filename:comptia-secplussy0601-4-6-1-host-security-endpoint-protection
Showname: Security+ (SY0-601)
Topic: Implementing Security
Episode: Host Security - Endpoint Protection
Learner Objectives:

Given a scenario, implement host or application security solutions.

Description: In this episode, the viewer will identify common technologies that assist companies in endpoint protection such as antivirus, anti-malware, host-based intrusion detection and prevention systems, host-based firewalls as well as next-generation firewalls.

- Antivirus and Anti-malware
    - Signatures/definitions
    - Behavior monitoring
    - Heuristics and AI
    - Cloud-based submissions
    - Sandboxing vs. quarantining
- Endpoint Detection and Response
    - Endpoint threat detection
    - Monitoring endpoint behavior
        - Real-time
    - Uses IoCs
    - Examples
        - Fireye EDR
        - Datashield EDR
- DLP
- HIDS/HIPS
- Host-based Firewalls

- NGFWs