**END OF LIFE STATEMENT FOR EMET BY WINDOWS:**

**“**

We have listened to customers' feedback regarding the January 27, 2017 end of life date for EMET and we are pleased to announce that the end of life date is being extended 18 months. The new end of life date is July 31, 2018. There are no plans to offer support or security patching for EMET after July 31, 2018. For improved security, we recommend that customers migrate to the latest version of Windows 10.  “

What is EMET?

**Enhanced Mitigation Experience Toolkit** (**EMET**) is a security toolkit for Microsoft windows operating system developed by Microsoft. security tool that adds supplemental security defences to defend potentially vulnerable legacy and third-party applications.

Techniques used by EMET:

EMET uses 12 specific mitigation techniques that seek to prevent exploits related to memory corruption, making it harder for attackers to find and exploit vulnerabilities, including:

* Data execution prevention -- a security feature that helps prevents code in system memory from being used incorrectly
* Mandatory address space layout randomization -- a technology that makes it difficult for exploits to find specific addresses in a system's memory
* Structured exception handler overwrite protection -- a mitigation that blocks exploits that attempt to exploit [stack overflows](https://whatis.techtarget.com/definition/stack-overflow)
* Export address table access filtering -- a technology that blocks an exploit's ability to find the location of a function
* Anti-Return Oriented Programming -- a mitigation technique that prevents hackers from bypassing DEP(data execution prevention)
* [SSL](https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL)/[TLS](https://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS) certificate trust pinning -- a feature that helps detect [man-in-the-middle attacks](https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM) leveraging the [public key infrastructure](https://searchsecurity.techtarget.com/definition/PKI)

I will explain about some important words used in the above different techniques section:

* Stack overflow: A stack overflow is a condition in which a particular computer program tries to use more memory space than the call stack has availed to it and sometimes the program may crash. The call stack generally depends on the PC’s, the memory you assigned dynamically in your program
* . Man, in the middle attack: attacks pose a serious threat to online security because they give the attacker the ability to capture and manipulate sensitive information in real-time. The attack is a type of eavesdropping in which the entire conversation is controlled by the attacker. Sometimes referred to as a session [hijacking attack](https://searchsecurity.techtarget.com/definition/hijacking).

Reasons caused the end of EMET’s era:

some companies and organisations had found a way to bypass the EMET’s security restrictions like:

1. WikiLeaks’ [recent release](https://wikileaks.org/ciav7p1/) of documents purported to be from the Central Intelligence Agency demonstrate the agency’s ability to bypass widely used enterprise security tools such as Microsoft’s Enhanced Mitigation Experience Toolkit (EMET).
2. In 2014, Bromium Labs [announced](https://bromiumlabs.files.wordpress.com/2014/02/bypassing-emet-4-1.pdf) that it had developed an exploit code that bypassed EMET 4.1. The researchers said that their bypass used “generic limitations” of the tool and were not “easily repaired.”
3. FireEye researchers [disabled](https://www.fireeye.com/blog/threat-research/2016/02/using_emet_to_disabl.html) EMET by exploiting a function within the tool that is responsible for unloading it from the application once it has determined that the app is not malicious. “One simply needs to locate and call this function to completely disable" the security tool, the researchers explained.

Drawbacks of EMET stated by the developers and users:

* First, it was not developed as a “robust security solution,” but rather as a “stop-gap solution” to block zero-day exploits between Windows updates. As a result, there are a number of “well-publicized bypasses available to get around EMET,” .
* The security tool “hooks into low-level areas” of Windows, but the operating system was not designed for this type of use. This leads to degradation of performance and reliability of Windows and applications running on it. This causes an “ongoing problem for customers since every OS or application update can trigger performance and reliability issues due to incompatibility with EMET,”.
* its effectiveness against modern exploit kits has not been demonstrated, especially in comparison to the many innovations built-in to Windows 10.

The replacement for EMET:

Microsoft last week explained more about how its Enhanced Mitigation Experience Toolkit (EMET) is getting removed and also how it is getting integrated into the **Windows Defender Advanced Threat Protection (ATP)** service.  EMET's protections are getting moved into the ***"Windows Defender Exploit Guard"*** feature of the Windows 10 "fall creators update,"

WINDOWS DEFENDER EXPLOIT GUARD:

* Microsoft has included the Windows Defender Exploit Guard in the [Windows 10 Fall Creators Update](https://www.guidingtech.com/top-10-new-features-in-windows-10-fall-creators-update/), which helps prevent ransomware attacks on the PC.
* Ransomware encrypts your important files and documents with a known or custom RSA algorithm. later they ask for a sum of money in exchange for the key. Microsoft aims to nip the issue in the bud by blocking access to the file systems.
* Going by the name of ***Controlled folder access***, this feature essentially prevents [unauthorized access](https://www.guidingtech.com/58590/get-notified-weird-activity-online-accounts/) to the common folders. This means that apps, scripts, DLLs and executable files won't be able to access unless you give them explicit permission. Whenever an unauthorized app tries to have access to the protected folders, you're notified via a small notification window.

REFERENCES:

* <https://www.guidingtech.com/enable-windows-10-exploit-guard/>
* <https://redmondmag.com/articles/2017/08/14/microsoft-to-block-emet-in-windows-10.aspx>
* <https://searchsecurity.techtarget.com/definition/Microsoft-Enhanced-Mitigation-Experience-Toolkit-EMET>
* <https://www.ghacks.net/2016/11/04/microsoft-to-discontinue-emet-in-july-2018/>
* <http://techgenix.com/microsoft-retiring-emet/>
* https://en.wikipedia.org/wiki/Enhanced\_Mitigation\_Experience\_Toolkit