8

DETECTING, REMOVING, AND PREVENTING MALWARE

Malware such as viruses, trojans, and ransomware are significant threats to internet users and likely will be for the foreseeable future. As a result, it's important to arm yourself and your users with an antivirus solution that detects and removes malware. Additionally, keeping your endpoints up-to-date can prevent malware from infecting your network and in some cases provide more protection than an antivirus (AV) solution.

Antivirus solutions can be tricky to manage because they typically are not cross-platform (that is, they work on only one operating system). If you have multiple operating systems in your network, you'll need to find an effective AV product for each of them. Although this chapter discusses installing, configuring, and scanning with specific products, most options and settings will be the same across most antivirus solutions. The names of the settings and configuration options may differ slightly, but the same logic and processes should work for most products.

After exploring some antivirus solutions for various operating systems, we'll consider the differences between malware signatures and heuristic scans, the pros and cons of each approach, and the concept of creating an antivirus farm to catch as much malware as possible across different endpoints. Finally, we'll cover patch management for various operating systems and how best to keep your endpoints up-to-date.

Microsoft Defender for Windows

The latest iteration of the built-in Microsoft antivirus solution is *Microsoft Defender*. Defender automatically updates its virus definitions and scans for threats on a regular schedule, so Windows computers have decent protection out of the box.

Defender's automatic scans are *quick scans* that check only the folders where threats are commonly found. While a quick scan offers fast results and uses few system resources, it's unlikely to discover and remove malware residing outside of these folders. A *full scan* scans all your files and running programs, performing a thorough search for malware. It's recommended to run full scans somewhere between once a week and once a month. The longer the period between full scans, the more time an adversary has to wreak havoc on your systems.

You also have the option to choose custom and offline scans. A *custom scan* lets you select which folders and files to scan. An *offline scan* is similar to the Boot to Safe Mode method of malware removal available in earlier versions of Windows. Windows is now capable of automatically rebooting to a state that allows Microsoft Defender to remove persistent malware via this offline scan. This option is a last resort, rather than a scan you would run regularly. If you believe your computer is infected but are unable to find the infection using a full scan, run the offline scan to be certain. Failing this, your only recourse is to wipe your hard drive and re-install Windows from scratch.

To run scans, open **Settings ▸ Update & Security ▸ Windows Security ▸ Virus & Threat Protection**. Click **Scan Options**, select the type of scan you want, and then click **Scan now**.

In the Virus & Threat Protection4Manage Settings menu, ensure Real-time Protection is turned on to enable Defender to protect your computer constantly. You can also add file and folder exclusions from this menu. You might add exclusions when you have files or programs that are legitimate and not a risk to your system, but Defender classifies them as malware and tries to quarantine them anyway.

One setting in particular could be considered a risk to your privacy, Automatic Sample Submission, which allows Microsoft Defender to upload your files to Microsoft's servers in the cloud automatically to be analyzed and scanned for malware. This practice poses a risk: private or confidential data could be leaked to a third party without your knowledge, as Defender won't ask or advise you of files being uploaded to Microsoft. To turn off this setting, toggle Automatic Sample Submissions.

Related to this setting is the Cloud-Delivered Protection setting. This one isn't as risky, as it relays only file metadata to Microsoft rather than entire file contents. Cloud-Delivered Protection will still work with Automatic Sample Submission turned off, although it might not perform as well.

Windows will keep Microsoft Defender up-to-date, but it never hurts to update manually occasionally. To update, click **Check for Updates** on the main Virus & Threat Protection page.

XPROTECT FOR MACOS

macOS has a built-in antivirus solution called XProtect. When you download an application from the internet, XProtect will check its definitions file of known-bad files, which is updated when you receive software and operating system updates for your computer. This is less beneficial than an antivirus program that performs a heuristics-based scan (see the upcoming "**Signatures and Heuristics**" section for more information on heuristics) that evaluates files based on their content or behavior, rather than a specific file signature.

Choosing Malware Detection and Antivirus Tools

When deciding on the antivirus and malware detection tools you'd like to use, consider whether it's worth paying for a commercial tool (or the premium version of a free tool) and whether the tool will use signatures or heuristics to detect malware.

In general, if all you want is a simple malware scanning tool, there's rarely a good reason to pay for a commercial product. Typically, you'll pay for advanced features, such as an email or web browser scanner built-in to the malware file scanner.

Oftentimes, paid solutions allow for some form of centralized management. Whether that's a web portal or a management server or agent, you gain visibility and the ability to manage all of your devices from one place. If you have a larger network, there's value in having this capability; if your network consists of less than 30 devices, you probably don't need it.

Antivirus Farm

There's also a benefit in foregoing a single solution in favor of using multiple antivirus products in smaller networks. *Antivirus farms* use several products aiming to catch more malware than a single solution might. It also makes the attacker's job more difficult; instead of evading a single antivirus product, they need to evade multiple to move laterally through a network.

Antivirus farms are helpful because every antivirus vendor curates their own databases of *malware signatures*—sequences of bytes in the executable that can be used to identify that specific malware sample. These databases have to be optimized every so often; otherwise, the virus definitions that you download with the software would become too large and unwieldy to be useful. Therefore, older virus definitions may be removed from these databases over time, which means having products from multiple vendors will likely lead to greater coverage of known threats.

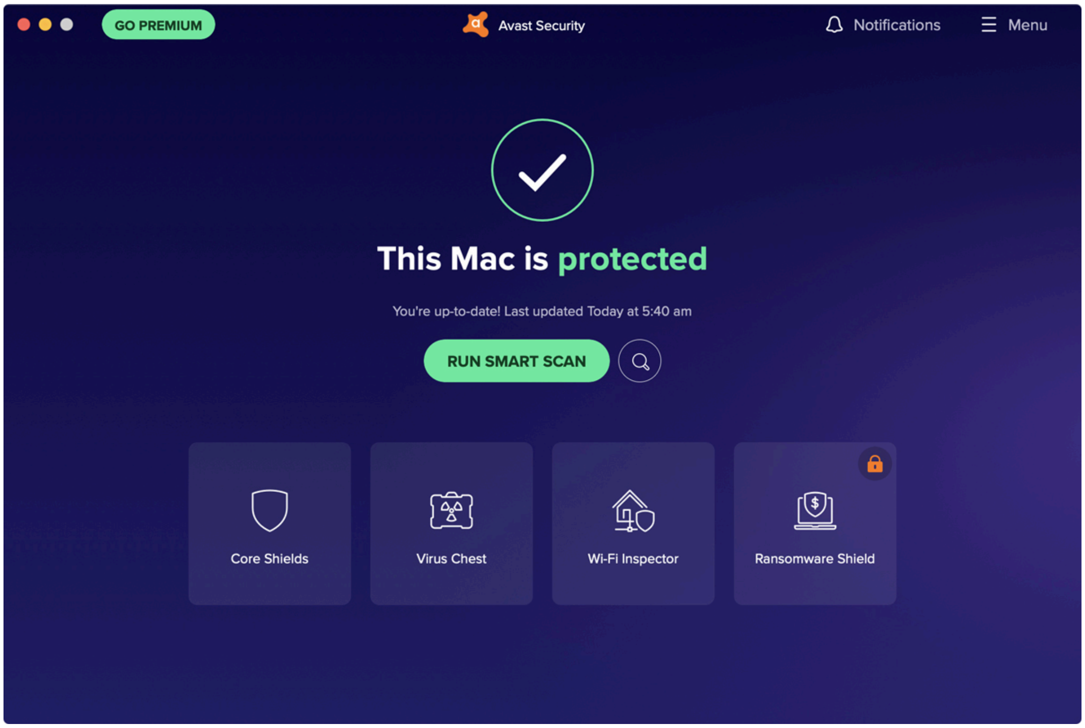
Signatures and Heuristics

You should also aim to use antivirus products that perform both signature-based detection and heuristics. *Signatures* identify known-malicious software by the contents of an executable or other file, though it's trivial for an attacker to change the signature of their malware by changing the contents slightly. This is a major weakness when it comes to malware detection software. *Heuristics*, on the other hand, analyze the way a file behaves and the commands a file might run to determine whether it's malicious. This is a much more reliable way of detecting known and unknown threats. How do you tell whether a particular antivirus program performs signature-based detection or heuristic scanning? The best way, if it's not listed on their website, is to contact the vendor and ask. There will always be a contact method listed on their website.

#26: Installing Avast on macOS

Apple devices, commonly believed to be less prone to malware, are becoming infected more often, which means you should install antivirus software on any Macs on your network. There are many options, both free and commercial, when installing a third-party heuristics-based antivirus solution on your Apple computer. Among these, Avast has topped many lists for several years. To install and configure Avast, use the following steps:

1. Download Avast from *http://www.avast.com/* and install the software. When the installation has completed, you should be presented with the Avast Security window (see Figure 8-1).



This Mac is protected

You're up-to-date! Last updated Today at 5:40 am

Figure 8-1: Avast Security window

2. Click **Menu ▸ Preferences** to reach Avast's settings page.
3. In the General tab, ensure that the **Turn on Automatic Updates** checkbox is ticked.
4. In the Privacy tab, *untick* the two checkboxes allowing your data to be shared with Avast. Similar to Windows Defender, it's best to protect your privacy.
5. In the Core Shields tab, enable each of the security checks Avast will run, such as file scanning and web and email protection.
6. Click the **Add Exceptions** button under each of the shields to specify any necessary exceptions. Add exceptions if you have files or programs that you know to be legitimate or low risk but that your antivirus classifies as potentially malicious.
7. In the Scans tab, ensure the checkboxes **Scan Whole Files**, **Scan External Drives**, **Scan Mounted Network Volumes**, **Scan All**

Time Machine Backups, and **Scan Archives** are ticked. By doing so, you can be certain your antivirus is doing as much as possible to identify threats and protect you from them.

A *Smart Scan* is designed to scan the most vulnerable areas of your computer quickly. While this is less resource intensive and less time consuming, it's not likely to catch all threats on your computer because it doesn't scan all areas of your hard drives. A *Deep Scan* is more comprehensive and includes all areas of storage on your device, optionally including external storage, network locations, Time Machine backups, memory, and rootkit detection. A *Targeted Scan* scans only specified areas.

All of these scans are run from the Scan Central screen in Avast on your Mac. Click the **Search** button to select the type of scan you want to run and then click **Scan Now**. Selecting Targeted, USB/DVD, or Custom Scans will prompt you for the locations to scan. Avast will scan your computer for threats, and if any are detected, it will ask what you'd like to do with the relevant files. Select all the files and click **Resolve Selected** to move them all to the Virus Chest; then click **Done**. Your computer should now be clean of all potentially malicious files and applications.

#27: Installing ClamAV on Linux

Linux is susceptible to viruses as well. However, Linux operating systems rarely come with a built-in antivirus application, and there are fewer available than for other operating systems. Most of the available solutions are commercial and therefore have a cost attached, such as Avast Core Security for Linux, though there is an open source solution: ClamAV.

ClamAV is a free application that can be used on Windows, macOS, and Linux. To install it on Ubuntu, log in to your server via SSH as a standard, non-root user. Run the following command to install the version of ClamAV that allows you to automate your virus scanning activity, as well as the GUI, clamtk, which may be useful later:

```
$ sudo apt install clamav clamav-daemon clamtk
```

With the installation complete, your antivirus definitions (the database that tells ClamAV what is malware) should be up-to-date, but you can run the following commands to update the virus definitions—either now or in the future—to stop, update, and then restart ClamAV:

```
$ sudo systemctl stop clamav-freshclam

$ sudo freshclam

$ sudo systemctl start clamav-freshclam
```

To run a malware scan, use the `clamscan` `folder_to_scan` command. To scan everything on the system, use `/` to indicate to ClamAV to scan everything in the root of the filesystem, supply the `-r` parameter to make the scan recurse all directories, and use `sudo` so that ClamAV has the necessary permission to read all files in the filesystem:

```
$ sudo clamscan -r /

--snip--

----------- SCAN SUMMARY -----------

Known viruses: 8927215

Engine version: 0.102.3

Scanned directories: 89954

Scanned files: 362758
```

```
Infected files: 0

Total errors: 82216

Data scanned: 8767.58 MB

Data read: 14195.27 MB (ratio 0.62:1)

Time: 1171.021 sec (19 m 31 s)
```

When the scan completes, `clamscan` will output a scan summary.

In addition to known malware, ClamAV can detect *potentially unwanted applications (PUAs)*, including software such as adware, peer-to-peer (p2p) programs, remote administration tools, bitcoin miners, and bundleware (software included with but not related to the application being installed), which are not inherently malicious but may pose a risk to or negatively impact your endpoints' security and performance. To scan for PUAs, include the `--detect-pua=yes` argument when running ClamAV.

If your scans are taking too long, you can use other advanced parameters to reduce their duration. You can limit the size of the files ClamAV will scan with `--max-filesize=` `n`, where `n` is the maximum file size in kilobytes. Any files larger than the size you specify will be skipped and assumed to be clean, reducing the time it takes your scan to complete. Similarly, `--max-scansize=` `n` scans only archive files (*.rar* files, *.zip* files, and so on) up to the specified size—all other archives will be skipped. To limit the depth of the recursion (that is, how many directories will be scanned below the directory where you start the scan), use the `--max-dir-recursion=` `n` parameter. For more parameters, use the `-h` argument, as in `sudo clamscan -h`, to print the help menu.

To run a scan on a regular schedule, use Crontab, a Linux utility designed to execute programs at preset times or intervals. In your terminal, use the `crontab -e` command to edit the scheduled tasks file:

```
$ sudo crontab -e
[sudo] password for user:
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron’s system
# daemon’s notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:

# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/

#

# For more information see the manual pages of crontab(5) and cron(8)

#

# m h  dom mon dow   command
```

The large comment at the start of the file explains how to specify tasks with an example. The last line of the comment provides the syntax for scheduling execution of scripts and applications. The order is minute, hour, day of month, month, day of week, and command to execute. Minutes and hours must be numbers, 0 to 59 and 0 to 23, respectively, and you can specify a list of minutes or hours by separating the values with commas (that is, you can run a command at 1, 2, and 3 AM by specifying `1,2,3`). You can specify days numerically (1 to 7, where 1 is Sunday), or as Sun, Mon, Tue, and so on. Months are 1 to 12 (where 1 is January). An asterisk (`*`) stands for all possible values for a field; if you want your command to run every month, put an asterisk in the month (`mon`) position.

Say you want to run `clamscan` over the entire filesystem at 1 AM every Sunday, including scanning for potentially unwanted applications. At the bottom of the Crontab file, add a new line and enter the following:

```
0 1 * * sun clamscan -r / --detect-pua=yes -l /path_to_logfile/clamav.log
```

By default, you won't be able to see the results of your scans unless you specify the logfile with the `-l` parameter. If you want to scan a specific folder, like the user home folders (*/home/*), every day, in addition to the full system scan, add another entry to the Crontab, following the previous example as a guideline.

Add another line to the Crontab to ensure ClamAV is kept up to date:

```
0 0 * * mon systemctl stop clamav-freshclam && freshclam && systemctl start clamav-freshclam
```

You can link multiple commands together and separate them with a pair of ampersands to run them in series. Find more information on Crontab (or any other terminal command) with the `man` function. Enter `man crontab` to open the manual for the application on the command line.

#28: Using VirusTotal

VirusTotal (VT) tests files to determine whether they're likely to be malicious (***https://www.virustotal.com/***) by taking the concept of an antivirus farm and implementing it on a large scale. It's a publicly available service where you can upload any file to scan for malware, and VT will scan it with more than 60 antivirus programs. It will then produce a report to let you know whether it contains malware or behaves in a way that may negatively impact your endpoints, security, or privacy. This capability is especially useful if you believe a file is malicious but is undetected by your antivirus.

Be aware that anything uploaded to VT becomes public, so anyone can search for and download the files you upload. To use VT without making your private information public, search VT for the hash of the file you want to check. *Hashing* is a process for calculating a fixed-length string based on the contents of a file. Hashing is expected to be a one-way process, meaning you can't take the hash of a file and reverse it to get the original file contents. By creating the hash of a file, you should get a unique string of characters that identify said file. Some hashing algorithms can result in *collisions*, where two files yield the same hash, though the chances of this happening in most modern hashing functions are slim to none. You can get the hash of a file by using built-in tools in any operating system.

Windows PowerShell In Windows, open a PowerShell window and enter the following command to get the MD5 hash of any file:

```
$ Get-FileHash path_to_file -Algorithm MD5
```

You can then search for the hash directly in the VirusTotal web portal.

Linux and macOS Terminal You can get the MD5 hash of a file in both Linux and macOS using the following command:

```
$ md5sum path_to_file
```

Then, search for the resulting hash in the VT web portal.

If a file with the same hash has been uploaded to VT at any point in the past, you'll be presented with the public report for that file, detailing the malware scan results from all the providers in VT. If it hasn't been uploaded previously, there's a good chance the file isn't malicious.

#29: Managing Patches and Updates

Along with using antivirus tools, patch management is an important defense because malware exploits are written to attack a specific vulnerability in a network, application, protocol, or operating system. Adversaries pay close attention to Windows updates and patches for other operating systems, as the patch notes call out the vulnerability it's designed to remediate. Attackers use that vulnerability information to write malware specifically for that security flaw, and anyone who hasn't downloaded the update can fall victim. This is why operating systems constantly ask you to install updates and patches.

In most cases, end users don't install updates right away, and adversaries have a window of opportunity to target unpatched systems. It's in your best interest to install software updates as soon as they become available. Luckily, the process of updating is exceedingly simple and easy to automate. This project describes how to configure system updates on individual systems, and the following section discusses a solution for patch management across multiple endpoints.

Windows Update

For Windows updates, open **Windows Settings ▸ Update & Security**. Windows checks for updates automatically at least once per day (assuming the device is left on at all times). To check for, download, and install updates manually, click the **Check for Updates** button.

If you'd prefer not to worry about updates for a while, click **Pause Updates for 7 Days**. Updates are critical for keeping your system secure, so pausing the updates is not recommended.

You can restrict Windows from updating your computer during certain times by setting active hours. If you use your computer primarily between 9 AM and 5 PM, you can tell Windows not to update during this window, which is a better option than pausing updates for an extended period of time.

In Advanced Options, you can allow Windows to update other Microsoft products via Windows Update—I recommend turning this on. You can also make Windows force devices to restart after updates are installed, which is useful if you, as the administrator, want to force your end users to restart their machines. You'll be unpopular, but your network will be more secure.

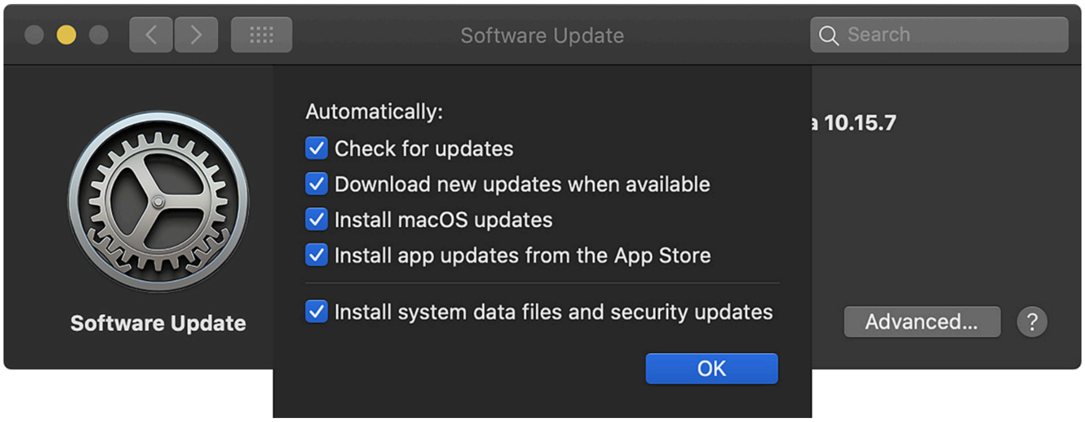
In the Advanced Options ▸ Delivery Optimization menu, you can enable the option to download updates from other PCs in your network. This reduces the bandwidth required to download the same updates to multiple computers from the internet. You should turn on this setting, with the caveat that downloads be allowed only from PCs on your local network and not from PCs on the internet.

Back in the Advanced Options pane, the last settings of particular interest are the Privacy settings. You can increase your privacy within this menu by disallowing Windows and Microsoft from sending you targeted ads and content based on your location, browsing habits, and application usage statistics.

macOS Software Update

Apple devices are much simpler than Windows or Linux because their update process can be almost entirely automated and requires very little user input. To ensure your Apple computers are kept up-to-date, open **System Preferences ▸ Software Update**. To allow automatic updates, check **Automatically Keep My Mac Up-to-date**.

With this check box ticked, click the **Advanced** button to select what actions should be taken automatically. From this menu (Figure 8-2), choose whether your computer can check for updates, download updates, or complete the installation process without user input, and then click **OK** to save the settings. In most cases, allowing your computer to keep itself up-to-date with no input from the user is desirable; the computer will still confirm with the user before restarting after any updates that require a reboot (which doesn’t happen often).



Automatically:

☑ Check for updates

☑ Download new updates when available

☑ Install macOS updates

☑ Install app updates from the App Store

☑ Install system data files and security updates

__Figure 8-2__: macOS advanced software update configuration

Keeping your devices up-to-date in this way ensures they are as secure as possible and protects your and your users' privacy.

Linux Updates with apt

As discussed in **Chapter 1**, the Linux operating system comes in multiple implementations, called *distributions*. Each of those distributions uses a package manager to maintain and update the software that the system or user installs. Throughout this book, we use Ubuntu Linux, which uses the Advanced Package Tool (APT) package manager. Package managers simplify the process of keeping your Linux endpoints up-to-date and secure.

To update an Ubuntu system, log in via SSH as a standard, non-root user. When you log in, you should be presented with a welcome message, including information about required and recommended updates:

```
--snip--

 * Documentation:  https://help.ubuntu.com

 * Management:     https://landscape.canonical.com

 * Support:        https://ubuntu.com/advantage
```

```
105 updates can be installed immediately.

68 of these updates are security updates.

To see these additional updates run: apt list --upgradable

--snip--
```

To make sure the list of updates is complete, run the `apt update` command:

```
$ sudo apt update
```

Once the list is up-to-date, run the `upgrade` command to update all of the software packages:

```
$ sudo apt upgrade
```

The command output will show the number of packages to update, the disk space they'll use, and various status messages. When prompted, type **Y** and press ENTER to continue.

As with Windows and macOS, some updates require you to reboot the system. If that's the case, you'll see something like:

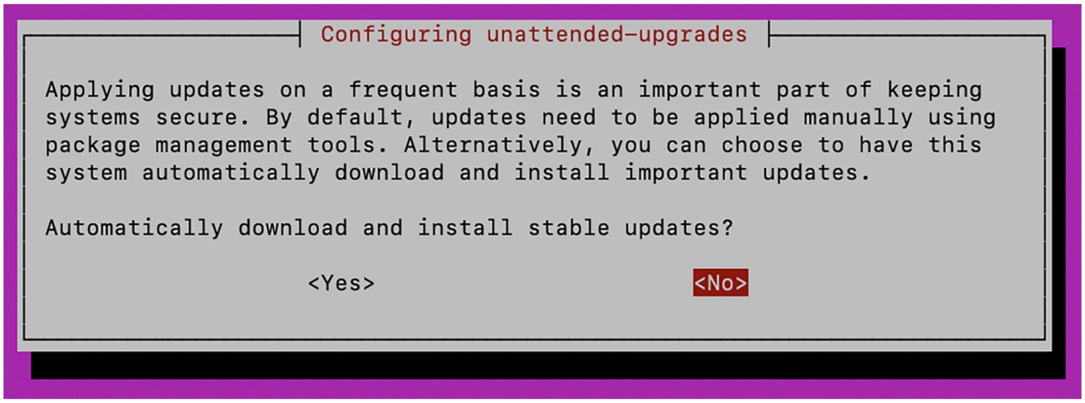
```
A reboot is required to replace the running dbus-daemon.

Please reboot the system when convenient.
```

To make Ubuntu update the system and installed packages automatically, use the following command:

```
$ sudo dpkg-reconfigure -plow unattended-upgrades
```

The command will produce the prompt shown in **Figure 8-3**.



```
Configuring unattended-upgrades

Applying updates on a frequent basis is an important part of keeping
systems secure. By default, updates need to be applied manually using
package management tools. Alternatively, you can choose to have this
system automatically download and install important updates.

Automatically download and install stable updates?

                  <Yes>                        <No>
```

__Figure 8-3__: Ubuntu unattended updates

By selecting **Yes** and pressing ENTER, you'll ensure your servers are kept up-to-date, thereby making them inherently more secure. However, you should still check for updates manually and reboot your server once a month.

#30: Installing Automox

Depending on the size of your network, keeping all your endpoints up to date manually or even semi-manually might feel tedious or overwhelming. A centralized patch management solution like Automox allows you to easily manage all of these things in one place. Automox operates on a per-endpoint subscription model: you can start managing one or more Windows, macOS, or Linux systems (workstations or servers) for a nominal monthly fee, which allows you to patch all of your endpoints, with both system and third-party software patches, from one dashboard. Automox also maintains an asset and software inventory, which is the first step anyone should take to keep their network secure.

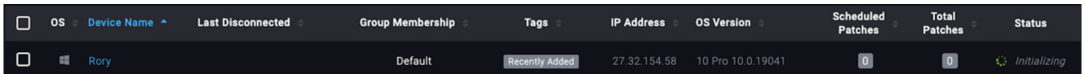
Installing Automox

Head to the Automox website (*https://www.automox.com/*) to sign up for an account (or free trial). Then log in to your account dashboard at *https://console.automox.com/*. The dashboard is where you'll see a summary of your managed endpoints and the updates they require. Of course, until you add some endpoints to your account, this dashboard will be sparse. In the following sections you'll require a user key to connect your endpoints to Automox. Your key can be found by going to your profile settings page in the Automox web UI, under the Keys tab.

Windows

To install the Automox agent on Windows endpoints, access the **Devices** tab from your Automox console, and then click the **Add Devices** link at the top of the page. You'll be presented with an OS selection pop-up. Select Windows, and then download the agent.

Once the agent is downloaded, run the installer (an *.msi* file) as an administrator. Follow the installation wizard, entering your Automox user key from the console when prompted. When the installation has completed, refresh your Automox dashboard to see the newly added endpoint (Figure 8-4).



□	OS	Device Name	Last Disconnected	Group Membership	Tags	IP Address	OS Version	Scheduled Patches	Total Patches	Status
□	⊞	Rory		Default	Recently Added	27.32.154.58	10 Pro 10.0.19041	0	0	Initializing

***Figure 8-4**: Automox asset list*

macOS and Linux

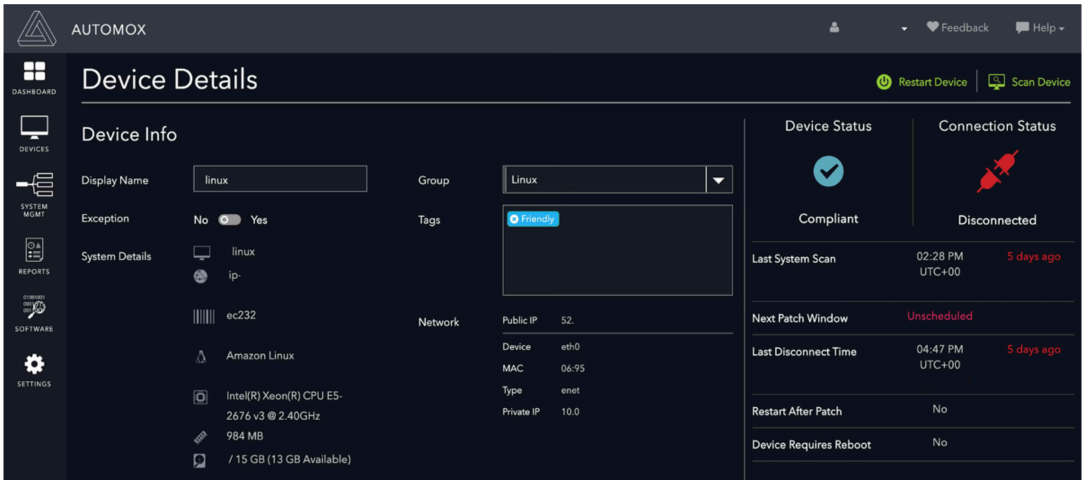
In a Terminal window on a Mac or Linux computer, run the following command, substituting your user key for `yourkey`:

```
$ curl -sS "https://console.automox.com/downloadInstaller?
accesskey= yourkey " | sudo bash
```

Refresh your console again to see the newly added endpoint(s).

Using Automox

Now that you've installed Automox on your endpoints, you'll be able to manage operating system and third-party software patches from a central console. From the Devices tab, you can view all of your managed endpoints and add them to groups—if you'd like to manage them that way. You can also scan your endpoints to identify hardware changes and check for new updates they require, reboot your endpoints remotely, or remove endpoints from your account. By clicking an endpoint, you can see its hardware configuration, IP and MAC addresses, device type, operating system, CPU and RAM details, and other critical information, as shown in Figure 8-5. You can also force updates to be applied to the endpoint immediately, rather than wait for the endpoint to be updated according to the update policies specified in the System Management tab.



Device Details

Device Info

Display Name: linux
Exception: No ○ Yes
System Details:
linux
ip-
ec232
Amazon Linux
Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
984 MB
/ 15 GB (13 GB Available)

Group: Linux
Tags: Friendly
Network:
Public IP 52.
Device eth0
MAC 06:95
Type enet
Private IP 10.0

Device Status: Compliant
Connection Status: Disconnected

Last System Scan	02:28 PM UTC+00	5 days ago
Next Patch Window	Unscheduled	
Last Disconnect Time	04:47 PM UTC+00	5 days ago
Restart After Patch	No	
Device Requires Reboot	No	

Figure 8-5: Automox device details

The System Management tab allows you to create and assign patching policies, which is useful if you want to schedule patch installation. For example, you may decide to automatically install any critical patches daily at 5 PM. Alternatively, you might want to force the installation of all required patches at 12 AM every Saturday, when people are less likely to be using their computers. You will need to define your own requirements and decide what patching schedule works best for you and your network.

In the Reports tab, you can generate reports of actions taken by Automox to keep your endpoints up-to-date, report on the state of any or all endpoints in your console, or identify noncompliant endpoints. Depending on the size of your network, it may be easier to view this information in your dashboard than to run these reports.

Automox will provide you with an inventory of all the software installed on your managed endpoints and their patch level in the Software tab. This allows you to easily identify software that requires updating and to update it if possible. You can also use this list to identify software that you don't want in your environment, whether it's potentially unwanted applications or specific software, like games or other software that violates an organizational policy.

Finally, the Settings tab allows you to create new users to allow other administrators to access your Automox console to manage your endpoints. You can also find and add your agent access keys in this tab. One thing you should absolutely take advantage of is the two-factor authentication setting. By enabling two-factor authentication, you make your account more secure and therefore make unauthorized access to your devices and patch management information much more difficult (discussed further in Chapter 11).

Summary

Keeping your systems up-to-date is critical in keeping your network secure. Whether you choose to use the built-in antivirus and patching options for your operating system or a managed patching solution like Automox, updates should be regularly scheduled and virus scans regularly run; otherwise, you leave your network vulnerable to all sorts of adversaries and unnecessary risk.