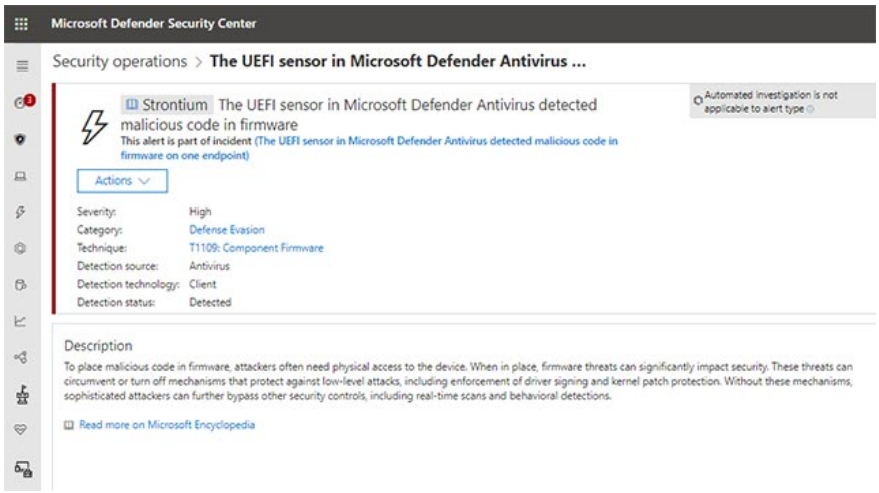
Microsoft is about to add a useful security feature to Windows 10 to help detect software attacks early

UEFI scanner feature in the Defender Advanced Threat Protection (Defender ATP) tool.

Windows Defender, now known as Microsoft Defender, is becoming more powerful, useful, and becoming a tool to detect and respond to security threats that are widely used on Windows 10. instead of using third-party antivirus software like before. In the near future, this tool will continue to be added with another extremely useful security feature, which is the UEFI (Unified Extensible Firmware Interface scanner) scan.

Specifically, on June 18, Microsoft officially announced that it will add the UEFI scanner feature in the Defender Advanced Threat Protection tool (Defender ATP) to enhance an additional layer of active security. helps detect software attacks early on Windows 10. In other words, Microsoft Defender ATP will soon be able to detect malware entering the system through firmware updates.

In theory, malware that infects the firmware level is often difficult to detect because it is launched before the operating system boots. Microsoft's new UEFI scanning engine was created to solve this problem, by actively interacting directly with the motherboard chipset and reading the firmware's file system when it is launched.



UEFI scanner

In general, this new tool will use the following components and solutions to deploy dynamic analysis at the firmware level:

1. UEFI anti-rootkit, helps access firmware via Serial Peripheral Interface.
2. Full file system scanner, which helps check the content inside the firmware.
3. A detection tool that helps identify all signs of malicious code and malicious behavior in firmware.

In case malware is detected at the firmware level, users will receive security alerts displayed in the Defender Security Center. Here, the system will give the results of threat analysis and take appropriate steps to respond to suspicious activity in the system at each level.

IT (enterprise-class) security groups can also use the advanced scanning capabilities in Microsoft Defender ATP to hunt for these complex threats. According to Microsoft, the new security tool mentioned above is an essential part of the policy to improve security efficiency in Microsoft Defender ATP, and users can expect many such exciting new features in the future. Microsoft Defender ATP is now provided as the default security application on all Windows 10 devices and when installing the operating system, this antivirus tool will also be automatically activated.