

Race

СОЗДАЙТЕ ПОРЯДОК

РАМ-система для организации и управления доступом
привилегированных пользователей к критическим ИТ-ресурсам

НЕКОНТРОЛИРУЕМЫЕ ПРИВИЛЕГИИ В ИТ-СИСТЕМАХ – ПРИЧИНА КИБЕРАТАК

9 из 10 уязвимостей ИТ-систем связаны с излишними привилегиями

(2018 Microsoft Vulnerabilities Report, BeyondTrust)

РАМ-решения входят в список **топ-10 проектов** кибербезопасности, реализация которых в наибольшей степени снижает риски и оказывает влияние на бизнес.

(Gartner Top 10 Security Projects for 2019)

Причиной **80%** кибератак являются скомпрометированные привилегированные учетные данные

(2018 Forester Wave: Privileged Identity Management)

В 2019 году в России на **40%** выросло количество атак, направленных на получение контроля над инфраструктурой

(2020 Отчет Solar JSOC Security Report)

В России **61,5%** утечек по вине привилегированных пользователей являются умышленными.

(2018 Forester Wave: Privileged Identity Management)

РАСШИРЕНИЕ ИТ-ИНФРАСТРУКТУРЫ КОМПАНИЙ ПРИВОДИТ К УВЕЛИЧЕНИЮ КОЛИЧЕСТВА ЦЕЛЕЙ ДЛЯ КИБЕРАТАК

On-Premises

- Административные Учетные Записи
- Desktops (Windows, Mac)
- Серверы (Unix, Linux, Windows)
- Промышленные Системы Управления
- Безопасность и Сетевая инфраструктура
- Приложения и Базы Данных
- Учетные данные машин (App to App)
- Гипервизоры и Виртуальные машины

Cloud & Hybrid Cloud

- Облачные Платформы Управления (AWS, Azure)
- Виртуальная среда (VMWare, MSFT)
- Виртуальные Машины (Unix, Linux, Windows)
- SaaS-Приложения (Facebook, LinkedIn, Custom)

Internet of Things

- Роуминг Рабочих Станций
- BYOD
- Видеокамеры
- Аппаратура наблюдения
- Принтеры
- Любое устройство со встроенным подключением к интернету

Dev Ops

- DevOps & SecDevOps Tools
- Dynamic Virtual окружение
- Containers
- Microservers

ИСПОЛЬЗОВАНИЕ ТРАДИЦИОННЫХ МЕТОДОВ УПРАВЛЕНИЯ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ НЕ СНИЖАЕТ РИСК КИБЕРАТАК

ТРАДИЦИОННЫЕ МЕТОДЫ

- Учетные данные известны пользователям. Отсутствуют механизмы эффективной организации доступа и автоматического управления паролями
- Неконтролируемый или полный доступ к ИТ-системам. Доступ не ограничивается только целевыми системами
- Отсутствует контроль за соблюдением требований регуляторов в отношении безопасного использования привилегий
- Отсутствует единая отчетность и прозрачность использования привилегий

НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ

- Финансовые и репутационные потери от неработоспособности ИТ-систем, потери данных или нарушения их целостности
- Утечки привилегированных учетных данных приводящие к инцидентам
- Штрафы регуляторов или высокие затраты по исправлению ситуации
- Высокие внутренние издержки на организацию и обеспечение привилегированного доступа

Использование PAM систем (Privilege Access Management) позволит минимизировать риски, предоставить защиту от угроз и обеспечить безопасный доступ к критическим ИТ-ресурсам компании

sPACE PAM

УДОБНЫЙ ИНСТРУМЕНТ
УПРАВЛЕНИЯ
ПРИВИЛЕГИРОВАННЫМ
ДОСТУПОМ

sPACE - функциональная PAM система
компании Web Control (Россия),
позволяющая компаниям:

- обеспечить удобный и безопасный доступ пользователей к критическим ИТ-системам
- организовать эффективную работу привилегированных пользователей
- защитить компании от финансовых и репутационных потерь из-за компрометации привилегированных учетных данных

sPACE RAM

ОСНОВНЫЕ ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ

Полный контроль над паролями доступа к критическим ИТ-ресурсам компании, невозможность утраты и компрометации паролей

- Пользователи не знают пароли доступа к критическим ИТ-системам
- Пароли хранятся в защищенном хранилище внутри системы и автоматически подставляются при подключении
- Ротация паролей происходит автоматически

Защита критических ИТ-ресурсов в процессе доступа пользователей

- Доступ гранулирован до целевой системы, нецелевые ресурсы недоступны во время сеанса
- Сеанс доступа к целевой системе осуществляется в Защищенной среде, непроницаемой для вредоносного ПО

Контроль сессий и фиксация действий пользователей, помощь в поиске причин инцидентов и восстановлении работоспособности ИТ-систем

- Все действия пользователя записываются и доступны в любое время для аудита действий и расследования причин инцидентов
- Все сеансы отображаются в Журнале сеансов

sPACE PAM

ВОЗМОЖНОСТИ СИСТЕМЫ

- Обеспечение доступа к критическим ИТ системам
- Управление персонализированными и разделяемыми привилегированными учетными записями
- Гибкий механизм назначения ролей и повышения привилегий
- Реализация принципа «наименьших привилегий»
- Контроль сессий и фиксация действий пользователей
- Обеспечение безопасности сеансов привилегированного доступа
- Простота и удобство использования
- Интеграция с другими решениями информационной безопасности

sPACE RAM

ВОЗМОЖНОСТИ СИСТЕМЫ

Обеспечение доступа к критическим ИТ системам.

Управление персонализированными и разделяемыми привилегированными учетными записями

- ✓ Доступ сотрудников и внешних подрядчиков к критическим ИТ-системам
- ✓ Исключение компрометации привилегированных учетных данных
- ✓ Ограничение ущерба в случае ошибочных или неправомерных действий пользователей при администрировании критических ИТ-систем
- ✓ Соблюдение требований регулятора по персонификации разделяемых учетных данных

- Доступ гранулируется до уровня конкретной целевой системы или приложения
- Доступ предоставляется на определенное время для выполнения конкретной задачи
- Пароли доступа к критическим ИТ-системам неизвестны пользователям
- Учетные данные хранятся в защищенном хранилище и подставляются системой автоматически
- Обеспечивается автоматическая реализация полного жизненного цикла паролей (назначение, хранение, ротация, отзыв)
- После завершения сеанса проводится автоматическая ротация паролей доступа
- Разделяемые учетные данные на время сеанса привязываются к четной записи пользователя

sPACE RAM

ВОЗМОЖНОСТИ СИСТЕМЫ

Гибкий механизм назначения ролей и повышения привилегий.

Реализация принципа «наименьших привилегий»

- ✓ Соблюдение политик информационной безопасности компании
- ✓ Повышение производительности пользователей благодаря возможности оперативного изменения уровня привилегий
- ✓ Устранение избыточных привилегий

- Доступ строго персонифицирован, ограничен целевой системой и решаемой задачей.
- Механизм согласования нарядов-допусков позволяет обеспечить необходимый набор пользовательских ролей и наделить их необходимыми привилегиями
- Изменение уровня привилегий осуществляется по мере необходимости в рамках согласования новых нарядов-допусков
- В случае необходимости уровень привилегий может быть оперативно изменен

sPACE RAM

ВОЗМОЖНОСТИ СИСТЕМЫ

Контроль сессий и фиксация действий пользователей

Обеспечение безопасности сеансов привилегированного доступа

- ✓ Прозрачность действий пользователей
- ✓ Записи сессий пользователей для расследования инцидентов, аудита действий и обучения сотрудников
- ✓ Защиту от вредоносного ПО при подключении рабочих станций пользователей
- ✓ Ограничение ущерба, возможность быстрого восстановления работоспособности системы и доступности данных

- Сеансы запускаются в защищенной среде, что позволяет обеспечить безопасное и контролируемое подключение
- Действия пользователей фиксируются, система автоматически ведет журнал сеансов
- Просмотр действий пользователей для расследования инцидентов, аудита и обучения сотрудников
- Ограничение ущерба и быстрое восстановление системы в случае ошибочных или неправомерных действий пользователей при работе с критическими ИТ-ресурсами

sPACE RAM

ВОЗМОЖНОСТИ СИСТЕМЫ

Простота и удобство использования

Интеграция с другими решениями информационной безопасности

Возможность кастомизации системы

- ✓ Простота использования системы, быстрое внедрение и отсутствие затрат на обучение пользователей
- ✓ Доступ к критическим ИТ-ресурсам компании через единую точку доступа
- ✓ Поддержка множества приложений (в тч. legacy-систем), единая платформа для интеграции имеющихся ИБ решений
- ✓ Повышение производительности и оптимизацию процесса предоставления доступа, снижение запросов в службу поддержки

- Система имеет интуитивно понятный веб-интерфейс, а для использования системы не требуется обучение и специальная подготовка
- Пользователи самостоятельно оформляют и направляют запросы на подключение к целевым системам
- Привилегированные учетные данные хранятся в системе и подставляются автоматически при запуске сеансов
- Система поддерживает множество инструментов управления объектами ИТ-инфраструктуры, позволяет интегрировать имеющиеся ИБ системы и работать в привычном окружении
- Система позволяет интегрировать любые целевые системы и приложения

Задачи для sPACE:

Целевая аудитория:

- ✓ Руководители бизнеса
- ✓ ИТ руководители и ИТ администраторы
- ✓ Руководители ИБ

Крупные компании

- Обеспечение безопасного доступа сотрудников и внешних подрядчиков к критическим ИТ-системам, контроль и фиксация действий пользователей
- Устранение угрозы утраты привилегированных учетных данных и снижение риска кибератак
- Минимизация ущерба от остановки ИТ-систем и потери данных, быстрое восстановление работоспособности
- Использование sPACE как единой платформы для интеграции имеющихся у компании решений ИБ (IDM, Inventory, SIEM, Session Recording, UEBA и т.д.), расширение возможностей используемых систем (в частности IDM-систем для управления доступом привилегированных пользователей)
- Минимизация затрат на внедрение и масштабирование системы
- Соблюдение требований регуляторов по обеспечению персонифицированного доступа и контроля персональных данных

Задачи для sPACE:

Целевая аудитория:

- ✓ Владельцы компаний
- ✓ Руководители бизнеса
- ✓ ИТ руководители

Компании МСБ

- Простота использования, для работы в системе не требуется обучение и специальная подготовка
- Быстрое и эффективное обеспечение контроля доступа к ИТ-ресурсам компании (например, в собственной или поглощаемой компании)
- Контроль и фиксация действий пользователей в ИТ-системах
- Быстрое восстановление работоспособности ИТ-ресурсов, минимизация ущерба от остановки систем и потери данных
- Устранение угрозы утраты паролей доступа к критическим ИТ-ресурсам, снижение риска кибератак и потери данных
- Обеспечение удаленного доступа к ИТ-системам сотрудников и внешних подрядчиков

sPACE RAM

НАШИ ПРЕИМУЩЕСТВА

- Оптимальное соотношение цены и функциональных возможностей: вы платите за то, чем реально будете пользоваться
- Быстрое внедрение и интеграция с ИТ-системами заказчика
- Высокая степень кастомизации, гибкий подход к использованию имеющихся у заказчиков систем ИБ
- Удобство и простота использования: эксплуатация системы не требует специальных знаний
- Нетребовательность к ИТ-ресурсам, минимизация затрат на масштабирование
- Российская разработка
- Техническая поддержка 24x7

Опыт компании Web Control

12 лет на рынке информационной безопасности

- Дистрибьютор решений Web и ИТ безопасности
- Профессиональная команда экспертов

100 + проектных внедрений

- Авторизованный вендорский сервисный и тренинговый центр



Контактная информация

www.s-PACE.ru

e-mail: info@s-pace.ru

www.web-control.ru

e-mail: info@web-control.ru

+7 (495) 925 77 94