Kingston TECHNOLOGY

La sicurezza ideale per gli endpoint analizzata e spiegata in partnership con Matrix42

MATRIX42

#KingstonIsWithYou

La sicurezza ideale per gli endpoint analizzata e spiegata in partnership con Matrix42

Introduzione

Nel mondo moderno, la protezione dei dati rappresenta un dovere basilare di qualsiasi azienda, governo o soggetto privato.

Violazioni dei dati, hacking e "il fattore umano" ci ricordano costantemente delle minacce e dei rischi presenti in tutto il mondo. Il costo da pagare in caso di violazione dei dati, sia in termini economici che d'immagine, può raggiungere cifre astronomiche. I requisiti dettati dalle strategie di sicurezza informativa e di prevenzione dalla perdita dei dati (DLP) negli endpoint fanno tutte affidamento sull'adozione di memorie e storage affidabili ed efficienti.

L'impiego della crittografia, di storage e memorie veloci, unitamente al ricorso a best practice, standard e criteri adeguati rappresenta un importante passo avanti nel data management. I laptop e i drive USB andati persi lasciano soggetti privati e aziende vulnerabili all'esposizione dei loro dati personali e delle loro informazioni private. Kingston offre soluzioni di IT security e prevenzione delle minacce per contribuire a mitigare i rischi, fungendo da elemento complementare ai piani di sicurezza esistenti o come parte di piani in programmazione.

La sicurezza ideale per gli endpoint analizzata e spiegata in partnership con Matrix42

Contenuto

Questo breve eBook è dedicato alle soluzioni per endpoint e al modo in cui i drive USB Kingston dotati di crittografia, i connessi programmi di personalizzazione e il software di protezione dei dati Matrix42 EgoSecure sono riusciti a risolvere le problematiche tipiche di sei diversi settori di impiego, fornendo una soluzione che risponda a tutte le loro esigenze operative.

Esamineremo in dettaglio questi sei diversi settori per vedere in che modo vengono gestite le problematiche connesse alla sicurezza degli endpoint.

Sommario

Sezione 1	Settore – Pubblica amministrazione	4
Sezione 2	Settore – Sanità	5
Sezione 3	Settore – Finanza	6
Sezione 4	Settore – Automotive	7
Sezione 5	Settore – Telecomunicazioni	8
Sezione 6	Settore – Manifatturiero	9
Sezione 7	Soluzioni di Kingston e Matrix42	10
	Riepilogo	11
	Informazioni su Kingston	12

Sezione 1: Settore Pubblica amministrazione

Scenario:

Nel settore della pubblica amministrazione l'uso di dispositivi USB è molto frequente. Ad esempio, gli uffici di polizia devono trasferire tramite il canale USB al sistema sanzionatorio tutte le immagini che le telecamere digitali acquisiscono quando vengono commesse trasgressioni quali la sosta vietata o altre simili infrazioni. Le autorità di polizia ricevono dati su cui investigare tramite dispositivi di storage esterni. Alcuni di questi dati devono essere elaborati ed è quindi necessario impedirne l'accesso non autorizzato.

Problematiche:

Vista la notevole diffusione dei dispositivi USB, la richiesta di drive USB da parte dei dipendenti è divenuta incessante. L'uso di dispositivi di storage privati e non autorizzati deve essere impedito per ragioni di sicurezza. Quando un dipendente necessita di un nuovo dispositivo di storage USB, deve essergli immediatamente fornito dall'apposito dipartimento, per evitare di rallentare il suo lavoro. È importante sottolineare che quando si utilizzano dispositivi di storage USB appropriati non sussistono rischi per la sicurezza.

Soluzione:

L'integrazione tra le funzionalità di controllo del dispositivo, crittografia e filtraggio dei dati consente di realizzare il seguente scenario:

I dispositivi sconosciuti vengono bloccati dai computer endpoint. Ai dispositivi di storage dei dati, quali le telecamere digitali, sono permesse solo alcune funzioni, come ad esempio la lettura dei file di immagine. Le operazioni di scrittura avvengono solo con crittografia e solo sui dispositivi USB autorizzati. Tutti gli accessi ai dati vengono registrati. La gestione dei dispositivi autorizzati può essere semplificata usando numeri di serie personalizzabili e identificativi hardware. A tale scopo, Matrix42 Service Management permette all'utente di richiedere i drive USB personalizzati di Kingston Technology all'interno del Self-Service Portal. Ricevuta l'approvazione, il dispositivo USB viene automaticamente autorizzato per essere utilizzato all'interno dell'EgoSecure Data Protection.

> “I nostri dipendenti sono entusiasti di poter ricevere facilmente e rapidamente i nuovi dispositivi USB, dopo la breve procedura di approvazione. Siamo pienamente soddisfatti dei risultati conseguiti nella sicurezza degli endpoint e nella gestione dei servizi grazie alla fusione del programma di personalizzazione di Kingston Technology e alla gestione semplificata di Matrix42.”
>
> **Responsabile dell'Helpdesk, Pubblica amministrazione**

Sezione 2: Settore Sanità

Scenario:

I dispositivi di storage esterni continuano ad essere frequentemente utilizzati per scambiarsi dati, tra dipendenti e/o altre istituzioni.

Ad esempio, gli ospedali in Germania devono fornire al Registro dei tumori le informazioni relative ai casi di tumori attuali e al loro decorso. Per facilitare l'operazione, spesso questi dati vengono trasferiti tramite dispositivi di storage di tipo mobile.

O, ancora, i dottori sono soliti usare i drive USB per portare ai loro convegni documenti di vario tipo, come i dati delle ricerche.

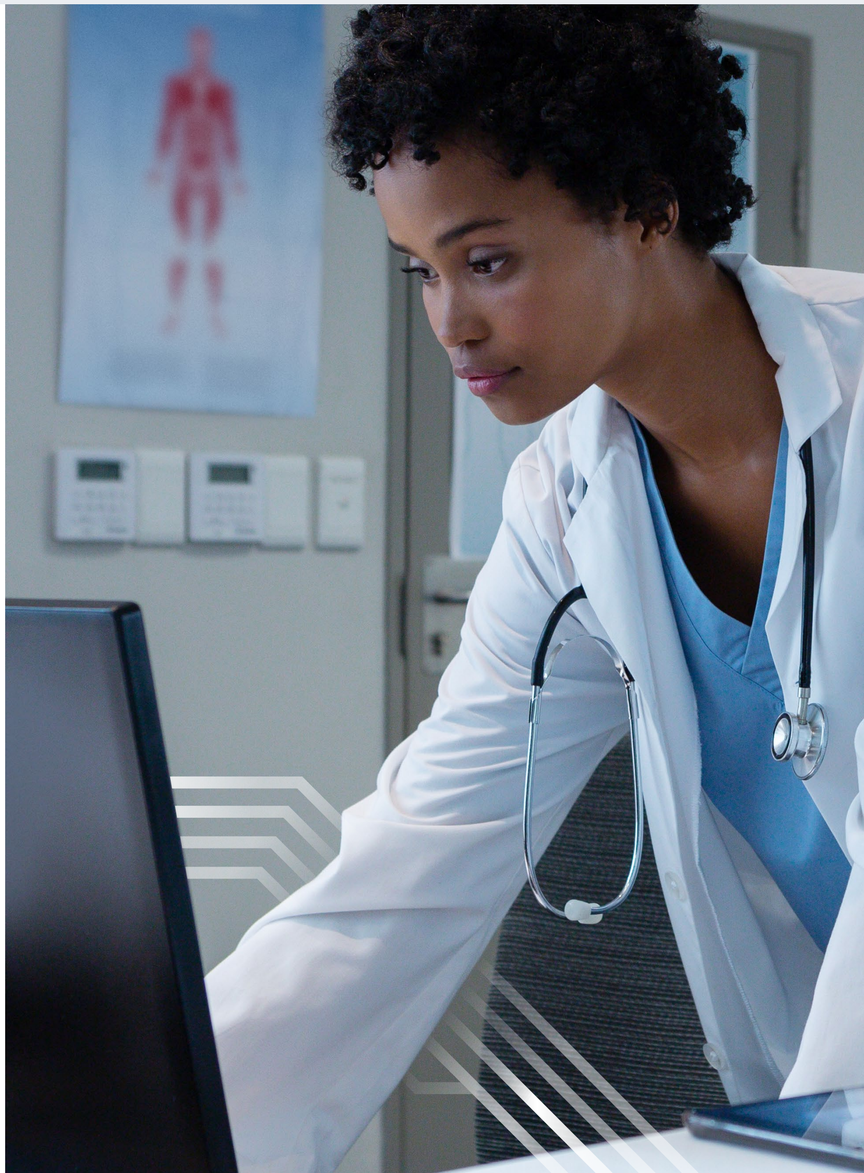
Problematiche:

I dati dei pazienti sono considerati dati molto sensibili e non devono quindi finire nelle mani di persone non autorizzate. Ne consegue che occorre intensificare e rafforzare la protezione dei dati. Nel caso in cui venisse smarrito il dispositivo che trasporta i dati, potrebbero verificarsi problemi molto gravi, sia sul piano della salute dei pazienti che delle sanzioni previste dal GDPR. Ecco perché è importante che l'accesso agli storage di dati USB avvenga in modo controllato, monitorato e crittografato.

Soluzione:

EgoSecure Data Protection riunisce in un'unica soluzione diverse misure di protezione quali il controllo accessi, il filtraggio, la crittografia e l'audit dei dati. Gli amministratori IT sono così in grado di decidere quali dipendenti possono avere accesso e ai singoli dispositivi. È inoltre possibile creare eccezioni basate, ad esempio, sul numero di serie o l'ID hardware - identificativi questi che possono essere definiti grazie al programma di personalizzazione di Kingston Technology - in modo che nella gestione di EgoSecure Data Protection basterà inserire un solo valore tramite cui consentire l'uso dei soli dispositivi autorizzati dalla società. Ciò riduce enormemente l'impegno lavorativo richiesto agli amministratori, elevando contemporaneamente il livello di sicurezza dei dati (GDPR, CCPA, HIPAA, ecc.), visto che l'accesso è crittografato e controllato.

> “In passato abbiamo già usato i drive USB crittografati di Kingston. Oggi, grazie a EgoSecure Data Protection, riusciamo anche a garantire che la tracciabilità dei trasferimenti dei dati dei pazienti avvenga in modo conforme al GDPR dell'Unione Europea.”
>
> **CISO, Ospedale universitario**



Sezione 3: Settore Finanza

Scenario:

Le banche devono rispettare numerosi regolamenti di conformità. Uno di questi, è il noto PCI-DSS (Payment Card Industry Data Security Standard), che richiede la crittografia dei dati, l'analisi della vulnerabilità e il filtraggio dei dati. L'obiettivo consiste nel ridurre al minimo o annullare del tutto le minacce e i rischi per la sicurezza IT.

Problematiche:

La sicurezza IT negli endpoint è minacciata da diversi rischi. Ogni giorno i dipendenti si trovano a dover elaborare le informazioni delle carte di credito di privati e aziende, oltre a dover processare dati sensibili di istituzioni finanziarie, trovandosi così esposti alla minaccia che i dati provenienti dal cloud, dalle email o dai dispositivi USB possano essere compromessi dai malware o che possano accidentalmente finire nelle mani di terze parti, se non vengono adeguatamente protetti. Un tale evento creerebbe un incidente di notevole rilevanza finanziaria per una banca, sanzionato da GDPR, PCI-DSS oltre che dal Sarbanes-Oxley Act. Inoltre i cyber criminali provano continuamente a entrare nei sistemi bancari per manipolarli, diventando ogni giorno più creativi. Di recente, ad esempio, c'è stato il caso di un distributore bancomat la cui alimentazione è stata disattivata per poi riavviare il sistema tramite un dispositivo USB programmato per rubare il denaro.

Soluzione:

I sistemi IT devono essere messi in sicurezza attuando misure protettive a più livelli. Un risultato che richiede il ricorso a controlli delle applicazioni, controlli dei dispositivi, rilevazione delle anomalie, UEBA (User and Entity Behaviour Analytics), monitoraggio e crittografia full-disk con autenticazione di tipo PreBoot. Matrix42 è in grado di implementare queste soluzioni in un ecosistema integrale e automatizzato, che consente l'uso delle sole applicazioni autorizzate e dei dispositivi USB dotati di crittografia. Inoltre, la attività sospette o malevoli vengono automaticamente rilevate, con il conseguente avvio di apposite contromisure. Integrando queste soluzioni software con i drive USB personalizzati di Kingston Technology è possibile creare con estrema semplicità una white list dei dispositivi autorizzati, garantendo la crittografia dei dati in modo tracciabile. Tutto ciò eleva enormemente il livello di conformità e senza ulteriori sforzi.

> “Grazie a EgoSecure Data Protection e alla funzionalità di whitelisting, possiamo consentire l'accesso ai soli drive USB dotati di crittografia di Kingston. Basta includere nella whitelist l'ID hardware dei drive USB dotati di crittografia di Kingston e tutti gli altri vengono bloccati. Così riusciamo a ridurre significativamente il carico di lavoro degli amministratori, arrivando a incrementare la sicurezza!”
>
> **IT Manager, società finanziaria**

Sezione 4: Settore Automotive

Scenario:

Nel settore automotive, l'uso dei dispositivi USB è frequente in diverse aree. Ad esempio, i dati della ricerca vengono memorizzati nei dispositivi di storage esterni per poi essere scambiati tra gli ingegneri della società. I file vengono trasportati dall'ambiente IT all'ambiente OT per configurare le macchine di produzione. Si tratta di dati ad elevato tasso di sensibilità, che vanno protetti dal rischio di spionaggio industriale e furto dei dati, altrimenti il know-how incrementale potrebbe finire nelle mani sbagliate.

Problematiche:

Il settore automotive è tenuto al rispetto di normative sulla conformità quali TISAX, protezione dei prototipi, ENX, ISO27001, "connessione con terze parti" e GDPR. Ad esempio, gli articoli Control 9.1, 9.5 e 10.1 della normativa TISAX prevedono che gli accessi ai dati devono essere controllati, filtrati e crittografati. Gli stessi obblighi sono previsti anche in altre normative, quali il GDPR e nei vari standard ISO27001 dei settori in cui operano le società dell'automotive.

Soluzione:

I drive USB dotati di crittografia di Kingston Technology proteggono i dati con la crittografia di tipo hardware. È possibile assegnare a questi dispositivi un numero di serie e un ID hardware personalizzati, che EgoSecure Data Protection utilizzerà poi per creare una white list di dispositivi autorizzati ad usare specifiche tipologie di dati, in modo del tutto automatico. In più, gli spostamenti dei dati possono essere monitorati e analizzati, nel caso dovessero essere rilevate attività sospette.

> “Grazie a Matrix42 e Kingston Technology, siamo riusciti a implementare i requisiti TISAX come il Control 9.5 (accesso alle informazioni e alle applicazioni) e il Control 10.1 (crittografia) senza dover ricorrere a significative variazioni nel comportamento dei nostri utenti.”
>
> **CTO, Fornitore di automotive**

Sezione 5: Settore Telecomunicazioni

Scenario:

I fornitori di telecomunicazioni raccolgono moltissime informazioni dei loro clienti, che spesso si rivelano molto sensibili per il GDPR. Per questo motivo è necessario predisporre misure adeguate che prevengano sottrazioni e perdite di dati.

Problematiche:

I dipendenti delle società di telecomunicazione lavorano ogni giorno con i dati dei clienti. La maggior parte dei dati viene archiviata all'interno delle applicazioni aziendali. Ciononostante esiste sempre il rischio che i contratti dei clienti o addirittura le esportazioni dei database vengano trasferiti negli endpoint e nei dispositivi esterni connessi ad essi. Per scambiarsi i dati, gli utenti spesso usano storage esterni. È quindi molto importante che le pratiche errate di archiviazione dei dati vengano tempestivamente rilevate e corrette.

Soluzione:

Per agevolare il processo di approvvigionamento, i drive USB con crittografia di Kingston Technology contrassegnati da un ID di prodotto personalizzato possono essere rapidamente acquistati attraverso una whitelist predefinita in EgoSecure Data Protection e ricevuti attraverso Matrix42 Service Catalog. Tramite processi di rilevazione approfondita dei contenuti, basati sulla scansione sia dei dati in uso che di quelli archiviati, è possibile individuare e bonificare automaticamente l'archiviazione e l'esportazione dei dati che dovessero contenere dati sensibili. Gli spostamenti dei dati vengono registrati centralmente. Pertanto, il dipendente può ricevere il nuovo hardware per lo storage dei dati subito dopo che è stato ordinato e autorizzato. Tutto ciò garantisce la piena conformità al GDPR.

> “Grazie al portale self-service di Matrix42, i nostri utenti possono richiedere i supporti di storage di cui necessitano. Una volta autorizzato e consegnato l'ordine, il dispositivo è autorizzato dal relativo controllo di EgoSecure. L'integrazione delle soluzioni offerte da Matrix42 e Kingston Technology incrementa la produttività e la sicurezza della nostra società.”
>
> **CTO, Fornitore di telecomunicazioni**

Sezione 6: Settore Manifatturiero

Scenario:

Il futuro è nei dati digitali. Per un'attività manifatturiera questi dati coincidono essenzialmente con i piani di produzione, i dati relativi ai clienti e ai fornitori e il know-how aziendale. La perdita di questi dati avrebbe come conseguenza le gravi sanzioni previste dal GDPR, oltre agli inevitabili danni di immagine e reputazionali. Ed è purtroppo vero che ogni giorno vengono ritrovati drive USB smarriti all'interno di taxi, lavanderie, aeroporti, stazioni ferroviarie o parcheggi.

Problematiche:

I dispositivi di storage spesso contengono dati altamente sensibili e, sfortunatamente, non sono quasi mai crittografati. Senza contare i rischi connessi al fatto che i tecnici dell'assistenza spesso utilizzano drive esterni per installare aggiornamenti nelle macchine di produzione. Dispositivi questi, che insieme agli aggiornamenti, potrebbero trasportare anche malware che si insidierebbero così nella rete.

Soluzione:

I drive USB dotati di crittografia di Kingston Technology proteggono i dati con la crittografia di tipo hardware. È possibile ricevere questi dispositivi con un numero di serie e un ID hardware personalizzati, che EgoSecure Data Protection utilizzerà poi per creare una white list di dispositivi autorizzati ad usare specifiche tipologie di dati, in modo del tutto automatico. In più, gli spostamenti dei dati possono essere monitorati e analizzati, nel caso dovessero essere rilevate attività sospette.

> "Crittografare i nostri dati di produzione è molto importante, perché ci mette al riparo dal furto dei dati. Questi dati così importanti possono risiedere solo su drive USB con crittografia di Kingston, precedentemente autorizzati e successivamente filtrati attraverso il software EgoSecure Data Protection. Nel resto dei dispositivi USB i dati di produzione verrebbero bloccati; inoltre, il diritto di scrittura di tali dati negli storage esterni risulta protetto dalle funzionalità di crittografia e logging in tempo reale di EgoSecure."

Responsabile della sicurezza IT, Azienda manifatturiera

Sezione 7: Soluzioni di Kingston Technology e Matrix42

L'impiego della crittografia, di storage e memorie veloci, unitamente al ricorso a best practice, standard e criteri adeguati rappresenta un importante passo avanti nel data management. I laptop e i drive USB andati persi lasciano soggetti privati e aziende vulnerabili all'esposizione dei loro dati personali e delle loro informazioni private. Kingston offre soluzioni di IT security e prevenzione delle minacce per contribuire a mitigare i rischi, fungendo da elemento complementare ai piani di sicurezza esistenti o come parte di piani in programmazione.

Drive USB con crittografia di Kingston Technology

I drive USB con crittografia hardware di Kingston Technology integrano soluzioni di protezione per dati mobili, dentro e fuori dei firewall aziendali. Progettati per proteggere i dati che richiedono sicurezza assoluta, questi drive contribuiscono a soddisfare i requisiti standard, direttive e regolamenti di settore. I prodotti hanno conseguito la certificazione FIPS, sono conformi allo standard TAA e hanno capacità fino a 128 GB, dimostrandosi quindi una soluzione ideale sia per utenti corporate che per agenzie governative

Programma di personalizzazione sicura

I drive USB protetti mediante crittografia di Kingston Technology offrono svariate opzioni di personalizzazione, per andare incontro alle esigenze della vostra azienda. Aggiungete le funzionalità desiderate, per creare drive dalle caratteristiche uniche e indispensabili. Kingston Technology mette a vostra disposizione una procedura d'ordine semplice e conveniente che consente di ordinare i drive USB con crittografia personalizzati direttamente presso un rivenditore o distributore di fiducia. La gamma di prodotti USB di Kingston Technology dotati di funzionalità di crittografia include i modelli DTVP30, DT4000G2 e IKD300S. Questo programma si basa sui servizi più richiesti dai clienti e include serializzazione numerica, doppia password e uso di loghi personalizzati. Con un ordine minimo iniziale di 50 pezzi e di 25 pezzi per gli ordini successivi, il programma è in grado di offrire alla vostra azienda esattamente ciò di cui ha bisogno.

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection offre alle organizzazioni soluzioni di gestione sicura a 360°, per la prevenzione e la protezione di dispositivi, sistemi e dati. Tali soluzioni prevedono la completa automatizzazione del processo, dalla prevenzione e rilevazione delle minacce all'adozione di adeguate contromisure in caso di danni, senza comportare alcun calo di produttività.

Riepilogo

Garantire la protezione dei dati e la sicurezza informatica può sembrare una responsabilità gravosa. Le caratteristiche del lavoro digitale sono cambiate in modo significativo, visto che i dipendenti si trovano a poter decidere autonomamente quando, dove e con quali dispositivi lavorare. Integrando correttamente i drive USB con crittografia hardware e la gestione dei software negli endpoint è possibile conseguire il pieno controllo dei dispositivi utilizzati all'interno di un'organizzazione. In questo modo, si riesce inoltre a mitigare il rischio di data breach e supportare la strategia adottata per la conformità costante al GDPR.

Informazioni su Kingston

Grazie ai suoi 30 anni di esperienza, Kingston Technology è in grado di individuare e risolvere efficacemente le problematiche poste dalla sicurezza degli endpoint all'interno della vostra organizzazione, senza alcun compromesso per la produttività aziendale.

©2021 Kingston Technology Europe Co LLP e Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Regno Unito.
Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469. Tutti i diritti riservati. Tutti i marchi e i marchi registrati sono proprietà dei rispettivi titolari.

#KingstonIsWithYou