SOPHOS

Security made simple.

Sophos for Virtual Environments

Startup guide -- Sophos Central edition

Product version: 1.0

Contents

1 About this guide

This guide tells you how to:

- Use Sophos for Virtual Environments to provide central threat protection for virtual machines (VMs) in a VMware ESXi or Microsoft Hyper-V environment.

- Use Sophos Central to manage Sophos for Virtual Environments.

If you are migrating to Sophos for Virtual Environments, see Migrate to Sophos for Virtual Environments (page 28).

If you want to use Sophos Enterprise Console instead of Sophos Central, see *Sophos for Virtual Environments Startup guide -- Enterprise Console edition*.

2 About Sophos for Virtual Environments

Sophos for Virtual Environments is a security system that protects VMs. It works like this:

- You put one or more installations of **Sophos Security VM** on each host. The Security VM can then detect and block threats on the guest VMs.

- You must put a **Sophos Guest VM Agent** on each guest VM.

- You use **Sophos Central** to manage the Security VMs.
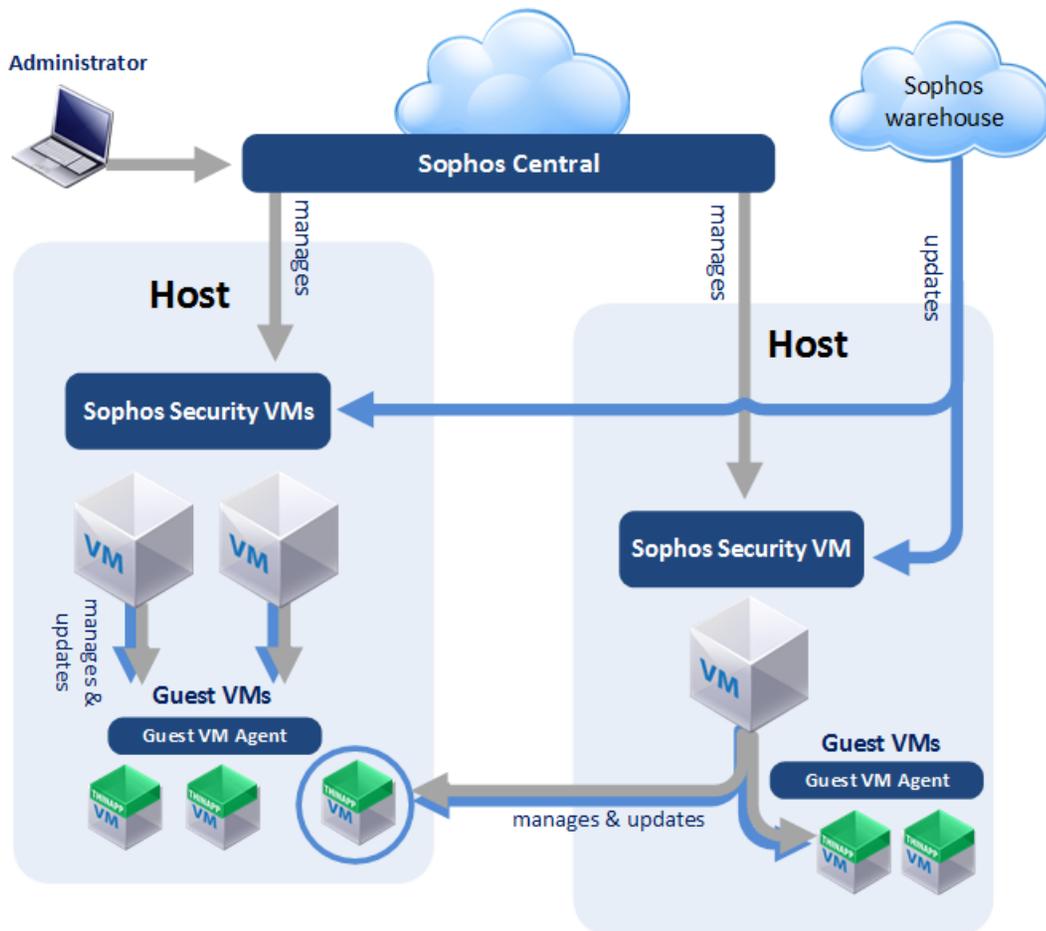
Which environments can Sophos be used in?

Sophos for Virtual Environments can protect VMs in a VMware EXSi environment or a Microsoft Hyper-V environment.

Which guest VMs can be protected?

The Sophos Security VM can protect guest VMs that run Windows operating systems. For full details, see Guest VM requirements (page 10).

Note: The Security VM can protect guest VMs that are on a different host.

How does scanning work?

When a guest VM tries to access a file:

- The Sophos Guest VM Agent running on the VM notifies the Sophos Security VM.

- The Security VM scans the file.

- If the Security VM detects a threat, access to the file is blocked, and the Security VM sends an alert to Sophos Central.

The Security VM can also perform a full scan of all the guest VMs. You can run this scan immediately or schedule it.

The file scanner uses intelligent caching to retain the results of previous scans. This helps improve overall performance when there are many connected guest VMs or when the same file is accessed repeatedly.

How is the Security VM managed?

Sophos Central displays the status of the Security VM, including how up to date it is and whether it has detected any threats.

Sophos Central also enables you to configure scanning by means of a policy.

How do you deal with threats?

The Security VM provides the ability to clean up threats automatically. For more information, see Clean up a threat (page 24).

How is the Security VM updated?

The Security VM receives fetches and installs updates automatically from Sophos.

How is the Guest VM Agent updated?

The Guest VM Agent is updated automatically.

The agent doesn't scan files, so it doesn't need updated threat identities. However, it does get updates when we improve the product.

The Security VM receives these product updates from Sophos and applies them to the guest VMs.

Updates are staggered to minimize the load on the Security VM and the underlying hypervisor host.

3 Key steps in installation

Installation involves these key steps, which are described in the sections that follow:

- Check the system requirements.
- Uninstall other anti-virus products.
- Install the Sophos Security VM.
- Install the Sophos Guest VM Agent on guest VMs.
- Check that guest VMs are protected.

4 Check the system requirements

This section tells you the system requirements and how to check that you comply with them.

It also tells you about any information (such as computer details) that you should gather now so that you will have it available when you install a Security VM.

It covers requirements for both VMware EXSi or Microsoft Hyper-V environments.

4.1 VMware requirements

This section shows you the software you need in a VMware environment.

4.1.1 VMware ESXi host

You should install the following on each host that will run a Sophos Security VM:

- VMware ESXi host 5.5, 6.0, or 6.5.

Note: We recommend that you configure the host to get updates from VMware.

Hardware requirements

The VMware ESXi host must be able to allocate the following resources for each Sophos Security VM:

- 2 CPUs.
- 20 Gb disk space.
- 4 Gb RAM.

Notes

You should not place a CPU resource limit on the Sophos Security VM.

By default, 2 CPUs are allocated. If you have many guest VMs to protect, you can configure more CPUs after you install the security VM. This guide tells you how.

The Security VM reserves memory. High-availability and load-balancing systems make automatic choices based on resource reservations for the VMs in your VMware environment. You should not remove the Security VM memory reservation.

4.1.2 VMware vCenter and vSphere

You require the following vCenter and vSphere software.

Software	Version	Notes
vCenter	Version 5.5, 6.0, 6.5	You will also need: The network address. An administrator account.
vSphere Client	Version 5.5, 6.0, 6.5	

4.1.3 VMware Tools

We recommend that you use VMware tools on Guest Virtual Machines because they can improve performance.

4.2 Microsoft Hyper-V requirements

This section shows you the software you need in a Microsoft Hyper-V environment.

The Microsoft Hyper-V system should be one of the following:

- Hyper-V in Windows Server 2012 (Core, full)
- Hyper-V in Windows Server 2012 R2 (Core, full)
- Hyper-V in Windows Server 2016 (Core, Server with Desktop Experience)

Microsoft Hyper-V integration components

The Microsoft Hyper-V integration components will install automatically if Windows updating is enabled and works successfully. Without these tools your VM performance maybe degraded.

Guidelines for anti-virus for Microsoft Hyper-V

Microsoft publish guidelines for how to secure your Hyper-V server most effectively. See Microsoft KBA 3105657.

4.3 Guest VM requirements

Guest VMs should run one of the operating systems listed here.

Operating system	Service packs	Comments
Windows 10 (32 and 64-bit). Knowledge base article 125679 lists all supported versions.		Windows and Hyper-V containers not supported.
Windows 8.1 (32 and 64-bit)	---	
Windows 7 (32 and 64-bit)	SP1+	
Windows Server 2016 (64-bit)		Windows and Hyper-V containers not supported.
Windows Server 2012 R2 (64-bit)	---	
Windows Server 2012 (64-bit)	---	
Windows Server 2008 R2 (64-bit)	---	

4.4 Network requirements

The infrastructure requirements are:

- The Security VM and guest VMs need to share a network connection. Ideally this should be a high-speed LAN with no network traffic throttling.

- The network traffic between Security VM and guest VMs should not be blocked by firewalls or network access controllers.

4.4.1 NAT networks requirements

If you have guest VMs inside a NAT (Network Address Translation) network, you can protect them with a Security VM inside or outside of that network.

During installation you must configure the Security VM with the following:

- a primary IP address outside of the NAT (this address must be able to communicate with the management console)

- and a secondary IP address that is within the NAT.

4.4.2 Subnets

You can configure the Security VM with up to five IP addresses. Each IP address must be on a different subnet.

4.5 Sophos management requirements

Before you can protect and manage your VMs, you need:

- A Sophos Central account.

5 Uninstall other anti-virus products

You should uninstall any anti-virus products, **including Sophos products**, that are already installed on your guest VMs.

You need to disable Windows Defender on server platforms where the security center is not present. We recommend that you do this using a group policy.

You cannot use Sophos for Virtual Environments to protect guest VMs that run other anti-virus products. If you try to do this, there may be reduced performance or a system deadlock in which the guest VM stops responding.

This limitation also applies to VMs with Sophos gateway or server products that include or require anti-virus components.

For more information, see knowledgebase article 125679.

6 Install the Sophos Security VM

You can install one or more Security VMs on each host where you want to protect guest VMs.

Before you start, make sure the host meets the system requirements. We also recommend that you configure the host to get updates from VMware.

Installation involves these steps, which are described in the sections that follow:

- Check that you have the passwords you need.
- Check that the systems are synchronized.
- Download the installer.
- Install the Security VM.
- Check that the Security VM is installed.

6.1 Check that you have the passwords you need

When you run the Security VM installer, you need to enter certain passwords. You should make sure that you have the passwords for the following accounts:

- The Sophos Central account.
- If you're in a VMware environment, the vCenter Administrator account.

6.2 Check that systems are synchronized

You must ensure that the time is synchronized on the host where you install the Security VM, and on the guest VMs.

You can use NTP (Network Time Protocol) synchronization for each host.

⚠ **Warning:** If the time is not synchronized, you can install a Security VM but you cannot manage it from Sophos Central.

6.3 Check the installer requirements

Check that the computer and user account you're going to use meet the requirements.

- The installer must be on a Windows computer that has access to your VMware vCenter or Microsoft Hyper-V server over the network.
- Installation of the Security VM must be done on the local network. The installer does not currently support the use of a proxy.
- The installer cannot be used on a Windows XP or Windows Server 2003 computer.

- If you use Microsoft Hyper-V, you must run the installer as a user with rights to create and control VMs on the Hyper-V server. This can be a local user account on the Hyper-V server or a domain user.

The computer where you put the installer is used only for installation. It is not used for management or protection of your Security VM or guest VMs after installation.

6.4 Download the Sophos Security VM installer

You download the installer from Sophos Central (if you have not already done this).

The following steps assume that you have a Sophos Central account.

Notes:

- You can download the installer at any computer and then copy it to the computer where you will use it.

- The installation instructions in later sections tell you which computer or computers you should use the installer on.

To download the installer:

1. Log in to Sophos Central.
2. Go to the **Protect Devices** page.
3. Under **Virtual Environment Protection**, click the link to download the installer for your environment (Hyper-V or ESXi).

After you install the Security VM, you will be able to get the Sophos Guest VM Agent from a public share on the Security VM.

6.5 Install the Security VM

To install a Security VM, you need the Sophos Security VM installer. If you haven't downloaded it yet, see Download the Sophos Security VM installer (page 15).

Make sure the computer and account you use meet the requirements (page 14).

Some installation steps apply only to VMware ESXi or only to Microsoft Hyper-V. These are indicated at the start of the step.

1. Double-click the installer.

   A wizard runs to guide you through the installation.

2. Accept the license agreement.
3. At the welcome page, click **Install** to extract the installation files to a folder on your computer.
4. Check that you have installed all the **Prerequisites for installation**.
5. **Only if you're in a VMware ESXi environment:**

   In **VMware vCenter credentials**, enter your details and a name for the Security VM.

   Note: Enter the administrator username in the form you use to log in to vCenter using vSphere Client. In other words, with or without the domain prefix, as required, and with the same capitalization.

6. In **ESXi host** or **Hyper-V host name**, specify the host on which you want to install the Security VM.

7. In **Management console**, select **Use Sophos Central**.

8. Enter your **Sophos Central account details**:

   a) Enter the email address and password you use when you log in to Sophos Central.

   b) Enter details of the proxy server used to connect to Sophos Central (if applicable).

9. Create a **Password for access** to your Security VM.

   You need this password in order to view your protected guest VMs. You also need it if you want Sophos Technical Support to troubleshoot your installation remotely. They will use it to collect logs, which you can review and send to Sophos if required.

10. Select the **Timezone** that the Security VM will use to schedule scans.

11. **Only if you're in a VMware ESXi environment**:

   In **Datastore for the Security VM**, select the type of datastore on which you want to install the Security VM.

   Note: The Security VM protects guest VMs even if their templates are stored in different datastores.

12. In **IP settings for the Security VM**, enter the IP settings for all the networks where you want to protect guest VMs. One Security VM can protect VMs on multiple networks.

   a) In **Select virtual LAN** (ESXi) or **Select vSwitch** (Hyper-V), select from those available.

   b) Enter the **Static IPv4 address**. You can only use static addresses.

   c) Enter the **Subnet mask**.

   d) Enter the **Domain suffix**.

   e) Select **Make Primary** if this is the network that should have access to the Sophos management console. You can only have one primary network.

   You can use the "+" button above the fields to add another network. The "-" button removes a network. The "<" and ">" buttons let you move between your settings for different networks.

13. In **Gateway and DNS server details for the primary network card**, enter details that will enable the Security VM to communicate with the management console and download updates.

   Note: You can enter one DNS Server or, optionally, two.

14. **Only if you're in a Microsoft Hyper-V environment:**

   In **Disk image location**, specify a location for the Security VM disk image. This can be a network share or a local folder on the host.

15. At the **Summary of installation** page, you can see full installation details. Click **Install**.

16. At the **Finished** page, you can see whether the installation of the Security VM was successful. If there was a failure, check the log for details.

   Tip: You can click **Start Over** to run another installation or try again if there was a failed installation.

17. The **What to do next** page tells you how to configure the Security VM and protect guest VMs.

Follow the instructions in the next section to check that you can see the Security VM in Sophos Central.

⚠️ **Warning:** Don't "suspend" the Security VM. If you do, communications with the management software will not be able to resume later.

6.6 Check that the Security VM is installed

This section tells you how to check that the Security VM is installed and has the resources it needs.

Check that you can see Security VM

When the security VM has been installed, go to Sophos Central.

You can see security VMs in the **Servers** page in Sophos Central. Look for "Sophos Security VM" in the "Name/OS" column.

To see only the Security VMs, select **Virtual servers** in the list filter.

Check whether you need to configure resources

Usually you do not need to configure resources for the Security VM. Note that:

- **If you have a large number of guest VMs** on a single host, ensure that the Security VM has enough processing power for scanning. See Appendix: Add CPUs to the Security VM (page 29).

- **The installer reserves memory for the Sophos Security VM.** In a VMware environment, high-availability and load-balancing systems make automatic choices based on resource reservations for the VMs, so these choices could be different after you install the Security VM. You should not remove the Security VM memory reservation.

7 Install the Sophos Guest VM Agent

The Sophos Guest VM Agent must be run on each guest VM that you want to protect.

Check which operating systems you can install the Guest VM Agent on. See Guest VM requirements (page 10).

1. On the guest VM, browse to the host where the Security VM is installed. You must use the IP address.
2. In the **Public** share, find the installer **SVE-Guest-Installer.exe**
3. Double-click the installer to run it, or transfer the installer to the guest VM and run it. Follow the on-screen instructions. Alternatively you can:

   - Use the command line. You can choose to install with (limited UI) or without (no UI) a progress bar being displayed to indicate the progression of the installation. The commands are case sensitive. Enter either:

     Limited UI: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /passive`

     No UI: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /quiet`

   - Use Group Policy deployment. For details, see this Microsoft article: http://support.microsoft.com/kb/816102

We recommend that you snapshot the guest VM after installing the agent. This will allow you to revert the guest VM safely later if you need to.

8 Check that guest VMs are protected

This section tells you how to check that your guest VMs are protected. You can:

- Check the protection settings on a guest VM.
- Test on-access scanning on a guest VM.
- Troubleshoot on-access scanning.

8.1 Check the protection settings

To check that a guest VM is protected:

1. Go to the guest VM and search for **Security and Maintenance** from the Start menu. If this option is not found search for **Action Center**.

   Attention: If neither of these options are found then the guest VM does not provide Windows Security Center. You must check whether the guest VM is protected using the steps described in Test real-time scanning (page 19).

2. Click the drop-down arrow beside **Security**. You should see that Sophos for Virtual Environments is enabled.

   Note: If it is not enabled, see Troubleshoot real-time scanning (page 20)

8.2 Test real-time scanning

Real-time scanning is your main method of protection against threats. When you open, write, move, or rename a file the Security VM scans the file and grants access to it only if it does not pose a threat. When you run a program the Security VM scans the executable file and any other files it loads.

Important: Ensure that Sophos Endpoint for Windows is *not* installed on any guest VMs that are protected with a Security VM.

To check that a security VM is scanning files on access:

1. Go to eicar.org/86-0-Intended-use.html. Copy the EICAR test string to a new file. Give the file a name with a .com extension and save it to one of the guest VMs.
2. Try to access the file from the guest VM.
3. Log in to Sophos Central.

   - **If you have automatic cleanup on**, go to the **Servers** page and click the Security VM to open its details page. On its **Events** tab, you should see that EICAR has been detected and cleaned up.
   - **If you don't have automatic cleanup on**, look at the **Alerts** page. You should see an alert on the Security VM. EICAR has been detected but not cleaned up.

If EICAR has not been detected, see Troubleshoot real-time scanning (page 20). If EICAR is not cleaned up, simply delete it.

8.3 Troubleshoot real-time scanning

If real-time scanning is not working:

1. Ensure that real-time scanning is enabled in the server policy applied to the Security VM:

   a) In Sophos Central, go the **Servers** page, find the Security VM and click on it to display its details.

   b) In the **Summary** tab, under **Summary**, you can see the Threat Protection Policy applied to the server. Click the policy name.

   c) In the policy, find the **Real-time scanning** section. Ensure that **Scan** is enabled.

   d) Check that the Security VM is compliant with the policy.

2. Ensure that the guest VM is protected. Go to the Security VM host and look in the log file, see View protected guest VMs (page 21).

3. Ensure that Windows Security Center shows the guest VM as protected by Sophos for Virtual Environments.

4. Check that there are no pending restarts requested by Microsoft updates. These can prevent installation of the Sophos Guest VM Agent from being completed.

5. Check that aren't any other anti-virus products installed. On server platforms where the security center is not present check that Windows Defender isn't active. Remember that you cannot use Sophos for Virtual Environments to protect guest VMs that run other anti-virus products.

6. If on-access scanning is still not working, contact Sophos Technical Support.

9 View protected guest VMs

You can view all guest VMs that are protected by a Security VM.

1. Browse to the Security VM. You must use Windows Explorer and you must use the IP address.
2. Double-click the **Logs** share.
3. When prompted, enter your credentials:

   - Username is "Sophos".
   - Password is the access password you set when you installed the Security VM.

4. Open **ProtectedGVMs.log** to view the protected guest VMs.

   Note: The ProtectedGVMs.log file only appears when the Security VM starts protecting guest VMs.

10 Scan guest VMs

The Security VM always scans files on access, that is, when they are opened and closed.

The Security VM can also perform a full scan of all guest VMs. You can either run a scan immediately or at set times.

The full system scan detects but doesn't clean up threats.

Note: The Security VM staggers scans so that the host is not placed under a high load. By default, two guest VMs are scanned at a time. Therefore, it may take longer for the scanning of all guest VMs managed by the Security VM to complete.

Scan guest VMs now

To run a full scan of all the guest VMs immediately:

1. Log in to Sophos Central.
2. Go to the **Servers** page.
3. Find the Sophos Security VM and click on it to open its details page.
4. In the left pane, click **Scan Now**.

Scan guest VMs at set times

To run a full scan of all the guest VMs at set times:

1. Log in to Sophos Central.
2. Go to the **Servers** page.
3. Find the Sophos Security VM and click on it to view its details page.
4. On the **Summary** tab, look under **Summary** for the Threat Protection policy that applies. Click on it to edit it.
5. In the policy, go to the **Scheduled scanning** section. Enable scanning and specify the times when the scan will be run.

11 What happens when a threat is detected

If the Security VM detects a threat on one of the guest VMs, it:

- Blocks the threat.

- Attempts to clean up the threat automatically.

- Sends an alert to Sophos Central if you need to take any action.

Note: The Security VM does not automatically clean up threats detected during a full scan of all guest VMs.

What you see in Sophos Central

Sophos Central:

- Shows that the threat has been blocked. See the **Events** tab of the Security VM's details page.

- Displays an alert in the **Alerts** page. This shows what the threat is, which VM it is on, and whether it is cleanable.

- Removes the alert if automatic cleanup is successful.

If automatic cleanup is not available or is not successful, an alert in the **Alerts** page prompts you to clean up manually.

For more information on cleanup, see Clean up a threat (page 24).

What the user sees on the guest VM

If the Security VM detects a threat when a user tries to access a file, a message may be displayed on the guest VM informing the user that the file cannot be accessed. This depends on the application used to access the file.

12 Clean up a threat

This section describes both automatic and manual cleanup of threats.

For information about a threat and advice on cleanup, log in to Sophos Central, go to the **Alerts** page, look for the threat alert, and click on the threat name.

Automatic cleanup

The Security VM automatically cleans up threats it detects.

Note: Automatic cleanup is not available on CDs, read-only file systems and media or on remote file systems.

Manual cleanup

You can clean up a guest VM manually.

To clean up manually, you restore the guest VM. Note that you may lose data (see details below).

Use one of these methods:

- Delete the guest VM and reclone it from the template image. You will lose your data.

- Revert the guest VM to the previous known clean snapshot. You will lose data added since the taking the snapshot.

Whichever method you use, run a full scan of the guest VM afterwards to ensure that it is clean.

13 Maintain the Security VM

This section gives advice on post-installation and maintenance tasks.

- **You must power on the Security VM manually whenever the host is taken out of maintenance or standby mode.** Do this before you power on the guest VMs, so that the guest VMs are protected immediately.

- **Don't "suspend" the Security VM.** If you do, communications with the management software will not be able to resume later.

- **Verify that the Security VM is receiving security updates from Sophos.** You can do this by checking its update status in Sophos Central.

- **Backups.** We recommend that the Security VM is excluded from regular backup tasks, as this can degrade its performance. If the Security VM needs to be recovered due to infrastructure failures, we recommend you redeploy the Security VM.

14 Uninstall the Security VM

To uninstall a Security VM, you delete it.

Before you start, ensure that guest VMs will continue to be protected. Go to the Security VM and View protected guest VMs (page 21). Then move guest VMs to another Security VM with similar policy settings.

To move your guest VMs:

1. Uninstall the Guest VM Agent, see Uninstall the Guest VM Agent (page 27).
2. Reinstall the Guest VM Agent with the new Security VM IP address, see Install the Sophos Guest VM Agent (page 18).

Once you have moved your guest VMs you can delete the Security VM. To do this:

1. Go to your hypervisor.
2. Power down the Security VM.
3. Delete the VM.

15 Uninstall the Guest VM Agent

You can uninstall the Guest VM Agent from Control Panel.

1. On the guest VM, open **Control Panel**.
2. Click **Programs and Features**.
3. Select these features and click **Uninstall**:

   - Sophos for Virtual Environments

   - Sophos Guest VM Scanning Service

   - Sophos Virus Removal Tool.

16 Migrate to Sophos for Virtual Environments

Which products can I migrate from?

You can migrate to Sophos for Virtual Environments from these products.

- Sophos Anti-Virus for vShield in a VMWare ESXi environment
- Sophos Anti-Virus running locally on each guest VM in either a VMware ESXi environment or a Microsoft Hyper-V environment
- Other vendors' anti-virus products in either a VMware ESXi environment or a Microsoft Hyper-V environment

Note: Sophos for Virtual Environments protects guest VMs on a VMware ESXi host including when running in a NSX environment. However, Sophos for Virtual Environments does not integrate with the NSX manager. You should not install any anti-virus software to run on NSX as this will impact performance and could cause deadlocks.

Note: Sophos for Virtual Environments uses a Security VM to provide central threat scanning. Once you install this, guest VMs no longer need threat data updates.

How do I migrate?

Follow the steps below. You can find more details on each step in this guide.

Note: If you're migrating from third-party anti-virus software, be aware that:

- Sophos for Virtual Environments requires network connectivity between the Security VM and guest VMs.
- Sophos for Virtual Environments supports dynamic VM load balancing technologies like vMotion and Live migration, but performance is best if high speed network connectivity between the Security VM and guest VMs is maintained.

To migrate:

1. Install a Security VM.

   Note: This new Security VM can be on the same host as an existing SAV vShield Security VM.

2. Go to your management console and verify that the Security VM is successfully updating.
3. Shut down the old Security VM or uninstall your old anti-virus software.

⚠ **Caution:** Your guest VMs will become unprotected so please ensure their security.

4. Install the new lightweight Sophos Guest VM Agent.
5. Verify, as described in this guide, that all guest VMs are now protected.

17 Appendix: Add CPUs to the Security VM

If you have many guest VMs on a host, you should ensure that the Security VM has enough processing power to scan the files they use when they all start up.

To do this, add more CPUs for the Security VM. You can do this any time.

Depending on the type of load, adding CPUs can also improve overall system performance.

Add CPUs in VMware ESXi

Add CPUs as follows:

1. Power off the Security VM.
2. In vSphere Client, select the Security VM.
3. Select **Edit Settings** > **Hardware** > **CPUs.** Then specify the number of CPUs.

Add CPUs in Microsoft Hyper-V

Add CPUs as follows:

1. Click **Start**, select **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the results pane, under **Virtual Machines**, select the Security VM.
3. In the **Action** pane, under the VM name, click **Settings**.
4. Click **Processor** and specify the number of processors.

18 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.

- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.

- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.

- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

19 Legal notices

Third-party licenses

For third-party licenses that apply to your use of this product, please refer to the following folder on the Sophos Security VM: `/usr/share/doc`.

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by following the instructions in knowledge base article 124427.