**TrueCrypt is old and dangerously unsecure (Initial Post)**

White and black hat hackers have been battling each other for as long as computers and the internet have been around. White hat hackers would find exploits and vulnerabilities in software and report them to the appropriate organisation to fix them. In contrast, black hat hackers find exploits and vulnerabilities to steal financial, personal, and medical data. It is a balance that must be maintained at all times.

TrueCrypt was once one of the best software to encrypt personal and organisational data from hackers. However, sadly the software has not been updated since 2014. As mentioned in the first paragraph, a balance must be maintained between black hat and white hat hackers. When software does not receive any updates for almost a decade, that balance is disrupted. A decade of no updates in software development is considered a lifetime. Therefore one cannot in good conscious recommend any software that does not receive updates for such a long time, especially security software like TrueCrypt.

Reading through the TrueCrypt cryptanalysis by Junestam & Guigo (2014), it is evident that even when the software development was active, TrueCrypt had many high-risk vulnerabilities that needed to be addressed as soon as possible. Some of these are integer overflow, buffer overflow, Weak Volume Header key derivation algorithm, the usage of "memset" instead of the more secure "burn" function to clean sensitive data and much much more.

Furthermore, the report outlined more issues regarding code readability, maintenance, and ease of use. Some of these issues are related to uncommented code, long functions that are 700+ lines of code, and the mixing of user and kernel mode, which is a big no-no.

Therefore I would not recommend using TrueCrypt in 2022 whatsoever. Even if the application were secure but had its development cease in 2014, I would still not recommend it.

References:

Junestam, A. and Guigo, N. (2014) ISEC - ISEC Final Open Crypto Audit Project TrueCrypt Security assessment, Open Crypto Audit Project TrueCrypt Security Assessment . Open Crypto Audit Project. Available at: https://pentestreports.com/reports/iSEC/iSec\_Final\_Open\_Crypto\_Audit\_Project\_TrueCrypt\_Security\_Assessment.html (Accessed: December 12, 2022).