➡ Historic anti-virus - signature based detection

➡ Heuristics and behavioural based detection

- Implemented as an extension to the kernel often with user-space components

- Passive or Active mode, event logging and streaming

- Often featuring a cloud component for incident investigation and security overview

➡ Still software hence can be contain vulnerabilities

Endpoint Protection

Endpoint Protection

- Historic anti-virus - signature based detection
- Heuristics and behavioural based detection
- Implemented as an extension to the kernel often with user-space components
- Passive or Active mode, event logging and streaming
- Often featuring a cloud component for incident investigation and security overview
- Still software hence can be contain vulnerabilities

Endpoint Protection