Система Stealthwatch

Система Stealthwatch® обеспечивает лучшие в отрасли возможности мониторинга сети и анализа безопасности для ускорения и более точного обнаружения угроз, реагирования на инциденты и проведения расследований.

С помощью Netflow и других телеметрических данных, полученных из существующей инфраструктуры, это решение позволяет экономически эффективно превратить всю сеть в сенсорную систему. Решение позволяет обнаруживать аномальный трафик и поведение, включая вредоносное ПО нулевого дня, распределенные атаки отказа в обслуживании (DDoS), внутренние угрозы, а также новейшие целенаправленные угрозы (APT). Система Stealthwatch снабжена интуитивно понятным веб-интерфейсом. Она обеспечивает единое представление о горизонтальном движении трафика в сети. Кроме того, система предоставляет высокотехнологичные возможности для анализа и оповещений. Эта простая, удобная и мощная платформа расширяет возможности для использования, анализа безопасности и раннего обнаружения угроз.

Преимущества

Благодаря своему уникальному ракурсу и анализу сетевого трафика система Stealthwatch значительно улучшает:

- обнаружение угроз в режиме реального времени;
- реагирование на инциденты и расследования;
- сегментацию сети;
- производительность сети и планирование пропускной способности;
- возможности для обеспечения соответствия регулятивным требованиям.

Консоль управления системы Stealthwatch

Консоль управления системы Stealthwatch Management Console обеспечивает единую точку наблюдения для распределенных ИТ-групп с возможностью просмотра контекстуальной информации обо всей активности в сети. Простой наглядный интерфейс позволяет операторам быстро находить проблемы и реагировать соответствующим образом.

Мощность консоли определяет объем данных Netflow, которые могут быть проанализированы и отображены, а также количество сборщиков данных потока Stealthwatch Flow Collector, которое можно развернуть. Консоль предлагается в виде аппаратного устройства или виртуальной машины.

В таблицах 1–3 указаны преимущества консоли, ее модели и технические характеристики.

Консоль управления Stealthwatch обеспечивает следующие основные функции.

- Отслеживание пользователей
- Гибкие возможности развертывания, включая виртуальные устройства
- Быстрый анализ основной причины и устранение неполадок
- Реляционные карты потоков
- Сшивка NAT
- Настраиваемые инструментальные панели (dashboard)
- Настраиваемые отчеты
- Автоматизированная блокировка, устранение проблем и ограничение скорости
- Отчеты типа Top-N для приложения, сервисов, портов, протоколов, узлов, одноранговых узлов и сеансов
- Разбивка трафика на составляющие
- Настраиваемый пользовательский интерфейс на базе технологии Point-of-View™

- Поддержка многогигабитных сетевых сред и крупномасштабных сетевых сред с многопротокольной коммутацией на основе меток (MPLS)
- Расширенная визуализация потока
- Массовая масштабируемость
- Комбинированный внутренний и внешний мониторинг
- Планирование пропускной способности и определение тенденций на базе исторических данных о трафике
- Отчетность об оптимизации WAN
- Использование полосы пропускания с поддержкой точки кода дифференцированных услуг (DSCP)
- Визуализация распространения червей
- Внутренняя защита для высокоскоростных сетей

Таблица 1. Основные преимущества консоли управления Stealthwatch

Преимущество	Описание
Данные в режиме реального времени с ежеминутным обновлением	Обеспечивает предоставление потока данных для одновременного мониторинга трафика через сотни сетевых сегментов для выявления подозрительного поведения сети. Эта функция особенно ценна на уровне предприятия.
Возможность обнаружения и приоритизации угроз безопасности	Быстро обнаруживает и приоритизирует угрозы безопасности, точно определяет ненадлежащее пользование сетью и неоптимальную производительность, а также управляет реагированием на события в рамках одного центра управления.
Сетевые группы	Создает сетевые группы и карты отношений для простого представления состояния трафика в организации. В течение считаных секунд рабочие группы и группы безопасности могут точно увидеть места, которые требуют их внимания.
Графическое представление	Обеспечивает графическое представление состояния сети в ясном и простом для понимания формате.
Быстрая оценка состояния защиты	Отображает несколько категорий оповещения на начальной инструментальной панели, чтобы операторы могли быстро оценить состояние защиты организации.
Управление устройствами Stealthwatch	Настраивает устройства Stealthwatch, координирует их и управляет ими, включая устройства Flow Collector (сборщик данных потока), Flow Sensor (сенсор потока) и IDentity.
Использование нескольких типов данных потока	Использует несколько типов данных потока, включая Netflow, экспорт информации о потоке интернет-протокола Internet Protocol Flow Information Export (IPFIX) и sFlow. Результат: экономичная защита сети на основе поведения.
Масштабируемость	Поддерживает даже самые большие потребности сети. Отлично работает в сверхбыстродействующих средах и в состоянии обеспечить защиту каждой части сети с доступностью по IP-адресу вне зависимости от размера.
Выбор методов реализации	У вас есть возможность заказать Appliance Edition — масштабируемое устройство для организаций любого размера. Кроме того, можно заказать Virtual Edition, которое разработано для выполнения тех же функций, что и Appliance Edition, но в среде VMware.
Расширенный функционал управления сетью	Обеспечивает расширение возможностей для управления сетью за счет анализа тенденции, сетевого экрана и планирования пропускной способности, а также мониторинга производительности.
Обработка угроз APT, вредоносного ПО и внутренних угроз	Обеспечивает глубокий анализ и контекст, необходимые для отражения возникающих угроз. К ним относится все, от червей, вирусов и другого вредоносного ПО до целевых атак, попыток атак DDoS, внутренних угроз и угроз APT. Обеспечивает оповещения с контекстуальной информацией, которая нужна специалистам по безопасности для принятия быстрых и решительных мер с целью предотвращения потенциального ущерба.
Журналы аудита для сетевых транзакций	Обеспечивает полные журналы аудита всех сетевых транзакций для более эффективных расследований.
Настраиваемые реляционные карты потока, работающие в режиме реального времени	Обеспечивает графические представления текущего состояния трафика организации. Администраторы могут легко создавать карты своих сетей на базе любого критерия, например местоположения, функции или виртуальной среды. Создавая соединение между двумя группами узлов, операторы могут быстро анализировать обмен трафиком между ними. Затем, просто выбрав интересующую их точку передачи данных, они могут выполнять еще более глубокий анализ того, что происходит в тот или иной момент времени.

Таблица 2. Модели консоли управления системы Stealthwatch

Модель	Максимальное поддерживаемое количество сборщиков данных потока	Емкость хранилища потока
Stealthwatch Management Console VE	До 5	1 ТБ
Stealthwatch Management Console 1000	5	1 ТБ
Stealthwatch Management Console 2000	25	ТБ

Таблица 3. Технические характеристики консоли управления системы Stealthwatch по моделям

	SMC 500 и 1010	SMC 2010
Сеть	1 порт управления: 10/100/1000BASE-TX, по медному проводу	
Емкость базы данных	1 ТБ (RAID 6 с резервируемостью)	2 ТБ (RAID 6 с резервируемостью)
Аппаратная платформа	R630	
Поколение оборудования	13G	
Форм-фактор (при монтаже в стойку)	1RU	
Электропитание	Резервируемое, 750 Вт перем. тока, 50/60 Гц, автоматическая настройка диапазона (от 100 до 240 В)	
Рассеиваемая тепловая мощность	2891 брит. тепл. единиц в час макс.	
Габариты	Высота: 1,68 дюйма (4,3 см) Ширина: 17,08 дюйма (43,4 см) Глубина: 27,25 дюйма (69,2 см)	
Вес устройства:	41 фунт (18,6 кг)	
Рельсы	Направляющие рельсы с держателем кабеля	
Нормативные требования	FCC (только США) Класс A DOC (Канада) Класс A Знак CE (EN 55022 Класс A, EN55024, EN61000-3-2, EN61000-3-3, EN60950) VCCI Класс A UL 1950 CSA 950	

Примечание. Технические характеристики выше относятся к устройству Stealthwatch 6.7.

Сборщик данных потока Stealthwatch

Сборщик данных потока Stealthwatch Flow Collector обеспечивает мониторинг сети и анализ безопасности в физических и виртуальных средах в целях улучшения реагирования на инциденты.

Объем телеметрических данных Netflow, собранных из сети, определяется емкостью развернутых сборщиков данных потока. Имеется возможность для установки нескольких сборщиков данных потока. Сборщики данных потока предлагаются в виде аппаратных устройств или виртуальных машин. В таблице 4 указаны преимущества сборщика данных потока, а в таблице 5 его технические характеристики.

Таблица 4. Основные преимущества сборщика данных потока Stealthwatch

Преимущество	Описание
Расширенный контекст потока	Анализирует URL-адрес и данные пользователя, полученные от прокси-серверов, и связывает их с соответствующими данными потока в сети.
Улучшенный мониторинг трафика	Улучшает мониторинг для системы Stealthwatch с учетом сетевых сеансов, которые проходят через веб-прокси.
Мониторинг набора угроз SLIC	Автоматически сравнивает данные URL-адреса в записях прокси с набором угроз центра аналитики лабораторий Stealthwatch Labs Intelligence Center (SLIC).
Поддержка расследований	Анализ данных консоли в ручном режиме.
Высокая точность	Обеспечивает данные контекста для системы Stealthwatch для повышения точности событий безопасности.
Корреляция данных прокси-сервера и потока	Анализирует URL-адрес и данные пользователя, полученные от прокси-серверов, и ассоциирует их с соответствующими данными потока в сети. Эта информация автоматически сравнивается с набором

Преимущество	Описание
	угроз SLIC. Она также используется для поддержки расследования в ручном режиме в рамках консоли.
Мониторинг	Устраняет «белые пятна» в сети, предоставляя организациям возможность просматривать транслированные адреса, связанные с другой стороной в прокси-сеансе.
Обнаружение угроз	Анализирует записи прокси и ассоциирует их с записями потока, указывая пользовательское приложение и информацию об URL-адресе для каждого потока с целью повышения уровня контекстуальной осведомленности. Этот процесс расширяет возможности вашей организации с точки зрения точного определения угроз и сокращает среднее время получения сведений о них (MTTK).
Реагирование на инциденты	Обеспечивает дополнительный контекст для веб-трафика, который передается через прокси-сервер, для более точного устранения неполадок, реагирования на инциденты и проведения расследований.
Анализ трафика в режиме реального времени	Обеспечивает анализ трафика в режиме реального времени для выставления счетов, учета использования полосы пропускания, а также для устранения неполадок, связанных с производительностью сети.
Мониторинг потока трафика	Обеспечивает одновременный мониторинг потока трафика через сотни сетевых сегментов для выявления подозрительного поведения сети. Эта функция особенно ценна на уровне предприятия.
Определение основной причины проблемы с защитой	Локализует основную причину в считаные секунды для ускоренного реагирования на инциденты безопасности.
Аналитика, имеющая практическую ценность	Обеспечивает получение аналитических данных о производительности, имеющих практическую ценность, без использования дорогостоящих сенсоров.
Увеличенный срок хранения данных	Позволяет организациям и агентствам сохранять большие объемы данных в течение длительных периодов.
Использование нескольких типов данных потока	Использует несколько типов данных потока (Netflow, IPFIX и sFlow) для обеспечения экономичной защиты сети на основе поведения.
Масштабируемость	Отлично работает в сверхбыстродействующих средах и в состоянии обеспечить защиту каждой части сети с доступностью по IP-адресу вне зависимости от размера.
Дедупликация и сшивка	Выполняет дедупликацию для того, чтобы любые потоки, которые могут пройти более чем через один маршрутизатор, учитывались только один раз. Затем информация о потоках собирается вместе, чтобы обеспечить полный мониторинг сетевых транзакций.
Комплексный мониторинг географически распределенных сетей	Выполняет агрегирование данных о поведении высокоскоростных сетей, полученных от нескольких сетей или сетевых сегментов, для обеспечения комплексной защиты и повышения производительности всех географически распределенных сетей.
Выбор методов реализации	У вас есть возможность заказать Appliance Edition — масштабируемое устройство для организаций любого размера. Кроме того, можно заказать Virtual Edition, которое разработано для выполнения тех же функций, что и Appliance Edition, но в среде VMware. Решение масштабируется автоматически в соответствии с выделенными для него ресурсами.

Таблица 5. Технические характеристики сборщика данных потока системы Stealthwatch по моделям

	FC 1010	FC 2010	FC 4010	FC 5020
Описание	Резервируемое питание, хранилище данных и дополнительные интерфейсы для сбора данных потока на нескольких интерфейсах. Достаточная мощность для средних и больших сетей.	Полная аппаратная резервируемость и мощность обработки потока для сверхбольших сред Netflow, sFlow или IPFIX.	Массовая масштабируемость с возможностями расширения хранилища и обработки очень больших объемов данных потока.	Решение большой мощности для анализа потока, созданное для корпоративных заказчиков, которым необходима исключительная производительность. Построено на платформе Cisco UCS.
Макс. количество потоков в секунду *	До 30 000	До 60 000	До 120 000	До 240 000
Макс. количество экспортеров или маршрутизаторов	500	1000	2000	4096
Аппаратная платформа	R630	R630	R630	• **Модуль:** UCSC-C220-M4S • **Узел базы данных:**UCSC-C240-M4S2

	FC 1010	FC 2010	FC 4010	FC 5020
Сеть	1 порт управления: 10/100/1000BASE-TX, по медному проводу 3 монитора или слушающих порта			• 1 выделенный порт управления 1 Гбит/с • 1 порт 10000SFP + канал исходящей связи к узлу модуля/ базы данных • 2 порта контроллера Intel i350 GbE Ethernet (LAN1, LAN2)
Хранилище данных потока	1 ТБ (RAID 6 с резервируемостью)	2 ТБ (RAID 6 с резервируемостью)	4 ТБ (RAID 6 с резервируемостью)	8 ТБ (RAID 10 с резервируемостью)
Поколение оборудования	13G			
Форм-фактор (при монтаже в стойку)	1RU		2RU	• **Модуль:** 1RU • **Узел базы данных:** 2RU
Электропитание	Резервируемое, 750 Вт перем. тока, 50/60 Гц, автоматическая настройка диапазона (от 100 до 240 В)			• **Модуль:** резервные источники питания 770 Вт (1 + 1) • **Узел базы данных:** резервные источники питания 1200 Вт (1 + 1)
Рассеиваемая тепловая мощность	2891 брит. тепл. единиц в час макс.			**Модуль:** 2891 брит. тепл. единиц в час макс. **Узел базы данных:** 4100 брит. тепл. единиц в час макс.
Габариты	• **Высота:** 1,68 дюйма (4,3 см) • **Ширина:** 17,08 дюйма (43,4 см) • **Глубина:** 27,25 дюйма (69,2 см)	• **Высота:** 1,68 дюйма (4,3 см) • **Ширина:** 17,08 дюйма (43,4 см) • **Глубина:** 27,25 дюйма (69,2 см)	• **Высота:** 3,4 дюйма (8,7 см) • **Ширина:** 17,5 дюйма (44,4 см) • **Глубина:** 27,25 дюйма (69,2 см)	**Модуль:** • **Высота:** 1,7 дюйма (4,32 см) • **Ширина:** 16,89 дюйма (43,0 см) • **Глубина:** 29,8 дюйма (75,6 см) **Узел базы данных** • **Высота:** 3,43 дюйма (8,7 см) • **Ширина:** 17,65 дюйма (44,8 см) • **Глубина:** 29,0 дюйма (73,8 см)
Масса	41 фунт (18,6 кг)		65 фунтов (29,5 кг)	• **Модуль:** 38 фунтов (17,24 кг) • **Узел базы данных:** 65 фунтов (29,48 кг)
Рельсы	Направляющие рельсы с держателем кабеля			Направляющие рельсы (UCSC-RAILB-M4)
Нормативные требования	• FCC (только США) Класс A • DOC и ICES (Канада) Класс A • Знак CE (EN55022 Класс A, EN55024, EN61000-3-2, EN 61000-3-3, EN60950) • VCCI Класс A UL 1950 • CSA 950 • Напишите по адресysales@lancope.com для получения полного списка.			• Продукты должны соответствовать требованиям, предъявляемым к маркировке CE, согласно директивам 2004/108/EC и 2006/95/EC • UL 60950-1, второе издание • CAN/CSA-C22.2 № 60950-1, второе издание • EN 60950-1, второе издание • IEC 60950-1, второе издание • AS/NZS 60950-1 • GB4943 2001 • Напишите по адресysales@lancope.com для получения полного списка.
Виртуальные сборщики данных потока				

	FC 1010	FC 2010		FC 4010	FC 5020
L-LC-FC-NF-VE-K9	Сборщик данных потока для NetFlow Virtual Edition	30 000 *	1000 *	1,0 ТБ	Виртуальный
L-LC-FC-SF-VE-K9	Сборщик данных потока для sFlow Virtual Edition	30 000 *	1000 *	1,0 ТБ	Виртуальный
L-LC-SW-VE-CONV-K9	Переход с физического устройства на Virtual Edition				

Примечание. Технические характеристики выше относятся к устройству Stealthwatch 6.7.

* Максимальное количество потоков в секунду может изменяться в зависимости от состояния сети.

Сенсор потока Stealthwatch

Сенсор потока Stealthwatch Flow Sensor — это компонент, обеспечивающий создание данных Netflow для сегментов коммутирующей и маршрутизирующей инфраструктуры, которая не поддерживает Netflow. Он также работает в средах, в которых оверлейное решение мониторинга больше подходит для операционной модели ИТ-организации. Сенсор потока может обеспечивать информацию о приложениях уровня 7 для сред, в которых не поддерживается технология распознавания приложений средствами сети Cisco® Network-Based Application Recognition (NBAR).

Сенсор потока обеспечивает комплексный мониторинг сети, а также получение показателей производительности серверов. Он объединяет глубокий анализ пакетов (DPI) с анализом поведения для определения приложений и протоколов. В результате обеспечивается оптимизированная защита, эксплуатация сети и производительность приложений.

Объем данных Netflow, созданных в сети, определяется емкостью развернутых сенсоров потока. Имеется возможность для установки нескольких сенсоров потока. Сенсоры потока предлагаются в виде аппаратных устройств или программного обеспечения для мониторинга сред на базе виртуальных машин. В таблицах 6 и 7 приведены основные преимущества и технические характеристики сенсоров потока.

Сенсор потока Stealthwatch обеспечивает следующие основные функции.

- Контекст приложения уровня 7
- Мониторинг потока
- Создание данных Netflow
- Мониторинг виртуальной среды
- Обновления в режиме реального времени для текущих угроз
- Вычисление времени передачи обоих пакетов (RTT) и времени отклика сервера (SRT) для TCP-соединений

Таблица 6. Основные преимущества сенсора потока Stealthwatch

Преимущество	Описание
Обзор приложений уровня 7	Обеспечивает мониторинг приложения уровня 7 за счет сбора информации о приложении вместе со статистикой производительности на уровне пакетов.
Производительность и анализ на уровне пакетов	Обеспечивает мониторинг приложения уровня 7 за счет сбора информации о приложении вместе со статистикой производительности на уровне пакетов.
Оповещения об аномалиях в сети	Точно определяет необычное поведение сети и немедленно отправляет оповещения с контекстуальной аналитикой для того, чтобы специалисты по безопасности могли быстро предпринять необходимые действия и предотвратить ущерб.
Снижение затрат	Повышает операционную эффективность и уменьшает затраты благодаря определению и локализации основных причин проблемы или инцидента в течение считаных секунд
Выбор методов реализации	У вас есть возможность заказать Appliance Edition — масштабируемое устройство для организаций любого размера. Кроме того, можно заказать Virtual Edition, которое разработано для выполнения тех же функций, что и Appliance Edition, но в среде VMware.

Таблица 7. Технические характеристики сенсоров потока Stealthwatch

	FS 1010	FS 2010	FS 3010	FS 4010
Обмен данными				
Пропускная способность	1,0 Гбит/с (пакеты 512 байтов) 400 Мбит/с (пакеты 64 байта)	2,5 Гбит/с (пакеты 512 байтов) 800 Мбит/с (пакеты 64 байта)	5,0 Гбит/с (пакеты 512 байтов) 1,2 Гбит/с (пакеты 64 байта)	20,0 Гбит/с (пакеты 512 байтов) 4 Гбит/с (пакеты 64 байта)
Интерфейсы				
Порт управления	1 порт: 10/100/1000BASE-TX, по медному проводу			
Порт мониторинга	3 порта: 10/100/1000BASE-TX, по медному проводу	5 портов: 1 ГБ (5 по медному проводу или 3 по медному проводу и 2 оптоволоконных); рассчитан на мониторинг 2,5 Гбит/с	2 порта: 10 ГБ, оптоволоконный; рассчитан на мониторинг 5 Гбит/с (всего)	4 порта: 10 ГБ, оптоволоконный; рассчитан на мониторинг 20 Гбит/с (всего)
Консольный порт	Последовательный, виртуальная машина на основе ядра (KVM)			
Физические характеристики				
Аппаратная платформа	R220	R630		
Поколение оборудования	12G	13G		
Форм-фактор		Стекируемые		
Габариты	**Высота:** 1,67 дюйма (4,24 см) **Ширина:** 17,09 дюйма (43,4 см) **Глубина:** 15,5 дюйма (39,37 см)	**Высота:** 1,68 дюйма (4,3 см) **Ширина:** 18,99 дюйма (48,24 см) с фиксаторами в стойке; 17,08 дюйма (43,4 см) без фиксаторов в стойке **Глубина:** 29,25 дюйма (74,3 см)		
Масса	35 фунтов (15,4 кг)	41 фунт (18,6 кг) в максимальной конфигурации		
Хранилище	500 ГБ, без резервируемости	300 ГБ (RAID 1 с резервируемостью)		
Требования к условиям окружающей среды				
Электропитание	Один блок; 250 Вт (без резервируемости)	Резервируемое, 750 Вт перем. тока, 50/60 Гц, автоматическая настройка диапазона (от 100 до 240 В)		
Рассеиваемая тепловая мощность	1040 брит. тепл. единиц в час	2891 брит. тепл. единиц в час макс.		
Температурный диапазон	При работе: от 10 до 35 °C (от 50 до 95 °F) Хранение: от –40 до 65 °C (от –40 до 149 °F)	При работе: от 10 до 35 °C (от 50 до 95 °F) с максимальным изменением 10 °C (50 °F) в час. Примечание. При использовании на высоте более 2950 футов (900 м) максимальная рабочая температура уменьшается на –17 °C (1 °F) на 550 футов (168 м). Хранение: от –40 до 65 °C (от –40 до 149 °F) с максимальным изменением 20 °C (68 °F) в час.		
Относительная влажность	При работе: от 10 до 80 % (без конденсации) с максимальным изменением 10 % в час. Хранение: от 5 до 95 % (без конденсации)			
Соответствие нормативным требованиям	CE выбросы/FCC Класс A/RoHS	FCC (только США) Класс A DOC (Канада) Класс A VCCI Класс A/UL 1950/CSA 950 Знак CE (EN 55022 Класс A, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 60950)		

Примечание. Технические характеристики выше относятся к устройству Stealthwatch 6.7.

Виртуальный сенсор потока

Номер компонента продукта	Описание	Макс. сетевой трафик	Порты мониторинга сети	Формфактор
Виртуальный сенсор потока				
L-LC-FSVE-VMW-K9	Виртуальное устройство Flow Sensor для VMware	*	—	Виртуальный
L-LC-SW-VE-CONV-K9	Переход с физического устройства на Virtual Edition			

* В зависимости от ресурсов виртуальной машины.

Примечание. Потоки, созданные устройством Flow Sensor или Flow Sensor VE, не учитываются при определении общих лимитов по лицензии Flow Collection.

Устройство Stealthwatch UDP Director

Устройство UDP Director® упрощает сбор и распространение данных сети и безопасности в рамках предприятия. Оно помогает уменьшить вычислительную мощность сетевых маршрутизаторов и коммутаторов за счет получения необходимой информации о сети и защите из нескольких мест, а затем переадресовывает эту информацию в единый поток данных и направляет его одному или нескольким получателям.
В таблицах 8 и 9 приведены основные преимущества и характеристики устройства.

Таблица 8. Основные преимущества устройства Stealthwatch UDP Director

Преимущество	Описание
Сокращает незапланированное время простоев и прерывания в обслуживании	Функция высокой доступности UDP Director High Availability предлагается только на устройствах UDP Director 2000. Она не поддерживается на устройствах серии 1000.
Упрощает защиту сети и мониторинг	Устройство UDP Director выполняет агрегацию и представляет собой единого стандартизованного получателя для Netflow, sFlow, системных журналов, а также информации упрощенного протокола управления сетью (SNMP). Выполняя эту функцию, устройство значительно упрощает интегрирование нескольких типов данных сети и безопасности на крупных предприятиях. Устройства UDP Director могут получать данные от любых UDP-приложений, не требующих установки соединений, а затем передавать их нескольким получателям, дублируя данные, если это необходимо.
Поддерживает любые UDP-приложения, не требующие соединений	Записи tFlow, отправленные от нескольких маршрутизаторов, могут быть реплицированы для нескольких сборщиков Netflow. Такая гибкость позволяет отказаться от спецификаций различных получателей Netflow в конфигурации экспортера Netflow. Выборки sFlow, отправленные от нескольких маршрутизаторов или коммутаторов, могут быть реплицированы для нескольких сборщиков данных sFlow. Как и в примере с Netflow, это позволяет отказаться от нескольких спецификаций получателей sFlow в конфигурации экспортера sFlow. Сообщения системного журнала могут автоматически реплицироваться для нескольких сборщиков данных системного журнала. SNMP-прерывания от маршрутизаторов, коммутаторов и других сетевых устройств могут автоматически собираться и распределяться нескольким станциям управления SNMP.
Возможность направления данных UDP от любого источника любому получателю	Получает данные от любых UDP-приложений, не требующих установки соединений, а затем передает их нескольким получателям, дублируя данные, если это необходимо.
Отсутствует необходимость перенастраивать инфраструктуру	Направляет данные журнала для точки (Netflow, sFlow, системный журнал, SNMP) одному получателю без необходимости перенастраивать инфраструктуру при добавлении или удалении новых средств.
Предоставляет подробную статистику потока	Использует функцию Flow Statistics (статистика потока), чтобы помочь организациям оценить количество потоков в секунду (к/с) в их средах и определить свои требования к мониторингу.
Уменьшает время конфигурации для сетевой инфраструктуры	Упрощает защиту сети и мониторинг.
Уменьшает полосу пропускания	Обеспечивает меньше дублирований данных журнала сети, уменьшая использование полосы пропускания WAN.
Сокращает прерывания в обслуживании	Сокращает незапланированное время простоев и прерывания в обслуживании.

Таблица 9. Технические характеристики устройства UDP Director

	UDP Director 1010	UDP Director 2010
Скорость репликации пакетов (вход) **	25 000 пак. в секунду (pps)	37 500 пак. в секунду (pps)
Скорость репликации пакетов (выход) **	50 000 пак. в секунду (pps)	75 000 пак. в секунду (pps)
Сеть	• 1 порт управления: 10/100/1000BASE-TX, по медному проводу • 1 монитор или слушающий порт • Интегрированный пользовательский веб-интерфейс HTTPS; последовательный и KVM доступ к интерфейсу командной строки (CLI)	• 1 порт управления: 10/100/1000BASE-TX, по медному проводу • 3 монитора или слушающих порта • Дополнительно: 2 дополнительные оптоволоконные однопортовые сетевые интерфейсные платы (NIC), Гбит/с
Хранилище	160 ГБ, без резервируемости	300 ГБ, RAID 6 с резервируемостью
Аппаратная платформа	R220	R630
Поколение оборудования	12G	13G
Форм-фактор (при монтаже в стойку)	1RU	
Электропитание	Один источник питания (250 Вт)	• Резервный источник питания 750 Вт перем. тока, 50/60 Гц • Автоматическая настройка диапазона (от 100 до 240 В)
Рассеиваемая тепловая мощность	1039 брит. тепл. единиц в час макс.	2891 брит. тепл. единиц в час макс.
Операционная система	Hardened Linux	
Габариты	**Высота:** 1,67 дюйма (4,24 см) **Ширина:** 17,09 дюйма (43,4 см) **Глубина:** 15,5 дюйма (39,37 см)	**Высота:** 1,68 дюйма (4,3 см) **Ширина:** 18,99 дюйма (48,24 см) с фиксаторами в стойке; 17,08 дюйма (43,4 см) без фиксаторов в стойке **Глубина:** 29,25 дюйма (74,3 см) с источниками питания и держателем; 27,25 дюйма (69,2 см) без источников питания и держателя
Масса устройства	34 фунта (15 кг)	65 фунтов (29,5 кг)
Рельсы	Шасси для стойки с рельсами Versa Rail, круглые отверстия для стоек сторонних производителей	Направляющие рельсы с держателем кабеля
Нормативные требования	FCC (только США) Класс A DOC (Канада) Класс A Знак CE (EN 55022 Класс A, EN55024, EN61000-3-2, EN61000-3-3, EN60950) VCCI Класс A UL 1950	

Устройство Virtual Edition UDP Director

Номер компонента продукта	Описание	Макс. кол. пакетов (вход) (п/с)	Макс. кол. пакетов (выход) (п/с)	Порт монитора	Формфактор
L-LC-UDP-VE-K9	Лицензия UDP Director VE				

* В зависимости от ресурсов виртуальной машины.

Лицензия Proxy

Компонент Proxy License обеспечивает аналитиков по вопросам защиты сети еще большими возможностями для мониторинга сети и обнаружения угроз. Он получает дополнительный контекст, связанный с сеансами, с другой стороны прокси-сервера, а это помогает принимать более взвешенные решения при возникновении угроз безопасности.

Функция Proxy License поддерживает следующие веб-прокси.

- Blue Coat
- McAfee
- Squid
- Cisco

В таблице 10 приводится информация для заказа компонента Proxy License.

Таблица 10. Информация для заказа лицензии Proxy

Номер компонента	Описание
PX-100-U	Лицензия для сбора, сопоставления и анализа записей прокси-сервера не более чем для 100 пользователей
PX-1000-U	Лицензия для сбора, сопоставления и анализа записей прокси-сервера не более чем для 1000 пользователей
PX-10000-U	Лицензия для сбора, сопоставления и анализа записей прокси-сервера не более чем для 10 000 пользователей
PX-25K-U	Лицензия для сбора, сопоставления и анализа записей прокси-сервера не более чем для 25 000 пользователей
PX-50K-U	Лицензия для сбора, сопоставления и анализа записей прокси-сервера не более чем для 50 000 пользователей
PX-100K-U	Лицензия для сбора, сопоставления и анализа записей прокси-сервера не более чем для 100 000 пользователей

Облачная лицензия Stealthwatch Cloud

Рабочие нагрузки все чаще перемещают из локальных сред в облачные. Несмотря на то, что это создает больше гибкости для вашей организации, в результате ограничивается возможность просматривать потоки трафика в таких виртуальных экземплярах. Однако лицензия Stealthwatch Cloud обеспечивает полноценный мониторинг сети, обнаружение угроз и аналитические возможности системы Cisco Stealthwatch в общедоступных, частных и гибридных облачных средах. Лицензия Stealthwatch Cloud — это дополнение виртуальной лицензии к системе Cisco Stealthwatch, которая расширяет и использует сеть как сенсор в облаке, поддерживая ситуационную осведомленность в режиме реального времени, а также улучшенную защиту всей инфраструктуры.

Функция Cisco Stealthwatch Cloud License поддерживает установку веб-сервисов Amazon Web Services (AWS) — сервисы облачных вычислений.

В настоящее время компонент поддерживает следующие операционные системы узлов.

- Linux
- CentOS 5, 6 и 7 (только x64)
- RedHat Enterprise Linux 5, 6 и 7 (только x64)

В таблице 11 указаны основные функции и преимущества компонента. В таблице 12 приводится информация о размерах.

Таблица 11. Функции и преимущества облачной лицензии

Преимущество	Описание
Улучшенный мониторинг	Расширяет возможности сети и использует ее как сенсор в облаке, устраняя «белые пятна» в общедоступной, частной и гибридной облачной инфраструктуре.
Повышенная безопасность	Обеспечивает повышенную безопасность за счет обнаружения угроз на основе подозрительной активности и потенциальных атак.
Ускоренное реагирование	Обеспечивает возможности для расследования высочайшего уровня со сложными функциями анализа безопасности.
Улучшенное соответствие нормативным требованиям	Обеспечивает ситуационную осведомленность и обзор сети в режиме реального времени для соответствия нормативным требованиям всей сети.

Таблица 12. Информация о размерах концентратора облачной лицензии

Операторы	Тип экземпляра Rec AWS	Эквивалент виртуального устройства			
		Ядра ЦП	Память (ГБ)	Диск (ГБ)	Пропускная способность сети
1000	c4.large	2	4	8	250 Мбит/с
2000	c4.xlarge	4	8	16	500 Мбит/с
4000	c4.2xlarge	8	16	32	1 Гбит/с
10 000	c4.4xlarge	16	32	64	2 Гбит/с
20 000	c4.8xlarge	32	64	64	4 Гбит/с

Использование ресурсов агентом облачной лицензии

Использование ресурсов зависит от объема активности, возникающей на узловой виртуальной машине (ВМ), на которой развернут агент.

- 1 % ЦП типично, 5 % максимально
- 128–200 МБ RAM, 1–2 % типично, ~1 % в наихудшем случае
- < 1 ГБ дискового пространства

Основные референсные точки конечного использования:

- ЦП: 8 ядер, при использовании 100 %
- RAM: ~ 20 тыс. соединений, комбинация активных/неактивных

Информация для заказа облачной лицензии

Таблица 13. Информация для заказа облачной лицензии

Base PID	Уровни
L-SW-CL-LIC=	1–400 узлов
	401–800 узлов
	801–1200 узлов
	1201–2000 узлов
	2001–6000 узлов
	6001–20 000 узлов
	20 001–80 000 узлов
	80 001–200 000 узлов
	200 001–400 000 узлов
	400 001–2 000 000 узлов

Лицензия Stealthwatch Flow

Лицензия Stealthwatch Flow требуется для агрегирования потоков на консоли управления системы Stealthwatch. Лицензии Flow также определяют объем потоков, который может собираться. Лицензии могут комбинироваться в любом сочетании для получения необходимого уровня пропускной способности. Доступные варианты лицензий:

- 1000 потоков
- 10 000 потоков
- 25 000 потоков
- 50 000 потоков
- 100 000 потоков

Информация для заказа

Руководство для заказа системы Stealthwatch поможет сориентироваться в моделях системы, ее компонентах и типах лицензий.

Для размещения заказа обратитесь к своему представителю.

Обслуживание и техническая поддержка

Для системы Stealthwatch предлагается ряд программ обслуживания. Эти инновационные программы представляют собой уникальное сочетание людей, процессов, инструментов и партнеров, вместе обеспечивающих высочайший уровень удовлетворенности заказчиков. Предоставляемые услуги позволяют защитить вложения в сеть, оптимизировать эксплуатацию сети и подготовить сеть к внедрению новых приложений, расширяющих интеллектуальные возможности сети и повышающих эффективность вашего бизнеса. Для получения дополнительной информации о профессиональных услугах посетите домашнюю страницу Службы технической поддержки.

Cisco Capital

Программы финансирования Cisco Capital® помогут вам приобрести технологии, необходимые для достижения поставленных целей и обеспечения конкурентоспособности. Мы способны помочь вам снизить капитальные затраты. Ускорьте развитие своего бизнеса. Оптимизируйте свои инвестиции и их окупаемость. Программы финансирования Cisco Capital обеспечивают гибкие возможности при приобретении оборудования, программного обеспечения, сервисов и дополнительного оборудования сторонних производителей. И это всего лишь за один прогнозируемый платеж. Программы Cisco Capital доступны более чем в 100 странах. Подробнее.

Дополнительная информация

Для получения дополнительной информации о системе Cisco Stealthwatch посетите веб-сайт www.cisco.com/go/stealthwatch.

Для получения дополнительной информации напишите по адресу Stealthwatch-interest@cisco.com.

Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
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, www.cisco.com

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 этаж
Телефон: +994 (12) 437 4820, 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