MAC Motivation

Prevent users from disclosing sensitive information (whether accidentally or maliciously) e.g. classified information requires such protection

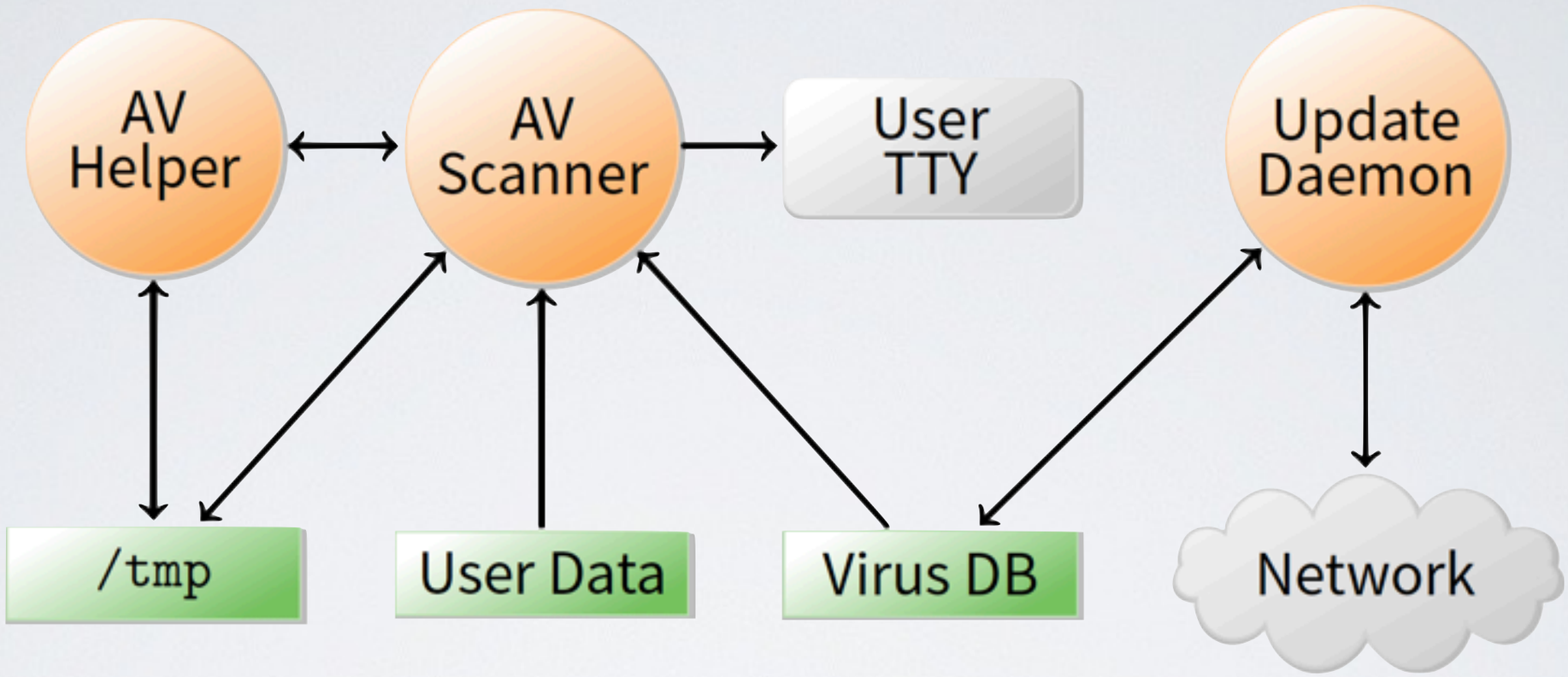
Prevent software from surreptitiously leaking data - seemingly innocuous software may steal secrets in the background (Trojan Horse)

Case study - Symantec AntiVirus 10

- Inherently required access to all of a user's files to scan them
- Contained a remote exploit (attacker could run arbitrary code)

➡ Can an OS protect private file contents under such circumstances?

Example - anti-virus software



How can OS enforce security without trusting AV software ?

- Must not leak contents of your files to network
- Must not tamper with contents of your files