ЗАЩИТА ДАННЫХ

СОХРАНИТЬ ВСЁ

Privileged Account Management

неотъемлемый технологический инструмент при реализации концепции Zero Trust

Андрей Акинин,
генеральный директор
Вэб Контрол

Что такое Zero Trust?

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Zero Trust (Концепция нулевого доверия) представляет собой набор концепций, предназначенных для минимизации неопределенности при обеспечении точных решений о доступе с наименьшими привилегиями для каждого запроса в информационных системах и службах в условиях сети, которая рассматривается как оспариваемая.

Что? Набор концепций.
Зачем? Снижение неопределенности доступа.
Когда? В условиях недоверенной сети (то есть теперь всегда!).

Zero Trust предполагает отсутствие доверия к пользователям, активному оборудованию и ресурсам, основанного на их физическом или сетевом расположении (в офисе, локальной сети, корпоративном дата-центре), принадлежности активов (корпоративный или личный), способу подключения (физическое, локальное или корпоративный vpn).

Основная цель Zero Trust – обеспечение киберустойчивости предприятия в условиях «неминуемой» компрометации ИТ-инфраструктуры.

Как защитить ресурсы?

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Firewall

- Разделение сети и создание ресурсных сегментов.

Шлюз доступа (VPN)

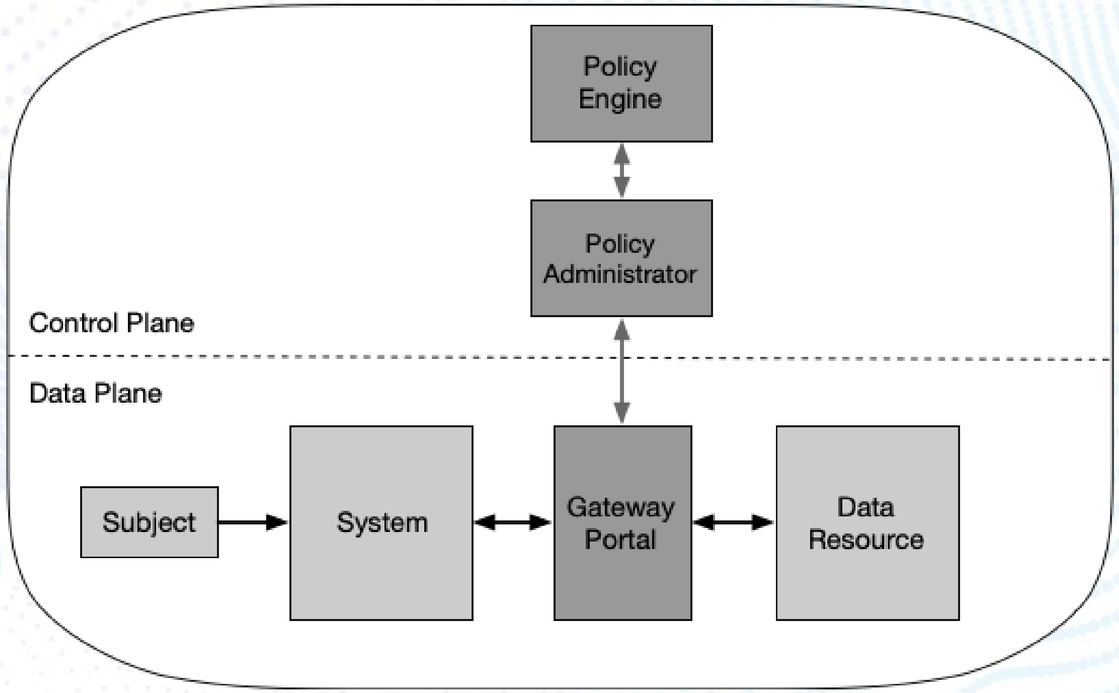
- Строгая авторизация пользователя.
- Организация защищенного канала доступа.

Терминальный сервер

- Создание среды исполнения.

Запись сеансов

- Мониторинг сеанса и запись действий.
- Реагирование на неправомерные действия.
- Расследование инцидентов.



Контроль ресурсных сегментов

Основные постулаты Zero Trust

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Идентификация в сети:

- Динамическая аутентификация и авторизация всех ресурсов строго выполняется перед разрешением доступа.

Управление конечными точками:

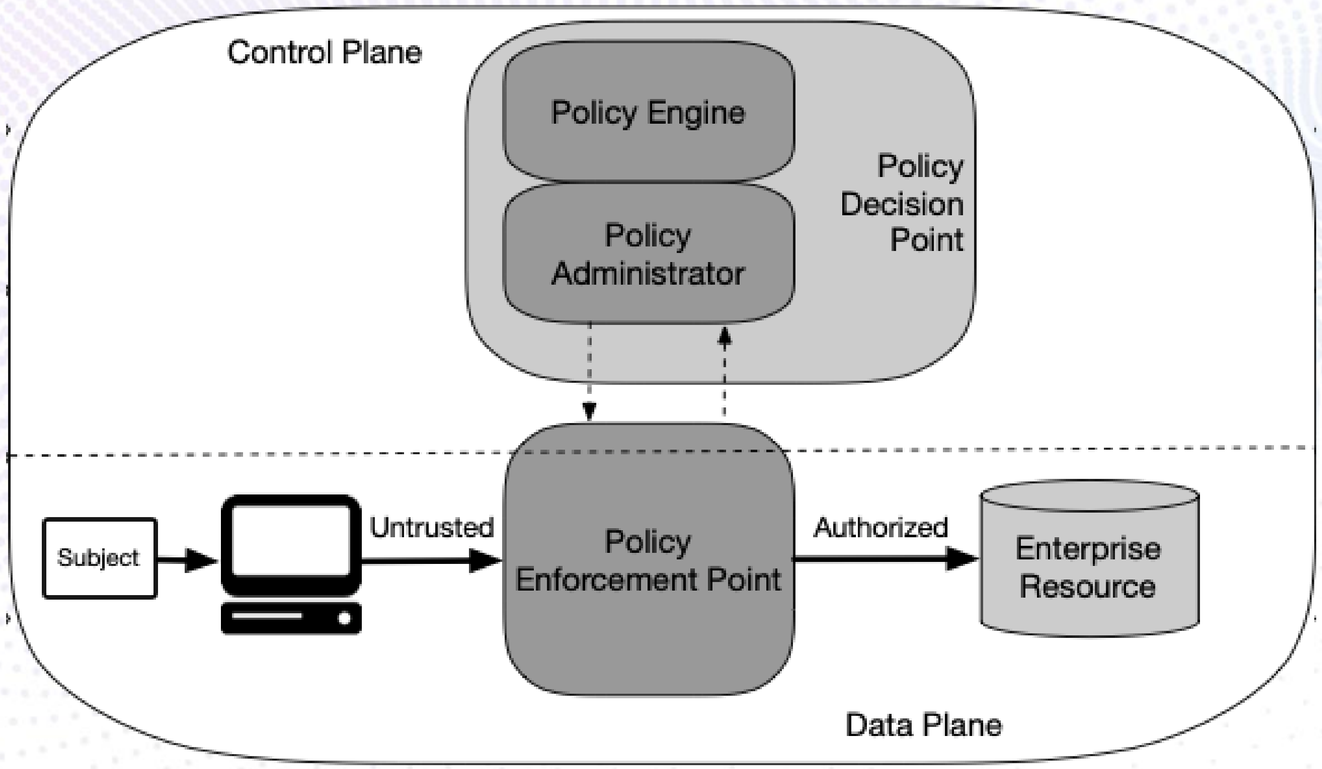
- Все источники данных и вычислительные сервисы считаются ресурсами.
- Предприятие контролирует и измеряет целостность и уровень безопасности всех принадлежащих ему и связанных с ним ресурсов.

Управление потоками данных:

- Ни одна сеть не считается доверенной. Все соединения защищены независимо от расположения сети.
- Точечный доступ с минимальными привилегиями. Контроль каждого сеанса, в идеале каждой операции.
- Непрерывный аудит доступа. Доступ к ресурсам определяется динамическими правилами.
- Сбор максимального числа данных о состоянии системы и ее компонентов, динамическое реагирование.

Ключевой элемент архитектуры

Нулевое доверие предполагает, что ни одно сетевое подключение, ни один ресурс не может считаться доверенным только на основе нахождения в периметре компании.
Для доступа к ресурсу необходима авторизация и наделение правами непосредственно перед установкой сеанса (Just-in-Time).



Подсистема обработки политик

Принимает решение о предоставлении, запрете или отмене доступа конкретного пользователя или актива в случае межмашинного взаимодействия к ресурсу.

Подсистема администрирования политик

Подтверждает сеанс доступа по решению подсистемы обработки политик.

Точка применения политик

Обеспечивает наделение правами в момент организации сеанса доступа к корпоративным ресурсам.

Контроль ресурсного сегмента

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Firewall

- Сегментация и создание ресурсных анклавов.

Шлюз доступа (VPN)

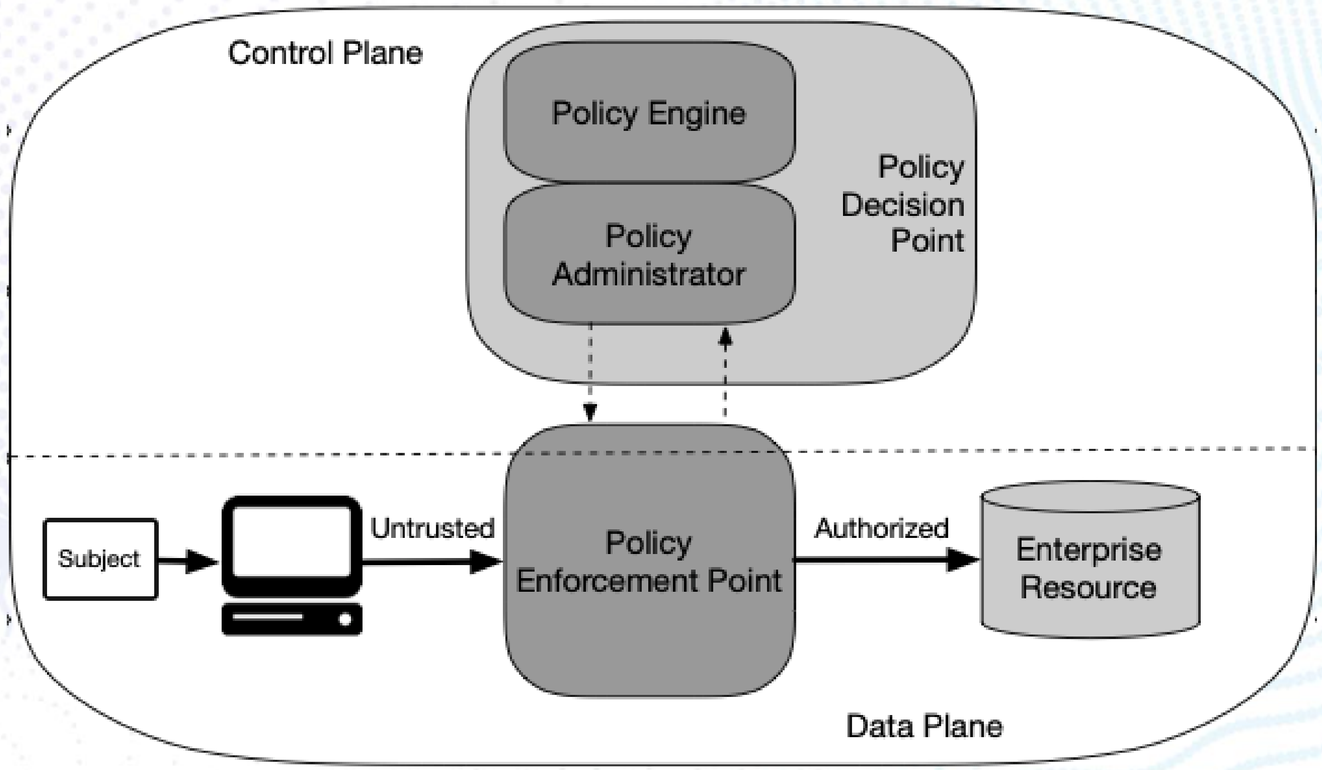
- Строгая авторизация пользователя.
- Организация защищенного канала доступа.

Терминальный сервер

- Создание среды исполнения.

Запись сеансов

- Мониторинг сеанса и запись действий.
- Реагирование на неправомерные действия.
- Расследование инцидентов.



Что может быть этой точкой?

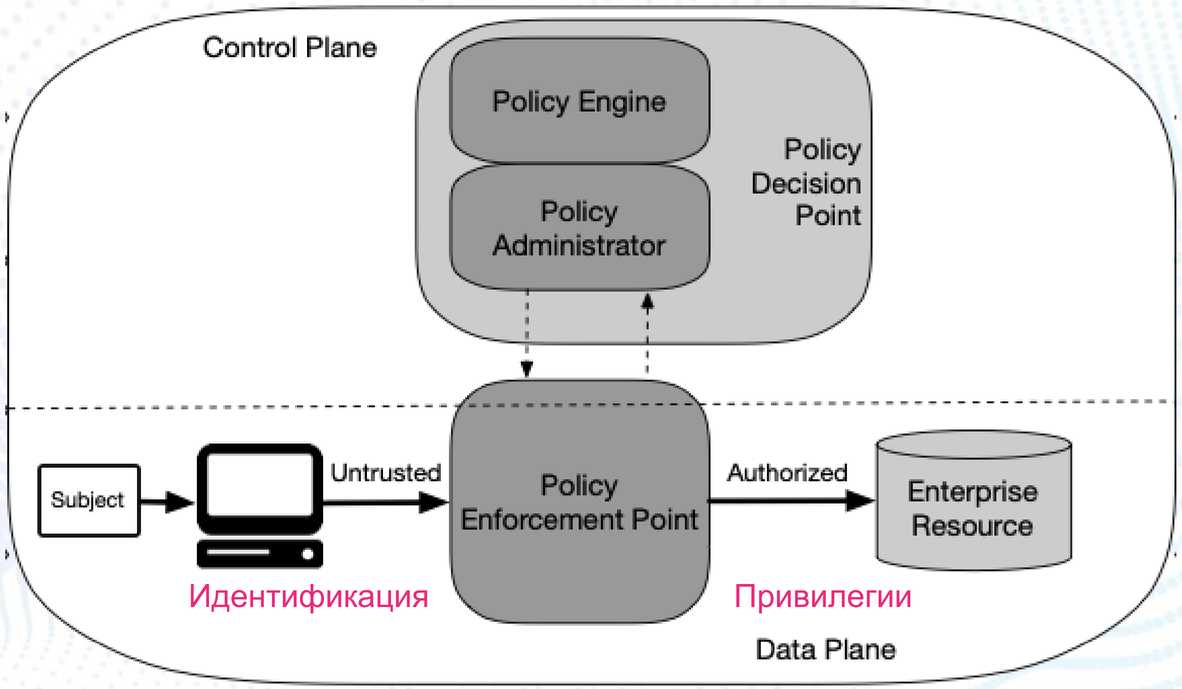
Принцип минимальных привилегий

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Пользователь в каждый момент времени имеет только те права, которые необходимы ему именно сейчас.

Принцип минимальных привилегий позволяет уйти от постоянных привилегий, которые означают бессрочные права на выполнение особо важных задач.

Если учетная запись с постоянными привилегиями когда-либо будет скомпрометирована или неправильно использована, она предоставит значительные возможности злоумышленникам.



Отказ от постоянных привилегий

Убрав привилегии из сети, мы создаем микропериметр для каждого ресурса

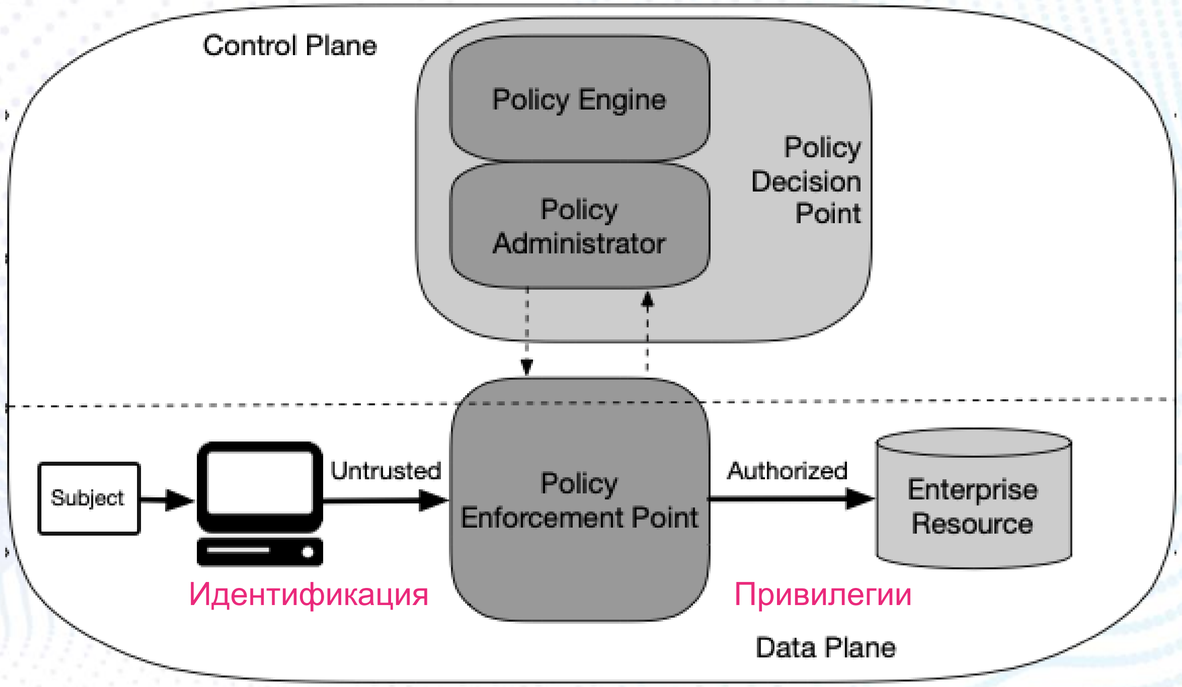
Детальный контроль каждой сессии

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Идея подхода “Just-in-Time” заключается в том, что для снижения самих рисков кибератак и уменьшения поверхности атак нужно сокращать доступность постоянных привилегий.

Для сокращения объема постоянных привилегий в среде необходимо рассмотреть три аспекта:

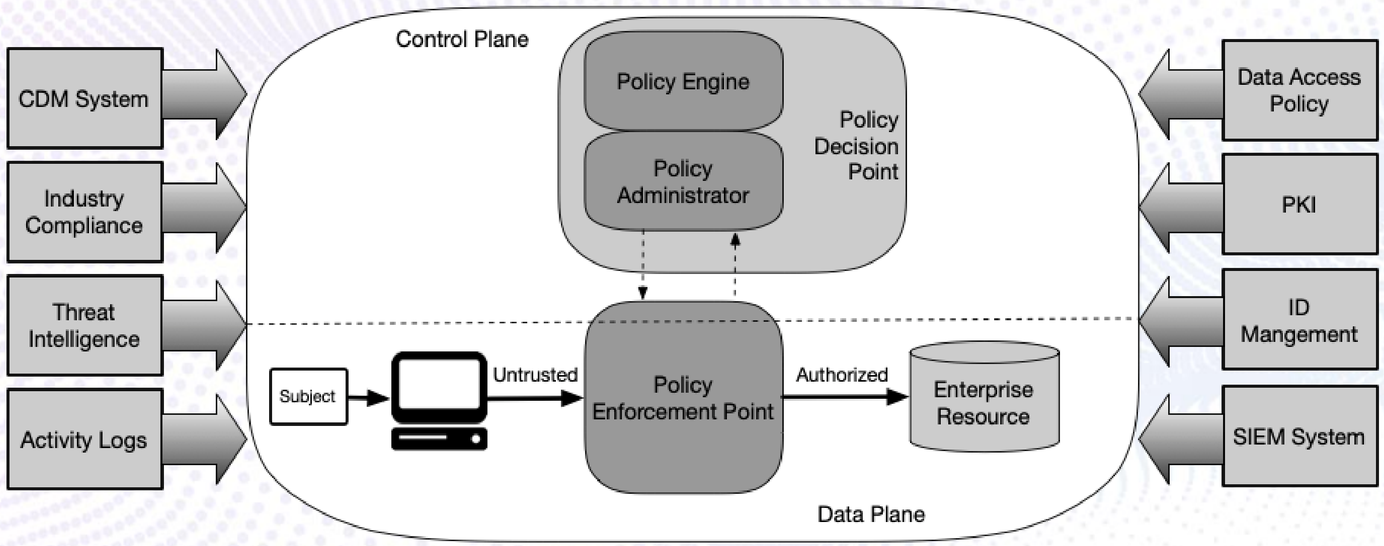
- операционная область — кому и какие разрешения предоставляются,
- инструментарий — каким образом они применяются,
- время — когда и на какой срок они предоставляются.



Just-in-Time

PAM – как точка наделения правами

Доступ к привилегированным административным учетным записям предоставляется только в тот момент, когда они необходимы, и в минимальном объеме.
Регулируется не только кто и куда должен иметь доступ, но и какие конкретные действия он может предпринимать в рамках назначенного временного окна доступа — принцип **"4К: Кто? Куда? Как? и Когда?"**.



Подсистема обработки политик

PAM-решения содержат компонент, который инициирует сеансы доступа на основе различных критериев. Они могут предоставлять доступ на основе ролевой модели, на основе политик, на основе разных атрибутов, по данным третьих систем.

Подсистема администрирования политик

PAM-решения содержат компонент, который позволяет настраивать, обновлять и управлять политиками доступа пользователей и устройств, в том числе и на сторонних системах.

Точка применения политик

PAM-решения инициируют сеанс доступа. Как правило, пользователю не предоставляется прямой доступ к ресурсу. Все сеансы доступа управляются и контролируются. При необходимости они могут быть заморожены и принудительно прекращены.

И почему только для администраторов?

PAM – в контексте Zero Trust

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Идентификация в сети:	
Динамическая аутентификация и авторизация всех ресурсов строго выполняется перед разрешением доступа.	Идентификация и динамическое наделение наименьшими привилегиями пользователей, приложения и системы непосредственно перед сеансом.
Управление конечными точками:	
Все источники данных и вычислительные сервисы считаются ресурсами.	PAM должен иметь универсальный коннектор к произвольному ресурсу.
Предприятие контролирует и измеряет целостность и уровень безопасности всех принадлежащих ему и связанных с ним ресурсов.	PAM обеспечивает жизненный цикл учетных записей (обнаружение, ротацию секретов, верификацию и предоставление).
Управление потоками данных:	
Ни одна сеть не считается доверенной. Все соединения защищены независимо от расположения сети.	Данные в сеансах привилегированного доступа передаются по защищенным каналам.
Точечный доступ с минимальными привилегиями. Контроль каждого сеанса, в идеале каждой операции.	PAM-системы способны инициировать сеансы доступа для выполнения определенного типа работ на конкретной системе с использованием специфического инструмента. Для критических действий — с онлайн наблюдением и контролем каждой операции.
Непрерывный аудит доступа. Доступ к ресурсам определяется динамическими правилами.	Запись каждого действия. Доступ к ресурсам определяется динамическими правилами.
Сбор максимального числа данных о состоянии системы и ее компонентов, динамическое реагирование.	PAM предоставляют единую консоль управления и сбора данных о всех действиях, связанных с привилегированным доступом. REST API позволяет третьим системам исполнять скрипты реагирования на инциденты под специфическими привилегиями.

ЗАЩИТА ДАННЫХ

СОХРАНИТЬ ВСЁ

Благодарю за внимание!