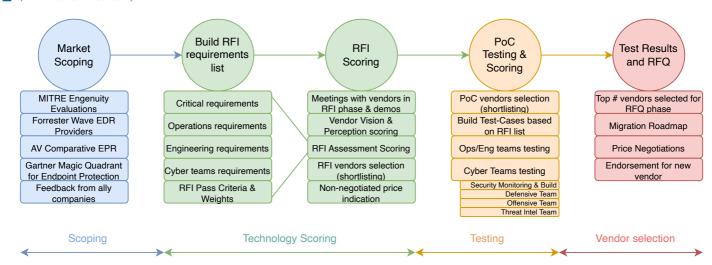
## **Unified Endpoint Protection (selection process)**

simple guide for anyone by Martin Holovský





- Find key players on the market
- See their portfolio and company fit
- Ignore results from paperwork tests (e.g. Gartner)
- · Ask for recommendations from ally companies, especially what does not work well
- · Define scope of what "endpoint" is:
  - Desktops
  - Servers
  - Mobile
  - Containers

  - Corp Owned / BYOD

- Invite all relevant teams (Desktop, Servers, Containers, Mobile, ...)
- Define all your expectations from product
- · Set importance/weight of each requirement
- Define scoring mechanism
- · Meet vendors and ask for demo
- subjective opinions matter as well
- Review past ~2Y of product development
- Ask for a Roadmap session
- · Check feature parity
- · Estimate ability of each vendor to deal with advanced threats 2Y from now

Often you can recognize top players just from demos, but assess their architecture as well-

- Pick top # for PoC phase
- Build Test environments and isolated env for Security testing
- · Red Team testing is vital, try to bypass detection and protection mechanisms
- Test as much as possible from RFI as reality is often different
- · Execute each test-case for each platform, ideally same test-case by same person to spot differences
- · Subjective scoring is valid as well
  - · Clarity of information
  - Level of customization
  - Platform UI/UX

- Run RFQ to have solid price
- Summarize scoring
  - PoC results
    - Vision & Strategy
    - Price
- Decide on final vendor
- · Plan migration