File system security features in Windows 11

**Description**

In this report we will be analysing the following file system security features in Windows 11 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. (et al., *Bitlocker* 2023) |
| **Personal data encryption (PDE)** | PDE is a separate data encryption tool 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 a 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. (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. (Support, *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 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**

**Bitlocker** is a key out-of-box feature that is deeply integrated into Windows 11. It utilises the AES-128 encryption standard alongside a TPM chip found in almost all modern computers’ motherboards to render all the files in a drive unreadable and inaccessible if the hardware is compromised, and the machine is modified, stolen or the drives themselves are stolen. (et al., *Bitlocker Security FAQ*) This behaviour is default and occurs as soon as Windows 11 is installed on a machine and logged into for the first time as an administrator. It also allows the option of an administrator set Key/Password and an external USB key as further methods of authorising access to a drive to enhance file security and it is often recommended to use all three methods together. (et al., *Protectkeywithtpmandpinandstartupkey method of the win32\_encryptablevolume class - win32 apps* 2021)

Alongside Bitlocker, Windows 11 utilises **Personal data encryption** to protect individual files specified by the administrator of a system. It is able to work on top of existing encryption methods however unlike Bitlocker, it utilises ‘Windows Hello for Business’ to log in the user by scanning biometric information with onboard hardware such as a fingerprint scanner or facial recognition software and a camera. Upon receipt of authorised biometric data the key is released, and the files can be accessed. (et al., *Personal Data Encryption (PDE)* 2022)

Every object in Windows 11 is assigned a **security descriptor**. They can be assigned at a granular level for each individual file/parts of a file or broadly apply to a volume of many files. They are made up of security identifiers (SIDs) that describes the owner of the object or optionally an additional SID that describes a group ownership, where owners can reset the security of an object ( et al., *Security descriptors in file systems* 2021), a system access control list (SACL) describing which actions on the object are logged for **auditing** purposes and a discretionary access control list (DACL) describing which users can perform actions on the object. (Sherer, *Security descriptors* 2021)

With **Controlled folder access (CFA)**,users can select folders in a file system that will prevent untrusted applications from accessing the contents of these folders. Trusted applications are selected “based on their prevalence and reputation” (et al., *Protect important folders with Controlled Folder Access* 2023) or can be added to the list of trusted apps by the system administrator. Any applications that are not on this list will not be allowed to access specific folders, also chosen by the administrator of a system, and a log will be created in the device timeline view for every CFA block that occurs for **auditing** purposes.

**Windows File Protection (WFP)** protects crucial system files through 2 primary mechanisms. The first mechanism is a process that runs in the background of the operating system that alerts the system when a change is made to a file in a protected directory, it then uses **File signature validation** to check if the file was changed appropriately (e.g. Windows Update to system files). If not, the new file is replaced with its previous version held in the cache folder, network installation path or windows CD-ROM, and the attempted change is logged in the system log to be viewed by an administrator for **auditing** purposes. If the original file cannot be found, a dialogue box is opened for the admin of a system asking to have the physical installation media inserted to recover the unchanged file. (Support, *Description of the Windows File Protection feature*) The second mechanism used is the System File Checker tool which provides the same security checks but for the cache folder and catalog files responsible for providing the correct version of the system files in the first mechanism.

**File signature validation** identifies a file via its header with the first 20 bytes of the file as hexadecimal characters, the first two bytes of which identify the file type. It can be used by system admin’s to scan a system and look for unsigned files that can pose a risk to a system such as unsigned .exe files.

Timeline

Description automatically generated

**Comparison**

|  |  |
| --- | --- |
| **Windows 11** | **macOS Ventura** |
| Bitlocker | FileVault is macOS’ solution to drive encryption. Much like Bitlocker, it is enabled by default as out-of-box behaviour for the OS and utilises the AES encryption standard to encrypt all the files in the system. (Support, *Volume encryption with FileVault in macos* 2021) However, macOS has a much more advanced approach to security for its systems utilising a separate processor called ‘Secure Enclave Processor’ as a microkernel to perform its security functions alongside a T2 chip which is Apple’s alternative to a TPM chip that works with their proprietary hardware found in apple systems. (Support, *Secure enclave* 2021) |
| Personal data encryption | Personal data is protected by Secure Enclave in the process of full drive encryption rather than a separate level of encryption over individual files. However, Face/Touch ID for file encryption is not tied to a separate version of software like Microsoft’s Hello for business and is instead a default feature offered to systems with biometric capabilities. (Support, *Face ID and touch ID security* 2021) |
| Security descriptors | Apple uses their own APFS file system where security descriptors are not used. Rather, APFS allocates space on demand and uses separate volumes per user as a means of user access control. (Support, *Role of apple file system* 2022) |
| Controlled folder access | Similar to Windows 11, apple allows users to control which applications have access to their files through their own system called ‘Data Vault’ and applications are denied access to user files by default unless it is specified otherwise. (Support, *Protecting app access to User Data* 2022) |
| Windows File Protection | MacOS uses System Integrity Protection to protect important system files by preventing user access and therefore preventing access to applications that would ask the user to enter credentials for access. This is a different approach to Windows 11 which instead amends changes to these files where they occur. Both methods check that changes being made to protected files are coming from signed processes. (Support, *About system integrity protection on your mac* 2022) |
| File signature validation | Both operating systems utilise the existing standard for file signatures to verify file validity. |

**Effects on developers**

As **Bitlocker** and **Personal Data Encryption** are designed to protect the file system in cases of compromised hardware, there are not many considerations to be made for these features when developing an application for Windows 11 systems. However, in situations where developers are relying on remote restart and log in for their application (e.g. remote access software) this can be a blocker as Windows Hello for business can prevent logging back into a system remotely.

Developers may want to configure SACLs for the **security descriptor**s of their files to allow for logging and **auditing** of changes made to files in their applications in a user’s system. This can be an important tool for managing the integrity of an application.

**CFA** has a major effect on application developers as it requires the application to be built to request addition to the trusted applications list in a system if it requires access to user protected files.

**WFP** should not have an effect as applications should not need to access/modify system critical files in Windows 11.

All application developers should ensure that the files in their application are signed appropriately with a digital signature for purposes of **file signature validation** checks not raising security issues with their applications.

**Conclusion**

Overall, Windows 11 has a plethora of features that provide great file system security; however, it is my personal reflection that Apple’s macOS has a much more advanced security system due to its tighter trust policy of applications and inclusion of features like a separate processor for security related functions and wider adoption of and default support for biometrics tied encryption. I feel that there are several improvements to be made to Windows 11’s file system security practices such as:

* Biometrics encryption keys should be integrated into the Bitlocker tool and not tied to Windows Hello for business to improve availability and adoption of better security practises by users
* Bitlocker should enable TPM+PasswordKey+USBKey+Biometrics by default wherever possible with available hardware. This will ensure the greatest level of encryption in the file system unless an admin opts to do otherwise rather than relying on users to enable further levels of encryption.
* WFP should always alert the user immediately if a file change was attempted and leave the user with the option to turn the alerts off so that problematic software can be detected and removed sooner.
* CFA blocks should always generate alerts in the Alerts queue of the system and again leave the administrator with the option to turn the alerts off for the purposes of greater auditing capabilities and transparency of what is happening in the file system with protected files.

**References**

|  |
| --- |
| 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). |
| 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). |
| 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). |
| 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). |
| 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). |
| 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. |
| frankroj *et al.* (no date) *Bitlocker Security FAQ*, *Microsoft Learn*. Microsoft. Available at: https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-security-faq (Accessed: March 2, 2023). |
| alvinashcraft *et al.* (2021) *Protectkeywithtpmandpinandstartupkey method of the win32\_encryptablevolume class - win32 apps*, *Win32 apps | Microsoft Learn*. Microsoft. Available at: https://learn.microsoft.com/en-us/windows/win32/secprov/protectkeywithtpmandpinandstartupkey-win32-encryptablevolume?redirectedfrom=MSDN (Accessed: March 2, 2023). |
| Support, A. (2021) *Secure enclave*, *Apple Support*. Apple. Available at: https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web (Accessed: March 3, 2023). |
| Support, A. (2021) *Volume encryption with FileVault in macos*, *Apple Support*. Apple. Available at: https://support.apple.com/en-gb/guide/security/sec4c6dc1b6e/1/web/1 (Accessed: March 3, 2023). |
| Support, A. (2021) *Face ID and touch ID security*, *Apple Support*. Apple. Available at: https://support.apple.com/en-gb/guide/security/sec067eb0c9e/1/web/1 (Accessed: March 3, 2023). |
| Support, A. (2022) *Role of apple file system*, *Apple Support*. Apple. Available at: https://support.apple.com/en-gb/guide/security/seca6147599e/1/web/1 (Accessed: March 3, 2023). |
| Support, A. (2022) *Protecting app access to User Data*, *Apple Support*. Apple. Available at: https://support.apple.com/en-gb/guide/security/secc01781f46/1/web/1 (Accessed: March 3, 2023). |
| Support, A. (2022) *About system integrity protection on your mac*, *Apple Support*. Apple. Available at: https://support.apple.com/en-us/HT204899 (Accessed: March 3, 2023). |

# Appendix

References: 492 words

Word count excluding Cover Sheet, Appendix and references: 1625

Link to GitHub repository: https://github.com/EmirK224/OSSecurity