illusive

# Attack Surface Manager

## Упреждающая защита от нацеленных атак

Скрытные злоумышленники перемещаются по вашей сети, используя существующие учетные данные и подключения, созданные пользователями. Корпоративная связность необходима для ведения бизнеса, но в каждой сети существует ее избыток. Учетные данные кэшируются, права доступа повышаются, пользователи подключаются к различным системам. Чем шире такая "поверхность доступа", тем больше перед злоумышленниками открывается путей к ценным активам, и тем быстрее вы можете стать жертвой атаки.

### Знаете ли вы, как хакеры перемещаются по вашей сети, если им удалось проникнуть внутрь?

Поверхность доступа изменяется непрерывно, по мере того как пользователи входят и выходят из систем, перезапускают хосты, меняют роли и получают новые доступы. Иногда сотрудники умышленно получают доступ, который им не полагается, но большинство подключений возникает в результате вполне обычных, легитимных действий. Например:

- Имена пользователей и пароли непреднамеренно сохраняются в истории браузеров;
- Учетные данные администратора домена могут оставаться в памяти системы после сеанса удаленной поддержки;
- Данные для доступа хранятся в приложениях для обновления ПО и технического обслуживания;
- Права пользователей случайно расширяются из-за сложной структуры корпоративной службы каталогов.

До сих пор все это мог обнаружить только опытный аналитик во время тщательной проверки каждой отдельной системы.

### Непрерывное уменьшение поверхности атаки — без усилий и в корпоративном масштабе

Модуль ASM автоматически обнаруживает и устраняет все нарушения, связанные с учетными данными, позволяя изучать пути к критически важным активам и предоставляя глубокую аналитику рисков для принятия взвешенных решений, ограничивающих мобильность злоумышленников.

*Модуль Attack Surface Manager (ASM) выявляет скрытые учетные данные и пути к критическим системам, так что вы всегда можете остановить злоумышленников, при этом не останавливая свой бизнес.*


**Меняйте правила игры для раннего выявления атак**

*Сокращение количества настоящих артефактов и наполнение конечных точек фиктивными данными повышает вероятность того, что злоумышленники выберут приманку и будут моментально обнаружены.*

illusive

## Функции модуля ASM:

**Траектории движения:** автоматическое обнаружение путей атаки от произвольных машин до особо ценных систем с подробными сведениями о хостах, задействованных на каждом пути, а также возможностью выбирать и блокировать избыточные подключения одним щелчком мыши исходя из оценки рисков и сетевой связности.

**Правила поверхности атаки:** простой интерфейс создания и применения политик учетных данных и подключений для различных ролей и групп пользователей, включая учетные записи локальных администраторов, учетные записи с повышенными привилегиями и допустимые подключения к критическим активам.

**Модуль Attacker View:** экран консоли управления Illusive отображающий рискованные скопления учетных даннных относительно критически важных активов компании.

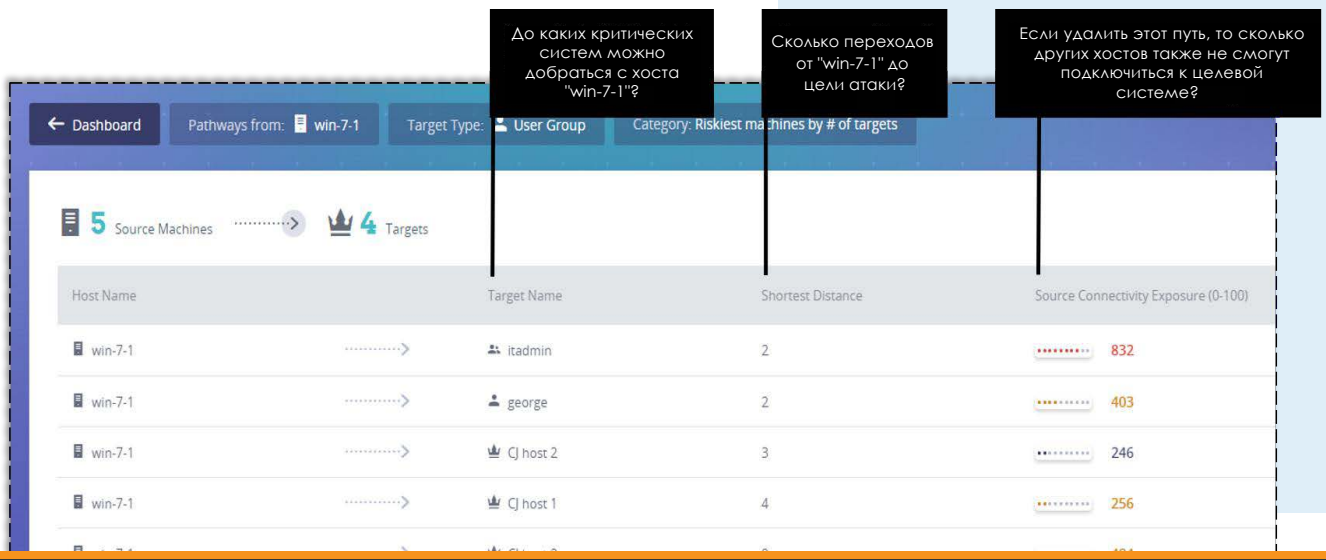
**Механизм снижения поверхности атаки:** исправление одного или нескольких нарушений с выбранной степенью автоматизации.

**Дашборд ASM:** обзор метрик поверхности атаки и локаций с наиболее высоким уровнем риска для проведения детальных расследований.

**Сервисы упреждения FirstMove:** используя модуль Attack Surface Manager (ASM), Illusive анализирует поверхность атаки организации, усиливает и укрепляет среду, а также настраивает модуль ASM для выявления и маркировки нарушений политики ИБ, что позволяет непрерывно повышать уровень кибергигиены организации.

## Ограничение мобильности злоумышленников без помех для бизнеса

- **Узнайте, как злоумышленники могут добраться до ваших критических активов**, выявив скрытые возможности латерального движения по вашей сети.
- **Уменьшайте поверхность атаки непрерывно и без ручной работы**, выявляя нарушения политик кэширования учетных записей и удаляя соединения с высоким уровнем риска.
- **Обнаруживайте атаки быстрее**, повышая вероятность того, что злоумышленники активируют приманки.
- **Усиливайте киберустойчивость.** Невозможно запретить пользователям устанавливать подключения, но можно снизить риски, непрерывно уменьшая возможность латерального движения злоумышленников по вашей сети.




**Illusive Networks** помогает специалистам по кибербезопасности сокращать бизнес-риски, порождаемые современными высокотехнологичными целевыми угрозами за счет предотвращения латерального передвижения злоумышленников к критически важным активам. Illusive Networks уменьшает поверхность атаки для упреждения угроз, обнаруживает несанкционированное латеральное движение на начальных стадиях атаки и предоставляет подробную форензику в режиме реального времени для более эффективного реагирования на инциденты и принятия взвешенных решений.

Безагентная технология Illusive позволяет организациям активно предотвращать атаки, избегать сбоев в работе и потерь бизнеса, а также с большей уверенностью работать в сегодняшнем сложном, сверхсвязанном мире.



**Тайгер Оптикс – дистрибьютор в России и СНГ**

Дистрибьютором Illusive Networks в России и странах СНГ является компания Тайгер Оптикс.

Телефон +7 499 504 1670
Email sales@tiger-optics.ru
Блог blog.tiger-optics.ru

ТАЙГЕР ОПТИКС