Программное обеспечение для защиты паролей Specops

Безопасность ИТ начинается с укрепления самого слабого звена - паролей

Specops sofware

- Шведская компания, основанная в 2001 году
- Является частью группы Outpost24
- Штаб квартира находится в Стокгольме, Швеция
- Офисы Specops имеются в Великобритании, Германии, Франции, США и Канаде
- Поддержка мирового класса
- ПО становится «нативной» частью Windows
- ПО занимается:
  - Защитой паролей и аудитом
  - Самостоятельным восстановлением паролей
  - Самостоятельным восстановлением шифрования HD
  - Синхронизацией паролей

”Мы – эксперты, помогающие вам помочь вашим пользователям”

Пароли…

- по-прежнему остаются аутентификатором номер один
- Являются часто используемым вектором атаки
- Увеличивают расходы на поддержку
- Не помогают пользователям
- Не меняются, пока вы не поможете/не заставите их сменить

Что такое хороший пароль?

- 8 символов – супер сложный
  - g%5Y#9wQ - на перебор уйдет несколько часов.
  - Очень трудно запомнить - скорее всего, придется записывать.
- 17 символов – разрешенные слова, обязательно строчные
  - lemon, box, redwine - на перебор уйдет триллион лет.
  - Нетрудно запомнить
- Взломанный пароль всегда небезопасен, поэтому нужно предотвратить его использование

Сложные пароли сложны для людей, но не для компьютеров

Specops Password Policy

- Никаких изменений в процессах Windows, продукт активен только во время смены пароля
- Параметры, определенные в одном/нескольких традиционных GPO
- Будет контролировать каждую смену пароля
- Все настройки, которые только можно придумать.
- Несколько различных типов "словарей”
- Отправляйте электронные письма с предупреждением об истечении срока действия пароля
- Легкая эксплуатация для конечного пользователя, так как не требует обучения

Защита от утекших паролей

- База данных с утечками паролей с добавлением наших “honey pots", расположенных на шести континентах
- Новые записи ежедневно поддерживаемые Specops-ом
- Около 2,4 миллиарда уникальных хэшей паролей
- Блокирует только при точном совпадении
- 2 версии
  - Полная - Размещается на сервере Specops, локальный сервер выступает в качестве прокси. Верификация "задним числом" - 2 секунды!
  - Express - около 750 миллионов хэшей, хранятся в виде файлов в Sysvol, обновляются 5 раз в год. Верификация в режиме реального времени.

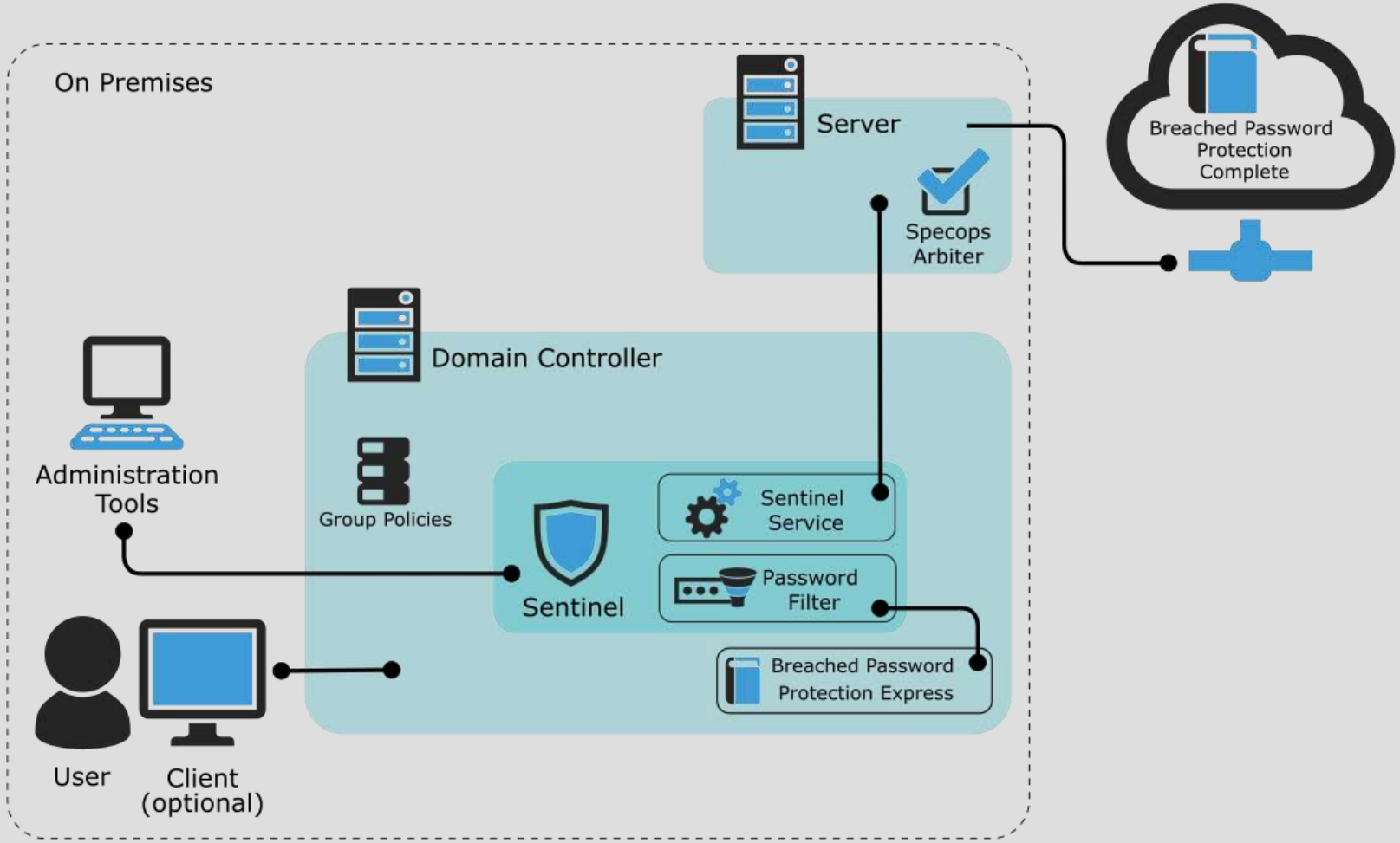
"Разочарованные пользователи не помогут вам обеспечить безопасность сети".

Словари

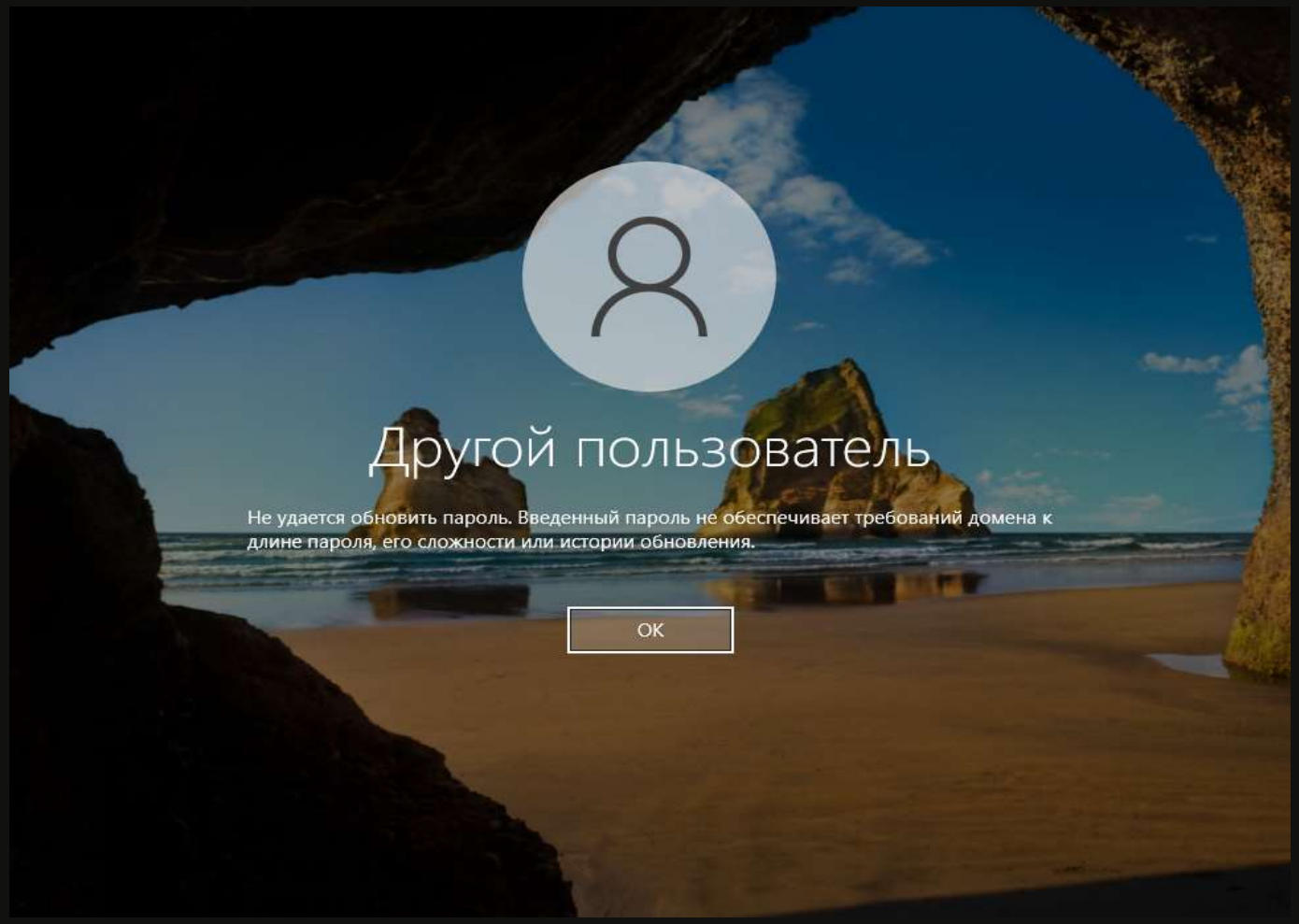
- Создаются и поддерживаются заказчиком
- Могут включать в себя нежелательные слова, например:
  - Общие слова
  - Географические места
  - Бизнес-термины
  - Календарные единицы (May2020!)
  - Графические клавиатурные паттерны (соседство символов)
- Можно блокировать части пароля
- Защита от подмены символов
  (s = S = 5 = $ = § и т.д.)
- Запускаются в оперативной памяти вашего DC.

"Разочарованные пользователи не помогут вам обеспечить безопасность сети".

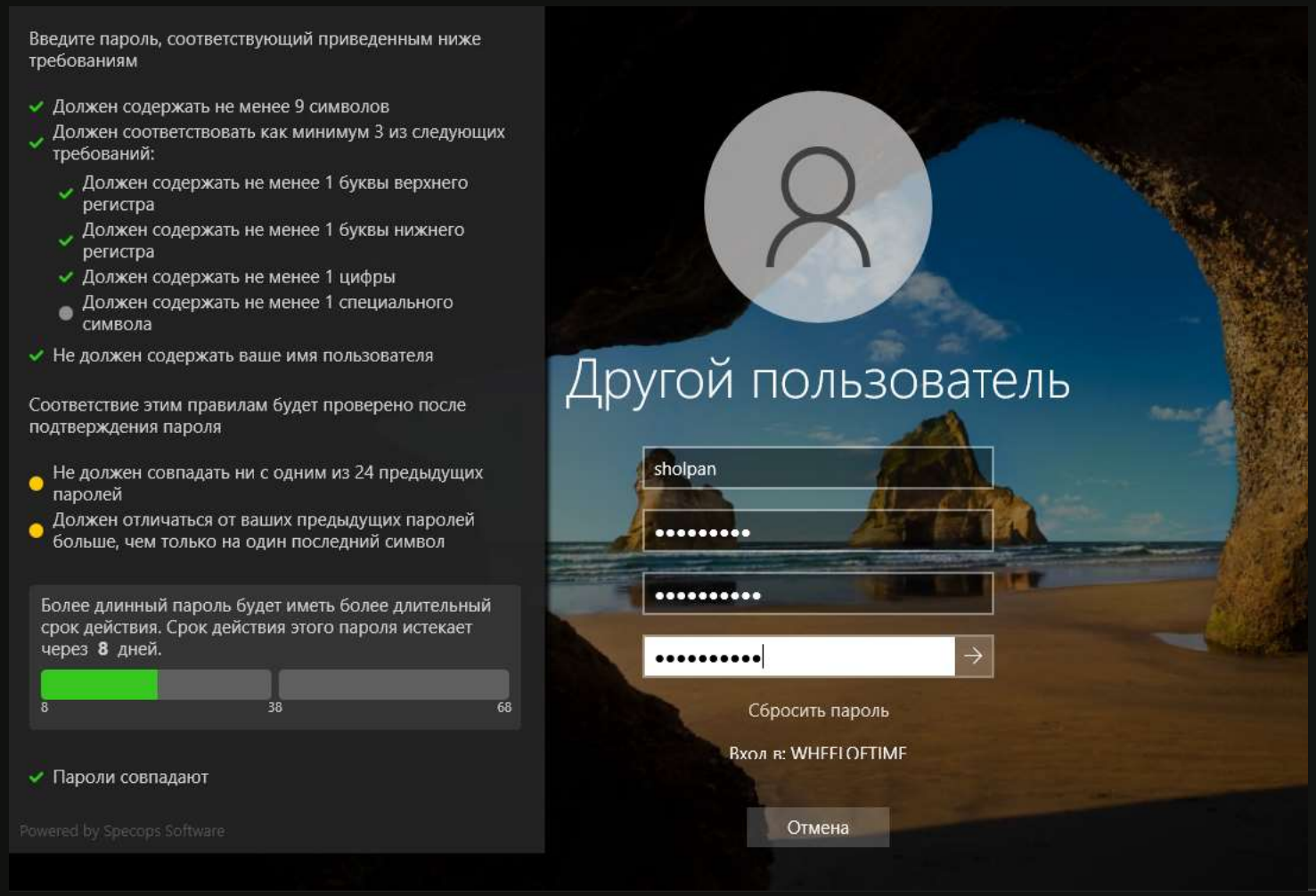
Обзор архитектуры



Политика паролей Specops с защитой от взлома паролей



Вот как работает Windows (без клиента)



Вот как работает Specops (с клиентом)

Пароли нового поколения

- Уже давно существуют "парольные фразы", но с изюминкой.
- Сложные пароли по-прежнему доступны (люди не хотят их менять)
- Когда пароль достаточно длинный, чтобы быть безопасным
  - Устранение требований к сложности
  - Применяйте обычные слова
  - Награждайте пользователей за большее время между изменениями

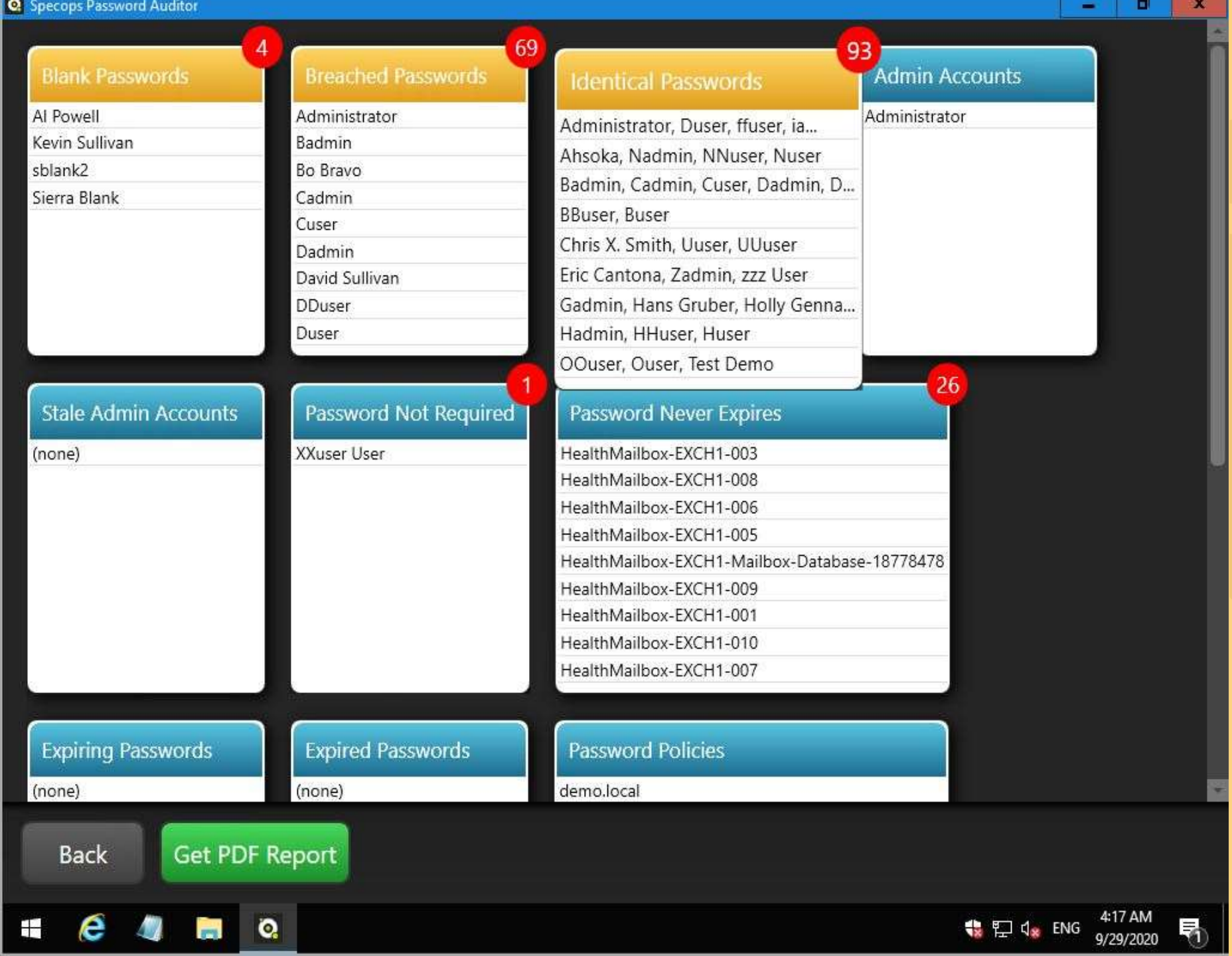
- Всегда блокируйте взломанные пароли

Обучение и поощрение конечных пользователей

Specops Password Auditor

- Бесплатно, но не проактивно
- Hash <> Сравнение хэша с экспресс-списком
- +750 миллионов взломанных паролей
- Необходимо быть администратором домена
- Никто больше не узнает.

Хотите узнать, в безопасности ли вы?



Хотите узнать, в безопасности ли вы?

Лицензирование

- Через GPO - OU, группы безопасности и т. д.
- Отключенные учетные записи игнорируются
- Подписка на 12 месяцев - все включено
- Автоматическое продление без сюрпризов
- Никаких изменений схемы
- Поддержка мирового класса

Подписка на основе пользователя

PoC

- 2-3 часа - установка, настройка и передача знаний
- Большинство клиентов тестируют на производстве - "test-OU".
- В основном нужен 1 сервер
- Рассмотрим DDP, FGPP и политику паролей Specops
- 30-дневный тест - полная поддержка
- Нет покупки - нет затрат

Сложные пароли сложны для людей, но не для компьютеров

Полезные ссылки

- Официальный сайт Specops Software
- Влияние запуска Specops Password Auditor на Active Directory
- Влияние запуска Specops Password Policy на Active Directory
- Specops Breached Password Protection

Specops Software