

# COURSE: SECURITY+ SY0-401

---

## MODULE 4: APPLICATION, DATA AND HOST SECURITY

- Given a scenario, select the appropriate solution to establish host security
- Implement the appropriate controls to ensure data security
- Compare and contrast alternative methods to mitigate security risks in static environments

- Operating system security and settings
- OS hardening
  - Anti-malware
  - Antivirus
  - Anti-spam
  - Anti-spyware
  - Pop-up blockers
- Patch management
- White listing vs. black listing applications



- Trusted OS
- Host-based firewalls
- Host-based intrusion detection
- Hardware security
- Cable locks
- Safe
- Locking cabinets
- Host software baselining

- Virtualization
  - Patch compatibility
  - Host availability/elasticity
  - Security control testing
  - Snapshots
  - Sandboxing



The screenshot shows the configuration interface for a virtual machine named "Windows XP Pro". It includes several sections: "Devices" with a list of hardware components and their settings; "Description" with a text input field; and "Virtual Machine Details" with state, configuration file, and hardware compatibility information. A large black rectangular area on the right side of the window is currently blank.

**Windows XP Pro**

- ▶ Power on this virtual machine
- ⚙ Edit virtual machine settings
- 🔄 Upgrade this virtual machine

▼ **Devices**

Memory	1 GB
Processors	1
Hard Disk (SCSI)	40 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	Bridged (Autom...
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

▼ **Description**

Type here to enter a description of this virtual machine.

▼ **Virtual Machine Details**

**State:** Powered off  
**Configuration file:** C:\VM\WinXP\Windows XP Pro.vmx  
**Hardware compatibility:** Workstation 9.0 virtual machine

- Cloud storage
- SAN
- Handling Big Data
- Data encryption
  - Full disk
  - Database
  - Individual files
  - Removable media
  - Mobile devices



- Hardware based encryption devices
  - TPM
  - HSM
  - USB encryption
  - Hard drive
- Data in-transit, Data at-rest, Data in-use
- Permissions/ACL
- Data policies
  - Wiping
  - Disposing
  - Retention
  - Storage

## Environments

- SCADA
- Embedded (Printer, Smart TV, HVAC control)
- Android
- iOS
- Mainframe
- Game consoles
- In-vehicle computing systems





- Methods
  - Network segmentation
  - Security layers
  - Application firewalls
  - Manual updates
  - Firmware version control
  - Wrappers
  - Control redundancy and diversity



# THANK YOU

---