Cisco Stealthwatch Enterprise

Для аппаратного обеспечения UCS

Stealthwatch™ Enterprise — это лучшее в отрасли решение для мониторинга и аналитики безопасности, в котором используются корпоративные данные телеметрии из существующей сетевой инфраструктуры. Оно повышает эффективность обнаружения угроз, ускоряет реагирование на них и упрощает сегментацию сети с помощью многоуровневого машинного обучения и усовершенствованного поведенческого моделирования в рамках распределенной сети.

Stealthwatch Enterprise позволяет проводить мониторинг в режиме реального времени, благодаря чему вы сможете получать больше полезных сведений о происходящем в сети. Такой мониторинг может охватывать облако, всю сеть, филиалы, центр обработки данных и оконечные устройства.

Основу Stealthwatch Enterprise составляют инструменты Flow Rate License, Flow Collector, Management Console и Flow Sensor. Дополнительные функциональные возможности описаны в отдельных спецификациях.

- Cisco Stealthwatch Endpoint License. Доступно в виде лицензируемого дополнительного модуля для обеспечения функций мониторинга на устройствах конечных пользователей.
- Cisco Stealthwatch Cloud. Доступно как предложение продукта для обеспечения мониторинга состояния и обнаружения угроз в общедоступных облачных инфраструктурах, таких как Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform.
- **Threat Intelligence License**. Это канал глобальной аналитики угроз, разработанный Cisco Talos, лучшей в отрасли командой специалистов по аналитике угроз, который обеспечивает дополнительный уровень защиты от ботнетов и других сложных атак. Это решение сопоставляет подозрительную активность в локальной сетевой среде с данными о тысячах известных кампаний и серверов управления и контроля, благодаря чему обеспечивается высокая точность обнаружения угроз и высокая скорость реагирования на них. Cisco Talos выявляет 1,5 млн уникальных образцов вредоносного ПО и блокирует 20 млрд угроз в день.

Преимущества системы

Благодаря своему уникальному интерфейсу и анализу сетевого трафика система StealthWatch Enterprise в значительной мере совершенствует:

- обнаружение угроз в режиме реального времени;
- реагирование на инциденты и техническую экспертизу;
- сегментацию сети;
- производительность сети и планирование мощностей;
- возможность отвечать регулирующим требованиям.

Необходимые компоненты системы

Flow Rate License

Компонент Flow Rate License необходим для сбора и анализа телеметрических данных о потоке, а также управления ими. Он агрегирует потоки в Management Console. Flow Rate License также определяет объем потоков, которые могут быть собраны, и лицензируется по числу потоков в секунду (fps). Для достижения требуемого уровня емкости потоков можно использовать любое сочетание лицензий.

Flow Collector

Flow Collector использует корпоративные данные телеметрии от NetFlow, IPFIX и другие типы потоковых данных, поступающих из существующей инфраструктуры, например от маршрутизаторов, коммутаторов, межсетевых экранов, оконечных устройств и других сетевых инфраструктурных устройств. Flow Collector также может получать и собирать телеметрические данные от прокси-источников данных, которые можно анализировать с помощью Global Threat Analytics (ранее Cognitive Threat Analytics) — механизма многоуровневого машинного обучения для углубленного мониторинга как сетевого, так и веб-трафика. Кроме того, Stealthwatch Enterprise совместно с Encrypted Traffic Analytics может использовать аналитику для выявления шаблонов вредоносного кода в зашифрованном трафике, чтобы определить угрозы и ускорить реагирование на них. Хотя эта функция встроена в систему без дополнительной платы, ее необходимо включить после развертывания.

Телеметрические данные анализируются для формирования полной картины сетевой активности. Можно хранить данные за несколько месяцев или даже лет, создавая контрольный журнал, который можно использовать для улучшения возможностей технической экспертизы и обеспечения соответствия нормативным требованиям. Объем данных телеметрии, собираемых из сети, определяется исходя из емкости развернутых компонентов Flow Collector. Можно установить несколько компонентов Flow Collector. Компоненты Flow Collector доступны в качестве аппаратных устройств или виртуальных машин. В таблице 1 представлены преимущества Flow Collector.

Таблица 1. Основные преимущества Flow Collector

Преимущество	Описание
Обнаружение угроз	Сбор записей прокси и их сопоставление с записями потоков позволяют получить информацию об URL и пользовательских приложениях для каждого потока, а также повысить степень учета контекстных данных. Такой процесс способствует более точному выявлению угроз в организации и сокращает среднее время обнаружения (Mean Time To Know, MTTK).
Мониторинг потоков трафика	Мониторинг потоков трафика одновременно в сотнях сегментов сети для выявления подозрительного сетевого поведения. Такая функция имеет особую ценность для крупных предприятий.
Длительный период хранения данных	Возможность сохранения организациями и ведомствами больших объемов данных в течение длительных периодов.
Масштабируемость	Бесперебойная работа в высокоскоростных средах и возможность защиты каждого участка сети, охватываемой IP-технологией, независимо от ее размера.
Дедупликация и связывание	Выполнение дедупликации позволяет учитывать любые потоки, проходящие через несколько маршрутизаторов, только один раз. Затем информация о потоках связывается воедино для обеспечения полного мониторинга сетевых операций.
Выбор способов доставки	Можно заказать аппаратную версию Appliance Edition — масштабируемое устройство, подходящее для организации любого размера. Кроме того, для заказа доступна виртуальная версия Virtual Edition, выполняющая те же функции, что и аппаратная версия, но в среде VMware. Данное решение динамически масштабируется в соответствии с выделенными для него ресурсами.

* Максимальное количество потоков в секунду зависит от условий в сети.

Технические характеристики Flow Collector

- Stealthwatch Flow Collector 4200 — номер компонента: ST-FC4200-K9
- Stealthwatch Flow Collector 5200 — номер компонента: ST-FC5200-K9
- Stealthwatch Flow Collector Virtual Edition можно настроить как FCVE-1000, FCVE-2000 или FCVE-4000 — номер компонента: L-ST-FC-VE-K9

Примечание. Эти технические характеристики относятся к системе Stealthwatch версии 6.9.1 и более поздним версиям.

Management Console

Консоль управления Stealthwatch Management Console агрегирует, упорядочивает и представляет результаты анализа данных, получаемые от коллекторов Flow Collector (поддерживается до 25 таких коллекторов), платформы Cisco Identity Services Engine и других источников. В ней используются графические представления сетевого трафика, данные об идентификации, настраиваемые сводные отчеты, а также интегрированная аналитика по безопасности и деятельности сети, что позволяет осуществлять всесторонний анализ.

В зависимости от емкости консоли определяется объем данных телеметрии, которые можно проанализировать и представить, а также количество развертываемых компонентов Flow Collector. Консоль доступна в качестве аппаратного устройства или виртуальной машины. В таблице 2 перечислены преимущества консолей.

Таблица 2. Основные преимущества Management Console

Преимущество	Описание
Данные в режиме реального времени с точностью до минуты	Схема передачи данных для одновременного мониторинга трафика в сотнях сегментов сети позволяет выявить подозрительное сетевое поведение. Такая функция имеет особую ценность для крупных предприятий.
Функция обнаружения угроз безопасности и назначения приоритетов для них	Оперативное обнаружение угроз безопасности и назначение им приоритетов, точное указание на ненадлежащее использование сети и недостаточную производительность, а также управление реакцией на события в организации — все эти возможности доступны из единого центра управления.
Управление устройствами	Настройка, согласование и управление устройствами Cisco StealthWatch, в том числе устройствами Flow Collector, Flow Sensor и UDP Director.
Использование различных типов потоковых данных	Использование различных типов потоковых данных, в том числе NetFlow, стандарт Internet Protocol Flow Information Export (IPFIX, экспорт информации об IP-потоках) и sFlow. В результате недорогая защита сети на основе оценки активности в ней.
Масштабируемость	Поддержка даже самых масштабных сетевых потребностей. Бесперебойная работа в высокоскоростных средах и возможность защиты каждого участка сети, охватываемой IP-технологией, независимо от ее размера.
Контрольные журналы сетевых операций	Ведение полного контрольного журнала всех сетевых операций для более эффективного проведения технической экспертизы.
Настраиваемые схемы связанных потоков в режиме реального времени	Графические представления текущего состояния трафика в организации. Администраторы могут легко создавать схемы имеющихся сетей на основе любых критериев, таких как местоположение, функция или виртуальная среда. Создавая взаимосвязь между двумя группами узлов, операторы могут быстро проанализировать трафик между ними. Затем, просто выбрав интересующую точку передачи данных, они могут получить еще более глубокое представление о том, что происходит в любой момент времени.
Гибкие варианты доставки	Можно заказать физическое устройство, поддерживающее масштабирование и подходящее для организаций любого размера. Кроме того, для заказа доступна виртуальная версия Virtual Edition, выполняющая те же функции, что и аппаратная версия, но в среде VMware.

Технические характеристики консоли управления Management Console

- Stealthwatch Management Console 2200 — номер компонента: ST-SMC2200-K9
- Stealthwatch Management Console Virtual Edition можно настроить как SMC VE или SMC VE 2000 — номер компонента: L-ST-SMC-VE-K9

Примечание. Эти технические характеристики относятся к системе Stealthwatch версии 6.9.1 и более поздним версиям.

Дополнительные компоненты системы

Flow Sensor

Flow Sensor — это дополнительный компонент системы Stealthwatch Enterprise, который создает данные телеметрии для сегментов инфраструктуры коммутации и маршрутизации, не способных генерировать потоки NetFlow самостоятельно. Он также обеспечивает контроль над данными уровня приложений. В дополнение ко всем данным телеметрии, собираемым Stealthwatch, Flow Sensor предоставляет дополнительный контекст безопасности для расширения возможностей аналитики безопасности Stealthwatch. К этому набору данных применяется усовершенствованное поведенческое моделирование и многоуровневое машинное обучение на основе облака для обнаружения сложных угроз и ускорения технической экспертизы.

Flow Sensor устанавливается на зеркалированный порт или сетевой отвод и создает телеметрические данные на основе наблюдаемого трафика. Объем данных телеметрии, получаемых из сети, зависит от емкости развернутых компонентов Flow Sensor. Можно установить несколько компонентов Flow Sensor. Компоненты Flow Sensor доступны в качестве аппаратных или виртуальных устройств для мониторинга сред виртуальных машин. Они также работают в средах, в которых для модели операций ИТ-организации лучше подходит оверлейный мониторинг, требующий дополнительного контекста безопасности.

В таблице 3 перечислены основные преимущества Flow Sensor.

Таблица 3. Основные преимущества Flow Sensor

Преимущество	Описание
Мониторинг работы приложений уровня 7	Обеспечение реального мониторинга работы приложений уровня 7 посредством сбора информации о приложениях и оперативного перехвата пакетов по требованию (PCAP). Включает такие данные, как RTT (время прохождения сигнала в прямом и обратном направлениях), SRT (время отклика сервера), повторные передачи.
Производительность и анализ на уровне пакетов	Обеспечение реального мониторинга работы приложений уровня 7 посредством сбора информации о приложениях и оперативного перехвата пакетов по требованию (PCAP). Включает такие данные, как RTT (время прохождения сигнала в прямом и обратном направлениях), SRT (время отклика сервера), повторные передачи.
Оповещения при возникновении аномалий в сети	Дополнительные данные телеметрии от Flow Sensor, например информация об URL-адресах для веб-трафика и сведения о флагах TCP, помогают создавать предупреждения с использованием контекстной аналитики, позволяя сотрудникам отдела безопасности быстро принять меры и свести ущерб к минимуму.
Сокращение затрат	Повышение эксплуатационной эффективности и сокращение расходов за счет выявления и локализации первопричины возникновения проблемы или инцидента за считаные секунды.
Выбор способов доставки	Можно заказать аппаратную версию Appliance Edition — масштабируемое устройство, подходящее для организации любого размера. Кроме того, для заказа доступна виртуальная версия Virtual Edition, выполняющая ту же функцию, что и аппаратная версия, но в среде VMware или KVM Hypervisor.

* Эти значения получены в наших тестовых средах с использованием усредненных данных заказчиков.

Технические характеристики Flow Sensor

- Stealthwatch Flow Sensor 1200 — номер компонента: ST-FS1200-K9
- Stealthwatch Flow Sensor 2200 — номер компонента: ST-FS2200-K9
- Stealthwatch Flow Sensor 3200 — номер компонента: ST-FS3200-K9
- Stealthwatch Flow Sensor 4200 — номер компонента: ST-FS4200-K9
- Stealthwatch Flow Sensor Virtual Edition — номер компонента: L-ST-FS-VE-K9

Примечание. Эти технические характеристики относятся к системе Cisco Stealthwatch версии 6.9.1 и более поздним версиям.

UDP Director

UDP Director упрощает процесс сбора и распространения данных о сети и системе информационной безопасности на предприятии. Этот компонент позволяет сократить интенсивность обработки операций на сетевых маршрутизаторах и коммутаторах. Для этого он получает необходимую информацию о сети и системе безопасности из нескольких источников и далее направляет ее в единый поток данных по одному или нескольким направлениям. В таблице 4 перечислены основные преимущества UDP Director.

Таблица 4. Основные преимущества UDP Director

Преимущество	Описание
Сокращение числа незапланированных простоев и прерываний обслуживания	Функция обеспечения высокого уровня доступности UDP Director High Availability присутствует только на устройствах UDP Director 2200.
Упрощение процессов мониторинга и обеспечения безопасности сети	UDP Director агрегирует и предоставляет единую стандартизированную точку сбора информации, передаваемой через NetFlow, sFlow, системный журнал и протокол SNMP. Устройства UDP Director способны получать данные от любого приложения UDP без создания подключений, а затем передавать их в несколько точек назначения, дублируя данные при необходимости.
Возможность направления данных UDP из любого источника в любую точку назначения	Получение данных от любого приложения UDP без создания подключений и их последующая передача в несколько точек назначения с дублированием данных при необходимости.
Устранение необходимости в перенастройке инфраструктуры	Направление данных журналов (NetFlow, sFlow, системного журнала, SNMP) в единую точку назначения без необходимости повторной настройки инфраструктуры при добавлении или удалении инструментов.

Технические характеристики UDP Director

- Stealthwatch UDP Director 2200 — номер компонента: ST-UDP2200-K9
- Cisco Stealthwatch UDP Director Virtual Edition — номер компонента: L-ST-UDP-VE-K9

Информация для заказа

Руководство по оформлению заказа на систему Cisco Stealthwatch поможет получить общее представление о моделях, компонентах и типах лицензирования системы. Обратитесь к своему представителю по работе с заказчиками для размещения заказа.

Обслуживание и поддержка

Для Cisco Stealthwatch доступны различные программы обслуживания. Подобные услуги позволят защитить инвестиции в сетевую инфраструктуру, оптимизировать сетевые операции, подготовить сеть к внедрению новых приложений, чтобы расширить возможности сетевой аналитики и вывести бизнес на новый уровень. Дополнительные сведения о профессиональных услугах см. на главной странице службы технической поддержки.

Cisco Capital

Программы финансирования Cisco Capital® помогут вам приобрести технологии, необходимые для достижения поставленных целей и обеспечения конкурентоспособности, уже сегодня. Мы поможем вам снизить капитальные затраты. Развивайтесь еще быстрее. Оптимизировать капиталовложения и повысить окупаемость инвестиций. Программы финансирования Cisco Capital обеспечивают широкие возможности для приобретения оборудования, программного обеспечения, сервисов и дополнительного оборудования сторонних производителей. И всего один прогнозируемый платеж. Программами Cisco Capital можно воспользоваться более чем в 100 странах. Узнайте больше.

Дополнительная информация

Для получения дополнительной информации о системе Cisco Stealthwatch посетите страницу https://www.cisco.com/go/stealthwatch или обратитесь к представителю службы по работе с заказчиками Cisco Security, чтобы узнать, каким образом ваша организация может обеспечить мониторинг распределенной сети, приняв участие в дополнительной оценке эффективности мониторинга сети с помощью Stealthwatch.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Отпечатано в США. C78-739398-03 04/18

