SentinelOne

ОБЗОР

SentinelOne

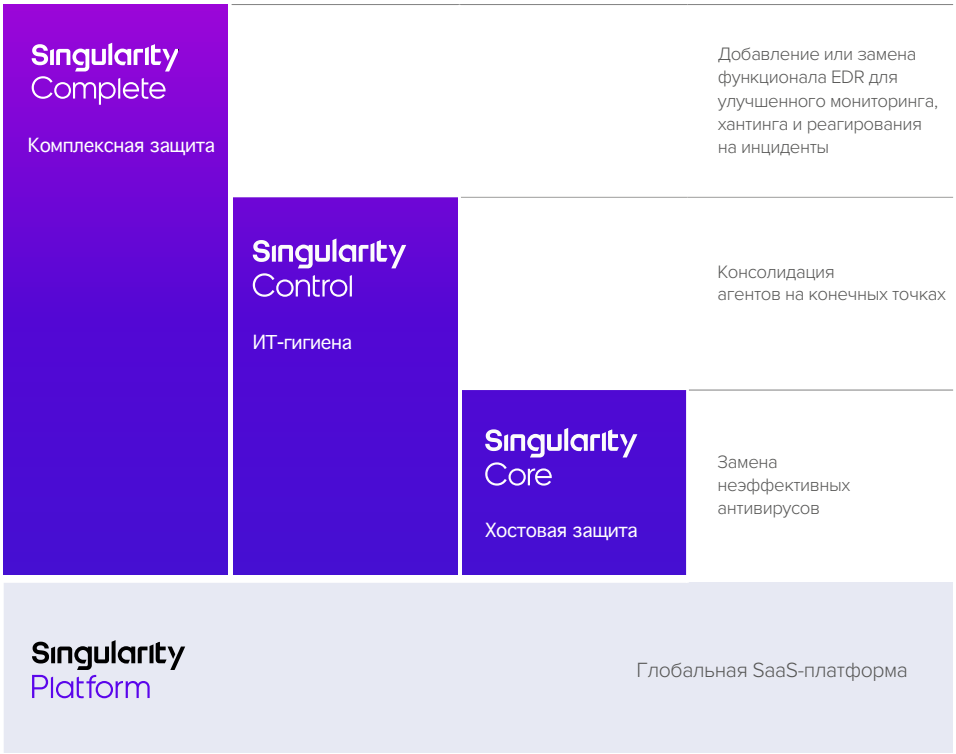
Антивирус и EDR нового поколения

Платформа защиты конечных точек SentinelOne Singularity расширяет возможности команд SOC и ИТ благодаря более эффективному подходу к защите информационных активов от современных сложных угроз.

Singularity предоставляет дифференцированную защиту конечных точек, обнаружение и реагирование на угрозы (EDR), безопасность Интернета вещей и облачных ресурсов, а также функционал для повседневных ИТ-операций, объединяя множество технологий в одно решение. SentinelOne предлагает автономные агенты "Sentinel" для Windows, Mac, Linux и Kubernetes и поддерживает различные форм-факторы: физические, виртуальные, VDI, корпоративные и гибридные ЦОДы, публичные облака.

Агенты Sentinel управляются мультитенантной серверной платформой с гибкой ролевой моделью доступа. Заказчикам также доступна подписка на управляемые услуги Vigilance Managed Detection & Response (MDR) для круглосуточной поддержки организаций в вопросах безопасности.

В этой спецификации описаны три пакета функционала, которые предлагает компания: SentinelOne Core, Control и Complete. Каждый пакет включает в себя весь функционал пакета предыдущего уровня.



ПОЧЕМУ СТОИТ ВЫБРАТЬ SENTINELONE?

- Превосходная защита конечных точек. SentinelOne объединяет возможности EPP и EDR, что позволяет избавиться от лишних агентов и снизить расходы
- Уровень удовлетворенности техподдержкой составляет 97%
- 96% клиентов рекомендуют SentinelOne
- Настраиваемая консоль с удобной автоматизаций частых действий
- Программы-вымогатели больше не являются проблемой благодаря высококлассному поведенческому ИИ
- Автономное реагирование на угрозы происходит мгновенно
- Экономия времени и снижение выгорания благодаря технологиям Storyline и ActiveEDR для хантинга и реагирования на инциденты
- Доступное по цене расширенное хранение данных EDR
- Простые XDR-интеграции с продуктами других вендоров

ГОТОВЫ К ДЕМО?

Закажите демонстрацию или расчет стоимости по ссылке www.sentinelone.com

Возможности платформы Singularity

У всех клиентов SentinelOne есть доступ к следующим возможностям консоли управления:

- Внедрение SaaS или на площадке заказчика (имеются особенности)
- Гибкая аутентификация и авторизация администраторов: SSO, двухфакторная аутентификация, ролевая модель доступа
- Управление настраивается в соответствии с вашей организационной структурой
- Хранение истории инцидентов в течение 365 дней
- Встроенная кибеpразведка SentinelOne и индикаторы угроз MITRE ATT&CK
- Настраиваемые дашборды и панели управления
- Гибкие уведомления по электронной почте и syslog
- XDR-интеграции на основе Singularity API (SIEM, песочницы, Slack, сторонние решения по кибеpразведке и т.д.)
- Единый API с более чем 340 функциями

Singularity Core

Core — это основа SentinelOne для защиты конечных точек, базовый продукт для организаций, которые хотят заменить устаревшие антивирусы, в том числе нового поколения (NGAV) на более эффективное и простое в управлении EPP-решение. Core также предлагает базовые функции EDR, демонстрируя настоящее слияние возможностей EPP и EDR. Функционал кибеpразведки — часть стандартного предложения, интегрированный через функции ИИ и компонент Sentinel Cloud. Возможности SentinelOne Core:

- **Встроенный анализ на основе статического и поведенческого ИИ** позволяет предотвратить и обнаружить широкий спектр атак в реальном времени до того, как организация пострадает от них. Core защищает от известных и неизвестных вредоносных программ, троянов, инструментов взлома, программ-вымогателей, эксплойтов, связанных с доступом к памяти, а также от вредоносного использования скриптов и вредоносных макросов и т. д.
- **Агенты Sentinel автономны,** а значит они применяют технологию предотвращения и обнаружения угроз вне зависимости от наличия подключения к облаку и будут запускать защитные ответные меры в реальном времени.
- **Быстрое восстановление,** которое позволяет вернуть пользователей к нормальной работе за минуты без перезаливки образов или написания скриптов. Любые несанкционированные изменения, которые происходят во время атаки, можно отменить одним щелчком с помощью функций восстановления «1-Click Remediation» и отката «1-Click Rollback» для Windows.
- **Безопасный доступ к консоли управления**. Выбор локации в Европе, США или Азиатско-Тихоокеанском регионе. Дашборды, управление политиками по сайту и группе, анализ инцидентов с интеграцией MITRE ATT&CK и др.

Singularity Control

Control предназначен для организаций, которым требуется лучшая в своем классе безопасность, которую можно найти в SentinelOne Core, с добавлением расширенных функций для управления конечными точками. Функции SentinelOne Control включают:

- **Весь функционал SentinelOne Core**
- **Хостовой межсетевой экран**: контроль за входящими и исходящими сетевыми подключениями с учетом местоположения
- **Управление устройствами,** включая USB и Bluetooth, в том числе с низким энергопотреблением (BLE)
- **Выявление «чужаков»** — устройств в сети, на которых нет агента SentinelOne, и применение к ним различных политик
- **Управление уязвимостями** наряду с инвентаризацией приложений позволяет получать понимание о сторонних приложениях с известными уязвимостями, которые сопоставлены с базой данных MITRE CVE.

SENTINELONE БЛОКИРУЕТ ПРОГРАММЫ-ВЫМОГАТЕЛИ И ДРУГИЕ БЕСФАЙЛОВЫЕ АТАКИ С ПОМОЩЬЮ ПОВЕДЕНЧЕСКОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МОЩНЫХ ФУНКЦИЙ АВТОМАТИЧЕСКОГО ВОССТАНОВЛЕНИЯ

Singularity Complete

Пакет Complete предназначен для организаций, которым нужна современная хостовая защита, а также расширенный функционал EDR, который мы называем ActiveEDR. В Complete входит запатентованная технология Storyline («сюжетная линия»), которая автоматически контекстуализирует все взаимосвязи процессов ОС, даже при перезагрузках, ежедневно и ежесекундно сохраняя их для будущих расследований. Storyline избавляет аналитиков от выполнения рутинных задач по корреляции событий и позволяет им быстро найти первопричину инцидента. SentinelOne Complete позволяет снизить нагрузку на администраторов ИБ, аналитиков SOC, специалистов по хантингу и реагированию на инциденты — это возможно благодаря автоматической корреляции телеметрических данных и их сопоставления с базой MITRE ATT&CK®. Редакцию SentinelOne Complete используют самые зрелые организации для удовлетворения своих самых жестких требований по ИБ. Возможности SentinelOne Complete:

- **Весь функционал SentinelOne Core и SentinelOne Control**
- **Запатентованная технология Storyline** для быстрого выявления первопричины инцидента и легкого перехода между событиями ИБ
- **Интегрированный мониторинг на основе ActiveEDR** как легитимных, так и вредоносных данных;
- **Хранение исторических данных EDR от 14 до 365 и более дней**, а также высокая скорость выполнения запросов в любом масштабе
- **Хантинг на основе техник MITRE ATT&CK®**
- **Возможность помечать легитимные сюжетные линии как угрозы** для применения функций защиты и восстановления с помощью EPP-функционала
- Автоматические функции мониторинга **Storyline Active Response (STAR)**
- История развития инцидента, функционал удаленной командной строки, скачивание файлов, интеграция с песочницами и др.

Gartner peerinsights™

> “
>
> Гибкие возможности управления в дополнение к мощному функционалу EPP и EDR.
>
> **Государственный сектор / Образование, 5 000–50 000 сотрудников**
> 13 марта 2020 года

> “
>
> Отличное противодействие программам-вымогателям. SentinelOne вне конкуренции.
>
> **Ритейлер, оборот 1–3 млрд. долл. США**
> 20 марта 2020 года

> “
>
> Настройка и развертывание прошли очень легко, а облачный дашборд прост в использовании.
>
> **Оборот 250–500 млн. долл. США**
> 2 июля 2020 года

Подписка на управляемые услуги Vigilance MDR

SentinelOne Vigilance MDR — это подписка на услуги, предназначенная для усиления системы корпоративной безопасности клиентов. Vigilance MDR повышает ценность продукта, гарантируя, что каждая угроза проверяется, устраняется, документируется и эскалируется по мере необходимости силами аналитиков из SentinelOne. В большинстве случаев они интерпретируют и устраняют угрозы примерно за 20 минут и связываются с клиентами только по срочным вопросам. Услуги Vigilance MDR позволяют клиентам сосредоточиться на действительно важных инцидентах, что делает их идеальным помощником для перегруженных команд ИТ или SOC.

Больше информации http://bit.ly/s1vigilance

Подписка на услуги сопровождения SentinelOne Readiness

SentinelOne Readiness — это консультационный сервис по подписке, предназначенный для сопровождения заказчика до, во время и после установки продукта по структурированной методике, которая позволяет быстро приступить к работе и поддерживает работоспособность продукта в течение долгого времени. Клиенты, воспользовавшиеся SentinelOne Readiness, получают рекомендации по развертыванию на основе лучших практик, периодическую помощь в обновлении агентов и ежеквартальные проверки состояния по методике ONEscore™, что гарантирует оптимальную работу платформы SentinelOne.

Больше информации http://bit.ly/s1readiness

Набор функций

	Singularity Complete	Singularity Control	Singularity Core
Безопасный доступ, высокая доступность, администрирование политик EPP, реагирование на инциденты и хантинг за угрозами на основе EDR, аналитика, управление Интернетом вещей (с опцией Ranger)	✓	✓	✓
Функционал EDR для SOC			
Глубокий мониторинг ActiveEDR	✓		
Функция Deep Visibility для пивотинга с помощью Storyline™	✓		
Хантинг с помощью модуля Deep Visibility на основе техник MITRE ATT&CK®	✓		
Автоматические функции наблюдения Storyline™ Active Response (STAR)	✓		
Скачивание файлов автоматически или вручную (для Windows, Mac и Linux)	✓		
Возможность отметить легитимные события как угрозы для применения защитных мер	✓		
Расширенное хранение исторических данных EDR от 14 до 365 дней	✓		
Функционал удаленной командной строки (Windows Powershell, Mac и Linux Bash)*	✓	✓	
ИТ-операции, ИБ-гигиена и пакет защитных функций			
Управление межсетевым экраном с учетом местоположения (для Win, Mac, Linux)	✓	✓	
Управление USB-устройствами (для Win, Mac)	✓	✓	
Управление технологией Bluetooth® или Bluetooth Low Energy® (для Win, Mac)	✓	✓	
Выявление устройств-«чужаков»	✓	✓	
Обнаружение уязвимостей в приложениях (для Win, Mac)	✓	✓	
Базовые функции защиты конечных точек			
Технология Storyline™ в автономных агентах Sentinel	✓	✓	✓
Предотвращение файловых атак с помощью статического ИИ и Sentinel Cloud	✓	✓	✓
Обнаружение бесфайловых атак поведенческим ИИ	✓	✓	✓
Автономное реагирование на угрозы — блокировка и изоляция (для Win, Mac, Linux)	✓	✓	✓
Автономное восстановление — в один клик, без написания скриптов (для Win, Mac)	✓	✓	✓
Автономный откат — в один клик, без написания скриптов (для Win)	✓	✓	✓
Изоляция устройства от сети	✓	✓	✓
Анализ инцидентов (таймлайн, анализ, MITRE ATT&CK®, комментарии аналитиков)	✓	✓	✓
Защита агента от взлома	✓	✓	✓
Инвентаризация приложений	✓	✓	✓

*функционал в редакции Singularity Control действует ограниченное время

Глобальная поддержка и услуги

Техподдержка по телефону, электронной почте или онлайн	**Включено**
Доступ к внутреннему ресурсному центру и порталу поддержки	**Включено**
Стандартная поддержка 5 дней в неделю по 9 часов	**Включено**
Круглосуточная поддержка организаций, модель Follow-the-Sun для угроз 1-й и 2-й степени критичности	Доступно
Выделенный специалист техподдержки и поддержка организации	Доступно
Подписка на управляемые услуги Vigilance MDR	Доступно
Подписка на SentinelOne Readiness для проверки состояния инсталляции	Доступно

ПОДДЕРЖКА ОС

SentinelOne поддерживает широкий спектр версий Windows, Mac и Linux, в том числе виртуальных. Единый список исключений по совместимости ПО представлен на портале поддержки.

Агент Sentinel для Windows
все рабочие станции Windows от версии 7 SP1 до Windows 10;
все сервера Windows от версии 2008 R2 с SP1 до Windows Server 2019 Core

Агент Sentinel для Mac
macOS Catalina, Mojave, High Sierra

Агент Sentinel для Linux
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Устаревшие версии Windows
XP, Server 2003 & 2008, POS2009

Поддержка контейнерных платформ
Самоуправляемый Kubernetes 1.13+, AWS Kubernetes (EKS), Azure AKS

Виртуализация и VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, Vmware Workstation, VMware Fusion, Vmware Horizon, Microsoft Hyper-V

AWS GovCloud · SE Labs AAA Enterprise Endpoint Protection · VB 100 VIRUS virusbtn.com · MITRE ATT&CK · TEVORA HIPAA Attestation · TEVORA PCI DSS Attestation · ISO 27001 CERTIFIED by schellman · Gartner peerinsights customers' choice 2020

SentinelOne — клиенты на первом месте

Постоянная оценка работы и улучшения позволяют SentinelOne превосходить ожидания своих клиентов.

96%

96% положительных отзывов о SentinelOne в отчете Gartner Peer Insights «Голос клиента»

97%

Индекс удовлетворенности клиента (CSAT) ~97%

Индекс лояльности NPS: промежуток от «отлично» до «превосходно»

О компании SentinelOne

SentinelOne — компания-разработчик ПО для обеспечения информационной безопасности, основанная в 2013 году в Израиле. SentinelOne Singularity — единая платформа для предотвращения, обнаружения и реагирования на угрозы, а также для хантинга по всем корпоративным активам. Talgar Systems является дистрибьютором SentinelOne в странах СНГ.

www.talgarsystems.com
hello@talgarsystems.com

S1-PROD-CCC-260820-1