



[Portaal](#) > [Kennisbank](#) > [Endpoint Solutions](#) > [You receive an ESET UEFI detection](#)

## You receive an ESET UEFI detection

Anish | ESET Nederland - 2018-10-08 - [0 Comments](#) - in [Endpoint Solutions](#)

### Issue

- Your ESET product notifies you of a UEFI detection (for example, EFI/CompuTrace, Win32/CompuTrace, EFI/Lenovo, Win32/Lenovo)
- What is UEFI malware and how to prevent them
- How to resolve detections of applications in UEFI

### Details

### Solution

## ESET detects UEFI malware or applications

UEFI scanning is available in the latest versions of ESET products. See the Details section above for a list of ESET products that contain the UEFI scanner.

By default, the detection of potentially unsafe or unwanted applications is disabled in ESET products. Because UEFI infections are very specific to the hardware firmware that they infect, ESET can only detect and notify you of a UEFI infection. UEFI is only scanned during startup scan or during On-demand scan when the option "Boot sectors/UEFI" is selected.



Figure 1-1

## How to protect your computer from UEFI malware

- **Use a computer with a newer chipset**  
Verify all of your systems have modern chipsets with Platform Controller Hub (starting from Intel Series 5 chipsets onwards).
- **Ensure that your computer has Secure Boot enabled**  
Typically, UEFI malware is not properly signed and having Secure Boot enabled will keep it from loading and infecting your computer.
- **Upgrade your UEFI firmware on your computer**  
We recommend that you perform a UEFI firmware update even if your computer does not notify you of a detection. As a preventive measure, it may help minimize the chances of this type of infection.

## How to resolve ESET UEFI detections

Since UEFI detections are specific to the hardware firmware that they are on, ESET cannot remove a UEFI detection. See below for possible remediation steps you can take.

- Upgrade the firmware from your computer vendor and rescan with ESET UEFI scanner. If the UEFI detection remains, you can ask your computer vendor to update their firmware to remove the problematic detection.
- Exclude the detection of this threat in your ESET product. If you have enabled detection of potentially unsafe applications and your computer vendor does not remove the application from its firmware, you can exclude the detection from future scans.

**Home users:** [Exclude an application by name from scanning in ESET Windows home products.](#)

**Business users version 7:** [Exclude files or folders on endpoints from Real-time scanning using ESET Security Management Center \(7.x\).](#)

**Business users version 6:** [Exclude endpoint files or folders from Real-time scanning using ESET Remote Administrator \(6.x\).](#)

For example, use Threat name: @NAME=EFI/CompuTrace.variant@TYPE=ApplicUnsaf

- Disable the "detection of potentially unsafe applications" option in your ESET product.

**Home users:** [Configure ESET products to detect or ignore unwanted, unsafe and suspicious applications.](#)

**Business users:** [Enable or disable endpoint detection of potentially unwanted/unsafe applications using ESET Security Management Center \(7.x\).](#)

- Reflash the SPI Flash Memory where the UEFI lives. This is a delicate and complex procedure and is different for every motherboard. Your computer manufacturer will be able to tell you if this is possible.

**If you are not familiar with UEFI**

If you are not familiar with UEFI settings or the updating/flashing process, we recommend that you contact an experienced professional to help with this procedure.

- If you think that the detection is incorrect, [submit the detection to the ESET malware lab for analysis.](#)

For detailed information about UEFI malware including prevention and remediation, see the following WeLiveSecurity.com post: [Lojax: First UEFI rootkit found in the wild, courtesy of the Sednit group.](#)

If you are still unable to resolve your issue, please [email ESET Technical Support.](#)