Что такое PAM?

Контроль привилегированных пользователей или Privileged Access Management (PAM) – это класс решений, предназначенный для осуществления мониторинга и контроля учетных записей сотрудников. Его используют для управления аутентивикацией и авторизацией сотрудников, аудита выполняемых действий, контроля доступа и записи сессий IT-подразделений, системных администраторов, сотрудников аутсорсинговых организаций, занимающихся администрированием инфраструктуры компании.

PAM-системы включают в себя следующие функциии:

— Централизованное управление учетными записями с расширенными возможностями;
— Аудит действий привилегированных сотрудников;
— Управление настройками парольной защиты;
— Контроль доступа сотрудников к административным ресурсам;
— Управление процессом аутентификации и авторизации;
— Запись сессии, запущенной учетной записью из списка привилегированных.

Ключевые клиенты в нашем регионе:

One Identity Safeguard –

простое и удобное в использовании PAM-решение, лидер в категории PAM-решений по оценке аналитического агентства KuppingerCole 2020

Функционал Safeguard

One Identity Safeguard – это мультифункциональная платформа, которая состоит из следующих модулей:

- *Safeguard for Privileged Passwords;*
- *Safeguard for Privileged Sessions;*
- *Safeguard for Privileged Analytics;*
- *Safeguard Authentication Services;*
- *Safeguard for Sudo.*

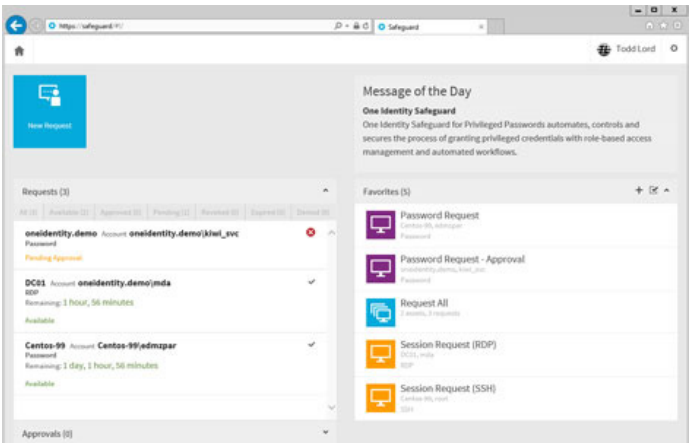
Данная платформа поддерживает все распространённые сетевые устройства, базы данных и операционные системы. Возможно внедрение как on-prem, так и Cloud.

Лидер в

Safeguard for Privileged Passwords

Safeguard for Privileged Passwords автоматизирует, контролирует и защищает процесс предоставления привилегированных учетных данных с помощью управления доступом на основе ролей и автоматизированных рабочих процессов. Решение позволяет управлять паролями из любого места и практически любого устройства. Как результат – полное понимание действий привилегированных сотрудников с их фиксацией и отчетом для дальнейшего анализа. А удобный и понятный интерфейс существенно сокращает время на обучение.

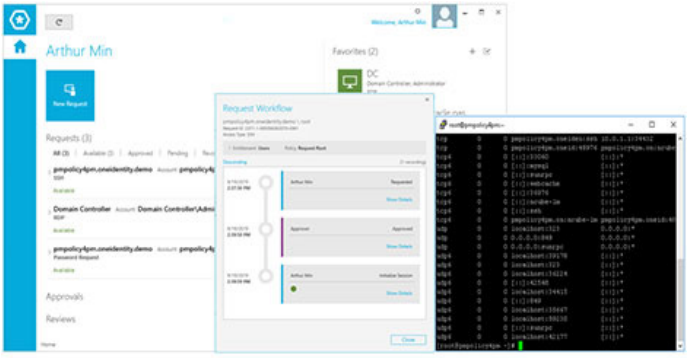
Ключевые преимущества:
— Быстрое обнаружение и подключение ресурсов
— Автоматизация рабочих процессов
— Возможность подтверждать запросы из любого места
— Полноценный REST API
— Бесплатное хранилище личных паролей
для бизнес-пользователей



Safeguard for Privileged Sessions

Safeguard for Privileged Sessions позволяет контролировать, отслеживать и записывать привилегированные сеансы администраторов, удаленных сотрудников и других пользователей с высокими привилегиями в системе. Записанные сеансы могут индексироваться в режиме реального времени, что дает возможность отслеживать аномалии, упрощает поиск и создание отчетов для проверок на соответствие аудиторским требованиям. Также Safeguard for Privileged Sessions выступает в качестве прокси-сервера и проверяет трафик протокола на уровне приложений. Если осуществляются действия, нарушающие политики безопасности – действие может быть автоматически заблокировано. Благодаря этому данный модуль является эффективной защитой от внутренних угроз.

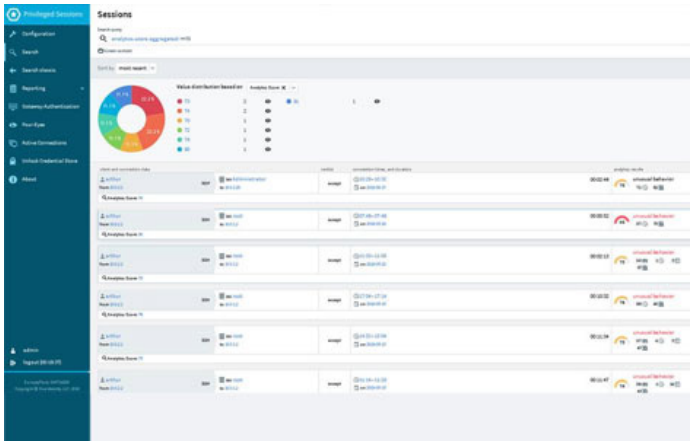
Ключевые преимущества:
— Полный аудит сеанса, запись и воспроизведение
— Оповещение и блокировка в реальном времени
— Запуск рабочих процессов или развертывание решения в прозрачном режиме без изменений для конечных пользователей
— Полнотекстовый поиск, включая оптическое распознавание символов



Safeguard for Privileged Analytics

Safeguard for Privileged Analytics позволяет в режиме реального времени предотвратить нарушения политик безопасности организации. Модуль использует технологию анализа поведения пользователей – он записывает «нормальное» поведение пользователей, ранжирует их на основе риска, и, в случае выявления аномалий, может в режиме реального времени уведомить ответственного администратора о злонамеренных действиях пользователя. Это дает возможность превентивно реагировать на нарушения политик и качественно повысить уровень безопасности компании.

Ключевые преимущества:
— Анализ действий для обнаружения аномального поведения
— Полный анализ сессий, включая содержимое экрана, введенные команды и заголовки окон
— Использует динамику нажатия клавиш и анализ движения мыши, чтобы помочь выявить несанкционированный доступ
— Снижение количества ложных предупреждений за счет классификации предупреждений по уровням риска и отклонения

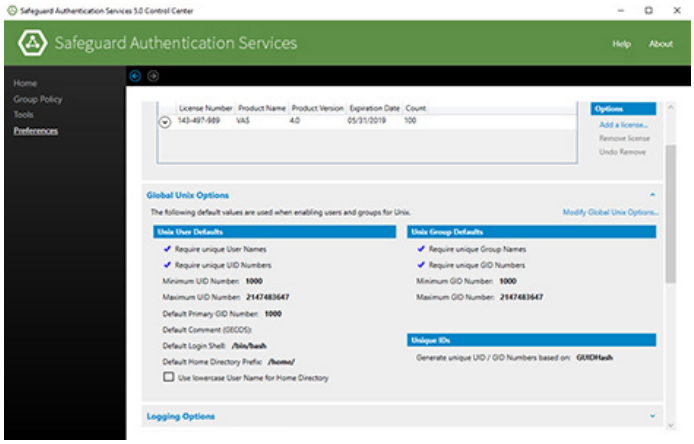


Safeguard Authentication Services

У Safeguard доступна интеграция Unix, Linux и Mac OS X с Active Directory. Он создает мост между Active Directory и не-Windows системами, что позволяет пользователям входить в системы с использованием учетных данных AD. Это дает возможность повысить операционную эффективность и обеспечить соответствие межплатформенному контролю доступа за счет централизованной аутентификации и единому входу.

Ключевые преимущества:

— Объединение локальных и доменных учетных записей с сохранением прав в системе
— Распространение групповых политик на не-Windows системы
— Возможность использовать существующие ресурсы для централизированного управления всей инфраструктурой
— Единый вход для Unix, Linux и Mac

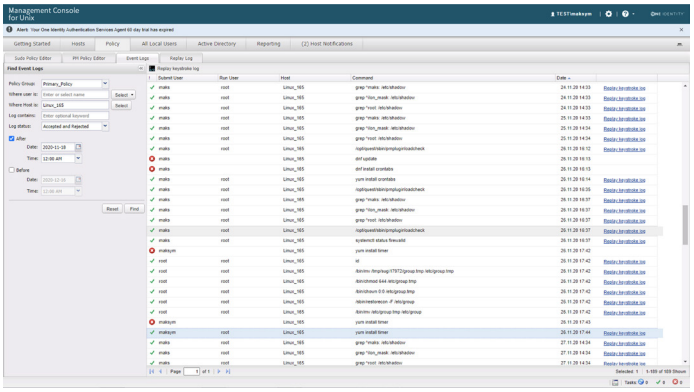


Safeguard for Sudo

One Identity Safeguard для sudo дает возможность централизированно управлять файлами политик sudoer. Благодаря ему можно легко создавать отчеты о правах доступа и действиях sudoer.

Ключевые преимущества:

— Централизованное управление файлом политики sudoers
— Журнал нажатий клавиш для всех действий sudo
— Отчеты о правах доступа и активности для sudo
— Полная видеозапись активности с использованием sudo



Почему заказчики выбирают Safeguard

1. Продвинутый аудит

- Видеофиксация всех действий
- Поиск записей по ключевым словам
- Восстановление переданных файлов

2. Лучшая на рынке производительность

- До 500 конкурентных сессий через апплаенс
- Незаметность для пользователей

3. Простота интеграции и удобство эксплуатации

- Простота внедрения
- Не требует установки агентов
- Прозрачность работы
- Широкий охват протоколов
- Мобильное предложение для согласования доступа

4. Расширенный контроль

- Согласование подключений
- Сокрытие паролей важных аккаунтов
- Контроль передачи файлов
- Принудительная персонификация доступа

5. Анализ данных онлайн

- Онлайн оповещения о подозрительных действиях
- Блокирование команд

Кто покупает PAM в Украине?

1. Банки и финансовые организации (страхование)

1. PAM–один из самых эффективных инструментов снижения рисков кибер-атак.

2. Требование PCI DSS (дополнительный контроль администраторов)

3. Требование Постановления 95 НБУ (Safeguard обеспечивает выполнение 11 пунктов Постановления)

2. Государственные органы и объекты критической инфраструктуры

Требование Постановления КМУ №518

3. Крупные коммерческие заказчики

— РИТЕЙЛ

— ЭНЕРГЕТИКА

— ТЕЛЕКОМ

— ЗДРАВООХРАНЕНИЕ