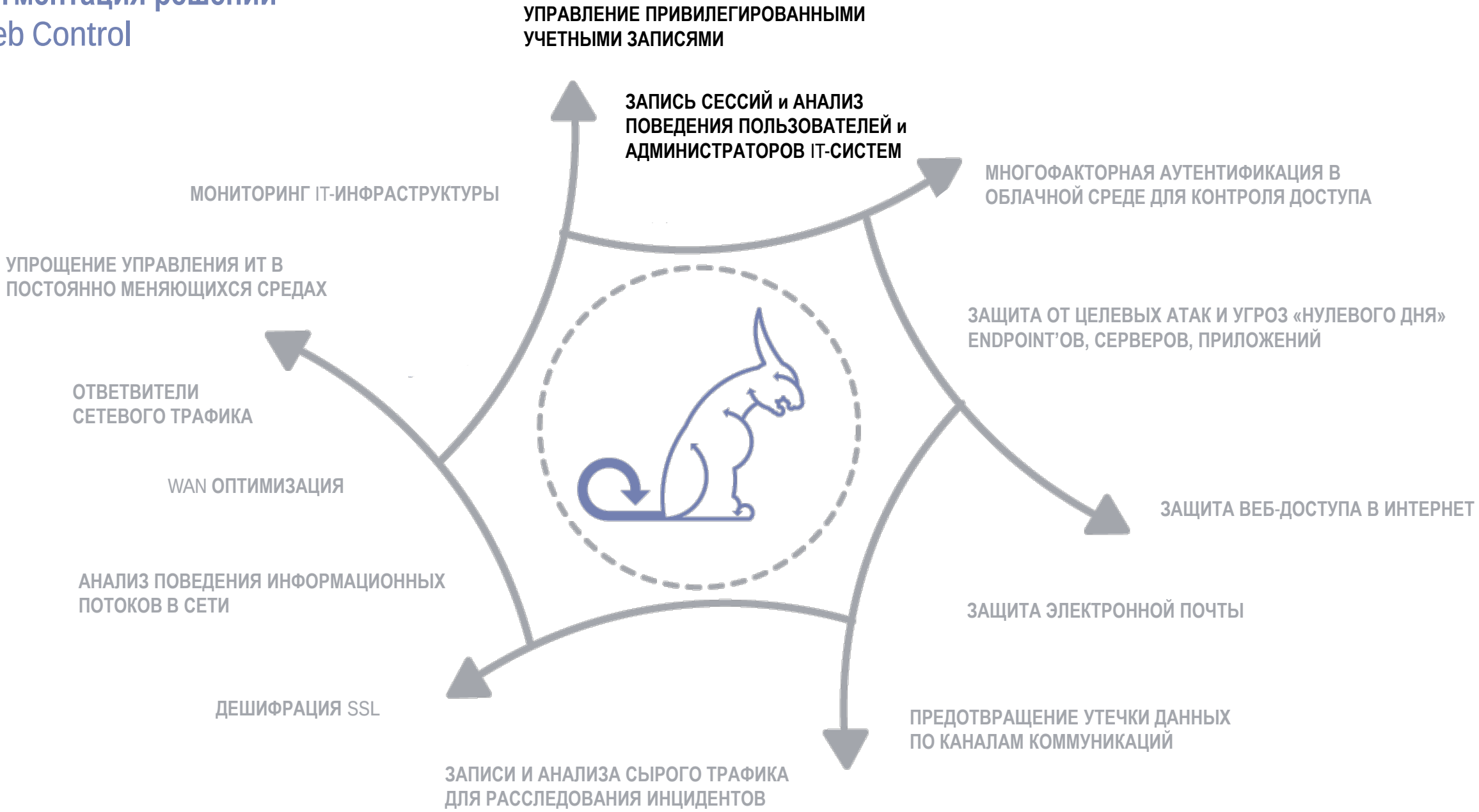
Сегментация решений
Web Control



Решение от Компании Web Control - CWPAM

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ УЧЕТНЫМИ ЗАПИСЯМИ

http://web-control.ru/

Система создана для комплексной организации бизнес-процесса администрирования IT-систем:

- Организован процесс согласования и предоставления допуска для удаленного подключения к IT-системам;
- Защищенная среда администрирования позволяет проводить работы с любыми IT системами;
- Есть возможность автоматической смены паролей и ключей, в том числе технологических;
- Администраторам не требуется знать пароли от систем;
- Мониторинг использования привилегированных учетных записей и вводимых команд на серверах в режиме онлайн и в ретроспективе;
- Обнаружение аномального поведения администраторов систем.

Администраторы систем должны получать необходимый уровень привилегий именно тогда, когда это требуется. Это снижает возможности реализации рисков ИТ/ИБ, связанных с администрированием. Перманентная роль администратора системы является мишенью для киберпреступников. CWPAM позволяет согласовывать и получать необходимые права администраторам IT-систем на заданный период времени, а также автоматически менять пароли и ключи для надежного контроля доступа к этим системам.

Как правило, непростой задачей является выяснить, кто конкретно под общей учетной записью администратора выполнил какие-то действия. Расследование может занимать много времени и быть весьма трудоемким. В таких случаях требуется изучать множество различных журналов и сопоставлять из них данные. Не все системы с нужной детализацией фиксируют действия администраторов, особенно, если работа выполняется из-под графических оснасток. CWPAM содержит исчерпывающую информацию о подключениях, что позволяет централизовано идентифицировать, кто и какие работы выполнял. Например, кто из штатных администраторов или аутсорсеров удалил каталог с сервера, внес изменения в базу данных, изменил правила на файерволле, кто отредактировал системные журналы и автоматический запуск задач в операционной системе.

Наличие инструментов контроля сессий удаленного администрирования и использования привилегированных учетных записей позволяет повысить качество проводимых работ и снизить количество инцидентов ИБ в ходе удаленных подключений. Если инцидент в ходе удаленной сессии все же произошел, то CWPAM поможет установить, кто из штатных сотрудников или аутсорсеров проводил работы в ИТ-системе.

В CWPAM разработаны расширенные функции сопровождения процесса администрирования IT-систем:

- Согласование доступа к IT-системам на определенный период времени;
- Прекращение доступа администратора при различных условиях;
- Изменение паролей и ключей;
- Обнаружение подозрительного поведения администратора при управлении системами;
- Детальная фиксация действий администраторов.

Таким образом, CWPAM является помощником при выстраивании взаимодействия с подрядчиками и аутсорсерами.

Привилегированные учетные записи используются не только людьми. **Бизнес-приложения и компьютерные службы** также должны хранить и использовать привилегированные учетные данные для подключения к базам данных, вспомогательному ПО и другим приложениям. Смена этих так называемых технологических паролей и ключей вызывают особые сложности у администраторов, так как необходимо учитывать все точки использования технологической УЗ и взаимодействие сервисов, где она используется. CWPAM устраняет этот пробел в безопасности и решает задачу по смене технологических паролей и ключей.

Решение от Lieberman Software - Rapid Enterprise Defense (RED)

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ УЧЕТНЫМИ ЗАПИСЯМИ

https://liebsoft.com/red-identity-management/

RED обнаруживает и фиксирует расположение привилегированных учетных записей – локальные и доменные учетные записи, настроенные службы, запланированные задачи, приложения, включая COM + и DCOM, веб-сайты IIS, базы данных и т.д. Затем **распространяет изменения паролей/ключей во всех точках использования**, на которые ссылается каждая учетная запись, чтобы предотвратить блокировки и сбои в обслуживании из-за устаревших данных учетных записей (функция pooled account rotation).

RED позволяет управлять привилегированными учетными данными, включая:

- **учетными записями СуперПользователей**, правомочные изменять параметры конфигурации, запускать программы и выполнять другие административные обязанности;
- **учетные записи служб**, требующие привилегированный доступ;
- доступ **приложений к приложениям** - учетные записи, используемые веб-службами, бизнес-приложениями, программным обеспечением и многим другим типам приложений для подключения к базам данных и вспомогательного ПО;
- **SSH ключи,** используемые для проверки подлинности отдельных лиц и приложений на системах UNIX-подобных системах.

Конечно, сразу возникает вопрос: что произойдет, если RED на части систем сменит пароль, а на одной или нескольких не сможет сменить? Останутся ли на разных системах разные пароли от одной и той же учетной записи?

Функция **pooled account rotation** при невозможности сменить пароль/ключ на одной из систем, где эта учетная запись используется, откатывает изменения, возвращая старые пароли, и оставляя их неизменными, пока возможность смены паролей для всех систем пула не будет восстановлена.
Администраторы ERPM имеют возможность настраивать пулы учетных записей, содержащие любое количество учетных записей.

Основные возможности RED:

- непрерывное автоматическое обнаружение компьютеров, сетевых устройств, баз данных, учётных записей процессов, локальных учётных записей и учётных записей для аварийного восстановления, служб и задач, а также регистрации каждого местоположения, где задействована конкретная учётная запись;
- создание паролей случайным образом для привилегированных учётных записей согласно установленным пользователем правилам и распространения новых паролей повсюду, где задействована соответствующая учётная запись, во избежание нарушения функционирования ИТ-инфраструктуры и блокировки учётных записей;
- хранение сложных, случайным образом составленных паролей в зашифрованном виде в базе данных Oracle или SQL Server ;
- предоставление пользователям паролей согласно заданным ролям и делегирование прав через защищённый веб-портал;
- аудит и отчётность по каждому факту запроса пароля, его раскрытия и изменения;
- высокая надежность и масштабируемость решения;
- возможность использования на предприятиях с разнородным парком оборудования и ПО;
- простота внедрения и интеграции (есть опыт внедрения в масштабах десятков тысяч контролируемых объектов инфраструктуры)

Привилегированные учетные записи используются не только людьми. **Бизнес-приложения и компьютерные службы** также должны хранить и использовать привилегированные учетные данные для подключения к базам данных, вспомогательного ПО и другим приложениям.

Решение от ObserveIT – ObserveIT Insider Threat Management

ЗАПИСЬ СЕССИЙ и АНАЛИЗ ПОВЕДЕНИЯ АДМИНИСТРАТОРОВ IT-СИСТЕМ

https://www.observeit.com/insider-threat-solution

ObserveIT - это легкое Endpoint-решение (агенты устанавливаются на контролируемые системы), фокусируется на выявлении и устранении внутренних угроз со стороны привилегированных пользователей. Постоянно отслеживая поведение пользователей, ObserveIT предупреждает службы ИТ и ИБ о деятельности, которая подвергает Компанию риску. Когда обнаруживается аномальное поведение, уведомления на экране информируют пользователей или рекомендуют альтернативные действия, которые являются безопасными и соответствуют политике Компании.

1. Отслеживание поведения пользователей и предупреждения в режиме реального времени с помощью экранных уведомлений в тот момент, когда они выполняют действия, которые ставят под угрозу бизнес. Уведомления в реальном времени более чем на 50% уменьшают число, связанных как с неумышленным, так и злонамеренным поведением.

2. Производится видеозапись, дополненная журналами активности пользователей для любого приложения, в том числе и тех, которые не имеют внутренних журналов или имеют только журналы отладки, в том числе: самописные, заказные или устаревшие приложения. Благодаря полной видимости всех действий пользователя в приложениях, ObserveIT способен мгновенно и точно обнаружить поведение, выходящее за рамки политик.

3. Оптимизация и эргономические свойства решения ObserveIT позволяют скорейшим оптимальным образом расследовать инциденты ИБ, связанные с проведением работ администраторами IT-систем.

Релиз ObserveIT версии 7.0

➢ Профиль активности пользователя теперь позволяет: исследовать производительность штатных или удаленных сотрудников – динамически фильтровать расход времени по приложениям и устройствам

➢ Предупреждения кей логгера помогают: обнаруживать и оповещать о вводимых ключевых словах и командах, о попытках вывода информации, идентифицировать и предупреждать о Unix командах, запускаемых из Mac Terminal

➢ Превентивные действия могут: принуждать пользователей к отключению (разлогиниванию), закрывать приложения или веб-сайты, связанные с несанкционированной деятельностью, собирать объяснительные от пользователей

➢ Библиотека инсайдерских угроз (ITL), усиленная менеджером контента и выпущенная в виде ZIP-архива для клиентов, клиенты могут получать и устанавливать регулярные обновления библиотеки без необходимости обновления ПО ObserveIT, офицеры ИБ постоянно и своевременно информируются о новых сценариях внутренних угроз, новые сценарии внутренних угроз из коробки

➢ Новые и улучшенные отчеты: новые возможности создания отчетов на базе посещения веб-сайтов, печати документов, подключениях запоминающих устройств USB, копирования файлов, установки и удаления приложений и т. д.

➢ Удаление данных из базы данных архива теперь может выполнять пользователь, являющийся членом Active Directory

Лицензирование

Наименование	Краткое описание	Самая свежая информация о решении	Принцип лицензирования
Решение от Компании Web Control - CWPAM	Управление привилегированными учетными записями	http://web-control.ru/	По пользователям
Решение от Lieberman Software – Rapid Enterprise Defense (RED)	Управление привилегированными учетными записями	https://liebsoft.com/red-systems-management/pricing-and-licensing/	По управляемым устройствам
Решение от ObserveIT – ObserveIT Insider Threat Management	Запись сессий и анализ поведения администраторов it-систем	https://www.observeit.com/insider-threat-detection	По управляемым устройствам