

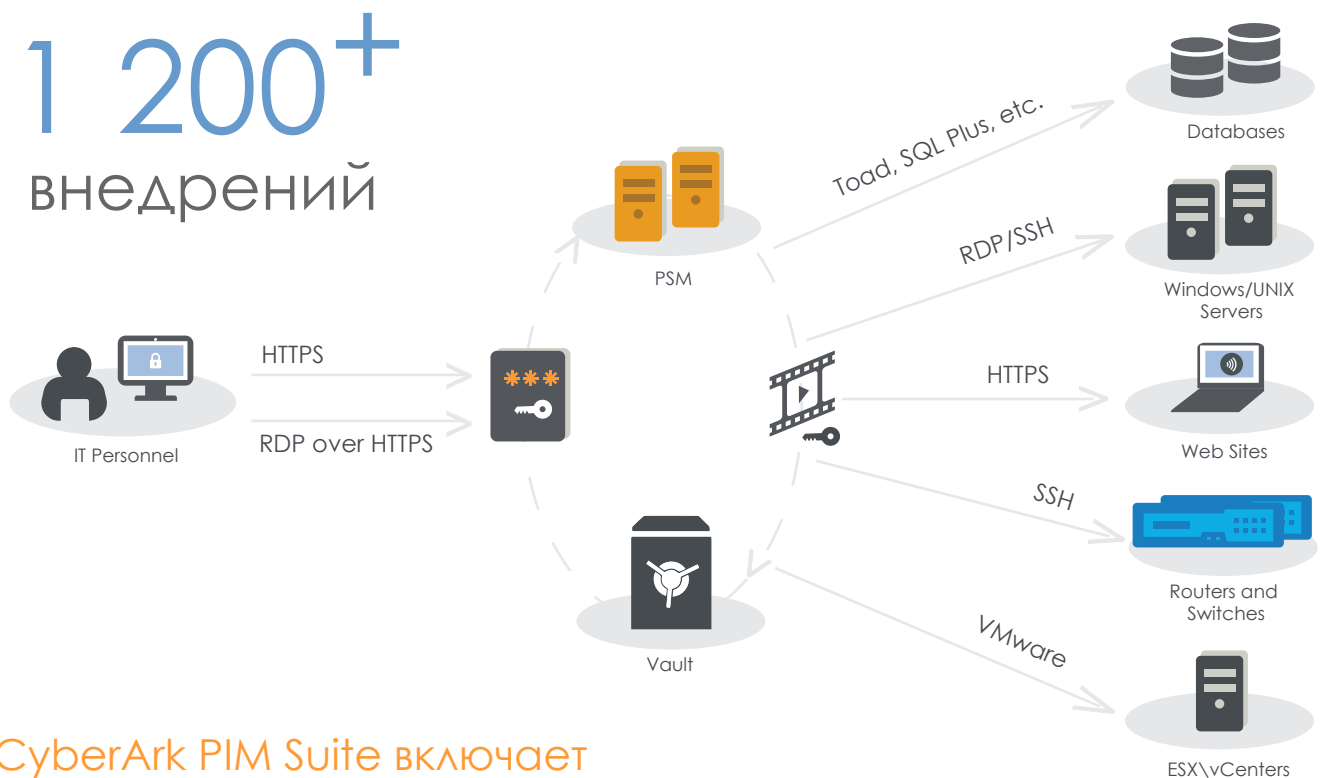
УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ УЧЁТНЫМИ ЗАПИСЯМИ CyberArk Privileged Identity Manager Suite

CyberArk Privileged Identity Manager Suite предназначен для поддержки всего жизненного цикла привилегированных идентификаторов в организации.

Решение обеспечивает контроль, управление и мониторинг всех действий, связанных с разными типами привилегированных учётных записей, и административных паролей, закодированных в приложениях и скриптах.

«Число учётных записей, которыми мы сейчас в состоянии управлять, почти в пять раз превышает количество учётных записей, которое изначально хранилось до внедрения EPV CyberArk в Rabobank International.»

Алекса Глинн, Менеджер по безопасности, Rabobank International



CyberArk PIM Suite включает

Enterprise Password Vault

предоставляет возможность надежно хранить и автоматически менять пароли и логины, а также сохранять полные записи действий с идентификационными данными привилегированных учётных записей. EPV характеризуется высокой масштабируемостью и интегрируемостью с любыми информационными системами

Application Identity Manager

решение для управления логинами и паролями, предназначенными для авторизации в приложениях, скриптах, автоматизирующих работу администрато-

ра, и конфигурационных файлах. AIM обеспечивает защиту информации, позволяя хранить, управлять и проводить аудит действий с чувствительными данными

Privileged Session Manager

позволяет контролировать привилегированный доступ к важным системам и устройствам, обеспечивая мониторинг всех привилегированных сессий, полную видимость всех привилегированных действий и поведения администраторов, а также анализ и оповещения о значимых событиях.

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ УЧЁТНЫМИ ЗАПИСЯМИ

CyberArk Privileged Identity Manager Suite

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

1. безопасная и простая в администрировании замена файловым хранилищам и ftp серверам
2. обеспечение надежного контроля доступа обслуживающих организаций к важным информационным системам и оборудованию
3. обеспечение аудита действий собственных администраторов и снижение угроз, связанных с действиями внутренних злоумышленников
4. минимизация угроз внешних атак, ведущихся с повышением привилегий
5. оптимизация процессов администрирования, повышение производительности труда и ответственности ИТ-персонала
6. соответствие международным регуляциям: SOX, PCI, HIPAA и BASEL II.

Eldorado
FERC
Leroy Merlin
National Gypsum
Rabobank In.
Raiffeisen Bank
Авиакомпания PC1
ВТБ 24
Киевстар
СТО БР РФ

«У нас есть тысячи привилегированных учетных записей, управляемых CyberArk. Мы позаботились, чтобы гарантировать, что люди имеют только тот уровень доступа, который необходим.»

Майк Браннон, Старший менеджер информационных систем, National Gypsum

КОМПОНЕНТЫ PIM SUITE

Компонент	Функционал	Ценность
Vault	Безопасное хранение данных (в том числе привилегированных учетных записей)	Сохранение конфиденциальности данных. Безопасный протокол доступа к данным. Проведение аудита доступа к данным
CPM	Автоматическая смена паролей на конечных системах (серверах, сетевых устройствах, базах данных и т.д.)	Механизм управления политиками безопасности относительно привилегированных учетных записей для всех информационных систем (далеко не все системы могут менять пароли пользователей в автоматическом режиме). Унификация политик
AIM	Запрос пароля у системы CyberArk вместо того чтобы прописывать пароль доступа в явном виде в коде приложения	Учетные данные не хранятся в коде приложения. Простота смены пароля. Сохранение конфиденциальности пароля
PSM	Текстовая и видео запись сессий администраторов	Возможность отслеживать действия администраторов. Возможность расследовать инциденты информационной безопасности. Изолирование рабочего места администратора от конечных информационных систем
On-Demand	Создание белого (черного) списка команд, доступных для выполнения администратором	Реализация принципа минимума полномочий. Администраторам предоставляются минимально необходимые права для выполнения служебных обязанностей. Минимизация количества обращений к сервис-деск