СБЕР АВТО

ZTA

Реализация архитектуры нулевого доверия

12 октября 2021

01

Про ZTA

Вызовы

СБЕР АВТО

Многие организации стремятся к нулевому доверию, но существуют проблемы.

Текущие проблемы при внедрении ZTA :

Зрелость продуктов поставщика для поддержки ZTA.

Способность / желание организации перейти на ZTA:

- большие инвестиции в другие (унаследованные) технологии
- отсутствие или недостаток управления идентификационной информацией
- отсутствие способности / ресурсов для разработки плана перехода, пилотного проекта или подтверждения концепции

Проблемы безопасности, такие как:

- компрометация плоскости управления с нулевым доверием
- способность распознавать атаки и обнаруживать злонамеренных инсайдеров

Вопросы совместимости продуктов / решений ZTA с унаследованными технологиями, такими как:

- стандартные и проприетарные интерфейсы
- возможность взаимодействия с корпоративными и облачными сервисами

Пользовательский опыт.

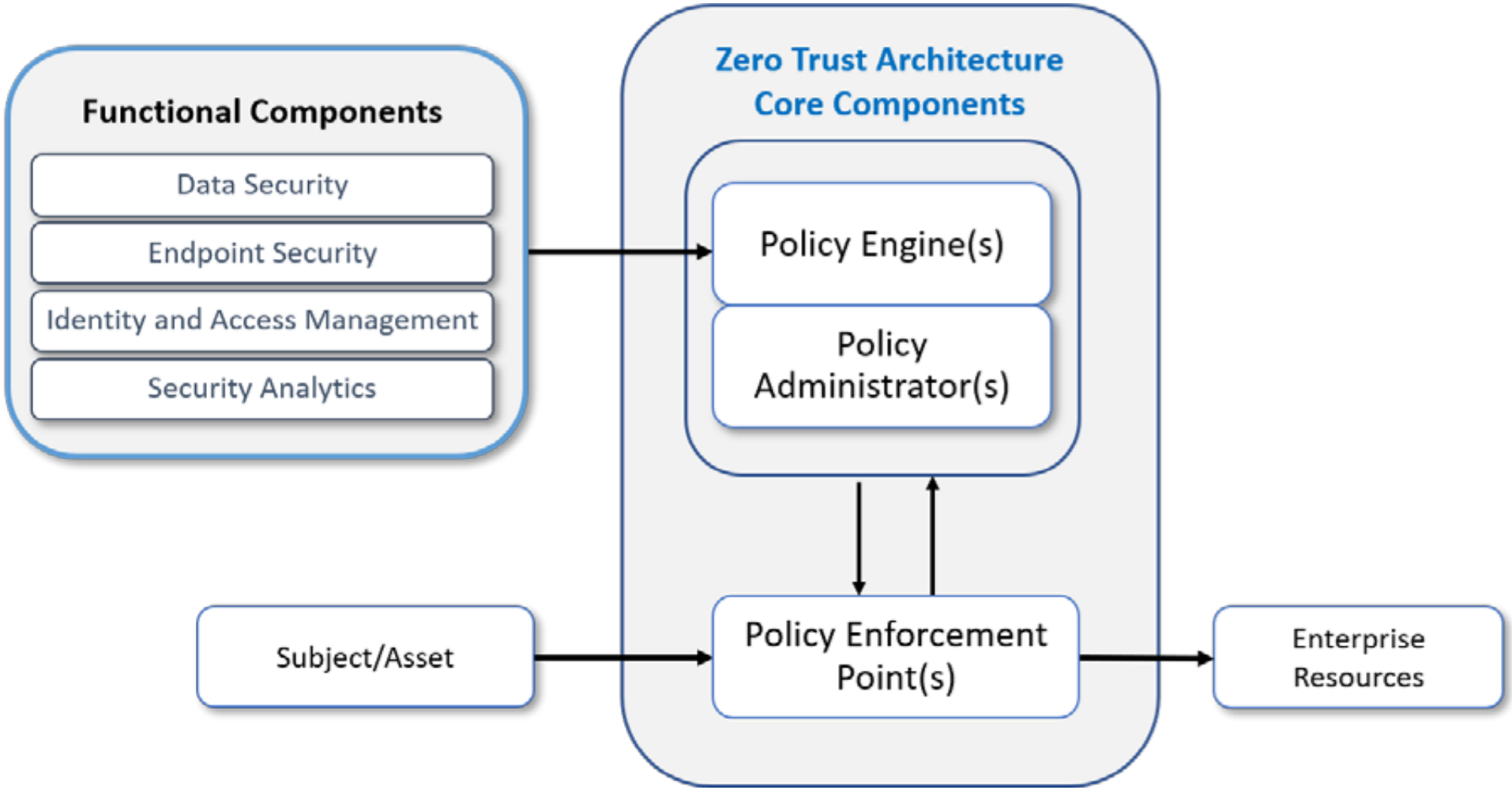
Целью ZTA должно быть повышение безопасности, прозрачное для конечного пользователя.

02

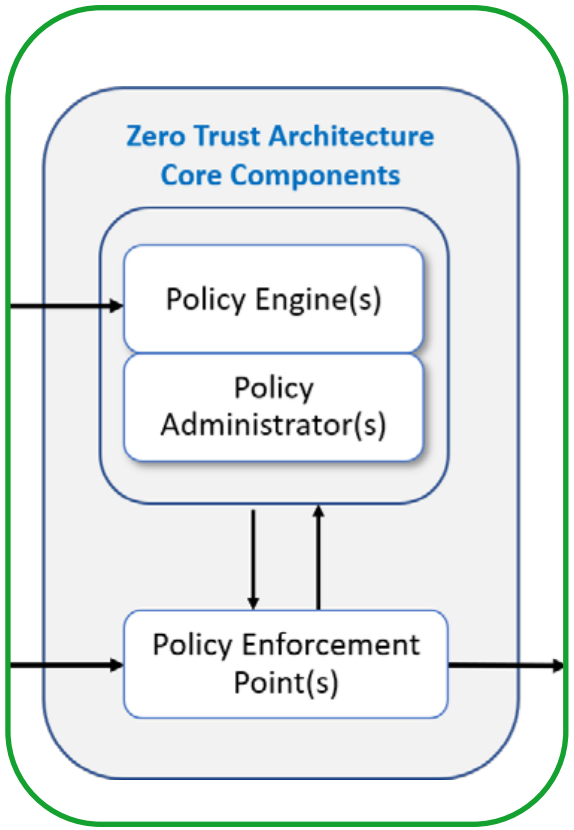
Про HIGH-LEVEL ZTA

HIGH-LEVEL Архитектура

СБЕР АВТО



HIGH-LEVEL Архитектура

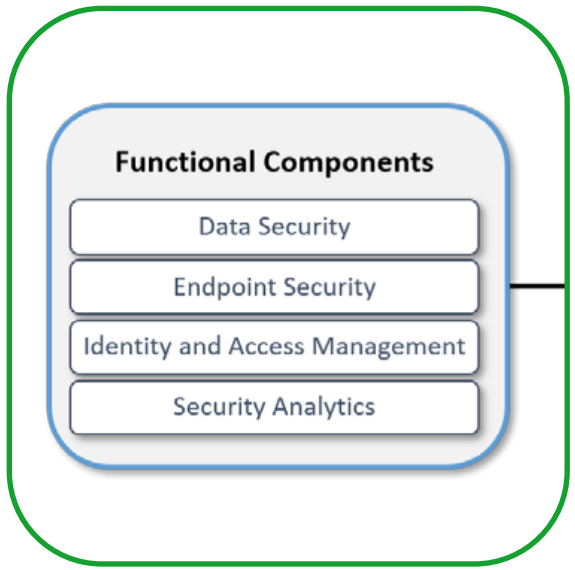


Ядро архитектуры:

Механизм политики принимает окончательное решение о предоставлении, отказе или отзыве доступа к ресурсу для данного субъекта. Механизм политики вычисляет оценки доверия / уровни достоверности и окончательные решения о доступе.

Администратор политики отвечает за установление / завершение транзакции между субъектом и ресурсом.
Он генерирует любой специфичный для сеанса аутентификации токен аутентификации или учетные данные, используемые клиентом для доступа к корпоративному ресурсу.
Он тесно связан с механизмом политики и зависит от его решения разрешить или запретить сеанс в конечном итоге.
Точка применения политики обрабатывает включение, мониторинг и, в конечном итоге, завершение соединений между субъектом и корпоративным ресурсом.

HIGH-LEVEL Архитектура



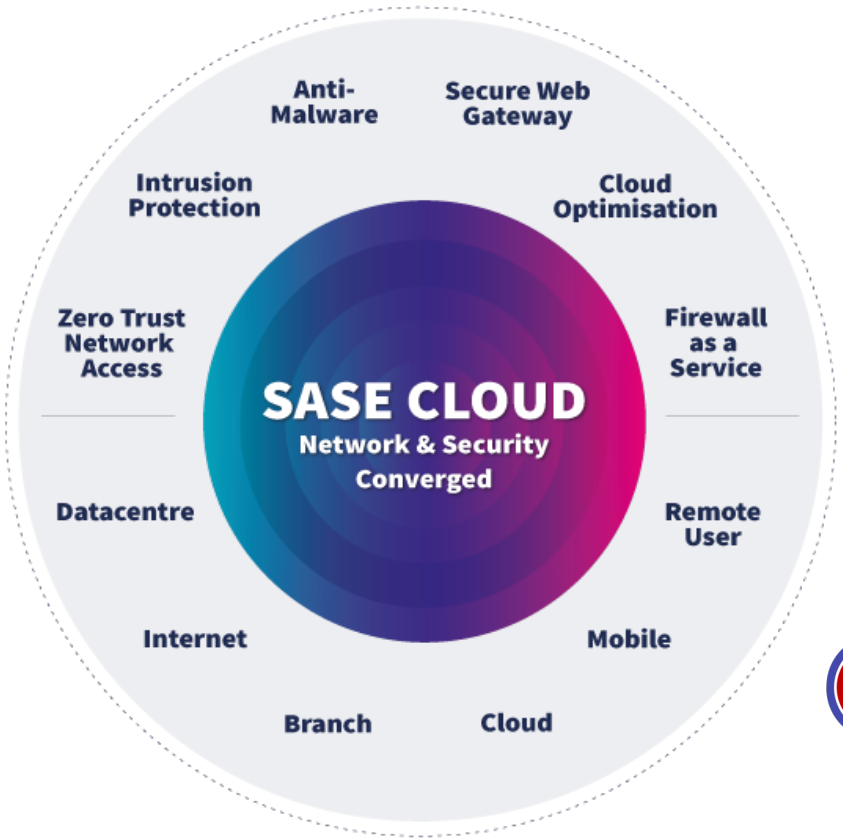
Функциональные компоненты:

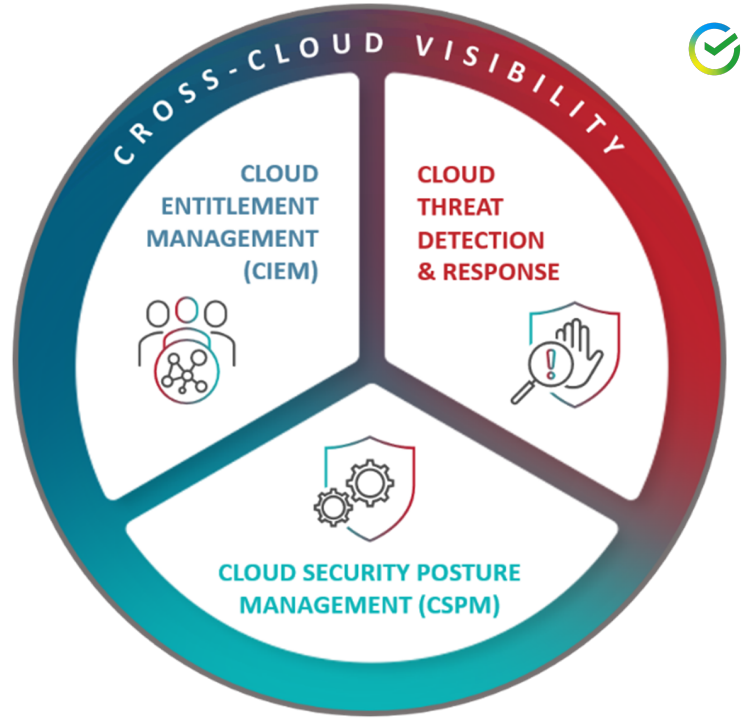
• **Компонент защиты данных** включает в себя все политики и правила доступа к данным, которые предприятие разрабатывает для защиты своей информации, а также средства защиты данных при хранении и передаче.
• **Компонент безопасности конечных точек** включает в себя стратегию, технологию и управление для защиты конечных точек (например, серверов, настольных компьютеров, мобильных телефонов,) от угроз и атак, а также защиты предприятия от угроз со стороны управляемых и неуправляемых устройств.
• **Компонент управления идентификацией и доступом** включает в себя стратегию, технологию и управление для создания, хранения и управления корпоративными пользовательскими учетными записями и идентификационными записями, а также доступом на их основе к корпоративным ресурсам
• **Компонент аналитики безопасности** включает в себя все каналы аналитики угроз и мониторинг трафика / активности для ИТ-предприятия. Он собирает аналитику безопасности и поведения о текущем состоянии корпоративных активов и постоянно отслеживает эти активы, чтобы активно реагировать на угрозы или злонамеренные действия. Эта информация может использоваться механизмом политик для принятия решений о динамическом доступе.
• **Компоненты устройств и сетевой инфраструктуры:**
• Активы включают устройства / конечные точки, такие как ноутбуки, планшеты и другие мобильные устройства или устройства Интернета вещей, которые подключаются к ИТ инфраструктуре компании.
• Корпоративные ресурсы включают данные и вычислительные ресурсы, а также приложения / сервисы, размещенные и управляемые локально, в облаке, на периферии или в некоторой их комбинации.
• Компоненты сетевой инфраструктуры включают в себя сетевые ресурсы.

03

Про SASE и не только

SASE





СБЕР АВТО

Спасибо за внимание!

Кирилл Ильин

CISO - руководитель отдела кибербезопасности

SberAuto

+7 (916) 655-14-57

k.ilin@sberauto.com