SentinelOne

ОБЗОР

Агент Sentinel для Linux

Компонент решения SentinelOne Cloud Workload Security

Предотвращение атак и EDR для серверов на Linux без ущерба стабильности

Службам ИБ необходимо решение, которое обеспечивает предотвращение и выявление угроз, реагирование на инциденты и хантинг по всем ОС. Linux не исключение. В отличие от устаревших антивирусов и EDR-систем первого поколения, SentinelOne предлагает расширенный набор функций, необходимых SOC для защиты активов на Linux во всех средах с высокой производительностью и автоматизацией.

Агенты Sentinel предназначены для использования на физических и виртуальных машинах в ЦОДе, средах AWS, Azure и Google Cloud Platform. Управление агентами Sentinel для Linux происходит из той же консоли, что и агентами для Windows, macOS и Kubernetes.

SentinelOne дает гибкое управление, основанное на политиках, отражающих организационную структуру компании. Агент совместим и поддерживается на многих популярных дистрибутивах и не использует модули уровня ядра, что исключает риск нестабильной работы.

ОТЛИЧИЯ АГЕНТА SENTINEL ДЛЯ LINUX

- Широкий спектр поддерживаемых дистрибутивов
- Стабильная работа без модулей ядра
- Блокирование атак в реальном времени, включая бесфайловые
- Полный EDR-мониторинг + хранение данных
- Расширенные возможности реагирования

ЕСТЬ РАБОЧИЕ НАГРУЗКИ В НАТИВНЫХ ОБЛАЧНЫХ КОНТЕЙНЕРАХ?

Агент Sentinel для Kubernetes сочетает возможности защиты среды выполнения, функционал EDR и уникальные специализированные решения для контейнеров.

ВОЗМОЖНОСТИ SENTINEL ДЛЯ LINUX

Эксплуатация

+ Поддержка всех популярных дистрибутивов Linux
+ Стабильная работа без модулей уровня ядра
+ Простая установка в физических, виртуальных и облачных средах
+ Единая мультитенантная консоль для управления агентами с ролевым доступом
+ Инвентаризация приложений

Предотвращение угроз

+ Локальные вердикты означают отсутствие задержки из-за обращений к облаку
+ Локальный статический ИИ — оперативная блокировка и карантин бинарных файлов с вредоносным кодом (ELF, Windows, Mach-O)
+ Локальный поведенческий ИИ — оперативная блокировка ранее неизвестных бесфайловых угроз
+ Сканирование дисков по требованию
+ Контроль приложений для контейнеризованных сред
+ Контроль безопасности приложений для облачных ВМ (Скоро)

ActiveEDR™ уровня Enterprise

+ Storyline™ для автоматического создания контекста событий и их взаимосвязей из дерева процессов
+ Автоматизированное реагирование через Storyline™ Active Response
+ Хранение данных EDR от 14 до 365 и более дней
+ Интеграция с техниками MITRE ATT&CK

Реагирование на инциденты

+ Безопасный доступ через удаленную командную строку
+ Управление межсетевым экраном
+ Сетевая изоляция
+ Скачивание файлов

Технология Storyline показывает преимущества SentinelOne

SentinelOne предложила инновационную технологию Storyline, которая позволяет оперативнее обнаруживать угрозы после их появления в инфраструктуре, а также существенно упростить действия по поиску и хантингу в рамках EDR. Storyline в реальном времени проводит автоматическую корреляцию всех программных операций, выполняемых на конечной точке, и непрерывно создает интерактивный контекст для всех связанных элементов в каждом дереве процессов, группируя их в цепочки. Реагирование агента на угрозы происходит в реальном времени и может осуществляться как автоматизированно, при помощи Storyline Active Response (STAR™) и XDR, так и аналитиками вручную.

В режиме защиты конечных точек (EPP) статический и поведенческий механизмы ИИ непрерывно проверяют тысячи параллельных цепочек событий, выявляя файлы и процессы, не соответствующие нормальной модели поведения, и запускают функции реагирования. В режиме обнаружения и реагирования (EDR) агенты Sentinel проводят сложнейшую работу по корреляции событий, что в дальнейшем облегчает работу аналитикам и экономит их время. Все цепочки событий и взаимосвязи процессов, которые формирует Storyline после анализа вредоносных и легитимных данных, длительное время (от 14 до 365 и более дней) хранятся на платформе Singularity, где они в любое время доступны для аналитиков. **Не нужно заново выстраивать дерево процессов. Мы сделаем это за вас.**

Linux-агент ничем не уступает по функционалу агентам других ОС. Sentinel для Linux предлагает нужный для SOC функционал, который повзоляет предотвращать и выявлять угрозы, реагировать на инциденты и вести мониторинг.

LINUX-АГЕНТ ПОДДЕРЖИВАЕТ РАБОЧИЕ СТОЛЫ И СЕРВЕРЫ НА МНОГИХ ДИСТРИБУТИВАХ И УПРАВЛЯЕТСЯ ИЗ ANSIBLE, PUPPET И РАСШИРЕНИЙ AZURE ДЛЯ ВМ:

- **Ubuntu** 14.04, 16.04, 18.04, 19.04, 19.10, 20.04
- **RHEL** 6.4+, 7.1-7.9, 8.0-8.4
- **CentOS** 6.4+, 7.1-7.8, 8.0-8.4
- **Oracle** 6.9, 6.10, 7.7, 8.0-8.4
- **Amazon AMI 2**, 2017.03, 2018.03
- **SUSE Linux Enterprise Server** 12.x, 15.x
- **Fedora** 25-30, 31 ядро 5.5.x+, 32-33
- **Debian** 8, 9, 10
- **Virtuozzo** 7
- **Scientific Linux** 6, 7

Среды выполнения, поддерживаемые Sentinel для Linux

ФИЗИЧЕСКИЕ И ВИРТУАЛЬНЫЕ

AWS EC2

MICROSOFT AZURE

GOOGLE CLOUD PLATFORM

2021 MITRE ATT&CK

- Ноль пропусков
- Наилучшая корреляция
- Без изменений конфигурации и задержки детектов

2020 FORRESTER WAVE™ EDR

«Сильный претендент»

2020 KUPPINGERCOLE MARKET COMPASS

Выдающийся EPDR-инноватор

SentinelOne — клиенты на первом месте

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

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

97% Удовлетворенность клиентов (индекс CSAT)

Attestation PCI DSS
Attestation HIPAA

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-GSS-LINUX-12042020