Создание образа Windows для устройств Windows 10

Windows IT Pro/RE

№6 ИЮНЬ 2016 | WWW.WINDOWSITPRO.RU | ИНФО ДЛЯ ИТ-ПРО

Вокруг Exchange и Office 365

Мобильная версия

App Store

Google play

Знакомимся с группами Office 365

Защита от потери данных в Exchange Server 2013

Используем группы Office 365 с Outlook 2016

Развертывание новых продуктов в «облаке» и на земле

Избавляемся от вредных привычек с помощью Delve Analytics

ISSN 1563-101X

16006

9 771563 101008

Windows IT Pro/RE
№6 июнь 2016
12+

Содержание

Издание для специалистов, интересующихся технологиями компании Microsoft.

Главный редактор: **Д. Торопов** (toropovd@osp.ru)
Ответственный редактор: **Е. Петровичева**
Корректор: **Л. Теременко**
Верстка и дизайн: **О. Шуранова**
Номер также готовили: **Е. Овсянников**
Т. Евдокимова, А. Китаев, А. Федотов,
Н. Басалова, Ю. Власов, Д. Щепкин, А. Адзиев

Адрес для писем: 127254, Москва, а/я 42
Телефоны: (495) 725-4780/83, (499) 703-1854
Факс: (495) 725-4783
E-mail: windowsitpro@osp.ru

Реклама: ООО «Рекламное агентство 'Чемпионс'», тел.: (495) 725-4780,
Е. Амелехина (kam@osp.ru)

Свидетельство о регистрации средства массовой информации ПИ №ФС77-63737 от 16 ноября 2015 г.
Выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором).
Цена свободная. Выходит 12 раз в год.

ОТКРЫТЫЕ СИСТЕМЫ
Open Systems Publications

Учредитель и издатель:
ООО «Издательство «Открытые системы»
127254, Москва, пр-д Добролюбова, д. 3, строен. 3, каб. 13.
Президент **М. Е. Борисов**
Генеральный директор **Г. А. Герасина**
Директор ИТ-направления **П. В. Христов**
Коммерческий директор **Т. Н. Филина**

Подписные индексы:
Объединенный каталог «Пресса России» — 38185,
«Каталог российской прессы» — 99483.
Отпечатано в ООО «Богородский полиграфический комбинат».
142400, Московская область, г. Ногинск, ул. Индустриальная, д. 40б
Тел.: (495) 783-9366, (49651) 73179
Тираж 10 000 экз.

ИЛЛЮСТРАЦИЯ НА ОБЛОЖКЕ SHEELAMOHANACHANDRAN© (FOTOLIA.COM)

Delve Analytics:

Большой Брат или Fitbit для корпорации?

Интеллектуальные системы для анализа повседневной деятельности

Все мы неизбежно сталкиваемся с проблемой производительности труда на рабочем месте. В течение обычной рабочей недели среди совещаний и рутинных обязанностей нам порой чрезвычайно трудно бывает выкроить достаточно времени, чтобы сосредоточиться на главных вопросах. Нас отвлекает то важное текстовое сообщение, то телефонный звонок или письмо, полученное по электронной почте, а затем мы пытаемся вспомнить о деле, от которого пришлось оторваться.

Учитывая головокружительный темп работы в наш век коллективного взаимодействия, мы задаемся вопросом: как измерить эффективность работы организации? Как, с точки зрения компании, можно объединить различные способы обмена информацией и организации рабочего времени сотрудников? Как отслеживаются и в конечном итоге оцениваются цели, поставленные внутри компании? Наконец, насколько благополучно состояние компании?

В результате недавнего опроса компании Gallup выяснилось, что 47% времени, проведенного на совещании, проходит непродуктивно, и типичный сотрудник тратит 28% времени на разбор сообщений электронной почты. Эти цифры выглядят очень правдоподобно. Если подсчитать все потраченное время в течение недели, месяца или года, то легко убедиться в необходимости применения интеллектуальных систем для анализа повседневной деятельности.

В этом поможет компонент пакета Office 365, известный под названием Delve Analytics (https://products.office.com/en-us/business/explore-office-delve) и предназначенный для повышения производительности труда в компаниях. Мне приходилось слышать, как Delve Analytics называют «навигатором для корпорации».

Что такое Delve Analytics

В основе Delve Analytics лежит представление о прогнозировании таких важных бизнес-показателей, как продажи, производительность и общий уровень вовлеченности сотрудников. Анализируя ключевые запросы сотрудников, можно предсказать, например, вероятность (в процентах) достижения заданного уровня продаж. Интересная мысль.

В сентябре 2015 года компания Microsoft приобрела компанию VoloMetrix, лидирующую в области аналитики работы организаций, чтобы задействовать возможности машинного обучения, реализованные Office Graph. Благодаря этому приобретению Microsoft надеется занять собственную нишу на рынке средств повышения производительности организаций.

Основная цель Delve Analytics — помочь контролировать распределение времени в течение рабочего дня. Сколько часов в неделю вы проводите на совещаниях или сколько времени требуется, чтобы ответить на сообщения электронной почты, — это показатели, которые уже существуют в почтовом ящике Exchange Online. Знания, получаемые от Delve Analytics через специальную панель мониторинга, — представление различных показателей способом, удобным для восприятия. Delve Analytics собирает информацию о сообщениях электронной почты, совещаниях, совместной работе, продолжительности времени, отработанного вне совещаний, и сверхурочной работе.

Уникальная особенность Delve Analytics как организатора совещаний — возможность увидеть, насколько актуальны ваши совещания. Например, сколько участников отправили сообщения электронной почты получателям вне списка участников во время совещания? Сколько часов в неделю потрачено на совещания или отправку электронной почты? Сколько человек действительно прочитали отправленные сообщения электронной почты? На панели мониторинга Delve Analytics из ответов на эти вопросы формируются данные, на основе которых можно принимать решения относительно распределения вашего рабочего времени.

Как это работает

Многие действия, предпринимаемые пользователем в Office 365, такие как подготовка ответов на сообщения электронной почты, сохраняются в базе данных Office Graph. Благодаря машинному обучению Office

Graph позволяет охватить многие показатели деятельности, которые иначе были бы пропущены сотрудником, и получить уточненную оценку состояния. Office 365 Unified API позволяет проанализировать информацию и отыскать показатели, представляющие интерес. Сейчас Microsoft Graph обучается, выполняя индексацию сообщений электронной почты, файлов, бесед Yammer и Skype, чтобы поставить работу пользователя в определенный контекст через прогнозный алгоритм. Служба анализирует сигналы, поступающие от почтового ящика пользователя, и использование календаря. В результате благодаря применению Delve Analytics удается действительно учитывать себестоимость процесса и отношений для каждого пользователя.

Требования

Delve Analytics требует лицензии E5 (http://windowsitpro.com/blog/microsoft-releases-office-365-e5-plan) для всех «облачных» пользователей в клиенте Office 365. Важно помнить, что локальная активность, связанная с почтовым ящиком Exchange, не улавливается алгоритмами Delve Analytics; не поддерживается и гибридный подход. Отображаются только «облачные» почтовые ящики внутри самого клиента, а начальная фаза обнаружения при подготовке пригодных для выполнения действий данных обычно занимает несколько недель. Работа с Delve Analytics не сводится исключительно к запуску программы с последующим изучением отчетов.

Есть ли повод для беспокойства

Как уверяют представители Microsoft, данные очищаются и не привязаны к конкретным пользователям на панели отчетов. Преобладающая часть информации, выдаваемой Delve Analytics, основывается на ваших собственных действиях, но может содержать и ценную информацию о действиях, выполняемых другими сотрудниками. Каждый пользователь может включить или отключить Delve Analytics для своего почтового ящика. Группа разработчиков Microsoft заявила, что в дополнение к неперсонализированным данным Delve Analytics повышает надежность защиты конфиденциальности, предоставляя информацию о группах, только если группа достаточно велика, чтобы исключить возможность распознавания отдельных пользователей.

Похоже, Delve Analytics стала важным первым шагом к тому, чтобы помочь пользователям внутри компании повысить производительность своей работы. Управлять Delve Analytics тоже немного проще, чем IBM Watson, платформой когнитивного машинного обучения. Думаю, большинство руководителей компаний, использующих пакет Office 365, будет заинтересовано в таком продукте.

Джастин Харрис — главный архитектор решений компании Binary Tree. Занимается проектированием продуктов миграции следующего поколения. Имеет сертификаты Microsoft Certified Master для Exchange Server и Microsoft MVP для Exchange Server

Интеграция PT MaxPatrol SIEM и DeviceLock

12 апреля 2016 года, Москва. Positive Technologies и «Смарт Лайн Инк» объединили технологии для защиты корпоративных ресурсов: теперь PT MaxPatrol SIEM может автоматически подключать DeviceLock DLP Suite в качестве источника событий информационной безопасности.

«Ценные корпоративные данные могут быть скопированы с рабочих компьютеров на флеш-накопители, мобильные устройства, в «облачные» хранилища или переданы третьим лицам по электронной почте и через другие каналы. DeviceLock DLP Suite осуществляет контроль доступа к устройствам хранения и обработки данных, контроль пользовательских каналов коммуникации и фильтрацию содержимого передаваемых файлов. Подключение системы PT MaxPatrol SIEM к DeviceLock DLP Suite позволит выводить на единую панель мониторинга все необходимые корреляции от DLP-системы, что принципиально повысит оперативность реагирования служб безопасности на инциденты, связанные с утечкой информации, и позволит проводить расследования по горячим следам»,— рассказывает Сергей Вахонин, директор по решениям АО «Смарт Лайн Инк».

Доработка MaxPatrol SIEM проводилась совместно с компанией «Смарт Лайн Инк». Эксперты Positive Technologies развернули тестовый стенд системы контроля утечки данных, воспроизвели события подключения внешних носителей и подготовили расшифровку и описание событий в журналах из базы данных DLP-системы. Специалисты «Смарт Лайн» дали необходимые пояснения о типах и формате событий, генерируемых DLP-системой, и обеспечили возможность подключения к базе данных. По итогам работ были разработаны правила преобразования данных, получаемых от DLP-системы, в формат MaxPatrol SIEM. В результате доработки система мониторинга и корреляции событий информационной безопасности обеспечивает сбор информации из базы DeviceLock DLP Suite, в том числе о таких событиях, как присоединение к рабочим компьютерам флеш-накопителей, смартфонов и других устройств.

«Количество поддерживаемых источников — одна из ключевых характеристик SIEM-системы. Но заказчику важна не сама цифра, а уверенность в том, что будут поддерживаться источники событий именно его ИТ-инфраструктуры. А для российского заказчика в приоритете поддержка средств защиты информации отечественного производства. MaxPatrol SIEM уже сейчас поддерживает десятки систем отечественных производителей, и мы продолжаем расширять их перечень. Угроза утечки конфиденциальных данных всегда актуальна, и многие компании активно используют DLP-системы, в том числе и пользователи MaxPatrol SIEM. Поэтому мы начали адаптацию MaxPatrol SIEM к нюансам работы DLP-систем, в частности российского программного комплекса обнаружения и предотвращения утечек конфиденциальных и критически важных данных DeviceLock DLP Suite, широко используемого в государственных учреждениях, в финансовых, энергетических и телекоммуникационных компаниях»,— отметил Максим Филиппов, директор Positive Technologies по развитию бизнеса в России.

Помимо самой интеграции продуктов сотрудничество с компанией «Смарт Лайн Инк» позволило Positive Technologies создать методику и алгоритм расширения возможностей MaxPatrol SIEM, которые в дальнейшем будут применяться для поддержки DLP-систем других производителей.

Защита от потери данных в Exchange Server 2013

Ценная технология для некоторых компаний

Тони Редмонд

Сообщение о реализации технологии защиты от утечек данных DLP (http://technet.microsoft.com/en-us/library/jj150527%28v=exchg.150%29.aspx) в Exchange Server 2013 (в том числе Exchange Online) и Outlook 2013 не произвело на меня сильного впечатления. Мне казалось, оно не принесет особых преимуществ потребителям, а для развертывания DLP был необходим новый настольный клиент. Кроме того, технология была несовместима с Outlook Web App (OWA) и отсутствовала перспектива ее реализации на стороне мобильного клиента. В целом я пришел к выводу, что польза от DLP не очень велика. Однако в зависимости от ваших требований к технологиям защиты, это утверждение может быть спорным. Давайте рассмотрим некоторые интересные аспекты реализации данной технологии компанией Microsoft.

DLP — не новшество

Необходимость предотвратить потери данных хорошо осознается, вероятно, потому, что известно множество примеров умышленного или случайного разглашения корпоративной или персональной информации. В техническом документе компании McAfee, Data Loss by the Numbers (http://www.mcafee.com/us/resources/white-papers/wp-data-loss-by-the-numbers.pdf), приведены графические примеры потери в той или иной форме миллионов записей, хранившихся в крупных акционерных компаниях. Результатом может быть ущерб, нанесенный репутации компании, увеличение затрат на юридические услуги, потеря клиентов и почти гарантированный конфуз в глазах общественности. Поэтому защита данных — задача первоочередной важности. В прошлом основной акцент делался на возведении и поддержании традиционных барьеров безопасности. Это позволяло остановить взломщиков и мошенников, но не помогало предотвратить потери данных, происходившие по недосмотру сотрудников. Как отмечается в документе McAfee, общее количество внутренних инцидентов достигает 44%, но «большинство из них были случайными».

DLP — отнюдь не новая технология. В течение многих лет такие поставщики, как Symantec (http://www.symantec.com/products-solutions/families/?fid=data-loss-prevention), EMC (http://web.emc.com/rsa-data-loss-prevention?reg_src=website&activity_id=181829&division=rsa) и Cisco Systems (http://www.cisco.com/en/US/netsol/ns895/), предлагали решения DLP для борьбы с рас-

крытием конфиденциальных данных. Давно публикуются и технические документы на данную тему. Например, институт SANS опубликовал документ Data Loss Prevention (http://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883) в 2008 году.

В январе 2013 года Gartner опубликовала «магический квадрант» для защиты от потери данных с учетом контента (http://www.computerlinks.de/FMS/22876.magic_quadrant_for_content_aware_data_loss_prevent.pdf), в котором специалисты компании анализируют решения класса DLP в области электронной почты. Бросается в глаза отсутствие в «магическом квадранте» компании Microsoft. Версия DLP в составе Exchange 2013 — первый опыт Microsoft в этой области, естественно связанный с ошибками и недостатками, самый очевидный из которых — охват клиентов.

К преимуществам реализации Microsoft относится то, что в ней получили дальнейшее развитие следующие функции.

- Возможность переслать каждое сообщение в компании через известную контрольную точку (транспортный конвейер Exchange), в которой можно проанализировать содержимое сообщения.
- Настольный клиент с мощной функциональностью и встроенным интеллектуальным анализом информации по мере ввода текста пользователем.

Специалисты Microsoft расширили транспортные правила Exchange, чтобы выполнять проверку конфиденциальных данных, пересылаемых по транспортному конвейеру. Microsoft также предоставляет особые подсказки, чтобы пользователям было легче заметить, когда их сообщения содержат конфиденциальные данные. Подсказки от политики выглядят очень похоже на почтовые подсказки в Exchange 2010 и Outlook 2010.

Важно понимать, что DLP не предназначается для контроля над поведением пользователей и содержимым отправляемых ими сообщений. Другие инструменты, такие как транспортные правила, политики хранения и поиск с помощью функции обнаружения электронных данных, обеспечивают более явные формы соответствия требованиям. Технология DLP проектировалась для того, чтобы помочь компаниям защитить себя, не позволяя сотрудникам вводить конфиденциальную информацию, например номера социального страхования и данные кредитных карт, в неподходящие сообщения. При этом обучение пользователей является составной частью DLP. Если решение DLP помогает пользователям понять, что они совершают ошибки, то, вероятнее всего, они не допустят промаха в будущем. Предполагается, что клиенты понимают политики DLP и сигнализируют об ошибках. Теперь давайте более подробно познакомимся с реализацией DLP в Exchange 2013 и Outlook 2013.

Компоненты DLP

На клиентской стороне необходимо задействовать Outlook 2013 Professional Plus, чтобы получить следующие возможности.

- Использовать пакет XML, описывающий политику DLP, определенную для компании. Клиенты загружают пакет из серверов почтовых ящиков Exchange 2013 через каждые 24 часа. В пакете указываются типы конфиденциальных данных, которые нельзя вставлять в сообщения, и действия, предпринимаемые при обнаружении конфиденциальных данных.
- Анализировать текст по мере написания сообщения и распознавать типы конфиденциальных данных, охваченные политикой DLP. Впечатляет механизм распознавания текста, способный связывать различные его фрагменты и определять с большой долей уверенности, что части текста, соединенные вместе, представляют собой конфиденциальные данные. Например, если 16-значное число соответствует алгоритму Луна (http://en.wikipedia.org/wiki/Luhn_algorithm), то оно может быть номером кредитной карты. Если помимо этого присутствует дата, которая может быть датой истечения срока действия (например, 11/15), то это дополнительное свидетельство, что два фрагмента текста представляют собой данные кредитной карты. Наконец, если рядом указано чье-нибудь имя, то высока вероятность, что в сообщении содержится достаточная информация для снятия средств с кредитной карты.
- Отображать подсказки политики DLP, когда обнаружены конфиденциальные данные, чтобы уведомить пользователей о наличии таких данных и действиях, которые следует предпринять. Подсказка политики может отображать уведомление о невозможности отправить почтовое сообщение из-за содержащихся в нем данных или может носить рекомендательный характер (например, «вам не следует пересылать данные такого типа»). Также можно разрешить пользователям переопределять политику, запросив аргументы в пользу переопределения. Затем аргументы можно переслать вместе с информацией о сообщении менеджеру, ответственному за соблюдение корпоративных требований, который может принять решение, ознакомившись с контекстом сообщения. Например, работнику отдела кадров иногда бывает нужно пересылать сообщения, содержащие номера социального страхования. Кадровику можно разрешить переопределение, но не администратору другого отдела, который пытается отправить информацию о сотрудниках.

На стороне сервера Exchange 2013 позволяет определить политики DLP в разделе управления соответствием требованиям центра администрирования Exchange (EAC). Фундаментом EAC являются команды административной консоли Exchange, которые при желании

можно использовать для управления политиками DLP.

В сущности, политика DLP представляет собой контейнер, содержащий набор специализированных транспортных правил для проверки сообщений, пересылаемых по транспортному конвейеру. Транспортные правила появились в Exchange Server 2007. Они представляют собой важную часть системы соответствия требованиям, так как обеспечивают надежный метод анализа сообщений, пересылаемых как внутренним, так и внешним получателям. Набор условий, действий и исключений, применяемых в транспортных правилах, значительно расширен по сравнению с Exchange 2007, и в результате транспортные правила можно использовать в самых разных ситуациях. Интеграция политик DLP достигается добавлением условия «если сообщение содержит конфиденциальные данные» с целью проверки указанного типа конфиденциальных данных и действий, предпринимаемых в случае выполнения условий. Exchange 2013 обеспечивает поиск конфиденциальных данных в тексте сообщений и вложениях.

Помимо гарантии, что все сообщения будут проверены на соответствие политикам DLP, самое важное преимущество использования транспортных правил заключается в их совместимости со всеми клиентами. Даже если вы не используете Outlook 2013, можно развернуть политики DLP через транспортные правила. Работать пользователю в этом случае чуть менее удобно, но действие политики будет эффективным. Однако необходимо помнить, что ответственность за пересылку сообщений в компании должна быть возложена на почтовые серверы Exchange 2013. Транспортным серверам Exchange Server 2010 и Exchange 2007 ничего не известно о политиках DLP, а транспортные правила, реализующие политики, остаются для них невидимыми. Таким образом, любое сообщение, прошедшее через транспортный сервер нижнего уровня, пересылается без проверки. Это небольшая, но важная деталь реализации, которую необходимо учитывать в любом развертывании DLP.

Типы конфиденциальных данных

Создавая политики DLP, необходимо знать, конфиденциальные данные какого типа нужно контролировать. Вспоминается несколько широко применяемых типов данных, которые обычно не рекомендуется передавать в сообщениях. Я уже рассказал о номерах кредитных карт и номерах социального обеспечения. Хотя для кредитных карт используется общемировой формат, личные сведения (PII) и другие типы конфиденциальных данных в разных странах различаются.

Со стороны компании Microsoft было бы неразумно предоставлять каждому желающему право самостоятельно определять степень конфиденциальности данных. В этом случае неизбежны многочисленные ошибки. Microsoft предоставила набор готовых определений конфиденциальных данных (http://technet.microsoft.com/en-us/library/jj150541%28v=exchg.150%29.aspx), которые можно использовать, не задумываясь о существенных характеристиках, лучше всего описывающих форматы данных. Так, имеются определения для:

- номеров маршрутизации ABA (Американской банковской ассоциации);
- номеров кредитных карт;
- номеров социального обеспечения США;
- номеров банковских счетов Канады;
- номеров дебетовых карт ЕС;
- номеров паспортов в Австралии;
- номеров водительских лицензий в Германии.

Вероятно, со временем список типов конфиденциальных данных будет расширен и в него войдут данные, используемые в других странах.

Шаблоны DLP

Политика DLP редко охватывает единственный тип конфиденциальных данных. Обычно компаниям приходится объединять в политике DLP многочисленные типы данных. Можно создать новую политику DLP, отражающую специфические нужды компании, но Microsoft предоставляет шаблоны DLP, спроектированные таким образом, чтобы помочь строить политики DLP для типовых сценариев. Каждый шаблон содержит набор правил для проверки типов данных, которые хочет защитить пользователь.

При создании новой политики DLP можно выбрать шаблон, и Exchange подготовит новую политику, используя информацию в выбранном шаблоне. Впоследствии политику можно изменить, удалив нежелательные правила или добавив новые по мере необходимости.

Специалисты Microsoft надеются, что независимые компании предложат подходящие шаблоны DLP для определенных отраслей и условий. Затем эти шаблоны можно будет предоставить потребителям в формате XML и импортировать для создания новой политики DLP.

Рассмотрим процесс определения политики DLP с использованием стандартного шаблона, предоставляемого Microsoft. Для этого нужно выполнить шаги, охватывающие:

1. Определение защищаемых типов конфиденциальных данных.
2. Создание новой политики DLP.
3. Анализ и проверку правил политики DLP.
4. Применение политики DLP и проверку транспортных правил.
5. Аудит политики DLP.

Шаг 1. Определение защищаемых типов конфиденциальных данных

Самый простой шаг в определении любой политики — понять, для какой цели она предназначена. В данном случае требуется защитить компанию от случайного раскрытия конфиденциальных дан-