IDC TECHNOLOGY SPOTLIGHT

Интеграция и контроль рабочих мест

Январь 2013

На основе статьи Western Europe Security Software Forecast, 2012-2016 (автор Кевин Бейли, IDC № IS01U) и статьи SMB Security Competitive Best Practices Key Performance Attributes (авторы Чарльз Колоджи и Реймонд Боггс, IDC №233439)

При поддержке «Лаборатории Касперского»

В данном обзоре рассматриваются преимущества комплексных платформ для обеспечения безопасности с централизованным управлением и то, как Kaspersky Security для бизнеса соответствует требованиям IT-специалистов к простоте, эффективности и окупаемости на стратегически важном рынке продуктов для обеспечения безопасности рабочих мест.

Введение

В наши дни перед организациями стоят сложные задачи: им нужно быть начеку перед лицом постоянно эволюционирующих угроз и при этом контролировать растущее количество устройств, программ, оборудования, приложений и профилей пользователей.

Как отмечают многие обозреватели, информация – это «новая нефть»: она имеет важное значение для бизнеса, но мы воспринимаем ее как должное. И большим, и малым организациям приходится хранить как терабайты и петабайты данных в структурированных хранилищах данных и информационных центрах, так и огромное количество неструктурированных данных, таких как журналы, видео, веб-страницы и другие документы. При этом пользователи хотят иметь доступ к данным в реальном времени независимо от того, в какой форме они хранятся. И так же, как нефть, информация, о которой не заботятся должным образом, очень быстро выходит из-под контроля. Одна маленькая утечка может привести к большой беде.

Компания IDC постоянно ставит перед поставщиками решений задачу производить надежные, интегрированные, интуитивно понятные и централизованно управляемые платформы для рабочих мест. Такие платформы не только помогают организациям противостоять новым угрозам, но и защищают интеллектуальную собственность, репутацию торговой марки, коммерческую доступность, личную информацию клиентов и их лояльность.

Сложность атак

Меры по защите рабочих мест начали предприниматься еще в 80-х годах XX века, когда в мире компьютеров появились первые образцы вредоносного ПО, например, вирус Vienna. Первые вирусы занимались в основном самовоспроизводством и редко содержали вредоносный код, предназначенный для разрушения системы или кражи информации. По мере того как вредоносное ПО и вирусы приобретали все более негативные качества, талантливые программисты и разработчики начали объединяться в союзы и дискуссионные группы, задачей которых было усовершенствование защиты и противодействие угрозам. Среди первых инициатив был список рассылки под названием VIRUS L, одним из создателей которого был Евгений Касперский.

Вчерашние создатели вирусов прошли длинный путь, прежде чем превратиться в сегодняшних «хакеров-активистов» и киберпреступников, авторов специализированного вредоносного ПО, способного использовать уязвимости в корпоративных сетях и работающих в них приложениях. Современные киберпреступники в полной мере используют развитые средства коммуникации и, как следствие, возросшую доступность информации.

Угрозы в наши дни постоянно эволюционируют, принося преступникам все большие доходы и нанося предприятиям-жертвам все больший ущерб (см. таблицу 1). Вот примеры таких угроз.

- **Таргетированный фишинг.** Вместо того чтобы подвергать заражению вредоносными программами всю организацию, преступники выбирают для атаки отдельных сотрудников.
- **Троянцы-вымогатели.** Чтобы вымогать деньги у пользователей или предприятий, преступники угрожают активировать вредоносный код, встроенный в троянскую программу, или используют лжеантивирусы, предупреждающие о якобы существующих угрозах.
- **Вредоносное ПО для мобильных устройств.** Взрывной рост количества интеллектуальных мобильных устройств стимулировал появление новых видов вредоносного ПО, созданного, чтобы использовать бреши в мобильных операционных системах и приложениях. Возросшее количество устройств, используемых для работы и имеющих доступ к корпоративной сети и конфиденциальной информации, дало преступникам новые источники дохода и новые способы нанести ущерб.

Таблица 1

Динамика кибератак во всех сегментах рынка

Вирусы, черви, троянцы	Вредоносное ПО	Ботнеты	Атаки из интернета	Кражи устройств	Внутренние злоумышленники	Фишинг и социальная инженерия	DDoS-атаки
Атаки в реальном времени, атаки «нулевого дня» и комплексные таргетированные угрозы (APT) распространены сейчас и будут развиваться в будущем на абсолютно всех рынках.	За первое полугодие 2012 года количество атак на операционную систему Android возросло в три раза. В начале 2012 года была заражена считавшаяся неприступной операционная система Mac OS (Apple). Всего заражению подверглись сотни тысяч компьютеров на базе Mac OS.	9 млн ПК заражены ботнетом ZeroAccess, большая часть из них – в США.	Скрытые загрузки обходят сетевые экраны и заражают компьютеры пользователей интернета. Часть вредоносного ПО остается на компьютерах, чтобы облегчить дальнейшие атаки.	Для преступных целей постоянно ведется охота за такими данными, как идентификаторы устройств, почтовые индексы, номера телефонов, адреса, имена пользователей, типы устройств.	Агенты организованной преступности или внутренние преступники, действующие с целью кражи данных, их изменения или подделки учетных записей. Более 71% атак происходят в обычное рабочее время.	Все более значимое взаимодействие бизнеса и социальных сетей (LinkedIn, Facebook, Chatter, Yammer и т. д.) используется как средство для проведения атак при недостаточно надежном обеспечении безопасности.	Никто не застрахован от таких атак. В октябре 2012 года были обрушены веб-сайты HSBC. В августе 2012 года была нарушена работа веб-сайта Wikileaks. Появились DDoS-атаки, направленные на телекоммуникационные компании. Кроме того, запланированным атакам нередко предшествует шантаж и вымогательство.

Источники: IDC, BGR, Wired, Computer Economics, Carnegie Mellon, InfoSecurity

Разнообразие угроз свидетельствует о падении эффективности узкоспециализированных решений для обеспечения безопасности. Чтобы бороться с современными атаками, идущими в нескольких направлениях одновременно, необходимы комплексные решения, способные закрывать уязвимости как на устройствах, так и при работе с интернетом и электронной почтой. Многие руководители отделов по обеспечению безопасности пытаются справиться с ситуацией, применяя комбинации специализированных решений, что приводит к повышенной трате ресурсов, необходимых для технического обслуживания и мониторинга. Сложившаяся

ситуация поощряет «авральный» подход к безопасности после каждой атаки и увеличивает время, необходимое для разработки и внедрения нужных политик для каждого отдельного решения. Это время можно было бы потратить на оптимизацию взаимодействия с клиентами, на работу над другими коммерчески выгодными проектами и на разработку проактивной системы обеспечения безопасности.

В дополнение к традиционным атакам (через интернет, электронную почту и т.п.) теперь киберпреступники используют уязвимости в операционных системах и приложениях, для которых не были установлены исправления, в топологии аппаратного и программного обеспечения и в гостевых подключениях к бизнес-сети.

Поскольку скорость появления новых киберугроз возросла с одной в день до одной в секунду, в IDC считают, что без интеллектуального объединения функций обеспечения безопасности и системного администрирования организации будут подвержены скрытым атакам. Такие атаки могут оставаться некоторое время нереализованными, но затем стать «лазейкой» для случайных и организованных злоумышленников.

Разнообразие продуктов для обеспечения безопасности

Текущие масштабы и интенсивность атак вынуждают разработчиков защитного ПО несколько расширять свою деятельность и создавать решения для обеспечения безопасности, которые смягчают последствия внешних и внутренних атак вредоносного программного обеспечения и закрывают бреши, ведущие к утечке данных. В таблице 2 отображен весь спектр категорий расширенных средств для обеспечения безопасности, который необходимо охватить поставщикам, чтобы усилить защиту организаций. Задача усложняется при использовании в важных для бизнеса операциях виртуальных сред, программного обеспечения как услуги (SaaS), облачной и локальной моделей представления данных, а также при использовании стратегий оптимизации бюджета.

Таблица 2

Категории средств обеспечения безопасности

Защита от вредоносного ПО	Сеть	Интернет	Предотвращение утечек данных	Шифрование	Сетевой экран
Контроль устройств	Управление приложениями	Управление установкой исправлений	Управление мобильными устройствами	Управление уязвимостями	Совместная работа
Хранение данных	Виртуализация	Управление обеспечением безопасности	Электронная почта	Управление политиками	Развертывание систем

Средства для обеспечения безопасности из каждой подкатегории, отображенной в таблице 2, укрепляют безопасность предприятия. Но все же это отдельные продукты, поэтому они требуют больше ресурсов и значительно повышают нагрузку на специалистов службы IT-безопасности. Внедрение этих продуктов по отдельности приводит к следующему:

- многократное развертывание и настройка;
- многократная установка обновлений;

- необходимость навыков работы с многообразным ПО;
- работа с многочисленными консолями управления;
- множество механизмов управления политиками;
- многократное выполнение задачи проверки;
- использование многочисленных профилей.

Сложность – это не просто враг в борьбе за безопасность. Сложность сдерживает любые инициативы по внедрению более отзывчивой проактивной защиты, способной одновременно защитить и гипермобильных работников, и активы (устройства, данные и сотрудников) от атак, а также предотвратить финансовый и репутационный ущерб.

Сотрудники службы IT-безопасности – обычные люди. Им приходится постоянно учиться, чтобы упростить управление несколькими операционными системами с неочевидными различиями, управление политиками, в которых используются различные таблицы приоритетов, чтобы тратить меньше времени на установку множества исправлений для защиты от уязвимостей. В то же время им необходимо поддерживать управляемую топологию архитектуры.

Рабочее место: от отдельных решений к единой платформе

Обеспечение безопасности рабочих мест всегда было последней линией обороны от вредоносного программного обеспечения и других угроз. В наши дни, когда работники стали значительно мобильнее, решения для обеспечения безопасности рабочих мест стали главным средством защиты.

Для эффективного обеспечения безопасности необходимо сочетать надежные продукты, квалифицированный персонал и оптимальные процессы. При выборе продуктов приходится внимательно изучать их, чтобы удостовериться, что это действительно платформы, а не собранные вместе так называемые «интегрированные» предложения, названные «решением» или «пакетом».

- **«Решение»** в IT-терминологии всегда скептически рассматривалось как способ объединения нескольких обычных (часто ресурсоемких) продуктов и консультационных услуг для решения известных проблем организации. При использовании «решений» к работе привлекаются консультанты из сторонних организаций, знающие, как решить проблему. Они покидают проект по его завершении. Их можно снова привлечь к работе над проектом за дополнительные деньги, если впоследствии возникают какие-либо (часто связанные с ранее решенными) проблемы из-за недостатка квалификации у штатных технических специалистов и специалистов по обеспечению безопасности.
- **«Пакет»** традиционно объединяет в себе несколько продуктов, предназначенных для решения определенной категории проблем, таких как управление обеспечением безопасности, защита рабочих мест или защита мобильных устройств. Пакеты позиционируются как простой и удобный способ продажи и поставки комплексного предложения для решения той или иной категории задач. «Врожденная» проблема пакетов состоит в том, что обычно они представляют собой просто набор продуктов без средств централизованного управления. Пакеты не обладают полностью интегрированными средствами взаимодействия и интеллектуальной архитектурой.

В полностью интегрированных, объединенных в платформу решениях каждый функциональный компонент максимально оптимизирован, при этом использование ресурсов

минимально. Платформенная архитектура обеспечивает взаимодействие и долговременное использование продуктов, а также корректное применение политик безопасности.

IDC считает, что поставщикам средств обеспечения безопасности следует активно разрабатывать платформы для обеспечения безопасности рабочих мест, чтобы дистанцироваться от традиционных технологий разработки решений или пакетов и убедить заказчиков в следующих преимуществах платформ:

- Единый код, позволяющий сократить эмуляцию, трансляцию или создание «мостов» между блоками кода.
- Единая система управления политиками, заданная для всех функций платформы.
- Единая система управления для обеспечения безопасности рабочих мест на всех имеющихся (и будущих) устройствах.
- Единая консоль для контроля, мониторинга и восстановления системы обеспечения безопасности до нужного состояния.

Удобство развертывания, управляемость и объединенная архитектура – это важные факторы при внедрении сложных систем, независимо от того, интегрированы ли они или просто объединены. Поэтому поставщикам следует включать в свои продукты следующие функции:

- Автоматизированные мастеры установки, позволяющие пользователям сразу же начать использование продуктов, что обеспечивает быструю окупаемость.
- Расширенные параметры настройки, позволяющие адаптировать продукты к конкретным потребностям пользователей и внешним угрозам.

В IDC считают, что сочетание надежности платформ для обеспечения безопасности рабочих мест и возможности быстрого их внедрения позволит небольшим организациям достичь высокой степени безопасности, характерной для крупных предприятий с их бюджетами и ресурсами.

Преимущества платформенной архитектуры для рабочих мест

Платформенная архитектура для рабочих мест сочетает в себе функции защиты и централизованного системного администрирования. Такой подход создает среду, способную противостоять растущим угрозам, а также справляться с внутренними изменениями в составе персонала, коммерциализации и технологиях. Любая платформа должна предоставлять возможность повторного использования программного кода, а также поощрять использование API для подключения к совместно работающим системам обеспечения безопасности и другим системам. Нацеленная на борьбу с комплексными таргетированными угрозами (APT) и совершенствование технологии, платформенная архитектура для рабочих мест должна предоставлять следующие преимущества:

- **Обнаружение вредоносного ПО.** Киберпреступники разрабатывают все более сложное вредоносное ПО, нацеленное на устройства, приложения и веб-сайты. Среди прочих методов преступники используют самомодифицирующийся полиморфный и параморфный код, который собирает нужную информацию до перезаписи загрузочных файлов с целью предотвращения перезагрузки системы. Чтобы ограничить использование уязвимостей, продукт на базе единой платформенной архитектуры может обнаруживать движение и присутствие кода на устройствах, в рамках компании или даже в нескольких странах с помощью методов эвристического и поведенческого анализа, белых списков и репутационного метода.

- **Управление устройствами.** В организациях любых размеров для работы все шире используются личные устройства. Единая платформенная архитектура гарантирует, что на всех корпоративных и личных устройствах будут использоваться приложения, соответствующие принятому стандарту обеспечения безопасности.
- **Контроль информации.** Корпоративная информация – важный актив и привлекательная цель для преступников. Возможность отслеживать использование, перемещение и хранение данных позволяет полностью контролировать их. Кроме того, можно контролировать, где, когда и как используются данные.

Социальная инженерия, наивность пользователей, кража и потеря устройств, обмен информацией – это всего лишь несколько видов рисков, которым подвергаются корпоративные данные. Только интегрированная платформенная архитектура может поддерживать единую систему администрирования, способную обеспечить фундаментальный процесс обеспечения безопасности, включающий применение политик, шифрование (автоматическое или по требованию) и разделение личных и корпоративных данных на мобильных устройствах.

Kaspersky Security для бизнеса

Продукт Kaspersky Security для бизнеса позволяет администраторам наблюдать, контролировать и защищать IT-среду с помощью средств и технологий неразрушающей многоуровневой архитектуры. Kaspersky Security для бизнеса работает на единой кодовой базе облачной и локальной моделей.

Основные возможности продукта:

- Прогрессивная защита рабочих мест, доступа в интернет, файловых серверов, мобильных устройств, виртуальных устройств и приложений, управление изменениями IT-архитектуры и коммерческим разнообразием.
- Шифрование на уровне дисков и файлов (FDE и FLE) с использованием алгоритма AES-шифрования органично интегрировано в технологии защиты от вредоносного программного обеспечения.
- Обеспечение безопасности мобильных устройств, выходящее за пределы базовых функций управления ими, дает возможность «контейнеризации» данных и приложений, удаленной установки приложений и блокирования устройств.
- Обеспечение безопасности электронной почты и интернет-шлюзов, защита серверов Microsoft Exchange, Lotus Notes и Lotus Domino, Sendmail, Qmail, Postfix и Exim, а также автоматическое удаление вредоносных и злонамеренных программ в трафике протоколов HTTP(S), FTP, SMTP и POP3.
- Управление уязвимостями путем интеграции функций системного администрирования для управления компьютерами на уровне операционной системы, мониторингом IT-инфраструктуры и установкой исправлений.

Ключевое отличие, органично разработанное на кодовой базе «Лаборатории Касперского», – это возможность реализовать интеграцию и контроль на единой платформе.

- Kaspersky Security Center предоставляет администраторам возможность осуществлять мониторинг сети, контроль и защиту устройств и работы пользователей в едином окне, управляя использованием функций продукта на виртуальных, физических и мобильных устройствах из единой консоли. Комплексная система применения политик и функции

формирования отчетов о состоянии дополняют список шагов на пути к стабильной безопасности.

- Инструменты контроля рабочих мест усилены технологией защиты от вредоносного программного обеспечения, разработанной «Лабораторией Касперского», что позволяет создать многоуровневую систему обеспечения безопасности, включающую следующие возможности:
  - **Контроль программ и динамические белые списки.** Служит для разрешения работы программ, работающих в сети или на устройствах пользователя, их блокирования и управления ими.
  - **Веб-Контроль.** Служит для ограничения (например, по времени) или запрета доступа в интернет с рабочих мест.
  - **Контроль устройств.** Используется для применения политик использования внешних устройств по типам устройств, серийным номерам, пользователям, а также способу подключения (не только USB или CD). Чтобы применять политики в рамках всей организации, контроль устройств интегрирован с Active Directory.

Проблемы при использовании платформ интеграции и контроля рабочих мест

Внедрение полностью интегрированных централизованно управляемых архитектур для обеспечения безопасности рабочих мест требует согласования с существующими, часто разрозненными политиками и процедурами. Интегрирование – небыстрый процесс. Если при этом не используется интуитивно понятная простая консоль и «прозрачные» инструменты контроля и защиты рабочих мест, то может потребоваться дополнительное обучение администраторов, конечных пользователей, а также изменение существующей архитектуры. В этом случае краткосрочный успех ограничен имеющимися в организации знаниями и межфункциональной деловой бюрократией.

Решению «Лаборатории Касперского» необходимо доказать простоту единого управления политиками для организаций, в которых должны использоваться одновременно различные политики безопасности. Законодательство и стандарты в области защиты данных могут сильно отличаться в разных регионах и отраслях промышленности, что делает простую систему управления политиками жизненно важным фактором успеха для администраторов, работающих в этих условиях.

По данным «Лаборатории Касперского», она первой на рынке предложила такую платформенную архитектуру, хотя существуют еще несколько других поставщиков, предлагающих похожие решения, но с меньшим набором продуктов. «Лаборатория Касперского» заявляет, что ее подход с использованием единой платформы будет полезен организациям любых размеров, от очень маленьких до крупных предприятий. В частности, преимущества могут получить малые и средние организации, так как «Лаборатория Касперского» помогает внедрять технологии комплексного обеспечения безопасности, которые ранее были доступны только большим предприятиям. Крупные компании выигрывают от сочетания знакомых технологий обеспечения безопасности с намного более простым управлением и гармоничной платформой.

В настоящее время растет важность решений категории «Управление информацией и событиями в области безопасности» (Security Information & Event Management, SIEM) для обеспечения безопасности IT-инфраструктур любого типа. Отсутствие предложений «Лаборатории Касперского» в этой области требует интеграции Kaspersky Security для бизнеса с решениями конкурентов или поставщиков SIEM, таких как IB'QI или ArcSight компании HP.

Заключение

За последние два-три года организации подвергались растущему числу атак, с которыми можно справиться с помощью интегрированных платформ для обеспечения безопасности. Поставщики ответили на это созданием работающих, но зачастую разрозненных или сложных в управлении продуктов в виде решений или пакетов, которые охватывают весь спектр угроз, но не соответствуют потребностям в интеллектуальной интеграции и централизованном управлении.

Эволюция предложений по безопасному управлению данными и угрозами, основанных на платформах, дает организациям возможность проактивно управлять защитой от целенаправленных, фишинговых и расширенных атак. При этом бюджет не должен становиться ограничивающим фактором. Напротив, следует направить значительные средства на внедрение платформ для обеспечения безопасности рабочих мест, удовлетворяющих потребностям организаций.

Консьюмеризация IT, Web 2.0 и высокая степень мобильности сотрудников – новое слово в деловой практике. Поэтому, чтобы внедрить технологии обеспечения безопасности и поддерживать высокий уровень защиты, администраторам потребуется пересмотреть действующие инфраструктуры и спланировать миграцию на платформенные архитектуры.

В компании IDC считают, что для предотвращения атак необходима защита всех рабочих мест и возможных направлений атак (физические, виртуальные и мобильные устройства, а также облака) на базе единой платформы с единой консолью управления. Kaspersky Security для бизнеса предлагает интеграцию и централизованное управление, что способствует успеху «Лаборатории Касперского» на сегодняшнем рынке.

Глобальная штаб-квартира: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com