cpl.thalesgroup.com

THALES

SafeNet Trusted Access

Сервис управления доступом к облачным приложениям

Переход к облачным технологиям на предприятии

Облачные приложения играют важную роль в удовлетворении производственных и инфраструктурных потребностей предприятия. Однако чем больше облачных приложений использует организация, тем сложнее управлять многочисленными удостоверениями пользователей. С каждым новым облачным сервисом отслеживать события доступа к облачным ресурсам становится все сложнее, а риск несоблюдения нормативных требований возрастает. Пользователям сложно удерживать в памяти разные учетные данные для входа в каждое приложение, и они часто отправляют в службу поддержки запросы на сброс пароля. А если облачные приложения изначально защищены только слабыми статическими паролями, риск утечки данных возрастает многократно.

Доступ в облако

SafeNet Trusted Access решает эти проблемы.

Сервис обеспечивает централизованное управление доступом к облачным и веб-приложениям с надлежащим уровнем защиты. SafeNet Trusted Access облегчает вход в учетные записи. Благодаря гибким политикам на основе рисков, единому входу в облачные приложения и универсальным методам аутентификации организации получают масштабируемые средства управления доступом в облако, учитывающие требования бизнеса, законодательства и сопутствующие риски.

Организации могут надежно защитить доступ к облачным приложениям и снизить риски, усовершенствовав собственную модель безопасности и существующие схемы аутентификации для доступа в облако.

Принцип работы

Каждый раз, когда пользователь входит в облачное приложение, SafeNet Trusted Access выполняет следующие действия:

- проверяет удостоверение пользователя;
- определяет применимую политику доступа;
- применяет подходящий уровень аутентификации на основе интеллектуального единого входа.

Преимущества SafeNet Trusted Access

SafeNet Trusted Access предотвращает утечки данных, помогает организациям соблюдать нормативные требования и делает переход в облако простым и безопасным.

Предотвращение утечек данных

- Применение различных методов многофакторной аутентификации и контроль доступа к каждому приложению без паролей

Безопасный переход в облако

- Дополнение существующих инструментов контроля доступа к облачным приложениям и применение стандартизированных политик доступа ко всем облачным ресурсам

Простое соблюдение требований

- Регистрация событий доступа каждого пользователя к каждому приложению в режиме реального времени помогает подтвердить соблюдение нормативных требований

Основные возможности SafeNet Trusted Access

SafeNet Trusted Access предлагает пять основных возможностей.

1. **Интеллектуальный единый вход.** Для входа во все облачные приложения применяется единое удостоверение. Пользователям больше не придется запоминать множество паролей и постоянно сбрасывать их, теряя время. SafeNet Trusted Access обрабатывает запросы пользователя на вход и обеспечивает интеллектуальное применение единого входа исходя из предыдущих операций аутентификации в том же сеансе единого входа и конкретных требований политики, применимых к каждой попытке доступа. Таким образом пользователи могут лишь один раз пройти аутентификацию для доступа к своим облачным приложениям или пройти дополнительную проверку, если того требует политика доступа.

2. **Политики доступа на основе сценариев.** SafeNet Trusted Access предлагает гибкую и простую в использовании систему политик доступа, которая позволяет в реальном времени применять политики на уровне отдельных пользователей, групп или приложений. Система политик доступа поддерживает разнообразные методы аутентификации, включая уже принятые в организации, что позволяет задействовать прошлые инвестиции в защите облачных и веб-сервисов.

3. **Аналитические данные.** Аналитические данные о событиях доступа позволяют организациям точно настроить политики доступа и выбирать оптимальный уровень их строгости. Статистика и журналы доступа по разным приложениям и политикам, а также регистрация причин неудавшихся или отклоненных попыток доступа помогают проводить проверки и расследования и выявлять лицензии на облачные приложения, которые используются не в полную силу.

4. **Универсальная аутентификация.** SafeNet Trusted Access поддерживает различные методы проверки подлинности и позволяет использовать существующие в организации схемы аутентификации. Обширный ряд поддерживаемых методов аутентификации и форм-факторов токенов в сочетании с контекстной аутентификацией делают доступ для пользователя более удобным и позволяют снизить риск, повышая степень доверия только при необходимости.

5. **Простое управление приложениями.** Постоянно пополняемая библиотека шаблонов интеграции позволяет с легкостью подключать сервис к самым популярным облачным приложениям, таким как Salesforce, AWS и Office 365. Просто воспользуйтесь встроенными заготовленными шаблонами интеграции для уже используемых вами приложений или настройте шаблон общего назначения.

Поддерживаемые методы аутентификации

- Одноразовые пароли в push-уведомлениях
- Программные генераторы одноразовых паролей
- Аппаратные генераторы одноразовых паролей
- Аутентификация на основе шаблонов
- Аутентификация по внешнему каналу: электронной почте и SMS
- Пароль
- Протокол Kerberos
- Учетные данные инфраструктуры открытых ключей (PKI)
- Google Authenticator
- Аутентификация без пароля
- Биометрия
- Голос
- Сторонние методы

Решения SafeNet компании Thales для управления доступом и аутентификацией

Компания Thales предлагает передовые решения для централизованного управления доступом и аутентификацией, которые помогают защитить доступ к ИТ-инфраструктуре предприятия и используемым облачным и веб-приложениям. Единый вход на основе политик доступа и универсальные методы аутентификации позволяют эффективно предотвращать утечки данных, безопасно мигрировать в облако и соблюдать нормативные требования.

Управление доступом к популярным приложениям

SafeNet Trusted Access поддерживает сотни приложений, в том числе:

amazon web services, Office 365, salesforce, G Suite, zendesk, WordPress, box, JIRA, Citrix ShareFile, f5, BLUE COAT, Drupal, IBM Connections, Pulse Secure, servicenow, OWA

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019 · ISO 27001:2013 CERTIFIED · AICPA SOC · GDPR Ready