KINGSTON IRONKEY™

# Enkripsi Perangkat Keras vs. Perangkat Lunak

Pahami perbedaan utamanya, dan cari tahu mana yang sesuai untuk kebutuhan Anda.

Dalam konteks keamanan data, perbedaan antara enkripsi perangkat keras dan perangkat lunak terletak pada lokasi sistem keamanannya dan seberapa rentan perlindungannya dalam penggunaan sehari-hari. Pada drive USB dan SSD, lokasi enkripsi menentukan seberapa aman data terlindungi dan seberapa besar ketergantungannya terhadap sistem di sekitarnya.

| PERANGKAT KERAS | VS | PERANGKAT LUNAK |
|---|---|---|
| **Pengelolaan kunci enkripsi**<br>Kunci enkripsi dibuat secara internal oleh perangkat keras dan disimpan secara aman di dalam drive. | | **Pengelolaan kunci enkripsi**<br>Kata sandi pengguna digunakan secara langsung sebagai kunci enkripsi, dan kunci tersebut dapat tersimpan di memori sistem. |
| **Perlindungan terhadap serangan brute force**<br>Dirancang untuk memberikan perlindungan dari serangan brute force dengan membatasi jumlah percobaan akses sebelum drive menghapus datanya sehingga dapat mencegah siapa pun memperoleh data sensitif jika drive hilang atau dicuri. | | **Perlindungan terhadap serangan brute force**<br>Rentan terhadap serangan brute force, jadi meskipun komputer mencoba membatasi jumlah percobaan dekripsi, hacker tetap dapat mengakses memori komputer dan mereset penghitung percobaan tersebut. |
| **Kebutuhan perangkat lunak atau driver**<br>Tidak memerlukan driver atau instalasi perangkat lunak pada sistem host. | | **Kebutuhan perangkat lunak atau driver**<br>Memerlukan instalasi perangkat lunak, dan driver serta kompatibilitas sistem operasi mungkin berbeda-beda. |
| **Sumber daya enkripsi**<br>Menggunakan prosesor kriptografis khusus yang tertanam ke dalam drive. | | **Sumber daya enkripsi**<br>Menggunakan sumber daya CPU dan sistem komputer untuk enkripsi dan dekripsi data. |
| **Ketergantungan terhadap sistem host/risiko paparan**<br>Keamanan diisolasi di dalam perangkat dan tetap terlindungi bahkan saat terhubung ke komputer yang tidak tepercaya atau terinfeksi. | | **Ketergantungan terhadap sistem host/risiko paparan**<br>Keamanan bergantung pada sistem operasi host dan lebih rentan jika komputer terinfeksi malware. |
| **Status enkripsi**<br>Enkripsi dirancang selalu aktif dan tidak dapat dihapus atau dilewati. | | **Status enkripsi**<br>Enkripsi dapat diaktifkan, dinonaktifkan, atau salah dikonfigurasi. |
| **Dampak terhadap kinerja**<br>Dampak terhadap kinerja sangat minim karena tugas enkripsi dialihkan ke prosesor perangkat keras. | | **Dampak terhadap kinerja**<br>Dapat secara negatif memengaruhi kinerja karena enkripsi menggunakan sumber daya CPU yang sama. |
| **Fleksibilitas**<br>Enkripsi hanya dapat digunakan pada drive USB atau SSD khusus. | | **Fleksibilitas**<br>Dapat diterapkan pada hampir semua media penyimpanan. |

Enkripsi perangkat lunak menawarkan fleksibilitas, sementara enkripsi perangkat keras menjaga keamanan tetap terisolasi dan mengurangi risiko paparan pada tingkat sistem. Dengan memahami cara masing-masing metode melindungi data dan mengendalikan akses, Anda dapat memilih tingkat keamanan yang tepat untuk alur kerja dan profil risiko Anda.

**www.kingston.com/ironkey**