



## Szyfrowane pamięci USB Kingston / Ironkey Zalety w porównaniu z funkcją BitLocker

<b>MICROSOFT BITLOCKER</b> 	<b>KINGSTON / IRONKEY SZYFROWANE PAMIĘCI USB</b> 
<b>Właściwości</b>	<b>Zalety produktów Kingston</b>
<ol style="list-style-type: none"> <li><b>Ograniczona zgodność z różnymi systemami operacyjnymi:</b> <ul style="list-style-type: none"> <li>- Dostępność TYLKO w wersjach Enterprise i Ultimate systemu Windows 7   Wersjach Pro i Enterprise systemu Windows 8.1   Windows 10.</li> <li>- Nie obsługuje systemu Mac OS</li> </ul> </li> <li><b>Problemy z poprawkami do systemu operacyjnego / aktualizacjami systemu</b> <ul style="list-style-type: none"> <li>- Aktualizacje z błędami — opóźnienia w udostępnianiu poprawek</li> </ul> </li> <li><b>Luka w zabezpieczeniach polegająca na podatności na ataki „ROCA”</b> <ul style="list-style-type: none"> <li>- Kryptograficzne błędy w rozwiązaniu BitLocker</li> <li>- „To jest gorsze niż KRACK” - Google i Microsoft ucierpiały z powodu luki w algorytmach szyfrujących, która istniała od 5 lat</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li><b>Lepsza zgodność między systemami OS:</b> <ul style="list-style-type: none"> <li>- Windows® 10   Windows 8.1   Windows 8   Windows 7 (SP1)   Mac OS X wersje 10.10.x–10.13.x   Linux Kernel wersja 2.6.</li> </ul> </li> <li><b>Brak zagrożeń ze strony ataków typu „ROCA”</b></li> </ol>
<ol style="list-style-type: none"> <li><b>Szyfrowanie programowe</b> <ul style="list-style-type: none"> <li>- Działa na komputerze-goście</li> </ul> </li> <li><b>Łatwiejsze ataki związane z lukami w zabezpieczeniach</b> <ul style="list-style-type: none"> <li>- Brak zabezpieczeń przeciwko keyloggingowi, sniffingowi, atakom z kompromisem pamięci / atakom techniką „pass the hash”</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li><b>Szyfrowanie sprzętowe</b> <ul style="list-style-type: none"> <li>- Zabezpieczenie w pełni autonomiczne</li> </ul> </li> <li><b>Brak ataków wynikających z luk w zabezpieczeniach oprogramowania</b> <ul style="list-style-type: none"> <li>- Eliminuje sniffing oraz ataki z kompromisem pamięci / ataki techniką „pass the hash”</li> </ul> </li> <li><b>Oprogramowanie sprzętowe podpisane cyfrowo</b> <ul style="list-style-type: none"> <li>- Brak możliwości modyfikacji</li> </ul> </li> <li><b>Fizyczna warstwa ochrony</b> <ul style="list-style-type: none"> <li>- Obudowy z materiałów epoksydowych zapobiegają dostępowi do elementów fizycznych</li> </ul> </li> </ol>
<ol style="list-style-type: none"> <li><b>Narażenie na ataki siłowe</b></li> </ol>	<ol style="list-style-type: none"> <li><b>10 stopni ochrony przed atakami siłowymi</b> <ul style="list-style-type: none"> <li>- Wymazywanie kasuje zawartość pamięci lub powoduje jej wyłączenie</li> </ul> </li> <li><b>Uniemożliwia dostęp do wrażliwych danych w przypadku zgubienia lub kradzieży pamięci USB</b></li> </ol>
<ol style="list-style-type: none"> <li><b>Nakład pracy dla administratorów systemów MIS / IT</b></li> </ol>	<ol style="list-style-type: none"> <li><b>Minimalny nakład pracy dla działu MIS — łatwe wdrożenie</b></li> </ol>
<ol style="list-style-type: none"> <li><b>Wykorzystuje starsze standardy dla USB</b> <ul style="list-style-type: none"> <li>- 256-bitowe szyfrowanie AES, CBC (poprzedni standard)</li> <li>- zgodność z wymogami FIPS (brak certyfikatu potwierdzającego)</li> </ul> <p><b>Uwaga:</b> Dyski szyfrowane za pomocą algorytmu XTS-AES nie będą dostępne w starszych wersjach systemu Windows.</p> <p><b>Nośniki wymienne powinny w dalszym ciągu obsługiwać 128-bitowe algorytmy AES-CBC lub 256-bitowe algorytmy AES-CBC.</b></p> </li> </ol>	<ol style="list-style-type: none"> <li><b>Firma Kingston korzysta z najnowszych standardów technologicznych</b> <ul style="list-style-type: none"> <li>- 256-bitowe szyfrowanie AES, XTS (najwyższy standard)</li> <li>- certyfikat FIPS 197 i 140-2 Level 3</li> <li>- zgodność z europejskim rozporządzeniem GDPR</li> <li>- NYDFS - zgodność z 23 NYCRR 500</li> <li>- zgodność z TAA</li> </ul> </li> </ol>

Szyfrowane pamięci USB Kingston / IronKey są wśród urządzeń przenośnych, które chronią dane, najlepsze pod względem niezawodności, zgodności i bezpieczeństwa. Oto, co je wyróżnia: 100% zgodności z przepisami i normami | Współpraca z zabezpieczeniami punktów końcowych na potrzeby DLP | Nie wymagają żadnego oprogramowania/sterowników | Przeznaczone do szybkiego i skutecznego wdrożenia.



NINIEJSZY DOKUMENT MOŻE ULEC ZMIANIE BEZ WCZEŚNIEJSZEGO POWIADOMIENIA.  
©2018 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA.  
Wszelkie prawa zastrzeżone. Wszelkie znaki towarowe i zastrzeżone znaki towarowe są własnością odpowiednich właścicieli. MKF - 818 PL

