BitLocker es una característica de seguridad de Windows que proporciona cifrado para volúmenes completos, que aborda las amenazas de robo de datos o exposición de dispositivos perdidos, robados o retirados inapropiadamente.

**Aplicaciones.**

Los datos de un dispositivo perdido o robado son vulnerables al acceso no autorizado, ya sea mediante la ejecución de una herramienta de ataque de software contra él o la transferencia del disco duro del dispositivo a otro dispositivo. BitLocker ayuda a mitigar el acceso a datos no autorizados mediante la mejora de las protecciones de archivos y del sistema y la representación de datos inaccesibles cuando los dispositivos protegidos por BitLocker se retiran o reciclan.

**BitLocker y TPM**

BitLocker proporciona la máxima protección cuando se usa con un módulo de plataforma segura (TPM), que es un componente de hardware común instalado en dispositivos Windows. El TPM funciona con BitLocker para asegurarse de que un dispositivo no se ha alterado mientras el sistema está sin conexión.

*Además* del TPM, BitLocker puede bloquear el proceso de inicio normal hasta que el usuario proporcione un número de identificación personal (PIN) o inserte un dispositivo extraíble que contenga una *clave de inicio*. Estas medidas de seguridad proporcionan autenticación multifactor y garantía de que el dispositivo no puede iniciarse ni reanudarse desde la hibernación hasta que se presente el PIN o la clave de inicio correctos.

En los dispositivos que no tienen un TPM, BitLocker todavía se puede usar para cifrar la unidad del sistema operativo. Esta implementación requiere que el usuario:

* use una clave de inicio, que es un archivo almacenado en una unidad extraíble que se usa para iniciar el dispositivo o al reanudarse desde la hibernación.
* usar una contraseña. Esta opción no es segura, ya que está sujeta a ataques por fuerza bruta, ya que no hay una lógica de bloqueo de contraseña. Por lo tanto, la opción de contraseña se desaconseja y deshabilita de forma predeterminada

Ambas opciones no proporcionan la comprobación de integridad del sistema de arranque previo ofrecida por BitLocker con un TPM