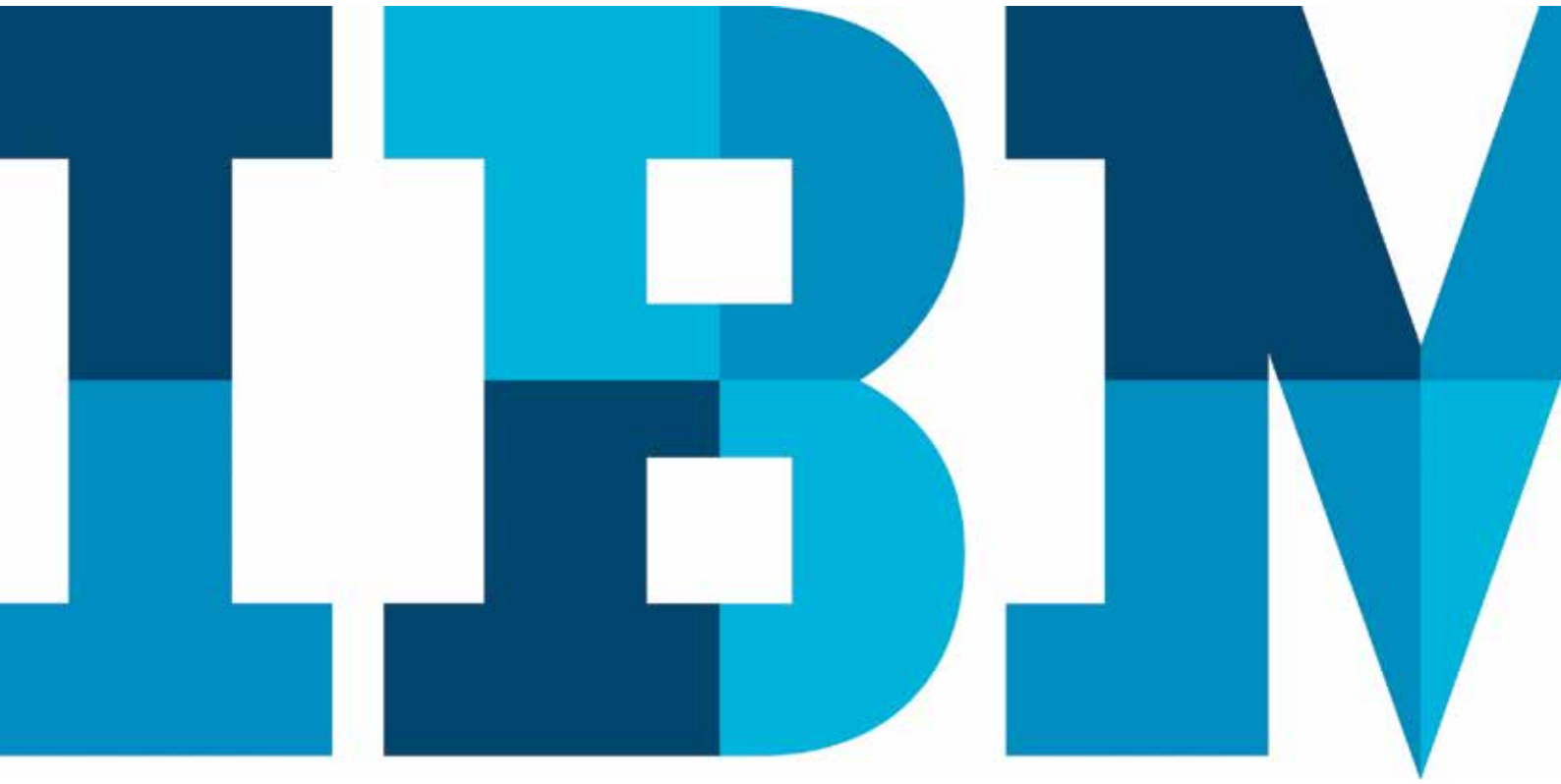
IBM Software
Thought Leadership White Paper

Un nuovo approccio per la gestione delle patch

IBM BigFix pone nuovi standard di riferimento per la gestione delle patch



IBM

Indice

Introduzione

Gli attacchi malware mirano a sfruttare le vulnerabilità dei sistemi IT prima che i produttori di software siano in grado di rilasciare patch in grado di risolverle. Un attacco può comportare per le imprese un calo di produttività e il rischio di perdere dati sensibili, con possibili cause giudiziarie e sanzioni. Le dimensioni del problema sono allarmanti - i costi per criminalità e spionaggio cibernetici nell'economia globale raggiungono le centinaia di miliardi di dollari, come segnalato dalla società di sicurezza informatica McAfee e dal Center for Strategic and International Studies. Solo negli Stati Uniti gli attacchi degli hacker comportano ogni anno costi superiori a 100 miliardi di dollari statunitensi.

Un numero in continua crescita di fornitori software risponde a queste minacce pubblicando numerose patch per tentare di stare al passo con l'impressionante numero di malware exploit. Purtroppo molte imprese non sono preparate per gestire questa mole di patch in modo efficiente. La struttura dei processi aziendali implica che i reparti IT necessitino di settimane o mesi per applicare le patch negli ambienti di destinazione. Di fatto, per ottenere una conformità globale delle patch si deve attendere mesi. Nel frattempo, vengono rilasciate ulteriori numerose patch e quindi le imprese sono costantemente esposte a notevoli rischi e non rispettano la conformità - e la situazione peggiora nel tempo.

La gestione delle patch è sempre stata complessa. Nonostante i rischi, alcune imprese si dimostrano riluttanti ad implementare le patch, visti i tempi e l'impegno lavorativo richiesti. In un'impresa con ambiente hardware e software eterogeneo, la gestione delle numerosissime patch offerte può superare decisamente le risorse del team IT e il budget. È quindi indispensabile trovare una soluzione per la gestione delle patch rapidamente applicabile, economica e strettamente legata alle policy, che:

- risulti facilmente scalabile per gestire tutti gli endpoint dell'azienda, indipendentemente dalle dimensioni - anche le più grandi - utilizzando un'infrastruttura ridotta al minimo
- sia in grado di supportare i sistemi operativi, le applicazioni e le piattaforme di vari fornitori (compresi Microsoft Windows, Linux e UNIX)
- operi con collegamenti e dispositivi di supporto a bassa velocità al di fuori della rete aziendale
- minimizzi l'impegno del team IT
- funzioni in tempo reale, applicando le patch in tutta l'impresa
- gestisca le macchine virtuali anche offline.

IBM BigFix®, combina i singoli aspetti della gestione patch in una soluzione intelligente e semplice, che snellisce e ottimizza il processo di ricerca, valutazione, correzione, conferma, applicazione e reporting sulle patch.

La risposta alla sfida della gestione delle patch

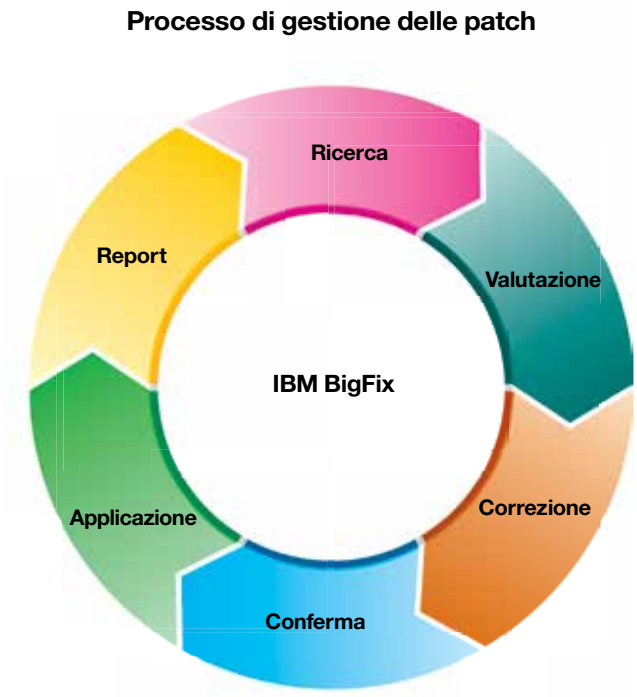
La gestione delle patch sembra essere semplice, ma in realtà rappresenta una delle sfide più complesse e critiche per un'impresa. Una gestione efficiente delle patch richiede molto più del semplice intervento di un amministratore per la sostituzione delle patch o l'applicazione delle misure patch fornite dai distributori. Le seguenti domande rappresentano esempi di complessità da gestire:

- Come trattare patch "out-of-band"- vale a dire al di fuori del consueto - inviate con urgenza e che non rientrano negli schemi di routine?
- In un ambiente con centinaia o centinaia di migliaia di endpoint che sfruttano vari sistemi operativi (OS) e applicazioni, gli amministratori come possono essere sempre aggiornati sulle patch?
- Come si suppone che gli amministratori possano monitorare pc e altri dispositivi mobili in roaming?
- Quanto tempo richiede il processo complessivo di patch? Come possono gli amministratori confermare (e comprovare) che ogni endpoint della loro infrastruttura sia stato correttamente raggiunto - mantenendo i requisiti richiesti?
- Come possono gli amministratori controllare rapidamente le patch prima di applicarle - ripristinando lo stato precedente se causano problemi?
- Come è possibile implementare le patch senza interferire con la produttività degli utenti finali?
- Come si possono integrare le patch nelle applicazioni di business durante i fermi previsti per la manutenzione, con interruzioni operative minime?

È evidente che la gestione delle patch rappresenta uno dei requisiti principali per la sicurezza delle imprese, ma le domande sopra riportate sottolineano quali barriere debbano affrontare le aziende per implementare processi di gestione delle patch veramente efficaci. Gli ostacoli sono numerosi: lacune a livello di visibilità e personale, possibili impatti sul business, limiti di banda richiesti dalla rete, gestione insoddisfacente, problemi di scalabilità e di copertura con piattaforme diverse, applicazioni di terzi ed endpoint in roaming.

Fortunatamente questi ostacoli sono superabili. BigFix li supera grazie ad una soluzione globale appositamente progettata per ambienti distribuiti ed eterogenei. Con questa soluzione le imprese possono finalmente visualizzare, modificare, utilizzare ed eseguire i report sullo stato di conformità delle patch in tempo reale, su scala complessiva e con una sola console.

Processo di gestione delle patch



BigFix rende la gestione delle patch un processo univoco e a circuito chiuso, che ottimizza la sicurezza e permette di risparmiare.

I nuovi standard di riferimento per la gestione delle patch

Non esiste una best practice ufficiale per la gestione delle patch, quindi l'approccio generalmente adottato si basa su un processo definito da sei fasi fondamentali: ricerca, valutazione, correzione, conferma, approvazione e report. In passato, spesso questi interventi sfruttavano tecnologie separate e non integrate, rendendo virtualmente impossibile creare un processo di gestione delle patch in tempo reale. BigFix mette a disposizione tutte queste fasi operative come parte di un processo univoco e completamente integrato, in grado di ottimizzare la sicurezza e far risparmiare tempo e risorse.

Di seguito riportiamo un esempio "prima/dopo" di come questa soluzione sia in grado di modificare le regole per la gestione delle patch.

Fase 1: Ricerca

Prima: la prima fase del processo di gestione delle patch consiste nell'individuare le patch disponibili. Ciò significa spesso ricercare la disponibilità delle patch rivolgendosi ai fornitori via e-mail, mediante segnalazioni pop-up delle applicazioni, siti, blog e altre fonti. La procedura va ripetuta ogni settimana - o giornalmente - per centinaia di patch, su sistemi operativi, applicazioni e prodotti anti malware di vari fornitori. Affidandosi agli aggiornamenti automatici del fornitore standard non si possono escludere possibili errori, con conseguenze decisamente negative. Accettare automaticamente le patch senza controllarle può comportare seri rischi per un'impresa, in quanto nessuna azienda può garantire controlli o report continui - e affidarsi al fatto che gli utenti effettuino gli aggiornamenti è rischioso e non attendibile.

Un approccio migliore consiste nel rivolgersi a un fornitore che gestisce le patch offrendo un flusso di patch più comuni, in modo che l'impresa debba solo valutare i singoli download delle patch al loro arrivo, eseguire i test della compatibilità con l'ambiente aziendale e quindi applicarle con policy altamente selettive a seconda dei profili di macchina specifici. Ciò permette di applicare patch specifiche solo agli endpoint che effettivamente le necessitano. Tuttavia il problema di questo approccio consiste nel fatto che la procedura non è automatizzata, e richiede notevoli risorse e tempo, spesso non a disposizione dell'impresa.

Dopo: IBM individua le release delle patch dal fornitore di sistema operativo, prodotti anti malware e applicazioni comuni e li rende disponibili per gli utenti, eliminando così le lungaggini correlate ai processi di ricerca delle patch. Patch e aggiornamenti sono analizzati con strumenti logici per garantire valutazioni accurate di vulnerabilità e correzioni, quindi sottoposti a numerosi test. Il risultato: i cosiddetti messaggi IBM Fixlet®. Tali messaggi Fixlet sono poi inviati automaticamente ai server dei clienti BigFix. Gli utenti devono semplicemente aprire la console BigFix per visionare gli ultimi aggiornamenti e selezionare le patch da applicare e possono quindi creare messaggi Fixlet personalizzati con un'interfaccia guidata di facile utilizzo. La procedura si applica virtualmente ad ogni aggiornamento, anche alle patch applicative interne.

Fase 2: Valutazione

Prima: per ogni patch identificata, l'impresa deve determinare l'applicabilità e la criticità dell'aggiornamento, stabilendo quali endpoint dell'impresa necessitano di implementare la patch. In caso di aggiornamenti di sicurezza i dati critici si trasformano in un vero e proprio rischio, e il rischio commerciale aumenta al crescere del numero degli endpoint senza patch. Molte imprese non possono accedere alla valutazione globale e attuale e ai dati di configurazione necessari per quantificare obiettivo e impatto delle patch nell'impresa stessa. Alcuni strumenti permettono di ottenere questi dati, ma richiedono giorni o settimane per raccogliere e raggruppare le informazioni, controllando ogni endpoint in rete - senza tener conto del fatto che molti endpoint sono connessi solo di rado alla rete. L'informazione però deve essere immediatamente accessibile per gli amministratori del sistema al momento del lancio della patch, in quanto per molte patch il tempo è un fattore cruciale, e il processo di valutazione del rischio e priorità delle patch deve avvenire il più rapidamente possibile.

Dopo: con BigFix in tutti gli endpoint è installato un agent software singolo e intelligente, che controlla continuamente lo stato dell'endpoint fornendo al server di gestione il report relativo, compresi fattori come livelli delle patch. L'agent compara la conformità dell'endpoint rispetto a policy predefinite, come livelli obbligatori di patch e configurazioni standard. Questa informazione risulta particolarmente critica durante gli scenari di emergenza quando un fornitore software rilascia una patch critica e out-of-band. In tal caso l'impresa deve infatti quantificare rapidamente l'estensione complessiva e il rischio degli exploit correlati. Un esempio: un cliente ha installato gli agent di BigFix su 5.100 endpoint e ha scoperto che oltre 1.500 endpoint (il 30%) non avevano installato una patch critica (come minimo). Complessivamente gli endpoint avevano perso 20.033 patch "critiche" - vale a dire una media di 13 patch per endpoint.

Dopo aver identificato il numero complessivo di patch correlate agli endpoint e aver definito la criticità di business, l'organizzazione IT può procedere con la fase di correzione.

Fase 3: Correzione

Prima: prima di poter valutare una patch e di decidere se distribuirla all'interno dell'impresa, va sottoposta a test per assicurare che non entri in conflitto con patch o software installati sugli endpoint di destinazione. Pertanto si devono dapprima determinare requisiti preliminari e dipendenze, come i livelli di service pack. A tal scopo di solito si applica e si esegue un test dell'aggiornamento su un determinato numero di endpoint selezionati prima del release complessivo - un processo che può durare giorni o settimane se si usano soluzioni manuali. Se il test evidenzia che la patch è sicura per l'applicazione in tutta l'impresa, viene utilizzata sugli endpoint interessati, di solito a lotti, ampliando così l'estensione della patch. Le tempistiche prolungate di correzione sono legate principalmente all'impossibilità di fare affidamento sulla qualità delle patch e in secondo luogo ai meccanismi di distribuzione poco affidabili. Questo è il motivo per il quale il successo al primo passaggio delle patch raggiunge percentuali solo minime. La maggioranza delle imprese inoltre è costretta a procedere con lentezza se una patch causa un problema imprevisto, per garantire che i collegamenti alla rete non siano sovraccaricati dal processo di distribuzione della patch. A livello aziendale è quindi spesso difficile applicare rapidamente ed efficacemente le correzioni.

Numerosi tools richiedono infatti profonde conoscenze operative e personale appositamente istruito per utilizzarli, oppure non funzionano su endpoint collegati ad una rete aziendale ad alta velocità - quindi i portatili in roaming o altri endpoint mobili rimangono esclusi dai cicli di aggiornamento per lunghi periodi. Molti tools non possono offrire i controlli minuziosi e basati sulla policy necessari agli operatori per applicare con efficienza le patch su tutti gli endpoint interessati dell'impresa. I processi automatici di aggiornamento devono disporre di elementi di controllo come intervalli per l'installazione delle patch - se un utente deve essere presente o meno - opzioni di reboot, metodo di distribuzione (compresa la larghezza di banda e throttling per la CPU), tipo di sistema e opzioni di segnalazione all'utente.

Dopo: i server del cliente BigFix scaricano automaticamente gli ultimi aggiornamenti delle patch, e gli endpoint possono immediatamente valutare se è necessaria una determinata patch, senza che l'operatore debba intervenire. I messaggi Fixlet comprendono le istruzioni di distribuzione, con OS, versione e requisiti preliminari richiesti, eliminando la necessità di eseguire i test sulla patch da parte del reparto IT. Gli operatori possono stabilire in pochi minuti quando debba essere abilitata la patch, quali segnalazioni debbano ricevere gli utenti finali (se necessarie), se permettere o no agli utenti di rimandare l'implementazione della patch e per quale periodo e se forzare o rimandare i reboot. L'agent sull'endpoint riceve la nuova policy ed esamina immediatamente l'endpoint per stabilire se sia possibile applicare la patch - in tal caso scarica e applica la patch, rilasciando in pochi minuti con un report sul successo o il fallimento dell'intervento. Tale approccio, in sinergia con l'infrastruttura relay BigFix e con la capacità di individuare gli apparecchi collegati a Internet, riduce notevolmente il carico sulla rete e può migliorare le percentuali di successo al primo passaggio oltre il 95 percento.

La soluzione mette quindi a disposizione un meccanismo molto sicuro, che sfrutta elementi crittografici per garantire che solo gli amministratori autorizzati possano creare e distribuire le policy. Le informazioni di audit vengono memorizzate per registrare chi ha definito le singole policy da applicare a determinati endpoint, e non sono richieste conoscenze specifiche da parte degli operatori che avviano il processo di correzione. Qualsiasi operatore che abbia seguito un corso di formazione base per BigFix sa elaborare rapidamente e in tutta sicurezza le patch Windows, Linux, UNIX e Mac OS, oltre ad applicazioni Windows e Mac, senza conoscenze o pratiche specifiche sui domini.

Fase 4: Conferma

Prima: dopo aver individuato ed elaborato le patch da applicare, si deve confermare se l'installazione è avvenuta correttamente. Ciò permette al personale IT di sapere quando è terminato il ciclo della patch e facilita il rispetto dei requisiti di report per la conformità. I dati vanno rinviati al sistema centrale di reporting, che informa in tempo reale il personale dell'andamento del processo, eccezioni comprese. Tuttavia molte tecnologie per la gestione delle patch non eseguono correttamente questo processo, impiegando settimane per ricontrollare tutti gli endpoint e ancor più per correggere le difformità. Questo scarto temporale comporta l'esposizione dell'azienda a rischi di sicurezza e mancata compliance.

Molti prodotti non forniscono la conferma di applicazione delle patch - oppure se eseguono la conferma necessitano di giorni o settimane per la stesura di un report complessivo. Nel peggiore dei casi alcuni tools segnalano l'applicazione delle patch mentre i file sono solo scaricati e non ancora applicati. I ritardi e le lacune sopra indicati lasciano spesso esposti alcuni endpoint, creando così una rischiosa vulnerabilità.

Dopo: dopo aver implementato una patch, l'agent di BigFix ricontrolla automaticamente e di continuo lo stato dell'endpoint per confermare la corretta installazione, aggiornando in tempo reale il server di gestione (o non appena possibile con gli apparecchi in roaming). Questa è una fase particolarmente critica per rispettare i requisiti di conformità, che richiedono un esame comprovato dell'installazione continua delle patch. La soluzione permette agli operatori di esaminare in tempo reale il processo di applicazione delle patch, grazie ad una console centralizzata e ricevendo la conferma dell'installazione entro pochi minuti dall'avvio del processo operativo. Questo processo permette alle imprese di garantirne la conformità in modo più rapido, intelligente ed affidabile.

Fase 5: Applicazione

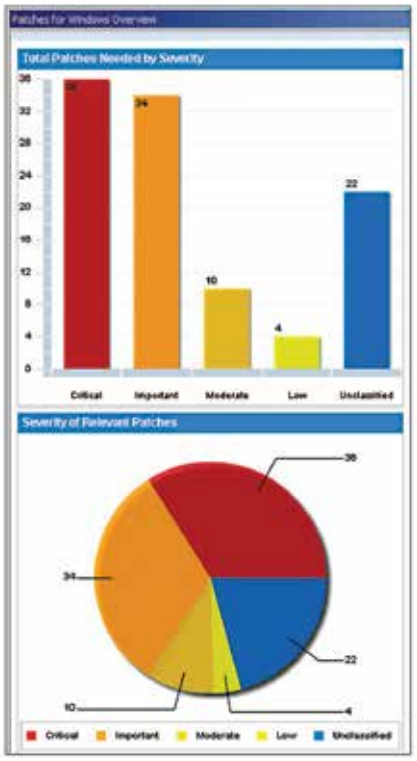
Prima: dopo l'applicazione è possibile che alcuni update non "risultino adeguati". Gli utenti disinstallano volutamente o involontariamente le patch, nuove applicazioni o nuove patch possono compromettere gli aggiornamenti installati, il malware può eliminare le patch oppure i problemi legati all'aggiornamento che richiedono un rollback. Le tecnologie di gestione delle patch devono controllare di continuo le macchine per garantire la conformità con le policy di update, fornendo risorse di rollback rapide e legate alla policy nel caso di problemi più seri. Se una patch viene eliminata contrariamente alle prescrizioni della policy di sicurezza, deve essere immediatamente reinstallata e se una patch crea un problema più grave dopo la sua applicazione, le imprese devono essere in grado di applicare un rapido rollback a larga scala. Senza gli strumenti adeguati questi interventi diventano impossibili.

Dopo: l'agent intelligente di BigFix garantisce di continuo la conformità alla policy per le patch, assicurando così lo stato di aggiornamento degli endpoint. Se per un qualsiasi motivo viene disinstallata una patch, la policy può stabilire che l'agent la riapplichi immediatamente sugli endpoint, se necessario. Nel caso di problemi con una patch, gli amministratori di BigFix lanciano rapidamente e facilmente il rollback sugli endpoint - su larga scala o su poche unità. Grazie alla console centrale unica, lo stato di conformità degli endpoint viene segnalato in tempo reale, permettendo agli amministratori informatici di controllare facilmente lo stato di tutti gli endpoint gestiti nell'impresa. Gli amministratori controllano così globalmente gli endpoint, gestendo una mole di lavoro decisamente maggiore rispetto ad altri prodotti, che esigono numerosi interventi manuali e significanti ritardi nel processo di reporting.

Fase 6: Report

Prima: conformità e policy aziendali richiedono dashboard e report dettagliati e aggiornati che evidenzino i rischi dell'impresa e lo stato di gestione delle patch per vari utenti, compresi i revisori della conformità, i dirigenti, il management e ogni utente finale. Senza una soluzione complessiva non è possibile ottenere report selettivi sullo stato globale delle patch nell'impresa.

Dopo: le risorse integrate di web reporting di BigFix permettono a utenti finali, amministratori, dirigenti, al management ecc. di visualizzare i dashboard e i report più aggiornati con la segnalazione di quali patch sono state applicate, indicando data, ubicazione ed endpoint correlati. Speciali dashboard "click-through" mostrano in tempo reale il progresso di gestione delle patch.



I report dashboard nel BigFix mostrano in tempo reale il progresso della gestione delle patch.

Il funzionamento della soluzione

I tradizionali metodi di approccio alla gestione delle patch con processi manuali e lenti meccanismi a scansione/sondaggio non rispondono con la velocità necessaria a soddisfare i requisiti commerciali e legali, con rischi elevati per le imprese e costi non accettabili. Le aziende che cercano di usare soluzioni gratuite o low-cost si rendono rapidamente conto che tali strumenti non sono all'altezza delle esigenze aziendali. Spesso le soluzioni provengono da un solo fornitore, non offrono un controllo relativo a dove le patch sono installate, i report sono scadenti e non rispecchiano lo stato operativo in tempo reale.

Gli endpoint che non implementano immediatamente le patch sono esposti agli attacchi dei criminali cibernetici e rappresentano un rischio per l'impresa. Inoltre le aziende devono gestire gli aggiornamenti per un'ampia varietà di prodotti di vari fornitori e per varie soluzioni hardware.

BigFix è leader di mercato per copertura, velocità, automazione ed efficienza economica, fornendo patch per sistemi operativi e applicazioni di terzi. La soluzione, che comprende l'applicazione di un agent intelligente, multifunzionale e snello per tutti gli endpoint, supporta un'ampia gamma di dispositivi, come server, PC, portatili connessi a Internet in roaming, e soluzioni specialistiche come gli apparecchi POS, ATM e chioschi self-service.

Un solo server di gestione è in grado di supportare fino a 250.000 endpoint, indipendentemente da ubicazione, tipo di collegamento, velocità o stato e con l'aggiunta di altri server si ottiene una scalabilità illimitata. I controlli basati sulla policy offrono agli amministratori IT risorse automatiche di gestione delle patch estremamente selettive e report precisi, per soddisfare i requisiti di conformità. La conformità alla policy è continuamente sottoposta a valutazione e applicazione dall'agent intelligente, indipendentemente dal collegamento degli endpoint alla rete. I prodotti della concorrenza possono risultare di difficile gestione , richiedendo un notevole impegno di hardware e personale in fase di deployment. In molti casi richiedono l'impiego di dozzine o centinaia di server, di agent multipli per gli endpoint, molti operatori per affrontare i problemi di un ambiente che BigFix è in grado di gestire con un solo server, un solo agent per gli endpoint e meno di un ventesimo del personale.

Un'ulteriore, essenziale caratteristica dell'architettura BigFix è il supporto offerto ai dispositivi in roaming come i computer portatili, che possono ricevere le patch attraverso una qualsiasi connessione a Internet, WiFi o dial-up. Il processo di gestione delle patch è virtualmente trasparente per l'utente e i messaggi Fixlet controllano l'intera larghezza di banda e la CPU mediante l'agent dell'endpoint, che è in grado di individuare ubicazione e connessione per ottimizzare l'uso della rete.

La garanzia di una conformità continua

Molte imprese devono elaborare, documentare e comprovare la conformità ai processi di gestione delle patch per soddisfare le prescrizioni di legge, gli accordi relativi al livello del servizio (SLA) e le policy aziendali. Prescrizioni come Sarbanes-Oxley (SOX), Payment Card Industry (PCI) Data Security Standard (DSS) e Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act richiedono un processo conforme e perfettamente documentato della gestione delle patch — con controlli sulla conformità continua per superare gli audit. Sfortunatamente molte imprese sprecano moltissimo tempo e risorse per la gestione delle patch, ma non soddisfano i requisiti per la conformità. BigFix è in grado di applicare le policy con report rapidi di conformità, per migliorare la reattività dell'impresa agli audit e il tasso di successo.

L'uso di IBM BigFix

Con BigFix le imprese affrontano faccia a faccia le sfide della gestione delle patch. I vantaggi per i clienti consistono in deployment più rapido, conformità ottimizzata, costi IT minori e cicli di gestione ridotti.

L'offerta di un ampio portafoglio di prodotti per la sicurezza e per la gestione degli endpoint

IBM offre risorse di gestione delle patch in un unico prodotto — IBM BigFix Patch — o come parte di due soluzioni più complesse di gestione degli endpoint — IBM BigFix Lifecycle e IBM BigFix Compliance. Il portafoglio di prodotti BigFix funziona utilizzando la stessa console, lo stesso server e lo stesso agent per gli endpoint, permettendo così alle imprese di ridurre i tools, il numero di agent per gli endpoint e i costi di gestione.

BigFix fa parte di un ampio portafoglio di prodotti IBM per la sicurezza, che aiuta le imprese a rispondere alle sfide di protezione per utenti e unità, dati e informazioni, applicazioni e processi, reti, server ed endpoint e per infrastrutture fisiche. Ottimizzando visibilità e controllo in tempo reale e migliorando la sicurezza e la gestione degli endpoint, il portafoglio di prodotti IBM supporta perfettamente i moderni data center in continua espansione, facilitando le attività IT sempre più strumentalizzate, interconnesse e intelligenti di un pianeta più intelligente.

La tecnologia BigFix fornisce:

- **Agent singolo intelligente -** BigFix sfrutta un approccio per essere leader nel settore, implementando un singolo e intelligente agent su ogni endpoint. Tale agent si occupa di diverse funzioni, compresi autovalutazione continua e applicazione della policy - con un impatto minimo sulla performance del sistema, visto che in media la CPU viene utilizzata per meno del due percento. L'agent opera con intelligenza, inviando i messaggi al server centrale di gestione e integrando patch, configurazioni o altre informazioni sull'endpoint quando necessario per risultare conformi alle policy correlate. Grazie alla velocità e all'intelligenza dell'agent, il server centrale dispone sempre delle informazioni aggiornate su conformità e stato di modifica degli endpoint, con report più rapidi e più aggiornati per la conformità.
- **Risposte immediate -** BigFix è grado di fornire risposte rapidissime in tutta l'azienda in pochi minuti, identificando il numero di Adobe Acrobat installati o di computer portatili interessati da una misura di ritiro da parte del produttore. Grazie all'agent intelligente, non è necessario attendere la conclusione di lente scansioni, i dettagli del server centralizzato o le migliaia di query SQL prima di generare dashboard e report. Ogni singolo agent valuta l'importanza della query, analizza l'informazione, rinvia i report e, se richiesto, applica determinati interventi in base ai risultati delle analisi.
- **Copertura degli endpoint in roaming -** Il computer portatile aziendale ha superato da tempo i confini degli uffici aziendali. Gli utenti si collegano sempre più spesso da abitazioni, alberghi, aeroporti e velivoli. BigFix consente di gestire gli endpoint in tempo reale anche in roaming.
- **Ampia copertura delle piattaforme -** È difficile stare al passo con gli aggiornamenti di sicurezza per i sistemi operativi, molto meno con gli aggiornamenti non critici e non correlati alla sicurezza e con i numerosi aggiornamenti applicativi - ma la vera sfida si presenta con le macchine virtuali offline. Tuttavia un ambiente BigFix ben gestito con contenuti e risorse continuamente aggiornati permette di affrontare la sfida, riducendo i tempi di inattività.

IBM BigFix RISPONDE ALLE SFIDE DELLA GESTIONE DELLE PATCH

Di seguito un esempio di come i nostri clienti abbiano ottenuto notevoli miglioramenti operativi con IBM BigFix in vari campi, che spaziano dal settore bancario, di distribuzione fino alla sanità.[1]

La sfida: velocizzare il deployment della gestione delle patch

Aggiornamenti software e tempi di ciclo delle patch **da 3 settimane a 3 giorni**

80% di tempo in meno per il deployment delle patch

90% in meno per le tempistiche di applicazione di nuove patch e aggiornamenti

La sfida: ottenere la conformità a licenze, policy aziendali e prescrizioni di legge

99.99% tasso di conformità delle patch

33% in più della conformità delle patch dal 60 al 93 percento

USD 1 milione di penali evitate per la non conformità delle licenze

La sfida: ridurre i costi IT

75% in meno di personale per la gestione degli endpoint

EUR 3.2 milioni risparmiati per costi di lavoro, licenze software e costi hardware

USD 500,000 risparmiati per i costi di licenza del software

[1] Si prega di consultare i case study dei clienti visitando: **ibm.com**/software/tivoli/solutions/endpoint/casestudies/

Conclusione

IBM BigFix risponde alle sfide essenziali che si pongono a un'impresa, fornendo una soluzione centralizzata e globale per la gestione delle patch su server, desktop e dispositivi mobili, snellendo notevolmente la procedura di test delle patch da parte del reparto IT. IBM BigFix effettua gli interventi in pochi giorni, e un solo server di gestione supporta fino a 250.000 endpoint, aumentando decisamente il tasso di successo per l'applicazione delle patch, migliorando la conformità alle prescrizioni di legge e riducendo le spese.

In un mondo dove contano i secondi IBM BigFix può rappresentare la differenza tra una strategia di successo per la gestione delle patch e una soluzione che non elimina i rischi per l'azienda.

Per ulteriori informazioni

Per avere maggiori informazioni su IBM BigFix, contattare il rappresentante IBM o l'IBM Business Partner, o visitare il sito: **ibm.com**/software/products/us/en/ibmendpmanaforpatcmana/

Le soluzioni IBM Security

IBM Security offre un portafoglio di prodotti e servizi più avanzati e integrati per la sicurezza aziendale. Grazie al supporto fornito dal team di ricerca e sviluppo IBM X-Force®, famoso in tutto il mondo, il portafoglio IBM fornisce soluzioni di security intelligence che aiutano le imprese a proteggere persone, infrastrutture, dati e applicazioni, con soluzioni di identity and access management, database security, application development, gestione del rischio, gestione degli endpoint, network security e molto altro. Tali soluzioni permettono alle imprese di gestire con efficienza i rischi e di proteggere dispositivi mobili, cloud, social media e altre architetture aziendali. Con oltre 6,000 ricercatori, sviluppatori ed esperti impegnati in iniziative di sicurezza, IBM gestisce una delle maggiori organizzazioni al mondo di ricerca e sviluppo in ambito security, e un'altrettanta vasta organizzazione globale per il delivery dei servizi di sicurezza. Le aziende possono inoltre trarre beneficio dall'intelligence che deriva dagli oltre 15 miliardi di eventi di sicurezza che si verificano ogni giorno e che il team dei Managed Security Services di IBM tiene sotto controllo in più di 130 paesi.

IBM Global Financing può aiutarvi nell'acquisto delle risorse software necessarie al vostro business. Supportiamo i clienti giudicati idonei al credito per realizzare una soluzione di finanziamento su misura, al fine di rispondere agli obiettivi commerciali e di sviluppo, di permettere una gestione efficiente del cash migliorando il TCO (total cost of ownership). Finanziate con IBM Global Financing i vostri investimenti critici IT e date slancio al vostro business. Per ulteriori informazioni, visitare il sito **ibm.com**/financing

Dichiarazione di pratiche di sicurezza efficaci: la sicurezza del sistema IT implica la protezione di sistemi e informazioni tramite la prevenzione, il rilevamento e la risposta ad accessi inappropriati provenienti dall'interno o dall'esterno dell'azienda. Un accesso inappropriato può avere come risultato l'alterazione, la distruzione, l'uso non idoneo o non corretto di informazioni o può causare un danno o un utilizzo non corretto dei sistemi, incluso l'utilizzo per attacchi verso altri. Nessun prodotto o sistema IT dovrebbe essere considerato totalmente sicuro e nessun singolo prodotto o misura di sicurezza può essere completamente efficace nella prevenzione dall'accesso inappropriato. I sistemi e i prodotti IBM sono progettati per fare parte di un approccio alla sicurezza nel completo rispetto delle norme, che implicherà necessariamente ulteriori procedure operative e può richiedere l'installazione di altri sistemi, prodotti o servizi per realizzare la massima efficienza. IBM non garantisce che sistemi e prodotti siano immuni da o rendano un'azienda immune da condotte dannose o illecite da parte di terzi.

[1] James Lewis e Stewart Baker, "The Economic Impact of Cybercrime and Cyber Espionage," *Center for Strategic and International Studies (CSIS) e McAfee*, luglio 2013. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (MI)
Italia

WGW03137-ITIT-00