Обнаружьте использование сотрудниками теневых ИИ и ИТ

Расширьте возможности мониторинга несанкционированных инструментов ИИ и SaaS с помощью анализа трафика Cloudflare

Выявите то, что скрыто

теневые информационные технологии — проблема не новая, но стремительное внедрение несанкционированных инструментов ИИ вызывает современный кризис:

- **20 %** организаций пострадали от утечек данных из-за инцидентов с теневым ИИ в 2025 году[1]
- **85 %** руководителей в сфере ИТ заявляют, что сотрудники вводят инструменты ИИ до того, как ИТ-отдел успевает их оценить[2]

Cloudflare возвращает организациям возможности мониторинга, необходимого для управления этой расширяющейся поверхностью атаки:

- **Проверяйте статус приложений:** классифицируйте приложения ИИ и SaaS как одобренные, не одобренные или находящиеся на рассмотрении.
- **Применяйте политики в зависимости от статуса приложения:** разрешайте, блокируйте, изолируйте, применяйте обнаружения DLP к взаимодействиям, ограничивайте загрузку файлов и многое другое
- **Анализируйте использование приложений:** отслеживайте общие тенденции и проводите детальные расследования.
- **Оценивайте риск приложений:** определяйте уровень их надежности с помощью рейтингов доверия приложений.

Уникальные риски теневого ИИ

Теневой ИИ отличается от традиционных теневых ИТ. В то время как SaaS-приложения в основном хранят файлы или обмениваются ими, инструменты ИИ преобразуют и обучаются на любых данных, вводимых сотрудниками.

Это означает, что конфиденциальные данные, такие как интеллектуальная собственность, данные клиентов или исходный код, могут быть необратимо поглощены для обучения модели, без возможности их удаления.

Как это работает

Платформа SASE от Cloudflare встроена в поток трафика между вашими сотрудниками и ресурсами, обеспечивая унификацию мониторинга и контроля.

Кроме того, интегрируйте CASB от Cloudflare через API для сканирования неправильных настроек, действий пользователей и конфиденциальных данных.
Управляйте безопасностью приложений ИИ (ChatGPT, Claude, Google Gemini), а также других SaaS-приложений.
Используйте CASB совместно с вашим поставщиком удостоверений, чтобы, отслеживать, когда пользователи аутентифицируются в любых несанкционированных сторонних приложениях.

Пример панелей управления

Фильтруйте этот обзор использования приложений по следующим критериям:

- Приложение и тип приложения
- Статус одобрения
- Защищено с помощью ZTNA
- Количество пользователей

Для получения более подробной информации нажмите на название любого ИИ-приложения, чтобы увидеть конкретных пользователей или группы, которые к нему имеют доступ, частоту использования, местоположение и объем переданных данных.

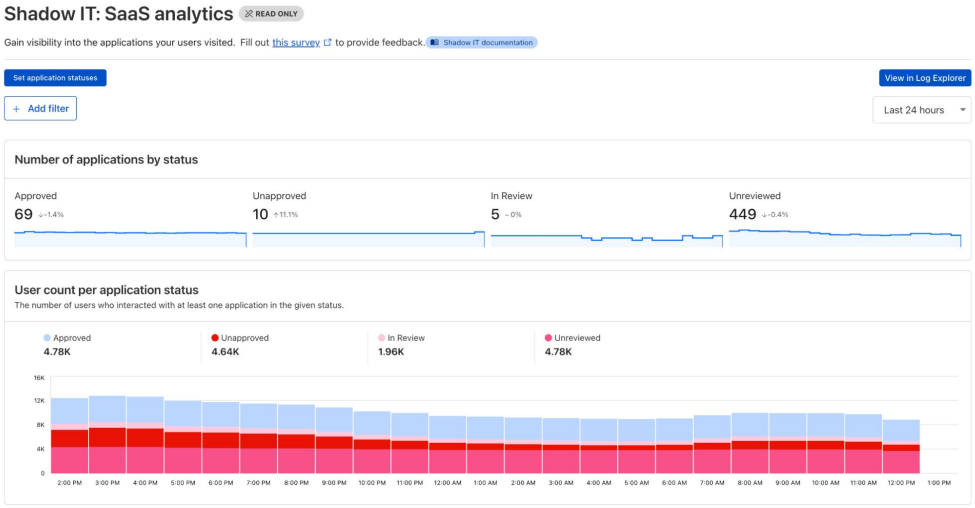

Рисунок 1: Панель аналитики теневых ИТ

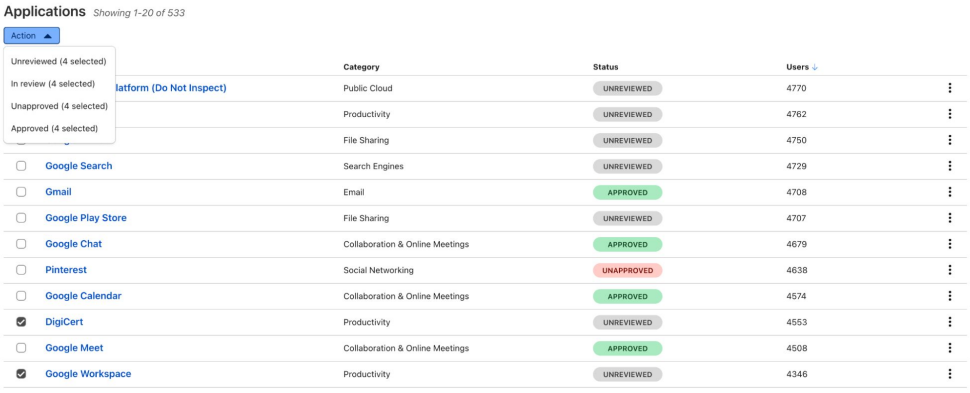

Рисунок 2: Отмечайте статусы приложений

Организуйте приложения и устанавливайте политики доступа в зависимости от статуса одобрения:

- Одобренные (санкционированные)
- Неодобренные (несанкционированные)
- На рассмотрении
- Не рассмотрено

Хотите получить дополнительные технические рекомендации? Узнайте, как создавать политики с помощью этого учебного маршрута..

Хотите подробнее узнать о том, как обеспечить безопасность при внедрении ИИ?

Изучить больше сценариев использования | **Запросить семинар**

1. IBM, отчет "Cost of a Data Breach" за 2025 г.: Источник
2. Исследование ManageEngine 2025: Источник

© Cloudflare Inc., 2025. Все права защищены. | 1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com