# Automate over-the-air (OTA) software updates across your connected device fleet

Deploy bug fixes, patch security vulnerabilities, and enable new features to field-deployed embedded Linux devices with an end-to-end open source platform

## Immense opportunities come with security risks

Securing embedded devices is an obstacle to widespread adoption of IoT. According to a report by Identify Theft Resource Center (ITRC), the number of data breaches increased by 40% in 2016 compared to 2015. This causes justified apprehension in connecting new devices. Many malicious attackers specifically scan for recently published security vulnerabilities with the intent of seeking systems and devices that remain outdated and vulnerable.

Malware such as Mirai, Hajime, and BrickerBot have successfully targeted insecure Linux devices, with the number of compromised devices in the millions. The risk is very real.

## At 40-60 days, the probability of a vulnerability being exploited reaches over 90%

A key finding by Kenna Security is at 40-60 days, the probability of a vulnerability being exploited reaches over 90%. If the vulnerability is remediated within 5-10 days after discovery, that number drops to below 10%.

## OTA software updates

Mender provides an open source tool to deploy OTA software updates across your fleet of Linux-based devices. It is end-to-end, with both the management server and the runtime client on the device licensed under Apache 2.0.

Mender addresses the following challenges:

### Rapid bug fixes and security patching

Bugs and vulnerabilities are patched quickly, reducing the attack surface and limiting the window for exposure.

### Extensible

Mender supports changing system requirements and integrates easily with other components of your system. Mender is compatible with existing workflows. It can easily be adapted to your platform rather than requiring you to adapt to it.

### Device groupings and rollback support

Mender's ability to create device groupings enables controlled rollout of software updates with rollback support built-in to confidently avoid bricked devices

### A fully integrated end-to-end solution

Mender provides a fully integrated, purpose-built solution with both the management server and the client tested together including full CI across all versions

## Ease of implementation

Minimize time spent deploying a difficult-to-use OTA solution that imposes significant changes to your system software. And avoid building your own updater and spend more time building your product.

Mender's automated OTA updater removes the manually intensive process in updating devices individually and eliminates the high cost of sending technicians to the field to repair device outages. Mender also removes the need to build and maintain a homegrown update mechanism, which can easily dominate the time of a full time employee.

## Architecture
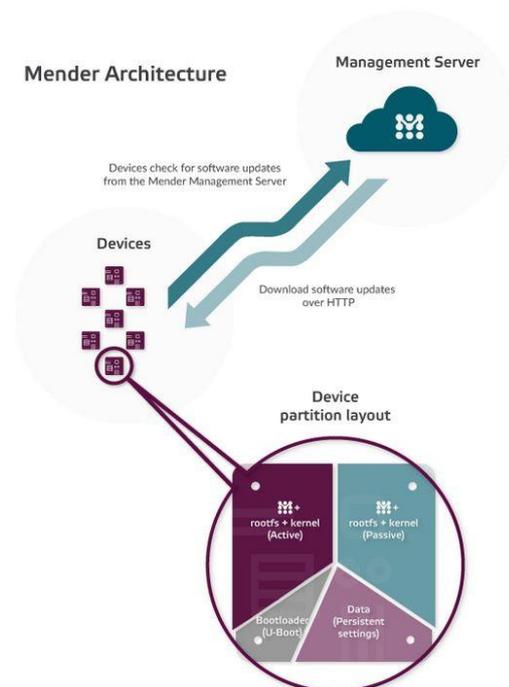


## Features

- Built-in rollback support with dual A/B root filesystem partition setup
- Secure TLS communication between client/server
- End-to-end signing and verification of image artifacts for authenticity & integrity
- Rootfs integrity check to avoid corruption
- Rootfs compression to save bandwidth

## OS & board support

### Operating system support

Mender currently supports Linux-based devices that use U-Boot and provides a feature layer for the Yocto Project for easy integration with Yocto-based projects.

Mender can be integrated into other Linux platform builders and distributions (e.g. OpenWRT, Buildroot, or Ubuntu Core) by setting up the required partition layout and U-Boot features similar to what is done in the meta-mender repository. Community contributions for these features will be gladly accepted or we can implement them on demand.

### Board support

Out of the box, Mender supports the BeagleBone Black. Support for a virtual device using QEMU is provided for development and testing purposes.

Integrating Mender into additional Yocto-supported platforms is easy requiring minimal updates to the meta-mender and platform layers.