Спецификация

Symantec Web Isolation

Надежная защита от угроз с помощью шлюзов безопасного доступа

Краткий обзор

Проблема:
Необходимо защитить пользователей от вредоносного кода и фишинга со стороны неклассифицированных и потенциально опасных веб-сайтов, не применяя чрезмерную блокировку доступа.

Решение:
Symantec Web Isolation (Fireglass) и шлюзы безопасного доступа.

Преимущества:

- Безопасный доступ к неклассифицированным и потенциально опасным веб-сайтам.
- Продуктивность сотрудников не ограничивается избыточными запретами.
- Руководители и привилегированные пользователи, работающие с конфиденциальными документами и являющиеся излюбленной мишенью киберпреступников, могут безопасно просматривать веб-сайты.
- Защита от раскрытия корпоративных учетных данных на вредоносных веб-сайтах.
- Блокировка сложных вредоносных программ и целенаправленного фишинга помогает не стать распространителем инфекции.

Критические векторы атаки: неклассифицированные и потенциально опасные сайты

Специалисты по информационной безопасности ежедневно отражают атаки злоумышленников, пытающихся взломать периметр защиты и украсть ценную информацию. Согласно отчету об угрозах безопасности в Интернете, публикуемому компанией Symantec, более 90 % таких атак начинаются с веб-сайтов и сообщений электронной почты. В распоряжении киберпреступников имеется обширный арсенал вредоносных программ и социотехник, направленных на заражение устройств и сетей, зачастую путем обмана пользователей и заманивания их на мошеннические веб-сайты.

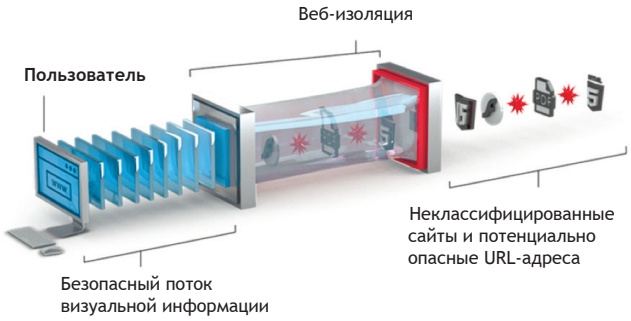
Ежедневно на свет появляются миллионы новых интернет-хостов — доменов, поддоменов и IP-адресов. Подавляющее большинство из них просуществуют менее суток и исчезнут так же быстро, как и появились. Результаты анализа свидетельствуют о том, что большая часть таких хостов создается с легитимной целью, однако многие являются инструментами в руках хакеров. Такие сайты — как добропорядочные, так и вредоносные — не классифицируются и не анализируются должным образом системами веб-фильтрации и анализа угроз, поскольку они не обладают сколько-нибудь осмысленной репутацией. Добавьте в этот список веб-сайты, которые были классифицированы как потенциально опасные, и вы поймете, с насколько сложным ландшафтом приходится иметь дело специалистам по ИБ.

Некоторые организации предпочитают полностью блокировать веб-сайты, которые не имеют классификации или были отнесены к категории потенциально опасных. Обычно это приводит к чрезмерной блокировке доступа сотрудников в Интернет, поскольку под действие таких политик попадают и многие легитимные сайты. Другие полагаются на удачу и разрешают доступ к таким сайтам, чтобы не мешать сотрудникам выполнять их рабочие обязанности, однако это делает организацию излишне уязвимой. Уязвимость становится особенно опасной в случае привилегированных пользователей, обладающих расширенными правами доступа и часто хранящими на своих компьютерах конфиденциальную информацию.

Веб-изоляция: свободный доступ к веб-сайтам, защита привилегированных пользователей и отражение атак фишинга

Технология веб-изоляции решает проблему безопасного доступа к неклассифицированным и потенциально опасным веб-сайтам. Наилучших результатов в этой области добилась компания Fireglass, недавно приобретенная Symantec для усиления портфеля корпоративных решений в сфере безопасности.

Идея веб-изоляции заключается в создании безопасной среды исполнения между пользователями и веб-сайтами. В браузеры пользователей отправляется только безопасный поток визуальной информации, а угрозы из Интернета никогда не попадают на пользовательские устройства.



С сочетании с продуктами Symantec ProxySG, ASG и VSWG технология веб-изоляции формирует изолирующий слой, который в режиме реального времени защищает пользователей от угроз со стороны неклассифицированных сайтов и потенциально опасных URL-адресов.

Механизм изоляции также может применяться для дополнительной защиты привилегированных пользователей, обладающих доступом к конфиденциальной информации и критически важным системам. Весь веб-трафик таких пользователей может направляться в среду изоляции, что позволяет защитить их от угроз, распространяемых с веб-сайтов.

Кроме того, продукт Symantec Web Isolation помогает бороться с фишингом, «обезвреживая» в электронной почте все ссылки на вредоносные сайты. Изолированные сайты не могут передать вредоносные программы, программы-вымогатели и другие опасные файлы на компьютер получателя электронного письма. Дополнительно Symantec Web Isolation может предотвращать отправку пользователями корпоративных учетных данных и другой конфиденциальной информации на такие веб-сайты, поскольку отображает их пользователю в режиме только для чтения.

Благодаря запатентованной технологии Symantec Transparent Clientless Rendering (TCR) пользователь может работать в браузере совершенно обычным образом — точно так же, как если бы он просматривал веб-сайты непосредственно в Интернете.

Для применения Symantec Web Isolation не требуется устанавливать какие-либо специальные конечные устройства или модули. Продукт поддерживает любые операционные системы, устройства и браузеры, и поэтому наилучшим образом подходит для развертывания сразу во всей организации.

Технология Symantec обрабатывает веб-ресурсы удаленно, исключая возможность передачи вредоносного веб-контента в браузер. Продукт Web Isolation поставляется в формате облачного сервиса, устанавливаемого у заказчика виртуального устройства или в виде гибридной модели. Он без труда интегрируется с уже установленными решениями Symantec ProxySG, ASG и VSWG. Политики, настроенные на прокси-серверах Symantec, могут пропускать трафик от неклассифицированных и потенциально опасных веб-сайтов через службу Web Isolation, что позволяет разрешить пользователям посещение таких веб-сайтов, не подвергая компанию дополнительным рискам.

Подключение компонента веб-изоляции к шлюзам безопасного доступа компании Symantec повышает эффективность пользователей и положительно сказывается на деятельности организации. При этом операционные расходы и дополнительные сложности, связанные с управлением политиками доступа в Интернет, поддержкой пользователей, обработкой предупреждений и проведением расследований, остаются на минимальном уровне.

О компании Symantec

Symantec Corporation (NASDAQ: SYMC) — лидирующая компания в сфере кибербезопасности. Мы обеспечиваем защиту важных данных как частных пользователей, так и крупных компаний, включая государственные учреждения. Интегрированные решения Symantec используются организациями в разных странах для защиты от комплексных атак на конечные точки, облачные среды и инфраструктуру. Более 50 миллионов индивидуальных пользователей и семей во всем мире доверяют продуктам линейки Norton защиту своих домашних и личных устройств. Под управлением компании Symantec находится одна из крупнейших гражданских сетей анализа киберугроз, что позволят нам распознавать и блокировать самые изощренные угрозы. Дополнительные сведения см. на веб-сайте www.symantec.com или на наших страницах в Facebook, Twitter и LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 США | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

© Symantec Corporation, 2017. Все права защищены. Symantec, логотип Symantec и логотип с галочкой являются товарными знаками или зарегистрированными товарными знаками Symantec Corporation или ее дочерних компаний в США и других странах. Другие названия могут являться товарными знаками соответствующих владельцев.

SYMC_DS_Web_Isolation_EN_v1a