McAfee Data Loss Prevention Endpoint

Не пополняйте статистику по утечке данных!

Теряете данные, даже не зная об этом? Быть может, прямо сейчас информация о клиентах, интеллектуальная собственность, финансовые данные и сведения о персонале покидают границы вашей компании. Злоумышленниками могут быть не только хакеры, но и ваши собственные сотрудники. Случайная или преднамеренная утечка данных может произойти через обычные каналы, например электронную почту, публикации на сайтах, USB-накопители и выгрузку данных в облако, и может обойтись вам в миллионы. Ежедневно компании становятся жертвами серьезных утечек данных из-за злоумышленной и случайной потери информации. А можно ли эффективно и просто предотвратить потерю данных? Что, если бы у вас была возможность и выполнять нормативно-правовые требования, и обеспечивать защиту интеллектуальной собственности? Теперь такая возможность у вас есть — благодаря комплексному решению McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).

DLP на устройствах и в облаке

Решение McAfee Endpoint DLP интегрировано с MVISION Cloud. Действие локальных политик DLP пользователь может распространить на облачные среды меньше чем за минуту всего одним щелчком мыши.[1] Использование классификационных тегов локально развернутых систем DLP в политиках облачных систем DLP обеспечивает согласованное обнаружение утечек данных.

Расширенные защитные функции

McAfee DLP Endpoint обеспечивает комплексную защиту всех потенциальных каналов утечки данных: съемных устройств хранения информации, облачных приложений, электронной почты, программ для мгновенного обмена сообщениями, веб-трафика, приложений для печати, буфера обмена, снимков экрана, приложений для обмена файлами и т. п.

Ключевые преимущества

- **DLP на устройствах и в облаке.** Локальные политики DLP легко переносятся в облако, что обеспечивает согласованное обнаружение утечек данных.
- **Расширенные защитные функции.** Средства создания цифровых отпечатков, классификации и маркировки файлов обеспечивают защиту конфиденциальных, неструктурированных данных (интеллектуальной собственности, коммерческих тайн и т. п.).
- **Централизованное управление.** Встроенные средства интеграции с McAfee® MVISION ePolicy Orchestrator® (MVISION ePO™) помогают оптимизировать управление политиками и инцидентами.[2]
- **Обеспечение нормативно-правового соответствия.** Обеспечивайте нормативно-правовое соответствие, выполняя мониторинг повседневных действий пользователей: работы с электронной почтой, публикации информации в облаке, загрузки файлов на съемные носители и т. п.

Подписаться

Основные функциональные возможности McAfee DLP Endpoint:

- Возможность присваивать передаваемым данным метки Microsoft Azure для защиты информации (Azure Information Protection — AIP) и распознавать файлы, помеченные метками AIP.[3]
- Интеграция со средствами анализа поведения пользователей (UEBA) от сторонних поставщиков устраняет внутренние угрозы. Анализируя данные об угрозах, продукт обнаруживает случаи необычного и крайне опасного поведения пользователей и организаций.
- Возможность классифицировать документы вручную позволяет пользователям классифицировать документы вручную: это ведет к повышению уровня осведомленности сотрудников в вопросах защиты данных и снижает нагрузку на администраторов.
- Инициируемое пользователем сканирование сети и обновление систем дает возможность самостоятельно запускать сканирование конечных точек и принимать меры самовосстановления.
- Гибкий механизм классификации, включающий в себя словари, алгоритмы поиска с использованием регулярных выражений, алгоритмы проверки и зарегистрированные документы, также поддерживающий сторонние классификационные решения для пользователей.
- Уникальная технология маркировки документов в соответствии с их происхождением позволяет предотвращать копирование, переименование и кражу конфиденциальной информации из веб-приложений, сетевых приложений и общих сетевых ресурсов.
- Расширенная поддержка виртуализации для защиты удаленных рабочих столов и решений для виртуальных рабочих столов (VDI).

Централизованное управление

- Управление осуществляется через облачную консоль управления MVISION ePO, что оптимизирует управление политиками и инцидентами.[4]
- В продукте используются те же самые модули политик и классификации, а также те же самые процессы работы с инцидентами, что и в McAfee® MVISION Cloud (CASB) и McAfee® Network DLP.
- Наличие большого количества политик и наборов правил с возможностью многократного использования позволяет задавать множество разных политик предотвращения утечек данных в масштабах всей организации, создавать политики в соответствии с требованиями офисов, подразделений, законодательства и др.
- Повышенный уровень детализации при управлении инцидентами дает возможность искать/фильтровать/просматривать инциденты по любому их свойству (серийному номеру устройства, имени файла подтверждения, группам и т. д.).
- **Обучение пользователей.** Информационные всплывающие окна, отображаемые в режиме реального времени в ответ на действия пользователя, помогают повысить осведомленность пользователей и корпоративную культуру безопасности.

Поддерживаемые платформы

- Windows 10 (32- и 64-разрядные версии)
- Windows 8 и 8.1 (32- и 64-разрядные версии)
- Windows 7 (32- и 64-разрядные версии)
- Windows Server 2019
- Windows Server 2016 (64-разрядная версия)
- Windows Server 2012 (64-разрядная версия) и Windows Server 2012 R2 (64-разрядная версия)
- Windows Server 2008 (32- и 64-разрядные версии) и Windows Server 2008 R2 (32- и 64-разрядные версии)
- macOS Catalina 10.15 или выше
- macOS Mojave 10.14 или выше
- macOS High Sierra 10.13 или выше
- macOS Sierra 10.12 или выше
- OS X El Capitan 10.11 или выше
- OS X Yosemite 10.10 или выше
- OS X Mavericks 10.9.0 или выше

Поддерживаемые веб-браузеры

- Internet Explorer 11 или выше
- Mozilla Firefox 48 или выше
- Google Chrome 65 или выше

- Функции централизованного мониторинга и аудита событий.
- Расширенный контроль доступа на основе ролей («разграничение полномочий»), помогающий управлять политиками и анализировать инциденты.
- Простой доступ к интерфейсу службы поддержки.

Обеспечение нормативно-правового соответствия и обучение пользователей

Поскольку периметр корпоративной сети становится все более размытым, корпорациям становится все сложнее обеспечивать нормативно-правовое соответствие. McAfee DLP Endpoint не только поможет вам вести мониторинг повседневного поведения пользователей, но и обеспечит нормативно-правовое соответствие путем обучения пользователей. Одним нажатием кнопки программное обеспечение McAfee DLP Endpoint позволяет создавать подробные отчеты, призванные подтвердить наличие мероприятий, направленных на обеспечение соответствия нормативным и корпоративным требованиям, для предоставления их аудиторам, руководителям предприятий и акционерам. В него включены готовые политики для разных законодательных требований и сценариев использования, что облегчит вам задачу обеспечения нормативно-правового соответствия. Кроме того, ваши пользователи будут в режиме реального времени получать обратную связь в виде принудительно всплывающих окон, информирующих их о требованиях корпоративной политики. Это позволит вам постепенно развить у своих сотрудниках более ответственное отношение к обеспечению безопасности.

Поддерживаемое ПО McAfee ePO

- McAfee ePO 5.9.1 и 5.10 for DLP 11.1 или выше

Поддержка for McAfee MVISION ePO (SaaS)

- Для версии DLP 11.5 и выше не требуется установки программного обеспечения или расширения DLP. Чтобы получить доступ к консоли управления MVISION ePO необходимо пройти процесс аутентификации, введя имя пользователя и пароль.

Полный перечень поддерживаемых платформ, веб-браузеров и программных продуктов см. в базе знаний McAfee.

Дополнительная информация

Для получения более подробных сведений посетите наш сайт www.mcafee.com/ru/products/dlp-endpoint.aspx.

1. По результатам проведенных в McAfee систематических лабораторных испытаний.
2. McAfee DLP Endpoint 11.5 или выше
3. Там же.
4. Там же.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru

McAfee, логотип McAfee, ePolicy Orchestrator и McAfee ePO являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2020 McAfee, LLC. 4456_0520
МАЙ 2020 г.