SentinelOne

ОБЗОР РЕШЕНИЯ

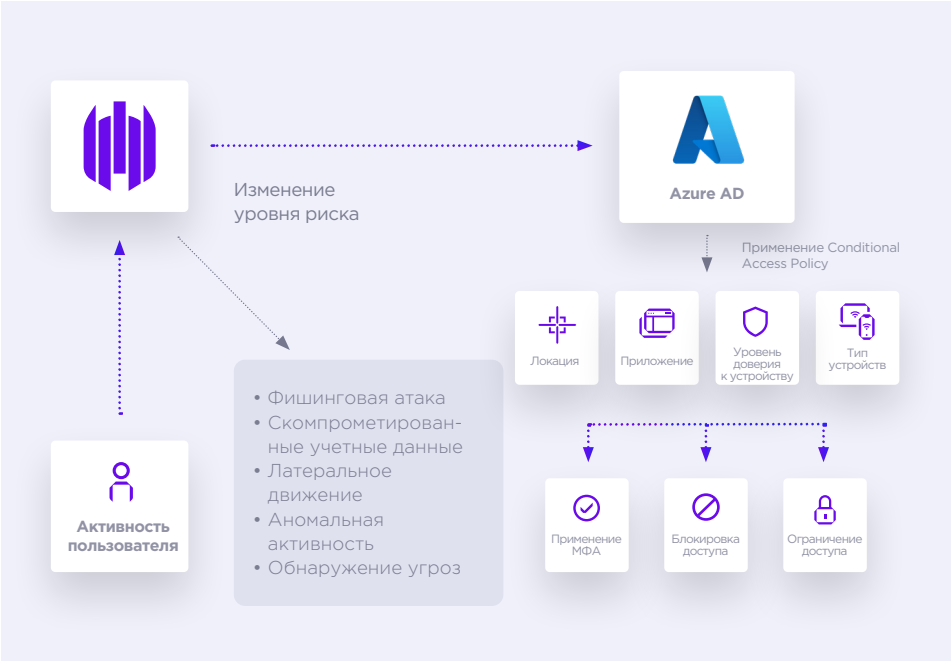
Приложение Singularity для Azure Active Directory

В связи с недавними кибератаками, например на Colonial Pipeline или Kaseya, а также переходом к удаленному формату работы многие организации поняли, что нужно модернизировать свои модели обеспечения безопасности. Подходы, основанные на защите периметра, устарели. Сейчас организации переходят к модели Zero Trust, при которой ни одна пользовательская учетная запись и конечная точка не является доверенной по умолчанию. Их состояние нужно непрерывно проверять, и только по результатам такой оценки предоставлять доступ к корпоративным ресурсам и сервисам.

Для этого организациям необходима платформа расширенного обнаружения и реагирования (XDR), которая может собирать данные в большом масштабе, анализировать их с помощью ИИ, централизовать процесс реагирования на инциденты и обеспечить его автономность, объединив решения по защите конечных точек и управлению учетными записями.

Приложение Singularity для Azure Active Directory

Клиенты SentinelOne и Microsoft могут воспользоваться первой в своем роде интеграцией XDR-платформы SentinelOne Singularity и службы управления учетными записями Azure Active Directory. Таким образом достигается автономное реагирование на угрозы, что помогает специалистам ИБ оперативнее выполнять свою работу.



КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Требование МФА для пользователей на скомпрометированном хосте

У пользователей зараженного хоста можно запрашивать дополнительный фактор аутентификации.

Блокирование доступа для скомпрометированных пользователей

В реальном времени блокировать доступ к корпоративным ресурсам и сервисам пользователям, находящимся на зараженном хосте.

Ограничение доступа для скомпрометированных пользователей

Ограничивать доступ к корпоративным данным, если пользователь находится на зараженном хосте.

Простая интеграция Singularity и Azure Active Directory

Не требуется сложной настройки API или обслуживания вручную.

Используя приложение SentinelOne для Azure Active Directory, организации объединяют защиту конечных точек и управление учетными записями. В результате при компрометации хоста информация о пораженном пользователе передается в Azure Active Directory в реальном времени, и политика доступа с учетом риска (Conditional Access Policy) оперативно активирует для его учетной записи многофакторную аутентификацию (МФА), запрещает или ограничивает ей доступ.

> “
>
> Открытые экосистемы играют критическую роль в реализации стратегии Zero Trust, поскольку организациям нужны лучшие в своем классе решения. Объединение ведущих платформ для защиты конечных точек и управления учетными записями поможет клиентам разработать и развить свои программы Zero Trust.
>
> **Радж Раджамани**
>
> Директор по развитию продуктов SentinelOne

ХОТИТЕ ДЕМО?

Посетите сайт Тайгер Оптикс и закажите демо.

Инновации. Надежность. Признание.

Gartner

Лидер в волшебном квадранте Gartner по оценке EPP-платформ за 2021 год
Наивысшие оценки во всех сценариях использования в отчете о критических возможностях EPP-платформ

MITRE ENGENUITY

Рекордные результаты в испытании ATT&CK

- Ни одной пропущенной угрозы — детект 100%
- Больше всего аналитических детектов 2 года подряд
- Без задержек и изменений конфигурации

Gartner peerinsights 4.9 ★★★★★

98% положительных отзывов™

в отчете Gartner Peer Insights™ «Голос клиента»

FedRAMP · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · TEVORA PCI DSS Attestation HIPAA Attestation

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?

Тайгер Оптикс — авторизованный дистрибьютор SentinelOne в России и СНГ

sales@tiger-optics.ru
https://www.tiger-optics.ru/