Domain Antivirus

Sophos Central

Jordan Brown

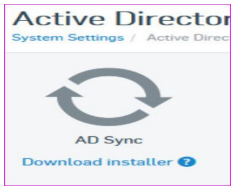
Overview

I am going to use Sophos as my antivirus for this project, first I am going to install Sophos on my secondary DC, then I am going to find a way to push out Sophos to at least one of my clients, and after everything is set up I am going to go through the list of Configuration of Sophos + Ransomware prevention.

AV Configuration

Initial setup

To set **Sophos Central** up I went to Sophos official website and found there Central edition, I installed it on my secondary DC, and completed the wizard using the defaults. Now we have to sync our AD with Sophos, go to your sophos centralized management console in the web browser, then go to **Global Settings > AD Sync Settings/Status**, and click on and then open the download installer located in Active directory sync.



Going through the **Sophos Cloud AD Sync Utility Setup** use all the defaults,
Click **next** agree to the **EULA** and click **next**, then **next** and **install.** Make sure "**Launch Sophos Cloud AD Sync Utility"** is checked then click **finish.**

When the **Sophos Active Directory Cloud Synchronization setup** window pops up read it then click **next**. Now inside the **Cloud Credentials** tab fill in the username and password you used to make your Sophos account with, then click **next**. In **AD Configuration *uncheck*** the **SSL Connection** leave the **host name or IP address** as is unless it is not there or isn't the right ip/hostname of your hosting server, Change the port number to **389** then bellow type in an admin username and password, and click **next**. Now in the **AD Domains** tab click **next**. In the **AD Filters tab** click **next.** Finally in the **Sync Schedule** tab leave the button on **Never** and click **finished**. Now a the new window will pop up click **Preview and Sync…** another new window will pop up called **Pending Changes** click **Approve Changes and Continue** and then **exit** to complete the syncing process.

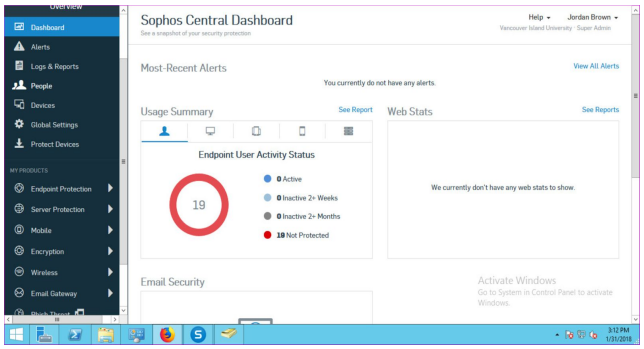
Deploying AntiVirus to Users

Go to **Protected Devices > Send Installers to Users** select all the users you wish to deploy the installer for, now once they check their email they should see a link to with instructions on how to install sophos AV (**Endpoint Protection**), this is only useful for small businesses as the administrator has to manually go through those emails and walkthrough the installer.

Sophos Central and Sophos Endpoint Interface

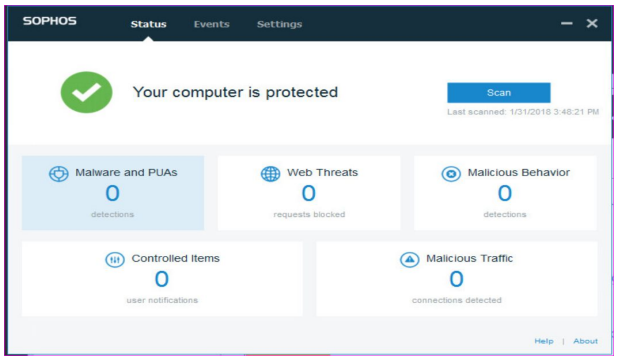
Sophos Central

Sophos Central has a large amount of features, the interface isn't the prettiest, but it's mainly built to be fully functional and responsive. There are so many features it comes with almost to many to look through. Sub categories into subcategories **Sophos Central** is filled with essential tools and comes compact with more tools you may not have thought you needed. Overall it's a great cloud management console built into the web.



Sophos Endpoint

Sophos Endpoint is an antivirus. If you have Sophos Central it can manage Sophos Endpoint. Mostly for users to look at the interface of Sophos Endpoint has a very nice color scheme and is very easy to use. With only 3 tabs for **Status**, **Events**, and **Setting** it makes navigation very easy; especially for the end user since they should only be able to use the first tab **Status**. Being very minimalistic and covering most aspects of an AV Sophos Endpoint does it's job well.



Ransomware Prevention

3rd party Ransomware simulator

For my 3rd party ransomware test I used **Ransim**, a ransomware simulator. It was the first link after searching for ransomware simulators or the download is down in resources. To use it you simply go through the setup and once it's set up click **run** and you should see a pile of notifications on your desktop or in the logs, since these issues are resolved by Sophos they aren't a threat so they won't appear under the **Alerts** tab just in the **logs & Reports** tab.

built in Windows Server 2012 method

Utilizing windows updates you are highly less vulnerable to ransomware then having not patched your machine (**FSRM** would not work for me). If you have to manually update your computer at least do it once a week on Tuesday as Tuesday is patch day for Windows.

Ways of Preventing and Removing Ransomware

Prevention

Be sure to backup your system or whatever it is you're protecting. Have a decent antivirus that can notice and take action to malware. Think before clicking\downloading links. Disable file sharing service, or remote services if you don't use them. Install browser extensions that help prevent ransomware. Always keep your firewall on and have it properly configured. Disconnect from the internet if you notice any suspicious activity. These are just a few ways key ways of preventing ransomware, there are so many iterations of ransomware that one way of preventing it will never work. Just be extra cautious and keep yourself up to date on new ransomware protection strategies and you will be fine.

Removal

In some cases ransomware can be easily removed, others they stick on your machine like super glue. Once you are infected by any sort of malware don't fret, there are over 100 ways of retrieving your system anew. Most antiviruses have features for removing ransomware, but if the ransomwares' malware is so powerful you can't even get past your computer's bios you may be in trouble; but there is a way. First figure out which key it is to get you to **Advanced Boot Options** then try a **System Restore,** which will completely roll back your windows, so this feature is last resort.

Tip: make sure you prevent ransomware sooner than later.

Review of AntiViruses used

Comodo Antivirus

Finding an msi download for Comodo antivirus was easy (Later I found out you can convert **exe** files into **msi** files with some third party programs), but when trying to set up the GPO for deploying it to my client I came to no success.

AVG Admin

At first I was using AVG Business Edition, but later found out it did not have a way I could find to push it out to clients without installing the agent on the clients themselves. So I tried **AVG Admin** Going through the install everything was well until coming to the part where you have to enter a license key, trying to find a license key I was to no avail as it was not in the email where they sent the download link to me nor anywhere online for free at least. **AVG Admin** did have a cool feature, if you have owned it before and the license expired you can just renew it very easily and worry free for a business owner.

ESET Endpoint Antivirus

After finding an msi version of ESET Endpoint You had to go through the process of making an account login, once you completed that you'd hit submit and have to wait for them to check if everything seemed right with your login info, that took about two days. Once I got the email for the download I tried setting up a GPO for it adding the share of the msi file for it, but this did not work. I tried installing it local and again ran into the same issue as AVG. It asks for a license key, which aren't free.

Avira Management Console

Avira Management Console Was easy to find and straightforward to install, but again with the GPO it failed. It came with three application files, **1** for console management, **2** an agent client for the client to connect with the main server, and **3** the frontend application used to configure the AMC (Avira Management Console). The only problem was they had no way of pushing out the agent application to clients so I had to use a GPO to deploy the application. What I first did was change the agent.exe file into a msi file using a third party application called **MSI Package Builder**, after creating the GPO I still came to no success which is a 0/3 rate with GPO.

Sophos Central

Sophos Central has incredible functionality resolving any refreshes and clicked links very quickly, it's customizable, and overall great for smaller businesses especially since its cloud based. That being said even though Sophos central works great in a smaller business environments. The product has way less efficiency than standard business AV's lacking in the deploying agents to clients department; however Since the assignment I am doing requires only one client this was the perfect AV to use and being cloud based is just the cherry on top. Overall after installation and deployment playing around with Sophos Centrals management features were enjoyable and worry free.

Summary

Overall this assignment was a great learning experience, I am now more knowledgeable of antiviruses and ransomware. The overall lab was a fairly smooth process, except when trying to figure out which antivirus I'd choose/which one would work as a domain wide antivirus, and the fact that FSRM would not work for me. All in all I now know Sophos inside and out.

References

-https://www.youtube.com/watch?v=zFC5kIa8ehw
-https://www.sophos.com/en-us/products/free-trials.aspx
-https://serverfault.com/questions/12516/what-is-the-best-antivirus-for-a-windows-domain-network
-https://en.wikipedia.org/wiki/Comparison_of_antivirus_software
-https://community.spiceworks.com/topic/405085-anyone-know-of-free-anti-virus-for-server-2012-r2
-https://community.sophos.com/kb/en-us/119265
-https://info.knowbe4.com/ransomware-simulator-tool-1chn
-https://www.pcworld.com/article/2084002/security/how-to-rescue-your-pc-from-ransomware.html
-https://community.spiceworks.com/how_to/128744-prevent-ransomware-by-using-fsrm
-https://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/
-https://www.starwindsoftware.com/blog/windows-server-2016-three-built-in-tools-to-protect-your-data-from-ransomware
-https://cloudblogs.microsoft.com/microsoftsecure/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
-https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips/
-https://www.theguardian.com/technology/askjack/2016/jul/28/how-can-i-remove-ransomware-infection