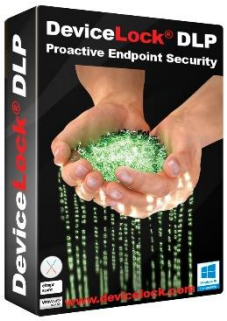


Контроль сетевых коммуникаций.

DeviceLock DLP как гибридная DLP-система с одновременным контролем сетевого трафика endpoint-агентом DeviceLock и сервером мониторинга трафика EtherSensor.

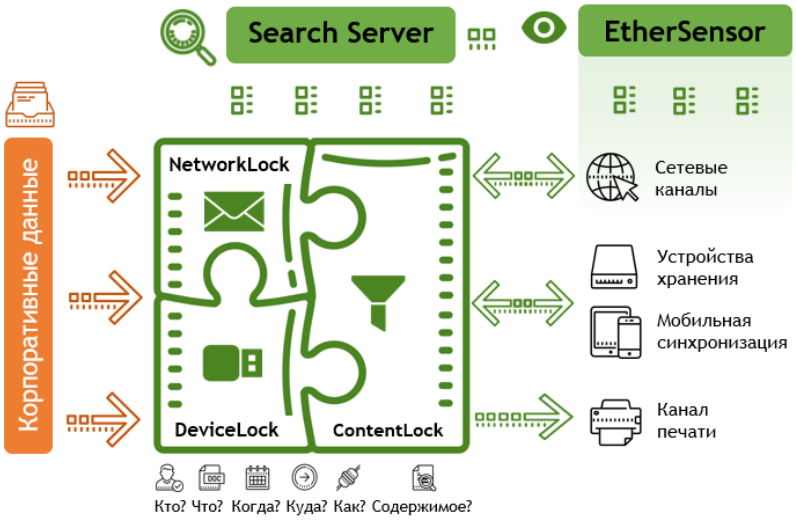
Программный комплекс **DeviceLock DLP** предлагает разработанный для предотвращения утечек данных из корпоративных ИС полнофункциональный набор контекстных и контентно-зависимых механизмов контроля **используемых**, **передаваемых** и **хранимых** данных, основанный как на базе полнофункциональных агентов на защищаемых рабочих станциях, так и сервера мониторинга сетевого трафика.

Совместное использование **агентов** DeviceLock DLP, обеспечивающих полнофункциональный DLP-контроль на защищаемых рабочих станциях, и сервера мониторинга сетевого трафика **DeviceLock EtherSensor**, позволяет построить гибридную DLP-систему в организации любого масштаба.

Гибридная DLP-система эффективно решает сразу несколько проблем и задач, стоящих перед службами информационной безопасности – мониторинга сетевого трафика с компьютеров и мобильных устройств, на которых по техническим причинам невозможно установить или эксплуатировать DLP-агент, либо снижения нагрузки на рабочие станции пользователей за счет раздельного контроля различных сетевых сервисов и протоколов на разных уровнях.

Автоматическое переключение различных DLP-политик для контроля сетевых коммуникаций в агенте DeviceLock DLP в зависимости от наличия подключения к корпоративной сети и/или корпоративным серверам позволяет обеспечить чрезвычайно гибкий контроль пользователей, когда, например, при нахождении ноутбука в офисе агентский контроль применяется для устройств, принтеров и особо критичных сетевых приложений и сервисов, в том числе с применением контентной фильтрации в режиме реального времени, а контроль и инспекция других сетевых протоколов и сервисов возлагается на сервер EtherSensor.

Единая база данных событийного протоколирования и теневого копирования, наполняемая событиями и данными, полученными при перехвате трафика с уровня сети и в результате контроля сетевых коммуникаций и устройств на рабочих станциях, позволяет выявлять инциденты информационной безопасности для широчайшего спектра потенциальных каналов утечки данных.



Компонент **NetworkLock** в составе агента DeviceLock
Агентский полнофункциональный контроль сетевого трафика

Компонент **NetworkLock** обеспечивает контекстный контроль каналов сетевых коммуникаций, событийное протоколирование, теневое копирование передаваемых файлов, данных и сообщений, тревожные оповещения (алертинг), а также реализует такие функции, как Белый список сетевых протоколов, Basic IP Firewall и др.

Контролируемые коммуникаций :сетевые протоколы и приложения, включая популярные почтовые платформы, сервисы веб-почты, мессенджеры, облачные файлообменные сервисы и социальные сети, поисковые системы, веб-доступ из стандартных браузеров и Tor Browser, Telnet-сессии а также передачу файлов по протоколам SMB, HTTP/HTTPS, FTP/FTPS и Torrent.

Агент DeviceLock – единственный на мировом рынке агент класса endpoint DLP со встроенным резидентным модулем, реализующим **технологию глубокого анализа и фильтрации сетевых пакетов** (deep packet inspection, DPI) непосредственно на защищаемом компьютере. С помощью DPI агентский компонент NetworkLock осуществляет универсальный, независимый от типов сетевых приложений и веб-браузеров, контроль пользовательских коммуникаций для большинства подверженных утечкам Интернет-протоколов и приложений, включая SMTP, SMTP over SSL/TLS, HTTP/HTTPS, FTP/FTPS, WebDAV, Telnet, а также P2P-передачу файлов в сетях Torrent. DPI-технология позволяет NetworkLock распознавать, перехватывать и инспектировать в реальном времени трафик контролируемых сетевых протоколов и приложений вне зависимости от используемых ими сетевых портов и SSL/TLS-туннелирования. Реконструируя перехваченные сессии и детектируя их контекстные параметры, NetworkLock контролирует, от кого (с чьей учетной записи), кому (идентификатор получателя) и куда (социальная сеть, файлообменник...) передаются данные, каков их тип (почтовое, сообщение, сессия чата, файл, веб-форма...), как они передаются (по электронной почте, мессенджером, при вэб-доступе...) и когда (время, дни недели...). Кроме того, анализируя перехваченные сессии, NetworkLock способен выделять передаваемые в них сообщения, файлы и иные объекты данных, которые могут быть направлены в ContentLock для оперативного контентного анализа и фильтрации.

Deep Packet Inspection в компоненте NetworkLock

DeviceLock **EtherSensor**
Серверный мониторинг сетевого трафика

Серверный модуль DeviceLock EtherSensor, автономный продукт в составе программного комплекса DeviceLock DLP Suite, позволяет организациям обеспечить всеобъемлющий мониторинг сетевого трафика, работая при этом на серийном серверном оборудовании или в виртуальной среде на ОС Windows с низкими системными требованиями для анализа больших потоков данных (гигабиты в секунду без потери пакетов).

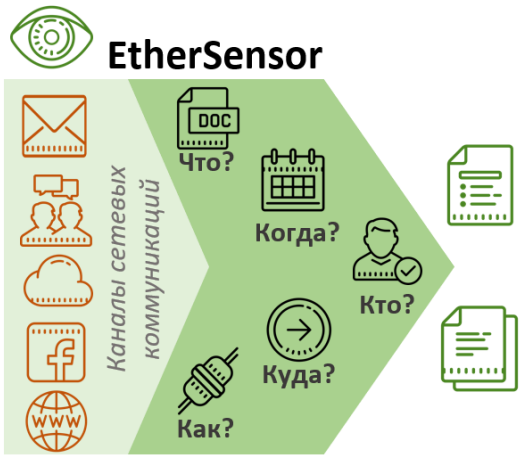
Сервер EtherSensor позволяет протоколировать сетевые события и передаваемые по сети сообщения и файлы, не задействуя при этом агенты DeviceLock, в целях мониторинга внутрикорпоративной и внешней электронной почты (включая входящую почту), веб-почты, социальных сетей, широкого ряда мессенджеров, сервисов поиска работы, форумов и блогов. Также перехватываются и протоколируются передача файлов по протоколам HTTP, FTP и в облачные хранилища. Перехваченные события, файлы и данные сохраняются в централизованной базе данных DeviceLock DLP для последующего хранения и анализа, включая возможности полнотекстового поиска с помощью DeviceLock Search Server.

Как работает сервер DeviceLock EtherSensor

Сервер DeviceLock EtherSensor выполняет три задачи:

- перехват зеркалированного сетевого трафика канального уровня;
- анализ перехваченного (зеркалированного) трафика для извлечения из него полезных объектов уровня приложения (объекты, их контент, события и т.д.);
- сохранение результатов анализа в базе данных сервера DeviceLock Enterprise Server.

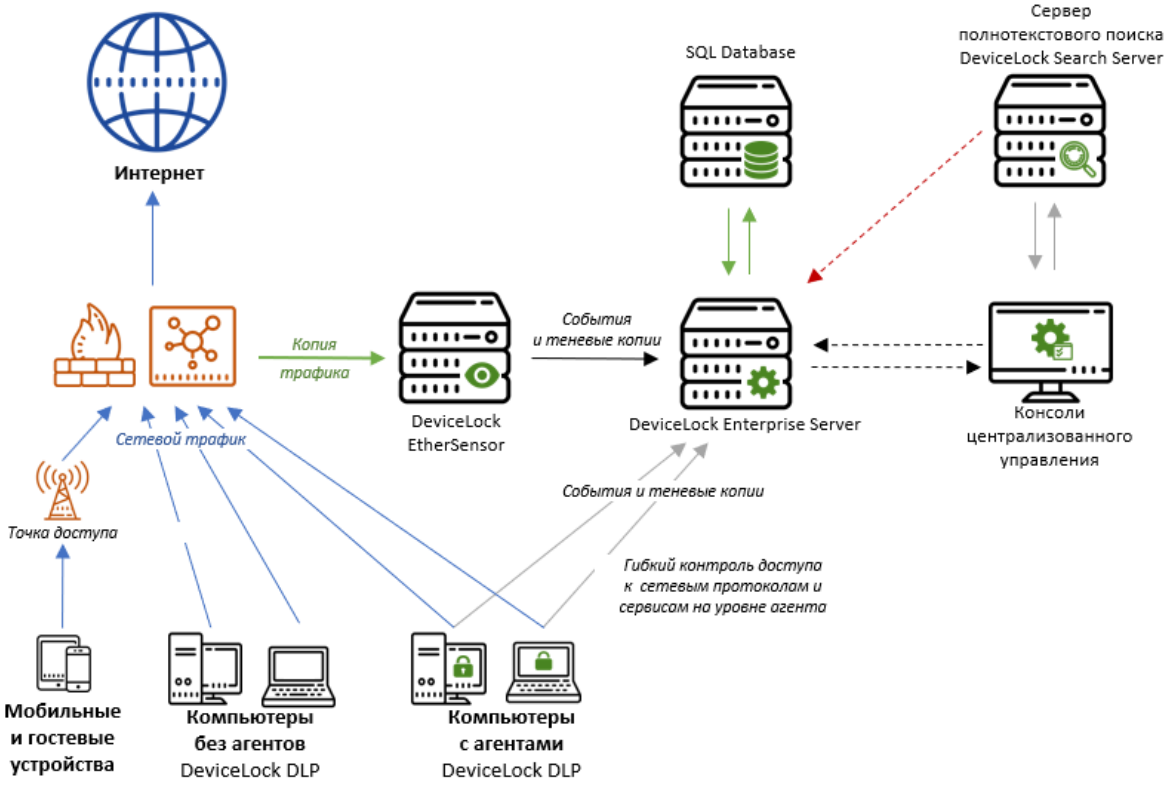
EtherSensor функционирует без использования агентов DeviceLock, устанавливаемых на рабочих станциях для реализации других функций DLP-контроля. Высокая производительность EtherSensor позволяет использовать серийное серверное оборудование или среду виртуализации для анализа больших потоков данных (гигабиты в секунду без потери пакетов) при достаточно низких системных требованиях.



EtherSensor работает в пассивном режиме получения сетевого трафика, следовательно, никак не воздействует на сетевую инфраструктуру и не требует ее изменения, кроме необходимости отведения копии сетевого трафика с помощью зеркалирования трафика или сетевого ответвителя на EtherSensor.

EtherSensor может получать сетевой трафик одновременно из нескольких источников следующих типов: зеркальные порты (Mirror ports), сетевые ответвители (Network taps), ICAP-клиенты, PCAP и PcapNG файлы.

Перехваченные данные сохраняются в централизованном архиве сервера DeviceLock Enterprise Server для последующего хранения и анализа, включая возможности полнотекстового поиска с помощью DeviceLock Search Server.



Источники данных для EtherSensor

1. Сетевые интерфейсы физического или виртуального сервера EtherSensor подключаются к Mirror-порту (SPAN, rx и tx пакеты) для прослушивания трафика с критичных устройств или целых сегментов сети. Аналогично настраивается интеграция с решениями класса NGFW, способными расшифровывать SSL/TLS (PaloAlto Networks, FortiGate, и т.д.), когда копия расшифрованного SSL-трафика направляется на сетевой интерфейс EtherSensor для анализа.
2. Прокси-серверы при условии ICAP-интеграции, имеющие возможность расшифровки HTTPS-трафика и передачи результатов по ICAP в EtherSensor (Blue Coat SG, Cisco WSA, SQUID и т.д).
3. PCAP-файлы на файловой системе. EtherSensor периодически опрашивает каталог на предмет появления новых PCAP-файлов с записанным трафиком. При обнаружении такие файлы немедленно обрабатываются и анализируются EtherSensor.
4. Lotus Notes Transaction Log для получения всех сообщений, проходящих через почтовую систему IBM (Lotus) Notes. Также производится обнаружение почтовых сообщений Lotus Notes в обрабатываемом трафике.
5. Плагин для сервера Microsoft Skype for Business (Lync) с ролью Edge, отправляющий копию переписки на сервер EtherSensor.

Сервер EtherSensor реконструирует и анализирует объекты трафика, начиная с уровня 2 модели OSI и до уровня 7 – объекты, специфические для определённого приложения, пользователя и Интернет-сервиса, при этом число поддерживаемых сервисов превышает несколько тысяч. Полученные в результате перехвата данные проходят предварительную фильтрацию с целью исключения заведомо неинтересного или мусорного трафика с использованием технологии Berkeley Packet Filter (BPF), которая позволяет предоставлять для дальнейшего анализа данные именно из тех сегментов сети, которые востребованы службой ИБ.

Расшифровка **SSL/TLS** трафика

Для решения задачи анализа SSL/TLS трафика EtherSensor может использовать программный компонент **SSLSplitter** или стороннее решение, имеющее функцию расшифровки SSL, например, методом MITM. Кроме того, встроенный ICAP-сервер позволяет серверу EtherSensor взаимодействовать с ICAP-клиентами, обрабатывающими HTTPS-трафик.

SSLSplitter устанавливается “в разрыв” сети на периметре организации, функционируя на физическом или виртуальном сервере. SSLSplitter работает по принципу подмены сертификатов (Man-In-The-Middle). SSL-соединения определяются не по порту назначения соединения, а с использованием сигнатур. SSLSplitter может работать в режиме Bridge (L2 сетевой модели OSI) и в режиме Router (L3 сетевой модели OSI), что значительно упрощает интеграцию в любую сетевую архитектуру. При любой схеме включения SSLSplitter предусматривает отказоустойчивость и балансировку нагрузки, что значительно повышает его надежность и масштабируемость.

Решаемые задачи:

- расшифровка данных, передаваемых по любым протоколам с использованием SSL-шифрования, среди которых:
  - веб-трафик (протокол HTTPS);
  - корпоративная и внешняя электронная почта (IMAP4S, SMTPS, POP3S, NRPC);
  - мессенджеры (протоколы Skype, XMPP, OSCAR, MRA, IRC);
  - передача файлов и облачные сервисы (Google Drive, Яндекс.Диск, iCloud, файлообменники, CRM, FTPS, WebDAV);
  - VPN-подключения, SIP, приложения для удаленного управления компьютером;
- отказоустойчивость, масштабирование, балансировка нагрузки;
- работа в прозрачном или полупрозрачном режиме.

Контролируемые сетевые коммуникации

Входящая и исходящая веб-почта: выделение из зеркалированного трафика входящих и исходящих сообщений служб веб-почты: Mail.RU, Yandex.RU, Pochta.RU, GMail и т.п.(40+ доменов), а также сервисов на популярных webmail-движках.

Электронная почта: выделение из зеркалированного трафика сообщений электронной почты, передаваемых по протоколам SMTP, POP3 и IMAP4.

Социальные сети: выделение из зеркалированного трафика сообщений разных типов (авторизация, сообщения, комментарии и т.п.) в социальных сетях и на форумах: Facebook, LinkedIn, Vk.com, Odnoklassniki, Mamba.ru, phpbb, ipb, vbulletin, mybb, а также SMS/MMS-сообщения пользователей, отправляемые через специализированные веб-сервисы (500+ доменов).

Протоколы и службы передачи файлов: выделение из зеркалированного трафика файлов, передаваемых по протоколам HTTP, FTP, SMB/CIFS и WebDAV.

Сервисы мгновенных сообщений: выделение из зеркалированного трафика сообщений, отправляемых и получаемых через службы мгновенных сообщений, работающие по протоколам IRC, MSN, XMPP/Jabber, MRA, YAHOO и OSCAR (ICQ, Skype, Google Hangout, Mail.ru Агент и т.п.).

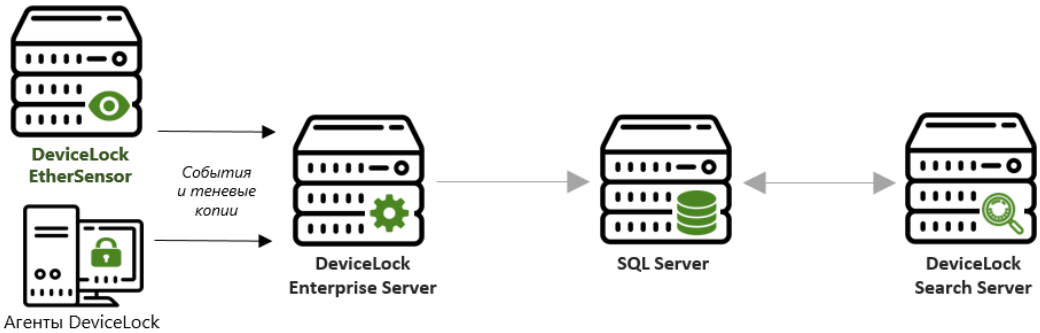
Сервисы поиска работы: выделение из зеркалированного трафика сообщений, вакансий, откликов и других событий сервисов вакансий и поиска работы, таких как HH.ru, SuperJob.ru, Job.ru и т.п. (150+ доменов).

Почтовая служба IBM (Lotus) Notes: выделение из зеркалированного трафика сообщений системы Lotus Notes (сейчас IBM Notes). В случае, если применяется шифрование трафика, сообщения могут извлекаться из Lotus Notes Transaction Log (данный метод никак не влияет на работу Lotus Notes).

Что понадобится для работы EtherSensor?

Для установки DeviceLock EtherSensor понадобится сервер с установленной ОС Microsoft Windows (Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016). Настоятельно рекомендуется наличие установленных последних обновлений. EtherSensor может использоваться в среде виртуализации. Для обработки сетевого трафика на скоростях 10Гб/с рекомендуется сервер со следующими характеристиками: 2 CPU x 10 Cores, 128 Гб ОЗУ, 6x500 GB SSD RAID10, 4 x 10Gbps. Для обработки трафика на меньших потоках требования существенно ниже.

Поскольку перехваченные данные сохраняются в базе данных в DeviceLock DLP для последующего хранения и анализа, для направления полученных сервером EtherSensor событий и данных в архив требуется предварительная установка и настройка сервера **DeviceLock Enterprise Server** и связанной СУБД MS SQL.



В комплект поставки модуля DeviceLock EtherSensor также входит программное решение **EtherStat**, предназначенное для анализа сетевой статистики, полученной от сервера EtherSensor. **EtherStat** позволяет строить отчеты различной сложности о сетевых событиях с использованием фильтров в ручном и автоматическом режимах, объединяя полученную от EtherSensor статистику с информацией о пользователях EtherStat и их устройствах, участвующих в сетевых соединениях.

Примеры использования гибридной DLP-архитектуры

1. Мониторинг сетевых коммуникаций при недопустимости блокировки передачи данных по сети.

В некоторых организациях задача контроля сетевого трафика ограничивается протоколированием и анализом архива перехваченных данных вследствие ряда факторов. Например, для реализации полноценного DLP-контроля с блокировкой утечки данных ограниченного доступа недостаточно ресурсов службы ИБ, или пассивный контроль определен руководством компании как достаточный вследствие уже введенных ограничений на использование сетевых коммуникаций в целом на уровне сетевого периметра, или руководство опасается риска вмешательства в выстроенные бизнес-процессы с сетевым обменом информацией. Известны случаи, когда организация не оценивает риски утечки данных как критичные для бизнеса, или, наконец, нет возможности классифицировать конфиденциальные данные либо определить критерии детектирования данных ограниченного доступа для применения механизмов контентной фильтрации и предотвращения утечки таких данных.

В таком сценарии организация получает в свое распоряжение традиционную DLP-систему Enterprise-уровня, способную отслеживать и анализировать трафик на очень больших потоках (вплоть до анализа трафика от сотен тысяч сотрудников) с низкими затратами на развертывание и текущую эксплуатацию, а также незначительными требованиями по техническому оснащению. Решение в данном сценарии полностью соответствует предыдущему сценарию, но с той разницей, что при появлении необходимости обеспечить блокировку недопустимых попыток передачи данных ограниченного доступа, либо появляется понимание критериев выявления конфиденциальных данных и возможность использования контентной фильтрации. В таком случае данный сценарий перетекает уже в другую вариацию – применения полноценной гибридной DLP-системы для отдельных сотрудников, подразделений или в масштабах всей организации.

2. Раздельный контроль сетевых коммуникаций в зависимости от подключения к корпоративной сети.

В зависимости от текущего статуса подключения к корпоративной сети (доступность локального сетевого подключения, доступность контроллера домена, доступность DLP-сервера) может варьироваться степень актуальности доступа к корпоративной информации, а следовательно, необходим гибкий подход к реализации защиты информации от утечек. Автоматическое переключение различных комбинаций DLP-политик для контроля сетевого трафика (различных комбинаций правил и параметров контроля) в агенте DeviceLock DLP в зависимости от наличия подключения к корпоративной сети и/или корпоративным серверам позволяет обеспечить чрезвычайно гибкий, раздельный контроль сетевых коммуникаций пользователей, когда, например, на уровне агента при нахождении лэптопа в офисе сохраняется контроль особо критичных сетевых приложений и сервисов, в том числе с применением контентной фильтрации в режиме реального времени в целях предотвращения утечки конфиденциальной информации, а инспекция других сетевых протоколов и сервисов возлагается на модуль EtherSensor. При переключении агента DeviceLock на защищаемой рабочей станции в режим offline происходит автоматическое переключение политик на максимально необходимый уровень контроля сетевых коммуникаций с учетом возможной недоступности исходящего сетевого трафика с рабочей станции для сервера EtherSensor.

В результате раздельного контроля с применением автоматического переключения online и offline режимов в агенте DeviceLock с мониторингом трафика на уровне сервера EtherSensor достигается полноценный контроль сетевых коммуникаций вне зависимости от местонахождения и способа подключения к сети Интернет контролируемых компьютеров. Такой подход будет особенно продуктивным в решении задачи контроля мобильных сотрудников, использующих ноутбуки и лэптопы для работы вне офиса.

Примеры использования гибридной DLP-архитектуры

3. Селективный контроль по типам сетевых коммуникаций.

Селективный контроль сетевых коммуникаций, когда благодаря совместному использованию функциональности endpoint-агента и технологий серверного перехвата сетевого трафика достигается извлечение всей полноты возможностей гибридной системы, является наиболее мощным сценарием контроля сетевых коммуникаций из всех возможных на сегодня.
В таком сценарии наиболее критическая часть сетевых приложений, рассматриваемых как потенциальные каналы утечки конфиденциальных данных (например, мессенджеры с возможностью передачи файлов), равно как и локальные порты и устройства, контролируются агентом DeviceLock. Процессы передачи данных ограниченного доступа (также на уровне агента, «в разрыв») подвергаются в режиме реального времени анализу содержимого с принятием решений о допустимости передачи, либо о создании теневой копии для значимых для целей расследования инцидентов, либо о направлении тревожного оповещения по факту срабатывания DLP-правила. Контроль прочих сетевых коммуникаций, рассматриваемых как имеющие меньшую степень риска с точки зрения противодействия утечки данным (когда для решения задач информационной безопасности достаточно мониторинга и анализа переданных данных, например, для серфинга веб-сайтов и сервисов поиска работы) выполняется сервером EtherSensor посредством перехвата и анализа сетевого трафика на уровне периметра. Кратко говоря, данную модель контроля сетевого трафика можно описать как «Мониторинг всего трафика (EtherSensor) + Селективная блокировка недопустимых попыток (агент DeviceLock DLP)». Что важно, политики включения или отмены блокировки любых сетевых протоколов и сервисов как на уровне контекста, так в контентно-зависимых правилах, могут быть изменены и применены службой ИБ в любое время без перезагрузки пользовательских рабочих станций и без участия пользователя.

В таком сценарии достигается качественный баланс возможностей и рисков: риски, связанные с блокировкой, делегируются агентам на защищаемых компьютерах, при этом задачи мониторинга сетевого трафика и детектирования событий безопасности по всей сети в целом поручаются серверу EtherSensor.

4. Избирательный контроль пользователей и компьютеров.

Данный вариант использования гибридной DLP-системы является логическим расширением и продолжением сценария, предполагающего селективный контроль в зависимости от типа используемых сетевых коммуникаций. Здесь помимо возможностей разделения уровней контроля (мониторинга и блокирования передачи данных) между агентом и сервером DLP-системы DeviceLock DLP, добавляется избирательный подход для различных пользователей и групп пользователей, либо для разных компьютеров и групп компьютеров.

В данном сценарии полнофункциональные агенты DeviceLock выполняют непосредственно и только на защищаемых рабочих станциях все DLP-функции (контроль доступа, протоколирование, тревожные оповещения) и только для указанных пользователей и групп пользователей. Сетевая активность пользователей и групп, которым для выполнения бизнес-задач требуется свободный доступ к различным каналам сетевых коммуникаций, отслеживается сервером EtherSensor посредством перехвата и анализа сетевого трафика на уровне периметра.

Данный сценарий также является крайне продуктивным для контроля так называемых групп риска, когда на агентах DeviceLock создаются специальные наборы политик для DLP-контроля различных учетных записей, а переключение применяемых политик выполняется в реальном времени путем включения таких пользователей в группу пользователей, соответствующих той или иной группе риска.

АО «Смарт Лайн Инк»
107023, г. Москва,
Семеновская Малая ул., д.9, стр. 14Б, 2 эт.
www.devicelock.ru
Телефон отдела продаж
+7 495 647 99 37
E-mail: ru.sales@devicelock.com