

STORMSHIELD

Soluzione per la protezione dei dati

Verso un’implementazione senza vincoli?

Ottobre 2022

PROTEZIONE DEI DATI

Ogni giorno i Responsabili IT e i loro team devono integrare aggiornamenti, patch di sicurezza, nuove applicazioni o configurare un computer per l'arrivo di un nuovo dipendente. Operazioni che non sono prive di rischi.

Richiedono infatti del tempo e possono generare errori o blocchi che si ripercuotono sull'attività dell'azienda. Per essere più agili, sempre più aziende hanno deciso di abbandonare le postazioni di lavoro "tradizionali" - con i loro numerosi fat client - per passare ai thin client o a postazioni virtuali.

Tuttavia, tale evoluzione non deve compromettere la protezione dei dati, la cui cifratura end-to-end ha il compito di garantirne la riservatezza. Inoltre, è importante non trascurare l'esperienza dell'utente, o meglio del dipendente, in quanto la crittografia deve essere effettuata nel modo più trasparente possibile per l'azienda. Il crescente utilizzo di applicazioni SaaS sta costringendo gli esperti in sicurezza a innovare, offrendo la soluzione di crittografia dei dati come servizio.

È questa una delle promesse garantite dalla soluzione Stormshield Data Security.

Stormshield
Leader europeo della sicurezza informatica, Stormshield è una società interamente controllata da Airbus Defense & Space Cyber Programmes e offre **soluzioni affidabili**, certificate e qualificate ai massimi livelli europei. È il fornitore che copre il più ampio perimetro di protezione tra i detentori dei Visti di Sicurezza ANSSI (Agenzia Nazionale per la Sicurezza dei Sistemi Informativi).

Sommario

04 **Gestire le postazioni di lavoro e i software: un bel grattacapo**

05 **I costi delle implementazioni software**

06 **Il periodo d'oro delle applicazioni pesanti è finito?**

07 **Feedback**

08 **Sicurezza dei dati rinforzata con meno vincoli**

09 **Stormshield Data Security: il servizio di crittografia agentless**

10 **Aspetti chiave**

Gestione delle postazioni di lavoro e dei software: **un bel grattacapo**

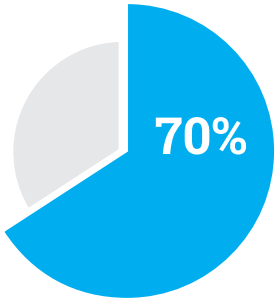
Sono anni che si preannuncia la fine del computer desktop. Tuttavia, è chiaro che le storiche postazioni di lavoro come PC e Mac siano ancora essenziali nelle aziende, anche se dimostrano tutta la macchinosità della gestione IT. Ciò è dovuto al fatto che l'implementazione e l'aggiornamento di sistemi operativi e software diversi sono troppo spesso restrittivi, rischiosi, lunghi e costosi.

Sistemi operativi non più supportati, nuovi prerequisiti, incompatibilità con una versione di un altro software, conflitti con un'applicazione installata da un dipendente... La gestione delle postazioni di lavoro è costellata di ostacoli che riguardano tutti i sistemi operativi, da Windows a MacOS a Linux. Sono molti i fattori che possono influire negativamente sui tempi d'implementazione delle applicazioni e delle patch. In pratica, potrebbero volerci diversi mesi per aggiornare completamente un sistema informatico.

Ma non è solo il sistema operativo a complicare il lavoro dei Responsabili IT (CIO). Una semplice valutazione del proprio parco clienti può rivelare che decine, o più spesso centinaia, di postazioni di lavoro non dispongono di aggiornamenti e patch per i software più comuni (come Java, Adobe Reader e altri). Ma l'implementazione di aggiornamenti e l'installazione di nuove applicazioni sono interventi cruciali sia per potenziare la sicurezza del sistema informatico (SI) sia per soddisfare le esigenze aziendali.

Implementazione dei software e **trasformazione digitale**

Per far fronte alla complessità della gestione delle postazioni di lavoro e dei software, i progetti di digitalizzazione si rivolgono sempre più spesso alle piattaforme Cloud. Secondo uno studio condotto da IDC nel 2021, questo tipo di soluzione è considerata un investimento strategico nei progetti di modernizzazione, con una crescita del 22% rispetto al 5% degli investimenti IT a livello globale.



Entro il 2024[1] il 70% delle applicazioni sarà cloud-native.

Se applicato all'IT, il TCO (*Total Cost of Ownership*) è definito come la somma dei costi di acquisizione, implementazione, gestione, supporto e utilizzo della tecnologia. Il prezzo di acquisto di un computer è solo una parte del costo totale di un dispositivo durante il suo ciclo di vita.

Per il reparto IT, che spesso è ancora considerato un semplice centro di costo, questi TCO di acquisto e monitoraggio rappresentano una metrica finanziaria molto importante. L'ottimizzazione di tali costi sta portando le aziende a migrare rapidamente verso il cloud. Sempre secondo IDC, la quota di applicazioni cloud-native passerà dal 10% al 70% entro il 2024, grazie all'adozione di tecnologie come i microservizi, i container, l'orchestrazione e DevOps.

[1] Fonte: Articolo di IDC per EasyVista – Maggio 2021: https://www.easyvista.com/fr/rapport-idc-service-client-et-support-it

Il periodo d'oro delle **applicazioni pesanti** è finito?

Le postazioni di lavoro "classiche" offrono molteplici opzioni. Ma la loro gestione rimane macchinosa e complicata. E se la soluzione fossero i thin client, più facili da usare, più economici da acquistare e gestibili da remoto?



Il parco macchine aziendale non è più basato esclusivamente sui sistemi operativi Microsoft. Gli utenti si collegano alle reti aziendali e alle loro sorgenti di dati anche da dispositivi con sistema operativo iOS e Android, o addirittura MacOS o Linux in alcune aree, spesso optando per una maggiore velocità e agilità. Questo desiderio di essere più agili si riflette anche nell'utilizzo di thin client a scapito dei fat client.

La consueta e ormai obsoleta pratica di scaricare e installare il software dal sito di un publisher ha subito un primo duro colpo con l'arrivo degli store di applicazioni come quelli di Google, Apple o Microsoft. Successivamente, le prime generazioni di thin client hanno enfatizzato questa tendenza: come un'applicazione web, questi thin client consentono agli utenti di accedere alla maggior parte degli strumenti da un semplice browser, anche da piattaforme non Windows dove spesso i fat client non sono supportati.

La situazione è cambiata con l'avvento delle nuove generazioni di thin client e delle loro applicazioni basate sul Cloud, come Salesforce, Microsoft Office 365 o Google Workspace. Tutte queste applicazioni sono sempre più integrate nelle aziende in modalità SaaS (Software-as-a-Service). Secondo uno studio di Syntec Numérique/IDC[1], alla fine del 2018 il 78% dei publisher offriva questo modello. Per i responsabili IT, la promessa è quindi quella di un'amministrazione semplificata e centralizzata di terminali e software. Una realtà in cui è possibile applicare automaticamente i criteri dei profili a gruppi di thin client configurati in modo simile. L'idea è quella di avere una postazione di lavoro "standard".

Sulla scia di questa idea, in seguito è nato il concetto di Desktop-as-a-Service (DaaS). In questo caso, il fornitore di servizi gestisce direttamente l'infrastruttura tecnologica: provisioning delle risorse, bilanciamento del carico, gestione dei problemi di rete, ecc. Questi vantaggi, tuttavia, non esimono il responsabile IT dal continuare a gestire le postazioni di lavoro virtuali e prestare attenzione al protocollo di dislocazione dei desktop, nonché controllare le licenze.

[1] Fonte: Comunicato stampa di Syntec Numérique - 6 dicembre 2018: https://syntec-numerique.fr/sites/default/files/Documents/2018_12_06_Communique_de_presse.pdf

Feedback

La postazione di lavoro è ancora al centro del sistema informatico di qualsiasi azienda. Ma ognuna di esse ha i propri obiettivi e le proprie sfide, basate sull'esperienza dell'utente.

Standardizzare le postazioni di lavoro nel settore dell'aviazione

L'obiettivo di questa prima organizzazione aziendale è semplice: mitigare l'impatto della gestione dei software (distribuzione delle patch di sicurezza, migrazione verso una nuova versione, ecc.) sulle attività dei dipendenti. In prospettiva, intende rendere tutte le operazioni effettuate sui desktop comode, veloci e trasparenti.

Per affrontare questa duplice sfida (riduzione dei costi di manutenzione e minor numero di implementazioni), l'azienda mira a "standardizzare" le postazioni di lavoro in modo da non dover più gestire applicazioni on-demand o livelli aggiuntivi. Indipendentemente dal profilo aziendale, ogni utente potrà disporre di una macchina con una configurazione comune.

Semplificare le implementazioni nel settore della consulenza e dei servizi

Questa seconda organizzazzione, ha invece un turnover del personale molto elevato, e che quindi deve fare i conti con partenze pressoché quotidiane. Per garantire tempi di inattività minimi, i responsabili IT sono chiamati a reinstallare una postazione di lavoro in tempi molto brevi. Ciò implica un livello minimo di complessità e personalizzazione da gestire.

Per non penalizzare i nuovi operatori, le applicazioni e i dati dovrebbero essere accessibili da un browser on-demand, come accade con l'ambiente Google Workspace.

Affidarsi agli store di applicazioni nel settore industriale

Per una terza organizzazione di livello internazionale, invece applicazioni come Outlook non sono più adattate e/o adeguate alla sua modalità organizzativa. Al suo posto si predilige Outlook Web Access, per postazioni di lavoro meno complesse e per ridurre le interazioni con le altre applicazioni presenti. L'obiettivo è quello di consentire ai dipendenti di accedere ai propri dati da qualsiasi luogo e su qualsiasi dispositivo.

L'obiettivo è di limitare l'implementazione di client fat su ciascun terminale a favore di soluzioni accessibili da un browser. Per mitigare l'impatto derivante dall'implementazione di soluzioni "tradizionali", questa azienda ha deciso di affidarsi a strumenti standard. I team possono accedere allo SharePoint Store e ed alle applicazioni disponibile.

Sicurezza dei dati rinforzata, **con meno vincoli**

La tendenza all'utilizzo di applicazioni SaaS sul posto di lavoro ha soddisfatto, almeno inizialmente, le aspettative degli utenti e dei team IT. La sfida per gli esperti in protezione e sicurezza dei dati è quella di offrire soluzioni meno invasive ma altrettanto efficaci.



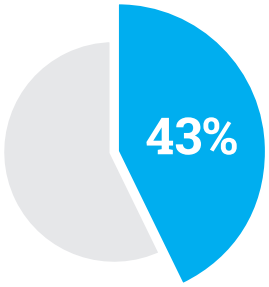
Indipendentemente dal reparto di appartenenza, oggi i dipendenti adottano un approccio incentrato sui dati, il che significa che i dati sono al centro del loro lavoro. Con l'avvento dell'iperconnessione, il perimetro aziendale è cambiato profondamente: gli scambi di dati avvengono in modo permanente tra i reparti interni e i partner esterni. Parallelamente, la mobilità dei team implica la possibilità di accedere ai dati indipendentemente dalla posizione e da diversi terminali fissi e mobili. Tutto ciò conferma la necessità di estendere la sicurezza agli strumenti che consentono l'accesso, in questo caso i browser, e di generalizzare la crittografia.

Tuttavia, i dipendenti sono sempre meno disposti ad accettare vincoli che considerano inutili o sproporzionati. Tra questi vincoli, troviamo anche quelli legati alla sicurezza informatica. Questa necessaria generalizzazione della crittografia dei dati si scontra ancora con l'idea preconcetta che la crittografia sia complicata. Poiché qualsiasi nuova soluzione o procedura ha valore solo se viene compresa, adottata e padroneggiata, è indispensabile sensibilizzare gli utenti sulla particolare natura dei dati e sulla semplicità della crittografia. I responsabili IT si ritrovano a svolgere un ruolo fondamentale in questo senso, poiché costituiscono una parte importante della strategia di protezione dei dati.

Una vera e propria rivoluzione che riguarda anche gli esperti di sicurezza del settore. È il momento di lasciarsi alle spalle i macchinosi agents legati agli esordi della sicurezza informatica, e di offrire soluzioni intuitive e facili da usare. L'obiettivo è di soddisfare gli utenti finali che ancora percepiscono la crittografia come un vincolo. **E se la chiave della trasformazione digitale fosse la fiducia dei dipendenti all'interno - e dei clienti all'esterno - nella capacità dell'azienda di proteggere i dati che le vengono affidati?**

Stormshield Data Security : **la soluzione di crittografia SaaS**

La protezione dei dati deve rimanere una priorità. Ma per soddisfare le aspettative dei team IT, è fondamentale affidarsi a soluzioni che seguano la tendenza dei thin client. E per i collaboratori, occorre integrare le aspettative di ergonomia e facilità d'uso. Queste sono le promesse e le caratteristiche della nuova soluzione Stormshield Data Security, il vostro prodotto di crittografia dei dati SaaS.



Il 43% delle aziende riconosce l'importanza di disporre di una strategia di crittografia completa[1].

La sicurezza informatica è più che mai vitale in un contesto di forte concorrenza e della crescente fuga ed esfiltrazione dei dati. Per questo motivo è necessario un uso diffuso della crittografia per rafforzare la riservatezza dei documenti e dei files critici condivisi online o scambiati via e-mail.

L'uso diffuso della crittografia dei documenti e delle e-mail è tanto più essenziale quanto più le aziende migrano parte dei propri sistemi informatici o delle applicazioni nel cloud. Il nuovo servizio di Stormshield Data Security rispecchia questa evoluzione integrandosi completamente con l'ambiente di Google Workspace per garantire la riservatezza dei dati scambiati. Tutto ciò senza la necessità di installare e mantenere aggiornato un agent, sulle postazioni di lavoro dei dipendenti. L'operazione di crittografia viene eseguita end-to-end sotto il controllo esclusivo dell'azienda, prima che i dati vengano archiviati sui server della piattaforma Cloud. L'amministratore e l'ownser del servizio cloud non avranno quindi accesso a tali dati.

L'offerta SaaS di Stormshield Data Security per Google Workspace è un servizio di protezione dei dati "chiavi in mano" e proprietario. I processi di crittografia e decrittografia, come pure la gestione delle chiavi utente, sono completamente gestiti da Stormshield.

[1] Fonte: Studio "Global Encryption Trends", Ponemon – aprile 2018

Aspetti da considerare

Con la proliferazione dei dispositivi mobili e delle nuove applicazioni web, i CIO hanno riconosciuto il valore di **interfacce utente semplici e intuitive.**

Ai dipendenti infatti non interessa tanto la tecnologia quanto l'agilità offerta. Per raggiungere questo obiettivo, sempre più aziende si affideranno ad applicazioni web intuitive e a strumenti di collaborazione **con la promessa di un più rapido scambio ed accesso ai dati.**

Spesso considerato un vincolo, il problema della protezione dei dati non deve essere sottovalutato, né dagli utenti né dai loro team IT. La questione della sicurezza informatica deve rimanere una delle priorità dei responsabili IT, al fine di **proteggere i dati senza comprometterne l'accessibilità.** Come prima risposta a tale obiettivo, avremo l'integrazione della crittografia end-to-end nel browser ed una naturale intuitività dell'applicazione.

Il successo di questa importante svolta nell'approccio alla sicurezza informatica, dipenderà dall'adesione dei dipendenti. A tal proposito, negli anni a venire **un atteggiamento diverso nei confronti della crittografia** rappresenterà una importante sfida per i CIO.

Il cloud computing è già il nuovo standard. Ed è la cultura aziendale a frenare tale transizione, non la tecnologia...



STORMSHIELD

Le aziende, le istituzioni governative e le organizzazioni di difesa di tutto il mondo devono garantire la sicurezza informatica delle proprie infrastrutture critiche, dei dati sensibili e degli ambienti operativi. È qui che entrano in gioco le tecnologie Stormshield, certificate e qualificate ai massimi livelli europei, per affrontare le sfide dell'IT e dell'OT, e per proteggere le loro attività. La nostra mission: **rendere sicuri dal punto di vista informatico i nostri clienti,** in modo che possano concentrarsi sui propri obiettivi principali, determinanti per il buon andamento delle istituzioni, dell'economia e dei servizi offerti alla popolazione. **Scegliere Stormshield significa avvalersi di una sicurezza informatica di fiducia a livello europeo.**

Per maggiori informazioni: www.stormshield.com

www.stormshield.com



Copyright Stormshield - 2018-2022