



## Enkripsi Perangkat Lunak

VS

## Enkripsi Perangkat Keras

### HOSTING

Berbagi sumber daya komputer untuk mengenkripsi data dengan program lain di komputer, hanya bisa seaman seperti keamanan komputer Anda.

Menggunakan **prosesor khusus** yang secara fisik berada di drive terenkripsi.

### KATA SANDI

Menggunakan **kata sandi pengguna** sebagai kunci enkripsi yang mengacak data.

Prosesor dilengkapi dengan **alat penghasil angka acak** untuk menghasilkan kunci enkripsi yang akan dibuka oleh kata sandi pengguna.

Dapat memerlukan pembaruan perangkat lunak.

### PEMBARUAN

Peningkatan kinerja dengan **dipindahkannya beban enkripsi** dari sistem host.

### DEKRIPSI

Enkripsi perangkat lunak rentan terhadap peretasan karena **lemahnya perlindungan terhadap serangan Brute Force** yang dilancarkan dengan alat yang mudah diperoleh secara online.

Melindungi kunci enkripsi dan parameter keamanan yang kritis di dalam **perangkat keras kriptografi**.

### AUTENTIKASI

Autentikasi menggunakan **sumber daya sistem host**.

Autentikasi berlangsung di **drive terenkripsi perangkat keras**.

### PERLINDUNGAN

Rentan terhadap **serangan** dan hanya bisa seaman seperti keamanan sistem host.

Perlindungan terhadap **serangan paling umum**, seperti serangan boot dingin, kode berbahaya, dan brute force.

### INSTALASI

Kompatibilitas sistem operasi **dapat berbeda-beda**.

**Tidak memerlukan** instalasi perangkat lunak jenis apa pun pada PC host.

Dapat diterapkan pada **semua jenis media**.

### FLEKSIBILITAS

Enkripsi **terikat pada perangkat khusus** sehingga enkripsi selalu aktif.

### BIAYA

Hemat biaya di lingkungan **penggunaan berskala kecil**.

Hemat biaya di lingkungan **penggunaan berkala sedang dan yang lebih besar** dengan kemudahan peningkatan skala.

## Minta Bantuan Pakar

Merencanakan solusi yang tepat membutuhkan pemahaman atas tujuan keamanan proyek Anda. Biarkan [para pakar Kingston](#) memandu Anda tentang cara terbaik untuk mempertahankan data sensitif Anda.