Get BadUSB protection
from IronKey USB Flash drives.

IronKey™ and DataTraveler® Secure USB devices are not vulnerable to BadUSB malware, which was revealed at The Black Hat conference held in August of 2016. BadUSB is the first USB malware designed to attack the device itself instead of attacking the data on the device. IronKey's leadership in security, including its use of digital signatures in all controller firmware, makes its products immune to this new threat.

As revealed at the Black Hat session on BadUSB, the attack changes the firmware that controls the behaviour of the USB hardware, allowing the USB device to become a host that can subsequently infect other computers and USB devices. The modified controller firmware cannot be detected by today's anti-malware solutions, and in many cases, may remain undetectable.

As explained by the researchers, the best protection against this vulnerability is to use code signing for firmware updates. If the signed firmware is modified, the device cannot authenticate the firmware and simply will not operate. This prevents the infection from spreading but results in an unusable device. That is why in addition to using signed firmware, IronKey protects the mechanism used to update the firmware with hardware-based security keys. This prevents tampering with the signed firmware, which would leave the device unusable.

ADDITIONAL KEY FEATURES

Additional Key Security Features Available for IronKey and DataTraveler Secure USB Drives:

- Secure, military-grade 256-bit AES full disk hardware encryption
- FIPS (Federal Information Processing Standards) 140-2 Level 3 validation
- Centralised management supporting remote wipe/disablement of lost or stolen devices
- Multifactor authentication
- Built-in password protection policies
- Ruggedised, waterproof metal case to resist physical break-ins tamper evident
- Virus/malware protection

IRONKEY™

Kingston TECHNOLOGY