Symantec
A Division of Broadcom

Краткое описание продукта

Symantec Endpoint Security

Внедрение единой стратегии безопасности на конечных точках важнее, чем когда-либо

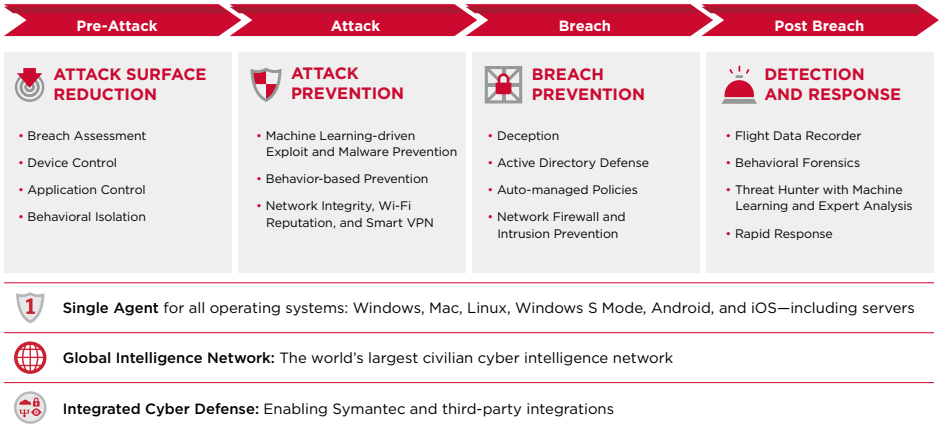
Вступление

Конечные точки являются основной мишенью для кибератакеров. По мере того, как последствия успешных атак и связанный с ними ущерб растут, многие компании пытаются усилить общую защиту, добавляя в неё различные продукты для защиты конечных точек. К сожалению, такой подход ослабляет безопасность компании.

Ponemon Institute провел исследование и выявил, что организации устанавливают в среднем семь различных агентов конечных точек для поддержки управления ИТ и безопасности. Каждый агент работает независимо с собственной консолью и набором правил и политик - все они должны быть сконфигурированы, развернуты, управляться и поддерживаться. В дополнение к увеличению накладных расходов и затрат на ИТ, многочисленные продукты создают пробелы и ошибки в системе защиты, увеличивая шансы того, что угроза будет упущена.

Предотвращение имеет важное значение, поскольку глобальные киберугрозы являются более агрессивными, чем когда-либо и могут оказывать ошеломляющее воздействие на бизнес. Например, за время, которое вы потратите для прочтения этой статьи, может быть скомпрометировано целое предприятие. Согласно сообщениям, атака NotPetya нанесла ущерб одной из крупнейших в мире транспортных компаний всего за 7 минут, и таких примеров - тысячи. Крайне важно предотвращать атаки как можно раньше, так как время для обнаружения и реакции на современную атаку очень короткое. Инвестиции в реагирование на инциденты также важны для создания более жёсткой позиции безопасности для предотвращения будущих атак. С помощью решений Symantec вы можете больше не выбирать между наилучшей безопасностью и максимальной простотой, а использовать и то, и другое.

Рисунок 1: Symantec Endpoint Security Complete



Ключевые особенности Symantec Endpoint Security Complete

- Защита всех конечных точек: ноутбуков, настольных и планшетных компьютеров, мобильных устройств и серверов.
- Единый агент для уменьшения поверхности атаки и предотвращения атак Endpoint Detection and Response (EDR).
- Единая консоль с возможностью просмотра угроз в реальном времени.
- Гибкое развертывание: локальные, облачные и гибридные модели.
- Возможности контроля приложений (Behavioral Isolation and Application Control capabilities).
- Управление безопасностью на основе искусственного интеллекта.
- Встроенный инструментарий Targeted Attack Analytics и Threat Hunter.
- Глобальная сеть киберугроз Global Intelligence Network (GIN), одна из крупнейших в мире, предоставляет в режиме реального времени информацию об угрозах, аналитику угроз, классификацию контента и всеобъемлющие данные по блокировке угроз.
- Интеграция со сторонними приложениями, включая Microsoft Graph, Open C2 и другие решения Symantec через Symantec ICDx.

Ключевые особенности Symantec Endpoint Security Сборка Enterprise

- Защита ноутбуков, настольных ПК, мобильных телефонов и планшетов.
- Единый агент для обеспечения безопасности конечных точек.
- Единая консоль с возможностью просмотра угроз в реальном времени.
- Гибкое развертывание: локальные, облачные и гибридные модели.
- Управление безопасностью на основе искусственного интеллекта.
- Глобальная сеть киберугроз Global Intelligence Network, одна из крупнейших, предоставляет информацию об угрозах в режиме реального времени.
- Интеграция со сторонними приложениями, такими как Microsoft Graph, Open C2 и другими решениями Symantec через Symantec Integrated Cyber Defense Exchange (ICDx).

Уменьшение площади атаки

Symantec обеспечивает упреждающую защиту конечных пользовательских устройств с уменьшением возможности провести атаку на основе расширенных средств управления политиками и технологий, которые непрерывно сканируют приложения, Active Directory и устройства на наличие уязвимостей и неправильных настроек. Благодаря встроенным средствам защиты многие тактики и приемы атакующих не могут быть использованы на конечных устройствах.

• **Breach Assessment** непрерывно проверяет Active Directory на наличие неправильных настроек домена, уязвимостей и стойкости, используя симуляцию атак для выявления рисков, позволяющую немедленно снизить риски с помощью прескриптивных рекомендаций по их устранению.

• **Device Control** определяет, на основе политик, блокировать или разрешать работу различных типов устройств, таких как USB, инфракрасные и FireWire устройства, подключаемых к клиентским компьютерам, чтобы снизить риск атаки.

• **Application Control** оценивает приложения на предмет их уязвимостей и позволяет запускать только приложения с положительной репутацией.

• **Behavioral Isolation** ограничивает необычное и рискованное поведение доверенных приложений с минимальным операционным воздействием на них.

• **Vulnerability Remediation**[1] повышает уровень безопасности, предоставляя информацию об уязвимостях и связанных с ними рисках. Обнаруженные уязвимости ранжируются по степени серьезности на основе CVSS (Common Vulnerability Scoring System - общая система оценки уязвимости) наряду с определением количества поражённых устройств, что позволяет в первую очередь обеспечить устранение наиболее критических угроз.

*__1.__ Поддерживается только на Win 10, MacOS, iOS и Android устройствах.

Профилактика атак

Многоуровневая защита от атак Symantec мгновенно и эффективно защищает от файловых и безфайловых векторов и методов атаки. Система машинного обучения и искусственного интеллекта использует передовые схемы обнаружения устройств и «облачных» вычислений для выявления эволюционирующих угроз в различных типах устройств, операционных систем и приложений. Атаки блокируются в режиме реального времени, что позволяет конечным устройствам сохранять целостность и предотвращать негативные последствия.

• **Malware Prevention** сочетает в себе предварительное обнаружение и блокировку новых и эволюционирующих угроз (усовершенствованное машинное обучение, песочница для обнаружения вредоносного ПО, скрытого в архивах, а также мониторинг и блокирование подозрительного поведения файлов) и методы, основанные на сигнатурах (анализ репутации файлов и веб-сайтов, а также сканирование на вредоносное ПО).

• **Exploit Prevention** блокирует основанные на памяти эксплойты «нулевого дня» уязвимостей в популярном программном обеспечении.

• **Intensive Protection** отдельно позволяет тонко настроить уровень обнаружения и блокировки для оптимизации защиты и повышения видимости подозрительных файлов.

• **Network Connection Security** идентифицирует несанкционированные Wi-Fi сети, использует технологию репутации точки доступа и предоставляет VPN с поддержкой политик для защиты сетевых подключений.

Предотвращение нарушений

Подход Symantec предусматривает «остановку злоумышленников» на конечной точке до того, как у них появится возможность продолжать работу в сети. Различные технологии предотвращения обмана и вторжений работают совместно, чтобы предотвратить сохранение работоспособности сети до и сразу после взлома конечных точек - до того, как может произойти полномасштабное вторжение.

• **Intrusion Prevention and Firewall** блокирует известные сетевые и браузерные атаки с использованием правил и политик и предотвращает настройку команд и управления с автоматическим внесением IP-адреса домена в черный список.

• **Deception** использует приманки и наживки (поддельные файлы, учетные данные, общие сетевые ресурсы, записи в кэше, веб-запросы и конечные точки) для обнаружения, определения намерений и тактики атакующих, а также для задержки атакующих с помощью раннего обнаружения.

• **Active Directory Security** защищает от кражи учетных записей администратора домена, контролируя ресурсы Active Directory организации с конечной точки с помощью создания поддельных активов и учетных данных). Благодаря такому подходу злоумышленник выдает себя, взаимодействуя с поддельными активами или пытаясь использовать учетные данные администратора домена.

• **Автоматически управляемые политики**, основанные на усовершенствованном AI и ML, уникальным образом сочетают в себе показатели компромиссов и исторических аномалий для постоянной адаптации порогов или правил политики конечной точки и поддержания их в актуальном состоянии и соответствии с текущим профилем рисков вашей организации.

Действия после нарушения и устранение неисправностей

Symantec сочетает в себе технологии обнаружения и реагирования (EDR) и непревзойденный опыт аналитиков операционного центра безопасности (SOC), предоставляя вам инструменты, необходимые для быстрого закрытия инцидентов на конечных точках и минимизации воздействия атак. Интегрированные функции EDR в архитектуре единого агента, охватывающей как традиционные, так и современные конечные устройства, позволяют точно обнаруживать современные атаки, проводить анализ в режиме реального времени, а также активно охотиться за угрозами и проводить расследования устраняя их последствия.

• **Behavior Forensics** предоставляет возможность записывать и анализировать поведение конечных точек с целью выявления передовых методов атаки, которые могут использовать легитимные приложения для вредоносных целей. Эти данные обогащаются системой MITRE ATT&CK, которая помогает специалистам по реагированию на инциденты в ходе расследования.

• **Advanced Threat Hunting** – передовой инструмент реализованный в EDR, в том числе встроенные сценарии, в которых обобщены передовые методы работы опытных охотников за угрозами по обнаружению аномального поведения.

• **Integrated Response** принимает непосредственные меры на конечной точке для исправления ситуации путем извлечения файлов, удаления файлов, изоляции конечных точек и занесения их в черные списки. Symantec EDR поддерживает автоматическую отправку выявленных подозрительных файлов в песочницу для полного анализа вредоносного ПО, включая обнаружение вредоносных программ, которые являются виртуальными машинами.

• **Threat Hunter** охотится за инцидентами с высокой степенью достоверности и сочетанием в себе передового машинного обучения и опыт экспертных аналитиков SOC, чтобы обнаружить инструменты, тактику и процедуры, используемые злоумышленниками. Она обеспечивает быструю идентификацию критических атак с учетом соответствующего контекста. Кроме того, он предоставляет интуитивно понятный доступ к глобальным данным Symantec по безопасности, что повышает эффективность работы вашей команды по отслеживанию угроз.

• **Быстрое реагирование** сводит к минимуму время на устранение угроз и ответ на действия злоумышленников в режиме реального времени.

С легкостью защищайте вашу динамическую среду конечной точки

Стек с одним агентом снижает нагрузку на систему безопасности конечных точек, интегрируя (и координируя) лучшие из доступных технологий предотвращения, обнаружения и реагирования. Управляйте всем из единой «облачной» системы управления (Integrated Cyber Defense Manager), минимизируя время, ресурсы и усилия, необходимые для настройки, развертывания, управления и обеспечения безопасности. Все, что вам нужно, доступно одним щелчком мыши, что повышает производительность администратора и ускоряет время отклика для быстрого закрытия событий безопасности.

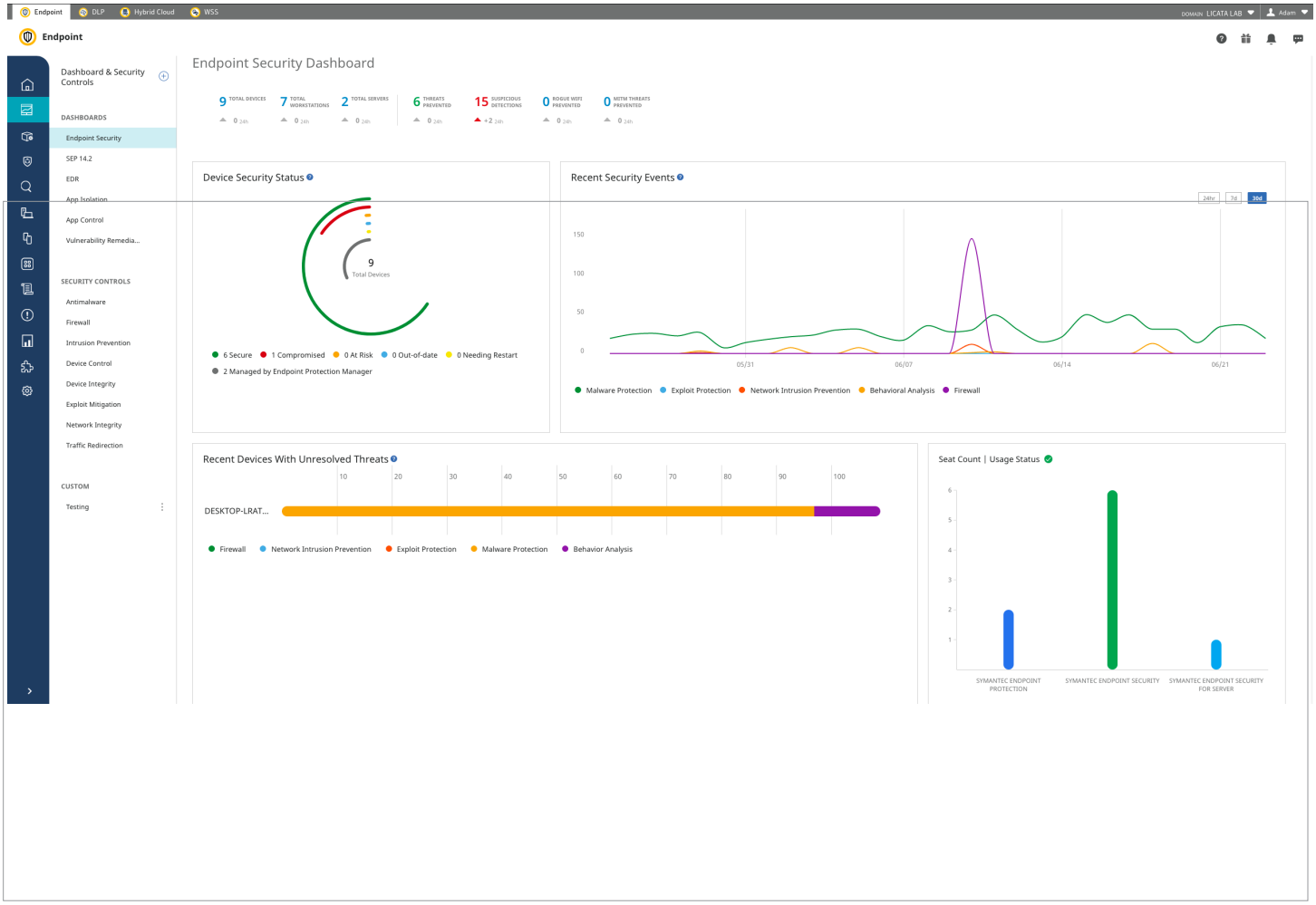
• **Управление безопасностью на основе искусственного интеллекта** более точно обновляет политики с меньшим количеством ошибок конфигурации для повышения уровня безопасности.

• **Упрощенные рабочие процессы** гарантируют, что все работает согласованно, повышая производительность, эффективность и продуктивность.

• **Рекомендации с учетом контекста** помогают достичь оптимальной производительности за счёт устранения рутинных задач и принятия более эффективных решений.

• **Автономное управление безопасностью** непрерывно учится на поведении администратора и пользователей, чтобы улучшить оценку угроз, настроить ответы и укрепить общую позицию безопасности.

Рисунок 2: Endpoint User Interface



Снижение сложности благодаря широкому портфелю Symantec и сторонним интеграциям

Symantec Endpoint Security — это базовое решение, которое облегчает интеграцию, позволяя командам ИТ-безопасности обнаруживать угрозы в любой точке сети и устранять их с помощью организованного реагирования.
Symantec Endpoint Security работает совместно с другими решениями Symantec, а также со сторонними продуктами с помощью специальных приложений и опубликованных API. Ни один другой поставщик не предоставляет интегрированного решения, которое организует ответ на конечной точке (чёрные списки и исправления), вызванный обнаружением угрозы в шлюзах безопасности веб-страниц и электронной почты. Конкретные интеграции включают в себя:

• **Symantec Web Security Service:** перенаправляет веб-трафик от пользователей Symantec Endpoint Security к Symantec Web Security Service и Symantec CASB с помощью файла PAC.

• **Symantec Web Gateway:** программируемые API REST делают возможной интеграцию с локальной инфраструктурой сетевой безопасности.

• **Symantec Validation and ID Protection:** многофакторная аутентификация, включая PIV/CAC смарт-карты в консолях управления Symantec Endpoint Security в режиме реального времени и в облаке.

• **Symantec Data Loss Prevention:** предотвращает утечку конфиденциальной информации, обеспечивая в реальном времени информацию об угрозах, связанных с подозрительными приложениями, в DLP.

Рисунок 3: Symantec Endpoint Security

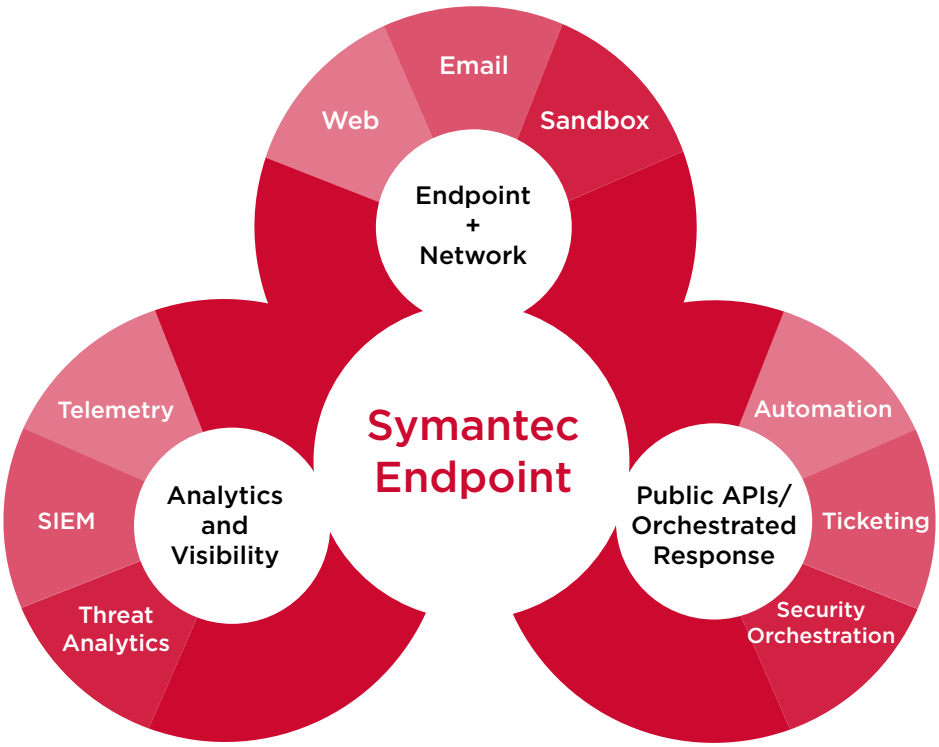


Рисунок 4: License Options

Features

	SEP	SES ENTERPRISE	SES COMPLETE
	Industry standard in Endpoint Protection. 5 years running as #1 Protection and now also #1 Performance by AV Test.	Extends SEP to all OSs and all devices including mobile. Offers cloud management.	Adds advanced protection, EDR, threat hunting, and other technologies for complete protection.
MANAGEMENT OPTIONS	On-Premises	On-Premises, Cloud, Hybrid	
AGENTS REQUIRED	SINGLE SYMANTEC AGENT		
DEVICE COVERAGE Corporate Owned, BYOD, UYOD	Laptop, Desktop, Server	Mobile, Tablet, Laptop, Desktop, Server	
OS COVERAGE	Windows, macOS, Linux	Windows (including S Mode and Arm), macOS, iOS, Linux, Android	

Protection Technologies

	SEP	SES ENTERPRISE	SES COMPLETE
ATTACK PREVENTION			
INDUSTRY-BEST ATTACK PREVENTION	✓	✓	✓
MOBILE THREAT DEFENSE		✓	✓
SECURE NETWORK CONNECTION		✓	✓
ATTACK SURFACE REDUCTION			
BREACH ASSESSMENT			✓
BEHAVIORAL ISOLATION			✓
APPLICATION CONTROL			✓
DEVICE CONTROL	✓	✓	✓
BREACH PREVENTION ...			
INTRUSION PREVENTION	✓	✓	✓
FIREWALL	✓	✓	✓

	SEP	SES ENTERPRISE	SES COMPLETE
... BREACH PREVENTION			
DECEPTION	✓	✓	✓
ACTIVE DIRECTORY SECURITY			✓
RESPONSE AND REMEDIATION			
ENDPOINT DETECTION AND RESPONSE			✓
TARGETED ATTACK CLOUD ANALYTICS			✓
BEHAVIORAL FORENSICS			✓
THREAT HUNTER			✓
RAPID RESPONSE			✓
IT OPERATIONS			
DISCOVER & DEPLOY	✓	✓	✓
HOST INTEGRITY CHECKS	✓	✓	✓

Подробная информация: go.broadcom.com/ses

SED-EPS-PB101 25 июня 2020 г.

Компания Oberig IT
является официальным дистрибьютором Symantec на территории Украины, Молдовы, Казахстана

info.ua@oberig-it.com
www.oberig-it.com

Symantec. A Division of Broadcom

Oberig it