АЙТИБАСТИОН

СКДПУ НТ

Комплексное решение контроля и мониторинга действий пользователей с привилегиями

1 Контроль доступа
Доступ к ИТ системам на основе IP-адреса, группы пользователя, интервала времени, протокола

2 Мониторинг действий
Аудит действий в гипервизорах, серверах Windows/Linux, базах данных и сетевых устройствах

3 Запись сессий
Запись RDP и VNC сессий в видеоформате, командной строки в текстовом формате

4 Управление паролями
Изменение паролей для административного доступа, защищенное хранилище

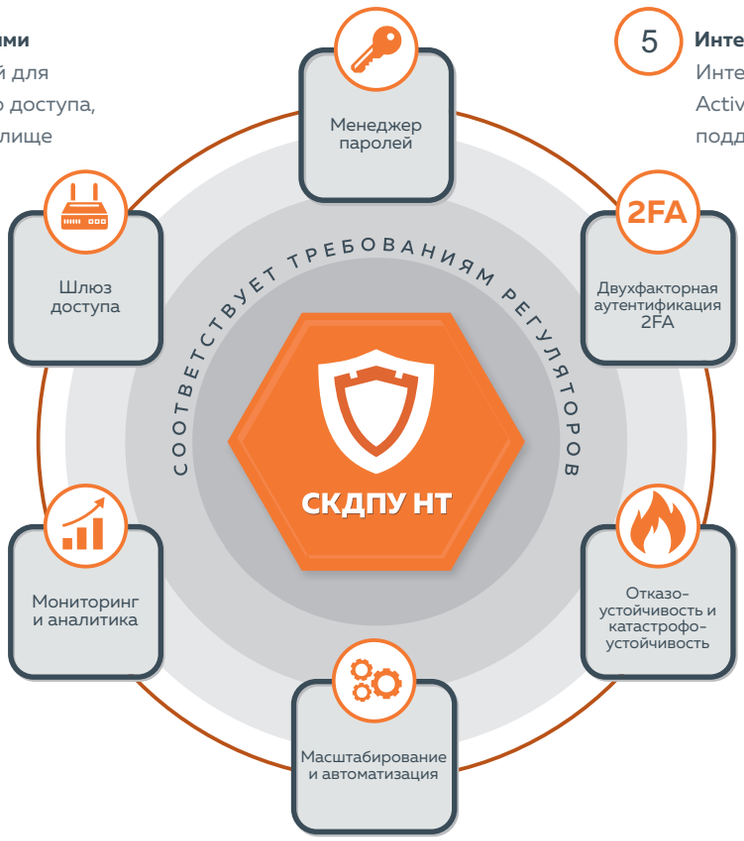
5 Интеграция
Интеграция с Radius, LDAP, Active Directory, Kerberos, поддержка сертификатов X.509

6 Статистика и отчёты
Журналы подключений, статистика подключений, действия пользователей

7 Единая точка входа
Доступ к разрешенным устройствам без повторного введения пароля (SSO)

8 Онлайн контроль
Уведомления о подключениях, неудачных и успешных попытках входа в СКДПУ и ИТ системы

9 Работа без агентов
СКДПУ не требует установки агентов на контролируемых устройствах



Единый центр мониторинга и аналитики:

- Контроль и мониторинг действий в реальном времени;
- Выявление аномалий в действиях пользователей;
- Автоматическое выявление инцидентов;
- Библиотека настраиваемых отчетов;
- Централизованный поиск по распределенной инфраструктуре шлюзов.

Взаимодействие с внешними системами

- SIEM • СОВ • Многофакторная авторизация
- Однонаправленные шлюзы
- Оркестраторы и автоматизация

Список систем постоянно пополняется, расширяя функциональные возможности всех решений в ИТ-инфраструктуре

24/7

Одна из лучших техподдержек на рынке, по мнению наших заказчиков

СКДПУ НТ и территориально распределенная ИТ-инфраструктура
(нефтяная и газовая промышленность, логистика, объекты КИИ и др.)

Инфраструктура заказчика:

Филиалы организации распределены по стране. Каждый филиал – независимый объект, к которому требуется доступ. Единый центр осуществляет контроль и мониторинг работы филиалов.

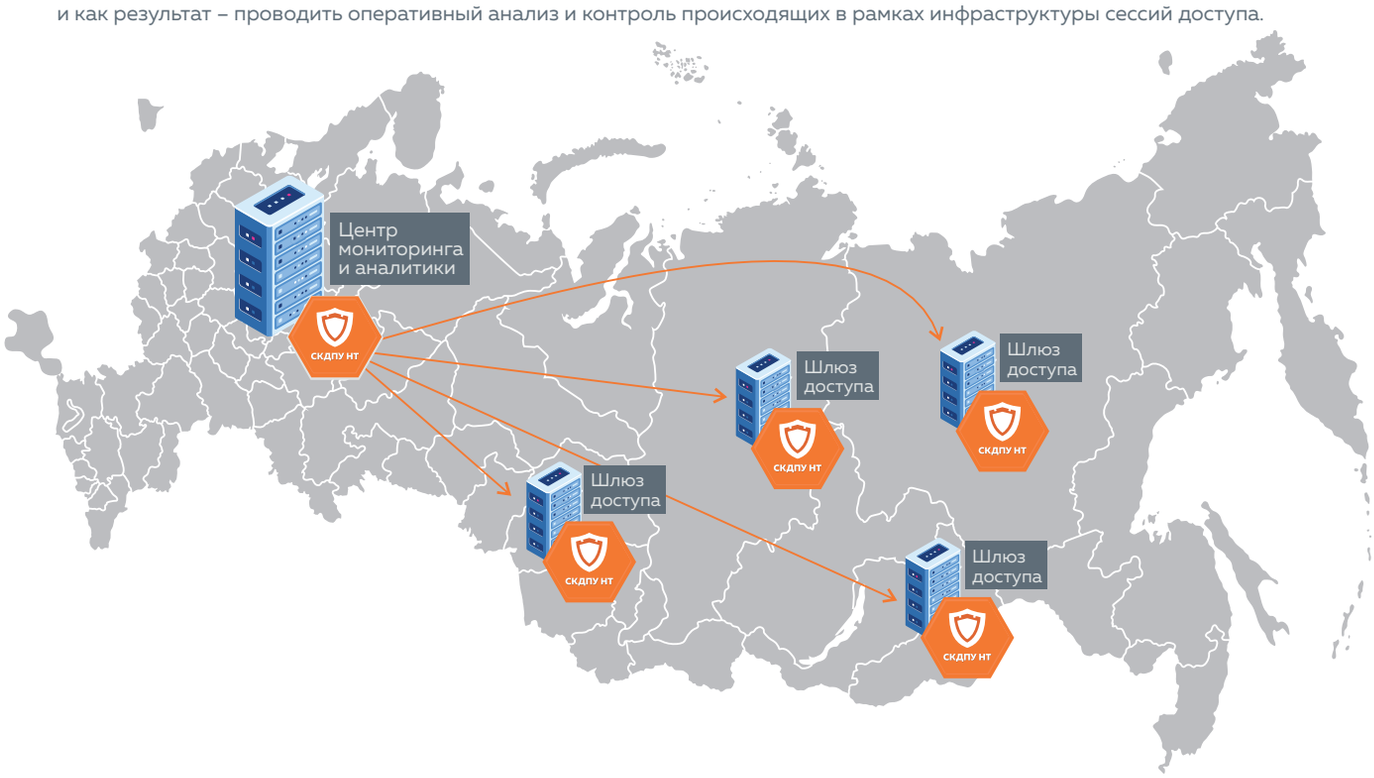
Задача:

Контролировать действия внешних подрядчиков и собственных сотрудников во время их работы на ИТ-инфраструктуре, организовать независимые точки доступа к каждому филиалу; дать возможность резервного доступа через резервный канал и точку входа; обеспечить единую точку мониторинга всех точек доступа; иметь базу всех действий в рамках всех точек доступа для быстрого расследования потенциальных инцидентов; повысить качество расследования и мониторинга без увеличения штата сотрудников; снизить риск утечек информации, в т.ч. персональных данных; обеспечить бесперебойную и надёжную работу внешних и внутренних специалистов.

Решение:

Использовано комплексное решение компании «АйТи Бастион» СКДПУ НТ.

Доступ специалистов в инфраструктуру обеспечивается через независимую точку доступа СКДПУ НТ Шлюз доступа. Доступ получают как внутренние специалисты, находящиеся на объекте, так и внешние специалисты – по шифрованному каналу в рамках политик безопасности. Для контроля всей распределенной инсталляции используется продукт СКДПУ НТ Центр мониторинга и аналитики, он позволяет объединить информацию со всех точек доступа в единую анализируемую базу данных и как результат – проводить оперативный анализ и контроль происходящих в рамках инфраструктуры сессий доступа.



СКДПУ НТ и виртуальные рабочие столы VDI
(банки, корпоративные сети, дата-центры)

Инфраструктура заказчика:

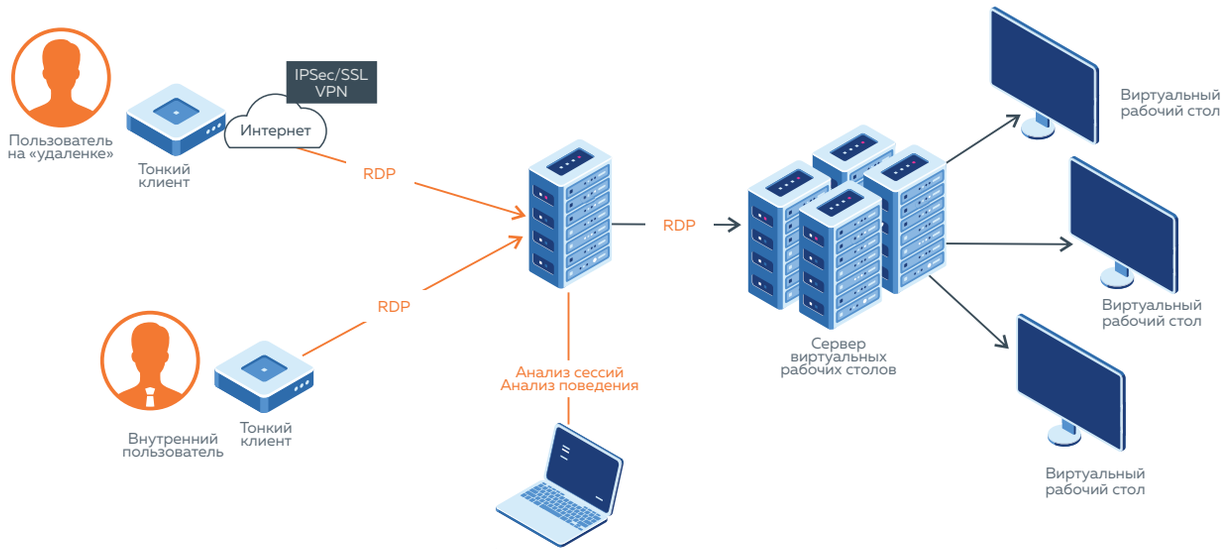
Доступ сотрудников осуществляется в рамках виртуальных рабочих столов, к которым они подключаются с помощью «тонких клиентов».

Задача:

Контроль подключений всех участников – рядовых пользователей, подключающихся к VDI, администраторов и техподдержки сервера. При этом необходимо сохранить текущую архитектуру решения, не снижая качество предоставляемого сервиса; снизить риски утечки данных; снизить риски выхода систем VDI из строя по вине персонала и предоставить инструмент для расследования инцидентов; обеспечить дополнительный сбор информации сессий доступа (видео и текстовые данные); организовать систему контроля активности и времени работы сотрудников в рамках виртуальных рабочих столов.

Решение:

Применение средств контроля доступа СКДПУ НТ. Решение обеспечивает подключение к ресурсам VDI по привычной схеме работы, накапливает информацию о действиях пользователей и проводит дополнительную их обработку в рамках разрешенных подключений, исключая несанкционированные. Доступ осуществляется средствами SSH или RDP протоколов через шлюз доступа СКДПУ НТ (схема).



СКДПУ НТ и легковесные шлюзы с единой точкой СКДПУ Компакт

(банкоматы, заправки и т.п.)

Инфраструктура заказчика:

Сеть устройств или небольшая ИТ-инфраструктура (банкоматы, АЗС и т.п.) без единой точки доступа и с разным качеством связи; отсутствие полно-ценного журналирования сессий удаленного доступа, сложность определения и расследования инцидентов.

Задача:

Организация безопасного удалённого доступа для администраторов сети и устройств, журналирование действий удаленных и локальных администраторов на всех важных устройствах сети.

Решение:

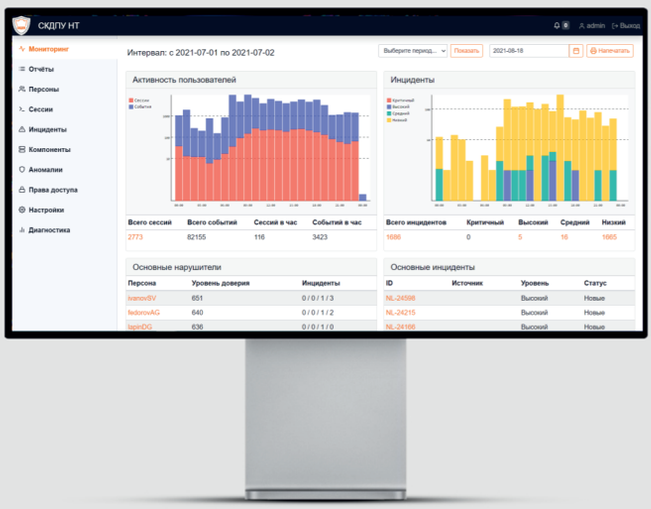
Каждый объект (банкомат, АЗС, магазин и т.п.) оборудован легковесным шлюзом доступа СКДПУ Компакт, таким образом организован безопасный удаленный доступ для администрирования и конфигурации оборудования. Создан централизован-ный архив событий действий в рамках инфраструктуры на основе СКДПУ НТ Центр мониторинга и аналитики, а так же организован анализ поведения действий пользователей для раннего оповещения о потенциальных инцидентах.

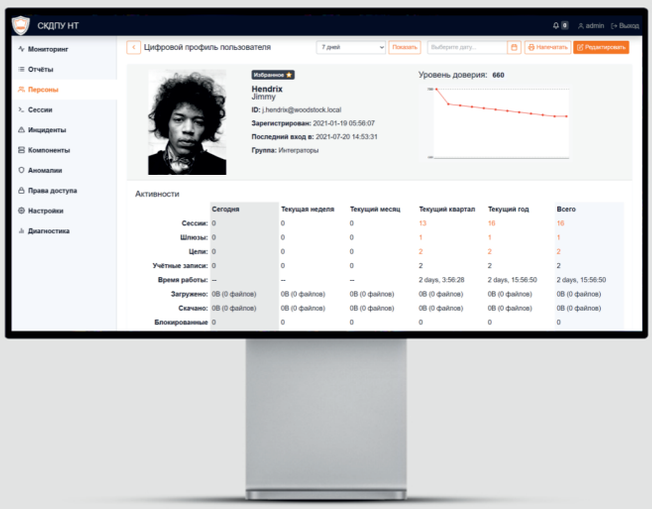
...и ещё более 10 сценариев и кейсов позволяют реализовать:

- Сбор и поведенческий анализ событий в рамках сессий (видео сессии, запуск процессов, буфер обмена, клавиатурный ввод и др.);
- Доступ по согласованию;
- Удобный веб-интерфейс для расследования потенциальных инцидентов;
- Доступ вне разрешенного времени только по согласованию;
- Доступ до критических систем обеспечения ИБ в прозрачном режиме без передачи доступов (пароль скрыт от исходного пользователя);
- Уведомления о потенциальных инцидентах.

В современных реалиях развития ИТ и ИБ структур наметилось несколько явных трендов и зависимостей от них.

Растёт число удалённых подключений и, соответственно, растёт количество инцидентов. При этом число ИБ-специалистов остаётся прежним, а это снижает скорость реагирования на инциденты.



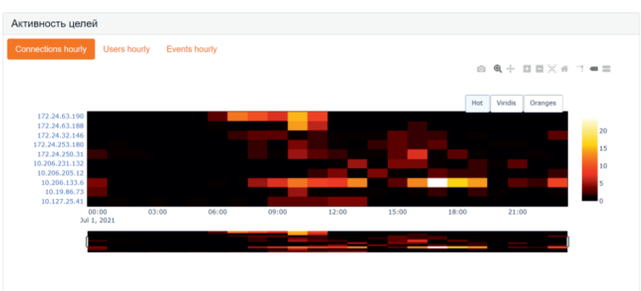


В таких условиях надежная и эффективная система должна обеспечивать качественную обработку поступающих событий и проводить необходимый предварительный анализ, чтобы сделать работу специалистов эффективной и качественной.

Оперативный доступ ко всей информации

Одной из базовых задач системы является предоставление полной информации по пользовательским сессиям и удобного инструментария для его анализа.

Анализ событий по «тепловым картам»



Анализ активности пользователей и работа с инцидентами на основе «тепловых карт» для большой наглядности в работе с информацией

Профилирование каждого администратора

На основе собранной информации и событий из сессий производится построение поведенческой модели пользователей и определяется уровень доверия системы к каждому конкретному пользователю.

Поведенческий анализ и детектирование инцидентов

СКДПУ НТ обрабатывает входящие данные и сохраняет обнаруженные показатели в наборе профилей для лиц, целей и инцидентов.

Настраиваемые политики

Гибкая настройка правил доступов и настройка аналитики по детекторам аномалий, а также системы отчетности позволяет адаптировать СКДПУ НТ к любой инфраструктуре и модели использования.

Отчетность и аналитика

Расширенные функции модуля отчетности позволяют формировать отчеты различной сложности и детализации, позволяя не только создавать настраиваемые отчеты и сохранять их для использования в будущем, а также планировать их запуск в определенное время.
Отчеты могут быть сформированы для различных подразделений: Отчёты для менеджмента, Отчёты для службы ИБ, Отчеты для службы ИТ

ООО «АйТи БАСТИОН» | 119501, Россия, Москва, ул. Староволынская, 15, к. 1. | E-mail: info@it-bastion.com Тел.+7 (499) 322 36 67 | Больше информации на сайте: www.it-bastion.com