SentinelOne™

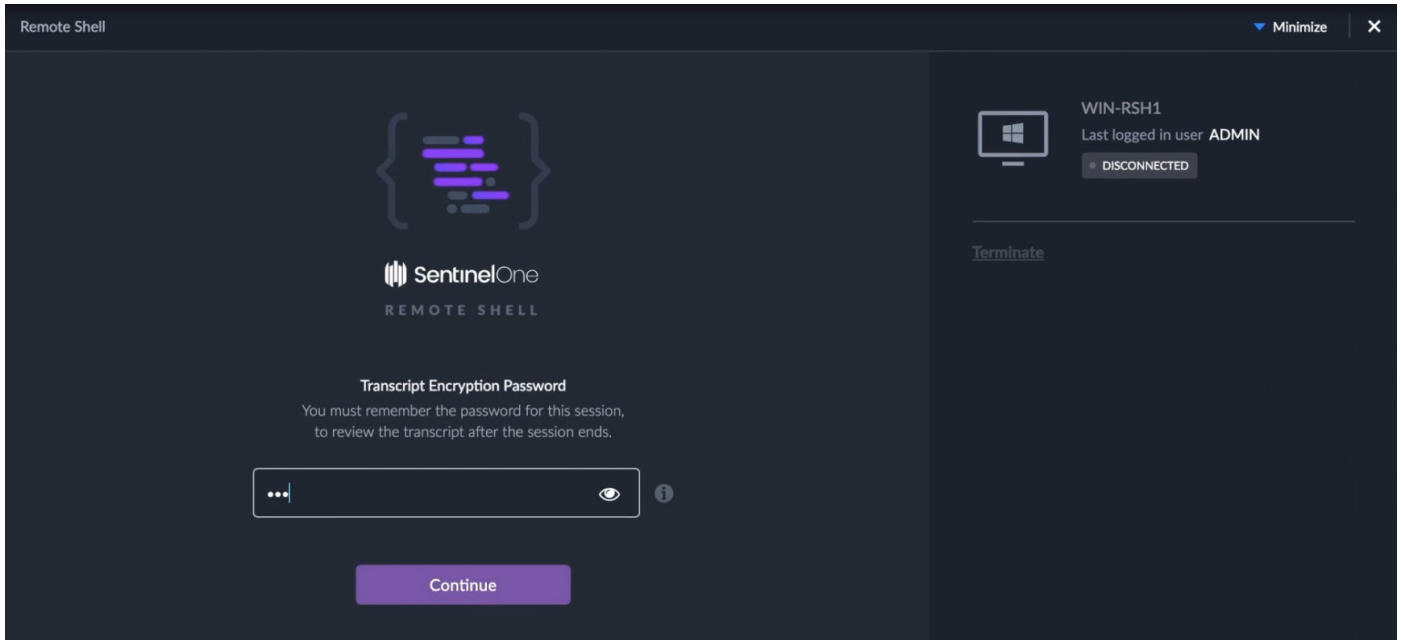
# Full Remote Shell

## ЭКОНОМЬТЕ СВОЕ ВРЕМЯ БЛАГОДАРЯ РЕШЕНИЯМ SENTINELONE ДЛЯ АВТОНОМНОЙ ЗАЩИТЫ КОНЕЧНЫХ ТОЧЕК

SentinelOne позволяет сделать защиту конечных точек автономной, используя единый агент, который выявляет и предотвращает атаки по всем основным векторам, а также принимает необходимые меры в отношении этих атак. Платформой SentinelOne предельно легко пользоваться и она экономит время благодаря тому, что использует ИИ для борьбы с угрозами в реальном времени как в локальных, так и в облачных средах. Это единственное решение, которое обеспечивает полную видимость ваших сетей прямо из конечной точки.

Благодаря Full Remote Shell службы ИБ могут быстрее расследовать атаки, собирать данные форензики и восстанавливать систему после взлома независимо от того, где находятся скомпрометированные конечные точки. Такие возможности исключают неопределенность и значительно сокращают время простоя после атаки.

SentinelOne предоставляет командам ИБ и ИТ беспрецедентные технологии для выявления и оценки атак на конечные точки, а также для последующего восстановления конечных точек по всей организации вне зависимости от местоположения. Full Remote Shell позволяет авторизованным администраторам получать доступ к конечным точкам прямо из консоли SentinelOne. Оттуда они могут установить удаленный сеанс и расследовать атаки, ознакомиться с их контекстом, а также восстанавливать системы, решая проблемы конечных пользователей — и все это происходит в режиме реального времени.



## Зачем нужна Remote Shell?

Ландшафт конечных точек постоянно меняется. Для оптимизации своих рабочих процессов пользователи устанавливают широкий спектр ПО, но из-за этого становится сложно идти в ногу с лучшими практиками по кибербезопасности и управлению рисками. В таких непростых условиях администраторы наверняка найдут множество способов применения Full Remote Shell. Например, администраторы смогут:

1. Устранять неполадки быстрее, поскольку им не обязательно находиться рядом с конечным устройством для решения проблем
2. Предоставить более качественную поддержку удаленным пользователям, ведь теперь им не нужно специально приходить в офис или ИТ-отдел
3. Легко менять локальную конфигурацию, не покидая свою локацию
4. Безопасно инициировать сессию удаленного управления
5. Углубиться в форензику с помощью дампа памяти и других инструментов
6. Завершить работу нежелательного приложения или процесса, запущенного на конечной точке
7. Отправить локальный запрос на любое устройство в сети

## В чем преимущества SentinelOne Full Remote Shell?

Перед началом работы над Full Remote Shell разработчики SentinelOne опросили системных администраторов по поводу их опыта работы с аналогичными инструментами в других продуктах. Главной проблемой являлось ограниченное количество команд, которые эти продукты могли выполнять. Если пользователям требовалась другая команда, то им приходилось отправлять своему вендору запрос на добавление функции или пройти через другие длительные процедуры. Чтобы избежать всего этого, SentinelOne использует возможности нативной оболочки. Другими словами, все, что вы можете делать в PowerShell и Bash, вы можете делать и в Full Remote Shell. Продукт даже поддерживает функцию автозаполнения, что упрощает работу системного администратора.

## БЕЗОПАСНА ЛИ FULL REMOTE SHELL?

Конечно, использование удаленной оболочки для доступа ко всем устройствам не всегда характерно для СЗИ, однако SentinelOne следует требованиям заказчиков. Вот как SentinelOne удалось совместить практичность с безопасностью:

1. Доступ к Full Remote Shell должен быть специально разрешен для хоста политикой управления
2. Для шифрования каждого сеанса администратор должен выбрать уникальный пароль
3. Прежде чем получить доступ, администратор должен включить двухфакторную аутентификацию.
4. Полный аудит: по каждому сеансу ведется журнал событий, включая всю историю сеанса в целом и каждый случай получения доступа к ресурсу или его использования.

## Миссия SentinelOne

Миссия SentinelOne — дать организациям возможность наиболее эффективно и результативно управлять рисками. Компания понимает, что службам ИБ нужно успевать больше, но с меньшими ресурсами, и при этом быть готовыми к любым изменениям ландшафта угроз. Именно это и определяет основные принципы разработки решений SentinelOne. Трансформация подхода к защите конечных точек — это только начало.

**ХОТИТЕ ДЕМО?** Закажите демонстрацию или расчет стоимости по ссылке http://bit.ly/get-s1-demo

SentinelOne™
www.sentinelone.com | sales@sentinelone.com
+1-855-868-3733 | 605 Fairchild Dr, Mountain View, CA 94043