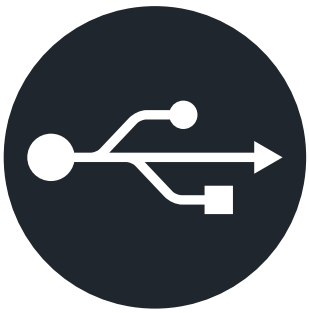
Come consentire l'accesso ai drive USB

senza compromettere la sicurezza degli endpoint

Introduzione

Nel gennaio 1996 veniva rilasciata la specifica ufficiale USB 1.0, con l'obiettivo di aprire la strada a una nuova era di uniformità, praticità e versatilità sia per i fornitori di periferiche che per gli utenti finali. Sono trascorsi 27 anni da allora e questo standard mantiene ancora la compatibilità con tutte le versioni precedenti, così che USB resta la pietra angolare dell'interfacciamento hardware con i computer - dai server agli smartphone.



La semplicità plug-and-play dello standard USB e le velocità sempre crescenti hanno fatto evolvere lo storage portatile USB facendolo diventare una delle soluzioni più diffuse. Tuttavia, tale comodità deve fare i conti con alcuni aspetti relativi alla sicurezza dei dati. Nel mondo attuale, senza l'uso di strumenti adeguati come la protezione degli endpoint sui computer host e senza le corrette pratiche di sicurezza dei dati, gli utenti che adottano atteggiamenti troppo disinvolti nell'uso degli storage USB portatili espongono se stessi e gli altri al rischio di data-breach, da cui possono derivare conseguenze molto gravose per l'utente finale, tali da poter compromettere persino un'intera organizzazione o amministrazione.

Oltre a proteggere l'ambiente che ospita il drive USB, è essenziale anche proteggere quest'ultimo tramite password e crittografia hardware on-device. In questo modo si raggiunge il massimo livello di difesa contro le intrusioni. Esamineremo alcune delle best-practice che garantiscono un impiego più sicuro delle unità USB, dando uno sguardo più approfondito al mondo dei drive USB.

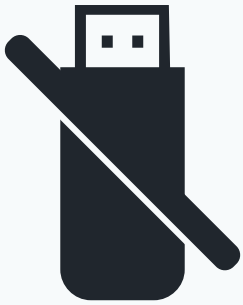
La sicurezza dipende essenzialmente dalla solidità della crittografia e dalla qualità dei componenti hardware che compongono il drive USB, sebbene sia la perfetta integrazione di questi due elementi a rappresentare la soluzione ideale. A trarne vantaggio possono essere praticamente tutti i settori, dalla finanza all'assistenza sanitaria, all'industria manifatturiera e al campo militare. Inoltre, si rivelano importanti anche per il lavoro in remoto, laddove accedere alla rete aziendale risulta impossibile, pericoloso o poco pratico.

È possibile scegliere drive USB dotati di crittografia con tipologie di certificazione diverse e numerose funzionalità di sicurezza. Considerando le tante funzionalità e possibilità di personalizzazione, la loro idoneità come soluzione stand-alone risulta dimostrata anche dalla loro posizione consolidata in ogni tipo di ambiente che tratta dati sensibili.

Gestione delle porte: incontro fra software DLP per la gestione degli endpoint e storage USB

Per decenni, le applicazioni antivirus e anti-malware hanno offerto il livello principale di protezione, scansionando automaticamente i file scaricati e i dispositivi collegati e segnalando o reagendo in caso di contenuti sospetti. La protezione offerta dal software antivirus di nuova generazione (NGAV) fa un ulteriore passo avanti. Invece di affidarsi esclusivamente a un database continuamente aggiornato di segnalazioni virus, l'NGAV apporta funzionalità di machine learning e rilevamento comportamentale in grado di identificare e mitigare le minacce sconosciute.

Tuttavia, questi software non sono l'unica freccia nella faretra: chi vuole una protezione assoluta dai rischi derivanti dalle periferiche utente e da altre fonti esterne, può utilizzare il software DLP ("Data Loss Prevention", ovvero prevenzione dal rischio di perdita dei dati) per la gestione di endpoint, che fornisce i mezzi per negare qualsiasi tipo di accesso alle porte USB e ad altri punti di accesso.



L'approccio alla sicurezza del tipo "Blocco totale delle porte" può certamente eliminare i rischi e, in alcune circostanze, può essere addirittura auspicabile, ma si tratta di una politica che spesso si rivela troppo brutale e può anche essere fonte di conseguenze poco desiderabili.

Tuttavia, alcuni amministratori IT preferiscono negare l'accesso alle porte USB dei computer degli utenti, visto che tali accessi offrirebbero un accesso diretto in grado di "bucare" il firewall aziendale. Parliamo di una cautela senz'altro comprensibile, che tuttavia – quando si tratta di archiviare qualcosa nei drive USB – non dovrebbe comportare eccessiva macchinosità nella gestione delle autorizzazioni, una volta che siano state adottate adeguate precauzioni.

È ad esempio essenziale adottare un'applicazione di gestione degli endpoint, dotata di una funzionalità di rilevazione delle minacce, tramite scansione con antivirus/anti-malware, oltre alla gestione e al monitoraggio centralizzati di tutti gli endpoint utente.

Fornitori molto noti, quali McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection e WinMagic SecureDoc – giusto per citarne alcuni – offrono soluzioni integrate di questa tipologia già pronte all'uso.

White-list granulari

Il metodo da adottare per mettere in sicurezza i dispositivi di storage USB dipende dal livello di protezione che è necessario raggiungere. Un approccio semplice e al tempo stesso efficace consiste nel creare liste di dispositivi USB autorizzati (cd. "white list"), in cui vengono elencati i rispettivi codici VID (Vendor Identifier) e PID (Product Identifier). Uno degli aspetti che occorre tenere presente per le periferiche USB è che ogni produttore ha un suo codice VID univoco, ma il codice PID varia ogni volta che viene creato un nuovo prodotto.

Nello stilare una white list, l'uso del solo VID del produttore sarebbe troppo generico, dal momento che risulterebbero autorizzati tutti i dispositivi USB fabbricati da un determinato produttore. Il codice PID offre un maggior livello di dettaglio, perché consente di stabilire che solo un determinato modello di storage possa accedere al sistema in cui dovrà essere ospitato.

Approccio questo sicuramente migliorativo, ma non risolutivo. I dispositivi di storage USB sono enormemente diffusi, visto che consentono agli utenti di acquistare i propri dispositivi, facendo riferimento ai modelli autorizzati. Ben consapevole di questa problematica, Kingston Technology ha prodotto una soluzione su misura in grado di rafforzare la sicurezza dei dispositivi di archiviazione USB.

Grazie al programma di Personalizzazione, un'organizzazione può richiedere la creazione e l'applicazione di un proprio profilo PID a un'intera gamma di drive flash USB con crittografia Kingston. Le società che adottano dispositivi dotati di un PID personalizzato possono così rendere più semplice ed efficace la propria strategia di white-list e raggiungere livelli di sicurezza più elevati. Infatti, i dispositivi acquistati privatamente dai dipendenti, per quanto possano risultare identici a quelli autorizzati, troverebbero comunque l'accesso negato visto che il loro PID non sarebbe riconosciuto.

Oltre all'uso di codici PID personalizzati, che consente ai responsabili IT di rendere disponibili nuovi dispositivi di storage USB in modo più semplice e veloce, esiste anche un'alternativa ancora più granulare, che consiste nell'utilizzo del numero di serie

del singolo dispositivo, disponibile nella maggior parte dei drive USB con crittografia di Kingston. In questo caso è necessario registrare nella suite di gestione dell'endpoint i numeri di serie di ogni singolo dispositivo autorizzato. Kingston può agevolare enormemente il processo di elaborazione iniziale svolto dal personale IT, fornendo in allegato a ogni ordine l'elenco dei numeri di serie – sempre alfanumerici e non sequenziali. La scelta di questo metodo consente politiche molto più flessibili basate sulla proprietà del singolo drive con l'ulteriore vantaggio del tracciamento preciso della provenienza dei dispositivi, che può rivelarsi prezioso negli scenari IT di tipo forense. Alcuni drive Kingston riportano un numero di serie e un codice a barre sull'involucro che può essere scansionato elettronicamente, mentre altri drive possono essere personalizzati in modo da aggiungere tali codici sull'involucro destinato alle aziende; grazie a questi elementi è possibile eseguire il tracciamento dei drive.

Per impostazione predefinita, i sistemi di gestione degli endpoint consentono di accedere ai codici VID/PID da utilizzare per il blocco delle porte e la stesura di white list. Il vantaggio aggiuntivo offerto da Kingston consiste nella maggiore versatilità d'uso di queste funzionalità, che permette di adottare policy più versatili e ingegnose tramite cui facilitare l'uso dei dispositivi di archiviazione USB. Una volta stabilito un metodo di identificazione appropriato, la posizione assoluta di "Blocco totale delle porte" non solo risulta eccessivamente semplicistica, ma diventa anche improduttiva.

Soluzioni conformi e sicure per gli utenti remoti

Parlando di sicurezza, la stesura di elenchi di dispositivi ammessi (white list) rappresenta solo metà del problema, o detto in altro modo, solo metà della soluzione.

La comodità e la semplicità dei dispositivi di storage USB li rende indispensabili in molte aziende e istituzioni, dove la fluidità del trasferimento dei dati non può prescindere dall'uso di questi strumenti. Nella maggior parte degli ambienti lavorativi – per conformarsi alle normative vigenti e mantenere una sana organizzazione dell'infrastruttura IT – risulta obbligatorio dotare il personale di drive USB crittografati. L'uso combinato della protezione mediante password e della crittografia del dispositivo equipaggia lo storage portatile con uno scudo insuperabile, capace di impedire l'accesso ai dati sensibili nel caso in cui il dispositivo venisse smarrito, sottratto o lasciato in un ambiente potenzialmente pericoloso.

Questo scudo può avere molteplici aspetti, dal momento che le tecniche di crittografia variano: le differenze più significative emergono mettendo a confronto soluzioni di crittografia hardware e software. Qual è la migliore? Dipende dalle esigenze, ma volendo formulare la domanda in modo più corretto bisognerebbe chiedersi "Qual è la più sicura?"

La crittografia software è sostanzialmente una soluzione economica, che si rivela idonea in quei settori caratterizzati da un'operatività contenuta. È una scelta adatta anche per le imprese in cui non si trasferiscono dati sensibili e in cui l'obbligo di adottare queste soluzioni è imposto per lo più da policy aziendali.

Tuttavia, il tallone di Achille della crittografia software risiede nel suo stesso funzionamento, visto che le attività di decodifica vengono svolte da applicazioni residenti sul computer, che in questo modo rendono possibile l'accesso ai dati presenti nello storage portatile. Ne consegue che un dispositivo di storage dotato di crittografia software risulta sicuro quanto il computer a cui è collegato.

Inoltre, risulta anche maggiore il rischio di intrusione, visto che gli hacker, tramite l'accesso alla memoria del computer possono "arrivare" alle chiavi di crittografia/decrittografia. I dati presenti sul drive possono poi essere soggetti ad attacchi di forza bruta, in quanto l'accesso protetto mediante password non è necessario se è consentito accedere e copiare i file crittografati.

Va poi ricordato che la crittografia di tipo software necessita di regolari aggiornamenti software, che possono complicarne l'implementazione e aumentare il carico di lavoro del personale IT. Ma l'aspetto peggiore sta forse nel fatto che la crittografia software può essere completamente rimossa da dipendenti frustrati che trovano complicato il collegamento del drive alle varie piattaforme. Gli utenti del drive USB potrebbero infatti copiare i dati di questa unità crittografata in un computer, riformattare il drive trasformandolo in un'unità non crittografata e, a quel punto, ricopiarvi sopra i dati. In questo modo, i dati cesserebbero di essere al sicuro e sarebbero totalmente esposti al rischio di una violazione. Questo approccio è dunque inattuabile nei contesti in cui è necessario preservare la conformità a leggi e regolamenti sulla privacy, visto che la sicurezza del drive USB può essere radicalmente disabilitata.

Crittografia "on-chip": la soluzione rapida e concreta

Al contrario, un drive USB con crittografia hardware funziona in modo indipendente dal computer, in quanto dispone di un processore integrato nel drive stesso che gestisce autonomamente la crittografia. In questo modo il processo di crittografia è sempre attivo attuando una protezione contro gli attacchi di forza bruta alle password: i dati crittografati non sono accessibili e non possono essere copiati.

I drive USB di Kingston con crittografia hardware di livello enterprise e militare utilizzano la crittografia AES a 256 bit in modalità XTS. Si tratta di una tecnologia crittografica approvata a livello globale, che fornisce rigorose garanzie sui dati. Utilizzando due chiavi indipendenti che agiscono in fasi diverse del processo di crittografia/decrittografia, la modalità XTS è come se effettuasse due volte la crittografia dei dati.

In pratica, la chiave di crittografia viene prodotta dal generatore di numeri casuali del controller interno al drive, che a sua volta viene sbloccato dalla password dell'utente. Poiché l'autenticazione viene realizzata da un meccanismo crittografico che si trova dentro il dispositivo, le chiavi di crittografia e le altre funzioni di sicurezza sono protette dai comuni attacchi quali BadUSB, avvio a freddo, codice dannoso e forza bruta.

Uno dei vantaggi più facilmente percepibili della crittografia hardware consiste nelle prestazioni del drive, che risultano significativamente migliori rispetto a un drive con crittografia software, in quanto non vi è alcun offload delle attività di crittografia nel computer host. Tutto avviene all'interno del drive.

I drive USB con crittografia hardware, come Kingston IronKey D500S, sono dispositivi protetti da password la cui crittografia è attiva "out of the box". In pratica, l'unico volume visibile da cui è possibile iniziare l'interazione con il drive è quello del launcher con protezione da lettura, visto che qui è contenuta l'applicazione usata per autenticare la password e sbloccare il volume di storage principale crittografato. Questa procedura evita l'installazione di qualsiasi tipo di driver o software nel PC a cui è collegato il drive.

Inoltre, i drive USB di Kingston con crittografia hardware sono dotati di driver firmware con firma digitale, così da prevenire qualsiasi rischio di manipolazione del firmware all'interno del dispositivo. Questo strato di sicurezza aggiuntivo protegge da attacchi BadUSB, che sfrutta una vulnerabilità tipica del firmware dei dispositivi USB. In questi casi infatti comandi e codice dannoso vengono eseguiti segretamente nel computer host.

Ovviamente, anche un approccio del tipo "Blocco totale delle porte" limiterebbe il rischio di attacchi BadUSB, ma perché sacrificare la produttività con pratiche così anacronistiche? Come abbiamo appena visto, l'uso di dispositivi di storage portatili non è incompatibile con un ambiente sicuro: basta solo attuare alcune semplici procedure di acquisizione e implementazione, volte a introdurre i drive USB con crittografia hardware nell'operatività dell'organizzazione.

Lavoro da remoto sicuro e conforme alle normative

Dal momento che il lavoro da remoto viene svolto da persone che si trovano fuori dal fossato che protegge l'ambiente di lavoro aziendale, è necessario predisporre una nuova strategia sulla sicurezza, rivedendo l'ordine delle priorità.

Nella stesura di un piano di sicurezza per accessi da remoto, ha davvero senso pensare di bloccare le porte USB nei laptop dei dipendenti, considerando che questi dovranno connettersi via Internet e accedere a un server per caricare/ottenere documenti? Quando sono per strada, l'unico canale di connessione disponibile potrebbe essere una connessione Internet aperta, come i tanti punti di accesso Wi-Fi senza protezione ed è da qui che nascono numerosi pericoli che potrebbero portare a un data-breach.

Pensiamo a minacce quali l'intercettazione e il controllo dei dati attraverso lo spoofing, gli attacchi Man-In-the-Middle (MitM) e le intercettazioni di rete e ai tanti altri metodi di hacking sempre più sofisticati inventati dai criminali informatici. Anche le VPN possono essere compromesse oggigiorno.

La connessione di rete di un'organizzazione a Internet rappresenta un endpoint e la sua esposizione intrinseca lo rende un punto di ingresso estremamente vulnerabile e appetibile per i criminali. Aprirlo all'accesso remoto comporta specifici rischi per la sicurezza, soprattutto quando vi sono in ballo dati sensibili.

Affidare ai lavoratori remoti drive USB protetti da password e crittografia hardware elimina efficacemente potenziali vulnerabilità di rete. Tuttavia, l'acquisto di tali dispositivi richiede un esame più approfondito delle soluzioni USB disponibili e del modo in cui possono soddisfare le esigenze dei diversi ambienti di lavoro remoto. Non si tratta semplicemente di scegliere un drive in base alla sua capacità o di decidere se deve avere il suo numero di serie registrato, ma bisogna andare oltre e valutare le caratteristiche fisiche del dispositivo

Misure a prova di manomissione: le scelte valide in campo

Il punto essenziale qui è capire se un drive USB con crittografia hardware è a prova di manomissione o meno. Il grado di sicurezza di un dispositivo a tale tipo di intromissione viene misurato dallo standard FIPS 140-3, che ha diversi livelli attestanti la resilienza della struttura fisica di un drive, a prescindere dall'utilizzo dei metodi crittografici.

La certificazione FIPS-197 osserva invece solo le caratteristiche di crittografia hardware, posseduti da dispositivi destinati ad aziende con esigenze di sicurezza dei dati di tipo non militare, come nel caso della serie Kingston IronKey Vault Privacy 50 e del drive SSD esterno Vault Privacy 80. Questi drive sono meno costosi, ma sono anche privi di una protezione efficace contro la manomissione fisica dell'unità.

I dispositivi cui viene riconosciuta la certificazione FIPS 140-3 di livello 3 dimostrano di essere dotati di metodi antimanomissione di grado militare. Kingston fornisce drive FIPS 140-3 di livello 3 a imprese, governi e forze armate in tutto il mondo.

Un'ulteriore barriera difensiva viene prodotta usando gli epossidici come rivestimento interno di tutti i circuiti del drive necessari alla sicurezza e per l'incollaggio dei componenti all'interno dell'involucro. Qualsiasi tentativo di aprire la custodia metallica sarebbe estremamente complesso e produrrebbe la rottura dei chip interni e di altri componenti, rendendo il drive di fatto inutilizzabile. Grazie all'impiego di questo epossidico duro e opaco, la manomissione dei componenti essenziali diventa pressoché impossibile. Kingston utilizza questa misura di sicurezza nei suoi drive IronKey D500S e S1000.

Le protezioni previste per questi dispositivi non si limitano alle sole misure fisiche e, ad esempio, Kingston IronKey S1000 porta la difesa anti-manomissione a un livello ancora superiore. Il criptochip interno all'IronKey S1000 è in grado di rilevare i tentativi di manomissione fisica e rende il drive inutilizzabile alla successiva accensione. Affidarsi a dispositivi di archiviazione USB dotati di crittografia hardware per accedere e trasferire file sensibili è una scelta pragmatica, che agevola l'operatività da remoto, garantendo efficacemente la sicurezza sul campo, senza tuttavia creare inutili difficoltà.

È essenziale valutare con cura le diverse tipologie di drive USB, per individuare il modello dotato delle caratteristiche di sicurezza e di hardware adeguate al tipo di attività, di esigenza e di impiego cui deve essere destinato. Ogni drive USB va esaminato infatti sullo sfondo del caso d'uso concreto, facendosi assistere da consulenti fidati, che aiutino ad adottare le giuste decisioni. Qualunque siano le priorità, Kingston offre una vasta gamma di soluzioni USB dotate di crittografia hardware e assistite da opzioni di personalizzazione, a prezzi accessibili e adatte a qualsiasi tipo di impiego: dalle esigenze di conformità generica fino ai più impegnativi impieghi di tipo militare.

La sicurezza al primo posto: nessuna rete, nessun problema

Oggi, l'ufficio non ha più pareti e il costante diffondersi del lavoro da casa ha messo in luce i problemi di vulnerabilità che l'accesso remoto crea per tante aziende. Sono in molti a stare sperimentando queste difficoltà per la prima volta e a cercare quindi modi più sicuri per adattarsi a questa tendenza in continua diffusione.

I dispositivi USB dotati di crittografia hardware rappresentano una soluzione sicura e ben consolidata, che risponde adeguatamente a questa esigenza in numerosi settori, inclusi quelli in cui il trasferimento dei dati tramite reti si rivela poco pratico o è sconsigliato per i più disparati motivi.

Nel settore finanziario, le autorità di regolamentazione richiedono spesso dati per verificare la condotta e la conformità di un'impresa. Il rischio di divulgazione incontrollata è troppo elevato per pensare di trasferire attraverso una rete documenti sensibili contenenti dettagli sugli investimenti, sui movimenti di mercato e su altre attività bancarie riservate. La soluzione semplice ed efficace consiste nel trasferire queste informazioni all'interno di un drive USB con crittografia hardware.

Anche nel settore sanitario il trasferimento dei file tramite drive USB sicuri è oramai all'ordine del giorno. Ciò risponde, ad esempio, alle esigenze di medici o consulenti, che spesso vogliono poter analizzare le cartelle cliniche, farvi riferimento per la ricerca o usarle come casi da mostrare agli studenti di medicina. Ma vi sono anche esigenze di natura pratica, legate ad esempio a sistemi proprietari come gli strumenti di diagnostica per immagine, per i quali l'accesso alla rete è impossibile o troppo pericoloso: in questo caso, i file possono essere facilmente trasferiti per essere usati altrove tramite drive USB conformi e dotati di crittografia hardware.

Cosa fare e non fare

✓ **Usare drive sicuri e conformi** ed esaminarne le specifiche in modo da dotarsi di drive che rispondano pienamente alle proprie effettive esigenze.

✗ **Non autorizzare politiche BYOD (Bring Your Own Device) che prevedano l'uso di dispositivi casuali o personali** – pericolosi per qualsiasi impresa: lo smarrimento di drive non crittografati rappresenta un prezzo troppo alto, sia in termini di danni finanziari che di immagine.

✓ **Adottare una suite di gestione dell'endpoint** e usare drive USB con crittografia hardware dotati di funzionalità di white list individuali.

✗ **Non lasciare nulla al caso.** Predisporre con cura la regolamentazione del lavoro in sede e da remoto.

✓ **Formare il personale** sul tema della sicurezza. La protezione dal rischio di violazione della sicurezza è un interesse primario delle stesse imprese.

✗ **Non rendere la sicurezza così complicata** da spingere gli utenti a cercare soluzioni che agirino le regole e portino all'adozione di dispositivi IT non autorizzati. Non è detto che i regolamenti generali adottati fino ad oggi possano adattarsi perfettamente a tutti gli scenari. Il posto di lavoro si sta evolvendo e la scelta di soluzioni adeguate consente di sviluppare e attuare nuove politiche.

È in scenari come questo che si rivela perfetto il drive Kingston IronKey Keypad 200 (KP200). Essendo indipendente dal sistema operativo, non esiste un volume di avvio in cui inserire la password: lo sblocco avviene infatti tramite un tastierino alfanumerico, che rende il drive utilizzabile su qualsiasi piattaforma. Al pari di un coltellino svizzero, questo drive USB con crittografia hardware si rivela perfetto anche per il settore industriale, dove consente di trasferire in modo sicuro le applicazioni messe a punto nei reparti di ricerca e sviluppo IT, direttamente all'interno dei macchinari controllati tramite piattaforme di tecnologia operativa (OT). E ciò vale anche per gli impieghi con piattaforme miste, in cui è presente anche Linux, dove il drive KP200 si rivela una fra le soluzioni disponibili più semplici e sicure.

I dispositivi di storage USB con crittografia hardware giocano un ruolo centrale anche nell'attività delle forze dell'ordine, consentendo di proteggere e trasferire in sicurezza i file, le immagini e le altre prove relative ai vari casi alle squadre investigative e ai collegi forensi. Kingston offre un ulteriore vantaggio in quanto può fornire drive che riportano il numero di serie interno stampato sull'involucro esterno insieme a un codice a barre. L'assegnazione e la catalogazione dei drive diventano agevoli e facilmente tracciabili: basta registrare manualmente il numero di serie o, ancora più rapidamente, scansionarne il codice a barre, per rendere così il controllo e la gestione dell'inventario estremamente facili. Si tratta di una caratteristica standard per i drive Kingston IronKey D500S, D500SM e S1000B/E, ma è disponibile anche per altri modelli con crittografia hardware come parte del programma di personalizzazione Kingston.

Sicurezza e storage mobili: lo stato dell'arte

Protezione mediante password, crittografia hardware, soluzioni anti-manomissione, whitelist granulare degli endpoint, certificazione FIPS 140-3 di livello 3 (in fase di approvazione) di grado militare e log-in immediato sono tutte funzionalità standard dei drive USB Kingston, che qualsiasi organizzazione può adottare con totale immediatezza.

Queste efficaci misure di sicurezza garantiscono una protezione continua dei drive USB e dei relativi dati all'interno degli ambienti host. E benché le specifiche sulla carta possano apparire esaustive, la scelta di un modello a caso, operata senza un'opportuna ricerca e riflessione preliminare, potrebbe non produrre la piena soddisfazione di alcune organizzazioni che hanno esigenze specifiche.

In qualità di produttore indipendente, Kingston offre una vasta gamma di opzioni in risposta alle necessità dei clienti. Attraverso il proprio programma di personalizzazione, Kingston rende disponibili soluzioni avanzate pensate per offrire un'esperienza utente perfetta.

La personalizzazione sicura va oltre l'offerta del solo PID univoco dell'organizzazione da usare per la stesura di white list dei drive USB. Kingston consente infatti di personalizzare anche il profilo di sicurezza dell'applicazione di avvio tramite quindici diverse preferenze, che includono i dettagli di contatto e aziendali, l'abilitazione dei suggerimenti sulla password e la determinazione del numero massimo di tentativi di password. E per quanto riguarda la parte esterna, è possibile personalizzarla con il marchio aziendale (co-logo) e con una gamma di colori diversa per le singole unità. Tutte queste funzionalità offrono un percorso di integrazione estremamente semplice da realizzare per la distribuzione di nuovi dispositivi, con un ordine minimo di sole cinquanta unità.

Nel caso in cui non fosse ancora stata adottata un'applicazione di gestione degli endpoint per l'archiviazione USB sicura, Kingston offre una soluzione di gestione indicata per le organizzazioni che desiderano gestire la propria flotta di drive Kingston che include anche la funzione di reimpostazione delle password da remoto.

L'ubiquità e la comodità tipiche dello standard USB gli hanno permesso di sopravvivere a una varietà di tecnologie pur promettenti e, per molti impieghi, l'immediatezza e la praticità dello storage USB risultano insuperabili. I drive USB protetti, agevolmente implementabili e sempre sicuri, rappresentano una soluzione semplice in grado di produrre vantaggi immediati.

Perché esporre gli ambienti di lavoro delocalizzati al rischio di sottrazione dei dati attraverso la rete? Grazie ai dispositivi di storage USB Kingston dotati di crittografia hardware la soluzione è già nel palmo della propria mano.

Per approfondire la conoscenza delle soluzioni Kingston, consultare la pagina kingston.com/ironkey; per inviare domande più specifiche è possibile contattare uno dei nostri esperti di drive USB crittografati.

#KingstonIsWithYou #KingstonIronkey