August 8, 2017

Securing Sensitive Data When It Leaves the Car

Jeff Rubin
Vice-President, Strategy and Business Development

All things mobile. **SimplySecure**™

BEACHHEAD

Auto data security is a growing problem – managing SED encryption on a diverse fleet is needed

Problem

Each car stores private data that must be made inaccessible for unauthorized use. As direct access to the vehicle isn't always possible, owners and fleet managers should manage this security remotely

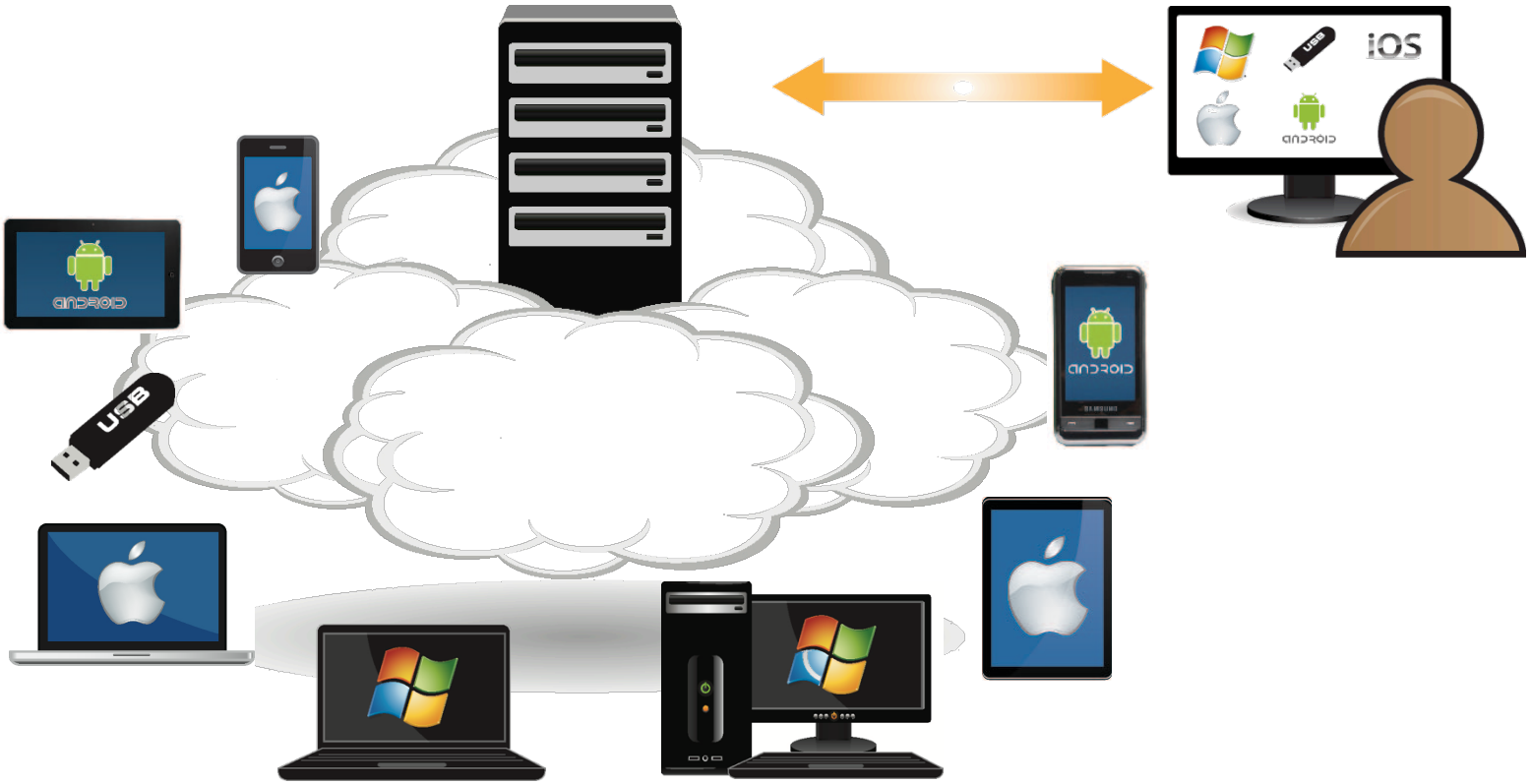
Solution

Web-managed centralized OPAL encryption management

- Simple interface for consumers
- Easy policy-management console for fleet/corporate

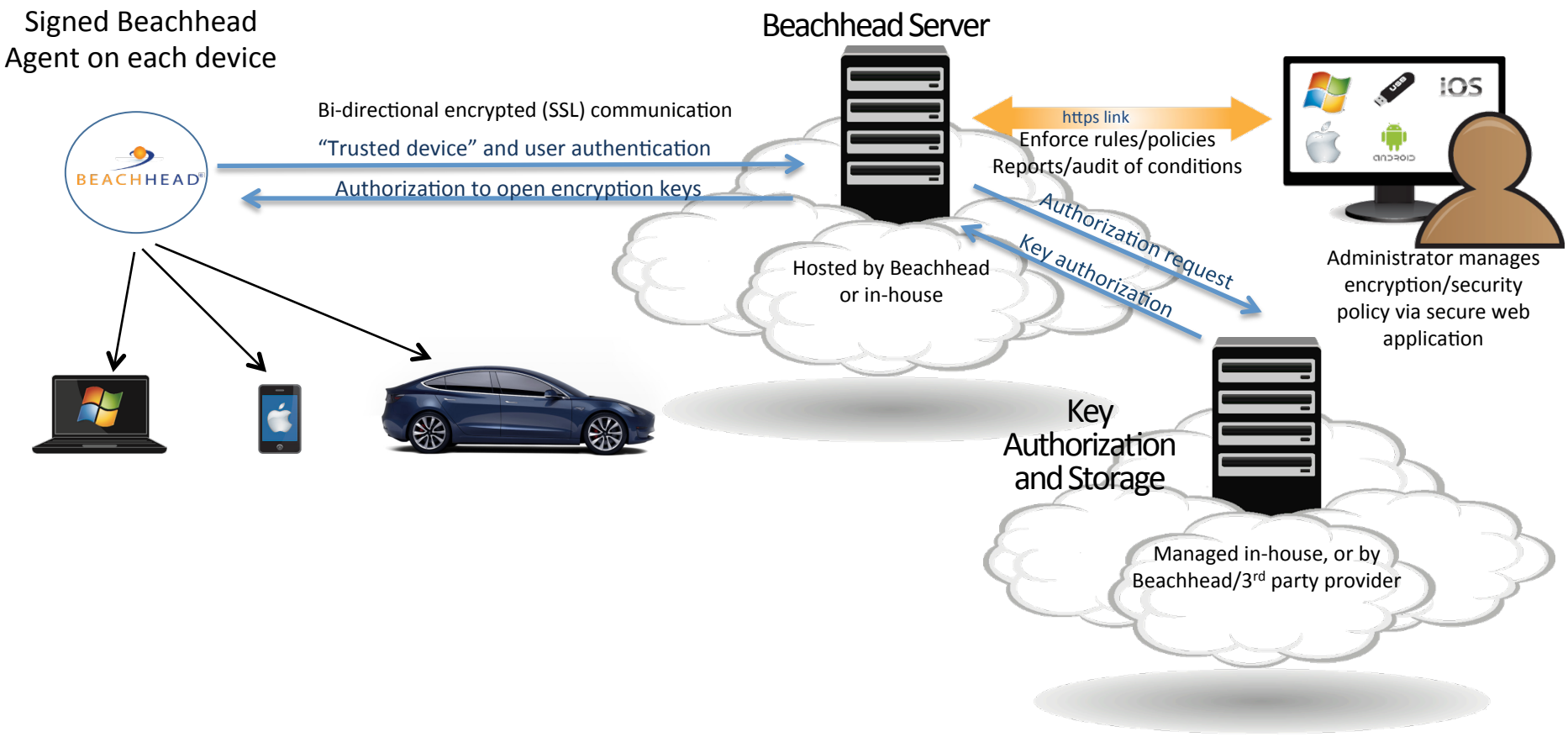
BEACHHEAD

Beachhead controls other devices from a single, unified management console



BEACHHEAD

We are now applying this experience to automobiles



BEACHHEAD

When is access management needed?

- Car under owner control
  - **Transfer of ownership** - cars usually have multiple owners and have an average life expectancy of 11-12 years
  - **Multiple drivers and passenger data** – syncing and voice recognition mean most cars are multi-user
  - **Fleet and rental/lease use** – multiple drivers, often for short periods
  - **Other security policy needs** – intentional disablement of data, audit
  - **Planned end of life**
- Owner has lost control of car
  - **Stolen or repossessed car**
  - **Accident or under repair**
  - **Other unplanned end of life**

BEACHHEAD

End-user experience should be easy and reassuring

- Simple Consumer web interface
  - Needs to only handle matrix of cars and drivers/passengers
    - Tools to add/alter registration of drivers and other users
    - Simple “lock” and “unlock” of data access by user and vehicle
- Fleet interface can expand range of security policies
  - Simple enrollment and wiping of information by user
  - Use GPS and other tools to limit access to data
  - Security audit capability to validate encryption status

BEACHHEAD

All things mobile. **SimplySecure**™

BEACHHEAD