SecurAccess

Мобильная бестокенная (tokenless®) двухфакторная идентификация для VPN, SSL, Remote Desktop, WiFi, веб-порталов и шифрования ноутбука. *SecurAccess* — это современная альтернатива физическим ключам/ токенам.

Токены больше не нужны!

SecurAccess позволяет воспользоваться существующим персональным устройством для аутентификации пользователя. Пользователи с несколькими устройствами могут перемещаться с одного устройства на другое без каких-либо помех.*

Особенности

Пароли сами по себе не достаточны для защиты данных более трех миллиардов организаций, работающих в режиме онлайн. Двухфакторная аутентификация обеспечивает надежную безопасность, и благодаря существующим мобильным устройствам пользователя ее можно развернуть легко и дешево.

Решение ***SecurAccess*** может быть реализовано как программного решения на территории клиента или хоститься в рамках управляемой услуги. Простота регистрации при 2FA обеспечена тем, что устройство пользователя является главным инструментом аутентификации, стоимость которого в разы ниже стоимости традиционных аппаратных токенов. Любой мобильное устройство может быть использовано как средство аутентификации.

В отличие от традиционных способов аутентификации с использованием аппаратных токенов, SecurAccess может быть развернута быстро и масштабироваться до 25 пользователей в секунду (1500 в минуту). Пользователи могут автоматически и просто развертываться через групповое членство в протоколе LDAP, без дополнительных затрат на оборудование.

SecurAccess использует текущий сервер LDAP как свою базу данных и легко интегрируется с Microsoft Active Directory, Novel eDirectory, SunDirectory Server и Open LDAP без необходимости дополнительных баз данных или аппаратного обеспечения, обеспечивая поддержку нескольких серверов в нескольких доменах.

SecurAccess доступна по фиксированной ежегодной цене, которая вносится за каждого пользователя, без скрытых доплат.

Преимущества

- Повторное использование существующего хранилища пользователей LDAP - нет потребности в дополнительных базах данных
- Пользователям нет необходимости запоминать дополнительные пароли, так как они могут использовать свой существующий LDAP пароль
- Не требует дополнительного PIN-кода, в отличие от других двухфакторных систем аутентификации (в случае необходимости предоставляется PIN поддержка)
- Использует существующие устройства — пользователям не нужно носить с собой дополнительные устройства аутентификации
- Отсутствие физических токенов развертывания или затрат на восстановление ключей
- Нет необходимости в ресинхронизации или сбрасывании PIN, что сокращает время на управление
- Развертывание для тысяч пользователей за считанные минуты, экономя время и деньги

Параметры доставки

- Коды на один или несколько дней
- SMS с кодом-паролем в режиме реального времени по требованию и блокировка сеанса
- Предварительно загруженные SMS, гарантируя 100% доставки кода-ключа
- Коды-ключи посылаются через безопасную электронную почту
- Приложения для программных токенов
- Голосовой вызов с кодами-ключами с вводом через клавиатуру телефона для блокировки интернет-сеанса через телефонную сеть
- Веб-интерфейс самопомощи, который позволит пользователям запрашивать временные коды-пароли в случае утери телефона.

*У пользователя может быть только один профиль, который может быть активирован только на одном устройстве в один период времени.

Authenticate your way

SecurEnvoy является первопроходцем в области бестокенной двухфакторной аутентификации. Наши инновационные решения обеспечивают удобную, безопасную аутентификацию, которая в разы дешевле, чем аутентификация с использованием маркеров, и применяется по всему миру тысячами клиентов.

Контроль получает пользователь

Мы считаем, что для аутентификации пользователи должны иметь возможность выбрать любое персональное устройство в качестве своего токена, будь то мобильный телефон, планшет, ноутбук или даже рабочий телефон. Пользователи должны иметь возможность легко переносить свои идентификационные данные с одного устройства на другое, не оставляя персональных сведений на устаревших носителях.

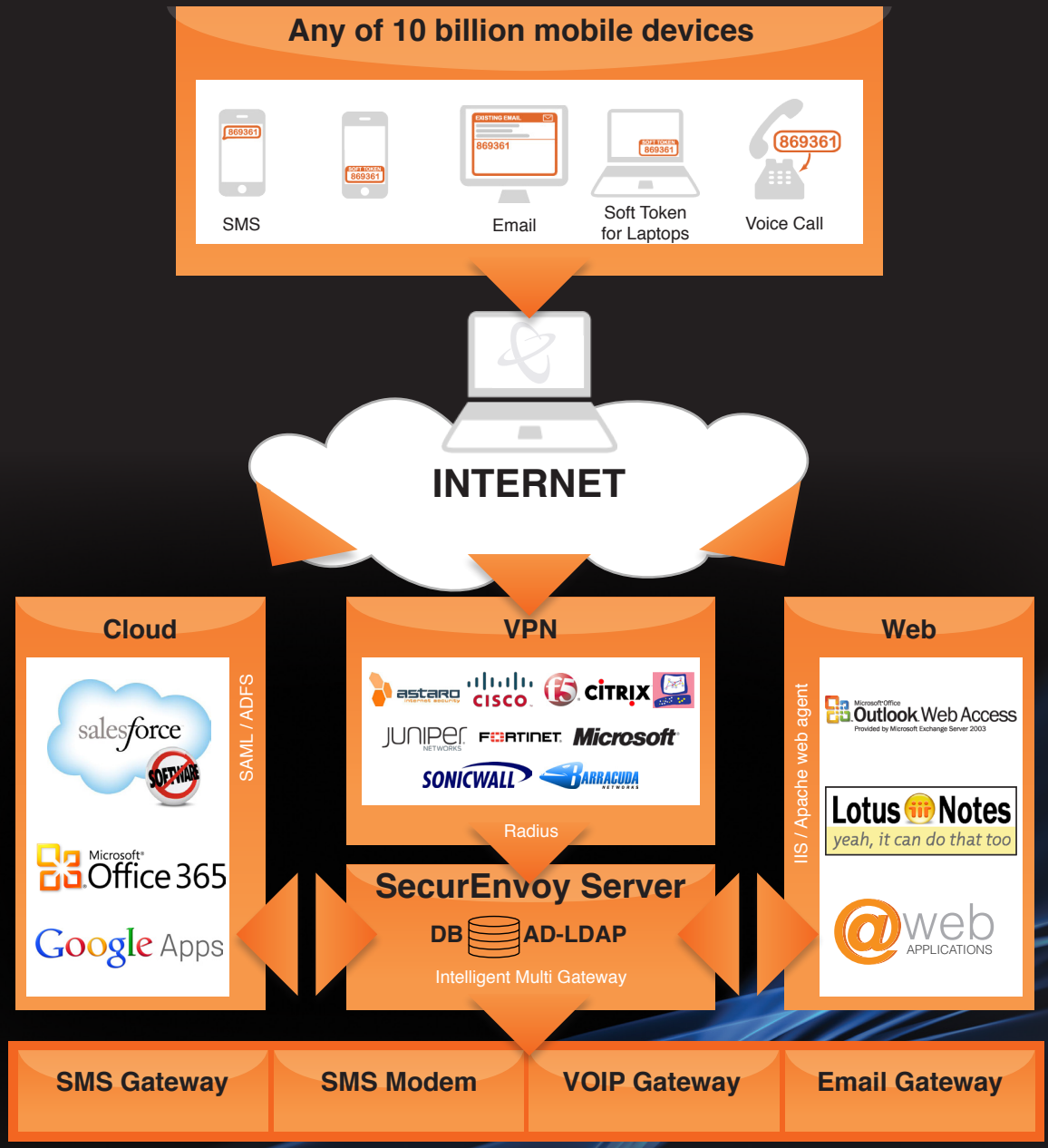
Мир без аппаратных ключей безопасности

Аппаратные ключи безопасности, появившиеся более 30 лет назад, препятствуют массовому распространению двухфакторной аутентификации, так как они дороги при развертывании и запуске и нелегко масштабироваться. Пользователи не могут носить с собой отдельные аппаратные ключи для каждого вида деятельности — офиса, банка и т.д. Становится очевидным, что использование существующего личного устройства, такого как мобильный телефон, является решением проблемы.

Будучи изобретателями бестокенной аутентификации, мы намерены продолжать разрабатывать инновационные решения, основанные на персональных устройствах пользователей и решать проблемы, мешающие распространению таких решений, такие как задержки SMS, отсутствие телефонного сигнала или проблемы синхронизации.

Элегантная простота

Мы считаем, что процесс входа в систему должны быть как можно более простым, что тысячи пользователей могут быть включены в работу нажатием одной кнопки, при этом сохраняя высокий уровень безопасности. Наши концепции усиливают существующую инфраструктуру, например, Active Directory в качестве центральной базы данных, и создают простые и элегантные решения.



SecurEnvoy plc I info@SecurEnvoy.com I www.SecurEnvoy.com