

## Решение McAfee Data Loss Prevention 9.0 — Что нового?

Новая версия решения McAfee® Data Loss Prevention предоставляет заказчикам более мощные, удобные и гибкие средства предотвращения потери данных (DLP). Эта новая версия, McAfee DLP 9, содержит ряд функций, которые обеспечивают тесную интеграцию с корпоративными системами управления учетными записями и профилями пользователей в сложных сетях. Приоритетной задачей было достижение максимального удобства применения, и эта задача решается средствами создания политик, управления списками, а также введением базы данных, которая составляется в результате сканирования — все это устанавливает новый стандарт простоты использования продукта. Наше решение не имеет себе равных по скорости развертывания и дополнительному эффекту, достигаемому благодаря средствам глубокого анализа данных.

Какие произошли изменения к лучшему? Мы значительно сократили нагрузку по администрированию, добавив новую единую политику для серверного и сетевого компонентов. Существенные усовершенствования в области интеграции с Microsoft Active Directory привели к улучшенной идентификации пользователей и более детальному управлению политиками — применимому даже к самым крупным организациям благодаря поддержке лесов Active Directory. Новый дизайн, знакомый заказчикам McAfee ePolicy Orchestrator® (McAfee ePO™), резко сокращает время, необходимое для обучения работе с продуктом. Тем, кто имеет дело с регулируруемыми данными, понравится возможность использовать политики для сканирования базы данных и сопоставления результатов с фактическими данными. Мы продолжили и работу, направленную на то, чтобы сделать McAfee Data Loss Prevention 9 логичным выбором для неанглоговорящих стран, и теперь поддерживаем 13 иностранных языков.

| Особенность   | Преимущество  |
|---|---|
| <b>Общая политика для сетевого и серверного компонентов</b> |   |
| Единая консоль для управления политиками                    | Теперь можно создавать политики, которые по мере необходимости загружаются как в серверный, так и в сетевой компоненты, позволяя легко настраивать все компоненты DLP. Это облегчает нагрузку на администраторов и обеспечивает лучшую согласованность политик по всей инфраструктуре, что, в свою очередь, значительно повышает эффективность работы и общую безопасность данных.  |
| <b>Сканирование базы данных</b>                             |   |
| Поддерживаемые базы данных                                  | В этой версии поддерживается сканирование следующих баз данных: <ul style="list-style-type: none"> <li>• Oracle 8i и более поздние версии</li> <li>• MySQL Enterprise 5.0 и 5.1</li> <li>• Microsoft SQL Server 7.0 до версии 2008</li> <li>• IBM DB2 5 до версии 9.1 включительно</li> </ul>   |
|   | Сканирование баз данных настраивается точно так же, как до сих пор настраивались функции инвентаризации или обнаружения. Настройка интерфейса пользователя (UI) усовершенствована с добавлением поддержки подключения к базе данных и фильтров, определяющих границы данных, подлежащих сканированию. Такой гибкий подход позволяет легко обнаруживать структурированные данные без необходимости применять схемы со справочной базой данных. |

| Особенность   | Преимущество   |
|---|--|
| <b>Сканирование базы данных</b>                       |  |
| Браузер базы данных                                   | Когда операция сканирования определена, администратор может просматривать подлежащую сканированию базу данных в режиме реального времени, определяя имена таблиц и строк, тип данных, число дочерних записей и количество записей, которые следует включить в процесс.   |
| Список операций сканирования                          | Список с указанием всех задач по сканированию в системе теперь содержит сканирование базы как новый тип сканирования. Это позволяет легко отличить сканирование базы данных от других задач, таких как сканирование с целью инвентаризации или обнаружения.  |
| Статистика сканирования                               | После сканирования базы данных предоставляется подробная статистика с результатами сканирования. Статистика включает количество обнаруженных каталогов, схем и таблиц. Кроме того, в состав статистических данных входит число таблиц и записей, выявленных в ходе операции сканирования. Такой уровень детализации позволяет администратору определить, какой процент данных отсканирован.                                      |
| Общие усовершенствования пользовательского интерфейса | В интерфейс администрирования добавлены элементы, относящиеся к сканированию базы данных. Это означает, что специфические элементы базы данных можно использовать для выбора данных, подготовки отчетов или указания исключений.   |
| <b>Динамическая регистрация данных</b>                |  |
| Обзор   | Динамическая регистрация данных (Dynamic Data Registration - DDR) представляет собой метод информирования системы о конкретных элементах данных, которые нуждаются в защите. Это могут быть списки имен клиентов и номеров счетов, номера кредитных карт, медицинские карты и многое другое. DDR сопоставляет конкретные значения данных, а не только модели, описывающие данные.  |
| Web-загрузки  | Для соблюдения требований уникальности новый Web-интерфейс позволяет загружать списки в формате CSV (элементы, разделенные запятыми) конкретных элементов данных, которые подлежат защите системой DDR.  |
| Загрузка результатов сканирования                     | Исходные данные для DDR можно извлекать также из результатов сканирования с целью обнаружения, что упрощает процесс заполнения системы и делает его более надежным по сравнению с другими решениями.   |
| <b>Улучшенная интеграция с Active Directory</b>       |  |
| Улучшенное управление идентификацией пользователей    | Личность пользователя теперь можно точно установить с помощью анализа перекрестных ссылок IP-адресов конечных точек, участвующих в выполнении действий над контекстом безопасности, и полного имени учетной записи пользователя (<DOMAIN/USER>) из Active Directory. Это позволяет точно идентифицировать любого пользователя, зарегистрированного в Active Directory, независимо от того, с какой рабочей станцией он работает. |

| Особенность   | Преимущество  |   |
|---|---|---|
| Использование атрибутов Active Directory в правилах | Усовершенствованные инструменты определения политики могут включать дополнительные атрибуты из Active Directory. Можно создать правило, ограничивающее возможности обработки данных для определенных групп или пользователей Active Directory. Теперь в определении политики можно использовать любую административную единицу (группу, отдел, отделение, регион, город, страну). |   |
| Поддержка лесов Active Directory                    | Теперь решение может использовать атрибуты из любого домена леса. Это означает, что даже самые крупные организации могут использовать упрощенные политики и схемы управления. Могут быть точно идентифицированы пользователи из любого домена леса.   |   |
| Дизайн  |   |   |
| Простота работы с сервером McAfee ePO               | Эта версия претерпела радикальные изменения в области дизайна пользовательского интерфейса. Теперь продукт естественно вписывается в сервер McAfee ePO, и любой пользователь, знакомый с этой консолью, немедленно признает, что ее удобство распространяется и на продукт DLP.   |   |
| Расширенная поддержка иностранных языков            |   |   |
| Поддерживаемые языки                                | Английский, Великобритания<br>Английский, США<br>Упрощенный китайский<br>Традиционный китайский<br>Корейский<br>Арабский<br>Русский<br>Турецкий   | Французский, Франция<br>Немецкий<br>Португальский<br>Испанский, Мексика<br>Испанский, Испания<br>Голландский<br>Иврит<br>Польский |
| Расширенная поддержка иностранных языков            |   |   |
| Встроенные политики                                 | Для каждого языка предусмотрено несколько полезных встроенных правил. Подробная информация о них содержится в файле README продукта.  |   |
| Новые политики                                      | Пользователи получили возможность создавать политики для поиска слов на их родном языке. Поддержка тех же возможностей, что и для английского языка, означает, что для защиты конфиденциальной информации во многих странах теперь можно использовать всю мощь решения McAfee Data Loss Prevention.   |   |
| Поиск   | Функции поиска продукта теперь поддерживает поиск неанглийских слов. Эта функция работает с результатами сбора данных, списками инцидентов и списками обнаружений.  |   |
| Интерфейс пользователя                              | Хотя в этой версии решения пользовательский интерфейс не локализован полностью, в него внесены изменения, гарантирующие корректное отображение неанглийского контента в пользовательском интерфейсе. Это облегчает применение неанглийских терминов или поиск нарушений при управлении системой или при выполнении расследований.   |   |

| Особенность   | Преимущество  |
|---|---|
| <b>Расширенный потенциал «концепций»</b>  |   |
| Расширенные возможности   | Предыдущие версии продукта поддерживали до 128 определенных концепций. (Концепции – это технология McAfee, которая позволяет легко идентифицировать данные на основе моделей и подобию.) В новой версии это число увеличено до 512 активных концепций, что повышает гибкость и уровень детализации, требуемые для крупных установок.  |
| <b>Усовершенствования в области правил и политик</b>                                |   |
| Помощь в определении политик  | Теперь интерфейс активнее помогает пользователю, максимально упрощая сложные задачи по созданию новых политик. При построении политики процесс отображается в окне, так что пользователь видит все условия, применяемые политикой. Теперь в окне создания политики при наведении курсора мыши на пункт появляется соответствующая подсказка. Списки концепций и протоколов сгруппированы по видам содержания, что облегчает поиск.  |
| <b>Автоматизированная проверка правил и политик</b>                                 |   |
|   | Теперь политики проверяют известные структуры данных, такие как номера социального страхования (SSN), гарантируя, что это действительно SSN, а не просто строка из девяти случайных цифр. Это резко снижает число ложных срабатываний и делает систему более точной и эффективной.  |
| <b>Шифрование конфиденциальных данных в базе данных McAfee Data Loss Prevention</b> |   |
| Безопасное хранение конфиденциальных данных   | В процессе работы решение собирает большое количество потенциально конфиденциальных данных. В новой версии все эти данные шифруются, что обеспечивает защиту от несанкционированного доступа.   |
| <b>Права на управление инцидентами на основе ролей</b>                              |   |
| Более детальный контроль  | Версия McAfee Data Loss Prevention 9.0 расширяет возможности по регулированию административных прав, предлагая гораздо более детальный контроль над тем, что может делать пользователь, наделенный правами администратора. В число дополнений входит возможность ограничивать права на чтение, запись и удаление данных для определенных групп пользователей; выбирать видимые элементы пользовательского интерфейса и устанавливать спецификацию пароля.   |
| <b>Интеграция с системой управления цифровыми правами Adobe LiveCycle</b>           |   |
| Распространение защиты за пределы сети  | Интеграция с системой Adobe LiveCycle DRM позволяет указывать в политиках атрибуты управления цифровыми правами (DRM). Решение McAfee Data Loss Prevention 9.0 может обеспечить применение политики DRM к конфиденциальным данным перед их отправкой по электронной почте, публикацией в Web или копированием на внешние устройства. После применения такая политика DRM продолжает следовать за данными, даже когда они покидают сеть. Таким образом, данные защищены везде, даже там, где контроль безопасности невозможен. |



## Решение McAfee Data Loss Prevention 9.0 — Что нового?

| Особенность                             | Преимущество  |
|---|---|
| <b>Расширенная поддержка документов</b> |   |
| Управление печатью PDF                  | Неанглийский текст теперь можно исключать из файлов PDF при их печати. Это позволяет защитить конфиденциальную или частную информацию от раскрытия во время печати.   |
| Классификация свойств документа         | Теперь система может классифицировать документы по содержанию свойств документа, таких как автор, тема, комментарии, ключевые слова и т.п. Это позволяет обнаруживать документы по создавшему их лицу или группе, независимо от содержания. Это полезно для групп, которые регулярно работают с конфиденциальной информацией, таких как отдел кадров, финансовый отдел или юридический отдел. |



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

McAfee, логотип McAfee, McAfee ePolicy Orchestrator и McAfee ePO — зарегистрированные товарные знаки или товарные знаки McAfee, Inc. или ее дочерних компаний в Соединенных Штатах и других странах. Все прочие наименования и товарные знаки являются собственностью их законных владельцев. Содержащиеся здесь планы выпуска новой продукции, технические характеристики и описания предоставлены исключительно в информационных целях, могут быть изменены без уведомления и не дают никаких гарантий, явных или подразумеваемых. Copyright © 2010 McAfee, Inc. 8606alrt\_dtp\_dlp9\_0310