3LM
Three Laws
of Mobility

Android for the Enterprise

Getting from Here to There

Overview

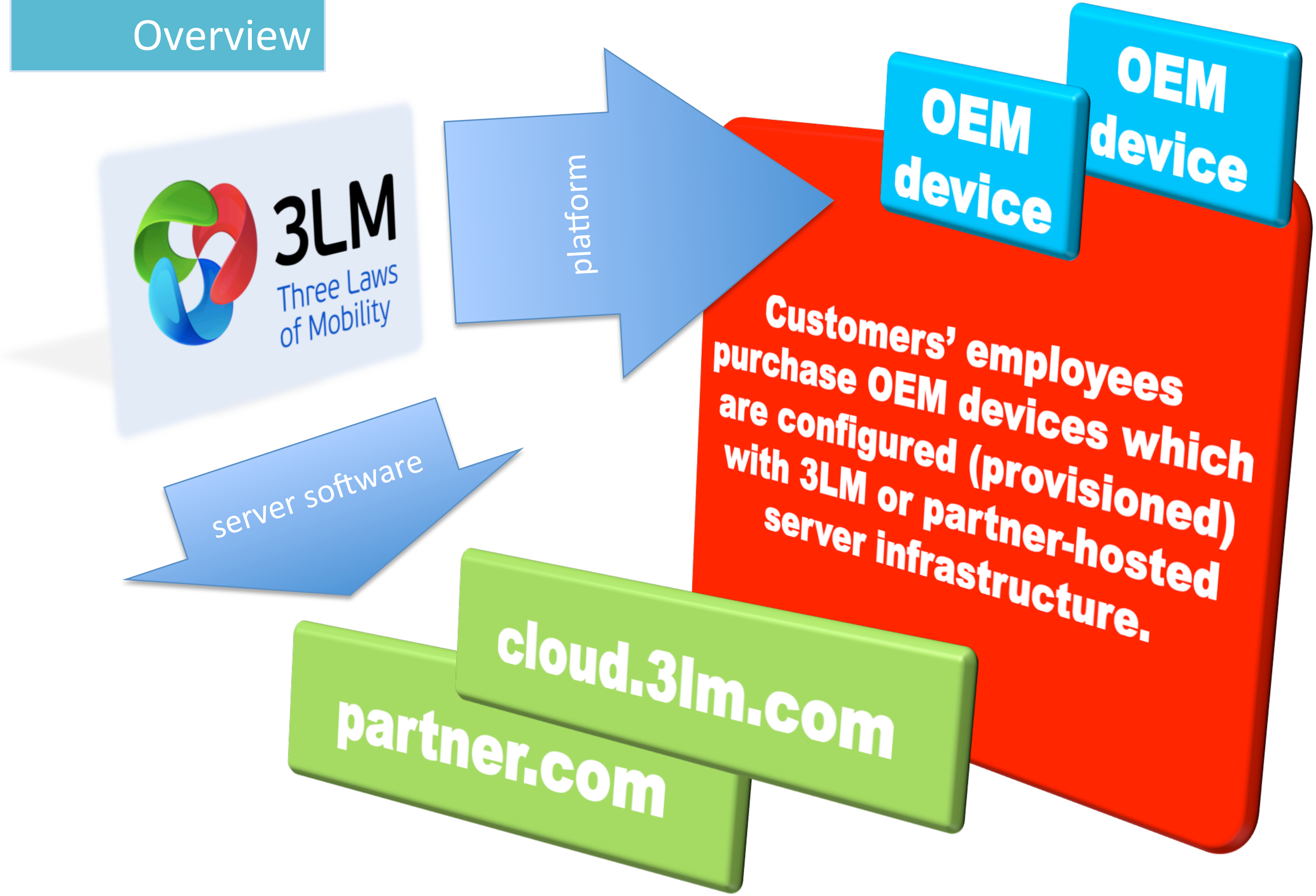
3LM addresses enterprise needs: security and device management.

Device Security

Device Management

Secure Remote Access

Overview



3LM Three Laws of Mobility

platform

server software

OEM device

OEM device

Customers' employees purchase OEM devices which are configured (provisioned) with 3LM or partner-hosted server infrastructure.

cloud.3lm.com

partner.com

Overview

SHARP

htc

Sony Ericsson

MOTOROLA

PANTECH

KYOCERA

FUJITSU

TOSHIBA
Leading Innovation >>>

NEC CASIO Mobile Communications, Ltd.

KDDI

BoxTone®

Use cases

Use cases

Loss Remediation

Minimize risk of data exposure on lost devices

1 Device is lost or stolen and reported to IT

2 IT locates device using 3LM console and locks it

3 If device cannot be retrieved, ALL or PART of the data on the device can be wiped

Use cases

Application Management

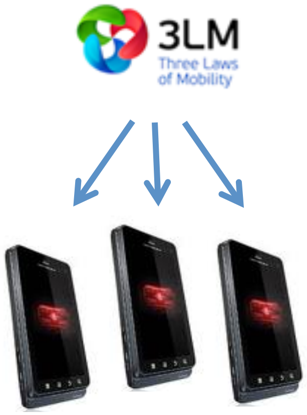
Manage which applications users can run

1

IT remotely deploys policy on which applications can be used on devices

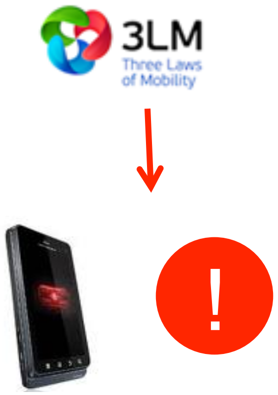
2

IT remotely installs approved enterprise applications to devices



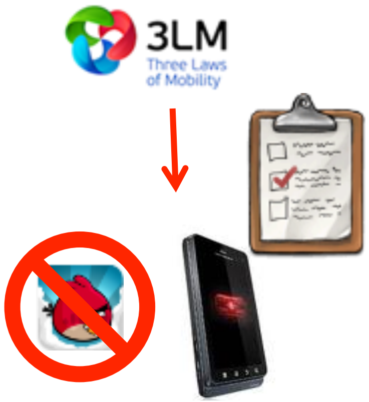
3

IT runs audit of devices and finds new unauthorized applications to block



4

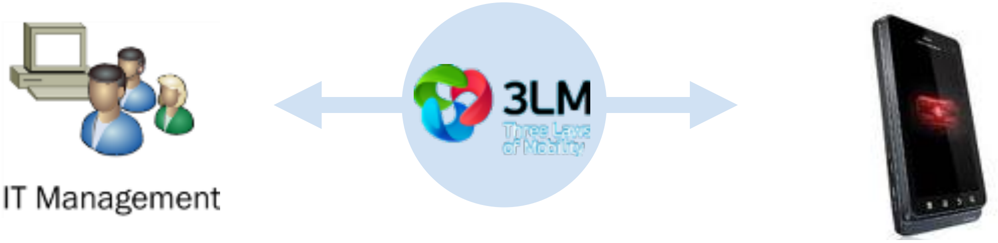
IT REMOVES the unauthorized application and updates policy



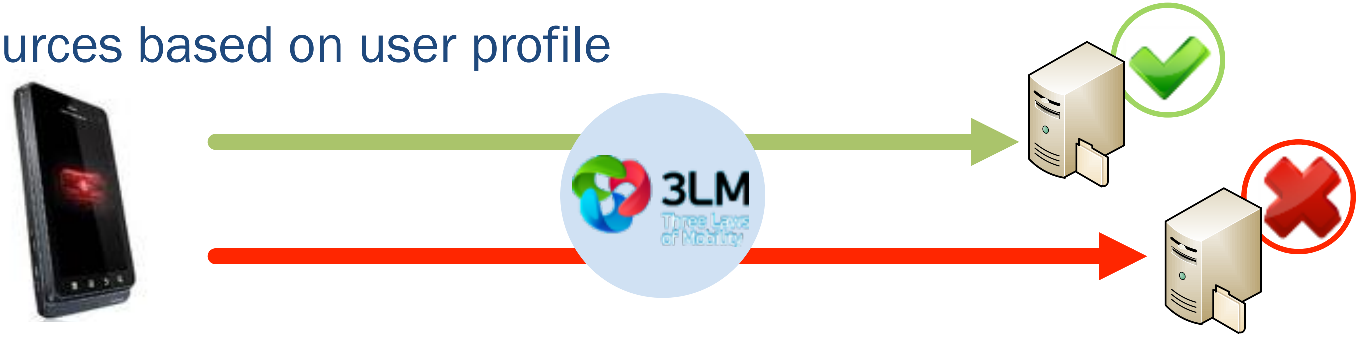
Permissions-Based Resource Access

Lock down which resources remote users can access

1 IT enables remote access for user and defines which resources they can access across the secure link



2 3LM routes and enables or blocks access to internal resources based on user profile

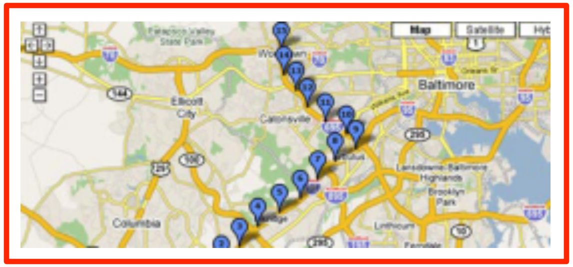


Use cases

Unique Configurations for Business

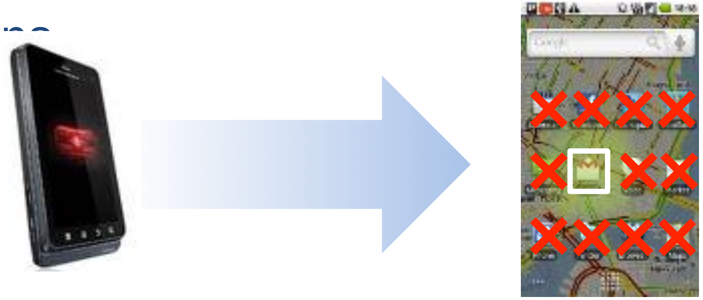
Track devices and whereabouts

Enable ‘breadcrumb’ tracking of devices to track history of location of a device



Lock down and manage devices to limited purpose

Enable ‘Kiosk-mode’ type scenarios limiting devices to only use one or a few applications



Features

Device and transport encryption

- Full device encryption and SD Card encryption using 192-bit AES
- TLS and AES encryption of data transport over the air

Application Control

- Disable pre-installed applications
- Remotely install applications and make permanent (user cannot remove)
- Remotely remove applications
- Set whitelist/blacklist of applications to be used
- Manage application permissions post-install

Leverage data protection tools

- Enforce strong passwords
- Remote device lock when devices are lost
- Remote data wipe – selective data or entire device

Set policy on hardware usage

- Lock usage of Camera, Bluetooth, Wifi, SD Card, etc.

Track location

- Fetch location of devices
- Track location history (breadcrumb)

Secure remote access (VPN)

- Enable remote access to internal enterprise resources
- Set permissions by user on resource access

Monitor device health

- Remote device health and status checking

How it works

Experience

End User

3LM is running on device and is unnoticeable in normal usage. It does not require 'launching' an app of any sort for each use once provisioned.

IT Administrator

IT can create and deploy policies to enable and disable software and hardware components as well as providing encryption for data protection. Policy management is performed from a remote console and gives IT complete control of 3LM enabled Android devices.

Requirements

Handheld

- 3LM features activated via app install and provisioning
- 3LM framework embedded on the Android device
- Subset of features for non-3LM devices
- Android 2.2 and higher

Server Components

- 3LM router and 3LM enterprise server
- Multiple network configuration options: based on who hosts what

How it works

Server Components

3LM Router

Server that handles setup and management of security of the data transport. Can be hosted by 3LM or located within a customer’s premise.

3LM Enterprise Server

Server that hosts the IT management console for setting up and managing policies on devices.   Also acts as the interface to Microsoft Exchange and other back-end systems.

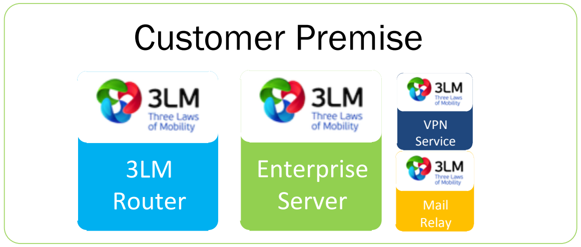
3LM VPN Service

Optional Service that allows for secure remote access to internal corporate resources

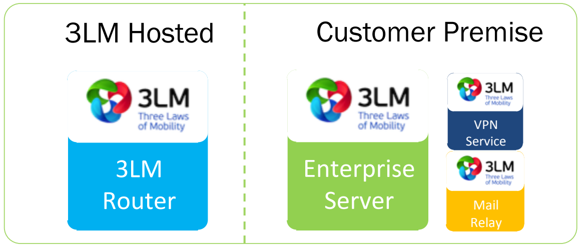
3LM Mail Relay

Optional Service that allows for integration with Microsoft Exchange through the 3LM secure transport channel

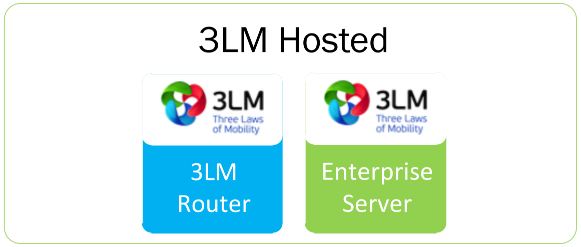
Multiple Configurations Possible



Enterprise Hosted



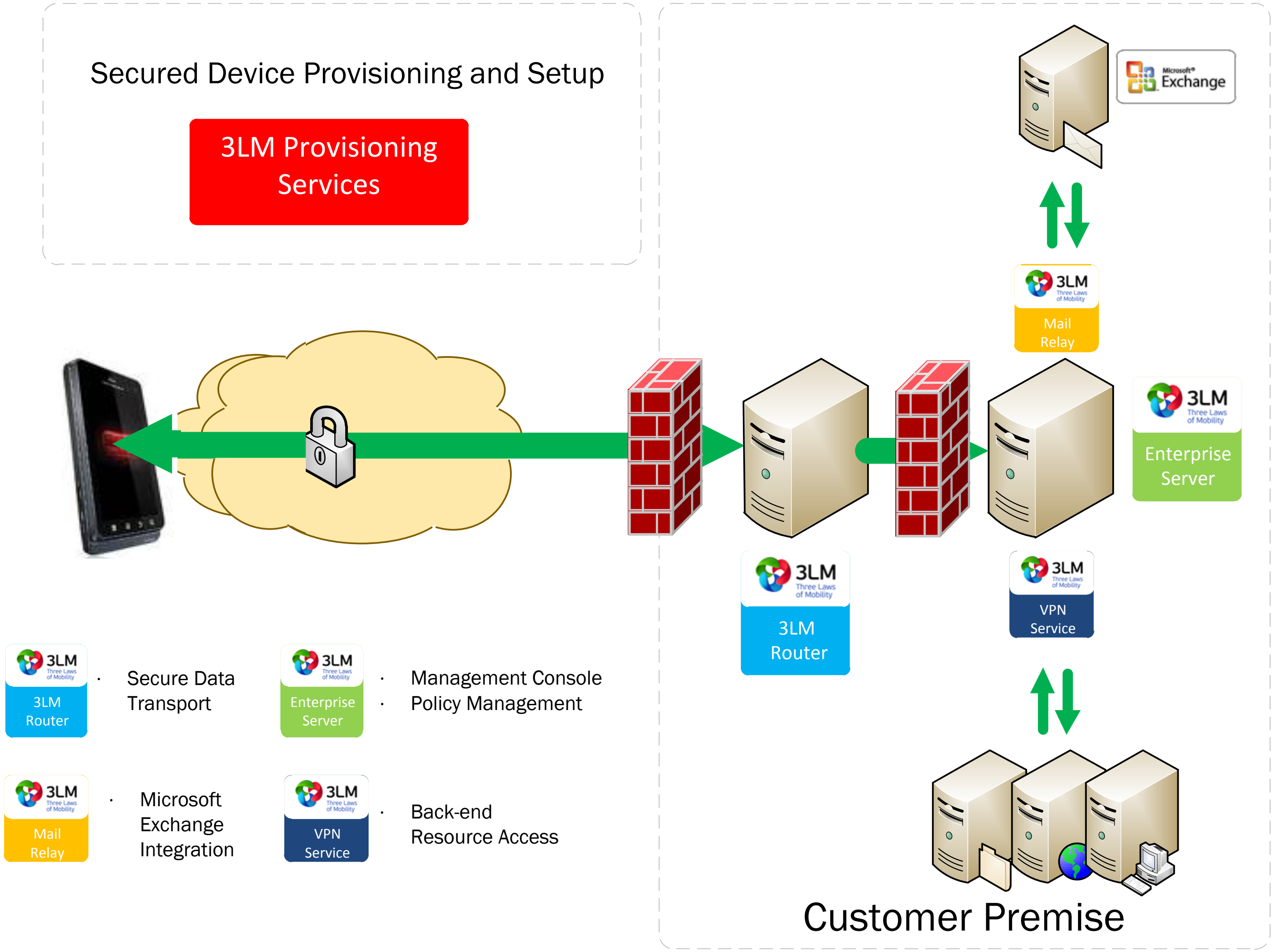
Hybrid Hosted



Full 3LM Hosted

How it works

Enterprise Hosted Model



Secured Device Provisioning and Setup

3LM Provisioning Services

Microsoft Exchange
3LM Three Laws of Mobility
Mail Relay
3LM Three Laws of Mobility
Enterprise Server
3LM Three Laws of Mobility
3LM Router
3LM Three Laws of Mobility
VPN Service

Customer Premise

3LM Router
- Secure Data Transport

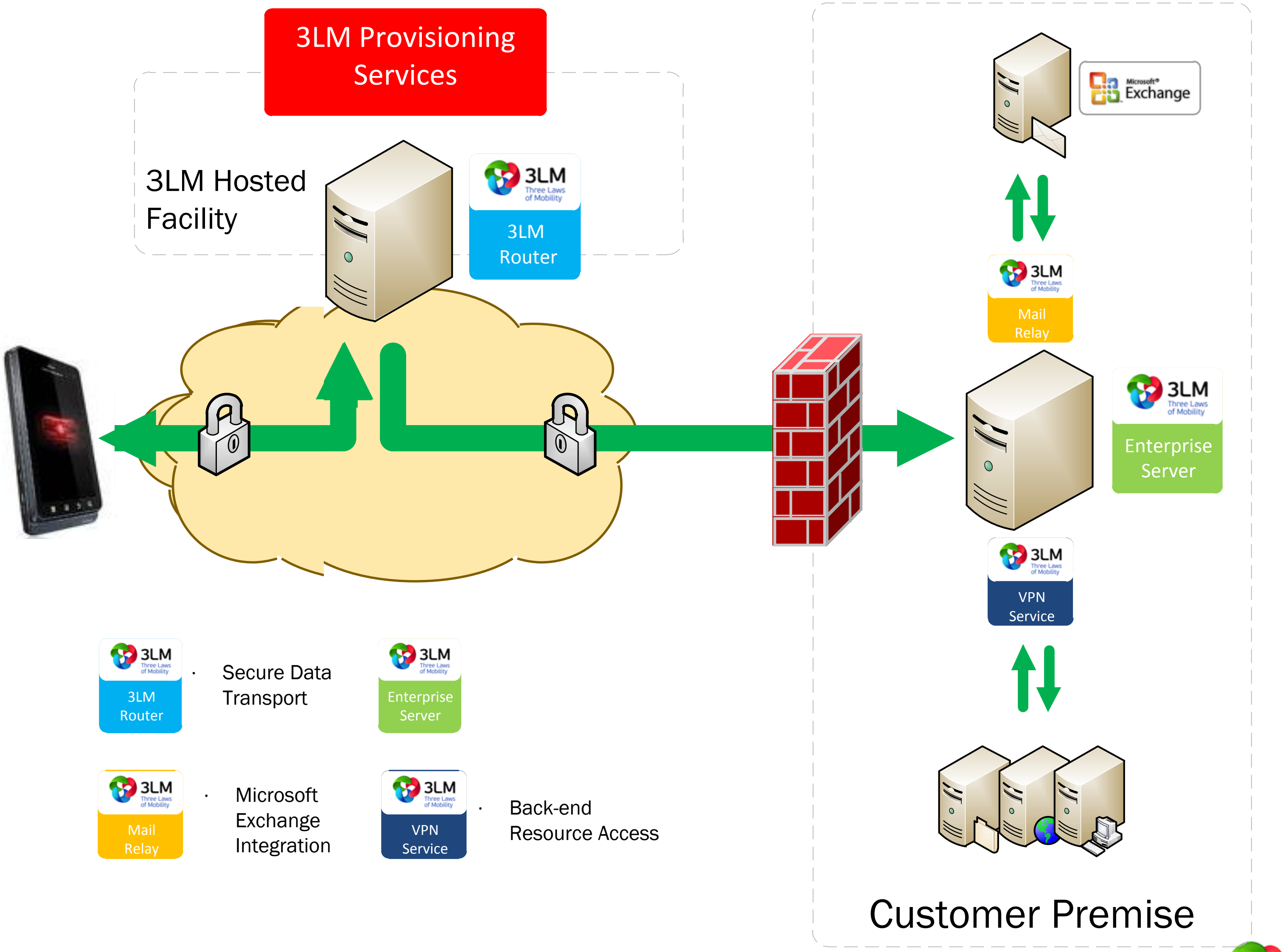
Enterprise Server
- Management Console
- Policy Management

Mail Relay
- Microsoft Exchange Integration

VPN Service
- Back-end Resource Access

How it works

Hybrid Hosted Model



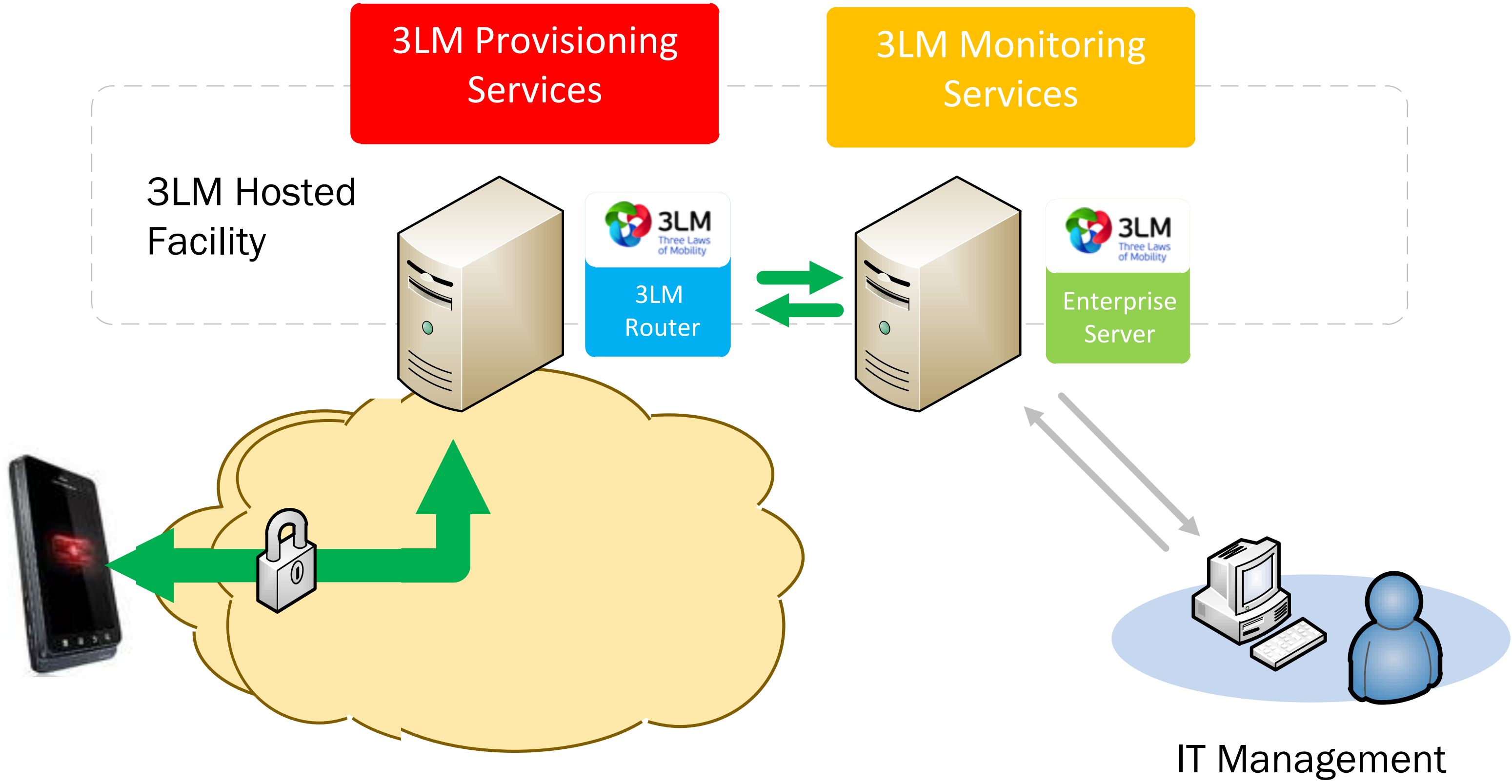
3LM Router · Secure Data Transport

Enterprise Server

Mail Relay · Microsoft Exchange Integration

VPN Service · Back-end Resource Access

Cloud/3LM Hosted Model



3LM Three Laws of Mobility 3LM Router — Secure Data Transport

3LM Three Laws of Mobility Enterprise Server — Management Console

Device Framework

Extending Android

Opportunities

- Leverage existing, mature modules such as eCryptFS, tun
- Possibility to contribute code back into AOSP
- Deep Android OS understanding
- Thriving ecosystem

Challenges

- Maintaining platform extensions on top of unknown future changes
- Reduced functionality for non-3LM devices
- Must exist within the constraints

Device Framework

OEM Collaboration

Benefits

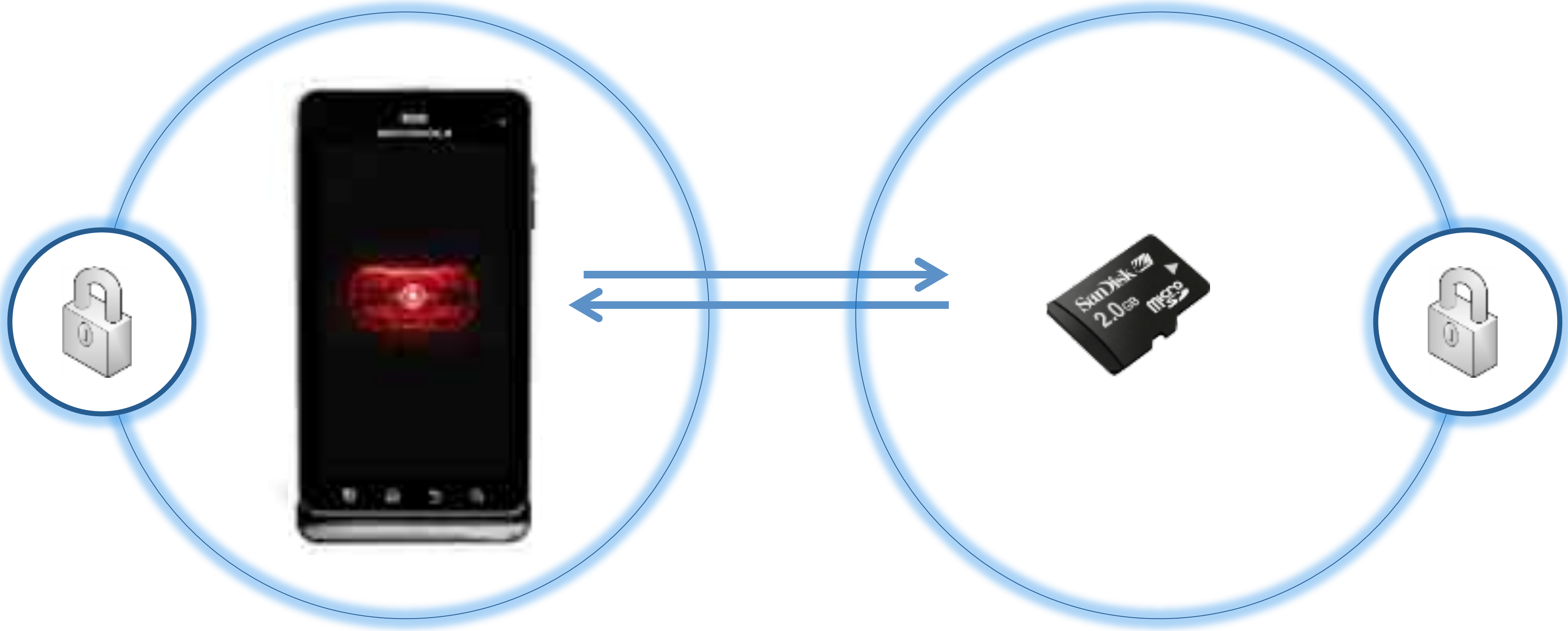
- Helps us re-validate and improve our design
- Helps strengthen our core “feature” set
- Visibility into the whole ecosystem

- A unique differentiator: there is a limit on what you can do with apps
  … and the path through VM-land is far from proven

Challenges

- Patch lifecycle: ensuring all change sets are correctly applied
- Debugging problems on unavailable codebase
- Customized OS software, and hardware

Case Study: SD Encryption



Onboard Flash Memory

192-bit AES using eCryptFS

Removable SD card

192-bit AES using dmCrypt

Device Framework

Case Study: SD Encryption

The easy part

- dmCrypt already available on the device!
- Use the stock credential storage module

The harder part

- Multiple SD devices, variety of partitioning schemes
- Various use models, custom media control apps

Other proprietary extensions

- Use of SD card for OTA storage (/cache too small...)

Server Infrastructure

Putting it all Together

Main components

- Provisioning server
- Message router
- Enterprise server
- E-mail / VPN components
- *But also: Monitoring, Load balancing and clustering, DB shards*

Hosting challenges

- Multiple hosting modes (cloud, intranet)
- Connection throttling (among other EC2 challenges)
- Switching between networks; internal hosting: scale in vs. scale out

Reliability and Tuning

Framework Hell

- SSL (Harmony, Netty, thread [un]safety, bugs in EDH implementation)
- Crypto providers (Android: an oldish built-in Bouncy Castle)
- C#...

Performance

- Memory demands: 100K's of live connections
- Fast asynch I/O, clustering

Questions?

jobs@3lm.com

info@3lm.com