Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

ОПИСАНИЕ ПРОДУКТА

Программный блейд DLP является единственным решением, которое сочетает технологии и процессы для предотвращения потерь данных, что позволяет компаниям предотвращать потери данных благодаря упреждающей защите конфиденциальной информации от непреднамеренной потери.

Программный блейд DLP

НАША ЗАДАЧА

Хотя во всем мире и растет число случаев потерь данных, у компаний небольшой выбор возможностей по защите конфиденциальных данных. Конфиденциальные данные сотрудников и клиентов, юридические документы и интеллектуальная собственность подвержены потере. Компании пытаются эффективно решить задачу защиты данных, и избежать при этим снижения производительности сотрудников и избыточной нагрузки на IT-персонал. Технологиии развиваются, но, в конечном счете, они неэффективны в понимании намерений пользователей. Кроме того, защита конфиденциальных данных редко обходится без длительного внедрения, тяжелого администрирования и высокой стоимости, связанных с традиционными продуктами DLP.

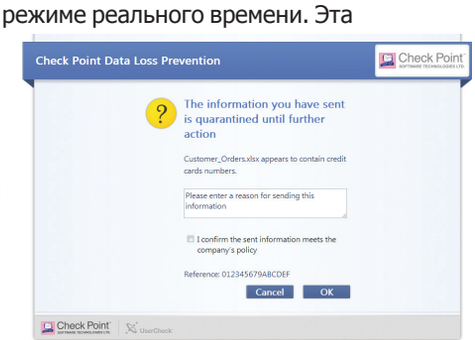
ОБЗОР

Компания Check Point предлагает революционно новый подход в DLP путем объединения технологий и процессов для перехода от пассивного обнаружения к активному Предупреждению Потери Данных. Инновационная система MultiSpect™ представляет собой механизм классификации данных, сочетающий в себе информацию о пользователе, типе данных и процессах для принятия верных решений, в то время как новая технология UserCheck™ позволяет пользователям устранять инциденты информационной безопасности в режиме реального времени. Сетевое решение Check Point DLP способствует высвобождению IT-персонала и сотрудников отдела безопасности от задач обработки инцидентов и обучает пользователей корпоративным правилам работы с информацией, предотвращая тем самым как преднамеренные, так и непреднамеренные потери данных.

Check Point UserCheck™

Check Point UserCheck позволяет пользователям устранять инциденты информационной безопасности в режиме реального времени. Эта инновационная технология уведомляет пользователей о предполагаемых нарушениях режима безопасности, позволяет оперативно устранить возникшее нарушение и не допустить утечки данных.

UserCheck дает возможность пользователям самостоятельно устранять инциденты информационной безопасности,



UserCheck позволяет пользователям устранять инциденты информационной безопасности в режиме реального времени.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- **Защита от потерь критически важной информации**
  Новая технология UserCheck позволяет пользователям устранять инциденты информационной безопасности в режиме реального времени
- **Интеграция технологий и процессов для обеспечения предотвращения потерь данных**
  Инновационная система MultiSpect представляет собой механизм классификации данных, сочетающий в себе информацию о пользователях, типах данных и процессах, что обеспечивает непревзойденную точность
- **Простое развертывание для немедленного предотвращения потери данных**
  Защита конфиденциальной информации обеспечивается с первого дня установки благодаря предустановленным политикам безопасности и поддержке широкого спектра файловых форматов и типов данных

СВОЙСТВА ПРОДУКТА

- Check Point UserCheck
- Check Point MultiSpect
- Комплексная защита
- Централизованное управление политиками безопасности
- Быстрое и удобное развертывание
- Контрольная сумма важных файлов
- Рекомендательный список файлов
- Добавление зашифрованных скрытых водяных знаков
- Гибкий выбор видимых водяных знаков в документах Microsoft Office

с возможностью отправки, отмены или пересмотра случившегося события, что позволяет повысить защищенность за счет повышения уровня знаний о корпоративных правилах работы с информацией. Уведомление о возможном нарушении режима безопасности приходит пользователю в режиме реального времени в виде всплывающего сообщения или электронного письма (не требует установки клиентского ПО). От этого организации выигрывают в нескольких направлениях:

- Полное предотвращение потери данных — позволяет перейти от обнаружения к предотвращению
- Система самообучения пользователей — способствует освобождению IT-персонала и сотрудников отдела безопасности от задач обработки инцидентов и обучает пользователей корпоративным правилам работы с информацией

Check Point MultiSpect™

Инновационная система MultiSpect представляет собой многофакторный механизм классификации данных — связей между пользователями, типами данных и процессами. Check Point DLP с исключительно высокой точностью проводит идентификацию уязвимых данных, включая персональные данные (PII), данных, связанных с соответствием требованиям (HIPAA, SOX, PCI, и т. д.) и конфиденциальной коммерческой информации. Это достигается благодаря технологии MultiSpect, являющейся основой мощного трехуровневого механизма проверки:

- Классификация и корреляция данных на основе многих параметров
- Проверка и соблюдение требованиям для многих протоколов: проверка контента и внедрение политик безопасности в отношении большинства популярных протоколов TCP включая SMTP, FTP, HTTP, HTTPS и TLS, а также веб-почты и Microsoft Exchange
- Сопоставление с эталоном и классификация файлов с целью идентификации содержимого независимо от расширения, включая архивированные файлы
- Распознает и защищает конфиденциальные данные: сравнение по типу файла/форме на основе заранее заданных шаблонов
- Идентифицирует поведение, которое не соответствует этике бизнес-коммуникаций: способствует применению лучших мировых практик

Кроме того, для создания собственных типов данных имеется в распоряжении открытый язык сценариев. Эта уникальная гибкость обеспечивает практически неограниченную поддержку для защиты уязвимых данных.

Различные варианты внедрения

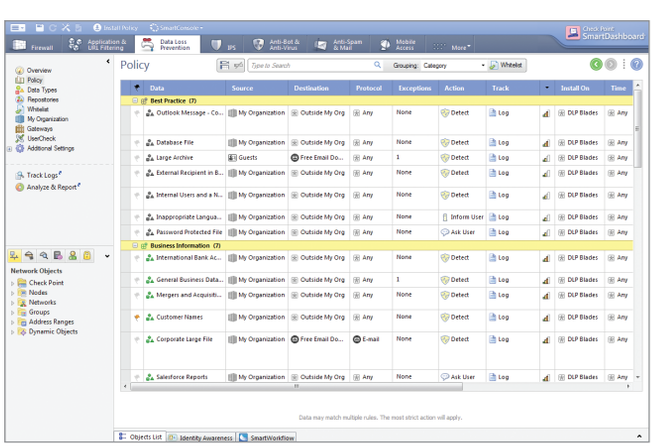
Решение Check Point DLP создано в виде нового программного блейда, который работает на любом имеющемся в наличии шлюзе Check Point. Программный блейд Check Point DLP — передовое решение для предотвращения потери данных, передаваемых по сетям, с поддержкой широкого спектра типов трафика, включая глубокие знания по защите протоколов SMTP, HTTP и FTP. В политиках безопасности DLP можно задать, что подлежит отслеживанию и как предотвратить инциденты, на уровне политики безопасности, сегмента сети, шлюза и группы пользователей.

Централизованное управление политиками безопасности

Security Management™ через удобный пользовательский интерфейс. Централизованное управление обеспечивает лучшие контроль и применение политик безопасности, дает возможность организациям использовать единое место хранения описаний пользователей и групп, сетевых объектов, прав доступа и политик безопасности во всей инфраструктуре безопасности. Унифицированные правила доступа автоматически применяются во всей распределенной среде, обеспечивая надежный доступ из любого места.

Развертывание единой политики безопасности на нескольких шлюзах позволяет вести контроль за действиями по применению каждой политики безопасности, то есть: Обнаружению (только регистрация) или Отправке в карантин (самостоятельное устранение инцидента). Управление политиками безопасности содержит следующие возможности:

- Выбор типа/типов данных и групп/группы пользователей — в том числе с использованием Active Directory
- Задание исключений — разрешенных пользователей
- Направление трафика — исходящего или трафика между сотрудниками департамента
- Предопределенные политики безопасности и типы данных по содержанию
- Дополнительные воздействия определенных политик безопасности на различные группы пользователей
- Интегрированные запись и корреляция событий
- Настройка внутреннего карантина
- Гранулированный контроль защиты — удобные в использовании профили защиты позволяют администраторам задавать сигнатуры и правила активации защиты в соответствии с потребностями защиты сетевых ресурсов
- Заданные по умолчанию и рекомендованные профили безопасности обеспечивают быстрые и готовые к использованию профили для оптимальной защиты или производительности



Легкое создание специализированных правил DLP для предотвращения потери данных.

Управление событиями

Извлечение иголки из стога сена — система SmartEvent в DLP позволяет вести мониторинг и отчетность только важных событий. Управление событиями содержит следующие возможности и опции:

- Представление данных в виде хронологических графиков и в режиме реального времени о событиях DLP
- Простая корреляция инцидентов
- График инцидентов по времени
- Легко настраиваемый интерфейс просмотра
- Управление событиями/инцидентами безопасности

Для получения дополнительной информации смотрите Программный блейд SmartEvent

Быстрое и гибкое развертывание

Организации любого размера будут защищены с первого же дня благодаря предварительно подготовленным шаблонам. Широкий спектр встроенных политик и правил безопасности, включая требования на соответствие, интеллектуальные права собственности, и санкционированное использование.

Программный блейд Check Point DLP можно установить на любой шлюз безопасности Check Point (на базе устройств Check Point или на открытые сервера). Легко и быстро разворачивается на существующих шлюзах безопасности Check Point, экономя время и средства, усиливая существующую инфраструктуру безопасности. Кроме того, для лучшего соответствия требованиям безопасности любой сети, имеется полный спектр мощных и высокомасштабируемых устройств DLP-1.

СПЕЦИФИКАЦИИ АППАРАТНЫХ УСТРОЙСТВ

Поддерживаемые семейства устройств	• Устройства Check Point 2200, 4000, 12000, 21000 и 61000 • Устройства Check Point IP • Устройство Check Point UTM-1 • Устройство Check Point IAS
Поддерживаемые операционные системы	• GAiA • SecurePlatform

ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ ПО

Программный блейд DLP — программное решение, на базе архитектуры «Программные блейды». Для установки блейда на открытые сервера, решение тестировалось на совместимость с большим числом аппаратных платформ. Для получения дополнительной информации смотрите список совместимого оборудования.

	Минимальные требования к оборудованию для установки программного блейда DLP	
Рекомендуемые требования к открытым серверам	До 1000 пользователей	До 5000 пользователей
Количество ядер CPU	2	8
Размер оперативной памяти	4GB	4GB
Емкость устройства хранения данных	250G	500G
Количество сетевых интерфейсов	2	2

ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ

	Контроль
Опции проверки	• Более 600 предопределенных типов данных по содержанию • По шаблону, соответствию ключевому слову и по словарю • Классификация и корреляция данных на основе многих параметров • Расширенный анализ, основанный на структурированном контенте • Сходство с широко используемыми шаблонами • Соответствие, основанное на атрибутах файла • Использование открытого языка сценариев для адаптации и создания особых типов данных
Типы файла	Проверка контента более 800 типов файлов
Протоколы	HTTP, HTTPS, TLS, SMTP, FTP
Соответствие нормативным документам	PCI-DSS, HIPAA, PII и другие
Типы данных, не связанные с требованиями регуляторов	• Данные интеллектуальной собственности • Финансовые и юридические термины • Национальные идентификационные номера • Международные номера банковских счетов (IBAN)
Многоязычная поддержка	Обнаружение по контенту на нескольких языках включая одно- и двух-байтовые шрифты (UTF-8)

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

	Принудительное применение
Типы	• Запрос пользователя (самостоятельное предотвращение при помощи UserCheck) — сообщение помещается в карантин, отправка уведомления пользователю, запрос самостоятельного восстановления • Предотвращение — блокирование отправки сообщения и оповещение пользователя • Обнаружение — регистрация инцидентов
UserCheck	• Включение и настройка политики с индивидуальным редактированием (многоязычного) уведомления конечному пользователю • Самообучение — предотвращает повторяющийся контроль происшествий в пределах одного почтового потока • Два метода уведомления — по электронной почте (не требуется инсталляция агента) или всплывающее окно в области пиктограмм панели задач (требуется инсталляция тонкого агента)
Возможности принудительного применения	• Политики исключения на пользователя, группы пользователей, сети, протокола или типа данных • Отправка уведомления о потенциальных нарушениях владельцу ресурсов данных (например, CFO для финансовых документов) • Регистрация всех инцидентов — с возможностью корреляции событий и аудита инцидентов
Обзор инцидентов	• Детализированные права администратора обеспечивают контроль над тем, кому доступны данные системы DLP • Можно замаскировать конфиденциальные данные в журналах регистрации событий DLP (например, отображены только последние четыре цифры номера кредитной карты) • Каждый раз при просмотре сообщения создается запись в файле регистрации
Регистрация всех почтовых сообщений	Все исходящие почтовые сообщения (включая те, которые не относятся к инцидентам) регистрируются по отправителю, получателю и теме
	Управление политиками
Централизованное управление	• Интеграция с панелью инструментов SmartCenter • Простое и интуитивно понятное создание политики • Простота создания типа содержания данных • Мощные опции классификации и поиска по типу содержания данных
Управление событиями	• Дополнительные встроенные функции в SmartEvent • Ведение журнала событий и график мониторинга в режиме реального времени • Круговая диаграмма с распределениями нарушений по пользователям или сетям
	Развертывание
Инсталляционные опции	• Программный блейд, работающий на всех шлюзах безопасности Check Point • Выделенное устройство
Опции развертывания по сети	• Встроенные подключения • Подключение к SPAN-порту или зеркальному порту 2-го уровня
Мастер инсталляции	Простой мастер, который на первом этапе помогает развернуть блейд DLP, обеспечить его связь с Active Directory и установить требуемые первоначальные настройки

АДРЕСА И ТЕЛЕФОНЫ CHECK POINT

Международная штаб-квартира
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: 972-3-753-4555 | Факс: 972-3-575-9256 | Эл. почта: info@checkpoint.com
Представительство в России и СНГ
Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николоямская, д. 13, стр. 17 | Тел./факс: +7 495 967 7444 | http://rus.checkpoint.com