Security Built into MacOS

X Protect has been on Macs since 10.6 High Sierra

We will look at:

Firewall

Gatekeeper

XProtect and XProtect Remediator

Look at: Silent Knight

Bruce Mitchell

My 2 main sources to learn about this:

macintouch.com

eclecticlight.co

Mac OS has built in security

No need to download XProtect as it is a feature of the Mac OS.

It is not an application.

Apple quietly updates XProtect.

This is invisible running in the **background**.

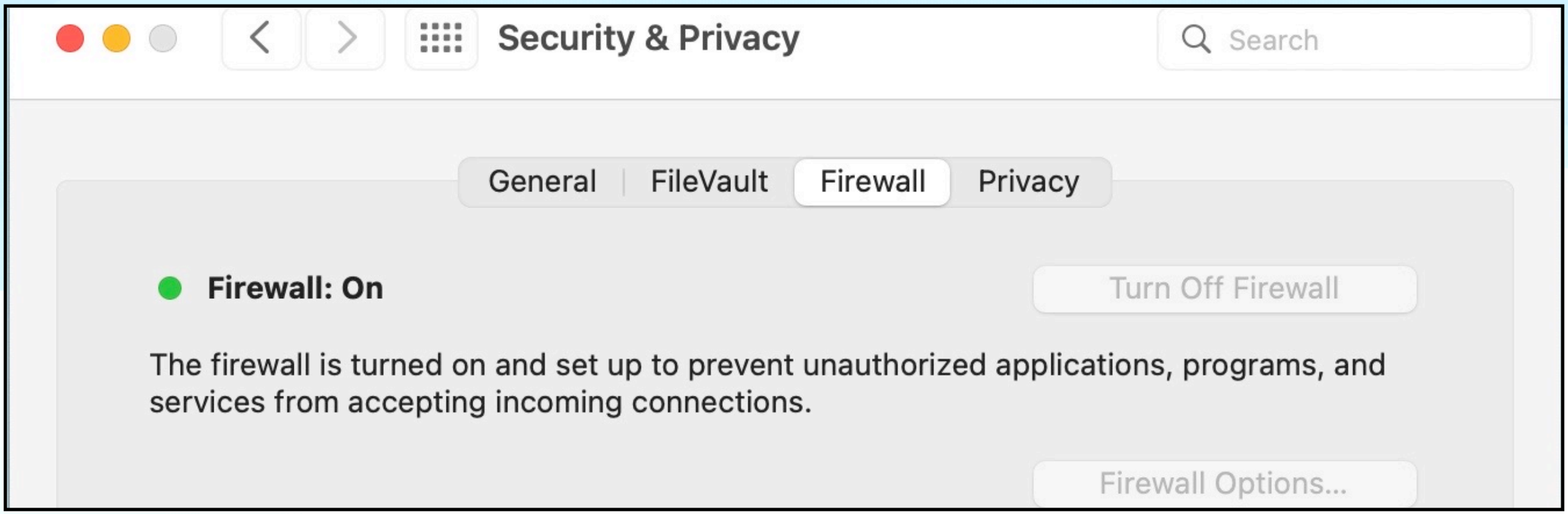
So how does one know if everything is current and turned on?

So we are talking about a **S**ystem **I**ntegrity **C**heck

In System Preferences or now Settings in our Mac OS Under Security and Privacy be sure these are active:

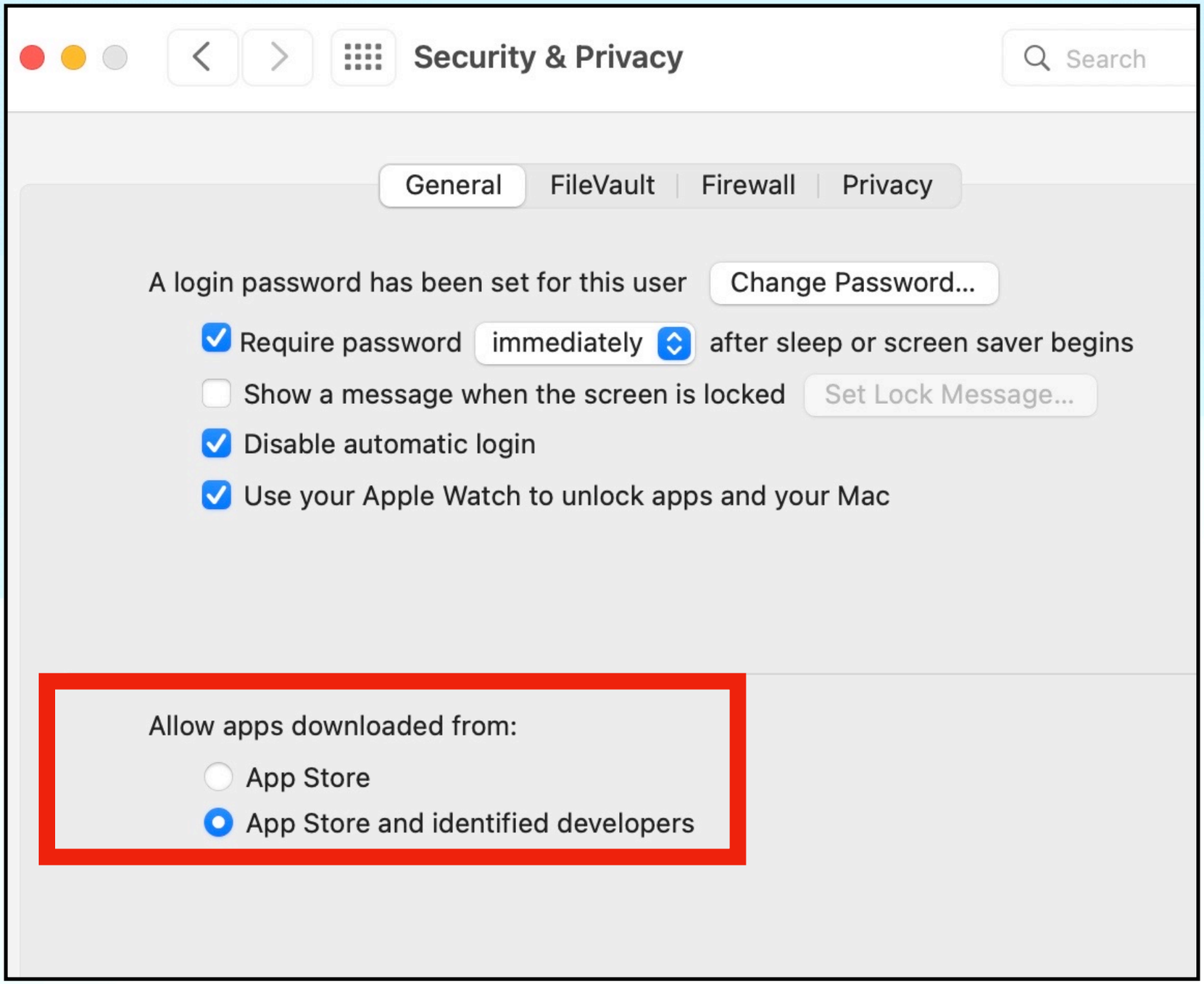
Firewall and GateKeeper

Firewall



Make sure this is turned on in System Preferences and now System Settings in Ventura

Gatekeeper



macOS includes a technology called Gatekeeper, that's designed to **ensure that only trusted software runs on your Mac**.

MRT

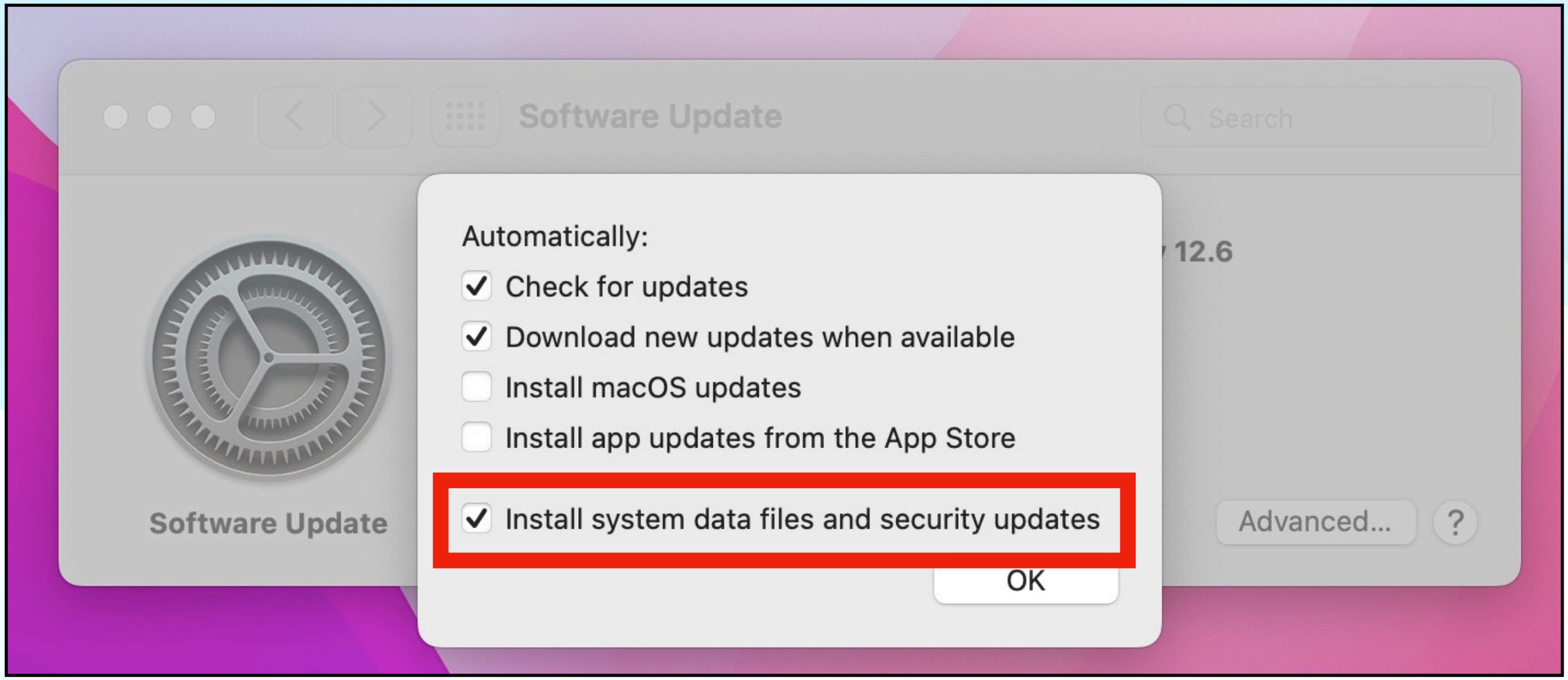
Malware Removal Tool

...malware protection technology that automatically removes harmful software from your Mac based on the information updated by Apple. It examines your Mac for malware when restarting and logging in...

Apple does not inform you what was removed or if there was an issue.

MRT is now a built-incomponent in XProtect Remediator

Enabled by Default on Mac
Keep X Protect Updated in Background



Apple logo > System Preferences > Software Update > Advanced

XProtect Remediator

XProtect Remediator removes malware

XProtect Remediator consists of 12 modules that briefly but regularly scan your Mac for specific nasties during periods of low user activity.

Think of remediator as what updates anti-virus definitions.

* These nasties are malware

Apple has become more aggressive keeping XProtect updated as malware activity has increased in recent months.

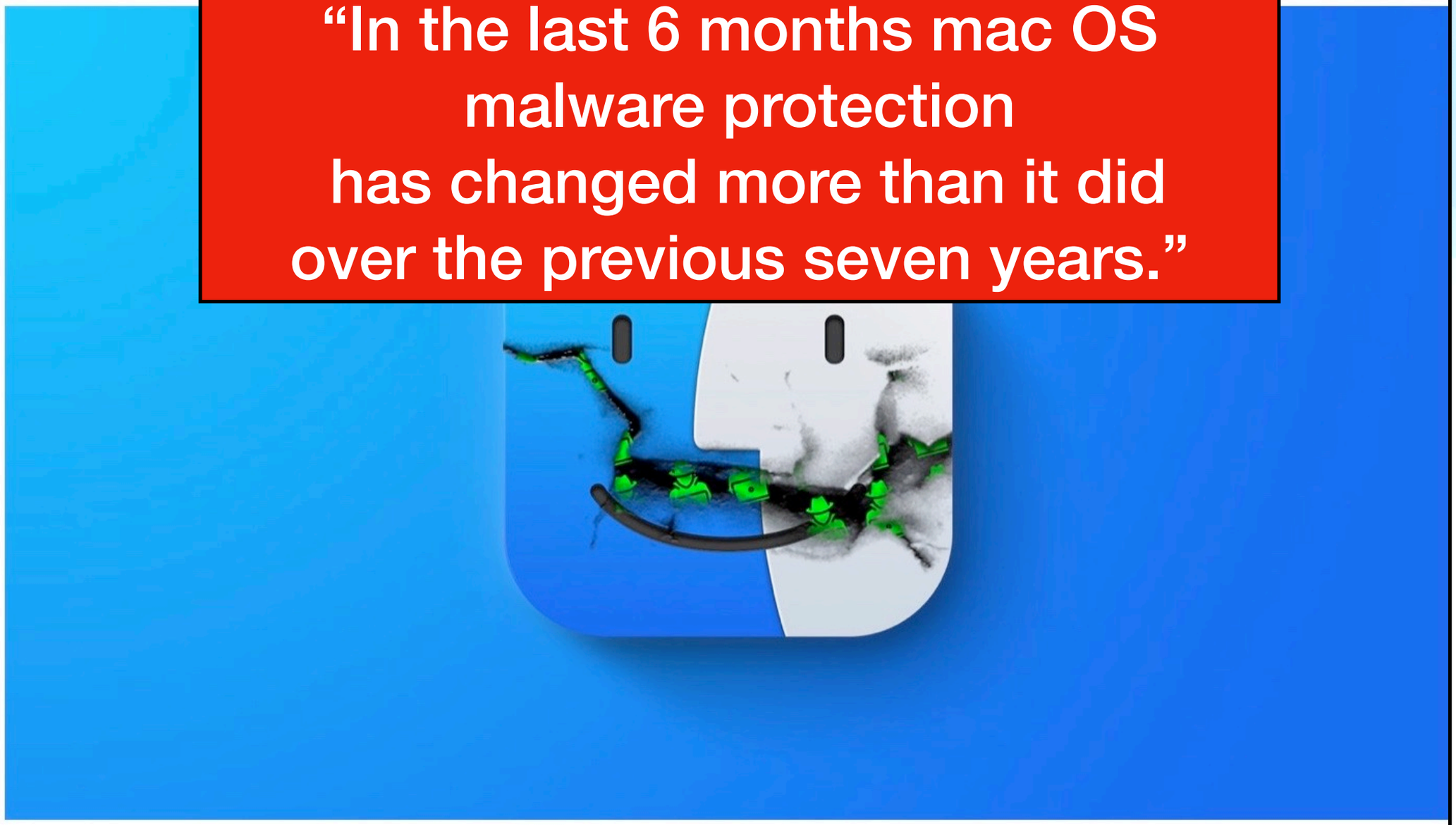
Lots of Remediator updates.

Apple Has Made Major Updates to macOS Malware Protection in 2022

Wednesday August 31, 2022 1:13 pm PDT by Juli Clover

Apple has made notable updates to macOS malware tools over the course of the last six months, according to updates tracked by Howard Oakley at Eclectic Lighting Company (via *Ars Technica*).

"In the last 6 months mac OS malware protection has changed more than it did over the previous seven years."



"In the last six months, macOS malware protection has changed more than it did over the previous seven years," writes Oakley in a blog post published this week. Malware detection on the Mac is now "fully pre-emptive" and as active as "many commercial anti-malware products."

XProtect Remediator removes harmful malware in the background

The app is invisible

It can’t be found in the App folder.

It is part of the System OS.

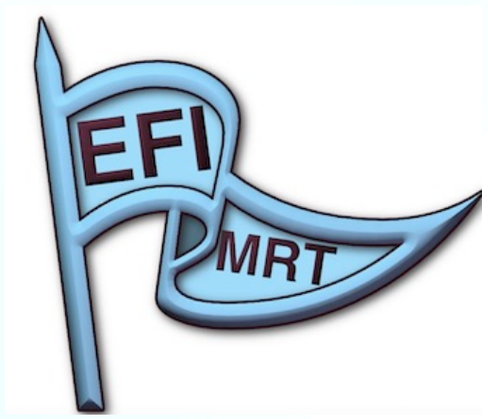
It is active and running when there is light activity.

This is another reason not to always shut down your Mac.

I learned more about XProtect this summer.

This application give us an insight.

Silent Knight



Silent Knight is a **security integrity check**

to see if everything is active and current

What Silent Knight tells us

XProtect is responsible for checking apps and some other files indicating if they are malicious. It should always be enabled. Apple periodically updates its signature and malware definitions using pushed security updates.

So Silent Knight shows the System Integrity Check.

It lets you know the status of the System Integrity Check.

The updates just happen and you can’t initiate them. Just leave the computer on and it will update in the background.

A green check means it is current

So how do you find and download Silent Knight?

Where to find Silent Knight and XProCheck

THE ECLECTIC LIGHT COMPANY

eclecticlight.co not .com

Visit eclecticlight.co > Downloads

SilentKnight – *automatic checking of security systems*

Product page.
SilentKnight 1.21 (Universal App for El Capitan, Sierra, High Sierra, Mojave, Catalina, Big Sur, Monterey and Ventura)

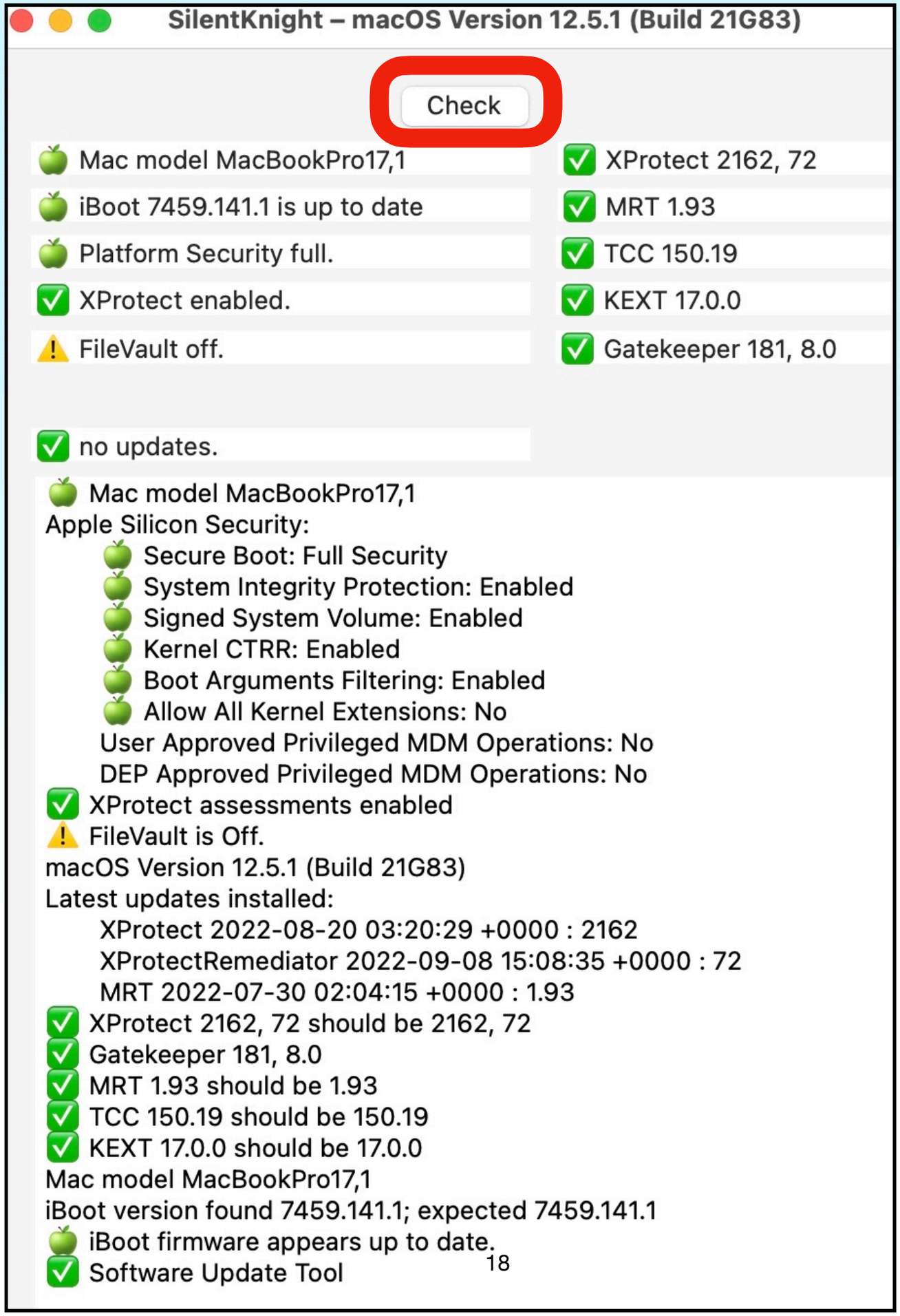
This is the Link

OR…

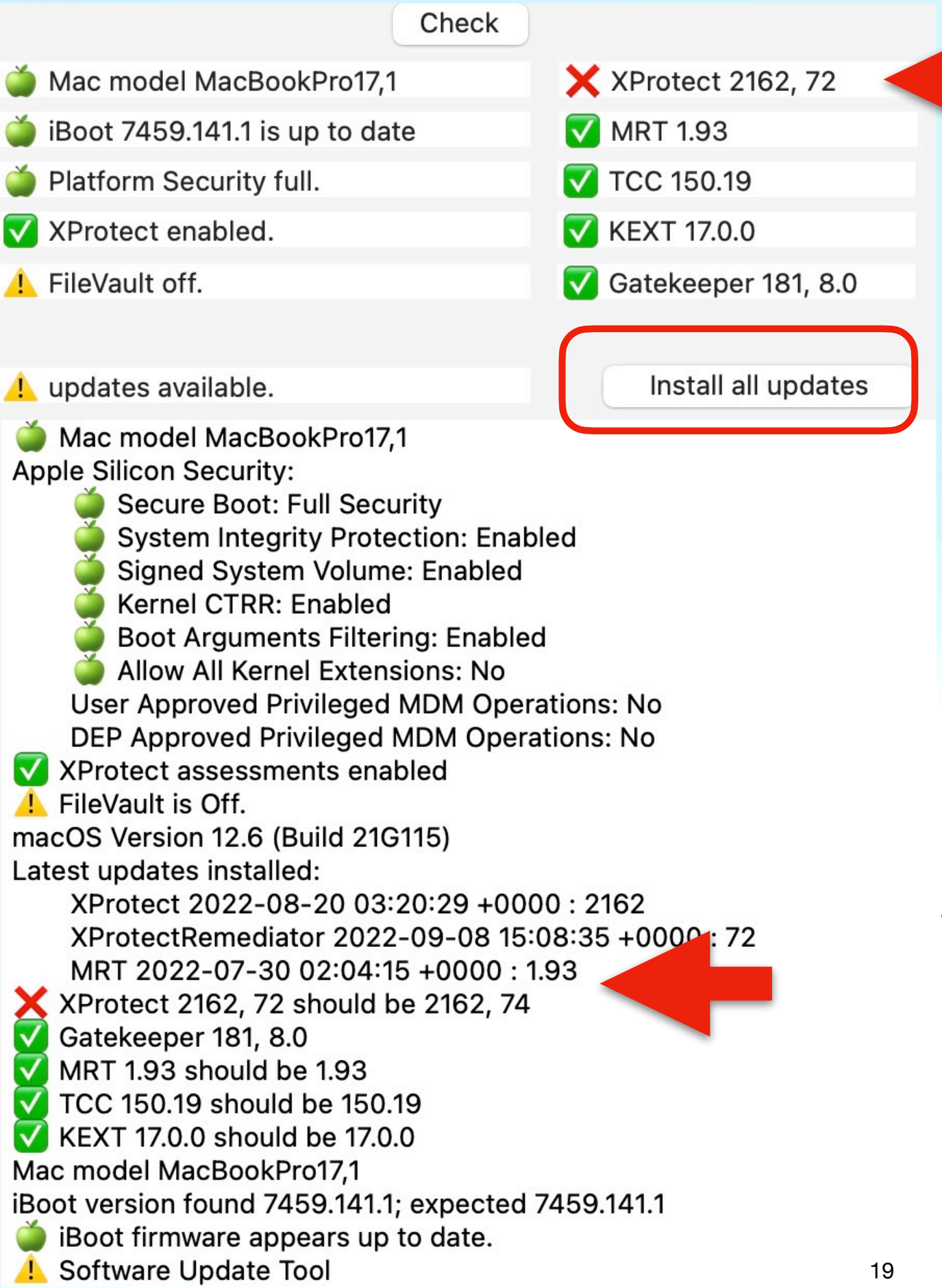
The Eclectic Light Company Freeware Menu

macOS Updates

- **SilentKnight** auto check of security systems (10.11+)
- **silnite** command tool security checks (10.11+ *not* M1)
- **ArchiChect** check apps are ready for Big Sur & Apple Silicon (10.14+)
- **LockRattler** detailed security systems checks (10.11+)
- **SystHist** full system and security update history (10.11+)
- **32-bitCheck** checks thoro for 32-bit onl (10.11-10.15



Launch **Silent Knight** and Click Check



XProtect Remediator needs an Update.
Thus a red X

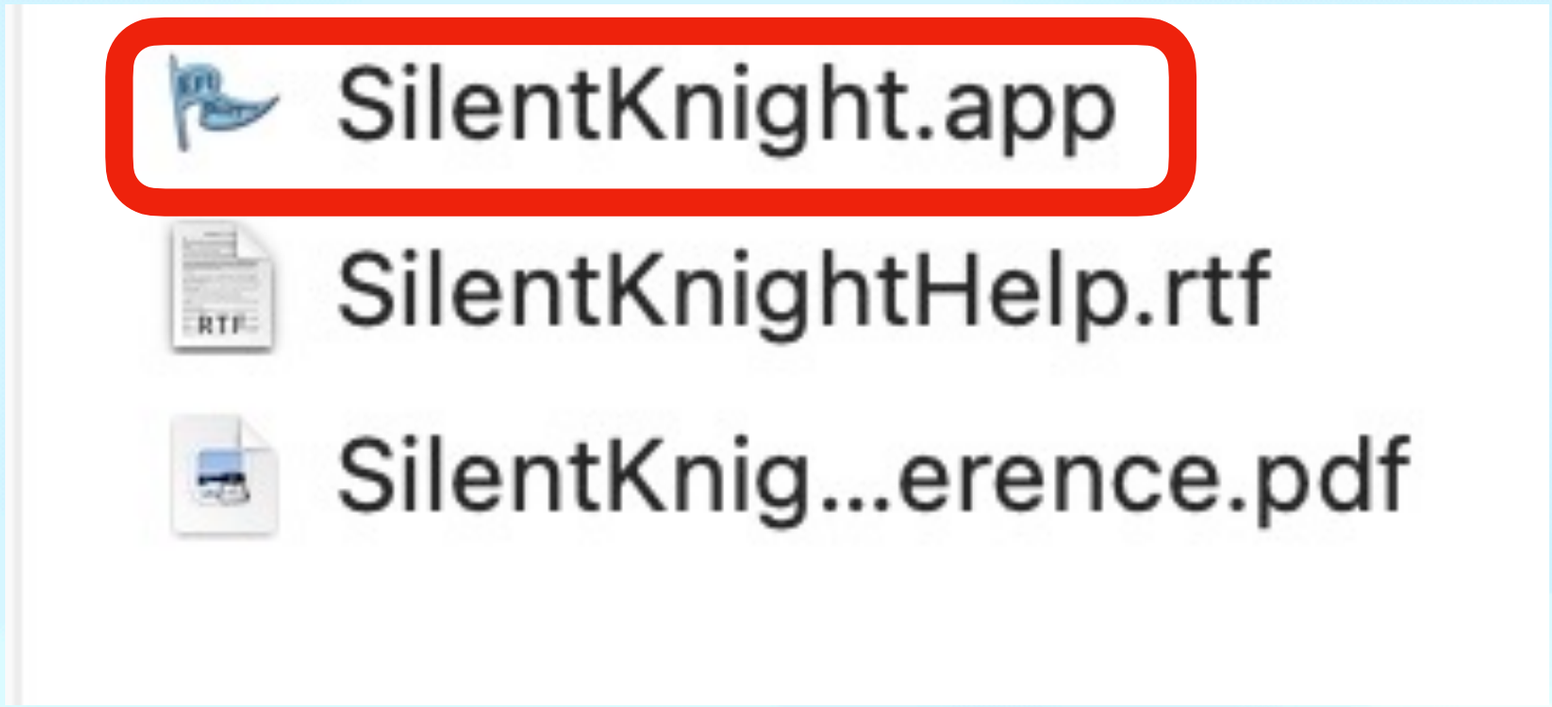
It should be ....

Just let the Mac run in the background

Remediator is just the

malware /antivirus definitions

that need updating in the background.



I keep a folder on my Desktop
and just open the app

It could also go in the Applications folder.

So where does that leave other anti virus programs like Intego Virus Barrier, Norton, BitDefender, etc.?

"While Apple offers its own antivirus protections in the form of Gatekeeper and XProtect, they don't always work so well due to the fact that they rely on out-of-date methods for stopping infections. The best Mac antivirus programs on the other hand do a better job, quickly spotting new malware strains and double-checking suspicious files that have been "signed" with an Apple developer ID."

https://www.tomsguide.com/best-picks/best-mac-antivirus

Intego gets high rankings https://www.comparitech.com/antivirus/best-mac-antivirus/

So I continue to use Intego Virus Barrier and be sure to keep Apple's built in protection up to date and I check this with Silent Knight.
xProtectCheck I use less.

So first focus on Silent Knight to see if everything is current.
The developer is working on a new version of Silent Knight called 2.0
It will work with Catalina all the way to Ventura.OS13.

XProtect works on older Macs going way back.
Though improvements were made for users running Catalina, Big Sur, Monterey, and now Ventura.

Remember that you will never find an application called XProtect.

It is just part of the MacOS.

If you have any questions just ask in the TVAUG forum.

Yes, there are ways to see what malware XProtect finds.