6 ШАГОВ НАВСТРЕЧУ БЕЗОПАСНОСТИ ВЕБ-ПОЛЬЗОВАТЕЛЕЙ

Станислав Михайлов

Директор по имплементации решений Trustwave

Trustwave®
Smart security on demand

КРАТКАЯ СВОДКА

1. Проблемы и угрозы в области безопасности, решаемые шлюзом SWG
2. Проблемы в сфере коммерческой деятельности, устраняемые шлюзом SWG
3. 6 рекомендаций по наращиванию возможностей шлюза SWG
4. Новое управляемое облачное решение SWG компании Trustwave

Trustwave®

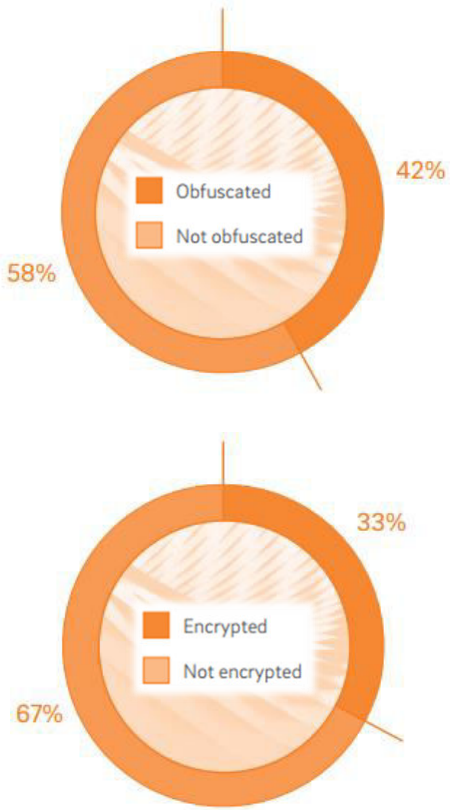
ПРОБЛЕМЫ И УГРОЗЫ В ОБЛАСТИ БЕЗОПАСНОСТИ, РЕШАЕМЫЕ ШЛЮЗОМ SWG

Trustwave®

ПРОБЛЕМЫ В ОБЛАСТИ БЕЗОПАСНОСТИ, РЕШАЕМЫЕ ШЛЮЗОМ SWG

Объемы неизвестного/нового вредоносного ПО

- Хакеры **автоматизируют процессы перекомпиляции, обфускации и шифрования вредоносного ПО**, делая невозможным его обнаружение ни по сигнатурам, ни методами статического анализа.
  - В прошлом году **42%** вредоносного ПО использовало обфускацию.*
  - **33%** вредоносного ПО использовало шифрование.*
- AV-Test.org **регистрирует >390 тыс. вредоносных программ в день.** Другие исследователи оценивают их количество примерно в 1 миллион в день.**



*Отчет по всемирной безопасности компании Trustwave за 2016 г.

**https://www.av-test.org/en/statistics/malware/

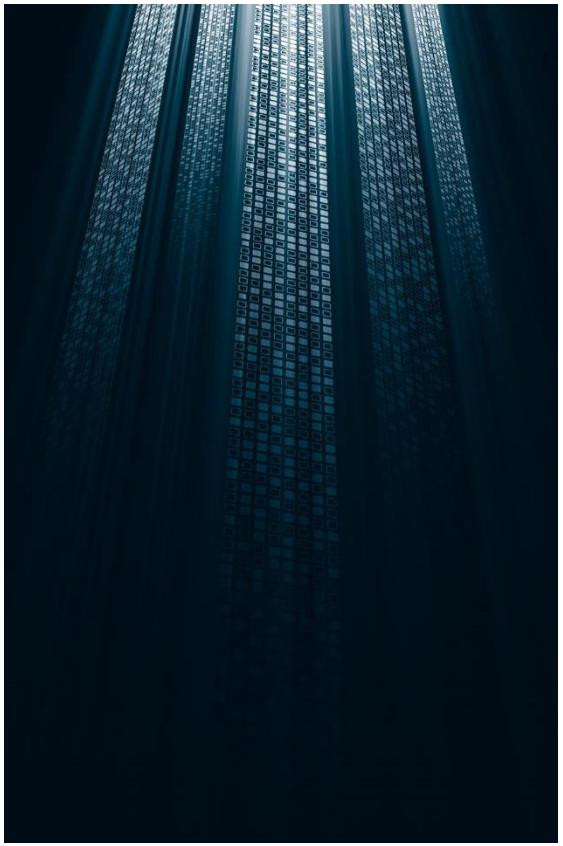
Trustwave®
Smart security on demand

ПРОБЛЕМЫ В ОБЛАСТИ БЕЗОПАСНОСТИ, РЕШАЕМЫЕ ШЛЮЗОМ SWG

Динамические угрозы: Вредоносное ПО претерпело изменения и научилось обходить статические сканеры

- **Вредоносное ПО с разделением кода** размещает свои фрагменты во многих частях веб-страницы так, чтобы исключить обнаружение этих отдельных фрагментов.
- **Динамическое вредоносное ПО** выполняет самоассемблирование, обнаружив среду с привлекательными целями.
  - Иногда во избежание обнаружения программы ее исполнение откладывается, если имеются признаки работы в виртуальной среде (например, в тестовой среде типа sandbox).
- Статический анализ зачастую не способен распознать компоненты, особенно при использовании дополнительного шифрования.

- **Результат:** Вредоносное ПО проходит через большинство шлюзов веб-безопасности (SWG).

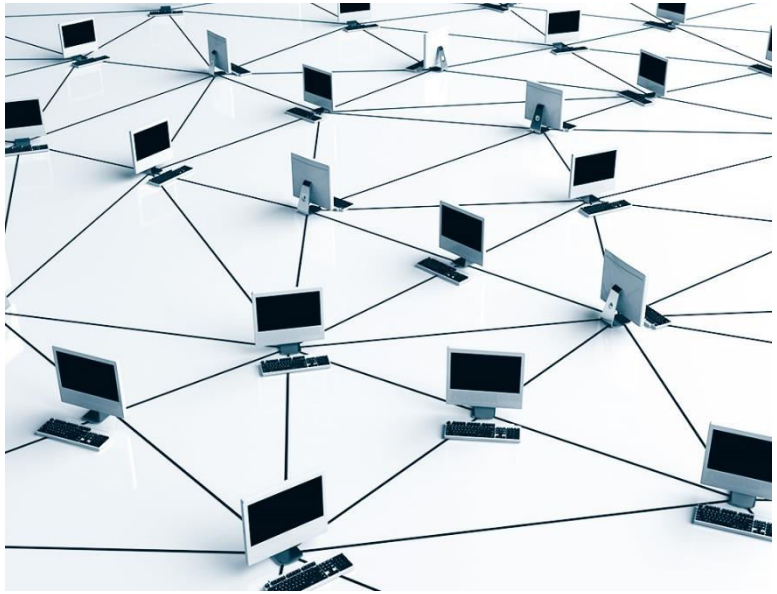


Trustwave®
Smart security on demand

ПРОБЛЕМЫ В ОБЛАСТИ БЕЗОПАСНОСТИ, РЕШАЕМЫЕ ШЛЮЗОМ SWG

Защита распределенных пользователей

- Развертывание и управление устройствами в каждом подразделении/филиале/удаленном/региональном офисе может быть дорогостоящим и требовать значительных трудозатрат.
- Ретрансляция всего трафика может создавать задержки и дополнительные расходы.
- Мобильные пользователи ноутбуков обычно используют прямое подключение к Интернету.



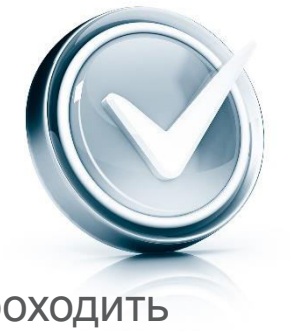
Trustwave®
Smart security on demand

ПРОБЛЕМЫ В СФЕРЕ КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ, УСТРАНЯЕМЫЕ ШЛЮЗОМ SWG

Trustwave®

ОПТИМИЗАЦИЯ SWG

Самопроверка



- Как вы думаете, позволяет ли ваш действующий шлюз SWG проходить через него вредоносному ПО?
- Беспокоит ли вас, что ваши пользователи загружают программы-вымогатели?
- Предпочли бы вы пресечение проникновения вредоносного ПО на уровне шлюза, а не на настольном компьютере?
- Имеются ли у вашего устаревшего шлюза SWG функции безопасности, которые не используются из-за чрезмерной трудоемкости их настройки?
- Нуждаетесь ли вы в дополнительной помощи специалистов в области безопасности?
- Есть ли в вашей организации филиалы, непосредственно подключенные к Интернету?
- Часто ли обновлению вашего шлюза SWG (или UTM-политик шлюза SWG) препятствует недостаток выделенных средств, опыта или времени?

Чем больше ответов «Да» на вопросы, тем больше поводов для улучшения.

Trustwave®
Smart security on demand

6 РЕКОМЕНДАЦИЙ ПО НАРАЩИВАНИЮ ВОЗМОЖНОСТЕЙ ШЛЮЗА SWG

Trustwave®

1. АНАЛИЗИРУЙТЕ ИМЕЮЩИЕСЯ ОТЧЕТЫ

Отмечайте, о чем в них сообщается, а о чем умалчивается

- Как часто вы получаете срочные предупреждения?
  - Если их становится слишком много, ваша команда начинает игнорировать их или не справляется с эффективной обработкой.
  - Если их слишком мало, то, вероятно, ваш шлюз пропускает новые угрозы.
  - В прошлом году 34,2% ПК подверглись хотя бы одной атаке.*
- Наблюдаются ли резкие изменения загрузки каналов?
  - Это может быть признаком как обхода политики пользователями, так и скрытного вывода данных вредоносным ПО.

*https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/

Trustwave®
Smart security on demand

2. ВЗВЕШЕННОСТЬ ПОЛИТИКИ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ

Средства управления приложениями – ваши союзники

- Социальные сети, сетевые накопители данных подвергают опасности данные и могут отрицательно сказаться на производительности.
  - Но многие веб-сайты являются вашими рабочими инструментами, повышая производительность труда работников.
- Поэтому не ограничивайтесь только «запретами» или «разрешениями».
  - Это приводит к жалобам со стороны пользователей, возникновению слабых мест в системе безопасности, или к тому и другому.
- В полной мере используйте возможности детализации, обеспечиваемые вашим шлюзом SWG.

Trustwave®
Smart security on demand

2. ВЗВЕШЕННОСТЬ ПОЛИТИКИ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ

Детализация – ваш помощник

- Примеры:
  - Сделайте приложения социальных сетей доступными только для чтения (блокировать новые посты, изображения или видео) или просто заблокировать обмен сообщениями в чатах.
  - Заблокируйте выгрузку в любые неутвержденные облачные хранилища, но разрешите загрузку для упрощения совместной работы с коллегами и партнерами.
  - Запретите размещение видеосюжетов и комментариев на портале YouTube.
- Пресекайте деятельность работников, снижающую производительность их труда, подвергающую данные непреднамеренным угрозам или связанную со скрытным выводом данных.

Trustwave®
Smart security on demand

3. ЗАБЛОКИРУЙТЕ ИСХОДЯЩЕЕ ВРЕДОНОСНОЕ ПО

Зачастую это работает надежнее блокировки входящего ПО

- Блокировка «звонков домой» вредоносного ПО может оказаться более легкой задачей.
  - Многие вредоносные программы используют одинаковые команды и средства управления.
  - Блокируется доступ к командному серверу, генерируется предупреждение для проверки машины.

Поступают ли к вам предупреждения безопасности при попытке ваших машин выгрузить информацию по этим URL-адресам?

Trustwave®
Smart security on demand

4. ОХВАТИТЕ ФИЛИАЛЫ И УДАЛЕННЫЕ ОФИСЫ

...И мобильные ноутбуки

Три основных варианта:

1. Выполняйте ретрансляцию всего трафика на центральное устройство.
   - Громоздко, дополнительные затраты и задержки, полоса пропускания, жалобы пользователей.
2. Разместите устройства на каждом предприятии.
   - Еще большие расходы на закупку, развертывание и сопровождение.
3. Используйте преимущества облачной платформы SWG.
   - Относительная эффективность для расположенных на удалении офисов и мобильных пользователей может вносить задержки, и, возможно, потребуется подписка.

Мобильные ноутбуки могут использовать агента для упрощения перенаправления на устройство или к облачному сервису.

Trustwave®
Smart security on demand

5. МАКСИМАЛЬНО НАРАЩИВАЙТЕ АДМИНИСТРАТИВНЫЙ ОПЫТ И КОНЦЕНТРАЦИЮ УСИЛИЙ

Навыки укрепляют вашу безопасность и сокращают ваши затраты

- 1. Изучите свое конкретное решение SWG.
  - Как сделать так, чтобы оно выполняло все изложенные выше функции для реализации защиты, разрешений, политик для отдельных пользователей/групп/времени суток, средств контроля приложений, производительности и т. п.
- 2. Станьте специалистом по веб-безопасности.
  - Ознакомьтесь с основными принципами и методами обеспечения безопасности, своевременно изучайте самые последние и изощренные угрозы, знайте ситуацию с угрозами, освойте составление правил безопасности, имейте представление о том, как политика может усилить или ослабить безопасность.
- 3. Определите пороговые значения, чтобы обеспечить фильтрацию и задание приоритетов для ответных действий.

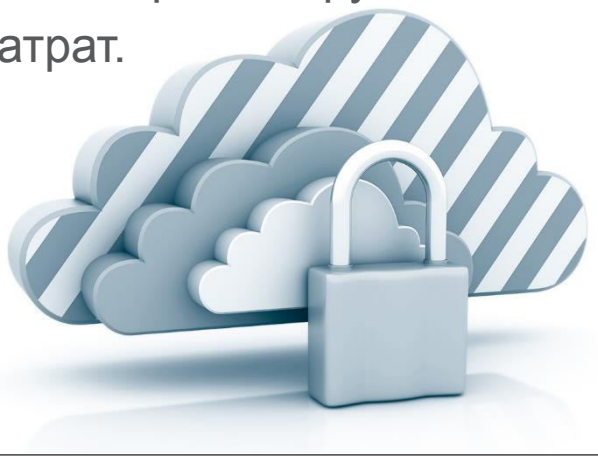
Если все это вам не подходит, обратитесь за помощью к сторонней организации.

Trustwave®
Smart security on demand

6. РАССМОТРИТЕ ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ УПРАВЛЯЕМОГО ОБЛАЧНОГО РЕШЕНИЯ SWG

Это решает множество проблем с оптимизацией

- Охватывает мобильные ноутбуки и удаленные офисы без установки дополнительного оборудования или ретрансляции трафика.
- Оптимально использует сетевые интеллектуальные ресурсы.
- Правила безопасности обновляются целой коллегией специалистов.
- Обновление политики безопасности может проводиться без ущерба для безопасности.
- Значительная экономия на персонале с учетом дефицита специалистов по безопасности на рынке труда.
- Сокращение капитальных затрат.



Trustwave®
Smart security on demand

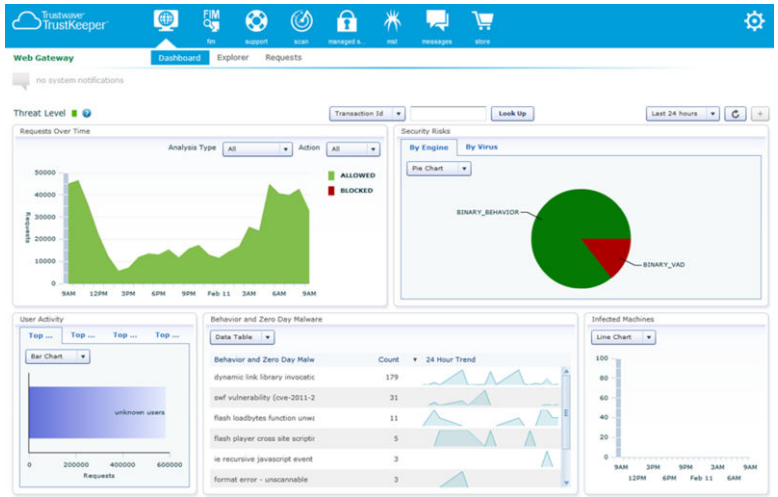
НОВОЕ УПРАВЛЯЕМОЕ ОБЛАЧНОЕ РЕШЕНИЕ SWG КОМПАНИИ TRUSTWAVE

Trustwave®

ПРЕДСТАВЛЯЕМ...

Управляемое облачное решение Secure Web Gateway компании Trustwave

- Что обеспечивает управляемое облачное решение Secure Web Gateway компании Trustwave распределенным предприятиям:
  - Действенное и простое в приобретении средство защиты в режиме реального времени от адресного вредоносного ПО.
  - Строгое исполнение политик.
  - Высокая эффективность эксплуатации.



Trustwave®
Smart security on demand

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

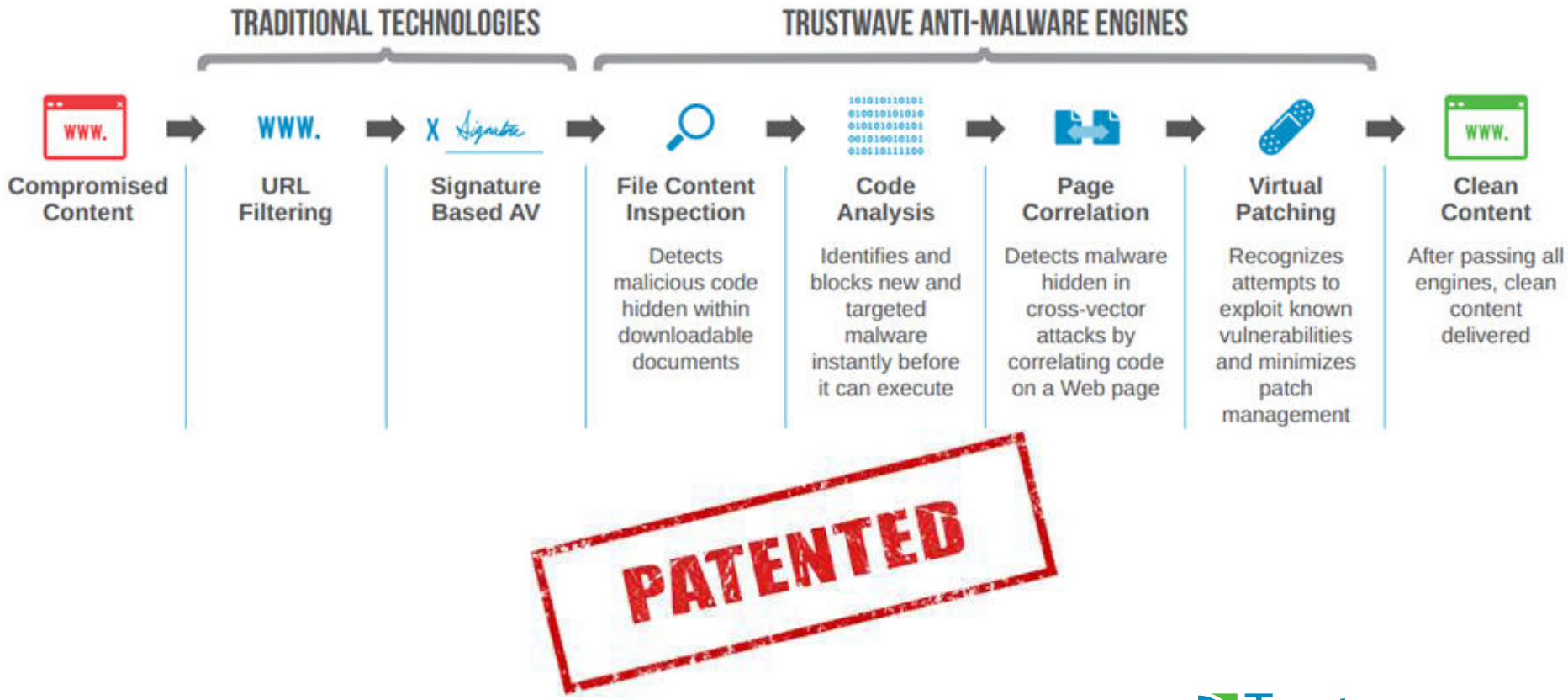
Управляемое облачное решение Secure Web Gateway компании Trustwave

- Отсутствие необходимости в аппаратуре и полная управляемость.
- Расширяет область применения патентованной технологии механизма перехвата вредоносного ПО компании Trustwave.
  - Пресекает в режиме реального времени действие вредоносного ПО «нулевого дня».
- Многопользовательская облачная платформа позволяет охватить любое количество объектов без физической аппаратуры.
  - Более широкий охват, ускоренное развертывание и меньшие капитальные затраты.
- Управляемая услуга развертывает SWG-защиту и осуществляет сопровождение политик для поддержания их высокой эффективности.
  - Сокращает затраты на средства ИТ и количество проблем.
  - Единственное решение с **гарантией нулевого уровня вредоносного ПО.**

Trustwave®
Smart security on demand

ЗАПАТЕНТОВАННАЯ ТЕХНОЛОГИЯ

Блокировка с первого раза нового вредоносного ПО



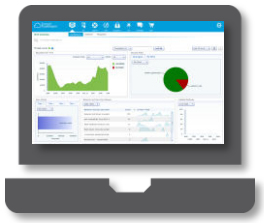
Trustwave®
Smart security on demand

УПРАВЛЯЕМАЯ МНОГОПОЛЬЗОВАТЕЛЬСКАЯ ОБЛАЧНАЯ ПЛАТФОРМА

Однократная аутентификация SAML

Управление политикой компанией Trustwave

Ближайшее облако Сканирующие серверы

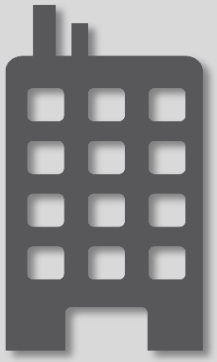


Портал и средства составления отчетов для заказчика

Серверное оборудование для больших массивов данных

Факультативный клиент конечной точки для мобильных ноутбуков

Ближайшее облако Сканирующие серверы



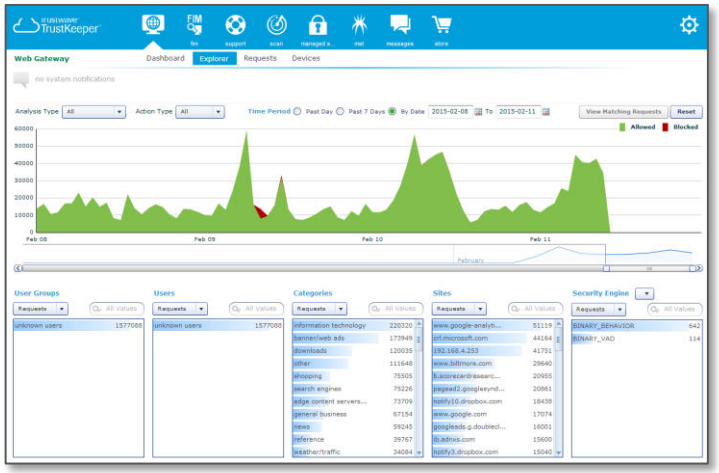
Главный офис
Штаб-квартира
Факультативный прокси-сервер стороннего поставщика для организации прокси-цепочки на любом объекте

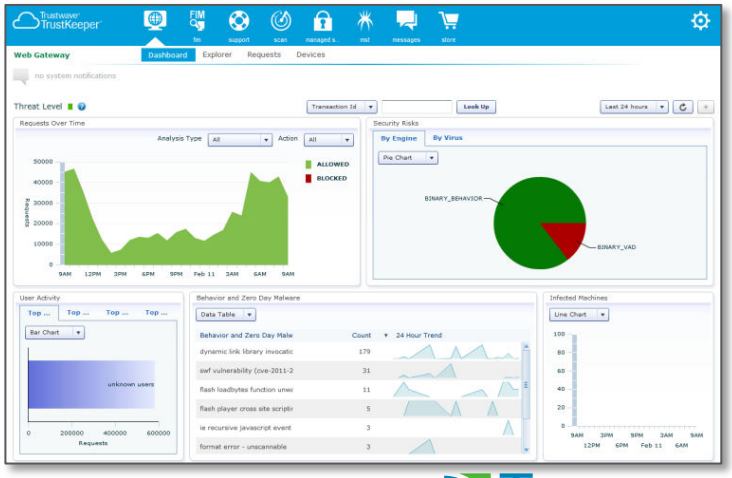
Филиалы компании
Без необходимости установки аппаратных устройств в офисе

УПРАВЛЯЕМОЕ ОБЛАЧНОЕ РЕШЕНИЕ SECURE WEB GATEWAY КОМПАНИИ TRUSTWAVE

Преимущества решения

- Способно справляться с большими объемами нового вредоносного ПО.
- Обнаруживает новое динамическое и обфусцированное вредоносное ПО.
- Блокирует вредоносное ПО





Trustwave®
Smart security on demand

ЕДИНСТВЕННОЕ РЕШЕНИЕ SWG С ГАРАНТИЕЙ НУЛЕВОГО УРОВНЯ ВРЕДОНОСНОГО ПО

Управляемая служба защиты от вредоносного ПО

- Наша патентованная технология, работающая под управлением наших специалистов, обеспечивает такую стабильность работы, что мы действительно гарантируем получение результатов.
  - Использует рекомендуемую нами политику (средний уровень безопасности) и управляемые услуги.
  - В случае доказанного проникновения вредоносного ПО через наш шлюз SWG мы предоставляем вам дополнительный бесплатный месяц управляемых услуг по защите от вредоносного ПО, до одного раза в квартал.
- Ни один из поставщиков не верит настолько в свой шлюз SWG, чтобы предоставлять такую гарантию.

«...в наше время, когда все утверждают, что нарушения и проникновение неизбежны, отрасль защиты от вредоносного ПО готова предоставить определенные гарантии». *

ZERO MALWARE GUARANTEE

Trustwave®
Smart security on demand

*Адриан Санабриа, Отчет исследовательской группы 451 «Компания Trustwave блокирует поступление вредоносного ПО с веб-сайтов, гарантируя возврат денег в случае неудачи», июнь 2014 г., https://451research.com/report-short?entityId=82103&referrer=marketing

ОБЗОР: 6 РЕКОМЕНДАЦИЙ ПО НАРАЩИВАНИЮ ВОЗМОЖНОСТЕЙ ШЛЮЗА SWG

Сокращение количества случаев загрузки вредоносного ПО

1. Анализируйте имеющиеся отчеты
2. Взвешенность политики с точки зрения безопасности и производительности
3. Заблокируйте исходящее вредоносное ПО
4. Охватите филиалы и удаленные офисы
5. Максимально наращивайте административный опыт и концентрацию усилий
6. Рассмотрите возможность применения управляемого облачного решения SWG

Trustwave®
Smart security on demand

У КОГО ЕСТЬ ВОПРОСЫ?

www.trustwave.com

@trustwave

infosales@trustwave.com

Trustwave®

Smart security on demand