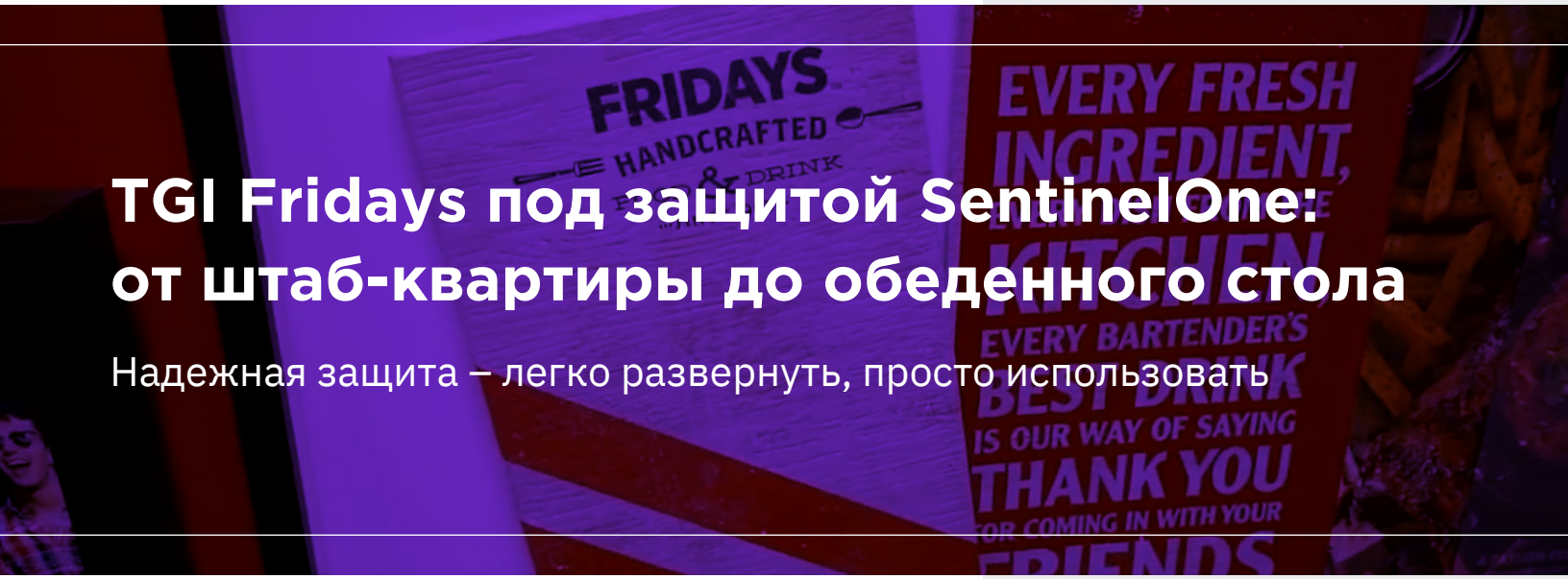
ИСТОРИЯ УСПЕХА



TGI Fridays под защитой SentinelOne: от штаб-квартиры до обеденного стола

Надежная защита – легко развернуть, просто использовать

Задача: обеспечить защиту от внутренних и внешних угроз

«Нашим пользователям постоянно угрожают кибератаки, будь то в этом здании, и за его пределами, – заявляет Сэм Лэнгли, вице-президент по ИТ, в штаб-квартире TGI Fridays в Далласе, штат Техас, – Нам нужна была надежная защита конечных точек, которая следовала бы за пользователями».

TGI Fridays была основана в Нью-Йорке в 1965 году. Сейчас сеть включает в себя более 900 ресторанов в 60 странах, и в ней около 74 000 сотрудников. TGI Fridays работает по модели франчайзинга и специализируется на высококачественных аутентичных американских блюдах и авторских коктейлях, которые подаются более 50 миллионам гостей ежегодно. Собирать людей вместе, чтобы отметить «пятницу», – вот о чем знаменитый слоган TGI Fridays: «У нас всегда пятница».

Чтобы стимулировать рост бизнеса и увеличить маржинальность, TGI Fridays сосредоточилась на приобретении инновационных цифровых технологий, которые бы улучшили качество обслуживания гостей. Приложение с искусственным интеллектом (ИИ) помогло повысить вовлеченность гостей, улучшить внутренние процессы и навыки членов команды, а следовательно, и качество предоставляемых услуг.

«В зоне моей ответственности все технологии для ведения ресторанного бизнеса, – объясняет Лэнгли, – от POS-терминалов и инфраструктуры служебных помещений до разработки ПО для работы в офисе и управления корпоративной инфраструктурой и информационной безопасностью».

ЗАДАЧИ:

- Надежная защита всей компании и всех ее конечных точек от киберугроз
- Быстрое и легкое развертывание, почти незаметное для пользователей
- Простое управление безопасностью конечных точек, позволяющее персоналу сконцентрироваться на критичных проектах

РЕШЕНИЕ:

- Платформа защиты конечных точек SentinelOne XDR

ПРЕИМУЩЕСТВА:

- Ускоренное выявление угроз, их приоритизация и реагирование на инциденты
- Агенты, занимающие мало места, со встроенной автономной системой безопасности в режиме реального времени
- Простое решение с минимальным управлением – «развернул и забыл»

Конкуренция с лучшими из лучших

Платформа SentinelOne, созданная для быстрого развертывания и простого управления как on-premise, так и в облаке, блокирует угрозы на конечных точках с помощью множества движков ИИ, автоматически отправляя файлы в карантин и устраняя риски в реальном времени.

«Обычно мы проводим параллельные пилоты нескольких решений около месяца, – заявляет Лэнгли, комментируя подход TGI Fridays к приобретению новых технологий, – по истечении этого периода мы оцениваем каждого вендора в соответствии с нашими ключевыми критериями успеха: надежной защитой и простотой в развертывании и управлении».

Агент SentinelOne занимает мало места, разворачивается на каждой конечной точке и тем самым обеспечивает автономную защиту. Он успешно выявляет как внутренние, так и внешние угрозы и реагирует, пока они не начали распространяться по сети. Независимые и динамические агенты SentinelOne минимизируют потребность в непрерывном мониторинге и управлении через SOC, сокращают затраты на управление и увеличивают результативность инноваций, способствующих росту бизнеса.

Использование ИИ для защиты от всех векторов угроз

«SentinelOne соответствовал всем нашим ключевым критериям успеха, – объясняет Лэнгли, – главный из которых – обеспечить надежную защиту».

Технология нового поколения SentinelOne в рамках единого агента использует ИИ для защиты устройств от всех векторов на всех этапах: до запуска атаки, во время запуска и после запуска.

До запуска: вместо использования традиционных сигнатур механизм SentinelOne Static AI обеспечивает защиту на уровне агента еще до атаки, устраняя необходимость в постоянном обновлении баз и периодическом сканировании, которое может повлиять на продуктивность пользователей.

Сэм Лэнгли

Вице-президент по ИТ в TGI Fridays

«Автономная модель защиты конечных точек SentinelOne помогает разгрузить мою команду для других критических проектов и позволяет мне сфокусироваться на других аспектах информационной безопасности».

Во время запуска: отслеживая все процессы и их воздействие на уровне агента, механизм Behavioral AI независимо от вектора атаки выявляет подозрительную активность и мгновенно реагирует на нее, защищает всю сеть.

После запуска: предоставляя подробную форензику, автоматический EDR / XDR-модуль SentinelOne устраняет угрозу, изолирует хост от сети и иммунизирует конечные точки от новых угроз. Он также осуществляет откат конечной точки к состоянию до заражения, если это необходимо.

«Мы получили отчет о том, что вредоносное ПО проникает к пользователю. – подчеркивает Лэнгли, – Мы локализовали вредоносное ПО на диске, где наше текущее антивирусное решение его не увидело, установили это ПО на экспериментальный рабочий стол с SentinelOne, и SentinelOne тут же его обнаружил и предотвратил сохранение на диск. Обычный антивирус увидел вредоносное ПО только на следующий день».

Сосредоточьтесь на бизнесе, а SentinelOne позаботится о безопасности сети

«Представляя повтор такого инцидента по всей нашей сети, мне стало ясно, что нужно выбрать SentinelOne, – заявляет Лэнгли, – Автономная модель защиты конечных точек SentinelOne помогает разгрузить мою команду для других критических задач и позволяет мне сфокусироваться на других аспектах информационной безопасности».

Узнайте больше о платформе защиты конечных точек SentinelOne и о будущем защиты конечных точек на сайте Talgar Systems, официального дистрибьютора в СНГ **https://bit.ly/demo-s1**

SentinelOne