VMware Security Recommendations and Best Practices

VMware Security Recommendations and Best Practices

On this page:

Overview

We strongly recommend treating each virtual machine as if it was a physical machine for most activities. Virtual machines are vulnerable to most of the same things as physical machines including data loss/corruption, hardware failures, viruses, and hackers. Install and use virus scanning software. Take regular updates to your operating system, preferably via an automatic update system. Make regular backups of important data. Follow the recommended best practices for your guest operating system. In most cases, simply treat your virtual workstation as you would any other machine.

Security Recommendations

We strongly recommend you treat each virtual machine as though it is a real machine for the purposes of security.

1. Install Anti-Virus Software
   While MIT does its best to prevent virus attacks, no computer is immune to them. Anti-virus software needs to be installed separately on the Virtual Machine, even if virus protection is already installed on the Macintosh operating system itself. For more information about virus protection, distributed by MIT at no cost. Sophos, the software distributed and supported by IS&T, includes protection against viruses, Trojans, worms and spyware, as well as adware.
2. While virus protection software offers some protection from spyware, we recommend using Windows Defender on your Windows virtual machines for additional protection. Defender is included with Windows. To find it, click on the Start button and type "Defender" in the search box.
3. Choose Strong Passwords
   Weak passwords can be guessed, thus giving someone else access to your files and your system. Create passwords that are at least eight characters long, containing numbers, upper and lower case letters, and symbols. More information on creating strong passwords can be found at Strong Passwords
4. Keep your Operating Systems Updated
   It is equally important to keep your host and virtual operating systems updated as compromises can occur in either kind of system. Install operating system security updates to keep your system current and protected from known vulnerabilities. We strongly recommend utilizing automatic updates, but note that virtual systems can only take updates when they are running. If your virtual system has not been started in some time (or is rarely left running long enough to take an update), we recommend you run a manual update as soon as you start your virtual system. For more information, see: MIT Windows Automatic Update Service, Red Hat Network.
5. Maintain Like Risk Postures for All Machines (Virtual and Host)
   Your system is only as secure as the least secure virtual or host machine. All guests on a host machine should have like risk posture - same level of accessibility, data sensitivity and level of protection. If any guest is more vulnerable than other guests or your host, it could be an entry to compromise the rest of your system.
6. Limit Host Access
   Access to the host should be limited (firewalled off).
7. Snapshots of Virtual Machines
   When taking a snapshot of a virtual machine and then branching off, make sure to save the image at the instance before the branch (the trunk) rather than at the branch level to ensure security patches are most up to date.

Best Practices

- Don't register a virtual machine for DHCP on wireless.
- When copying or backing up a VM image:
    1. Make sure the virtual machine is powered off.
    2. Do not copy the lockfile directory (the only subdirectory that ends in ".lck").
- When restoring from backup use move, not copy. This prevents issues with duplicate Mac Addresses on the same network.

- Treat each VM as a standalone computer for security purposes. Install virus scanning software. Take regular OS updates.
- Enable "Time synchronization between the virtual machine and the host operating system" via the VMware Tools installed on the virtual machine.
- Networking: use NAT Networking. This should be the default setting for your virtual machines.
  Advanced users, particularly running Linux guests, may discover they want or need to deal with the additional complexity of setting up a Bridged network interface.
- Carefully plan your disk allocations. Do not over-allocate your disk. It is dangerous to tell VMware to make images that, if they all grew to their full size, would take up more disk space than you have free. If this happens, VMware may pop up an alert warning you when you're about to use up more space than you have. That would give you a chance to free up disk space or exit cleanly. We don't recommend relying on the warning. There's no guarantee it will appear before bad things (data loss or corruption) happen.

Backups

The importance of backing up your data cannot be stressed enough. Virtual machines are at just as much risk, if not more, for data loss due to hardware failure, file corruption, system compromise, and other events. If data loss happens, a backup can make a world of difference in recovering from such an event. How you use your virtual machine (VM) will determine the best way to do backups for your VMs.

1. You have important software/data in the VM (research, data, etc):
   Install Code42/CrashPlan within your virtual machine and have it run regular backups of the data within your virtual machine. This method does not preserve your virtual machine, just the data within it. For more information on using Code42/CrashPlan for virtual machines, see: Code42/Crashplan Backup Accounts
2. Your VM is an appliance:
   We recommend that the system administrator manually makes backups. This preserves both the virtual machine and your data within it. Simply, drag and copy the VM somewhere (e.g., an external drive). Exclude your VM files from regular backups via Code42/Crashplan. See items 2 and 3 below for reasons. For more information, see: Q. I want to make a backup/copy of my virtual machine. What is the best way to do so?

Things to note regarding virtual machine backups:

- A virtual machine image is actually comprised of several files. All of those have to be in sync or behavior is erratic.
- From outside the virtual machine (host machine), if a backup is made when the virtual machine is running, the results are inconsistent. Backup your virtual machine files on the host machine when the virtual machine is not running.
- To backup virtual machines using Mac OS X 10.5's Time Machine, users will need to be running Mac OS X 10.5.2 or later. When backed up using Time Machine, virtual machines are duplicated and may take up considerable space on your backup drive.

Security Risks Specific to Virtual Machines

While virtual machines are at risk of all the same things as any other machine, you should be aware of a few additional issues.

1. If a host is compromised, scripts can be run on the host that can interact with the guest at whatever privilege level the guest is logged in as. This can result in malicious trojans being installed on the host and guest machines.
2. A virtual machine that is not virus protected, compromised, and in a shared networking configuration can be used by an attacker to scan both the private and public address spaces. The other virtual machines on the host (if not patched) can also be exploited via the network, so a software firewall on each of the guests is recommended.
3. (Enterprise version) When turning on shared folders, they can be accessed through a compromised guest. Files can then be placed on the host and attackers can access other guests' file systems.