File system security features in Windows 11

**Description**

In this report we will be analysing the following features that Windows 11 brings to tackle issues related to file system security and comparing them with the features provided by Apple’s latest version of its macOS operating system, macOS Ventura:

|  |  |
| --- | --- |
| **Bitlocker drive encryption** | Windows 11 utilises Bitlocker as its primary data encryption tool protecting all the files on a system’s drives from unauthorised access by rendering files on the drives unreadable by anybody without the password or recovery key. (et al., *Bitlocker* 2023) |
| **Personal data encryption (PDE)** | PDE is a data encryption tool that can be used on top of already existing encryption tools like Bitlocker. It is used to encrypt individual files rather than larger volumes of files or drives. (et al., *Personal Data Encryption (PDE)* 2022) |
| **Security descriptors** | Windows 11’s NTFS file system uses Security descriptors as means of storing relevant information for each file/directory that dictates their different levels of access for users. (Sherer, *Security descriptors* 2021) |
| **Controlled folder access (CFA)** | Controlled folder access works by preventing access to files and folders on a system from applications that are not on a list of trusted apps set by an administrator. (et al., *Protect important folders with Controlled Folder Access* 2023) |
| **Windows File Protection (WFP)** | WFP prevents critical Windows system files from being replaced or overwritten by any other programs unless it is from a Windows verified source such as an OS update. (*Description of the Windows File Protection feature*) |
| **Auditing** | Windows 11 uses an auditing system that logs specific security events including those related to file system security to provide information on any breaches that may occur in a system. (lorihollasch, *Auditing* 2021) |
| **File signature validation** | Files in Windows 11 have file signatures which identify the file type. This information can be used by Windows Defender to identify if a file is potentially dangerous or has been modified. (Malin et al., *Malware forensics field guide for windows systems: Digital Forensics Field Guides* 2012) |

**OS support**

**Comparison**

**Effects on developers**

**Conclusion**

**References**

|  |  |
| --- | --- |
| 1 | <https://support.microsoft.com/en-us/topic/description-of-the-windows-file-protection-feature-db28f515-6512-63d1-6178-982ed2022ffb> |
| 2 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/security-features-for-file-systems> |
| 3 | <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control> |
| 4 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/security-descriptors> |
| 5 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/security-descriptors> |
| 6 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/kernel-extended-attributes> |
| 7 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/privileges> |
| 8 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/access-mask> |
| 9 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/access-control-entry> |
| 10 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/security-descriptors> |
| 11 | <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/auditing> |
| 12 | <https://learn.microsoft.com/en-us/windows/security/encryption-data-protection> |
| 13 | <https://learn.microsoft.com/en-us/windows/security/information-protection/encrypted-hard-drive> |
| 14 | <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder> |
| 15 | <https://www.sciencedirect.com/topics/computer-science/signature-file#:~:text=A%20file%20signature%20is%20a,20%20bytes%20of%20the%20file>. |
| 16 |  |
| 17 | frankroj (2022) *Personal Data Encryption (PDE)*, *Microsoft Learn*. Edited by aczechowski et al. Microsoft. Available at: https://learn.microsoft.com/en-us/windows/security/information-protection/personal-data-encryption/overview-pde (Accessed: March 1, 2023). |
| 18 | frankroj (2023) *Bitlocker*, *Microsoft Learn*. Edited by paolomatarazzo et al. Microsoft. Available at: https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview (Accessed: March 1, 2023). |
| 19 | Lorihollasch (2021) *Security descriptors in file systems* , *Windows drivers | Microsoft Learn*. Edited by aviviano and matt-msft. Microsoft. Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/security-descriptors (Accessed: March 2, 2023). |
| 20 | tedhudek (2021) *Security descriptors* , *Windows drivers | Microsoft Learn*. Edited by T. Sherer. Microsoft. Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/security-descriptors (Accessed: March 2, 2023). |
| 21 | denisebmsft, Dansimp and beccarobins (2023) *Protect important folders with Controlled Folder Access*, *Protect important folders from ransomware from encrypting your files with controlled folder access | Microsoft Learn*. Edited by msbemba. Microsoft. Available at: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide (Accessed: March 2, 2023). |
| 22 | Microsoft (no date) *Description of the Windows File Protection feature*, *Microsoft Support*. Microsoft. Available at: https://support.microsoft.com/en-us/topic/description-of-the-windows-file-protection-feature-db28f515-6512-63d1-6178-982ed2022ffb (Accessed: March 2, 2023). |
|  | lorihollasch (2021) *Auditing* , *Windows drivers | Microsoft Learn*. Edited by matt-msft. Microsoft. Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/auditing (Accessed: March 2, 2023). |
|  | Malin, C.H., Casey, E. and Aquilina, J.M. (2012) *Malware forensics field guide for windows systems: Digital Forensics Field Guides*. Waltham, MA: Syngress. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |