One Identity Safeguard

Безопасность при массовом переходе на удаленный доступ

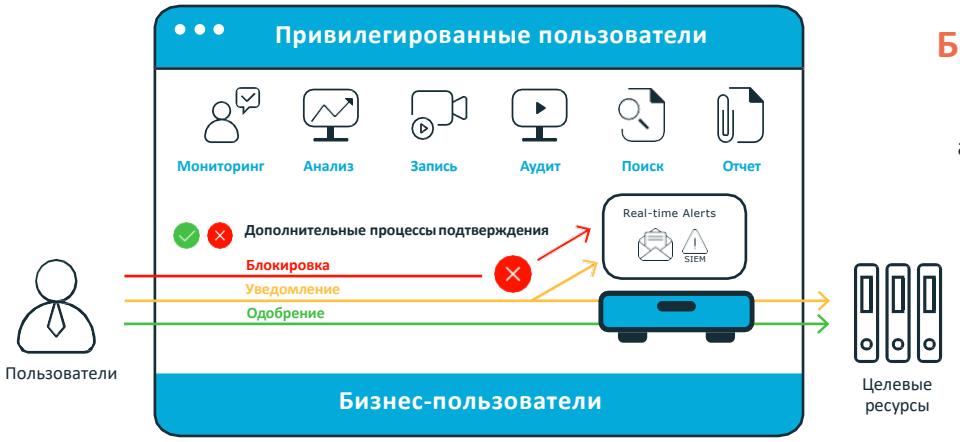
Safeguard for Privileged Sessions

- Распознавание всех данных в сессии (OCR)
- Выявление аномального поведения пользователей в режиме реального времени
- Блокировка возможности копирования информации через буфер обмена, подключенные диски, принтеры и т.д.
- Поддерживаемые протоколы: Citrix ICA (в т.ч. SOCKS proxy, Citrix STA), RDP (в т.ч. over TLS), Remote Desktop Services (RemoteApp), VNC (в т.ч. over SSL), SSH, Telnet, TN3270, SFTP (SCP), HTTP, HTTPS, MS SQL
- Не требует изменения архитектуры сети
- Работает без агентов
- Интеллектуальная система хранения сессий для экономии ресурсов

Предоставление администраторам удаленного доступа к IT-инфраструктуре является стандартом для многих компаний. Для снижения рисков при этом используют корпоративные ноутбуки, соответствующие всем требованиям информационной безопасности, а также применяют дополнительные меры защиты: многофакторную аутентификацию, шифрование каналов связи и прочие.

Но далеко не все компании готовы обеспечить аналогичные возможности доступа для бизнес-пользователей. Многие сотрудники работают со стационарных компьютеров, а имеющаяся инфраструктура удаленного доступа не рассчитана на стремительный рост количества пользователей, так как изначально создавалась для доступа администраторов и подрядчиков, выполняющих работы по обслуживанию IT-инфраструктуры.

В связи со срочной необходимостью массового перевода большого количества сотрудников на удаленную работу компании запускают дополнительные терминальные серверы, через которые обеспечивается возможность удаленной работы сотрудников. Это приводит к возникновению новых рисков, многие из которых можно минимизировать при использовании решений для контроля привилегированного доступа.



Безопасный удаленный доступ

One Identity Safeguard обеспечит запись и анализ сессий привилегированных и бизнес-пользователей, повысит ответственность сотрудников за производимые действия и упростит работу администраторов, специалистов ИБ и аудиторов.

Быстрое внедрение и простая эксплуатация помогают оперативно снизить риски при запуске удаленного доступа

Возможности продукта

Safeguard for Privileged Sessions

Safeguard for Privileged Sessions позволяет контролировать, отслеживать и записывать сессии администраторов, подрядчиков и других пользователей, представляющих высокий уровень риска.

Вся активность в рамках сессии (вплоть до нажатия клавиш, движений мыши и просмотра окон) записывается, индексируется и сохраняется в защищенных от несанкционированного доступа журналах аудита.

Сессии можно просматривать как видео-ролики и искать по любому слову, которое появлялось на экране пользователя.

Safeguard for Privileged Sessions помогает контролировать действия пользователей и блокировать команды, подвергающие опасности инфраструктуру компании.

Safeguard for Privileged Analytics

Safeguard for Privileged Analytics позволяет выявлять аномалии в поведении пользователей (UBA), находить и пресекать ранее неизвестные типы угроз.

Алгоритмы продукта умеют выявлять отклонения от базовой линии поведения конкретного пользователя: динамику нажатия клавиш и анализ движения мыши, время и место начала сессии, продолжительность сеанса. Эти и другие параметры служат для непрерывной биометрической аутентификации пользователей и помогают выявлять инциденты безопасности.

Доступ привилегированных пользователей

Одним из наиболее востребованных сценариев использования продукта является мониторинг действий привилегированных пользователей (т.е. использующих учетные записей с административными привилегиями):

- Внешние подрядчики
- Внутренние администраторы

Эти пользователи и раньше имели возможность удаленного доступа, но в период массового перевода сотрудников на удаленный режим работы количество подобных сессий резко увеличивается.

Решение для мониторинга увеличившейся активности этих пользователей должно позволять масштабироваться и оставаться таким же удобным на выросшем количестве обрабатываемой информации.

Доступ бизнес-пользователей

Причиной повышенного интереса к мониторингу действий бизнес-пользователей послужил массовый перевод сотрудников на удаленный режим работы. Многие компании, не имея возможности обеспечить всех сотрудников ноутбуками, предоставили доступ с домашних компьютеров сотрудников через терминальные серверы.

При таком сценарии возникают дополнительные риски как со стороны внешних, так и внутренних злоумышленников:

- Неконтролируемое перемещение информации за пределы инфраструктуры компании (через буферы обмена, подключенные диски и т.д.)
- Перехват учетных данных пользователей (как техническими средствами на слабо защищенных домашних компьютерах, так и с использованием методов социальной инженерии)
- Получение удаленного доступа злоумышленников к инфраструктуре компании

Сценарии использования

Повышение ответственности пользователей

- Пользователи понимают, что их действия контролируются и не производят неправомерных действий
- Учетные данные не передаются третьим лицам, чтобы не отвечать за операции, совершенных другими пользователями

Разбор инцидентов

- Ускорение расследований инцидентов: возможность поиска по ключевым словам (как по командам, так и по любым словам в графических сессиях), отчеты по интересующим командам
- Выгрузка сессий для передачи третьим лицам на анализ
- Централизованное расследование в рамках всей инфраструктуры

Дополнительный эшелон защиты

- Запрет выполнения потенциально опасных команд
- Ограничения по возможности использования каналов RDP-сессий (буфер обмена, диски, принтеры и прочее)
- Режим «4 глаза» для особо критичных систем
- Требования по обязательному пересмотру (валидации) сессии после ее завершения

Выявление аномального поведения пользователей

- Обнаружение сессии, в которых внутренние злоумышленники производят опасные действия
- Выявление сессий внешних злоумышленников, перехвативших учетные данные сотрудников компании

Получите информацию по продукту One Identity Safeguard со специальным предложением в вашем регионе:

Беларусь:

Алексей Кочнев
Territory Manager
M: +375 29 653 2841
Alexei.Kochnev@bakotech.com

Украина и другие регионы:

Игорь Смолянкин
Business Unit Manager
M: +380 67 447 8738
Igor.Smolyankin@bakotech.com

bako tech®

О БАКОТЕК

БАКОТЕК® – международная группа компаний, которая занимает лидирующие позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value Added IT-дистрибьютор, БАКОТЕК предоставляет профессиональную до- и пост-продажную, маркетинговую, техническую поддержку для партнеров и конечных заказчиков. Территориально группа компаний работает в 26 странах на рынках Центральной и Восточной Европы, Балкан, Балтии, Кавказа, Центральной Азии с офисами в Праге, Кракове, Риге, Минске, Киеве, Баку и Нур-Султане.

Группа компаний БАКОТЕК – официальный дистрибьютор One Identity в Украине, Беларуси, странах Балтии, Средней и Центральной Азии. За дополнительной информацией по решениям One Identity, пожалуйста, обращайтесь по тел. +38 044 273 3333 или пишите на **oneidentity@bakotech.com**, а также ищите на сайте **www.bakotech.com**