

FUDO PAM – БЕЗОПАСНАЯ РАБОТА С КРИТИЧЕСКИМИ ИТ-СИСТЕМАМИ

ПРЕИМУЩЕСТВА

ЗАЩИТА ОТ УТЕЧЕК ДАННЫХ В РЕЗУЛЬТАТЕ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Эффективное управление учетными записями пользователей и полный контроль их работы.

ПРЕДОТВРАЩЕНИЕ СЛУЧАЙНОГО ИЛИ УМЫШЛЕННОГО ЗЛОУПОТРЕБЛЕНИЯ ПОЛНОМОЧИЯМИ

Мониторинг всех рабочих сессий с возможностью записи, контроля и анализа действий.

ПРИМЕНЕНИЕ ПРИНЦИПА “ZERO TRUST” ДЛЯ ДОСТУПА К СЕТИ

Fudo PAM позволяет реализовать принцип ZTNA и успешно построить сетевую инфраструктуру с нулевым доверием.

ПРЕДОТВРАЩЕНИЕ ЗЛОУПОТРЕБЛЕНИЯ ПРАВАМИ ДОСТУПА

Предотвращения неправомерных действий при помощи прерывания сессии (до выполнения запрещенной команды).

ЗАЩИТА АДМИНИСТРАТОРОВ ОТ НЕПРАВОМЕРНЫХ ОБВИНЕНИЙ

При помощи записанных сессий администраторы могут доказать отсутствие ошибок и корректность своих действий.

ЗАЩИТА УСТАРЕВШИХ СИСТЕМ

Предотвращение использования известных уязвимостей в ОС и сетевых протоколах.

ШИРОКИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ В КАЧЕСТВЕ ПЛАТФОРМЫ ДЛЯ ОБУЧЕНИЯ

Записанные рабочие сессии с текстовым поиском и метками можно использовать для эффективного обучения и развития администраторов.

СБОР ДОКАЗАТЕЛЬСТВ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ

Запись сессии, сохраненная в сертифицированном формате – неоспоримое доказательство совершенных действий.

ОСНОВНОЙ ФУНКЦИОНАЛ

АВТОМАТИЧЕСКОЕ ОБНАРУЖЕНИЕ С ПЕРЕНОСОМ В КАРАНТИН

В FUDO PAM 5 вы можете сканировать контроллеры домена Active Directory на наличие новых учетных записей. Это позволяет автоматизировать процесс добавления профилей новых пользователей – они сразу перемещаются в список сейфов FUDO или переносятся в карантин на контроллере домена для добавления вручную. Благодаря функции карантина специалисты по безопасности могут не только улучшить контроль за инфраструктурой Active Directory, но и автоматизировать процесс настройки за счет встроенных правил добавления профилей.

ГРАФИЧЕСКАЯ ЗАПИСЬ ВЕБ-СЕССИЙ

Fudo позволяет просматривать в графическом формате текущие сессии работы пользователей в веб-браузерах, взаимодействовать с ними в режиме реального времени, сохранять их в архив и экспортировать их как видеоролики. Контролируйте и записывайте действия пользователей, избегая необходимости трудоемкого анализа log-файлов серверов.

СОВМЕСТНАЯ РАБОТА В РАМКАХ ОДНОЙ СЕССИИ

Функционал совместного использования сессии позволяет второму пользователю присоединиться к сессии для совместной работы, при этом действия каждого пользователя будут отмечаться отдельно. Стороннего пользователя можно пригласить наблюдать или выполнять действия в реальном времени при помощи одноразовой ссылки с ограниченным сроком действия.

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ ПРИ ПОМОЩИ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Fudo PAM позволяет создавать профили привилегированных пользователей на основе непрерывного анализа их действий и создания моделей поведения. Модуль искусственного интеллекта способен с высокой точностью обнаруживать аномалии в действиях пользователей чтобы проактивно реагировать на попытки неправомерного использования чужих учетных записей. Эта функция работает в рамках активных сеансов и обеспечивает реагирование в режиме реального времени с оповещением администратора FUDO. В организациях, где ежеминутно запускаются тысячи сессий, модель машинного обучения позволяет быстро выявить те сессии, которые требуют немедленного внимания.

УПРАВЛЕНИЕ ПАРОЛЯМИ С ВОЗМОЖНОСТЬЮ АВТОМАТИЧЕСКОГО ИЗМЕНЕНИЯ

В состав Fudo PAM входит полноценное решение для управления паролями, включая средства для их регулярного изменения и верификации, а также надежного хранения в зашифрованном виде. Таким образом, вы получаете возможность автоматизированно управлять учетными записями привилегированных пользователей на контролируемых серверах. Средства изменения паролей запускаются на отдельном транспортном уровне, что позволяет запускать встроенные сценарии или добавлять новые. Кроме того, Fudo позволяет создавать и загружать напрямую пользовательские подключаемые модули (plugins).

АВТОМАТИЗИРОВАННЫЙ ВРЕМЕННЫЙ ДОСТУП (JUST-IN-TIME)

Администратор Fudo может легко организовать временный доступ определенных пользователей к определенным ресурсам – как разовый, так и по расписанию. Эффективность работы значительно повышается, поскольку пользователи могут сами запросить временный доступ с помощью интуитивно понятного интерфейса, одобрение доступа со стороны администратора Fudo может быть выполнено как в веб-консоли, так и при помощи специализированного мобильного приложения Fudo Officer.

УДОБНЫЙ ПОЛЬЗОВАТЕЛЬСКИЙ ВЕБ-ПОРТАЛ

Веб-клиент Fudo с поддержкой протоколов RDP и SSH позволяет предоставлять пользователям доступ к ресурсам без привязки к конкретным платформам. В Fudo отсутствуют агенты, это исключает дополнительную нагрузку на критические системы и значительно ускоряет запуск решения. Для начала работы в веб-портале пользователю достаточно запустить браузер, использовать учетную запись Fudo для входа и выбрать одну из доступных сессий для автоматического подключения.

ПОДДЕРЖКА СЛУЖБ КАТАЛОГОВ

Fudo PAM поддерживает службы LDAP и Active Directory для импорта профилей пользователей и проверки их учетных данных.

МЕТКИ В СЕАНСАХ ДЛЯ КОМПЛЕКСНОГО АНАЛИЗА

Функция проставления текстовых меток в определенных местах записи сессий очень удобна для проведения расследований. Использование защищенного формата записи позволяет использовать их как доказательства в суде, также для автоматизации поддерживаются и сторонние службы проставления меток.

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ	ПОДДЕРЖИВАЕМЫЕ СТАНДАРТЫ
<ul style="list-style-type: none"> Графические протоколы: RDP, VNC, X11. Протоколы командной строки: SSH, Telnet, Telnet 3270, Telnet 5250. Протоколы баз данных: MS SQL. Протоколы приложений: HTTP, HTTPS (графический режим через нативный разбор протокола). Стандарт промышленной связи: Modbus. Поддержка IPv6 для будущих имплементаций сред. 	<ul style="list-style-type: none"> Поддержка SSH ProxyJump позволяет настроить промежуточную систему для подключения к целевому серверу. Перенаправление агента SSH для всех типов учетных записей. Позволяет пользователям хранить свои ключи SSH в секрете. Внешние системы аутентификации: Active Directory, Radius, LDAP. Аутентификация через Azure для серверов с визуализацией на базе HTTP (поддерживаются также Asana, Salesforce, LinkedIn, Facebook и Twitter). Многофакторная аутентификация через RADIUS, SMS, DUO и OATH (Google Authenticator). Поддержка VMware Tools.

МАКСИМАЛЬНАЯ ПРОИЗВОДИТЕЛЬНОСТЬ, РАБОТА В УСЛОВИЯХ ВЫСОКОЙ НАГРУЗКИ

Fudo PAM поддерживает кластерную конфигурацию по схеме «active-active», что гарантирует высокую доступность и почти линейное масштабирование производительности. Каждое программно-аппаратное устройство Fudo может обрабатывать несколько сотен параллельных подключений.

БЫСТРОЕ РАЗВЕРТЫВАНИЕ БЕЗ АГЕНТОВ

Fudo PAM — это комплексное решение для любой среды, где требуется максимально надежная защита ресурсов. Отсутствие агентов позволяет развертывать его в сжатые сроки. Решение поставляется в виде виртуального аплаенса, таким образом не требуется ни отдельная установка ОС, ни отдельная настройка хранилища.

ХАРАКТЕРИСТИКИ ПРОГРАМНО-АППАРАТНЫХ КОМПЛЕКСОВ FUDO

Модель	F1002	F3002	F5000
ФОРМФАКТОР	2U	3U	4U
ДОСТУПНЫЙ ОБЪЕМ ХРАНИЛИЩА	15.9 TB	59.9 TB	247 TB
СЕТЕВЫЕ ИНТЕРФЕЙСЫ	4 x 1 Гбит/с, доступны дополнительные платы***	4 x 1 Гбит/с, доступны дополнительные платы***	4 x 1 Гбит/с, доступны дополнительные платы***
ЧИСЛО ПАРАЛЛЕЛЬНЫХ ПОДКЛЮЧЕНИЙ*	До 100	До 200	До 300
ЁМКОСТЬ ХРАНЕНИЯ ЗАПИСЕЙ**	6 месяцев	2 года	7 лет

* При запуске сеансов с 30 % графики (FullHD, 16 бит) и 70 % текста (в среднем).

** Данные указаны, исходя из 50 сеансов в день с 70 % графики (RDP, FullHD, 16 бит) и 30 % SSH (в среднем).

*** Дополнительные платы в устройствах Fudo.