Обзор решения

Всесторонняя защита конечных точек и экономия бюджета

Предотвращение, обнаружение и устранение угроз с помощью единого агента

Инновационная защита от инновационных угроз

Комплексные атаки и связанные с ними угрозы становятся все более организованными и разнообразными. Согласно отчету Symantec о безопасности в Интернете[1], каждый день появляется почти миллион новых вредоносных программ. Злоумышленники умело скрывают свои действия, чтобы вредоносные программы было труднее обнаружить.

Современные продукты для защиты конечных точек должны развиваться быстрее противников и блокировать угрозы еще до того, как они проникнут в защищаемую систему. Поскольку конечные точки уязвимы и относительно легко поддаются взлому, рынок средств безопасности наводнен локальными решениями, ставящими разрозненные «заплатки». Такой подход увеличивает сложность системы и повышает стоимость ее обслуживания: заказчикам приходится иметь дело с несколькими поставщиками, проводить множество закупочных процедур, согласовывать поддержку, дополнительное ПО и оборудование.

Кроме того, простого блокирования угроз недостаточно. Согласно недавнему отчету[2], в 44 процентах компаний есть зараженные конечные точки — невзирая на наличие продуктов для их защиты. В среднем компании обнаруживают проникновение через 146 дней после того, как оно произошло[3]. Последствия этого могут быть разрушительными: в среднем устранение проблемы обходится в 4 млн долларов США[4]. Для того чтобы уверенно отражать атаки, компании должны:

- блокировать большинство угроз;
- выявлять аномалии;
- реагировать на попытки скрыть угрозу.

Всесторонняя защита конечных точек

Компания Symantec обеспечивает полный цикл безопасности конечных точек — от предотвращения угроз до обнаружения и реагирования. Единый агент отвечает за защиту, обнаружение, расследование и устранение угроз:

- Блокирует угрозы на каждом этапе атаки с минимальным числом ложных срабатываний.
- Выявляет аномалии и расследует подозрительные события.
- Отражает комплексные атаки за считанные минуты, всего одним щелчком мыши.
- Оптимизирует ваши инвестиции в безопасность, не требуя дополнительных агентов.

Блокирование угроз на всех этапах атаки

В основе безопасной инфраструктуры лежит принцип отражения сложных атак до того, как они могли бы заразить конечные точки. Архитектура продукта Symantec Endpoint Protection 14 позволяет ему развиваться быстрее, чем совершенствуются угрозы. Благодаря развитому машинному обучению, механизму ликвидации уязвимостей и поведенческому анализу в реальном времени Symantec Endpoint Protection 14 эффективно блокирует угрозы еще до начала атаки. Коллективный опыт участников Symantec Global Intelligence Network — крупнейшей гражданской сети анализа угроз — позволяет отражать опасные угрозы с минимальным числом ложных срабатываний. При этом все уровни защиты интегрированы в едином облегченном агенте, который работает в постоянном взаимодействии с другими продуктами и обеспечивает согласованный ответ на угрозы.

Symantec

Выявление и расследование подозрительных событий

После того как вторжение было обнаружено, необходимо провести расследование всех подозрительных действий, удалить угрозу и оставленные ею артефакты. Все это обеспечивает Symantec Advanced Threat Protection: Endpoint — наше решение для обнаружения угроз на конечных точках и реагирования (EDR).

Выявление других аномалий

Для выявления комплексных направленных атак компания Symantec использует технологию контролируемого заражения в изолированной среде. Решение Symantec EDR ищет подозрительные файлы и отправляет их на анализ. Получив образец, мы применяем технологии машинного обучения, анализа репутации, статического обнаружения, анализа сетевого трафика и глобального анализа угроз. Всестороннее изучение в изолированной среде позволяет обнаруживать даже самые устойчивые угрозы. Подробный отчет о контролируемом заражении и вся сопутствующая информация предоставляются специалистам на единой консоли.

На сегодняшний день 28 процентов сложных атак способны распознавать виртуальные машины.[5] Для решения этой проблемы в облачной «песочнице» Symantec реализованы защитные механизмы, имитирующие действия пользователя и запускающие подозрительные файлы как на виртуальном, так и на физическом оборудовании. В результате нами обнаруживаются атаки, которые остались бы незамеченными при классическом анализе в «песочнице».

Расследование подозрительных событий

Symantec EDR ведет постоянный анализ подозрительных действий, чтобы не упустить угрозы, которые все же смогли обойти предыдущие линии обороны. Сочетая возможности глобального расследования в крупнейшей гражданской сети анализа угроз со знанием локальной конфигурации конечных точек, Symantec EDR предоставляет подробные сведения о каждой просочившейся угрозе. В число этих сведений входят следующие:

- как угроза проникла в сеть организации;
- список зараженных компьютеров;
- список новых файлов, созданных в ходе атаки;
- список загруженных файлов и многое другое.

Symantec EDR автоматически отслеживает появление индикаторов компрометации (indicators of compromise, IoC) и предупреждает специалистов по безопасности, что на организацию предпринята целенаправленная атака. Это позволяет мгновенно приступать к защитным мероприятиям. Кроме того, аналитики имеют возможность искать конкретные артефакты, проверять все конечные точки на наличие определенных IoC и быстро получать интересующие их файлы с любого компьютера или устройства.

Отражение сложных атак за считанные минуты

После обнаружения вредоносного кода Symantec EDR локализует и устраняет все его экземпляры за считанные минуты. Вы можете быстро удалить все компоненты атаки или блокировать их исполнение на всех конечных точках нажатием одной кнопки. Зараженную конечную точку можно изолировать, запретив внутренние или внешние коммуникации.

Symantec EDR дает наглядное представление об индикаторах компрометации, связанных с атакой, включая графическую иллюстрацию взаимосвязей таких индикаторов между собой. На иллюстрации показаны все файлы, связанные с атакой, все IP-адреса и URL, откуда файлы были загружены, все измененные разделы реестра, а также последствия инцидента.

Оптимизация инвестиций в безопасность

Symantec EDR позволяет оптимизировать уже сделанные инвестиции в продукты Symantec и других поставщиков:

- Добавление функций EDR без необходимости установки новых агентов повышает отдачу от инвестиций в Symantec Endpoint Protection.
- Symantec EDR поддерживает экспорт расширенной аналитической информации в системы управления инцидентами безопасности и событиями (SIEM) сторонних поставщиков для дальнейшего расследования.
- Интеграция с Splunk® и ServiceNow® — популярными продуктами SIEM и поддержки рабочих процессов — обеспечивается через API сразу после установки. Такая интеграция позволяет создавать собственные сценарии реагирования на инциденты.

Всесторонняя защита при меньших затратах

Комплексные атаки безжалостны, происходят все чаще и постоянно усложняются. Простого блокирования угроз уже недостаточно. Эффективная защита конечных точек должна:

- блокировать большинство угроз до момента возможного заражения;
- выявлять аномалии и расследовать подозрительные события, если заражения избежать не удалось;
- быстро устранять все последствия атаки на всех конечных точках.

Наиболее эффективную защиту от комплексных атак обеспечивает многоуровневая система, действующая на всем цикле обеспечения безопасности. Компания Symantec предлагает надежный компонент предотвращения угроз, проверенный независимыми организациями, мощные средства обнаружения и реагирования. И все это — при одновременном уменьшении стоимости владения.

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 Norton и LifeLock 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.

Штаб-квартира Symantec Corporation

350 Ellis Street
Mountain View, CA 94043 США
+1 (650) 527 8000
1 (800) 721 3934

www.symantec.com

[1] Symantec ISTR, 2017 г.
[2] Gartner MQ for Endpoint Protection Platform, февраль 2016 г.
[3] FireEye M-Trend Report, 2016 г.
[4] Cost of Data Breach Study, Ponemon Institute for IBM, июнь 2016 г.
[5] Symantec ISTR, 2016 г.