Aktualizacja: 17.05.2021 r.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
5. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
6. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
7. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
9. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
10. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.
11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
    a) ilość znaków,
    b) czy hasło ma zawierać wielkie litery,
    c) czy hasło ma zawierać małe litery,
    d) czy hasło ma zawierać cyfry,
    e) czy hasło ma zawierać znaki specjalne,
    f) okres ważności,
    g) ilość nieudanych logowań,
    h) możliwość zmiany hasła.
12. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
13. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.