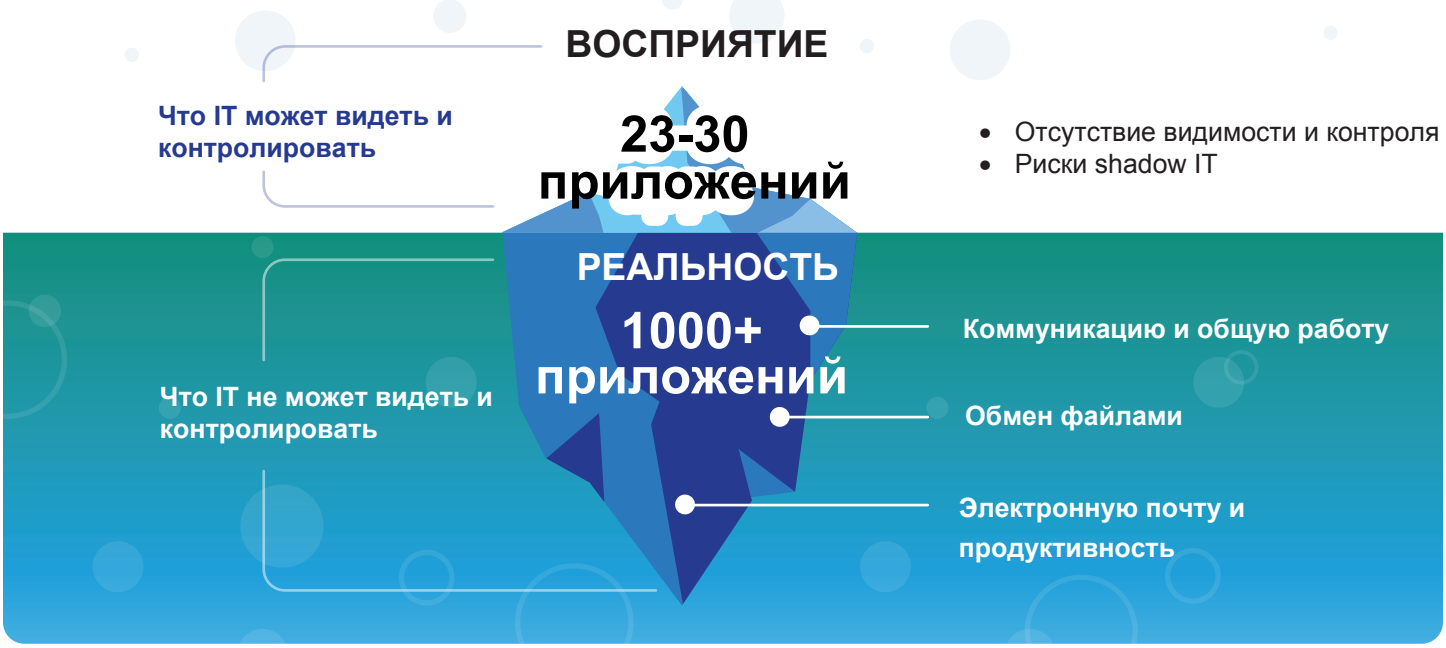
SpinSPM: Управление SaaS безопасностью

Обеспечьте полную видимость и быстрое реагирование на инциденты, связанные с неправильной конфигурацией, несанкционированными сторонними приложениями и расширениями браузера. Это позволит снизить риски безопасности, соблюдения требований стандартов, потери и утечки данных.

Вызов

Как организации управляют неправильной конфигурацией и доступом к SaaS приложениям или расширениям браузера, которые имеют доступ к важным для бизнеса SaaS данным?

Кажущиеся на первый взгляд 20-30 приложений на самом деле могут оказаться тысячами несанкционированных рискованных приложений и расширений браузера с опасными уровнями доступа. Отсутствие видимости приводит к рискам безопасности, соблюдения требованиям стандартов, потери и утечки данных.



Основные Характеристики

Более 80 % организаций сталкиваются с неправильной SaaS конфигурацией и рискованными сторонними приложениями, что приводит к непосредственным угрозам безопасности. Для команд безопасности, которым необходимо снизить риски неправильной конфигурации и сторонних приложений, SpinSPM обеспечивает полную видимость и автоматизированное реагирование на инциденты, что позволяет сэкономить время, снизить затраты на безопасность и повысить уровень соответствия стандартам.

В отличие от других решений SSPM, SpinSPM обеспечивает автоматизированную, детальную оценку рисков, определяя риски безопасности и соответствия стандартам, используя уникальную базу данных из более чем 300 000 приложений и расширений браузера, оцененных алгоритмами искусственного интеллекта. Google использует, рекомендует и отмечает данное решение как Strong Performer в отчете Forrester SSPM Wave. SSPM пользуется доверием 1500+ организаций по всему миру.

Управление случаями неправильной конфигурации

Выявляйте и устраняйте ошибки в конфигурации, отклонения в системе безопасности и нарушения нормативных требований в ваших SaaS-приложениях с помощью автоматизированного обнаружения и реагирования.

Управление доступом

Составьте список разрешенных или блокированных рискованных приложений или расширений браузера для всех или определенных организационных подразделений, чтобы предотвратить несанкционированный доступ к критически важным данным SaaS.

Полная видимость

Проведите инвентаризацию всех облачных сервисов, мобильных приложений, SaaS приложений и расширений браузеров, имеющих доступ к вашей SaaS среде. Узнайте, кто имеет доступ к этим приложениям.

Автоматизация

Автоматизируйте управление доступом, создавая детализированные политики безопасности для мониторинга, оповещения и блокировки/разрешения приложений и расширений браузеров на основе заданных критериев.

Оценка рисков

Используйте непрерывный мониторинг 24/7 и постоянную оценку рисков на основе искусственного интеллекта, принимая во внимание более 15 факторов риска. Получите полное представление о потенциальных рисках для вашего бизнеса, безопасности и соблюдения требований стандартов каждого приложения и расширения для браузера.

Быстрое реагирование на инциденты

Получайте немедленные настраиваемые уведомления об обнаруженных инцидентах, неправильных конфигурациях и изменениях показателей риска в одном месте, включающей расширенную отчетность и интеграцию с Splunk, ServiceNow, Jira и Slack.

Интеграция в Google

Компания SpinAI была выбрана Google для интеграции в Google Workspace Console с целью оценки риска санкционированных и несанкционированных расширений для браузера Chrome.

SpinSPM доступен для

Google Workspace

slack

Microsoft 365

salesforce

Кейс Клиента

Глобальный автопроизводитель защищает цифровое рабочее пространство с помощью SpinOne

Один из крупнейших автопроизводителей в мире хотел защитить данные SaaS в Google Workspace для тысяч сотрудников многочисленных отделов, заводов и офисов, расположенных по всему миру. Видимость всех используемых ими SaaS-сервисов стала критически важной, как и безопасность всех данных в этих SaaS-приложениях.

Производственной компании требовалось решение, которое может обнаружить, оценить и управлять доступом на всех сторонних OAuth-приложениях и расширениях браузера. Spin.AI было единственным решением, которое обеспечило оценку на основе искусственного интеллекта без необходимости использования агента.

С помощью SpinOne компания сократила время, необходимое для оценки риска приложений, с 2 лет при ручной проверке до 2 месяцев автоматической диагностики для 50 000 сторонних приложений. Это привело к окупаемости инвестиций в миллионы долларов.

Провайдер платформы контента защищает данные Google Workspace

Ведущая платформа в области контента и рекламы не имела видимости активности пользователей в Google Workspace, сторонних приложениях и расширениях браузера, что повышало риск утечки данных и теневых ИТ.

Чтобы уменьшить этот риск и защитить данные сотрудников, они объединили свои усилия по безопасности с помощью SpinOne для защиты утечки данных и управления SaaS безопасностью.

Используя SpinOne, они получили полную видимость пользователей и действий во всей среде, а также повысили эффективность с помощью политик и процессов утверждения для автоматической блокировки приложений и расширений с высокой степенью риска.

Рекомендовано Google Workspace

Попробуйте SpinOne в действии. Закажите бесплатную демонстрацию

Заказать демо-версию

iIT Distribution является официальным Value Added дистрибьютором, который постоянно развивается в сфере проектной дистрибуции сложных B2B решений в Украине, Польше, Казахстане и странах Балтии. Мы представляем программные решения от ведущих мировых поставщиков. Наша миссия заключается в том, чтобы обеспечить организации любого размера современными возможностями ИТ-инфраструктуры, обеспечивая их защиту от преобладающих угроз информационной безопасности.

E-mail: sales@iitd.com.kz
Больше информации на сайте: https://kz.iitd.com.ua/ru/