



## Kingston / Ironkey Encrypted USB Advantage Over BitLocker

<b>MICROSOFT'S BITLOCKER</b> 	<b>KINGSTON / IRONKEY ENCRYPTED USB</b> 
Feature	Kingston Advantage
<b>1. Limited compatibility between OS:</b> <ul style="list-style-type: none"> <li>- ONLY available in the Enterprise &amp; Ultimate editions of Windows 7   Pro &amp; Enterprise editions of Windows 8.1   Windows 10.</li> <li>- Does not Support Mac OS</li> </ul> <b>2. Issues with OS patches / system updates</b> <ul style="list-style-type: none"> <li>- Buggy updates - delays between fixes</li> </ul> <b>3. Vulnerable to "ROCA"</b> <ul style="list-style-type: none"> <li>- Cryptographic flaws in BitLocker</li> <li>- 'Worse Than KRACK' - Google And Microsoft Hit By Massive 5-Year-Old Encryption Hole</li> </ul>	<b>1. Better compatibility between OS:</b> <ul style="list-style-type: none"> <li>- Windows® 10   Windows 8.1   Windows 8   Windows 7 (SP1)   Mac OS X v. 10.10.x - 10.13.x   Linux Kernel v. 2.6.</li> </ul> <b>2. Not affected by "ROCA" Attacks</b>
<b>1. Software-based Encryption</b> <ul style="list-style-type: none"> <li>- Runs on host computer</li> </ul> <b>2. Easier vulnerability attacks</b> <ul style="list-style-type: none"> <li>- Open to keylogging, sniffing, memory / hash attacks</li> </ul>	<b>1. Hardware-based encryption</b> <ul style="list-style-type: none"> <li>- Fully self-contained protection</li> </ul> <b>2. No software vulnerability attacks</b> <ul style="list-style-type: none"> <li>- Eliminates sniffing and memory hash attacks</li> </ul> <b>3. Digitally-signed firmware</b> <ul style="list-style-type: none"> <li>- Cannot be altered</li> </ul> <b>4. Physical layer of protection</b> <ul style="list-style-type: none"> <li>- Epoxy dipped/filled cases prevent access to physical memory</li> </ul>
<b>1. Susceptible to Brute Force Attacks</b>	<b>1. 10 Attempt Brute Force Protection</b> <ul style="list-style-type: none"> <li>- Wipes the drive clean or disables it</li> </ul> <b>2. Prevent anyone from getting your sensitive data if USB drive is lost or stolen</b>
<b>1. MIS / IT Administrator-intensive</b>	<b>1. Minimal MIS efforts - Easy to deploy</b>
<b>1. Uses older technology standards for USB</b> <ul style="list-style-type: none"> <li>- 256-bit AES, CBC (previous standard)</li> <li>- FIPS-compliant (not certified)</li> </ul> <p><b>Note:</b> Drives encrypted with XTS-AES will not be accessible on older versions of Windows.</p> <p><b>Removable drives should continue to use AES-CBC 128-bit or AES-CBC 256-bit algorithms.</b></p>	<b>1. Kingston uses latest technology standards</b> <ul style="list-style-type: none"> <li>- 256-bit AES, XTS (highest standard)</li> <li>- FIPS 197 and 140-2 Level 3 "Certified"</li> <li>- EU GDPR Compliant</li> <li>- NYDFS - 23 NYCRR 500 Compliant</li> <li>- TAA Compliant</li> </ul>

**Overall, Kingston / IronKey Encrypted USB Drives prove to be the best solution in reliability, compatibility and security for portable data protection solutions.** They are 100% Compliant with regulations and standards | Works with endpoint security for DLP needs | No software/ drivers needed | Designed for quick and efficient deployment.



THIS DOCUMENT SUBJECT TO CHANGE WITHOUT NOTICE.  
©2018 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA.  
All rights reserved. All trademarks and registered trademarks are the property of their respective owners.  
MKF - 818

