DATA LOSS PREVENTION

защита от утечек информации

ZECURION

ZECURION

О КОМПАНИИ

Zecurion — первый российский разработчик систем защиты информации от внутренних угроз. DLP-продукты Zecurion позволяют минимизировать риски умышленной и случайной утечки корпоративной информации.

Компания Zecurion более 10 лет профессионально занимается вопросами информационной безопасности. С 2001 года Zecurion является лидером в области шифрования данных, а с 2005 года разрабатывает инновационные решения для защиты от утечек информации. Среди современных продуктов, представленных на рынке DLP, решения Zecurion признаны самыми технологичными (по версии аналитического центра Anti-Malware.ru). По оценке CNews Analytics за 2011 год компания Zecurion вошла в число 30 крупнейших ИТ-компаний России в сфере защиты информации, заняв первое место среди разработчиков DLP. В 2012 году компания провела ребрендинг, прекратив использование старого названия SECURIT.

Линейка продуктов Zecurion реализует полный спектр защиты информации от инсайдеров: контроль всех потенциальных каналов утечки, ведение архива действий сотрудников, защиту данных в процессе использования и хранения, а также управление доступом пользователей к корпоративной сети, приложениям и конфиденциальной информации. Использование DLP-решений компании обеспечивает комплексную защиту информации от утечек на протяжении всего ее жизненного цикла — от создания до записи в архив или удаления. Благодаря инновационным подходам и ориентированности решений на требования бизнеса комплексные системы Zecurion на текущий момент используются более чем в 7000 организаций. Компанию Zecurion поддерживают более 100 бизнес-партнеров из различных регионов России и СНГ, стран Азии и Тихоокеанского региона, Европы и США.

ZECURION

ЧТО ТАКОЕ DLP?

DLP расшифровывается как Data Loss Prevention и используется для обозначения продуктов и систем для защиты от утечек информации.

DLP-системы направлены на минимизацию рисков внутренних угроз информационной безопасности, или, иными словами, на защиту корпоративной информации от инсайдеров. Инсайдерами являются абсолютно все сотрудники компании, ведь утечки могут происходить не только по злому умыслу, но и по невнимательности сотрудников или незнанию правил информационной безопасности. Более того, согласно статистике, свыше 80 % зарегистрированных инцидентов приходится именно на случайные утечки. Впрочем, настоящая DLP-система предусматривает все возможные сценарии и защищает как от случайных утечек, так и от намеренной кражи информации сотрудниками.

Существует множество подходов к классификации DLP-систем, однако более-менее устоявшиеся представления рынка указывают на несколько характеристик, позволяющих относить ИТ-решения к классу DLP.

Тотальный контроль каналов утечки

Потенциальные каналы утечки информации составляют большие группы: сетевые каналы (к ним относится электронная почта, интернет-пейджеры, интерактивные веб-сайты, блоги, форумы и т. п.) и локальные (принтеры, съемные накопители, а также любые периферийные устройства, на которые можно скопировать конфиденциальную информацию). Для контроля этих каналов применяются соответственно сетевые и агентские DLP-системы. К ним также примыкает традиционно обособленная защита хранимых данных, которые подвержены рискам утечки при попадании физического носителя (жесткого диска, магнитной ленты, сервера или ПК) в руки злоумышленника.

Анализ информации

DLP-системы перехватывают весь трафик, выходящий за пределы корпоративной сети предприятий, и анализируют его на предмет наличия в нем конфиденциальной информации. Существует более десятка типов данных, обнаружить которые можно только с помощью различных специализированных технологий детектирования.

Блокирование утечек

На основании данных анализа DLP-система принимает решение согласно установленным политикам безопасности о разрешении или запрете передачи сообщения, записи или печати файла.

Архивирование информации

Весь перехватываемый трафик DLP-система помещает в собственный архив, который создает полноценную базу для расследования инцидентов информационной безопасности.

ZECURION

ZECURION DLP

Zecurion DLP (Data Loss Prevention) — комплексная система защиты от утечек корпоративной информации. Zecurion DLP включает в себя системы Zlock, Zgate и Zserver, которые предназначены соответственно для предотвращения утечек через периферийные устройства, сетевые каналы и носители при хранении. В комплекс Zecurion DLP также входит система Zdiscovery, реализующая поиск конфиденциальной информации на компьютерах пользователей и в хранилищах данных. Каждый из продуктов может применяться отдельно для защиты от утечек через конкретный тип каналов. В то же время для создания комплексной защиты от утечек все продукты легко интегрируются в единую DLP-систему и управляются централизованно с общей консоли.

Zecurion DLP позволяет контролировать:

- переписку в корпоративной электронной почте;
- письма и вложения, отсылаемые через сервисы веб-почты;
- общение в социальных сетях, на форумах и блогах (HTTP/HTTPS-трафик);
- сообщения интернет-пейджеров — ICQ, Mail.Ru Агент, QIP, Google Talk и более десяти других систем, включая Skype;
- FTP, POP3, IMAP, SMTP и другие сетевые каналы;
- файлы, записываемые на USB-накопители и любые внешние устройства;
- печать на локальных и сетевых принтерах;
- наличие конфиденциальных данных, хранящихся на компьютерах пользователей и серверах;
- доступ к информации, хранящейся на серверах, магнитных лентах и оптических дисках.

Основные преимущества Zecurion DLP

- Контроль всех наиболее опасных каналов утечки.
- Гибридный анализ перехваченных данных (эффективность более 95 %) с использованием морфологии, «цифровых отпечатков» DocuPrints, регулярных выражений, OCR и собственной технологии SmartID.
- Поддержка анализа более 500 типов файлов.
- Возможность блокирования утечек в режиме реального времени.
- Архивирование всей перехваченной информации, инструменты для последующего поиска и анализа данных архива.
- Сканирование локальных и сетевых хранилищ для поиска файлов с конфиденциальной информацией.
- Защита данных в местах хранения — на серверах и резервных носителях информации.
- Единая консоль управления.

Таким образом, использование Zecurion DLP обеспечивает комплексную защиту информации от утечек на протяжении всего ее жизненного цикла — от создания до записи в архив или удаления.

ZECURION

РЕШАЕМЫЕ ЗАДАЧИ

Оценка защищенности

Использование Zecurion DLP позволяет составить полную картину защищенности корпоративной сети от утечек информации.

Защита от случайных утечек

Большинство утечек происходит случайно — из-за невнимательности, равнодушия, отсутствия или незнания политик безопасности. Zecurion DLP автоматически обнаруживает и предотвращает утечки, снижая влияние человеческого фактора.

Защита от намеренных утечек

Намеренные утечки происходят по вине сотрудников, преследующих цель извлечь выгоду или нанести вред работодателю путем компрометации данных. Zecurion DLP учитывает всевозможные сценарии совершения утечек и попыток обхода системы защиты.

Реализация действующей политики безопасности

В большинстве организаций уже в той или иной форме существует политика безопасности. Использование Zecurion DLP позволяет сформировать правила реализации политики ИБ, контролировать их исполнение и оперативно выявлять нарушителей.

Архивирование критически важных данных

В отличие от многих существующих DLP-систем продукты Zecurion обладают встроенными функциями архивирования (теневого копирования) данных, перемещаемых за пределы сети.

Расследование инцидентов

Ретроспективный анализ по данным архива и журнала событий Zecurion DLP помогает не только расследовать произошедшие инциденты, но и предотвращать будущие.

Безопасное хранение, трансфер и утилизация

Данные, которые хранятся, обрабатываются и перевозятся на жестких дисках (например, в составе корпоративного сервера) и магнитных лентах, нуждаются в надежной защите, ведь они подвержены высоким рискам утечки при получении физического доступа к носителям.

Управление лояльностью сотрудников

Вовремя обнаружив подозрительное поведение, ИБ-специалисты совместно со специалистами по управлению персоналом и непосредственными руководителями могут выявить и устранить причины снижения лояльности и сохранить ключевых сотрудников в компании.

Сохранение конкурентоспособности

Внедрение Zecurion DLP может серьезно повысить конкурентоспособность компании, сделать ее более привлекательной не только для клиентов, но и для партнеров с инвесторами.

Безопасность переговоров, контроль закупочной деятельности

Для успешного ведения переговоров необходимо контролировать доступ к ключевой информации внутри компании и передачу ее третьим лицам.

152-ФЗ и отраслевые стандарты

Внедрение продуктов Zecurion помогает решать важную задачу — соблюдение требований отраслевых стандартов и законодательства, в том числе закона «О персональных данных».

ZECURION

DLP-система для защиты
от утечек по сети

ZGATE

Назначение

Сегодня сложно представить себе компанию, в которой сотрудники не пользуются электронной почтой и Интернетом. А если есть выход за пределы корпоративной сети, значит, есть и риски утечки конфиденциальной информации. Случайно ввел неправильный адрес при отправке письма, поделился «по секрету» инсайдерской информацией с другом по аське, выложил документ на открытый файлообменный ресурс вместо закрытого корпоративного — такие мелкие нарушения правил ИБ порой приводят к фатальным последствиям. Потеря или кража конфиденциальных данных ведет не только к прямым финансовым убыткам, но и к снижению доверия со стороны клиентов, партнёров и инвесторов, повышенному интересу со стороны регулирующих органов и СМИ. Предотвратить как случайные, так и намеренные утечки по сетевым каналам способна DLP-система Zgate.

Обзор Zgate

Zgate предназначен для предотвращения утечек конфиденциальной информации через электронную почту, социальные сети, интернет-мессенджеры и любые другие сетевые каналы передачи данных.

Zgate позволяет контролировать и архивировать:

- переписку в корпоративной электронной почте;
- письма и вложения, отсылаемые через сервисы веб-почты;
- общение в социальных сетях, на форумах и блогах;
- сообщения интернет-пейджеров;
- файлы, передаваемые по FTP.

Для анализа сообщений в Zgate используется гибридный анализ — комплекс современных технологий детектирования, которые с высокой точностью определяют уровень конфиденциальности передаваемой информации и категорию документов с учетом особенностей бизнеса, требований отраслевых стандартов и законодательства России, СНГ, Европы и США. Применение гибридного анализа позволило повысить эффективность детектирования со среднестатистических 60–70 % для существующих DLP до 95 % у Zgate.

Настройки Zgate позволяют назначить различные действия, которые будут производиться с обнаруженными подозрительными сообщениями в соответствии с политикой безопасности: их можно заблокировать, пропустить с уведомлением офицера безопасности или поместить в карантин для ручной проверки.

Zgate сохраняет в архиве переданные сообщения и документы, а также служебную информацию: сведения об отправителе, получателе, канале передачи, и т. д. Такой архив является незаменимым инструментом для анализа, проведения внутренних расследований и профилактики утечек. Встроенная система отчетности предоставляет полный набор возможностей для наглядного анализа перехваченных данных.

ZECURION

Решаемые задачи

- Анализ содержимого пересылаемых сообщений и файлов. Zgate анализирует сетевой трафик и с помощью специальных технологий детектирования обнаруживает передачу конфиденциальных данных.
- Категоризация всей пересылаемой информации. При анализе содержимого сообщений и файлов Zgate разбирает пересылаемые данные по различным категориям. Например, для телекоммуникационных компаний особую ценность имеют такие категории, как информация об объектах связи и данные об абонентах.
- Обнаружение и блокировка утечек конфиденциальных данных. Большинство DLP-систем работают в «пассивном» режиме, то есть лишь оповещают о факте утечки. В отличие от них, Zgate предотвращает утечки информации из компании в реальном времени.
- Предупреждение утечек информации. Большую часть утечек информации можно предотвратить, если своевременно оптимизировать политики безопасности. Zgate еще на ранней стадии обнаруживает подозрительную активность, что позволяет дополнительно сократить риски утечки конфиденциальных данных.
- Архивирование всей пересылаемой информации. Zgate архивирует корпоративную электронную почту, сообщения и файлы, передаваемые через интернет-пейджеры, социальные сети, веб-почту, форумы, блоги и т. д. Архивируемые данные записываются в СУБД Oracle Database или Microsoft SQL Server.
- Приведение политик безопасности в полное соответствие с требованиями отраслевых стандартов и законодательства. В частности, использование систем защиты от утечек регламентируется стандартами Банка России, Кодексом корпоративного поведения ФСФР, PCI DSS, SOX, Basel II и множеством других документов.

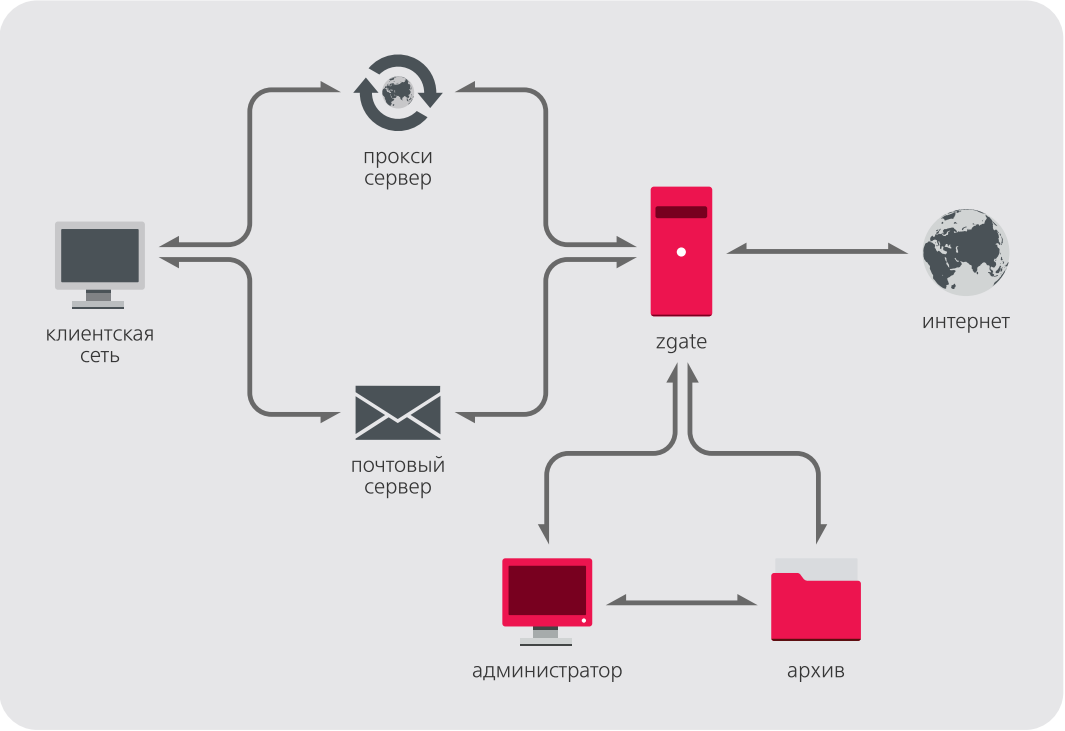
Возможности

- Работа как в режиме активной фильтрации, так и в режиме слежения, когда при обнаружении утечки не происходит блокировки.
- Поддержка протоколов HTTP, HTTPS, FTP, FTPS, SMTP, ESMTP, OSCAR, Mail.Ru Агент, AIM, MSNP, Yahoo! Messenger, XMPP и др.
- Совместимость с любой почтовой системой (MTA), работающей по протоколу SMTP: Microsoft Exchange Server, IBM Lotus Domino, CommunigatePro и др.
- Интеграция с Microsoft Forefront TMG (Microsoft ISA Server) и любым прокси-сервером, поддерживающим протокол ICAP — Blue Coat, Cisco ACNS, Squid и др.
- Анализ сообщений и файлов, отправляемых через ICQ, Skype, Miranda IM, QIP, Trillian, Licq, Kopete, AIM, Google Talk, Я. Онлайн, LJ Talk, Gizmo5, Yahoo! Messenger и др.
- Контроль передачи данных на популярные веб-сайты Mail.ru, Яндекс.Почта, Рамблер-Почта, Gmail, Hotmail, ВКонтакте, Одноклассники, MySpace, Facebook, LiveJournal, Twitter и др.
- Возможность ведения полного архива передаваемых данных, включая файлы-вложения.
- Применение политик в зависимости от времени передачи, направления трафика и местоположения пользователей.
- Специальные политики для зашифрованных вложений и архивов.
- Контентный анализ с помощью любой комбинации технологий обнаружения утечек.
- Возможность ручной проверки подозрительных сообщений и файлов.
- Модификация сообщений и уведомление пользователей о результатах фильтрации.
- Интеграция со сторонним ПО для дополнительной обработки, например, антиспам-системами.
- Инструменты для управления словарями, описывающими различные категории документов.
- Широкие возможности для разделения ролей администраторов.
- Поддержка импорта статистической информации в различные конструкторы отчётов.

Преимущества

- Zgate контролирует весь сетевой трафик. В отличие от существующих DLP-систем, кроме исходящего трафика, Zgate может анализировать входящий и внутренний трафик, что расширяет возможности для внутреннего контроля.
- Для обнаружения и своевременной блокировки утечек информации в Zgate применяется гибридный анализ, использующий более 10 специализированных технологий, в том числе «цифровые отпечатки», лингвистический анализ, проверку по шаблонам регулярных выражений, OCR и обучаемую технологию SmartID.

- Zgate контролирует сообщения и файлы, отправляемые через более чем 15 видов интернет-пейджеров и более чем 250 различных веб-сервисов — от почты Mail.Ru до видеохостинга YouTube.
- Zgate поддерживает анализ более 500 форматов файлов, в том числе Microsoft Office, OpenOffice.org, изображения, а также обработку архивов заданного уровня вложенности.
- Встроенная OCR-технология позволяет обнаруживать конфиденциальную информацию даже в графических файлах — скриншотах, сфотографированных или отсканированных документах.
- Все пересылаемые письма, сообщения и файлы помещаются в специальный архив, не имеющий ограничений по объему и сроку хранения данных и обладающий удобными инструментами для дальнейшего анализа данных и расследования.
- В установку Zgate включено более 50 шаблонов, с помощью которых можно определять конфиденциальные данные. Это существенно сокращает трудозатраты при внедрении.
- Для настройки защиты информации в Zgate используются специальные политики безопасности, имеющие до 30 различных параметров.
- Масштабируемость и модульная архитектура Zgate позволяют учесть самые жесткие требования к производительности.
- Управление Zgate осуществляется через единую систему управления DLP-решениями Zconsole, которая также поддерживает управление Zlock, Zdiscovery и Zserver Suite.



Технические требования

Процессор:	Pentium 4 и выше
Оперативная память:	1 Гб и выше
Операционная система:	Windows 2000 SP4, 2000 Server SP4, XP SP3, 2003 SP2, 2003 R2, Vista SP1, Windows 7, Server 2008 и R2
Прочие программные средства:	Oracle Database 10g Release 2 (10.2) или Microsoft SQL Server 2005 SP3, 2008, 2008 R2 для архива почтовых сообщений и карантина. WinPcap 4.1.2, Microsoft ISA Server 2006 или Microsoft Forefront Threat Management Gateway — для зеркалирования и фильтрации Web-трафика, Squid 2.6 (HTTP), Squid 3.1.12 (HTTPS), Microsoft Exchange 2007/2010 (x64) — для зеркалирования и фильтрации внутреннего почтового трафика.

ZECURION

DLP-система для защиты от утечек на конечных точках сети

ZLOCK

Назначение

Помимо сетевых каналов реально опасными с точки зрения утечек конфиденциальной информации всегда были периферийные устройства, подключаемые сотрудниками к своим рабочим компьютерам. Особую актуальность данная проблема получила в последние пять лет вместе с появлением огромного количества вместительных и мобильных устройств — флешек, портативных HDD, мобильных телефонов с большим объёмом памяти, внешних DVD-приводов и т. д. Отличительной особенностью периферийных устройств является то, что на них можно быстро и, соответственно, почти незаметно скопировать большие объёмы информации — от нескольких десятков мегабайт до терабайта или более. Во многих организациях необходимость использования USB-устройств продиктована структурой бизнес-процессов, но даже легальное копирование на внешние накопители несет в себе огромные риски, возникающие при перевозке и хранении носителей — их легко потерять, например, оставить в кафе, выронить из кармана в метро или автобусе.

Обзор Zlock

Zlock предназначен для предотвращения утечек конфиденциальной информации на конечных точках сети. Zlock позволяет контролировать использование устройств, подключаемых к портам USB, LPT, COM, IrDA, IEEE 1394, слоту PCMCIA, внутренних устройств — в том числе встроенных сетевых карт, модемов, Bluetooth, Wi-Fi, CD/DVD-дисководов, а также локальных и сетевых принтеров.

Для настройки политик доступа в Zlock могут использоваться любые атрибуты устройств, к которым она будет применяться: серийный номер, класс и идентификатор устройства, данные о производителе и другие параметры. В системе Zlock есть возможность хранения описаний устройств в едином каталоге и создания политик на их основе.

Встроенные инструменты контентного анализа позволяют реализовать фильтрацию записи документов на накопители и печати на принтерах по типам файлов и их содержимому. Такая гибкая настройка дает возможность минимизировать риски утечки конфиденциальной информации без малейшего препятствия нормальному ходу бизнес-процессов организации.

Zlock реализует автоматическое архивирование (теневое копирование) данных, которые пользователи копируют на внешние накопители и распечатывают на принтерах. Это позволяет гарантированно контролировать запись и печать документов, оперативно реагировать на возникающие нарушения, а также расследовать обстоятельства инцидентов.

Решаемые задачи

- Разграничение доступа. Zlock позволяет контролировать доступ к любым устройствам и портам на основе гибкой настройки политик доступа.
- Контроль выноса документов. Zlock контролирует все документы и файлы, которые копируются на съемные устройства и распечатываются на локальных и сетевых принтерах.
- Контентный анализ информации. С помощью специализированных технологий детектирования Zlock анализирует содержимое файлов, передаваемых на устройства и печать, и обнаруживает в них конфиденциальные данные.

- Блокирование утечек информации. В отличие от других агентских систем, Zlock способен предотвращать утечки информации через устройства в режиме реального времени. При выявлении нарушений политик безопасности Zlock блокирует печать, чтение или запись на устройства.
- Архивирование информации. Теневые копии всех записанных на устройства и распечатанных документов вне зависимости от их формата (PostScript, PCL и т. д.) заносятся в архив, не ограниченный по объему и времени хранения.
- Приведение политик безопасности в полное соответствие с требованиями отраслевых стандартов и законодательства. В частности, использование систем защиты от утечек регламентируется стандартами Банка России, Кодексом корпоративного поведения ФСФР, PCI DSS, SOX, Basel II и множеством других документов.

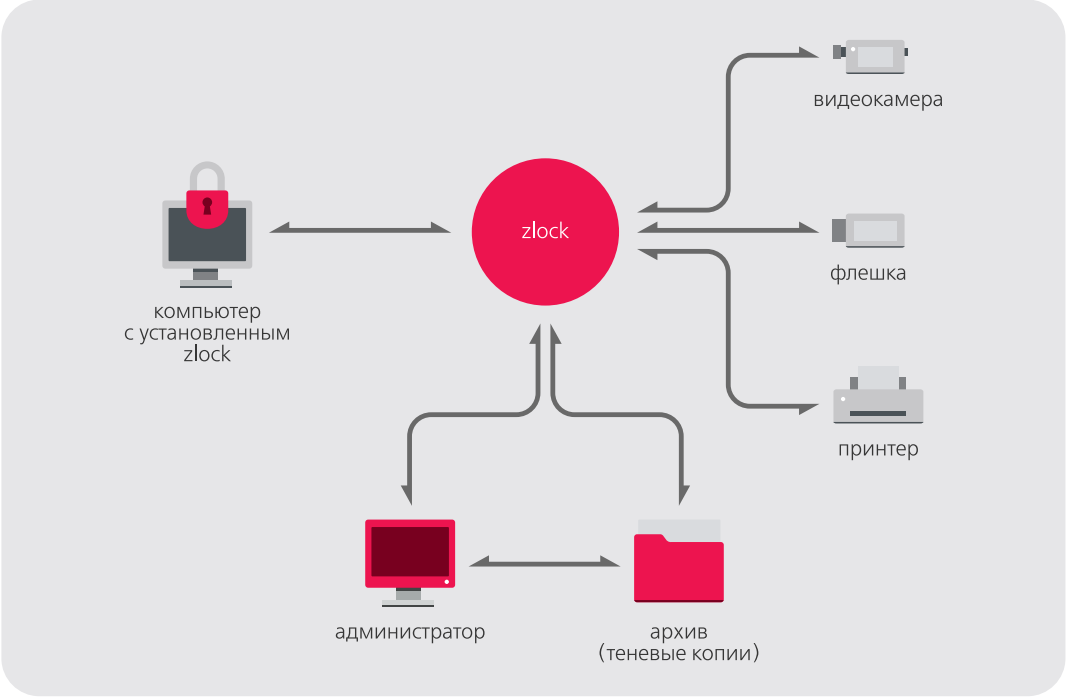
Возможности

- Совместимость с любыми моделями и марками периферийных устройств.
- Поддержка контроля любых USB-устройств, контроллеров Wi-Fi, Bluetooth, IrDA, сетевых карт и модемов, FDD-, CD- и DVD-дисководов, жестких дисков, портов LPT, COM и IEEE 1394, локальных и сетевых принтеров и любых других устройств, имеющих символическое имя.
- Применение политик в зависимости от времени, способа использования устройств и местоположения пользователей.
- Контентный анализ с помощью любой комбинации технологий обнаружения утечек.
- Сбор событий системы и возможности анализа журнала событий.
- Архивирование (теневая копия) всех файлов, распечатанных и записанных на устройства.
- Уведомление пользователей об ограничении доступа к устройству и запрету выноса из организации копируемых или распечатываемых ими данных.
- Развертывание и управление как через собственную консоль, так и через групповые политики Microsoft Active Directory.
- Модульная архитектура, обеспечивающая надежную работу в сетях до 250 000 компьютеров.
- Онлайн-мониторинг работы всех агентов Zlock.
- Защита от отключения системы пользователями, которые в нарушение политик безопасности имеют права локальных администраторов.
- Удалённое предоставление доступа по телефону или электронной почте.
- Инструменты для управления словарями, описывающими различные категории документов.
- Широкие возможности для разделения ролей администраторов.
- Поддержка импорта статистической информации в различные конструкторы отчётов.

Преимущества

- Zlock позволяет настраивать политики доступа максимально гибко, учитывая не только характеристики устройств, но и содержимое записываемых документов и типы файлов.
- Контентный анализ Zlock, использующий несколько специализированных технологий детектирования, позволяет настроить фильтрацию записи и печати по содержимому файлов, например, разрешить копировать любые файлы, кроме документов, содержащих конфиденциальную информацию.
- Zlock создает теневые копии распечатываемых и записываемых на накопители документов превентивным образом, что гарантирует сохранение копий в архиве даже при внезапном прерывании записи.

- Zlock поддерживает более 500 наиболее распространённых в корпоративной среде форматов файлов, в том числе Microsoft Office и OpenOffice.org.
- Тесная интеграция с Active Directory позволяет без лишних трудозатрат разворачивать Zlock, распространять политики и масштабировать систему на любое количество рабочих станций в пределах организации.
- Мониторинг агентов и контроль целостности гарантируют бесперебойную работу системы и надежно защищают от случайных или намеренных деструктивных действий пользователей.
- Новые политики в Zlock могут создаваться оперативно по запросам пользователей, в том числе удаленно: по телефону или электронной почте.
- Zlock имеет сертификаты Министерства Обороны и ФСТЭК.
- Управление Zlock осуществляется через единую систему управления DLP-решениями Zconsole, которая также поддерживает управление Zgate, Zdiscovery и Zserver Suite.



Технические требования

Процессор:	Pentium III и выше.
Оперативная память:	256 Мб и выше.
Операционная система:	Microsoft Windows XP SP2 (32 бита)/ Windows Server 2003 SP1 (32 бита) / Windows Vista SP1 (32 и 64 бита), Windows Server 2008 и R2 (32 и 64 бита) / Windows 7 (32 и 64 бита).
Прочие программные средства:	Microsoft SQL Server 2000 SP2 и выше — для хранения журнала.

ZECURION

Криптографический комплекс
для защиты информации
при хранении

ZSERVER SUITE

Назначение

Сегодня подавляющее большинство организаций для оптимизации своей работы использует централизованные хранилища информации — от простых сетевых NAS-накопителей и серверов начального уровня до специально построенных ЦОД с собственной охраной, системами пожаротушения и сигнализацией. Централизованное хранение информации кроме очевидных плюсов несет в себе и далеко неочевидный риск — риск того, что злоумышленники получат физический доступ непосредственно к носителям информации. Иллюзию защищённости создают обычно применяемые меры безопасности, ведь на первый взгляд физический доступ к носителям информации могут получить только доверенные люди, однако на деле это далеко не так.

Физический доступ посторонних лиц к носителям данных может возникать в следующих ситуациях:

- работы по обслуживанию серверного помещения;
- ремонт самого сервера или другого оборудования на месте или с вывозом из офиса;
- невнимательность или коррумпированность сотрудников, ответственных за охрану помещения;
- хранение данных в облачных сервисах или аренда ЦОДа;
- изъятие серверного и другого компьютерного оборудования компетентными органами;
- переезд и перевозка сервера в другое помещение или новый офис;
- транспортировка магнитных лент или дисков с резервными копиями данных в депозитарий;
- утилизация устаревшего, вышедшего из строя оборудования.

Другое распространенное заблуждение — на серверах не хранится такая информация, потеря которой могла бы причинить вред компании. Для того чтобы его опровергнуть, достаточно представить себе возможные последствия утечки следующих типов данных, которые хранятся на серверах и резервных носителях (лентах и дисках) практически в любой организации:

- информация о финансово-хозяйственной деятельности;
- персональные данные клиентов и сотрудников (имена, адреса, телефоны, номера счетов и т. п.);
- внутренние протоколы, приказы, должностные инструкции и штатное расписание;
- списки клиентов и поставщиков и другие данные CRM- и ERP-систем;
- договоры и условия работы с заказчиками и подрядчиками;
- маркетинговый, финансовый, производственный и другие тактические и стратегические планы руководства.

Защита информации в местах хранения успешно реализуется Zserver Suite с помощью шифрования. Данные всегда находятся на носителях в зашифрованном виде и становятся доступны только при загрузке ключа шифрования. Для оперативного реагирования на нештатные события, например, срабатывание сигнализации или появление в офисе компании «незваных гостей», в системе Zserver Suite существует специально разработанная система тревоги, которая позволяет мгновенно блокировать доступ к данным с помощью «красной кнопки», радио- или даже GSM-сигнала — звонка на специальный номер телефона.

ZECURION

Обзор Zserver Suite

Zserver Suite является комплексом криптографических решений для защиты данных, которые хранятся на серверах, магнитных лентах, оптических дисках, в хранилищах и на внешних неконтролируемых площадках. С помощью шифрования данных на уровне драйвера операционной системы Zserver Suite надежно защищает данные в процессе использования, хранения и транспортировки. Даже в случае попадания физических носителей в руки злоумышленников доступ к зашифрованным данным без ключа будет невозможен.

Zserver работает по принципу «прозрачного» шифрования носителей информации. Система автоматически в режиме реального времени осуществляет шифрование информации при записи на носитель и расшифровывает при чтении с него, так что наличие системы остается совершенно незаметным для пользователей. При этом такие операции остаются «прозрачными» не только для сотрудников, но даже для серверной операционной системы, что обеспечивает полную совместимость с любым локальным и сетевым программным обеспечением — 1С, Microsoft Exchange Server, Oracle Database и т. д.

Надежность защиты обеспечивают специальные стойкие алгоритмы шифрования с длиной ключа до 512 бит. Доступ к данным основан на двухфакторной аутентификации администратора: ключ шифрования записан на смарт-карту, защищенную PIN-кодом, который в свою очередь нельзя определить методом перебора — количество попыток его ввода ограничено.

Решаемые задачи

- Защита конфиденциальной информации в местах хранения.
- Безопасная транспортировка и утилизация данных.
- Защита баз данных, почтовых и файловых серверов в процессе работы.
- Контроль доступа к защищаемой информации для пользователей и приложений.
- Полное скрытие факта наличия на защищаемых носителях каких-либо данных и ПО.
- Оперативное блокирование доступа к информации в случае экстренной необходимости.
- Защита данных от несанкционированного доступа со стороны системного администратора.
- Гарантированное уничтожение информации.

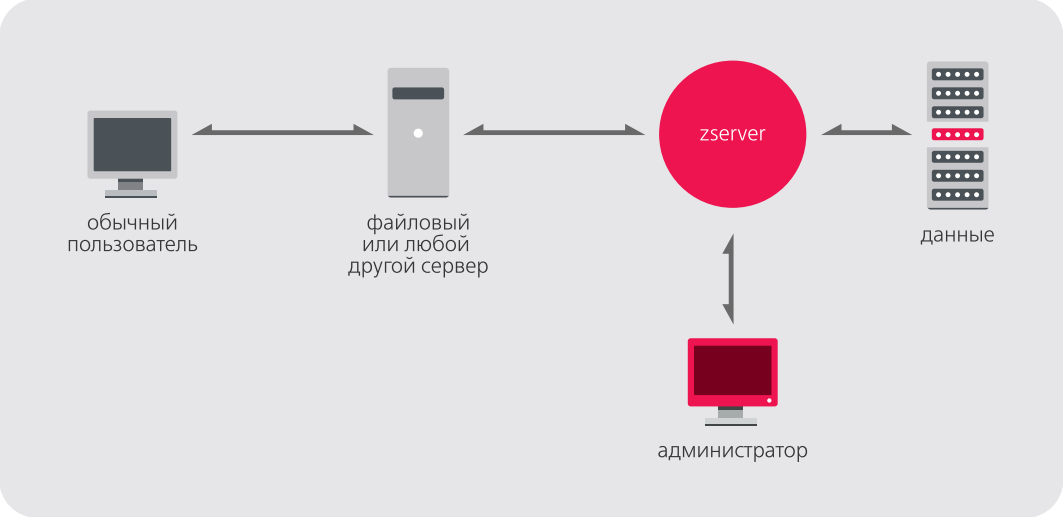
Особые возможности

- Модуль Zserver Enterprise Key Server даёт возможность централизованного управления ключами шифрования на неограниченном количестве серверов.
- Модуль Zserver Script Pack существенно расширяет стандартный функционал, позволяя задавать собственную реакцию на события системы, например, сделать «подмену диска» на заранее заготовленный сразу же после поступления сигнала «тревога».
- Модуль Zserver Disk Access Control позволяет управлять доступом к информации со стороны пользователей и приложений, давая возможность задавать роль дискового firewall.
- Модули GSM- и Radio-Alarm дают дополнительные возможности для оперативной блокировки доступа к данным с помощью телефона или радиобрелока.
- Кворум ключей шифрования позволяет минимизировать человеческий фактор за счет разделения ключей на несколько частей по аналогии с хранилищами в крупных банках.
- Zserver Suite может функционировать на серверах в кластере Microsoft Cluster Services.
- Технология определения испорченных секторов (Bad Block Sense) гарантирует стабильную работу системы даже в случае появления на диске испорченных секторов.

Преимущества

- Zserver Suite всегда хранит защищаемые данные в зашифрованном виде и расшифровывает их лишь по необходимости.
- В системе используются только сверхстойкие и проверенные временем алгоритмы шифрования с длиной ключа до 512 бит — RC5, AES, XTS-AES и ГОСТ 28147-89.

- Многопоточное шифрование Zserver Suite позволяет существенно повысить скорость шифрования данных на многопроцессорных и многоядерных серверах.
- За счет специальной технологии «фонового» шифрования не требуется прекращение доступа к информации на этапе внедрения Zserver Suite.
- Zserver Suite позволяет безопасно генерировать ключи шифрования с помощью движений мышью, шумов микрофона и множества других физических источников.
- Ключи шифрования записываются на смарт-карту, защищенную пин-кодом — это гарантирует, что доступ к данным всегда будут иметь только доверенные лица.
- Высокая скорость шифрования и низкие требования к аппаратным ресурсам делают Zserver Suite практически незаметным в работе.
- В Zserver Suite реализована возможность мгновенной блокировки доступа к данным с помощью кнопки «тревоги», специальных радиобрелоков, обычного телефона и любой современной сигнализации.
- Zserver Suite полностью совместим со всеми ИТ-системами, так как работает в «прозрачном» режиме для операционной системы, приложений и пользователей.
- Для полноценной работы с защищаемыми данными не требуется устанавливать какие-либо агенты или системы управления ключами на компьютеры рядовых сотрудников.
- Управление Zserver Suite осуществляется через единую систему управления DLP-решениями Zconsole, которая также поддерживает управление Zgate, Zlock и Zdiscovery.



Технические требования

Процессор:	Pentium III и выше.
Оперативная память:	128 Мб и выше.
Операционная система:	Microsoft Windows 2000 / Windows XP / Windows 2003 / Windows Vista / Windows 2008 / Windows 7 / Windows 2008 R2 Linux с ядром 2.6.x.
Прочие программные средства:	сетевой протокол TCP/IP (для удаленного управления Zserver).

ZECURION

Система поиска
конфиденциальной информации
на рабочих станциях и серверах

ZDISCOVERY

Назначение

Централизованное хранение и полный контроль над конфиденциальными документами является первым и необходимым шагом для обеспечения их безопасности. Защита информации начинается с ответа на вопрос: что нужно защитить? Предположим, руководство компании точно знает, что необходимо контролировать использование договоров или списков клиентов — это уже полдела. Однако реализация политик безопасности на практике незамедлительно наталкивается на препятствие в виде хаотичного хранения, перемещения и использования различных документов. Как обеспечить безопасность конфиденциальных документов, если они «гуляют» по компьютерам сотрудников без соблюдения каких-либо правил хранения?

Бесконтрольное хранение корпоративной информации несет в себе очевидные риски потери и утечки важных документов. Если данные хранятся не централизованно, их невозможно систематически защищать как от внутренних, так и от внешних угроз. Несложно представить себе последствия неосторожного хранения конфиденциальных данных на ноутбуке руководителя, который легко может быть потерян в командировке или украден злоумышленником. Статистика утечек говорит сама за себя: потеря ноутбуков не первый год лидирует среди популярных каналов утечки по всему миру. Локальное хранение информации на рабочих компьютерах сотрудников чревато потерей важных документов: при случайном удалении файла восстановить его будет практически невозможно. Кроме того, бесконтрольное хранение создает сложности при необходимости надежного уничтожения данных и при утилизации оборудования. Именно поэтому необходимо постоянно контролировать как уже имеющиеся, так и вновь создаваемые конфиденциальные документы и оперативно исправлять нарушения политик их хранения.

Обзор Zdiscovery

Система Zdiscovery предназначена для обнаружения конфиденциальной информации в корпоративной сети и предотвращения нарушений правил ее хранения. Для поиска данных в Zdiscovery используются специальные агенты. Они анализируют данные на жестких дисках компьютеров и серверов, в том числе и на «скрытых» логических дисках.

Zdiscovery позволяет обнаруживать:

- несанкционированные копии конфиденциальной информации на рабочих компьютерах и ноутбуках пользователей;
- конфиденциальные документы в общедоступных сетевых хранилищах;
- персональные данные, хранящиеся в корпоративной сети.

Для обнаружения конфиденциальной информации в Zdiscovery используется гибридный анализ — комплекс современных технологий детектирования. Они с высокой точностью определяют уровень конфиденциальности и категорию обнаруженного документа с учетом особенностей бизнеса, требований отраслевых стандартов и законодательства России, СНГ, Европы и США. Применение гибридного анализа повышает эффективность обнаружения конфиденциальной информации до 95% по сравнению с системами, использующими какие-либо отдельные технологии детектирования.

Настройки Zdiscovery позволяют задавать различные действия, которые будут производиться при обнаружении нарушений политик безопасности. Сами данные можно удалить или переместить в специальное хранилище, а информацию о нарушении незамедлительно сообщить администратору и пользователю, допустившему неправильное хранение. Помимо этого все события, в том числе список обнаруженных нарушений, сохраняются в специальных журналах (логах) для последующего анализа.

Решаемые задачи

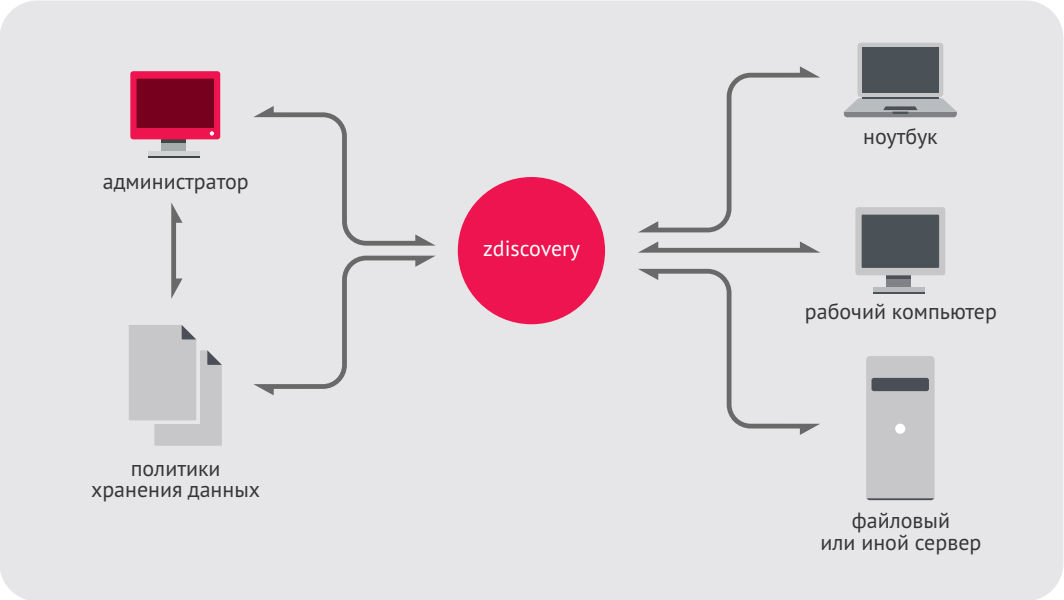
- Сканирование хранилищ данных в режиме реального времени и по расписанию.
- Поиск информации в корпоративной сети.
- Учет и анализ всех хранящихся данных.
- Обнаружение конфиденциальных данных.
- Определение информации, подлежащей защите.
- Предупреждение утечек информации.
- Обнаружение нарушений политик ИБ в организации.
- Приведение политики безопасности в соответствие с законодательством и отраслевыми стандартами.

Возможности

- Сканирование в онлайн-режиме и по расписанию всех доступных сетевых и локальных хранилищ информации, в том числе рабочих станций и ноутбуков пользователей, файловых и иных серверов.
- Обнаружение конфиденциальных документов различных типов, например, договоров с поставщиками, планов развития, резюме сотрудников и персональных данных.
- Контентный анализ файлов различных типов на предмет содержания в них конфиденциальных данных.
- Мгновенное уведомление администратора о нарушениях политик безопасности, в том числе имени хранилища, где были найдены нарушения, и точном расположении данных.
- Возможность настройки перемещения, удаления файлов, нарушающих определенную политику безопасности, или любого другого действия с помощью специальных скриптов.
- Предупреждение пользователей об обнаруженных нарушениях.
- Категоризация всей пересылаемой информации исходя из отраслевых особенностей деятельности компании.
- Теневое копирование в архив найденных подозрительных файлов.
- Быстрый просмотр содержимого файла, сохраненного в архиве.
- Удаленное и централизованное администрирование через единую систему управления DLP-решениями Zecurion.
- Широкие возможности для разделения ролей администраторов и регистрация всех действий администраторов в журнале событий.
- Гибкая настройка политик сканирования, анализа файлов и реакции на обнаруженные нарушения.
- Масштабируемость и модульная архитектура.
- Возможность работы как в доменных сетях, так и в сетях без домена.
- Специальные правила для оптимизации производительности (например, настройка сканирования в ночное время).
- Поддержка всех современных операционных систем Microsoft.

Преимущества

- Zdiscovery контролирует все основные хранилища информации в корпоративной сети: любые серверные хранилища и рабочие станции пользователей.
- Для анализа данных Zdiscovery использует множество специальных технологий, в том числе проверку по шаблонам регулярных выражений, лингвистику, цифровые отпечатки и обучаемую технологию SmartID.
- Zdiscovery обнаруживает конфиденциальные документы в режиме реального времени, моментально реагируя на создание новых файлов и внесение изменений в их содержимое. Это позволяет постоянно контролировать соблюдение политик хранения конфиденциальной информации и оперативно принимать меры при обнаружении нарушений.
- Для снижения нагрузки, создаваемой агентами Zdiscovery, в системе используются специальные поисковые технологии, существенно оптимизирующие процесс сканирования.
- Управление Zdiscovery осуществляется через единую систему управления DLP-решениями Zconsole, которая также поддерживает управление Zgate, Zlock и Zserver Suite.



Технические требования

Процессор:	Pentium IV и выше.
Оперативная память:	1 Гбайт и выше.
Операционная система:	Microsoft Windows XP SP3 (32 бит) / Windows Server 2003 SP2 (32 бит) / Windows Vista SP1 (32 и 64 бит) / Windows Server 2008 (32 и 64 бит) / Windows 7 (32 и 64 бит) / Windows Server 2008 R2.
Прочие программные средства:	Microsoft SQL Server 2005, 2008 или Oracle Database 10g и выше — для хранения журнала.

КОМПЛЕКСНОЕ DLP-РЕШЕНИЕ

Zecurion предлагает комплексную систему, обеспечивающую надежную защиту от утечек конфиденциальной информации. Очевидно, что именно комплексный подход к защите информации является наиболее эффективным. Если внедрение узкоспециализированного продукта помогает установить контроль над некоторыми каналами утечки, то создание комплексной DLP-системы позволяет минимизировать риски утечки данных по всем возможным каналам.

В комплекс Zecurion DLP входят средства для решения различных задач в рамках защиты информации, которые тесно интегрируются друг с другом в любой комбинации и составляют единую систему защиты от утечек. Zgate анализирует сообщения, передаваемые по сетевым каналам, Zlock контролирует печать на принтерах, копирование документов на USB-накопители и другие устройства, Zserver защищает информацию при хранении на серверах с помощью шифрования, Zdiscovery реализует поиск конфиденциальной информации на компьютерах пользователей и в хранилищах данных. Все четыре системы могут использоваться самостоятельно для решения специальных задач и в то же время дополняют друг друга. Zgate, Zlock, Zdiscovery и Zserver управляются из единой консоли Zconsole с общим удобным интерфейсом. Это позволяет минимизировать усилия по интеграции различных систем и централизовать администрирование системы защиты от утечек информации.

Благодаря масштабируемости DLP-систем Zecurion и гибкой лицензионной политике существует возможность поэтапного внедрения ПО в различных вариантах сочетания продуктов. Это позволяет создавать индивидуальные решения, максимально точно отвечающие существующим задачам ИБ. Комплексные системы Zecurion уже используются в нескольких тысячах компаний. Среди клиентов Zecurion такие организации, как Аэрофлот, Министерство финансов РФ, Роснефть, РОСГОССТРАХ, Сбербанк России, Ростелеком, Мосэнергосбыт, Федеральная таможенная служба, Райффайзенбанк, Crédit Agricole, банки в составе международных банковских групп Societe Generale и UniCredit.

КЛИЕНТЫ

Allianz

CRÉDIT AGRICOLE

СБЕРБАНК

РОСБАНК
SOCIETE GENERALE GROUP

ТУПОЛЕВ
Открытое акционерное общество

РОСНО
в составе Allianz

МЕТРОПОЛЬ®
ИНВЕСТИЦИОННАЯ ФИНАНСОВАЯ КОМПАНИЯ

ProCredit Bank
ПроКредит Банк

CENTERCREDIT

МОСКОВСКИЙ КРЕДИТНЫЙ БАНК

Ростелеком
Больше возможностей

ВТБ ПЕНСИОННЫЙ ФОНД

С нами приходит свет!
МОСЭНЕРГОСБЫТ

ОБИБАНК
ОБЪЕДИНЕННЫЙ ИНВЕСТИЦИОННЫЙ БАНК

TEZ tour THAILAND

TNT

1921 РОСГОССТРАХ

СИБУР ХИМПРОМ

АТФ Банк
Член группы UniCredit Group

СИББИЗНЕСБАНК®
www.sbrb.ru

АЭРОФЛОТ Российские авиалинии SKYTEAM

МИНИСТЕРСТВО ФИНАНСОВ РФ

РОСНЕФТЬ

ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО

ТЕХНОСИЛА®

ФЕДЕРАЛЬНАЯ ТАМОЖЕННАЯ СЛУЖБА

ZECURION

КОНТАКТЫ

129164, Российская Федерация,
Москва, Ракетный бульвар, 16
+7 495 221-21-60
info@zecurion.com
www.zecurion.ru