SentinelOne

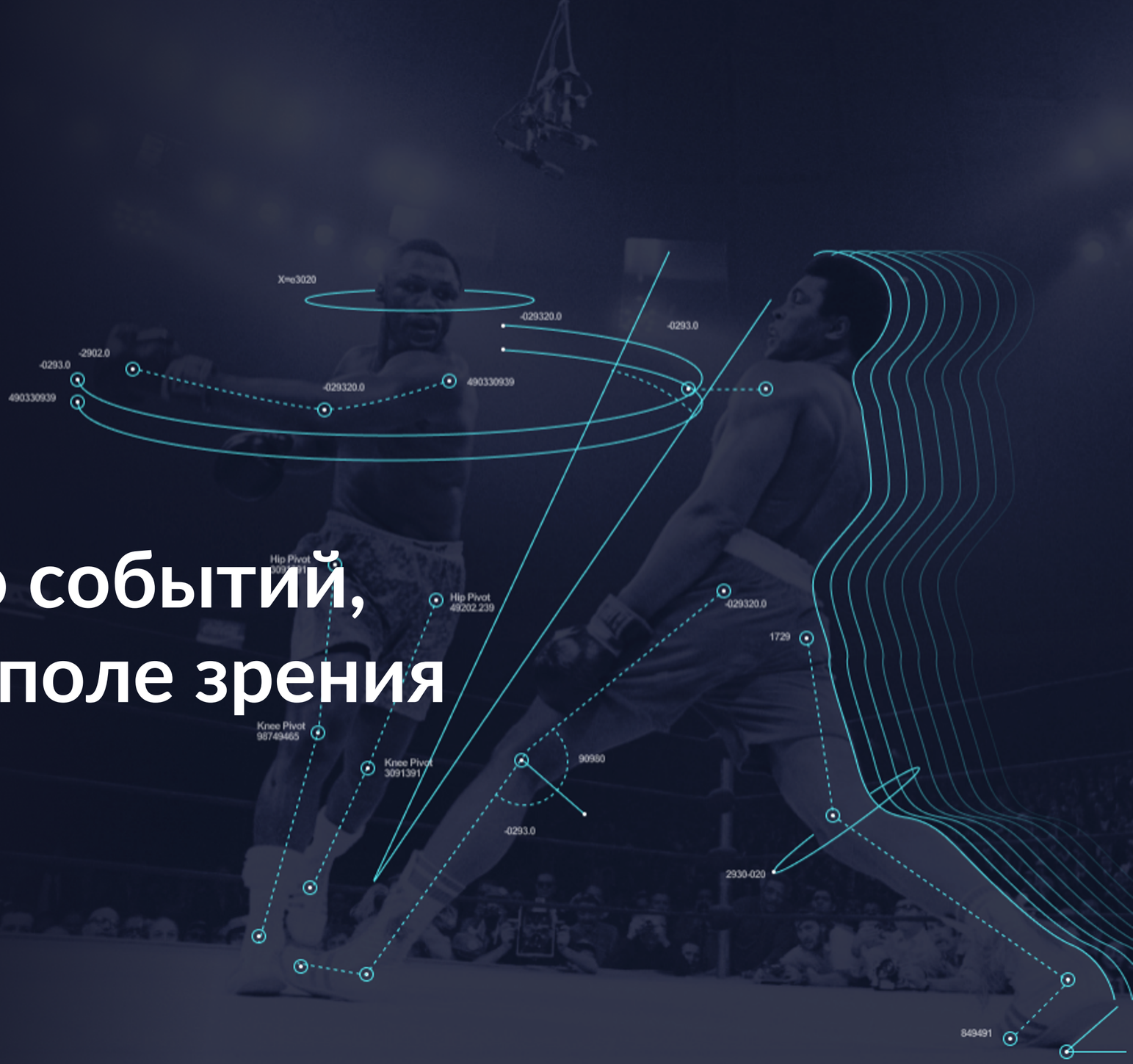
Антивирус, EDR и XDR нового поколения

Илья Осадчий, Тайгер Оптикс

SentinelOne®

Кибербезопасность пропускает входящие вызовы

SentinelOne



Почему?

Слишком много событий, слишком узкое поле зрения

Технологии должны усиливать людей

Устаревшие антивирусы

McAfee
kaspersky
Symantec

Сигнатуры

- Ручной труд
- Проблемы с масштабом и слепыми пятнами
- Редко видят продвинутые атаки

Технологии полагаются на людей

Microsoft
Carbon Black.
CROWDSTRIKE

Облачный мониторинг

- Автоматизированный ручной труд
- Отсылка всей телеметрии в облако
- Реактивное реагирование. Сложное восстановление от атак

Технологии усиливают людей

SentinelOne®

Автономный ИИ на устройстве

- Технологии масштабируют людей
- Машинный контекст + реагирование
- Автоматизация снижает время восстановления

SentinelOne™

Знакомьтесь, SentinelOne!

Антивирус, EDR и XDR нового поколения

SentinelOne. Антивирус, EDR и XDR нового поколения

1,100+
Сотрудников

6,000+
Заказчиков

$697M+
Инвестиции

$10B+
Капитализация

24/7

СЕРВИСЫ
MDR и DFIR

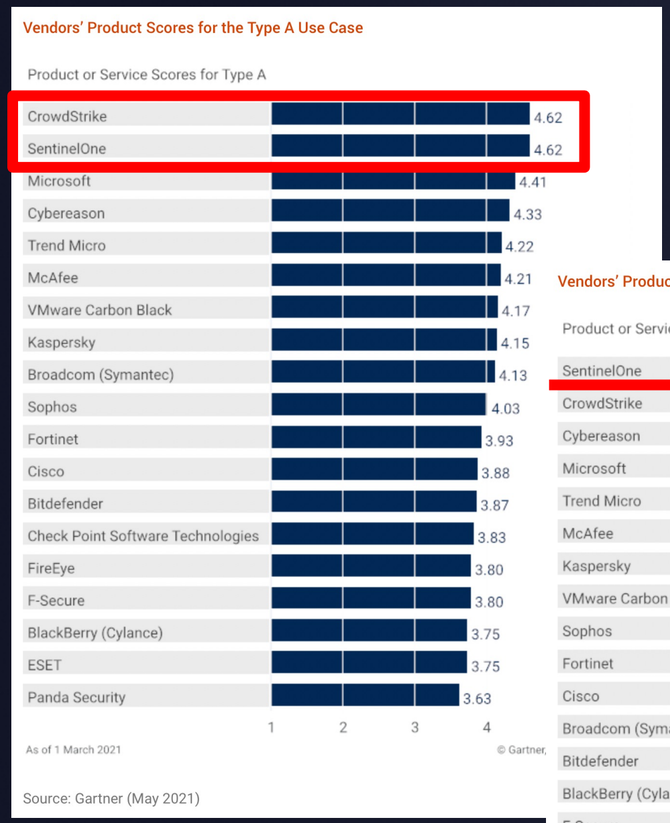
ПОДДЕРЖКА
Follow-the-Sun

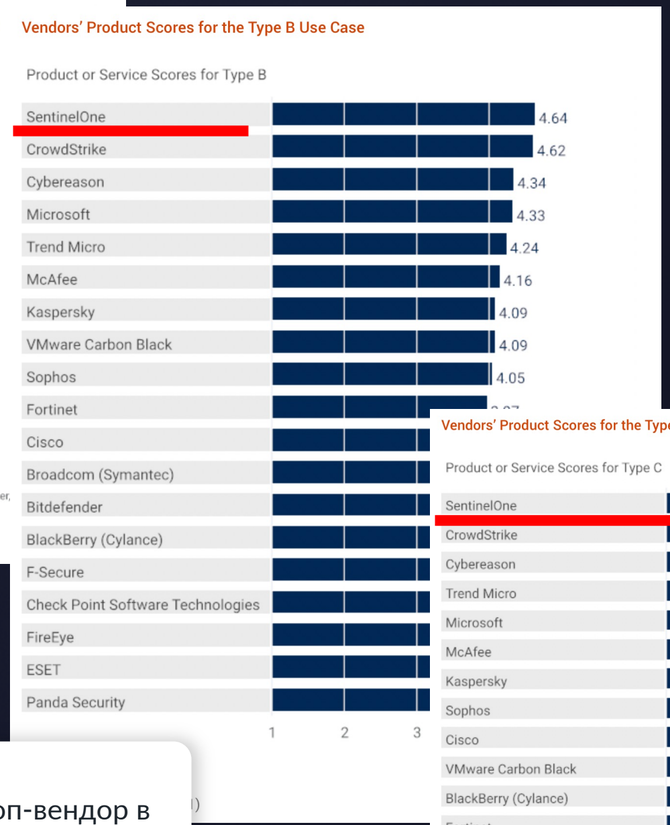
ЛОКАЦИИ
Тель Авив, Амстердам, Токио, Маунтин Вью

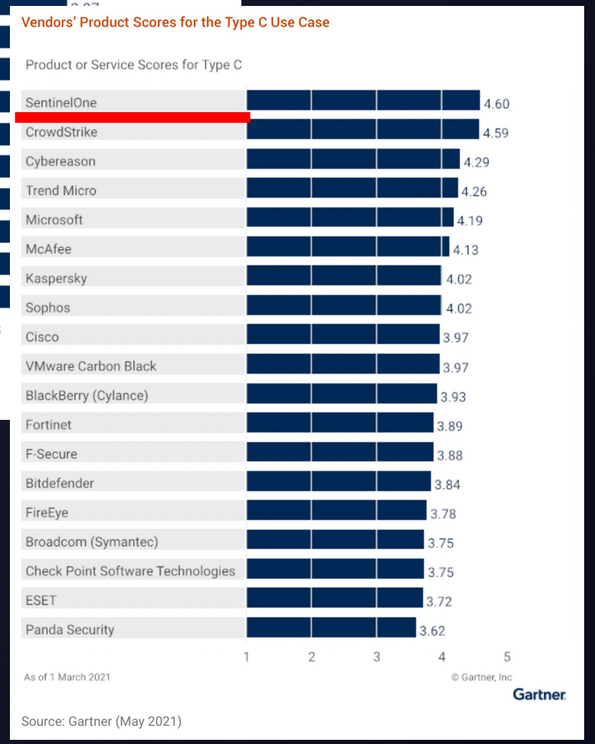
ЗАКАЗЧИКИ
Лидеры ИТ, финансов, ритейла и многие другие
Казахстан, Россия, Азербайджан, Беларусь, Украина

SentinelOne™

Gartner 2021







Gartner peerinsights™

EPP + EDR **4.9** ★★★★★

Топ-вендор в категориях EDR и EPP

Gartner peerinsights™

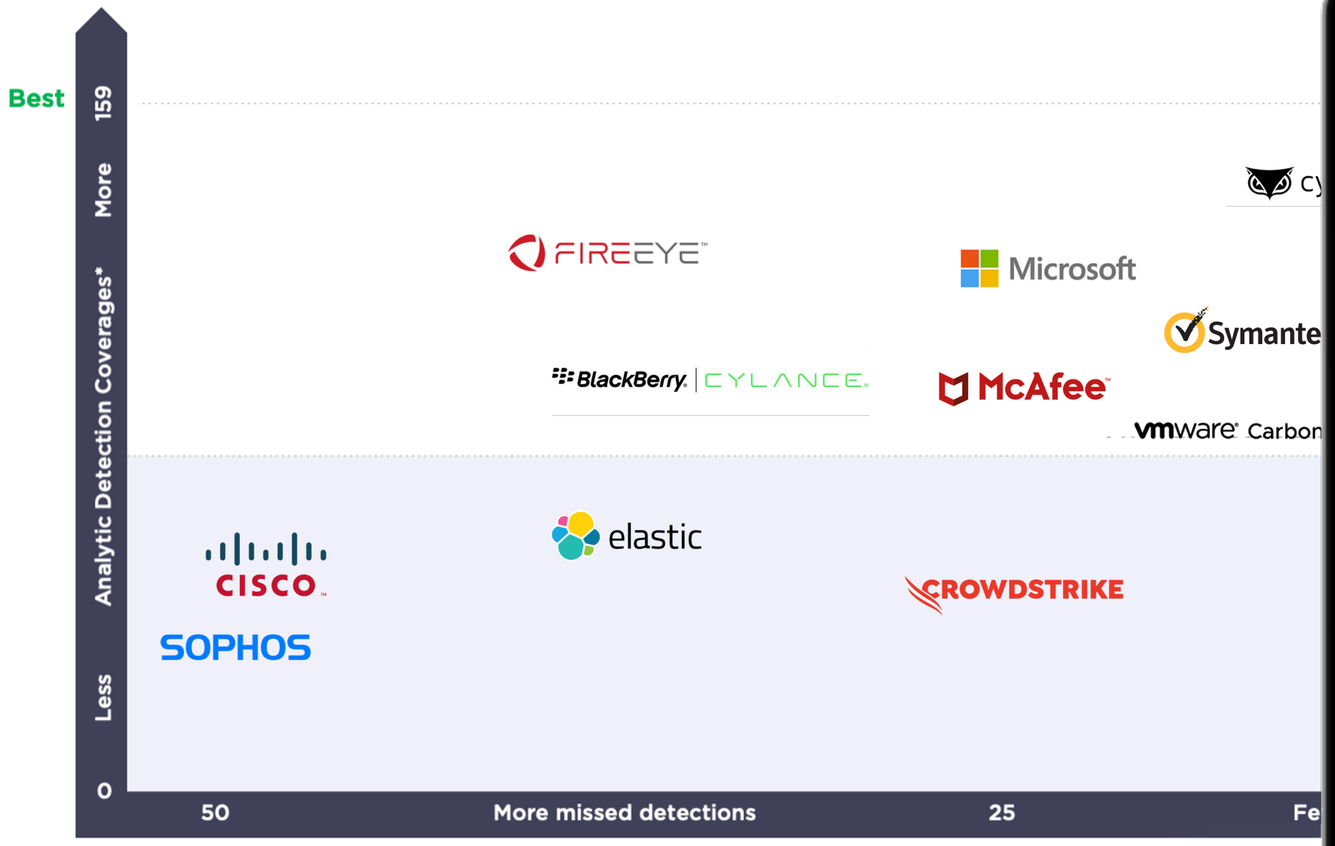
MDR **5.0** ★★★★★

Топ-вендор в категории MDR

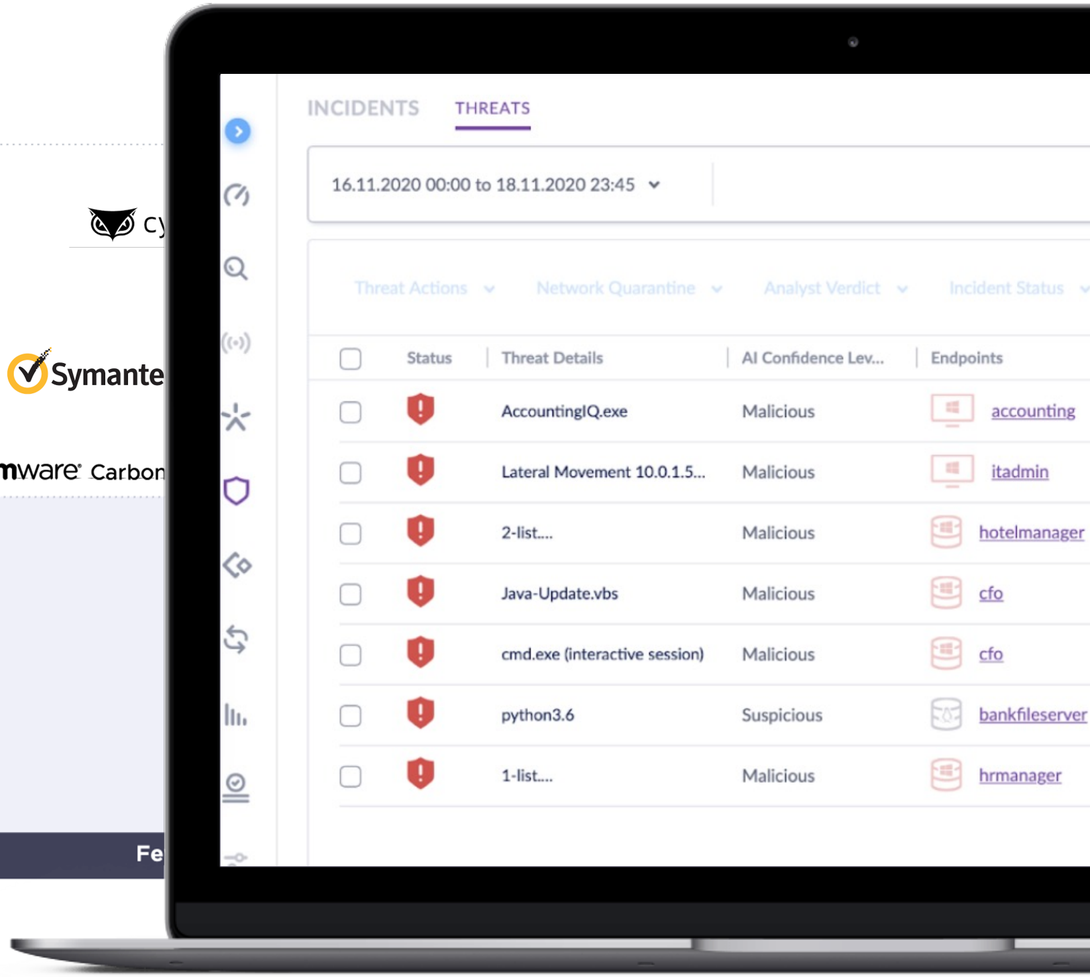
SentinelOne™

Результаты MITRE ATT&CK 2021

SentinelOne показал ноль пропусков и больше всего аналитических детектов



Source: https://attackevals.mitre-engenuity.org/enterprise/participants/?rounds=carbanak_fin7



Почему SentinelOne?

Storyline™

Автоматические причинно-следственные связи снижают нагрузку и ошибки

ActiveEDR®

9 движков в агенте. Проактивный EDR и восстановление на основе ИИ

Ranger®

Инвентаризация и контроль сетевой поверхности атаки без новых агентов или ПО

Singularity™ XDR

Лучший детект за счет интеграции NGAV+EDR с другими продуктами ИБ

1

Консоль

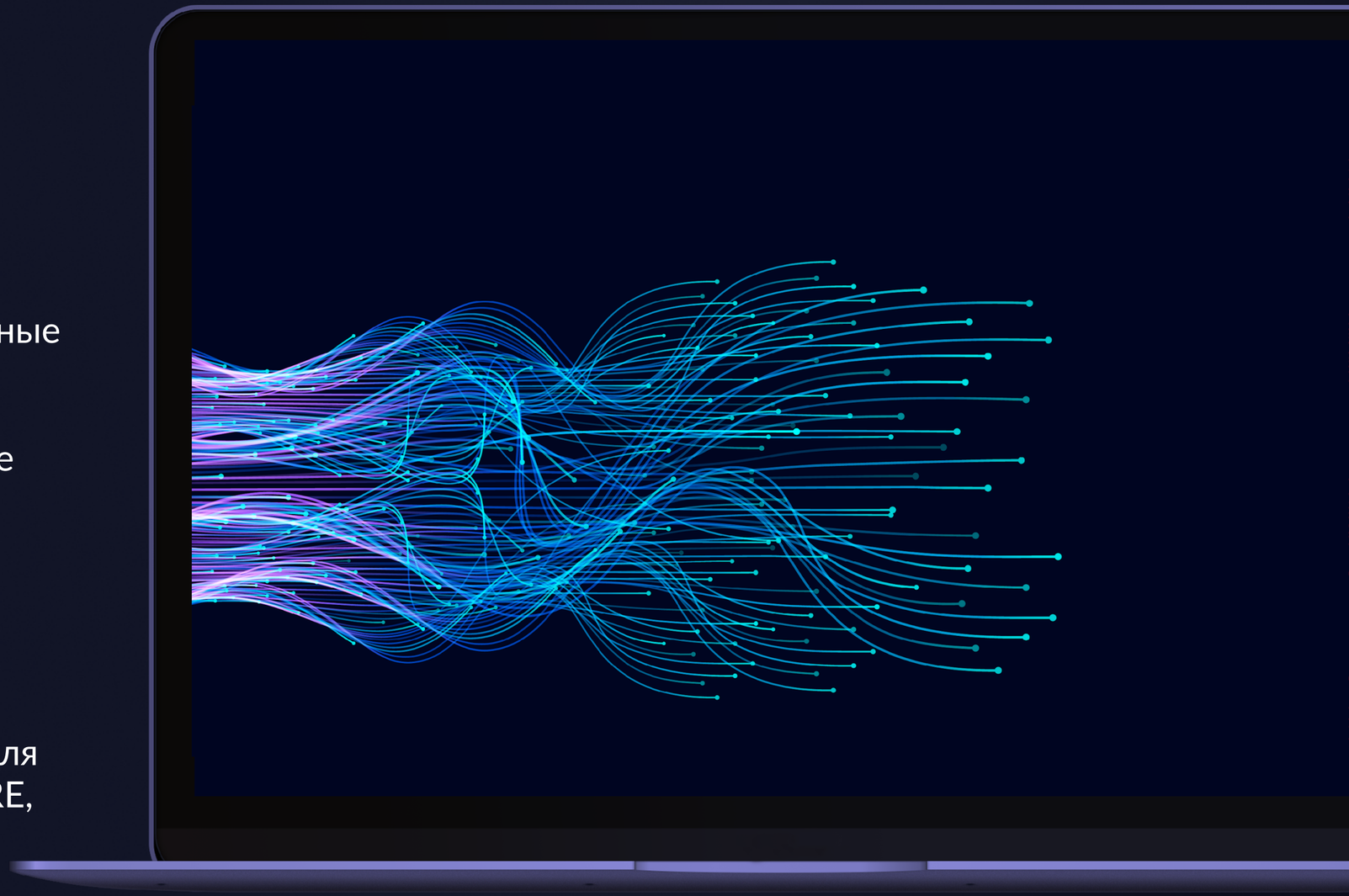
Все функции, все локации в рамках одной консоли

Singularity™ Platform

Storyline™

Автоматические сюжетные линии

- Запатентованные причинно-следственные связи в реальном времени для всех ОС
- Быстрое **блокирование** атаки на основе встроенного ИИ
- Выявление и откат **ВСЕХ** неавторизованных действий в цепочке атаки за один клик
- Долгосрочное хранения EDR-данных для любых запросов, хантинга по TTP MITRE, расследований, реагирования и т.п.



Спасибо!

Закажите демо или тестирование

Илья Осадчий, Тайгер Оптикс