encryption capabilities to be integrated with HDLP policies for use in the following ways:

Data protection on USB and removable media: After defining named encryption keys in the EEFF product and adding them in the HDLP console, these keys can be used to encrypt data via HDLP "Removable Storage Protection" rules.

Network Share rules enforcement: Using HDLP "File Access Protection" rules, EEFF-encrypted files can maintain an encrypted state even when copied to network shares where the EEFF product is not running.

Automatic encryption on discovered data: Endpoint discovery rules can be created within HDLP and assigned "Encrypt" and "Monitor" actions on sensitive data discovered. When sensitive data is discovered on a host, the files and/or data can be quarantined and automatically encrypted.

In this report card on integration, the Priority column has been removed, as the priority level of integration actions was too subjective.

Integration Report Card: McAfee Total Protection for Data

Feature	Comments	Grade
Alerting and Reporting	All HDLP, NDLP and Encryption violation alerts can now be centrally monitored from within ePO. Numerous other reports in the ePO allow for collection and aggregation of alerts into single reports, providing a "single pane of glass" for all data incident information. Top-level tabs in the ePO Dashboards area provide immediate visibility into violations involving data at rest, in use and in motion. Violations can be broken down into several categories (e.g., severity and types of event).	A
HDLP Integration into ePO	The Host DLP product is fully integrated with ePO at this time. The HDLP Policy Manager is available from within the System tab in ePO and can be used to create, modify, manage and monitor policies for host DLP agents. Full HDLP reporting is in place within ePO, as well.	A
Endpoint Encryption Integration into ePO	Today, both McAfee's EEPC and EEFF are deployed and audited leveraging the ePO framework. However, client configuration for EEPC and EEFF is not yet integrated into ePO for centralized control, so it must be done outside ePO. The next software release migrates the EE key escrow into ePO and will provide for full client configuration within ePO.	B
NDLP Integration into ePO	NDLP integrates into ePO to lesser extent than HDLP. ePO can now consolidate NDLP reports into the Dashboards tab, and the NDLP management console can be launched directly from within ePO. Multiple levels of NDLP reporting detail are available in ePO without having to launch the console. Additional integration of NDLP into ePO is planned for the next release cycle.	B
Rule and Policy Support	Although not fully integrated, an important feature has been added into NDLP 8.5 that relates to HDLP and EE capabilities. Known as "Discover Remediation," this feature allows an administrator to leverage NDLP Discover to search for sensitive data at rest within the network environment (a critical automation point because no IT person knows how or where to find critical data outside the database). When critical data types are discovered, administrators can take actions based on context and situation. For example, upon discovery of sensitive data on a file share, an administrator using the NDLP Discover management interface could elect to move, copy, encrypt, and/or delete the data based on system recommendations. This capability is not fully automatic and still involves the administrator, which is actually by design, as most enterprises do not currently want fully automated remediation actions involving sensitive data. Policy and rule configuration is currently done from different management consoles for HDLP, NDLP and EE, although integration is planned for the next release. However, this may or may not be a big issue for organizations, because many still maintain a separation of duties and have distinct groups assigned to manage policy creation, rule/control development, and enforcement.	B
Workflow	Although not yet integrated into ePO, incidents involving data at rest, in use or in motion can now be investigated from within the NDLP Management console. All three event types can be added to cases, which can then be assigned to individual users/owners and have notes added to them—a strong feature for forensics, audit and follow-up. Extensive details from each incident are maintained with the cases in a chain of custody fashion, and the McAfee Capture capabilities provide updates on data movement and disposition over time. In addition, the easy-to-use workflow system allows multiple administrators and role-specific users to monitor and manage different aspects of each incident and case until it's resolved. McAfee plans additional case and incident workflow integration within ePO in next release.	B

Conclusion: Looking Forward

McAfee has taken great strides in integrating its multiple product acquisitions in the data protection area into a cohesive and capable solution. In the product versions reviewed, SANS analysts assessed each individual product line (Network DLP, Host DLP and Endpoint Encryption) to see if each would perform as advertised. For the DLP product lines, sensitive data at rest, in motion, and in use were capably detected and then handled according to previously specified rules and policies. The Endpoint Encryption products were flexible and easy to use and offered numerous key definition and management options.

McAfee has integrated a number of features and functions so that the products work together, a value for most enterprises that haven't been able to integrate separate data protection components on their own. This is also a value from a forensics standpoint when you consider that all data incidents, including those that are unknown, can be logged, indexed and archived for follow-up searching and reporting. McAfee's NDLP component can now leverage HDLP data. All of the HDLP and Endpoint Encryption rules and policies can be monitored and reported on within ePO. And much of the management can be done in a single console.

McAfee's efforts to integrate all of the DLP and EE products into their best-of-breed ePO console are well underway and will be largely complete in the next product releases. This will allow existing ePO customers to leverage and manage data protection capabilities and processes without having to learn and build new consoles and management middleware.

Additional international rules and compliance support, and integration with other product lines and partners, will further integrate risk management, network security, and data protections where needed. For example, McAfee intends to integrate IDS/IPS and GRC (Governance, Risk and Compliance) products into ePO and DLP, deepen its relationships with forensics solutions providers, and introduce other expansions to its data protection outreach.

These partnerships and integration plans will go a long way in taking risk management, forensics and compliance to the next level in which the comprehensive protection of sensitive data becomes embedded in security, risk management and operations infrastructures, as it should be.

About the Author

Dave Shackleford, SANS GIAC Technical Director and Chief Security Officer for Configuresoft. Dave has authored numerous SANS Analysts Program whitepapers, is a SANS course author and instructor, and co-authored "Hands-On Information Security," and the 'Managing Incident Response' chapter in "Readings and Cases in the Management of Information Security," both published by Course Technology. Previously, he worked as Chief Technology Officer for the Center for Internet Security and for a security consulting firm in Atlanta. He has worked as a security architect, analyst, and manager for several Fortune 500 companies and consulted with hundreds of organizations in the areas of regulatory compliance, security and data protections, and network architecture and engineering.

SANS would like to thank this paper's sponsor

Last Updated: April 26th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Doha 2018	OnlineQA	Apr 28, 2018 - May 03, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced