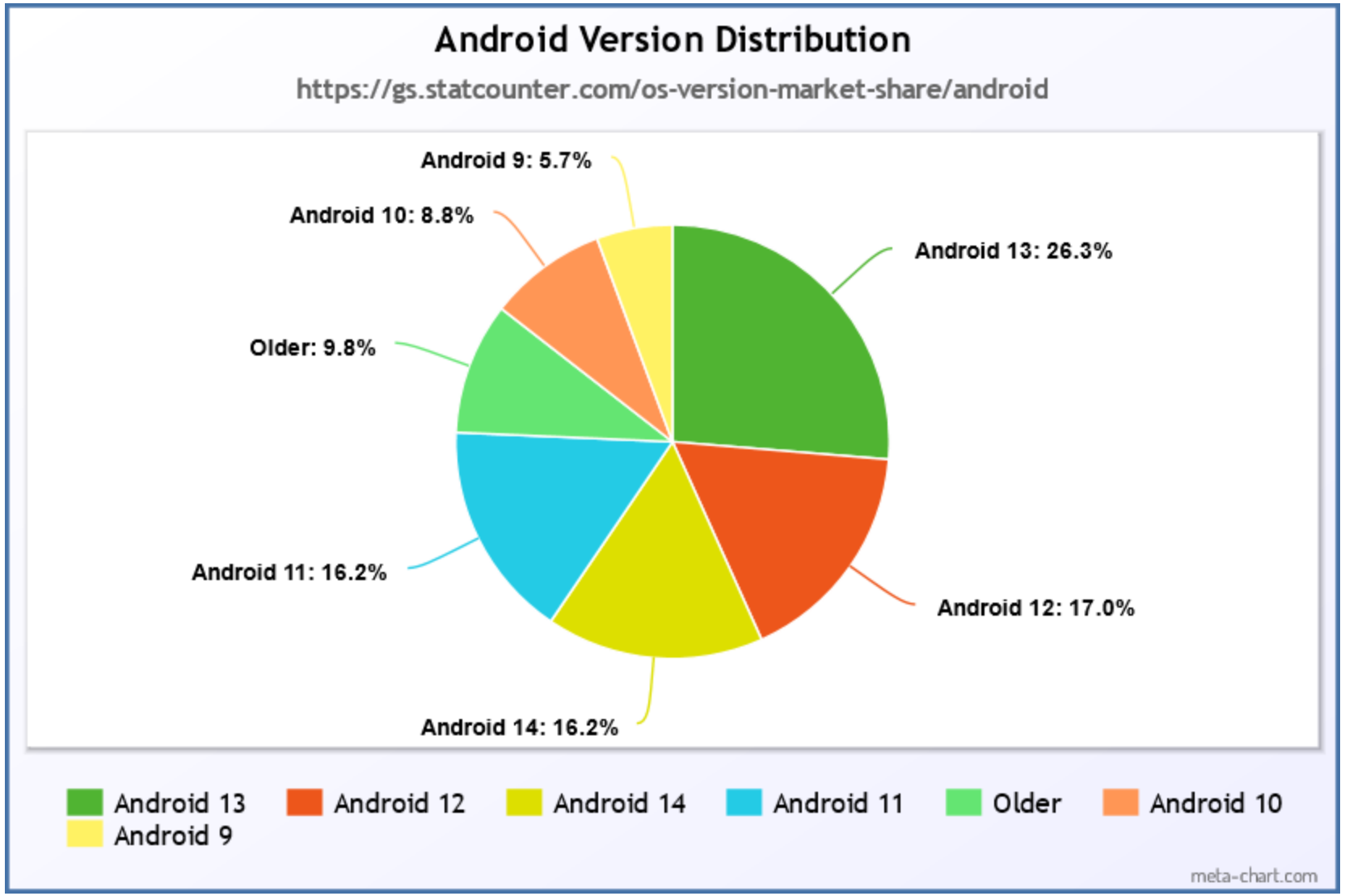
ANDROID OS OVERVIEW

Bitdefender

Android codenames and identifiers

- Android OS
  - open source
  - Linux-based
  - for a wide array of devices
- Android OS versions have 4 identifiers
  - Codename, Version, Version Code and API level
  - Often used interchangeable (although they are not quite interchangeable)

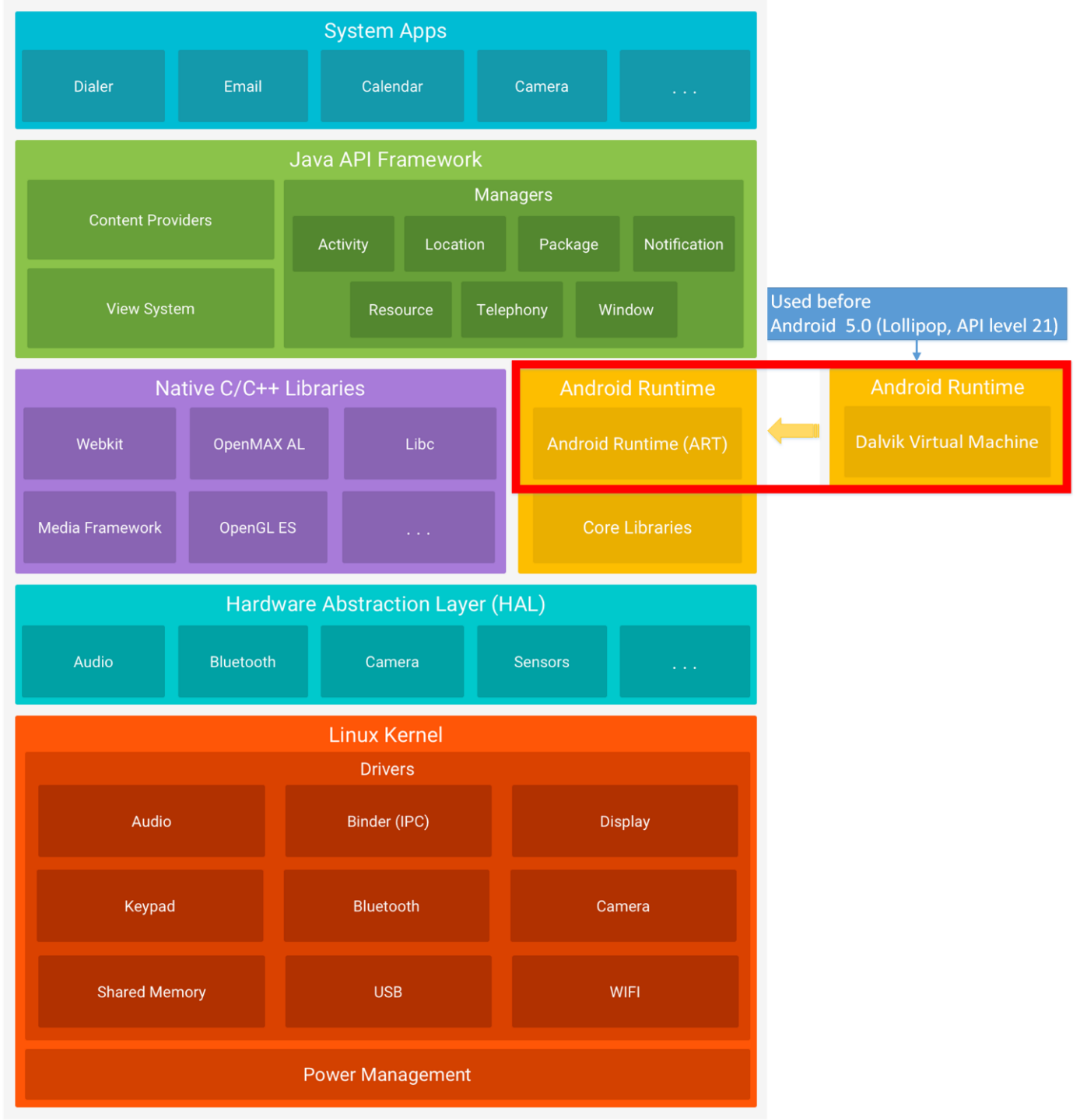
Version	Codename	Version Code	API level
Android 14	Upside Down Cake	UPSIDE_DOWN_CAKE	34
Android 13	Tiramisu	TIRAMISU	33
Android 12	Snow Cone	S/S_V2	31/32
Android 11	Red Velvet Cake	R	30
Android 10	Quince Tart	Q	29
Android 9	Pie	P	28


Android Version Distribution
https://gs.statcounter.com/os-version-market-share/android
Android 9: 5.7%
Android 10: 8.8%
Android 13: 26.3%
Older: 9.8%
Android 11: 16.2%
Android 12: 17.0%
Android 14: 16.2%
Android 13
Android 12
Android 14
Android 11
Older
Android 10
Android 9
meta-chart.com

- March 2024

Android Platform Architecture

- Linux Kernel
- Hardware Abstraction Layer (HAL)
- Android Runtime
  - ART/Dalvik
- Native C/C++ Libraries
- Java API Framework
- System Apps



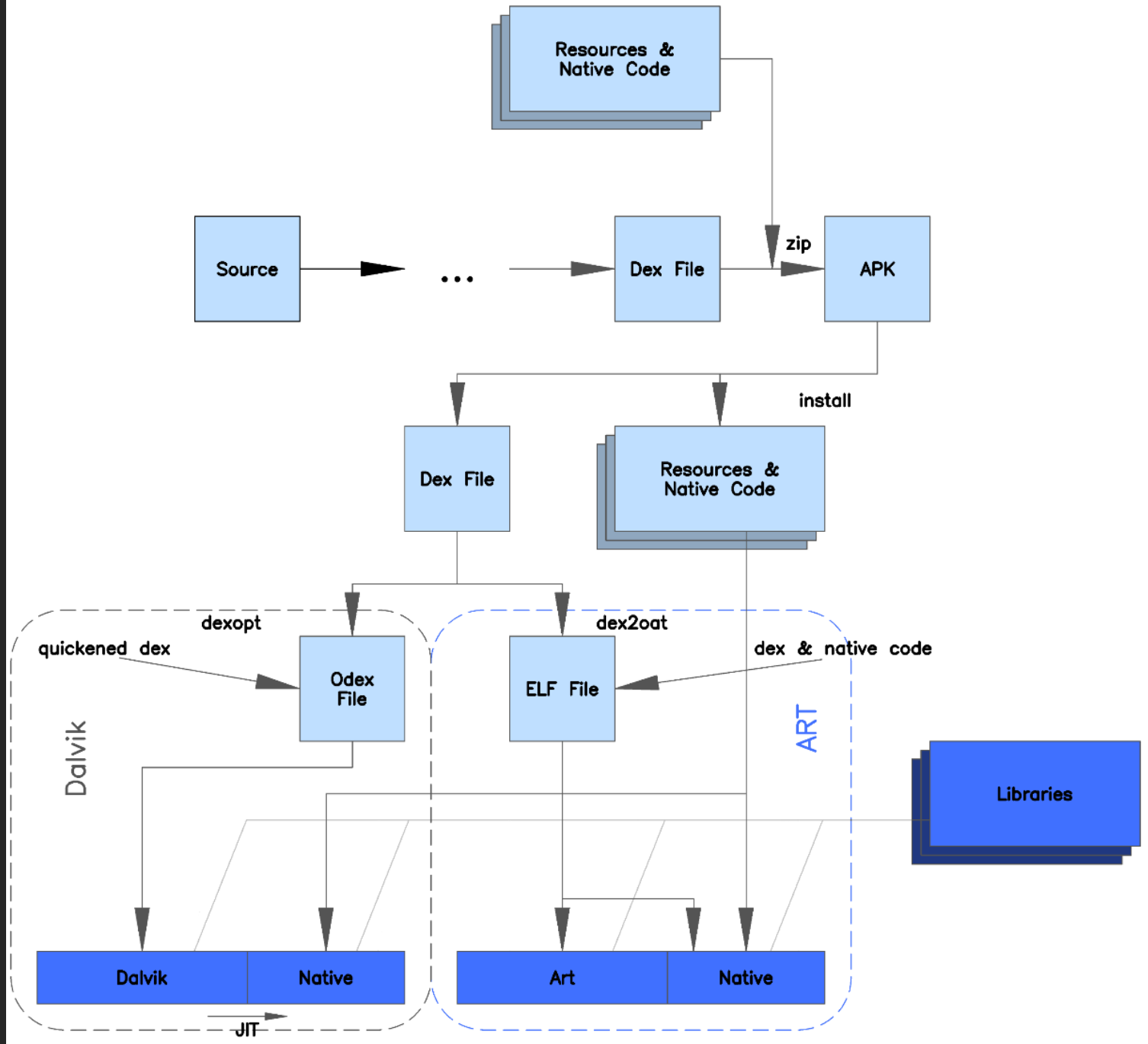
Dalvik Virtual Machine (DVM) versus ART runtime

Android runtime

- Dalvik VM (before API level 21)
- Android Runtime (API level 22+)

Both take input DEX files and convert them to a more optimized version

- .odex (optimized dex) for Dalvik
- .oat (shared objects, ELF files) for ART



Runtime code compiling

- There are 2 general versions code compilations and optimization:
  - just-in-time (JIT) compile
    - compilations are done at the exact moment when the application/code is executed
  - ahead-of-time (AOT) compiler
    - compilations are done before the execution of the application/code.

Example

Android OS	Runtime	Compilation strategy
KitKat	**Dalvik**	**JIT**
Lollipop	**ART**	**AOT**
Nougat	**ART**	**Hybrid JIT/AOT**

Runtime code compiling

Why does this matter to us?

Installation of applications*

- corrupt applications
  - install on a system with JIT and will crash on launch
  - fail to install on a AOT system (where optimization would occur on install)

- anti-threat solutions, if using custom parsers for applications, must take this into consideration

**applications are in a stopped state when they are first installed but have not been launched*