allot
See. Control. Secure.

Allot SmartSentinel
Решение для цифрового правоприменения

Введение

Защита национального киберпространства, обеспечение цифрового суверенитета и возвращение государству определенного уровня контроля над сетью передачи данных Internet имеют первостепенное значение для правительств по всему миру.

Allot SmartSentinel позволяет государственным учреждениям получать информацию о национальном сетевом трафике и контролировать его с помощью технологий цифрового правоприменения, гарантирующих соблюдение национальных законов и нормативов.

Мониторинг всего сетевого трафика на национальном и региональном уровнях, а также на уровне пользователя. **Контроль** над деятельностью в Интернете, приложениях и социальных сетях. **Защита** стратегических активов и национальной инфраструктуры от кибератак.

Allot SmartSentinel — это гибкое, мощное и масштабируемое решение для защиты от текущих и будущих угроз с помощью адаптивного машинного обучения, динамической идентификации угроз и других передовых технологий.

Решение

Allot SmartSentinel — это решение, работающее в канале передаче данных и специально разработанное, чтобы помочь правоохранительным органам, органам национальной безопасности и другим государственным учреждениям выполнить требования национальной безопасности, обеспечив соблюдение политик и нормативов во всех телекоммуникационных сетях.
Используя централизованную платформу управления, Allot SmartSentinel может проверять данные со скоростью несколько терабит в секунду, хранить и пересылать петабайты данных приложений и пользователей.

Преимущества

Allot предлагает уникальное унифицированное решение, основанное на масштабируемой системе защиты в канале передачи данных, которая проверяет каждый пакет и предоставляет следующие ключевые преимущества:

- Детализированная визуализация больших объёмов данных поведения сети, пользователей и приложений для поддержки и гарантированного соблюдения законов и нормативов.
- Возможности блокировки: порнография, насилие, наркотики, жестокое обращение с детьми, недостоверный контент и незаконные приложения.
- Неограниченное хранение и пересылку подробных записей об использовании сети передачи данных Internet.
- Защита сетевой инфраструктуры от DDoS-атак.
- Выявление и предотвращение незаконного использования VoIP.

Полнофункциональное решение

SEE

- Полная визуализация IP-трафика, включая зашифрованные данные и приложения, вплоть до уровня отдельного пользователя.
- Автоматический анализ и классификация приложений, пользователей, сеансов, устройств, местоположения, контента, интересов и др.
- Полная и детальная визуализация анонимайзеров, VPN, доступа к сети «Темного Интернета» (Tor) и операций с криптовалютами.
- Сохранение данных: сбор всех записей метаданных.

CONTROL

- Классификация и фильтрация веб-трафика и контента: педофилия, насилие, азартные игры, наркотики и др. (поддерживается черный список International Watch Foundation).
- Блокировка, перенаправление и подавления исходящего / приходящего трафика с указанных сайтов и приложений Мониторинг и блокировка VPN и анонимайзеров.
- Блокировка операций с криптовалютами.
- Выборочное перенаправление подозрительного трафика для дальнейшего анализа, включая трафик TLS/SSL.
- Изоляция протоколов и назначение приоритета трафика в чрезвычайных ситуациях.

SECURE

- Кибербезопасность сети на государственном уровне (защита от вредоносных программ, вирусов и фишинга).
- Блокировка доступа к «Темному Интернету» Tor.
- Обнаружение DDoS-атак и подавление входящих и исходящих массивных атак.
- Обнаружение и сдерживание активности бот-сетей.
- Подробный анализ угроз злоумышленников и их целей в сети.
- Реализация безопасной сети для государственных учреждений и агентств.

Готово к внедрению

Allot SmartSentinel поддерживает следующие распространенные сценарии:

- Фильтрация веб-трафика (по URL-адресу/домену) и контента в соответствии с нормативными требованиями, например жестокое обращение с детьми, порнография, насилие, наркотики, азартные игр и др.
- Блокировка или отключение любой услуги в любом приложении, используемом для незаконной деятельности.
- Выявление доступа пользователей к Tor.
- Обнаружение и отключение подозрительных анонимайзеров и VPN.
- Сохранение данных: сбор и хранение и пересылка метаданных для расследований правоохранительных органов и судебных экспертиз.
- Обнаружение DDoS-атак в национальном масштабе и подавление входящих и исходящих массированных атак.
- Кибербезопасность сети на государственном уровне (защита от вредоносных программ и вирусов, ботов и фишинга) для организаций и пользователей.

О компании Allot

Компания Allot (NASDAQ, TASE: ALLT), основанная в 1996 г., является мировым лидером в области инновационных решений для сетевой аналитики и обеспечения безопасности, предназначенных для регулирующих органов, поставщиков услуг связи и крупных организаций по всему миру. Мы даем нашим клиентам возможность преобразовать нормативные акты, правила и законы в действенные применимые сетевые политики, обеспечивающие кибербезопасность и национальную безопасность. Подкрепленные двумя с половиной десятилетиями доказанного успеха, наши решения для цифрового правоприменения превратят данные о вашей сети, приложениях, использовании и безопасности в действенную аналитику, которая поможет обеспечить защиту страны, сетей и пользователей.

Для получения дополнительной информации о решениях для государственного сектора свяжитесь с нами:
Allot ltd | digital.enforcement@allot.com

Октябрь 2020 г.