Symantec by Broadcom Software

Product Brief

Symantec® Data Loss Prevention

Полная защита конфиденциальных данных

Высочайший уровень защиты данных

• Самая широкая защита данных по каналам связи: облако, электронная почта, веб, конечные точки и хранилища.

• Меньшее количество ложных срабатываний благодаря комплексным технологиям обнаружения.

Единая панель управления

• Единая консоль для управления политиками, реагирования на инциденты, создания отчетов и администрирования.

• Единый набор политик и рабочих процессов для всех каналов связи: облака, электронной почты, Интернета, конечных точек и хранилищ.

Широкий спектр интеграций

• Входит в состав Symantec Enterprise Cloud, которое поддерживает концепцию SASE, ориентированную на данные и поддерживающую гибридные технологии.

• Полная интеграция с Microsoft Information Protection для классификации, шифрования и управления правами на данные.

Остановите потерю данных с помощью самого высокого уровня защиты

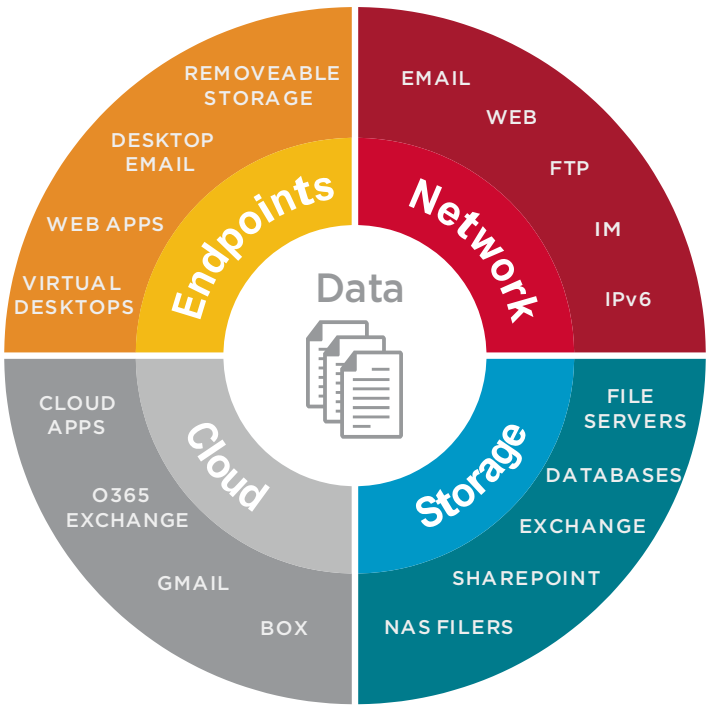
Обеспечить безопасность и соответствие информации нормативным требованиям всегда было непросто. Но сегодня предприятия сталкиваются с новыми и неожиданными проблемами безопасности. По мере того, как все больше компаний отказываются от использования локальных систем и переходят на облачные сервисы, данные компании становятся все более уязвимыми для случайного воздействия неопытных пользователей облака и ошибок в конфигурации. Безопасность облачных вычислений – не единственное, что беспокоит предприятия: целенаправленные кибератаки становятся все более распространенным явлением, поскольку злоумышленники разрабатывают новые эффективные методы, позволяющие обходить традиционные меры безопасности и использовать пользователей для кражи ценных данных компаний.

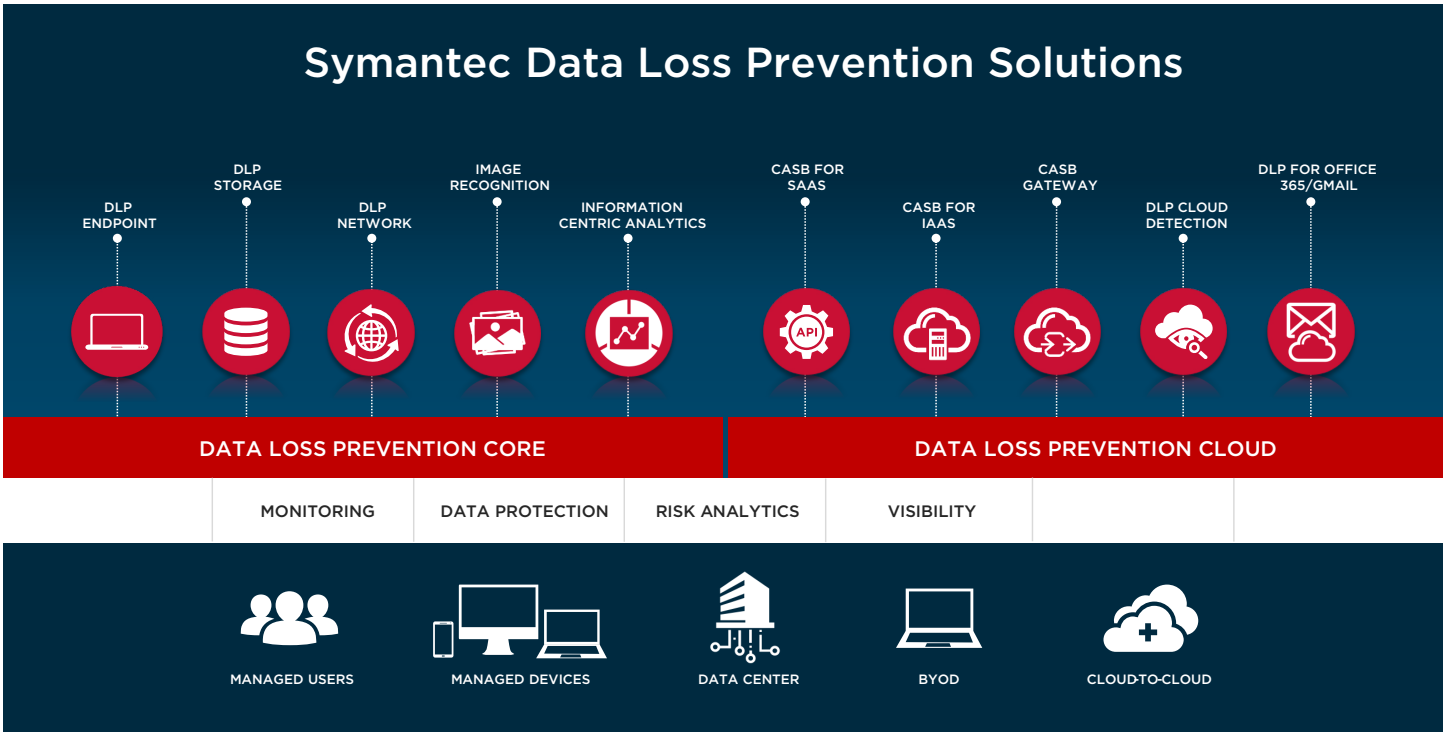
Решение Symantec Data Loss Prevention (DLP) обеспечивает высочайший уровень защиты, необходимый для предотвращения утечек данных и сохранения репутации компании. Благодаря нашей ведущей в отрасли технологии вы получаете комплексные возможности обнаружения, мониторинга и защиты, обеспечивающие полную видимость и контроль над конфиденциальными данными.

• Обнаружение местонахождения данных во всех каналах: облаке, электронной почте, Интернете, конечных точках и хранилищах.

• Мониторинг использования данных в корпоративной сети и за ее пределами.

• Защита данных от раскрытия или кражи в режиме реального времени.





Простой способ получить необходимое покрытие

Symantec DLP выпускается в виде двух наборов решений: DLP Core и DLP Cloud. Вместе они обеспечивают защиту информационной безопасности мирового класса на конечных точках, в сети, облаке и хранилищах. DLP Core включает в себя защиту конечных точек, сети и хранилищ, а также функции распознавания чувствительных изображений и информационно-ориентированной аналитики (User Entity Behavior Analytics). DLP Cloud позволяет распространить политики DLP на облачные среды, обеспечивая полный контроль CASB, а также облачные коннекторы DLP для шлюзов Web и Email.

Обеспечение безопасности данных на конечных устройствах

По мере повышения мобильности сотрудников за счет использования ноутбуков данные компании становятся все более уязвимыми для утечек и краж – как в корпоративной сети, так и за ее пределами. Решение Symantec DLP for Endpoint (поставляется вместе с DLP Core) обеспечивает всю необходимую защиту конфиденциальных данных на конечных точках. Оно обеспечивает полное обнаружение, мониторинг и защиту данных, используемых по широкому спектру каналов: электронная почта, облачные приложения, сетевые протоколы, внешние хранилища, виртуальные рабочие столы и серверы. В Symantec DLP единый легкий агент для конечных точек позволяет использовать два модуля: DLP Endpoint Discover и DLP Endpoint Prevent.

- **Symantec DLP Endpoint Discover** сканирует локальные жесткие диски и обеспечивает глубокую видимость конфиденциальных файлов, которые пользователи хранят на своих ноутбуках и настольных компьютерах. Он предоставляет широкий спектр ответных мер, включая локальный и удаленный карантин файлов, шифрование на основе политик и управление цифровыми правами с помощью DLP Endpoint FlexResponse API.
- **Symantec DLP Endpoint Prevent** отслеживает действия пользователей и осуществляет тщательный контроль над широким спектром приложений, устройств и платформ. Он обеспечивает широкий спектр ответных мер, включая шифрование на основе идентификационных данных и цифровые права для файлов, передаваемых на USB. С помощью Endpoint Prevent можно предупреждать пользователей об инцидентах с помощью всплывающих окон на экране или уведомлений по электронной почте. Пользователи также могут отменить политики, предоставив обоснование или отменив действие (в случае ложного срабатывания).

Endpoint	Availability
Browsers	Chrome | Safari | Firefox | IE and Edge
Cloud Apps	Box | Dropbox | Google Drive | Microsoft OneDrive
Email Apps	Outlook | Lotus Notes
Network Protocols	HTTP | HTTPS | FTP
Removable Storage	MSC devices | MTP devices
Virtual Desktops	Citrix | Microsoft Hyper-V | VMware
Others	Print | Fax | Network Share | Clipboard

Защита данных в движении по сети

Широкое распространение средств совместной работы и облачных приложений в сочетании с рискованным поведением сотрудников, о котором компании могут даже не подозревать, повышает риск утечки данных через деловые коммуникации. Решение Symantec DLP for Network (поставляется с DLP Core) контролирует и предотвращает утечку конфиденциальных данных по широкому спектру коммуникационных протоколов в сети.

DLP Network Monitor перехватывает и анализирует исходящий трафик в корпоративной сети, обнаруживает конфиденциальное содержимое и метаданные по стандартным, нестандартным и проприетарным протоколам. Он устанавливается в точках выхода из сети и интегрируется с сетевым коммутатором или анализатором коммутируемых портов (SPAN). Network Monitor выполняет глубокую проверку содержимого всех сетевых соединений с нулевыми потерями пакетов, в отличие от других решений, которые производят выборку пакетов во время пиковых нагрузок и подвергают вас высокому риску ложных отрицательных результатов.

DLP Network Prevent for Email защищает конфиденциальные сообщения от утечки или кражи сотрудниками, подрядчиками и партнерами. Решение отслеживает и анализирует весь корпоративный почтовый трафик, а также модифицирует, перенаправляет или блокирует сообщения на основе их конфиденциального содержимого или других атрибутов. Решение Network Prevent for Email развертывается в точках выхода из сети и интегрируется с агентами передачи почты (MTA) и облачной электронной почтой, включая Microsoft Office 365 Exchange. Network Prevent for Email поставляется в виде программного обеспечения или виртуального устройства.

DLP Network Prevent for Web обеспечивает защиту конфиденциальных данных от утечки в Интернет. Решение отслеживает и анализирует весь корпоративный веб-трафик и по желанию удаляет чувствительный HTML-контент или блокирует запросы. Network Prevent for Web развертывается в точках выхода из сети и интегрируется с прокси-сервером HTTP, HTTPS или FTP с помощью ICAP. Network Prevent for Web поставляется в виде программного обеспечения, аппаратного или виртуального устройства.

Защита данных в состоянии покоя в различных хранилищах

Объем цифровых данных значительно увеличивается, в основном за счет внутренних документов, однако мало кто из компаний уделяет внимание их управлению и защите. С помощью Symantec DLP для хранилищ (входит в состав DLP Core) можно обнаружить и защитить конфиденциальные данные в состоянии покоя – данные, хранящиеся на файловых серверах, конечных точках, в облачных хранилищах, сетевых файловых ресурсах, базах данных, SharePoint и других репозиториях данных.

Repository	Availability
File Servers	Windows via CIFS and DFS | Unix via NFS | Local Windows | Local Unix (Linux, AIX and Solaris) | NAS Filers
Distributed Machines	Laptops | Desktops
Document and Email Repositories	SharePoint | LiveLink | Documentum | Lotus Notes | Microsoft Exchange | PST
Web Content and Applications	Corporate Web Sites | Intranet | Extranet | Custom Applications
Databases	Oracle | Microsoft | IBM DB2

Во-первых, Symantec DLP Network Discover находит конфиденциальные данные путем сканирования сетевых файлообменников, баз данных и других хранилищ корпоративной информации. К ним относятся локальные файловые системы на серверах Windows, Linux, AIX и Solaris, базы данных Lotus Notes и SQL, а также серверы Microsoft Exchange и SharePoint. DLP Network Discover распознает более 330 различных типов файлов, включая пользовательские, на основе бинарной подписи файла. Кроме того, решение обеспечивает высокую скорость сканирования для больших распределенных сред и оптимизирует производительность за счет сканирования только новых или измененных файлов.

Далее, Symantec DLP Network Protect добавляет к Network Discover надежные возможности защиты файлов. Network Protect автоматически очищает и защищает все открытые файлы, обнаруженные Network Discover, и предлагает широкий спектр вариантов исправления ситуации, включая помещение файлов в карантин или их перемещение, копирование файлов в область карантина или применение к конкретным файлам шифрования и цифровых прав на основе идентификации политик. Network Protect даже информирует бизнес-пользователей о нарушениях политики, оставляя в исходном местоположении файла текстовый файл с маркером, объясняющим причину карантина.

Symantec DLP также включает платформу FlexResponse API, которая позволяет создавать пользовательские действия по устранению последствий для файлов. FlexResponse обеспечивает простую интеграцию "под ключ" с другими решениями Symantec и сторонних производителей в области защиты файлов, включая Symantec File Share Encryption и Adobe LiveCycle.

Защита данных в облаке

Проблемы безопасности не утихают, поскольку компании продолжают переносить устаревшие ИТ-приложения в общедоступные облачные службы, где сложно обеспечить такой же уровень видимости и контроля конфиденциальных данных, как на собственных частных серверах. С помощью Symantec DLP Cloud вы можете распространить мощные средства защиты данных на облако, обеспечив удобство использования облачной DLP. Оно предоставляет широкие возможности обнаружения, мониторинга и защиты для широкого спектра облачных приложений, а также локальных приложений.

Защита данных в облаке (продолжение)

Symantec DLP Cloud Detection Service проверяет содержимое, извлеченное из облачных приложений и веб-трафика, и автоматически применяет политики защиты конфиденциальных данных. Она предлагает расширенную интеграцию с Symantec CloudSOC, нашим ведущим в отрасли брокерским решением для защиты доступа к облаку, для защиты данных в движении и данных в состоянии покоя в более чем 100 санкционированных и несанкционированных облачных приложениях, таких как Office 365, G-Suite, Box, Dropbox и Salesforce. Интеграция позволяет расширить существующие политики и обеспечить надежное обнаружение облачных приложений, управляя всеми инцидентами с консоли DLP. Средства управления включают отказ от совместного использования конфиденциальных файлов, помещение их в карантин, блокировку выхода из приложения, а также автоматическое применение шифрования на основе идентификации и цифровых прав к определенным файлам, передаваемым третьим лицам. Symantec DLP Cloud Detection также предлагает расширенную интеграцию с Symantec Web Security Service для мониторинга веб-трафика – даже в зашифрованном виде – и защиты перемещающихся и мобильных пользователей.

Symantec DLP Cloud поддерживает электронную почту, обеспечивая точный мониторинг корпоративного почтового трафика в режиме реального времени за счет использования встроенных интеллектуальных средств и расширенных возможностей обнаружения, которые сводят к минимуму количество ложных срабатываний. Кроме того, решение обеспечивает защиту от утечки данных в режиме реального времени с помощью автоматического блокирования сообщений или их модификации для последующего шифрования или помещения в карантин. При передаче данных третьим лицам может быть автоматически включено шифрование на основе идентификации и цифровых прав для электронных писем и вложений. Облачный сервис DLP для электронной почты поддерживает Gmail for Work, Microsoft Office 365 Exchange Online, а также Microsoft Exchange Server. Он доступен как отдельно, так и в комплекте с превосходными возможностями защиты от угроз электронной почты, предоставляемыми облачным сервисом Symantec Email Security.cloud.

Управление с единой панели

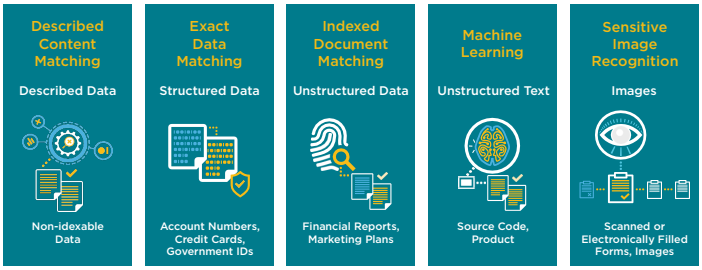
По мере распространения данных на все большем количестве устройств и сред хранения возможность последовательного определения и применения политик становится все более важной. Symantec DLP предоставляет единую консоль управления DLP Enforce Platform, которая позволяет один раз написать политики и затем применять их повсеместно – по всем каналам потери данных.

С помощью платформы DLP Enforce Platform:

- Используйте единую веб-консоль для создания политик защиты от потери данных, устранения инцидентов и системного администрирования всех конечных точек, мобильных устройств, облачных сервисов, а также локальных сетей и систем хранения данных.
- Воспользуйтесь более чем 70 готовыми шаблонами политик и удобным конструктором политик, чтобы быстро запустить систему в работу.
- Используйте надежные функции управления рабочими процессами и устранения последствий для оптимизации и автоматизации процессов реагирования на инциденты в средах с высокой проходимостью.
- Применяйте бизнес-аналитику для снижения рисков с помощью сложного аналитического инструмента – Symantec IT Analytics for DLP, который предоставляет расширенные возможности отчетности и специального анализа.

Получите непревзойденную видимость конфиденциальных данных

Основой любого DLP-решения является обнаружение с учетом содержимого. Методы обнаружения с учетом содержимого позволяют находить конфиденциальные данные, хранящиеся практически в любом месте и в любом формате файлов. Symantec DLP предлагает наиболее полное обнаружение с помощью передовых технологий машинного обучения, распознавания образов, отпечатков пальцев и описания, которые точно классифицируют данные, позволяя не беспокоиться о ложных срабатываниях и воздействии на бизнес-пользователей.



- Функция **Described Content Matching** обнаруживает содержимое путем поиска совпадений по определенным ключевым словам, регулярным выражениям или шаблонам, а также свойствам файлов. Symantec DLP предоставляет более 130 идентификаторов данных, которые представляют собой предварительно заданные алгоритмы, сочетающие в себе сопоставление шаблонов и встроенные интеллектуальные средства для предотвращения ложных срабатываний.
- **Точное сопоставление данных** позволяет обнаруживать данные по "отпечаткам пальцев" или индексировать структурированные источники данных, такие как базы данных, серверы каталогов и другие структурированные файлы данных.
- **Индексированное сопоставление документов** применяется для обнаружения данных, хранящихся в неструктурированных документах, включая документы Microsoft Office, PDF-файлы и двоичные файлы, такие как JPEG, CAD-проекты и мультимедийные файлы. IDM также обнаруживает "производное" содержимое, например текст, скопированный из исходного документа в другой файл.

• **Sensitive Image Recognition** (поставляется с DLP Core) обнаруживает текст, внедренный в такие изображения, как отсканированные формы, документы, скриншоты, фотографии и PDF-файлы, используя запатентованную технологию распознавания форм и встроенный механизм оптического распознавания символов (OCR).

• **Vector Machine Learning** защищает интеллектуальную собственность с нюансами, которые редко встречаются или трудно поддаются описанию, например финансовые отчеты и исходный код. В отличие от других технологий обнаружения, Vector Machine Learning не требует поиска, описания или снятия отпечатков пальцев с данных, которые необходимо защитить.

Symantec DLP также предлагает богатый набор готовых и дополнительных API-интерфейсов, которые позволяют настраивать и интегрировать с широким спектром сторонних продуктов безопасности, облачных и собственных приложений: DLP REST API, DLP FlexResponse API, DLP Content Extraction API, DLP Incident Reporting and Update API и DLP API Detection Virtual Appliance.

Расширение защиты данных за пределы DLP

При передаче конфиденциальных данных внешним пользователям или их перемещении в облако за пределы управляемой среды они становятся уязвимыми для нежелательного воздействия. Решение обеспечивает комплексную защиту данных на протяжении всего их жизненного цикла за пределами управляемой среды с помощью политик безопасности доступа к облаку, классификации,шифрования, пользовательской аналитики и веб-шлюзов.

• **Распространение политик DLP на облачные приложения**: Распространение обнаружения, политик и рабочих процессов DLP на облачные приложения благодаря интеграции с Symantec CloudSOC (CASB) и управление инцидентами на единой консоли.

• **Упрощение процесса устранения инцидентов и управления политиками**: Сокращение времени и усилий на устранение последствий инцидентов и управление политиками, а также снижение рисков для данных благодаря Symantec Information Centric Analytics (ICA) – аналитике поведения пользователей и объектов, входящей в состав DLP Core.

• **Более безопасный обмен данными с другими пользователями**: Предотвращение несанкционированного доступа к конфиденциальным данным с помощью строгой аутентификации при обмене данными с бизнес-партнерами с помощью Symantec VIP Identity and Access Management.

• **Предотвращение попадания данных на нежелательные сайты**: Обеспечение защиты конфиденциальных данных от утечки по недоверенному веб-трафику, даже зашифрованному, благодаря интеграции DLP с защищенными веб-шлюзами Symantec: Symantec ProxySG и Web Security Service.

• **Интеграция с Microsoft Information Protection (MIP)**: Symantec DLP интегрирована с широкими возможностями классификации и шифрования, предоставляемыми MIP. Это решение дает заказчикам возможность обнаруживать и читать документы и электронные письма, защищенные с помощью MIP.

Системные требования

DLP-решение Symantec состоит из единой унифицированной платформы управления, легкого агента для конечных точек и мощных продуктов для обнаружения контента. Предлагаем максимальную гибкость развертывания благодаря широкому спектру вариантов для любого типа среды: программное обеспечение для локальных сетей, виртуальные и физические устройства, публичные, частные и гибридные облачные сервисы, а также управляемые услуги, предоставляемые партнерами Symantec. В отличие от других решений, Symantec DLP доказала свою способность работать в высокораспределенных средах и масштабироваться до сотен тысяч пользователей.

Полные системные требования Symantec Data Loss Prevention можно найти на странице поддержки.

Начните защищать свою информацию уже сегодня

Symantec готова помочь вам расширить границы безопасности и соблюдения нормативных требований за пределы межсетевого экрана, чтобы вы могли более полно и эффективно обнаруживать, контролировать и защищать свою информацию. Это решение предлагает самую низкую совокупную стоимость владения благодаря проверенным методологиям развертывания, интуитивно понятным средствам управления политиками и инцидентами, а также комплексному охвату всех каналов с высокой степенью риска.

Откройте для себя преимущества комплексного решения для защиты информации, созданного для современного мобильного и облачного мира.