# Краткий обзор Cisco Umbrella

Как приобрести

Концепции защиты корпоративных инфраструктур и создания сетей претерпевают серьезные изменения. Из-за широкомасштабного использования облачных приложений, увеличения числа удаленных сотрудников и разрастания сетей филиалов единая модель защиты в локальной среде становится невыгодной. Прямой доступ к Интернету — это удобно, экономично и эффективно, поэтому при развертывании сетей все чаще предпочтение отдается новому децентрализованному подходу. Однако вместе с изменениями приходят риски и новые проблемы безопасности. Организациям требуется более комплексный набор средств защиты, которые не только выполняют свое основное назначение, но и упрощают управление.

## Комплексная защита на уровне облака

Cisco Umbrella — это облачная платформа, благодаря которой ежедневно более 100 миллионов пользователей подключаются к Интернету по самым защищенным, надежным и быстрым каналам. В состав Umbrella входят межсетевой экран, защищенный веб-шлюз, система защиты на уровне DNS, брокер безопасного доступа к облаку (CASB) и решения для анализа угроз. С таким пакетом средств оградить свою сеть от различных угроз сможет организация любого размера. Сегодня многие компании выбирают прямой доступ к Интернету, и Umbrella позволяет им без труда расширить периметр защиты для охвата удаленных пользователей и филиалов.

## Усиление защиты благодаря более подробной аналитике

В систему Umbrella загружаются аналитические отчеты Cisco Talos, одной из крупнейших в мире коммерческих организаций по анализу угроз, где работают более 300 исследователей. Благодаря этим данным Umbrella во время атак выявляет и блокирует множество вредоносных доменов, IP и URL-адресов, а также файлов. Кроме того, мы анализируем огромные объемы информации об активности в сети Интернет, преобразуя их в статистические модели и алгоритмы машинного обучения, поэтому Umbrella позволяет обнаруживать и новые, только готовящиеся атаки.

## Простая блокировка вредоносного ПО

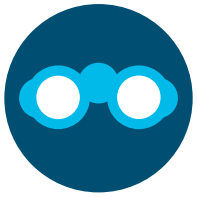
Интернет-протоколы являются одной из базовых составляющих Umbrella, и ежедневно решение обрабатывает 180 миллиардов интернет-запросов от более чем 18 500 организаций. Благодаря реализации защиты на уровне DNS и IP-адресов Umbrella блокирует запросы к вредоносному ПО, программам-вымогателям, фишинговым программам и ботнетам до еще установки подключения, предотвращая угрозы до того, как они достигнут сети или оконечных устройств. Защищенный и развернутый в облаке веб-шлюз регистрирует и анализирует весь веб-трафик, что гарантирует прозрачность, контроль над инцидентами и защиту. Облачный межсетевой экран позволяет записывать и блокировать трафик с использованием согласованных правил для IP-адресов, портов и протоколов в масштабе всей среды.

## Более быстрое и точное реагирование на инциденты

Umbrella классифицирует активность в сети Интернет и сохраняет все необходимые данные, чтобы упростить изучение инцидентов и ускорить реагирование на них. Благодаря использованию консоли Umbrella Investigate и API-интерфейса для запроса дополнительных сведений вы можете в любой момент просмотреть аналитику (историю и контекст), а затем определить важность инцидента и быстрее обработать его. Наше решение легко интегрируется с другими источниками аналитических данных и средствами оркестрации защиты, что повышает эффективность управления



## Проблемы безопасности



**Недостаточный мониторинг и охват**

**Количество и сложность инструментов защиты**

**Ограничения бюджета и ресурсов для обеспечения безопасности**

## Основные преимущества

- Надежная система безопасности, охватывающая все порты и протоколы
- Комплексная защита в сети и за ее пределами
- Быстрое развертывание и гибкие возможности применения
- Мгновенная окупаемость и низкая совокупная стоимость владения
- Единая панель мониторинга для эффективного управления

## Доступные пакеты

Мы предлагаем пакеты, которые могут удовлетворить потребности самых разных организаций. Небольшая компания без отдела по обеспечению безопасности или международное предприятие со сложной средой? Umbrella позволяет создать более эффективную систему защиты и обеспечить мониторинг доменов в Интернете при работе в сети и за ее пределами. Любой пакет можно интегрировать с программно-определяемой сетью WAN Cisco и добиться таких показателей производительности, безопасности и гибкости, которыми будут довольны и конечные пользователи, и ваши специалисты.

**Пакет Umbrella DNS Security Essentials** включает в себя базовые функции защиты на уровне DNS, позволяющие блокировать запросы к вредоносным доменам до того, как зараженный трафик попадет в сеть или на оконечные устройства. Стандартный пакет обеспечивает защиту за пределами сети и на мобильных устройствах, а также доступ к API-интерфейсам Umbrella (политики, отчеты и применение нужных параметров) и возможность экспорта журналов. Кроме того, в него входят консоль для нескольких организаций и средства интеграции с Cisco Threat Response. Доступна функция настройки политик на основе идентификационных данных (виртуальное устройство и коннектор Active Directory). Помимо перечисленного, этот вариант решения позволяет при помощи отчета для обнаружения приложений выявлять и блокировать теневые ИТ-ресурсы (на основании домена).

**В версию Umbrella DNS Security Advantage** входят все возможности DNS Security Essentials, а также инструменты, при помощи которых организации могут устанавливать соединение с потенциально опасными доменами через прокси-сервер для блокировки URL-адресов и проверки файлов в антивирусных системах и Cisco AMP. DNS Security Advantage также станет хорошим выбором для организаций, желающих получать больше контекстуальной информации при изучении инцидентов. С консолью Investigate и API-интерфейсом для запроса дополнительных сведений анализ угроз выполняется исключительно эффективно.

**Пакет Umbrella SIG Essentials** – это все возможности DNS Security Advantage, а помимо этого поддержка защищенного веб-шлюза (для пропуска всего трафика через прокси-сервер), облачного межсетевого экрана, анализа файлов в изолированной среде благодаря Cisco Threat Grid и брокера безопасного доступа к облаку (CASB). Единая облачная платформа позволяет объединить несколько служб защиты и анализа угроз, чтобы вам больше не пришлось беспокоиться о безопасности сети и удаленных пользователей. Упростите процесс управления и возьмите контроль над приложениями в масштабе всей децентрализованной среды в свои руки.

## Преимущества Umbrella

Umbrella представляет собой высокоустойчивую облачную инфраструктуру, бесперебойно работающую с момента запуска в 2006 году. Благодаря свободной маршрутизации любой из более чем 30 ЦОД Cisco с одинаковыми IP-адресами по всему миру доступен в любой момент. Таким образом, запросы сразу отправляются в ближайший ЦОД, а резервное переключение происходит автоматически. Umbrella – это более 900 ведущих интернет-провайдеров мира, сетей доставки содержимого (CDN) и платформ по предоставлению ПО как услуги (SaaS), которые мы объединили, чтобы молниеносно обрабатывать ваши запросы. Umbrella – это фантастическая скорость, надежная защита и самые довольные пользователи.

## Как приобрести

Чтобы ознакомиться с вариантами приобретения и пообщаться с одним из торговых представителей Cisco, посетите страницу www.cisco.com/c/ru_ru/buy.

## Выбор аналитиков и заказчиков

Узнайте, почему в 2019 году решение Umbrella было названо лучшим среди защищенных программных веб-шлюзов. Прочитайте обзоры и мнения заказчиков, собранные в рамках исследования TechValidate.

## Следующие шаги

Чтобы узнать, как Cisco Umbrella помогает защититься от угроз в Интернете, запросите демонстрацию или пообщайтесь с одним из наших торговых представителей.

Загрузите бесплатную пробную версию Umbrella на 14 дней с веб-сайта signup.umbrella.com.