SentinelOne

ОБЗОР

SentinelOne ActiveEDR

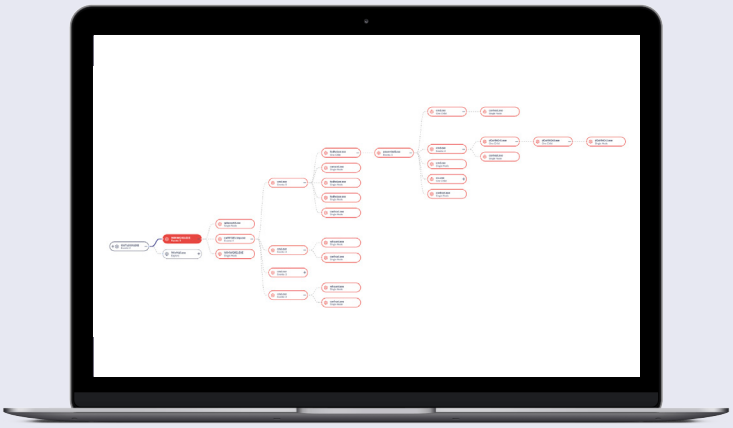
Эффективный мониторинг, автономное обнаружение угроз, автоматическое реагирование и проактивный хантинг — теперь это просто

Команды ИБ сталкиваются с множеством трудностей, пытаясь обнаруживать и расследовать продвинутые атаки, а также устранять их последствия. Неполная информация о наблюдаемых критичных контрольных точках, поиск данных по обширным и разрозненным источникам вручную без контекста и корреляции, усталость от большого количества бесполезных алертов и трудности быстрого купирования атак – все это мешает реализации критических бизнес-процессов, влияет на продуктивность специалистов и увеличивает расходы.

SentinelOne ActiveEDR™ – улучшенное EDR-решение для хантинга, которое позволяет осуществлять мониторинг в реальном времени благодаря скоррелированным инсайтам, обогащенным контекстом: они ускоряют приоритизацию угроз и анализ их первопричин. Это решение снижает нагрузку на сотрудников SOC благодаря автоматизированному устранению угроз, что позволяет серьезно сократить среднее время восстановления (MTTR) после инцидента. ActiveEDR предоставляет возможности проактивного хантинга, которые позволяют обнаруживать незаметные и изощренные угрозы, скрытые в пользовательской среде.

Ключевые возможности

Обнаружение быстро развивающихся угроз с помощью Storyline™



ОСНОВНЫЕ ДОСТОИНСТВА

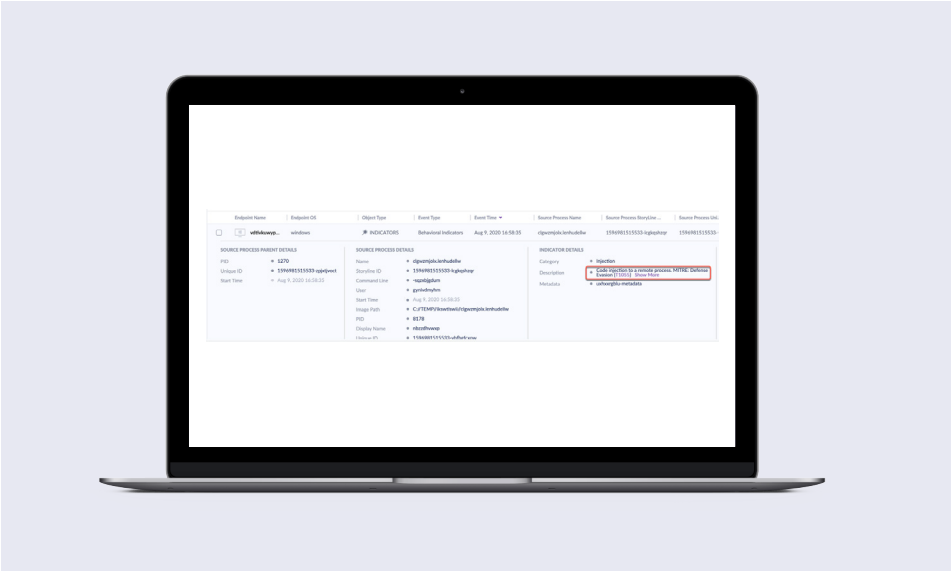
- Эффективное и практическое обнаружение угроз без нерелевантных алертов
- Быстрое обнаружение и сдерживание сложных атак, что позволяет сократить время нахождения злоумышленника в сети до его обнаружения и время разрешения инцидента
- Полное представление о первопричинах для устранения существующих пробелов безопасности
- Усиление и улучшение команды ИБ благодаря простому в использовании и интуитивно понятному решению
- Функция восстановления в один клик, автоматизация корреляции и других задач, выполняемых вручную, снижают нагрузку на сотрудников SOC
- Единая облачная платформа с поддержкой мультитенантности для удовлетворения потребностей глобальных организаций и MSSP-провайдеров
- Лучшая в отрасли защита для Linux, MacOS, Windows
- Доступное по цене хранение исторических данных EDR более 365 дней для их полного анализа

Storyline™ автоматически коррелирует отдельные события в единые цепочки развития атаки с детальным контекстом, предоставляя инсайты об атаке на уровне кампании.

SentinelOne ActiveEDR, оснащенный запатентованной технологией Storyline™, в реальном времени обеспечивает аналитиков контекстом и корреляцией, помогая понять сценарий событий, разворачивающихся в их среде. Storyline™ автоматически соединяет все связанные между собой события и действия в цепочку развития атаки и присваивает ей уникальный идентификатор. Благодаря этому команды ИБ могут за несколько секунд увидеть полный контекст инцидента, а не тратить часы, дни или недели на корреляцию логов и поиск связей между событиями вручную.

Поведенческий модуль SentinelOne отслеживает все действия в системе, включая изменения в файлах и реестре, запуск или остановку сервисов, межпроцессное взаимодействие и активность в сети. Он выявляет техники и тактики, которые являются индикаторами вредоносного поведения. Это позволяет отслеживать скрытое поведение и эффективно выявлять бесфайловые угрозы, латеральное движение, а также активное исполнение руткитов. SentinelOne автоматически коррелирует взаимосвязанные действия в единый алерт, отражающий всю кампанию злоумышленника. Благодаря этому можно сократить количество действий, выполняемых вручную, справиться с усталостью от алертов и значительно снизить квалификационные требования для реагирования на алерты.

Ускорьте расследования благодаря бесшовно интегрированным техникам MITRE ATT&CK



Коррелируйте детекты по MITRE в одну цепочку, сокращая время расследования, проводимого вручную, и уменьшая усталость от алертов у сотрудников SOC.

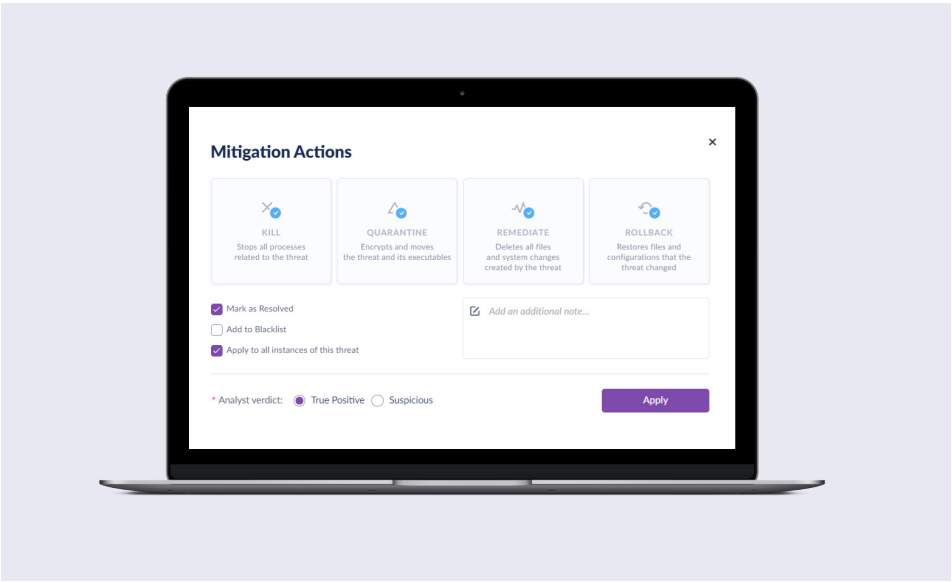
SentinelOne ActiveEDR сопоставляет атаки с базой MITRE ATT&CK в режиме реального времени, что дает аналитикам встроенные индикаторы и контекст о техниках атаки. SentinelOne коррелирует разрозненные детекты по MITRE в один Storyline, поэтому поиск тактик, техник и процедур (TTP) MITRE ATT&CK становится быстрым и удобным. Для начала расследования остаточно лишь указать ID искомой техники MITRE, что позволяет команде ИБ быстро понять суть сложных детектов.

Устраняйте все последствия атаки благодаря патентованным функциям восстановления и отката в 1 клик

SentinelOne позволяет аналитикам принять все необходимые меры для реагирования и устранения угрозы в один клик. Одним нажатием можно выполнить полный набор действий по восстановлению: изоляция от сети или блокировка вредоносного процесса и удаление механизмов персистентности. Функция отката автоматически восстанавливает файлы, удаленные или поврежденные программами-вымогателями до их незараженного состояния без необходимости перезаливки образов. Функция восстановления в один клик упрощает реагирование и значительно сокращает среднее время восстановления. SentinelOne также включает полноценные возможности Remote Shell на всех ОС. Благодаря им ваша команда ИБ сможет быстро расследовать атаки, собирать форензику и устранять пробелы безопасности

Устраняйте последствий всей цепочки событий атаки в один клик, быстрее восстанавливаясь после угрозы.

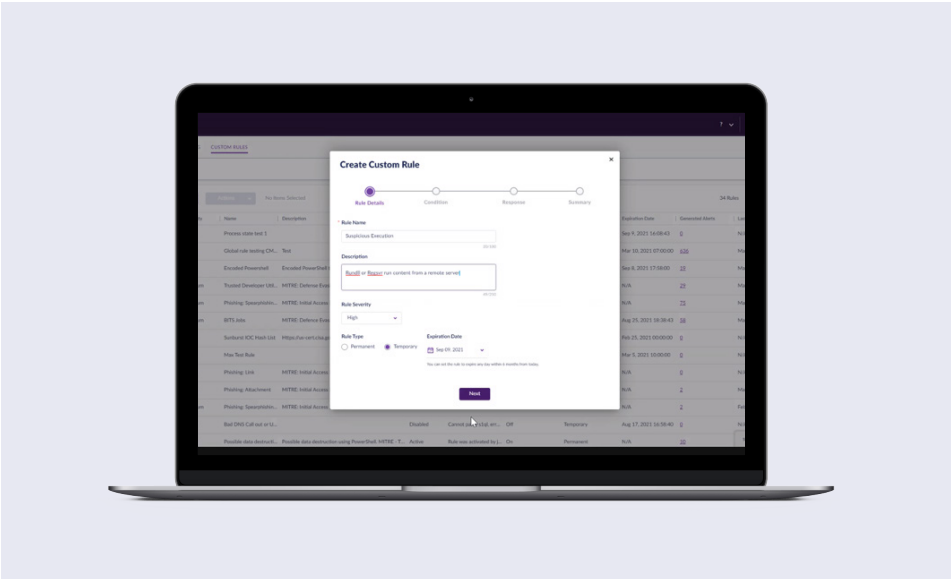
вне зависимости от местоположения конечных точек. Это устраняет неопределенность и значительно сокращает время нахождения злоумышленника в сети до его обнаружения.



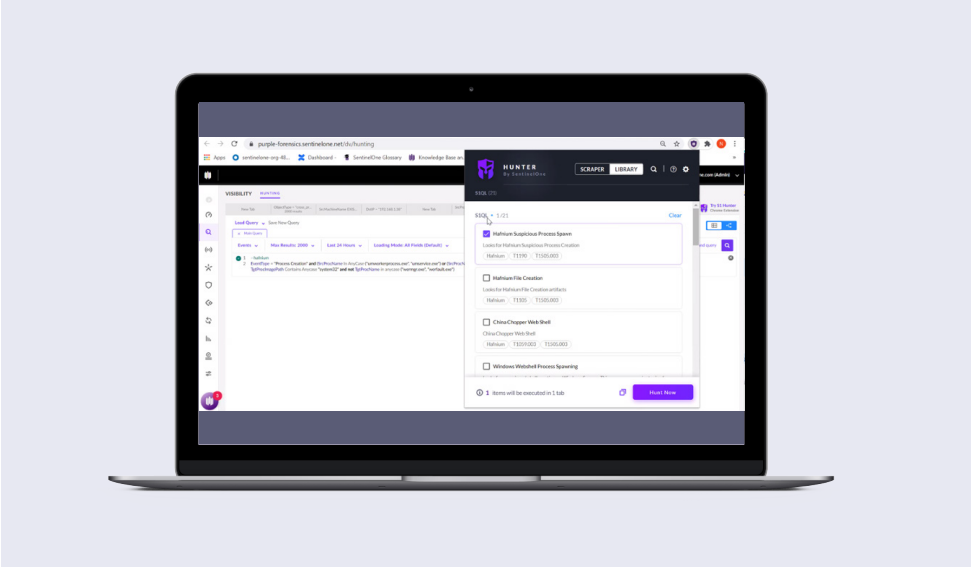
Настраивайте EDR под вашу среду с помощью STAR™

Чтобы обойти превентивную защиту, злоумышленники автоматизируют реализацию своих техник, тактик и процедур. В свою очередь, командам ИБ нужно тоже автоматизировать свои процессы, чтобы успевать за развитием современных атак. SentinelOne позволяет клиентам использовать аналитику Storyline и создавать собственные правила автоматического обнаружения для своей среды благодаря Storyline Active Response (STAR). С помощью STAR организации могут настраивать EDR-решение с учетом бизнес-контекста в соответствии со своими потребностями. Настраиваемые правила обнаружения STAR позволяют превратить запросы Deep Visibility в автоматизированные правила хантига, которые при обнаружении совпадений будут создавать алерты и выполнять заданные действия. STAR позволяет гибко настраивать алерты, характерные для среды клиента, что помогает оптимизировать процессы оповещения и расследования инцидентов.

Создавайте настраиваемые алерты под вашу среду с помощью правил автоматического хантинга.



Ведите проактивный хантинг для выявления нацеленных злоумышленников



Интуитивно понятный пользовательский интерфейс позволяет специалистам по хантингу с легкостью обнаруживать и останавливать скрытые атаки.

Модуль Deep Visibility ускоряет хантинг, позволяя проводить углубленные исследования и осуществлять хантинг в любом масштабе. Специалисты по хантингу могут быстро и легко формировать запросы и переключаться между полученными телеметрическими данными о конечной точке. SentinelOne автоматически коррелирует все взаимосвязанные процессы, файлы, потоки, события и многое другое. Например, один процесс внедряет вредоносный код в другой процесс, тем самым изменяя его. При выполнении запроса можно четко увидеть в детальном срезе все взаимодействия между исходным, целевым и родительским процессами. Это позволяет специалистам по хантингу быстро уловить связи между данными: первопричину угрозы и весь ее контекст, зависимости и действия, а также всю историю инцидента и полную цепь событий.

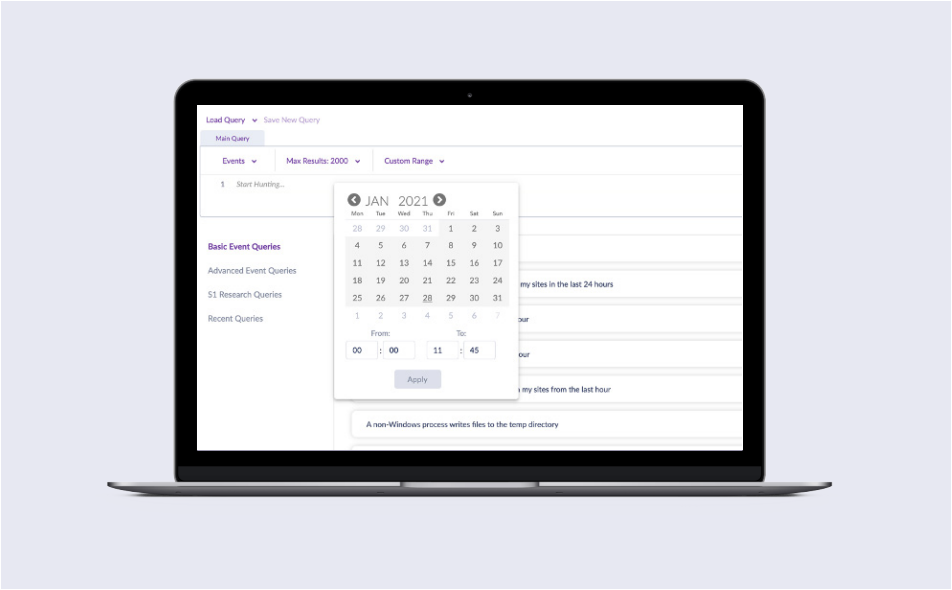
Вы можете создавать эффективные запросы для хантинга благодаря удобному синтаксису. Используйте библиотеку хантинговых запросов, подобранную исследователями SentinelOne, которые непрерывно проверяют новейшие методики выявления новых индикаторов угроз, а также техник, тактик и процедур злоумышленников. Эта аналитика рождается из гипотез, подтвержденных данными исследований, и применима для всех. Например, использование неуправляемой оболочки Powershell без цифровой подписи, скорее всего, является аномальным для большинства сред и обычно требует дополнительного расследования. Приведенный выше пример сам по себе не является вредоносным, но он вписывается в процесс хантинга, так как характеризует отклонение от нормы.

SentinelOne Hunter, расширение для браузера Chrome, помогает сотрудникам SOC и специалистам по хантингу повысить эффективность. Hunter позволяет быстро собрать данные из браузера и открыть запрос на консоли управления SentinelOne для поиска этих данных по всей организации. Hunter получает индикаторы компрометации прямо из открытой браузерной вкладки: IP-адреса, имена домена и хэши (MD5, SHA-1 и SHA-256). Когда необходимые индикаторы собраны, они перенаправляются на консоль управления SentinelOne. Расширение Hunter не собирает персональные или конфиденциальные данные пользователя браузера.

Исследуйте исторические данные благодаря их расширенному хранению по приемлемой цене

Возможность в любой момент заглянуть в прошлое позволяет аналитикам не только определить, сталкивалась ли организация с угрозой ранее, но и узнать всю информацию о развитии атаки, включая полное дерево процессов, временные рамки и связанные действия.

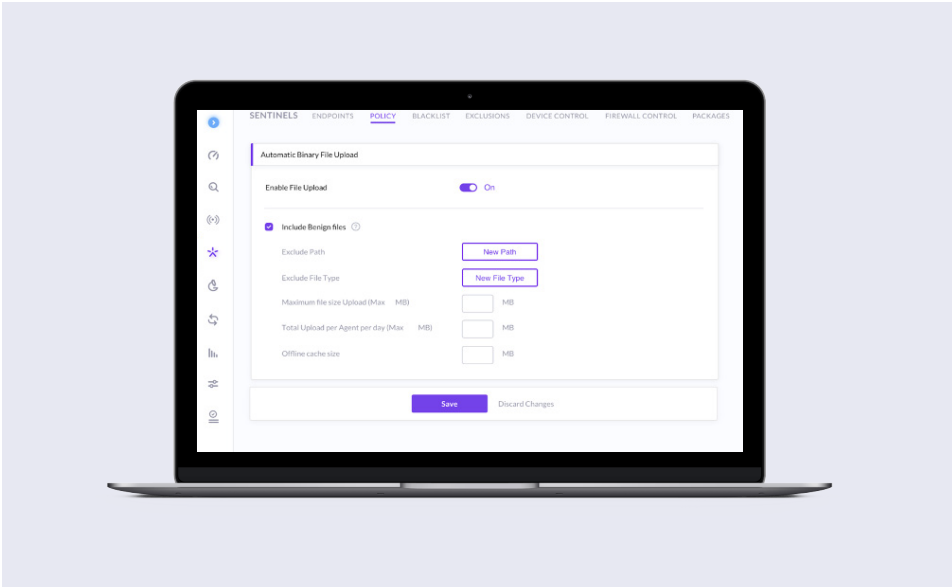
EDR данные хранятся в течение 365 и более дней для полного анализа истории любой атаки.



SentinelOne обеспечивает мониторинг среды благодаря хранению данных EDR в течение 365 и более дней. Это позволит команде ИБ анализировать инциденты и осуществлять ретроспективный анализ в рамках единого интерфейса.

Сохраняйте исполняемые файлы для автоматизированной аналитики с помощью Binary Vault

Аналитикам нужно быть в курсе новых уникальных исполняемых файлов в своей среде, чтобы их можно было тщательно изучить для проведения форензики. Хранилище бинарных файлов Binary Vault позволяет автоматически загружать безопасные или вредоносные исполняемые файлы в облако SentinelOne, где они хранятся в течение 30 дней. Для проведения форензики и дополнительных расследований эти образцы можно легко загрузить через консоль или по API. Выгружаются только уникальные исполняемые файлы. К примеру, любой стандартный набор бинарных файлов идентичен во всей организации. В случае обнаружения нового файла эта функция отправит его копию в хранилище, дав возможность провести реверс-инжиниринг и динамический анализ в SOC. Файлы можно извлечь разными способами: через консоль SentinelOne из подробной информации об инциденте или из модуля Deep Visibility, а также через API.



Передавайте телеметрию локально для автоматизации процессов SOAR с помощью Cloud Funnel

SentinelOne Cloud Funnel обеспечивает безопасную и почти мгновенную потоковую передачу телеметрических EDR-данных из SentinelOne Deep Visibility в ваше озера данных через подписку Kafka. SentinelOne Deep Visibility агрегирует в облако телеметрические данные, полученные от автономных агентов Сентинел на различных устройствах, на которых ИИ обнаруживает скрытые угрозы, коррелирует действия и предоставляет интерактивные инсайты. Подписка Kafka позволяет безопасно отправлять телеметрию в озеро данных. Подключение к Deep Visibility защищено протоколом TLS 1.2+, а доступ регулируется через SCRAM (Salted Challenge Response Authentication Mechanism), которые поддерживает Kafka. Когда появляются новые данные, Kafka отправляет их в ваше озеро данных. После этого команды ИБ могут совершать любые действия с полученными EDR-данными. Например, корреляция со сторонними источниками данных, интеграция с инструментами SIEM, а также оркестрация и обогащение процессов, связанных с инцидентами безопасности.

Gartner peerinsights

"SentinelOne вне конкуренции.

★★★★★

Старший директор, компания ИБ
Ритейл, оборот 1–3 млрд. долл.

Gartner peerinsights

"Простой и эффективный функционал EPP и EDR.

★★★★★

Аналитик по безопасности
Промышленность, оборот 3–10 млрд. долл.

Gartner peerinsights

"Одно из лучших EDR-решений, которое я когда-либо встречал!

★★★★★

Департамент управления рисками и безопасностью
Здравоохранение, оборот 3–10 млрд. долл.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

+ Обнаружение и устранение сложных угроз в реальном времени без вмешательства человека
+ Ускорение приоритезации угроз и анализа первопричин с инсайтами об инцидентах, лучшая на рынке интеграция с MITRE ATT&CK®, с предоставлением услуг MDR или без них
+ Интегрированная кибербарзведка для обнаружения угроз и обогащение данных о них из сторонних фидов ведущих вендоров, а также из собственных проприетарных источников SentinelOne
+ Запатентованные функции восстановления и отката «1-Click Remediation» и «1-Click Rollback»
+ Благодаря интуитивно понятному взаимодействию от сотрудников ИБ не требуется высокий уровень подготовки для того, чтобы начать хантинг за угрозами как дополнение к вашим процессам кибербезопасности
+ Срок хранения данных для любых потребностей от 14 до 365 и более дней. Хантинг на основе техник MITRE ATT&CK®
+ Бескомпромиссная защита для Windows, Linux и MacOS на любых ресурсах: на физических и виртуальных машинах, в облачных приложениях, контейнерах и центрах обработки данных
+ Быстрое и плавное развертывание благодаря функциям совместимости
+ RESTful API и встроенные интеграции с различными корпоративными приложениями и сервисами

SentinelOne — клиенты на первом месте

Непрерывная оценка работы и ее улучшение позволяют SentinelOne превзойти ожидания своих клиентов.

Gartner peerinsights customers' choice™

97%
Положительных отзывов о SentinelOne в отчете Gartner Peer Insights™ «Голос клиента»

97%
Индекс удовлетворенности клиентов (CSAT)

FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA

TEVORA
Аттестация PCI DSS
Аттестация HIPAA

Gartner peerinsights 4.9 ★★★★★

О компании SentinelOne

Больше возможностей. Меньше сложностей. SentinelOne в числе первых ведет кибербезопасность в будущее с автономным ИИ, аналитическое ядро которого находится не в облаке, а на конечной точке. Цель компании — упростить стек технологий безопасности, не снижая функциональные возможности организации. Наша технология разработана для того, чтобы дать людям больше возможностей для масштабирования благодаря автоматизации и удобному блокированию угроз. Вы готовы?

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733

S1-ACTIVE-EDR-03262021