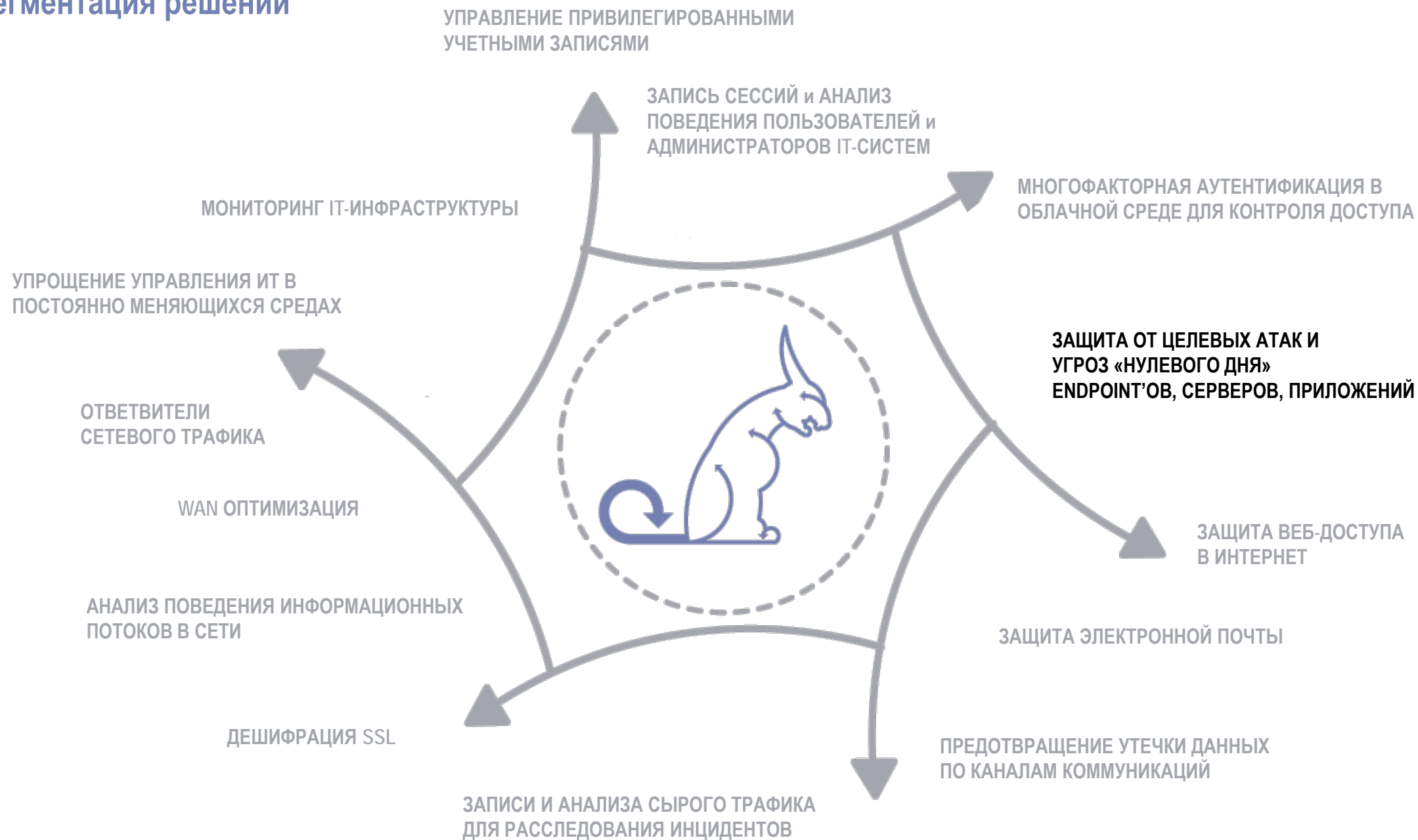


Сегментация решений



Решение от Symantec – Symantec Endpoint Protection

ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ И УГРОЗ «НУЛЕВОГО ДНЯ» ДЛЯ ENDPOINT'ОВ

<https://www.symantec.com/ru/ru/endpoint-protection/>

Многоуровневая система защиты блокирует направленные атаки и сложные устойчивые угрозы в конечных точках:

- Network Threat Protection анализирует входящие потоки данных и обеспечивает превентивное блокирование угроз.
- Технология анализа репутации Insight™ сортирует файлы на подверженные угрозам и безопасные – для более точного обнаружения вредоносных программ.
- Технология эвристической защиты SONAR™ отслеживает работу приложений в режиме реального времени, блокируя атаки нулевого дня и направленные угрозы.
- Надежные технологии брандмауэра, антивирусной защиты.

Оптимизация быстродействия в физических и виртуальных средах:

- Благодаря технологии Insight сканируются только файлы, подверженные угрозам, что позволяет сократить время сканирования до 70 %.
- Более низкие требования к ресурсам памяти для встраиваемых систем или VDI позволяют уменьшить размер клиента.
- Снижение загруженности сети и гибкое управление соединениями и пропускной способностью.

Одна консоль управления для всех физических и виртуальных платформ на основе политик:

- Один высокоэффективный агент с единой консолью управления для Windows, Mac, Linux, виртуальных машин и встраиваемых систем.
- Поддержка удаленного развертывания и управления клиентами Windows и Mac.
- Избирательное применение политик для блокировки систем, контроля приложений и устройств, а также определения расположения.

Облачная аналитика киберугроз



БРАНДМАУЭР И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

Контроль трафика и превентивная блокировка вредоносного кода



КОНТРОЛЬ ПРИЛОЖЕНИЙ И УСТРОЙСТВ

Контроль файлов, реестра и устройств; черные и белые списки.



ЗАЩИТА ОТ ЭКСПЛОЙТОВ В ПАМЯТИ

Блокировка эксплойтов нулевого дня в известном программном обеспечении



АНАЛИЗ РЕПУТАЦИИ

Выявление опасных файлов и сайтов с помощью сообщества



МАШИННОЕ ОБУЧЕНИЕ

Заблаговременное выявление новых и эволюционирующих угроз



ЭМУЛЯТОР

Виртуальная машина для выявления угроз, скрытых с помощью упаковщиков



АНТИВИРУС

Сканирование на вредоносные программы и удаление их из системы



МОНИТОРИНГ ПОВЕДЕНИЯ

Отслеживание и блокирование файлов с подозрительным поведением



БРАНДМАУЭР И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

Контроль трафика и превентивная блокировка вредоносного кода

ВТОРЖЕНИЕ

ЗАРАЖЕНИЕ

ЭКСФИЛЬТРАЦИЯ



Решение от Symantec – Advanced Threat Protection

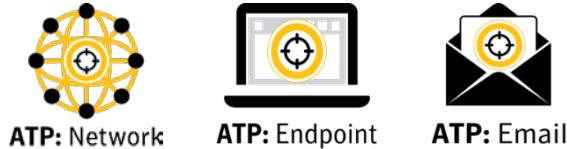
ЗАЩИТА ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК НА КОНЕЧНЫЕ ТОЧКИ, СЕТИ И ЭЛЕКТРОННУЮ ПОЧТУ

<https://www.symantec.com/ru/ru/advanced-threat-protection/>

Обнаружение новейших угроз на уровне конечных точек, сетей и шлюзов электронной почты

- Объединяет глобальные телеметрические данные, полученные из одного из крупнейших в мире источников аналитических данных о кибербезопасности, с локальными данными клиента на уровне конечных точек, сетей и электронной почты, что позволяет успешно обнаруживать атаки, которые невозможно выявить стандартными методами.
- Обеспечивает быстрый поиск любых артефактов атак во всех компонентах инфраструктуры. При необходимости подозрительные файлы можно извлечь из любой конечной точки для дальнейшей проверки.

Модули Symantec ATP



Быстрое исправление

- Централизованное представление всей необходимой информации об атаке без необходимости выполнять поиск вручную. Аналитикам в области безопасности доступны средства визуализации и быстрого исправления всех компонентов атаки, включая файлы, задействованные в атаке, электронные адреса, IP-адреса веб-сайтов, содержащих вредоносный код.
- Достаточно нажатия одной кнопки, чтобы устранить зараженный файл во всех контрольных точках — конечных точках, серверах и шлюзах электронной почты, защищенных продуктами Symantec.
- Позволяет локализовать сложные атаки за считанные минуты.

Защищайте наиболее важные ресурсы

- Технология сопоставления данных Synapse объединяет аналитическую информацию из различных контрольных точек для выявления зараженных систем, требующих незамедлительного устранения угроз.
- Значительно уменьшает число инцидентов, требующих изучения вручную, что позволяет аналитикам сосредоточиться на наиболее приоритетных событиях.
- Использует новую облачную услугу Symantec Cynic для обнаружения угроз с помощью изолированной среды выполнения — на 30 % эффективнее FireEye® и на 20 % эффективнее Cisco®*.

*Отчет Miercom: DR150218C, апрель 2015 г.

Современные решения Symantec для защиты от направленных атак





Решение от Symantec – Data Center Security (DCS)

МОНИТОРИНГ и ЗАЩИТА ОТ УГРОЗ БЕЗ ПРИМЕНЕНИЯ АГЕНТОВ НА ОСНОВЕ ПОЛИТИК
ЛОКАЛЬНЫХ СЕРВЕРОВ И ОБЛАЧНЫХ СРЕД AWS И OPENSTACK, ЗАЩИТА СРЕДЫ VMWARE

<https://www.symantec.com/ru/ru/data-center-security/>

Symantec DCS позволяет обеспечить непрерывный мониторинг и усилить защиту физических и виртуальных серверов, а также облачных сред AWS и OpenStack на основе хоста. Клиентам доступно автоматическое развертывание средств защиты от вредоносного кода и несанкционированного подключения для сред VMware. DCS использует платформу для автоматического управления параметрами безопасности на основе политик в компании Symantec и системе партнеров в области безопасности. Интегрируется с Symantec DeepSight, предоставляя технологии репутации для файлов и URL-адресов.

Семейство продуктов Symantec DCS

Data Center Security: Server

Основные возможности

- Обнаружение и защита от вредоносных **без применения агентов**.
- Operations Director предоставляет оперативную информацию о безопасности и автоматизирует координацию задач по обеспечению безопасности на основе политик для семейства продуктов Symantec Data Center Security, а также тесно интегрируется с VMware для охвата сторонних инструментов обеспечения безопасности.
- Консоль унифицированного управления (UMC) обеспечивает согласованное управление для семейства продуктов Data Center Security.
- Перемещение файлов гостевых систем в карантин и исправление на основе политик.

Основные преимущества

- Оптимизация производительности сети и приложений для гостевых систем и хостов с помощью ПО для защиты от вредоносного кода и сетевой системы IPS без агентов.
- Повышение быстродействия сети за счет единого механизма обновления описаний.
- Автоматическое развертывание виртуальных устройств для масштабирования нагрузки и минимизации затрат.

Data Center Security: Monitoring Edition

Основные возможности

- Все функции, доступные в Data Center Security: Server.
- Мониторинг безопасности на физических и виртуальных серверах, включая проверку целостности файлов в реальном времени, мониторинг конфигурации, консолидированный журнал событий и защиту системы и файлов от изменений.
- Мониторинг безопасности центров обработки данных OpenStack, включая мониторинг программных файлов и данных Keystone, а также мониторинг доступа и изменений конфигурации.
- Мониторинг безопасности общедоступных и смешанных облачных сред AWS (VPC), включая мониторинг конфигурации безопасности, проверку целостности файлов, создание «белых списков» приложений для локальных и удаленных ЦОД, а также автоматизация защиты в облачной среде с помощью API REST.

Основные преимущества

- Упрощенный непрерывный мониторинг и отчетность по кибербезопасности и соблюдению требований для смешанных инфраструктур ЦОД.
- API REST предоставляет соответствующий API для всех действий в консоли с целью автоматизации внутренних и внешних облачных приложений.
- Единый инструментарий для оперативного выявления нарушений политик и подозрительных действий на уровне приложений или экземпляров — на физических и виртуальных серверах, а также в облачных средах AWS и OpenStack.





Решение от Symantec – Data Center Security (DCS)

МОНИТОРИНГ и ЗАЩИТА ОТ УГРОЗ БЕЗ ПРИМЕНЕНИЯ АГЕНТОВ НА ОСНОВЕ ПОЛИТИК
ЛОКАЛЬНЫХ СЕРВЕРОВ И ОБЛАЧНЫХ СРЕД AWS И OPENSTACK, ЗАЩИТА СРЕДЫ VMWARE

<https://www.symantec.com/ru/ru/data-center-security/>

Семейство продуктов Symantec DCS (продолжение)

Data Center Security: Server Advanced

Основные возможности

- Все функции, доступные в Data Center Security: Server и Monitoring Edition.
- Готовые политики IDS и IPS для хостов.
- Изолированные среды выполнения и контроль доступа к процессам (PAC), брандмауэр на уровне хоста, компенсирующие средства HIPS, защита системы и файлов от изменений, а также контроль приложений и устройств.
- Повышение безопасности данных OpenStack Keystone.

Ключевые преимущества

- Защита сервера от атак нулевого дня.
- Защита незащищенных приложений и систем, работающих на устаревших платформах.
- Работа с технологиями виртуализации и широкая поддержка платформ, а также защиты целых ЦОД, включая устаревшие системы, в которых невозможно установить исправления.
- Мониторинг и защита физических и виртуальных ЦОД с использованием набора технологий выявления вторжений на уровне хоста (HIDS), предотвращения вторжений (HIPS) и предоставления минимальных полномочий.

Матрица сравнений Data Center Security: Server, Monitoring Edition и Server Advanced

https://www.symantec.com/content/en/us/enterprise/fact_sheets/data-center-security-6.5-product-matrix-en.pdf

Обзор ПО на Anti-Malware.ru

https://www.anti-malware.ru/reviews/Symantec_Data_Center_Security_Server_Advanced

<http://www.vmg.ru/articles/symantec-dcs-server-advanced>

Symantec Control Compliance Suite

Позволяет автоматически обнаруживать IT-активы, вычислять и агрегировать показатели рисков ИБ. Control Compliance Suite применяется для обеспечения базовой гигиены безопасности и обеспечения прозрачности в отношении безопасности, рисков и комплайнса. Данное решение может быть востребовано для приоритизации и оптимизации распределения ресурсов информационной безопасности.

Symantec Protection Engine

Обеспечивает сканирование содержимого, защиту от вредоносных программ, обнаружение аномалий, репутационные сервисы и технологии фильтрации контента для различных типов хранилищ данных. Такими хранилищами могут быть облачные сервисы, NAS, электронная почта и AWS. Встроенная поддержка доступна для NetApp NAS, Microsoft Exchange и SharePoint.





Наименование	Краткое описание	Самая свежая информация о решении	Принцип лицензирования
Решение от Symantec – Symantec Endpoint Protection	Защита от вредоносных программ и угроз «нулевого дня» для endpoint'ов	https://www.symantec.com/ru/ru/endpoint-protection/	По пользователям
Решение от Symantec – Advanced Threat Protection	Защита от целенаправленных атак на конечные точки, сети и электронную почту	https://www.symantec.com/ru/ru/advanced-threat-protection/	По модулям endpoint, email, network, roaming; объемы модулей набираются по пользователям
Решение от Symantec – Data Center Security (DCS)	Мониторинг и защита от угроз без применения агентов на основе политик локальных серверов и облачных сред aws и openstack, защита среды vmware	https://www.symantec.com/ru/ru/data-center-security/	По модулям server, monitoring, server advanced; объемы модулей набираются по серверам



