СПЕЦИФИКАЦИЯ

Symantec Endpoint Detection and Response — ATP: Endpoint

Выявление и устранение сложных угроз с помощью одного агента

Краткий обзор

Выявление и идентификация: быстрое обнаружение атак и определение их масштаба

- Использование машинного обучения и поведенческого анализа для выявления и классификации подозрительных действий.
- Сбор данных об атаках в реальном времени путем опроса агентов, установленных на конечных точках.
- Идентификация подозрительных сценариев и эксплойтов, автоматическое создание инцидентов.

Расследование и локализация: помощь аналитикам и надежная изоляция угроз

- Восстановление полной картины произошедшего благодаря записи всех действий на конечных точках, включая данные о каждом процессе.
- Идентификация угроз путем отслеживания индикаторов компрометации в режиме реального времени на всех конечных точках.
- Изоляция конечных точек, которые могли быть скомпрометированы, на время проведения расследования.

Устранение: быстрая установка исправлений и иммунитет от повторного заражения

- Удаление вредоносных файлов и связанных с ними артефактов на всех конечных точках.
- Ведение черных и белых списков файлов на конечных точках.
- Возможность экспорта любой таблицы в отчет об устранении угрозы.

Выгодная инвестиция: множество интеграций и публичных API

- Встраивание автоматической обработки инцидентов и запросов в существующие процессы с помощью приложения ServiceNow.
- Изучение данных EDR в совокупности с другой информацией о безопасности в специальных приложениях для Splunk и QRadar.
- Быстрая интеграция с другими продуктами безопасности через открытые API.

Введение

Комплексные атаки на организации никогда не прекращаются. Согласно некоторым данным[1], в среднем вредоносный код сохраняется в сети компании в течение 190 дней — во многом благодаря технологиям маскировки, используемым сложными устойчивыми угрозами. Получив доступ к ресурсам компании, злоумышленники применяют разнообразные уловки, чтобы избежать обнаружения и похитить ценные ресурсы и данные. Стремясь обнаружить и полностью раскрыть такие атаки аналитики сталкиваются с множеством проблем: необходимостью ручного поиска в огромных и разнородных источниках, отсутствием представления о происходящем на конечных точках, лавиной ложных сообщений об угрозах, сложностями с идентификацией и лечением зараженных конечных точек.

Обзор Advanced Threat Protection (ATP): Endpoint

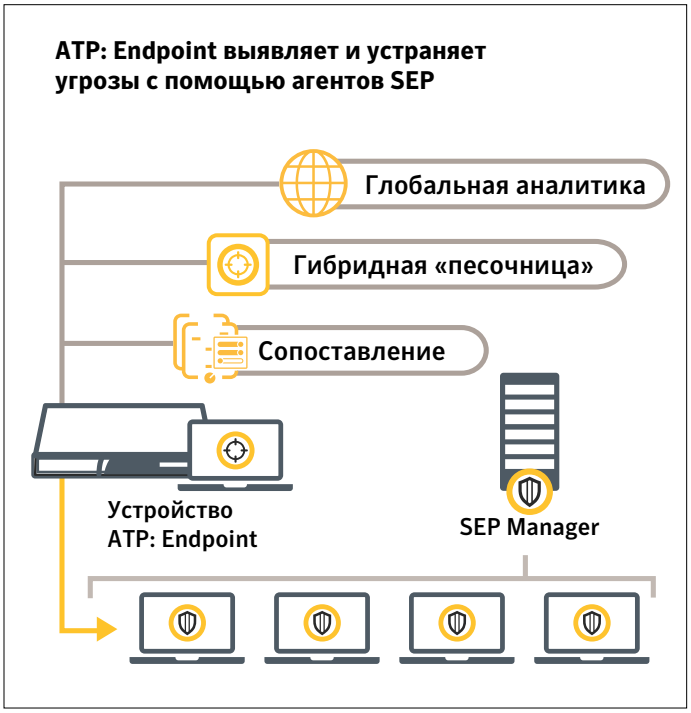
Решение Symantec ATP: Endpoint использует функции EDR, встроенные в продукт Symantec Endpoint Protection (SEP), поэтому его можно развернуть буквально за час и без установки дополнительных агентов. В результате

[1] Cost of Data Breach Study: United States, Ponemon 2017 г.

в руках аналитиков оказываются мощные инструменты, позволяющие выявлять, изолировать и устранять сложные устойчивые угрозы. Для обнаружения комплексных атак в ATP: Endpoint применяются передовые технологии машинного обучения и поведенческого анализа, минимизирующие число ложных срабатываний и открывающие доступ к ресурсам крупнейшей гражданской сети анализа угроз (GIN). С помощью ATP: Endpoint аналитики могут не только быстро находить и изолировать зараженные конечные точки, но и исследовать угрозы с использованием локальных ресурсов или облачной изолированной среды. Непрерывная запись всех действий на конечных точках позволяет точно знать, что на них происходит, и запрашивать информацию в режиме реального времени. Для удаления вредоносных программ и связанных с ними артефактов с зараженных конечных точек достаточно одного клика в консоли ATP: Endpoint.

Обнаружение угроз — даже «прячущихся у всех на виду»

Для обнаружения сложных угроз в ATP: Endpoint применяется несколько технологий. Глубокое машинное обучение и поведенческий анализ помогают выявлять опасные и подозрительные файлы. ATP: Endpoint диагностирует атаки, в которых используются не файлы, а эксплойты памяти и сценарии PowerShell.



Повышение эффективности работы аналитиков

Решение ATP: Endpoint помогает аналитикам расставить приоритеты при обработке инцидентов и автоматически генерирует инциденты для целенаправленных атак, выявленных с помощью Symantec Dynamic Adversary Intelligence.

Кроме того, функция Endpoint Activity Recording помогает отслеживать индикаторы атаки и выполнять анализ действий на конечных точках. Решение ATP: Endpoint способно восстанавливать информацию о множестве событий, включая изменение точек загрузки сеансов, процессов и модулей, операции с файлами и папками, изменение реестра и использование сетевых соединений.

По данным отчета Symantec об угрозах из Интернета (ISTR), более 20 % вредоносных программ умеют распознавать виртуальные машины, и тем самым избегать обнаружения в классических «песочницах». Решение ATP: Endpoint способно выявлять такие угрозы с помощью специальных технологий, в том числе имитации действий пользователя и, при необходимости, использования физических серверов.

Быстрое исправление конечных точек

Решение ATP: Endpoint способно быстро справляться с заражением, в том числе удалять файлы, вести черные списки и помещать конечные точки в карантин. Одним нажатием кнопки в консоли ATP: Endpoint администратор может применить исправление сразу на нескольких конечных точках.

ATP: Endpoint позволяет отражать комплексные атаки за несколько минут

Сопоставление данных из разных источников

ATP: Endpoint — это часть платформы Advanced Threat Protection (ATP), которая дает возможность сопоставлять данные от модулей мониторинга сети и электронной почты. Устройство ATP: Endpoint автоматически устанавливает взаимосвязи между событиями, зарегистрированными модулями SEP, мониторинга электронной почты и сети. Модули Symantec ATP (ATP: Endpoint, ATP: Network и ATP: Email) выявляют и ранжируют угрозы, используя один агент и одну консоль.

Symantec Advanced Threat Protection	**ENDPOINT**	Обнаруживает, исследует и блокирует атаки на конечные точки	Использует агент Symantec Endpoint Protection
	NETWORK	Выявляет и блокирует сложные угрозы, пытающиеся проникнуть в сеть с помощью нескольких технологий	Виртуальное или физическое устройство
	EMAIL	Выявляет и блокирует сложные угрозы, распространяющиеся через электронную почту; идентифицирует целенаправленные атаки	Использует изолированную «песочницу» или Email Security Cloud

Возможности версии 3.0

Запись действий на конечных точках

Непрерывное наблюдение за конечными точками через агент SEP

- Запись информации о важных действиях в системе, включая операции с файлами, изменение реестра, действия процессов, изменение точек загрузки, вход и выход пользователей.
- Релевантные события выбираются для дальнейшего анализа и создания инцидентов с помощью эвристических алгоритмов и правил, настроенных администратором.

Анализ конечных точек

Поиск, фильтрация и анализ событий на конечных точках

- Поиск в базе данных EDR и напрямую на конечных точках.
- Быстрая фильтрация по значениям атрибутов, выявление нестандартного поведения и определение взаимосвязи с источником.
- Получение данных для анализа с конкретных конечных точек.

Выявление угроз, не использующих файлы

Обнаружение и просмотр подозрительных сценариев и эксплойтов памяти

- Просмотр подозрительных сценариев и процессов PowerShell, классификация с использованием правил и автоматическое создание инцидентов.
- Для эксплойтов памяти, заблокированных Symantec Endpoint Protection, автоматически создаются инциденты, позволяющие анализировать взаимосвязанные артефакты.

Гибридная «песочница»

Контролируемое заражение в локальной или облачной «песочнице»

- Исследование поведения подозрительных файлов в локальной или облачной изолированной среде.
- Поддержка контролируемого заражения в виртуальных и физических системах.
- Учет репутации файлов, анализ трафика и глобальная телеметрия.

Улучшенные публичные API и новые интеграции

Простая интеграция и готовые компоненты

- Новые публичные API поддерживают новые функции, включая Endpoint Activity Recorder.
- Готовые компоненты для популярных решений SIEM и ITSM (Splunk, QRadar, ServiceNow).
- Предоставление доступа к консоли пользователям и группам Active Directory.

Требования

Symantec Endpoint Protection 14.X, Symantec Endpoint Protection 12.1 RU6 MP7 (компонент Recorder поддерживается только с ATP: Endpoint for SEP 14 и более новыми версиями).

Характеристики сервера			
Форм-фактор	**8880-30**	**8840***	**VMware ESXi**
	Стоечный модуль формата 2U	Стоечный модуль формата 1U	Виртуальная машина
ПРОЦЕССОР	2 x Intel Xeon E5-2697 v4, 2,3 ГГц, 18 ядер, 145 Вт	Intel Xeon E3-1270 V5, 3,6 ГГц, 4C/8T, 80 Вт	12 процессоров
ОЗУ	192 ГБ	32 ГБ	48 ГБ
Жесткий диск	RAID 10; 4 x 300 ГБ; 15K SAS RAID 10; 4 x 1,8 ГБ; 10K SAS	2 x 1 ТБ; 7,2K об./мин NLSAS 12 Гбит/с 2,5” (400-ALUN)	500 ГБ (для поддержки компонента Endpoint Activity Recording необходимо увеличить на 1 ТБ)
Сетевая карта	4 порта 1 Гбит/с Ethernet 4 порта 10 Гбит/с Ethernet с прямым аварийным соединением	2 порта 1 Гбит/с Ethernet 2 порта 1 Гбит/с Ethernet с прямым аварийным соединением	2 порта 1 Гбит/с Ethernet
DVD-ROM	DVD ROM, SATA	DVD ROM, SATA	н/д
Источник питания	2 источника питания на 750 Вт с резервированием	2 источника питания на 350 Вт с резервированием	н/д

*Устройство 8840 не поддерживает компонент Endpoint Activity Recording

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.

Symantec

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

SYMC_DS_ATP_Endpoint_Detection_Response_EN_v1a