

# McAfee Encrypted USB

## Protezione di dati mobili con dispositivi McAfee® Encrypted USB

I piccoli drive di storage USB con elevate capacità consentono ai lavoratori di trasportare ovunque enormi quantità di dati aziendali riservati. Inoltre, i dipendenti benintenzionati sono spesso ignari dei rischi e dei costi di sicurezza significativi a cui potrebbe andare incontro la loro azienda se le unità venissero smarrite o rubate. Per di più la maggior parte di queste chiavette USB non è controllata o gestita dal dipartimento IT, né rientra nelle policy di sicurezza aziendali. Tutto questo aumenta il rischio di accessi non autorizzati, fughe di dati e mancata conformità normativa. L'estensione delle policy di sicurezza aziendali centralizzate al controllo e alla gestione dei dispositivi USB è fondamentale per gli ambienti mobili di oggi.

### Vantaggi principali

- Conformità con le policy di sicurezza aziendali, le normative sulla privacy dei dati e i regolamenti di settore attraverso l'uso di dispositivi USB crittografati con l'hardware
- Mobilità dei dati senza compromettere le policy di sicurezza
- Possibilità di rintracciare e gestire i dispositivi USB crittografati dell'intera azienda tramite la piattaforma McAfee ePO per la generazione di rapporti di sicurezza, la verifica, il monitoraggio e la gestione della policy.
- Controllo dei dati di accesso con l'autenticazione a due o tre fattori
- Protezione dei dati con le convalide e gli algoritmi di cifratura migliori del settore, come AES-256 e FIPS 140-2, per una valida protezione

### Sicurezza dei dati

Le informazioni copiate nei dispositivi McAfee Encrypted USB vengono crittografate e possono essere lette solo da persone autorizzate. Il controllo dell'accesso utenti integrato e la cifratura dei dati hardware molto avanzata tutelano la sicurezza dei dati sensibili, ovunque questi dispositivi vengano spostati.

### Gestione centralizzata

L'implementazione e la gestione dei dispositivi portatili di storage in azienda possono essere attività complesse e costose. Inoltre, poiché le unità USB non sono solitamente gestite dal gruppo IT, spesso non sono tutelate dalle policy di sicurezza valide a livello di azienda. La piattaforma McAfee ePolicy Orchestrator® (McAfee ePO™) risolve tali problemi implementando e gestendo i dispositivi McAfee Encrypted USB centralmente da una singola console, così da migliorare la sicurezza aziendale e ridurre il costo totale di possesso. Gli utenti inizializzano i dispositivi semplicemente inserendoli in un computer gestito da McAfee ePO.

### Cifratura hardware efficace

Tutti i dati presenti sui dispositivi McAfee Encrypted USB sono cifrati utilizzando gli algoritmi di cifratura standard basati su hardware più efficaci, incluso AES-256, oltre a certificazioni industriali, come la certificazione Federal Information Processing Standards (FIPS) 140-2. La cifratura hardware incorporata, la generazione delle chiavi e l'archiviazione dei certificati, impediscono

di ottenere o copiare le chiavi di cifratura, dal momento che sono indivisibili dall'unità USB. Facoltativamente è possibile archiviare altre chiavi di cifratura e/o certificati PKI (Public Key Infrastructure).

Per accedere ai dati sui dispositivi McAfee Encrypted USB, gli utenti devono autenticarsi utilizzando una password o un'impronta digitale, impedendo l'accesso ai dati non autorizzato. Per la sicurezza massima, è possibile utilizzare l'autenticazione a due fattori. Se gli utenti dimenticano una password o se non hanno la possibilità di eseguire l'autenticazione biometrica, possono facilmente riottenere l'accesso ai dati attraverso un reset centralizzato della password oppure eseguendo un self rescue con il software McAfee ePO.

### Dimostrare la conformità normativa

Poiché sono integrati nella console di gestione McAfee ePO, i dispositivi McAfee Encrypted USB supportano le operazioni di conformità, dalle policy di sicurezza aziendali ai regolamenti specifici del settore fino alla legislazione sulla privacy dei dati. È possibile dimostrare che i dati presenti su un dispositivo USB rubato o smarrito erano cifrati ed eseguire dei rapporti in cui siano specificati l'accesso ai dati e l'utilizzo della USB a scopo di azioni di auditing.

### Funzionalità principali

- Implementazione di controllo accessi avanzato per dispositivi di storage USB rimovibili e cifratura dei dati su hardware utilizzando la cifratura hardware Advanced Encryption Standard (AES-256)

**Specifiche**

Nota: I requisiti di sistema variano a seconda dei dispositivi scelti dall'azienda.

**McAfee Encrypted USB Standard**

- Sistemi operativi: Microsoft Windows XP, Windows Vista, Windows 7 (a 32 e 64 bit)
- Hardware: disponibili nei formati da 1 a 64 GB

**McAfee Encrypted USB Bio**

- Sistemi operativi: Windows XP, Windows Vista, Windows 7 (a 32 e 64 bit); Mac OS 10.5 e 10.6 1
- Hardware: disponibili nei formati da 1 a 64 GB

**McAfee Encrypted USB Hard Disk**

- Sistemi operativi: Windows XP, Windows Vista, Windows 7 (a 32 e 64 bit); Mac OS 10.5 e 10.6 3
- Hardware: disponibili nei formati da 250 a 750 GB

**McAfee Encrypted USB Hard Disk Non-Bio**

- Sistemi operativi: Windows XP, Windows Vista, Windows 7 (a 32 e 64 bit)
- Hardware: disponibili nei formati da 250 a 750 GB

- Impostazione di un numero massimo di tentativi di inserimento password o di autenticazione biometrica per contrastare gli attacchi di tipo brute-force con opzioni per il ripristino utente o la distruzione dei dati
- Massimizzazione della flessibilità grazie al zero-client footprint e garanzia di sicurezza indipendentemente dall'ambiente del sistema operativo: non sono necessari diritti di installazione software o di amministratore. Basta una semplice porta USB.
- Prevenzione dell'accesso non autorizzato ai dati con l'autenticazione a due fattori che richiede agli utenti di autenticarsi utilizzando una password o la propria impronta
- Installazione ed esecuzione della applicazioni direttamente e in modo protetto dal dispositivo USB (PC-on-a-Stick, browser Internet, thin client e molto altro)<sup>2</sup>; gli utenti possono avviare delle applicazioni in modo comodo e sicuro ovunque si trovano.
- La generazione di chiavi di cifratura incorporata e l'archiviazione dei certificati impedisce alle chiavi di cifratura di essere copiate perché sono indivisibili dall'unità USB. Inoltre è disponibile l'opzione per memorizzare altre chiavi di cifratura e/o certificati per infrastrutture a chiavi pubbliche (PKI).
- L'antimalware incorporato contribuisce a proteggere le unità USB e i computer e le reti cui si connettono con un motore di scansione antimalware che rileva automaticamente e blocca le minacce presenti nei dispositivi USB (richiede la gestione della piattaforma McAfee ePO)

**Dispositivi McAfee Encrypted USB**

Nella tabella seguente sono elencate le funzionalità principali della gamma di dispositivi McAfee Encrypted USB. Le chiavette USB possono avere dimensioni di archiviazione che variano da 1 GB a 64 GB; i dischi rigidi USB possono avere dimensioni di archiviazione che variano da 250 GB a 750 GB.

**Semplice matrice delle caratteristiche del prodotto**

|   | McAfee Encrypted USB Standard | McAfee Encrypted USB Bio | McAfee Encrypted USB Hard Disk Non-Bio | McAfee Encrypted USB Hard Disk |
|---|-------------------------------|--------------------------|--|--------------------------------|
| Autenticazione tramite password o scheda CAC/PIV                    | ●                             | ●                        | ●                                      | ●                              |
| Autenticazione biometrica   |                               | ●                        |  | ●                              |
| Autenticazione hardware AES a 256-Bit                               | ●                             | ●                        | ●                                      | ●                              |
| Funzionalità di virtualizzazione (PC-on-a-Stick) <sup>2</sup>       | Opzionale                     | Opzionale                | Opzionale                              | Opzionale                      |
| Convalidato FIPS 140-2  | ●                             | ●                        | ●                                      | ●                              |
| Gestione centralizzata con McAfee ePolicy Orchestrator (McAfee ePO) | ●                             | ●                        | ●                                      | ●                              |
| Protezione antimalware McAfee                                       | ●                             | ●                        | ●                                      | ●                              |

<sup>1</sup> Mac OS X è supportato per i dispositivi gestiti dopo l'inizializzazione su un sistema Windows gestito da McAfee ePO e su dispositivi non gestiti solo se utilizzati con autenticazione biometrica (autonoma, biometrica).

<sup>2</sup> Software di altri produttori richiesto, con costi aggiuntivi.

<sup>3</sup> Mac OS X è supportato per i dispositivi gestiti dopo l'inizializzazione su un sistema Windows gestito da McAfee ePO e su dispositivi non gestiti solo se utilizzati con autenticazione biometrica (autonoma, biometrica).

Per ulteriori informazioni sui dispositivi McAfee Encrypted USB, visitare il sito [www.mcafee.com/it/products/data-protection/index.aspx](http://www.mcafee.com/it/products/data-protection/index.aspx).

