Сравнение пакетов

	Professional для небольших компаний	Insights для средних компаний	Platform для специалистов по расширенным функциям безопасности
Производительность			
Полностью облачное решение – не нужно устанавливать оборудование и обслуживать ПО	✓	✓	✓
Стопроцентная отказоустойчивость – ежедневная обработка более 80 млрд запросов без увеличения задержки в сети			
Одновременное блокирование более 7 млн уникальных вредоносных узлов в 25 центрах обработки данных			
Защита			
Добавление нового уровня защиты на основе прогноза для любого устройства в любой точке	✓	✓	✓
Предотвращение проникновения вредоносного ПО, фишинга и обратных вызовов командных серверов через любой порт			
Применение политик допустимого использования по 60 категориям контента			
Применение политик безопасности			
Блокирование запросов к вредоносным доменам и IP-ответов на уровне DNS	✓	✓	✓
Блокирование вредоносных URL-адресов и прямых IP-подключений на уровне IP		✓	✓
Передача трафика из сомнительных доменов на прокси-сервер для анализа URL-адресов и файлов с помощью антивирусных систем и Cisco AMP		✓	✓
Мониторинг			
Получение информации в реальном времени о действиях в масштабе всего предприятия, с возможностью поиска и запланированными отчетами	✓	✓	✓
Обнаружение целенаправленных атак путем сравнения локальной и глобальной активности		✓	✓
Выявление рисков, связанных с использованием облака и устройств Интернета вещей, на основании отчетов о более чем 1800 сервисах		✓	✓
Управление			
Настраиваемые списки запрещенных и разрешенных ресурсов, встроенные страницы блокировки и варианты обхода	✓	✓	✓
Применение политик и функции мониторинга для каждой внутренней сети или для каждого пользователя/группы AD		✓	✓
Бессрочное хранение журналов благодаря интеграции с контейнером Amazon S3		✓	✓
Уникальные возможности пакета Platform			
Интеграция на основе API-интерфейса для применения политик и управления сторонними списками запрещенных ресурсов			✓
Investigate Console – аналитика угроз по всем доменам, IP-адресам и хеш-суммам файлов			✓
Дополнительные возможности			
Варианты поддержки – все пакеты включают поддержку через Интернет и по электронной почте	См. варианты для всех пакетов		
API-интерфейс Investigate – добавление глобального контекста к локальным событиям (управление событиями и данными безопасности)	Пакет приобретается отдельно		
Multi-Org Console – централизованное управление децентрализованными подразделениями		дополнительная возможность	дополнительная возможность

Варианты пакетов начального уровня

Для организаций, которым требуется система защиты с более простым функционалом, мы предлагаем три дополнительных пакета Umbrella, предназначенные для сценариев использования начального уровня.

	Roaming для межсетевого экрана нового поколения Cisco и AnyConnect	Branch для маршрутизаторов Cisco ISR серии 4000	WLAN для Cisco WLAN и других точек беспроводного доступа
Лицензирование	по числу пользователей	по числу маршрутизаторов Cisco ISR серии 4000	по числу точек доступа
Производительность			
Полностью облачное решение – не нужно устанавливать оборудование и обслуживать ПО	✓	✓	✓
Стопроцентная отказоустойчивость – ежедневная обработка более 80 млрд запросов без увеличения задержки в сети			
Одновременное блокирование более 7 млн уникальных вредоносных узлов в 25 центрах обработки данных			
Защита			
Добавление нового уровня защиты на основе прогноза для любого устройства в любой точке	Только для устройств, не подключенных к сети	Только для устройств, подключенных к сети	Только для устройств, подключенных к сети
Предотвращение проникновения вредоносного ПО, фишинга и обратных вызовов командных серверов через любой порт	✓	✓	✓
Применение политик допустимого использования по 60 категориям контента		✓	✓
Применение политик безопасности			
Блокирование запросов к вредоносным доменам и IP-ответов на уровне DNS	✓	✓	✓
Блокирование вредоносных URL-адресов и прямых IP-подключений на уровне IP			
Мониторинг			
Получение информации реального времени о действиях в масштабе всего предприятия, с возможностью поиска и запланированными отчетами	✓	✓	✓
Управление			
Настраиваемые списки запрещенных и разрешенных ресурсов, встроенные страницы блокировки и варианты обхода	Только список разрешенных ресурсов и одна встроенная страница блокировки	✓	✓
Применение политик и функции мониторинга для каждой внутренней сети или для каждого пользователя/группы AD		Только для каждой внутренней сети (без Active Directory)	Для каждого идентификатора SSID, точки доступа, группы точек доступа и группы пользователей (без Active Directory)
Дополнительные возможности			
Варианты поддержки – все пакеты включают поддержку через Интернет и по электронной почте	См. варианты для всех пакетов		
Investigate Console – доступ к аналитике угроз по всем доменам, IP-адресам и хеш-суммам файлов с помощью веб-консоли	Пакет приобретается отдельно		
API-интерфейс Investigate – добавление глобального контекста к локальным событиям (управление событиями и данными безопасности)	Пакет приобретается отдельно		