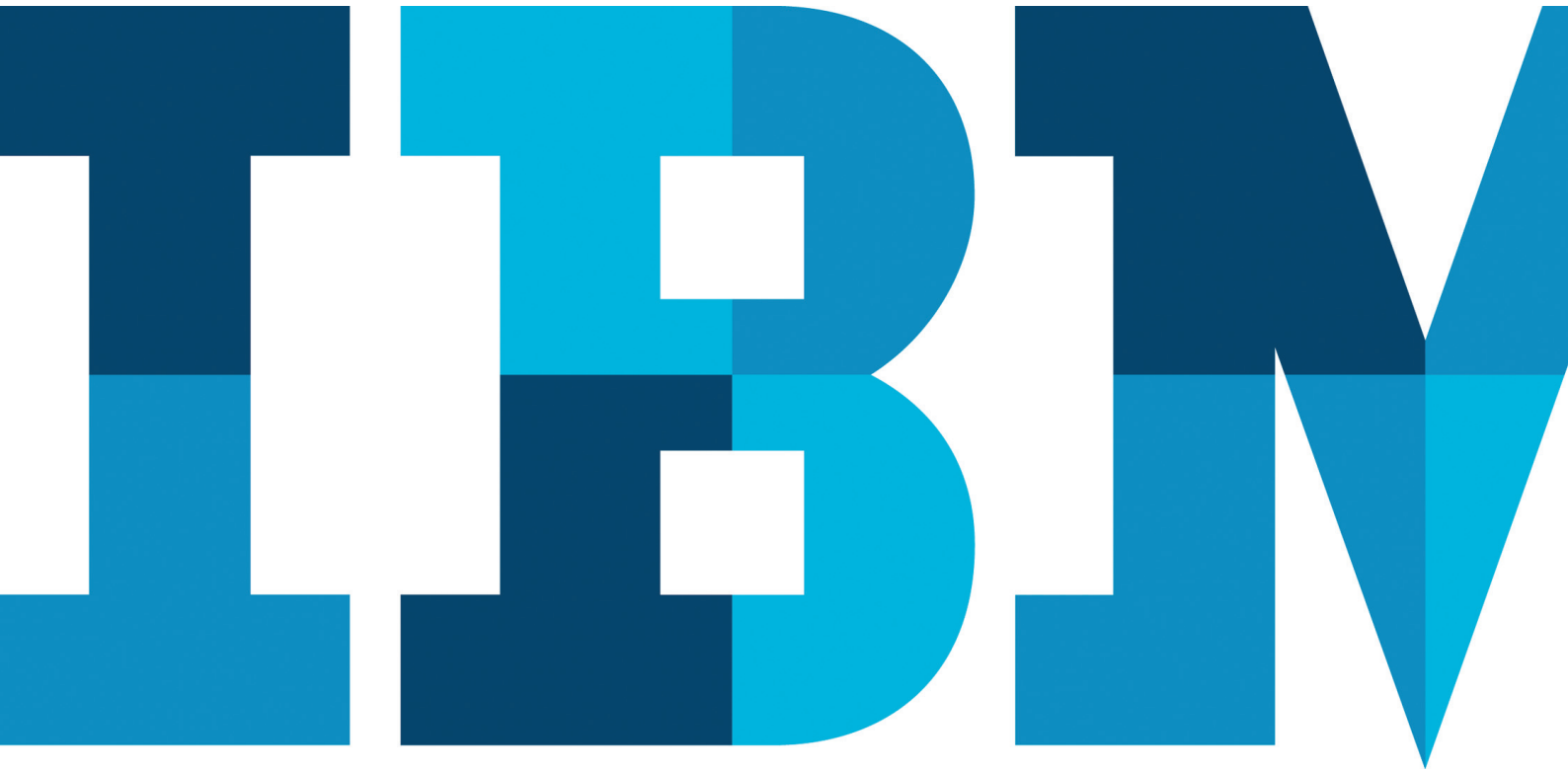
Software IBM
Thought Leadership White Paper

Febbraio 2011

Riscrittura delle regole di gestione delle patch

IBM Tivoli Endpoint Manager fa evolvere il paradigma di gestione delle patch



IBM

Indice

Introduzione

Gli attacchi malware sono in corsa contro il tempo per colpire i computer vulnerabili prima che i vendor dei software pubblichino le patch e che i clienti possano applicarle. Quando il malware raggiunge il suo scopo, le organizzazioni perdono produttività e rischiano perdite di dati sensibili, possibili conflitti e multe. L'enormità del problema è allarmante – la battaglia in corso tra hacker e società di software costa all'economia degli Stati Uniti una stima di $266 miliardi all'anno, secondo il Cyber Secure Institute, un gruppo di advocacy con sede a Washington, D.C.[1]

Per combattere questa minaccia, sempre più vendor stanno immettendo sempre più patch nel tentativo di essere al passo con la frenesia degli attacchi malware. Sfortunatamente, la maggior parte delle organizzazioni non dispone dell'attrezzatura adeguata per gestire l'installazione di questo elevato numero di patch in modo economico e puntuale. A causa dei processi organizzativi, la maggior parte dei reparti IT impiega settimane o addirittura mesi per distribuire le patch in tutto l'ambiente. Secondo alcune stime, le organizzazioni possono impiegare fino a quattro mesi per raggiungere un 90-95% di tasso di conformità delle patch installate. Fino a quel momento, è stato utilizzanto un numero indefinito di patch, ciò significa che le organizzazioni sono perennemente a rischio e non sono conformi – e la situazione può solo peggiorare con il passare del tempo.

La gestione delle patch è sempre stata un percorso in salita a causa della grande complessità intrinseca. Nonostante i rischi, alcune organizzazioni sono riluttanti ad utilizzare le patch per il lavoro ed il tempo richiesti e per le possibili interruzioni delle operazioni di business. In un'organizzazione con un ambiente hardware e software eterogeneo, essere aggiornati sulle molteplici patch – ed utilizzarle tempestivamente – può sovraccaricare lo staff IT ed i budget. È necessaria una soluzione di gestione delle patch basata sulle policy che sia distribuibile rapidamente, che sia economica e che:

- Funzioni per tutti gli endpoint nelle organizzazioni di tutte le dimensioni, incluse le più grandi
- Supporti più vendor, sistemi operativi, applicazioni e piattaforme
- Funzioni su connessioni lente o veloci e supporti periferiche all'interno della rete dell'organizzazione
- Minimizzi le richieste allo staff IT
- Operi in tempo reale, distribuendo patch in tutta l'azienda in poche ore.

IBM Tivoli Endpoint Manager, costruito sulla tecnologia BigFix, combina tutte le parti relative alla gestione delle patch in una soluzione intelligente, semplificata che ottimizza il processo di ricerca, valutazione, risoluzione, conferma, rafforzamento e notifica delle patch.

L'enigma della gestione delle patch

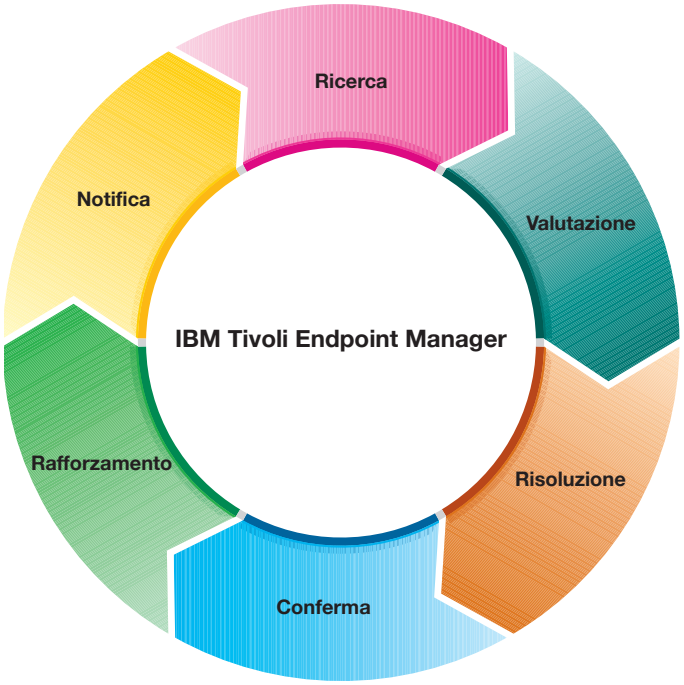
La gestione delle patch sembra chiara ma rappresenta una delle sfide più complesse e critiche che un'organizzazione deve affrontare. Le sfumature di una gestione efficace delle patch vanno al di là di avere un amministratore di sistema installa le patch oppure affidarsi o affidarsi ad un meccanismo di patch fornito da un vendor, sperando che vengano utilizzate in modo corretto, ma non avendo mai la certezza. L'enigma della gestione delle patch suscita domande alle quali molte organizzazioni potrebbero avere difficoltà – se non impossibilità – a trovare una risposta. Ad esempio:

- Un'organizzazione come può distribuire patch critiche "out-of-band" che arrivano urgentemente e non rientrano nella pianificazione delle patch di routine?
- In che modo gli amministratori di sistema possono tenere traccia delle patch in un ambiente con centinaia di migliaia di endpoint sui quali sono installati vari sistemi operativi e applicazioni?
- In che modo gli amministratori di sistema possono monitorare lo stato dei laptop in roaming e altri dispositivi mobili?
- Quanto tempo impiegherà il processo di patch dall'inizio alla fine e in che modo gli amministratori confermeranno (e proveranno) che ciascun endpoint nell'infrastruttura è stato aggiornato in modo appropriato – e rimarrà in quel modo?
- In che modo gli amministratori di sistema verificano rapidamente le patch prima di distribuirle e sottoporle a rollback se causano problemi?
- In che modo è possibile distribuire le patch senza che si interferisca con end-user experience e la produttività dell'utente finale?

Mentre ricerche mostrano che la gestione delle patch è una delle priorità di sicurezza più importanti per le organizzazioni, queste domande indicano solo il modo con cui le aziende affrontano le innumerevoli barriere che si presentano all'implementazione delle pratiche effettive di gestione delle patch. Tra la mancanza di visibilità e di personale, il possibile impatto sul business, le limitazioni dell'ampiezza di banda passante, la mancanza di maneggevolezza, tempi di risoluzione lunghi, problemi di scalabilità e copertura per diverse piattaforme, applicazioni di terze parti ed endpoint in roaming, gli ostacoli sono molteplici.

Fortunatamente, questi ostacoli sono superabili. Tivoli Endpoint Manager rimuove questi ostacoli con una soluzione completa creata appositamente per ambienti eterogenei largamente distribuiti. Con questa soluzione, le organizzazioni possono finalmente osservare, modificare, rafforzare e notificare lo stato di compliance delle patch in tempo reale, su una scala globale, attraverso una sola console.

Processo di gestione delle patch



Con Tivoli Endpoint Manager, la gestione delle patch diventa un processo completo completamente unificato che aiuta a migliorare la sicurezza e a risparmiare denaro.

Come cambia il paradigma della gestione delle patch

Poiché non esiste una sola best practice della gestione delle patch ufficiale, l'approccio generale interessa un processo completo con sei fasi basilari: ricerca, valutazione, risoluzione, conferma, rafforzamento e notifica. Storicamente, molte di queste fasi venivano implementate attraverso tecnologie separate, non integrate, rendendo virtualmente impossibile creare un processo di gestione delle patch completo in tempo reale. Tivoli Endpoint Manager fornisce tutte queste fasi come parte di un processo unificato, completamente integrato, che può aiutare a migliorare la sicurezza e a risparmiare denaro, tempo e risorse.

Di seguito viene presentata un vista prima-e-dopo del modo in cui la soluzione modifica le regole della gestione delle patch.

Fase 1: Ricerca

Prima: la prima fase nel processo di gestione delle patch interessa la scoperta di quali sono le patch disponibili. Ciò include la ricerca della disponibilità di patch nei messaggi email del vendor, nelle notifiche pop-up delle applicazioni, nei siti web, nei blog e in una varietà di altre fonti. Questo processo deve essere ripetuto ogni settimana – o anche ogni giorno – per centinaia di patch ed un numero elevato di sistemi operativi, applicazioni e fornitori di soluzioni anti-malware. Un'alternativa – affidandosi agli aggiornamenti automatici del vendor – può portare ad errori che possono avere conseguenze negative, poiché l'accettazione automatica delle patch senza verifica può mettere le organizzazioni a rischio, non esiste un controllo aziendale sulla tempistica e la notifica e affidarsi agli utenti per applicare gli aggiornamenti è una condizione rischiosa e inaffidabile.

Un migliore approccio è avere un vendor di gestione delle patch che fornisca un flusso consolidato delle patch più comuni in modo che l'organizzazione debba solo valutare ciascun carico di patch al momento della distribuzione, verificarne la compatibilità con l'ambiente di destinazione e distribuirle attraverso policy altamente granulari destinate a specifici profili di macchine, poiché consente che patch specifiche vengano applicate solo agli endpoint che le necessitano. Il problema con questo approccio è che non è automatizzato, richiede risorse e tempo significativi che le organizzazioni potrebbero non avere.

Dopo: IBM acquisisce, verifica, impacchetta e distribuisce le patch di vendor di sistemi operativi, anti-malware e di comuni applicazioni terze parti direttamente a clienti, rimuovendo un considerevole sovraccarico di ricerca della gestione delle patch. Quando un vendor supportato rilascia una nuova patch, IBM riceve la patch, esegue l'analisi preliminare e crea le patch policy, chiamate messaggi IBM Fixlet, che uniscono l'aggiornamento alle informazioni della policy come ad esempio le dipendenze tra le patch, i sistemiai quali appalicarle e il livello di severità. I Fixlet vengono automaticamente inviati ai server dei clienti di Tivoli Endpoint Manager. La soluzione fornisce anche un processo attraverso il quale i clienti possono configurare il prodotto per scaricare le patch direttamente dai siti dei vendor o memorizzare il contenuto della patch localmente; i clienti possono anche creare i propri Fixlet personalizzati utilizzando un'interfaccia basata su una procedura guidata. Questo processo funziona virtualmente per qualsiasi aggiornamento, incluse le patch di applicazione interna.

Fase 2: Valutazione

Prima: per ogni patch identificata, l'organizzazione IT deve determinare l'applicabilità e la criticità dell'aggiornamento, identificando quali endpoint nell'organizzazione hanno bisogno di patch. In caso di aggiornamenti di sicurezza, questi dati critici si traducono direttamente in rischio, poiché il rischio di business aumenta conseguentemente al numero di endpoint senza patch. Molte organizzazioni non hanno accesso alla valutazione corrente e completa dei dati sugli asset e le configurazioni necessari per quantificare l'ambito e l'impatto delle patch nell'organizzazione. Esistono strumenti che possono aiutare ad acquisire questi dati, ma molti richiedono giorni o settimane per raccogliere e riunire queste informazioni effettuando una scansione di ciascun endpoint sulla rete – e molti endpoint in roaming sono raramente connessi alla rete – un processo di questo tipo può impiegare giorni per essere completato. Queste informazioni devono essere immediatamente disponibili per gli amministratori di sistema al momento del rilascio della patch poiché molte patch sono critiche per quanto riguarda la tempistica e deve avvenire il più presto possibile il processo di valutazione dei rischi e di prioritizzazione delle patch.

Dopo: con Tivoli Endpoint Manager, un solo agent software intelligente viene installato su tutti gli endpoint gestiti per monitorare e notificare di continuo lo stato, inclusi i livelli di patch, a un server di gestione. L'agent confronta anche la conformità degli endpoint con le policy definite, come ad esempio i livelli di patch obbligatori e le configurazioni standard. Queste informazioni sono critiche soprattutto in caso di patch di emergenza quando un vendor rilascia una patch altamente critica, out-of-band e le organizzazioni devono rapidamente quantificare l' importanza e il rischio di attacchi correlati. In un esempio, un cliente che utilizza Tivoli Endpoint Manager ha installato agent su 5.100 endpoint e ha scoperto che a più di 1.500 (30%) mancava una patch critica. Nel complesso, agli endpoint nell'organizzazione mancavano 20.033 patch "critiche" – una media di 13 patch per endpoint. Una volta associato il numero totale di patch agli endpoint che le necessitano e una volta definita la criticità di business, l'organizzazione IT può procedere alla fase di risoluzione.

Fase 3: Risoluzione

Prima: una volta valutata una patch ed effettuata una verifica per distribuirla nell'organizzazione, deve essere impacchettata e testata per assicurare che non entri in conflitto con altre patch e con software terze parti installati sugli endpoint di destinazione. È necessario anche determinare i prerequisiti e le dipendenze delle patch, come ad esempio i livelli minimi di service pack. In genere ciò viene eseguito applicando e verificando l'aggiornamento su un numero selezionato di endpoint prima di un rilascio generalizzato – un processo che può impiegare giorni o settimane per essere completato se si utilizzano strumenti manuali. Quando il test indica che la patch è probabilmente sicura per essere distribuita nell'organizzazione, viene applicata agli endpoint interessati, in genere in modalità batch, estendendo poi la finestra delle patch. I tempi lunghi di risoluzione sono principalmente dovuti all'impossibilità di contare sulla qualità delle patch e secondariamente sono dovuti a meccanismi di distribuzione inaffidabili, entrambi questi elementi provocano dei bassi tassi di patch first-pass. La maggior parte delle organizzazioni sono quindi forzate a procedere lentamente nel caso in cui una patch causi un problema imprevisto e sono anche forzate ad assicurare che i link di rete non siano sovraccarichi dal processo di distribuzione patch. Quindi, la risoluzione è spesso difficile che avvenga in tempi rapidi e in modo efficiente al livello dell'organizzazione.

Un altro problema principale è che molti strumenti di gestione delle patch funzionano solo per Microsoft® Windows® a causa di dipendenze da strumenti Microsoft come WSUS (Windows Server Update Services). Molti strumenti richiedono una profonda expertise sulle piattaforme e un personale altamente qualificato che operi su di esse. Molti di questi strumenti non funzionano fino a che gli endpoint non sono connessi a una rete aziendale ad elevata velocità, lasciando i laptop in roaming e altri endpoint mobili fuori dal ciclo di aggiornamento per lunghi periodi. Molti non forniscono i controlli specifici basati sulle policy, con cui gli operatori devono distribuire in modo efficace le patch a tutti gli endpoint interessati nell'organizzazione. I controlli come ad esempio le finestre dei tempi di installazione patch, la possibilità che un utente sia presente o meno, le opzioni di riavvio, il metodo di distribuzione (inclusa l'ampiezza di banda passante e le limitazioni CPU), il tipo di sistema e le opzioni di notifica utente devono essere input disponibili nei processi di aggiornamento automatizzati.

Dopo: quando IBM pubblica nuovi Fixlet per le patch, tramite Tivoli Endpoint Manager, le organizzazioni possono determinare l'ambito dell'aggiornamento creando un report in pochi minuti che mostri quali endpoint aggiornare. I Fixlet per le patch includono le istruzioni di distribuzione, incluso il sistema operativo, i requisiti di versione ed i prerequisiti, eliminando la necessità da parte dell'IT di "impacchettare" e quindi verificare la patch. Gli operatori possono quindi impiegare pochi minuti a determinare quale patch distribuire, quale notifica far visualizzare agli utenti finali (se presenti), se consentire agli utenti di ritardare l'installazione di una patch e per quanto tempo e se forzare (o ritardare) i riavvii. Entro pochi minuti, l'agent di endpoint riceve la nuova policy e l'endpoint determina se la patch è applicabile, e nel caso lo fosse, scarica e applica la patch, notificando la riuscita o il fallimento entro pochi minuti. Questo approccio, combinato con la struttura del relay di Tivoli Endpoint Manager e la capacità di raggiungere i dispositivi connessi a Internet, riduce significativamente il carico di rete e migliora la percentuale di successo al primo tentativo di più del 95%.

La soluzione fornisce anche un meccanismo altamente sicuro che utilizza identità codificate, assicurando che solo gli amministratori autorizzati possono creare e distribuire policy. Inoltre, poiché non esiste alcuna dipendenza da Active Directory, gli amministratori di Tivoli Endpoint Manager non devono essere amministratori del dominio di Active Directory. La soluzione memorizza le informazioni di audit che tengono traccia di chi ha ordinato quali policy da applicare a quali endpoint e non richiede un'expertise specifica per un sistema operativo agli operatori che avviano il processo di risoluzione. Qualsiasi operatore di Tivoli Endpoint Manager con poche ore di formazione di base può applicare con sicurezza e rapidamente patch ai sistemi operativi Windows, Linux®, UNIX® e Mac senza un'expertise o conoscenza specifiche del dominio.

Fase 4: Conferma

Prima: una volta pianificate le patch da applicare, è necessario confermare che l'installazione sia avvenuta correttamente in modo che il dipartimento IT sappia quando è stato completato il ciclo della patch e sono supportati i requisiti di reporting di conformità. Questi dati devono essere comunicati al sistema di reporting centrale che aggiorna il personale sul processo, incluse le eccezioni, in tempo reale. Tuttavia, molte tecnolgie di gestione delle patch non eseguono in modo efficace questo processo, richiedendo settimane per effettuare una nuova scansione di tutti gli endpoint e anche di più per correggere le eccezioni. Questo ritardo introduce un'incertezza significativa intorno al rischio di business e alla posizione di conformità dell'azienda in generale.

Molti prodotti non danno conferma che le patch vengano applicate – o se lo fanno, ci vogliono giorni o addirittura settimane per ottenere un report per tutta l'organizzazione. Ancora peggio, alcuni strumenti riportano in modo non corretto che le patch sono state applicate quando in realtà i file sono stati scaricati ma la patch non è stata applicata. Con questa quantità di ritardi e incertezza, alcuni endpoint sono spesso lasciati esposti, con una significativa finestra di vulnerabilità.

Dopo: una volta distribuita la patch, l'agent di Tivoli Endpoint Manager automaticamente e continuamente rivaluta lo stato dell'endpoint per confermare l'installazione corretta, aggiornando immediatamente il server di gestione in tempo reale (o in caso di dispositivi in roaming, alla prima occasione). Questa fase è critica nel supportare i requisiti di conformità, che richiedono una prova definitiva di un'installazione di patch continua. Con questa soluzione, gli operatori possono osservare in tempo reale il processo di distribuzione delle patch tramite una console di gestione centralizzata, ricevendo conferma dell'installazione delle patch in pochi minuti dall'avvio del processo di patch. La chiusura del loop sulla distribuzione delle patch consente alle organizzazioni di assicurare la conformità alle patch in un modo più intelligente, rapido e affidabile.

Fase 5: Rafforzamento

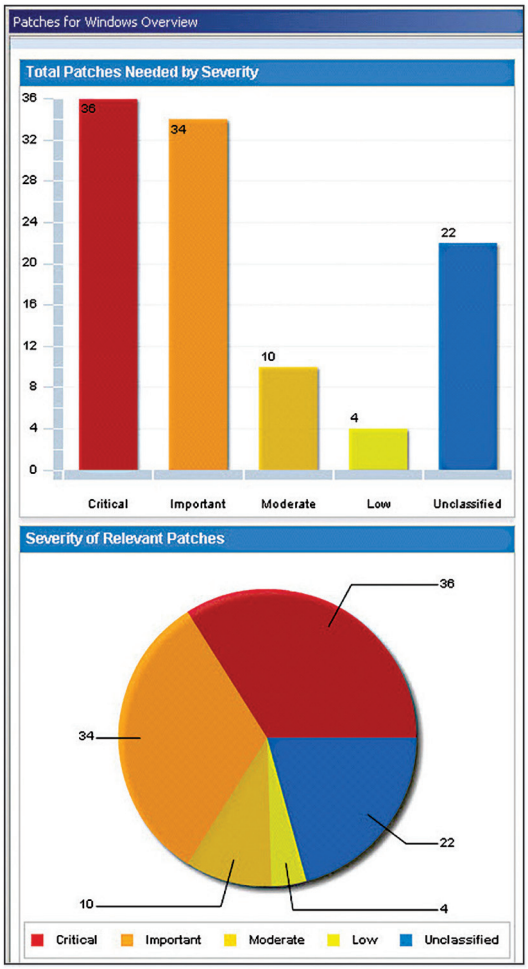
Prima: dopo l'applicazione iniziale, molti aggiornamenti non sempre "rimangono". Gli utenti intenzionalmente o accidentalmente disinstallano le patch, le nuove applicazioni o le patch possono corrompere gli aggiornamenti esistenti, il malware potrebbe deliberatamente rimuovere le patch o i problemi creati dall'aggiornamento possono necessitare di un rollback. Le tecnologie di gestione delle patch devono continuamente monitorare le macchine per assicurare la conformità alle policy di aggiornamento, fornendo funzioni di rollback rapide, basate sulla policy nel caso di un grave problema di patch. Se una patch viene rimossa violando la policy di sicurezza, deve essere immediatamente reinstallata e se una patch crea un problema importante dopo l'applicazione, anche le organizzazioni devono essere in grado di immettere un rollback di massa rapido. Senza gli strumenti appropriati, questa fase diventa praticamente impossibile.

Dopo: l'agent intelligente di Tivoli Endpoint Manager controlla in continuazione la conformità alla policy delle patch, assicurando che gli endpoint rimangano aggiornati. Se una patch viene disinstallata per un qualsiasi motivo, la policy può specificare che l'agent deve automaticamente riapplicarla all'endpoint se necessario. In caso di problemi con una patch, gli amministratori di Tivoli Endpoint Manager possono rapidamente e facilmente immettere un rollback agli endpoint – in massa o ad alcuni selezionati. Tramite la stessa console centralizzata, lo stato di conformità degli endpoint viene riportato in tempo reale, consentendo agli amministratori IT di monitorare facilmente lo stato di tutti gli endpoint gestiti nell'organizzazione. Gli amministratori possono godere di un controllo completo dei propri endpoint, potendo gestire molte volte la quantità di lavoro di altri prodotti che richiedono un significativo intervento manuale e introducono ritardi di tempo significativi nel processo di notifica.

Fase 6: Notifica

Prima: la notifica è una componente critica del processo di gestione delle patch. Le policy aziendali e di conformità richiedono report e dashboard aggiornati e altamente dettagliati che indicano la posizione a rischio dell'organizzazione e lo stato di management delle patch per una varietà di clienti, inclusi gli auditor di conformità, gli executive, il management ed anche gli utenti finali. Senza una soluzione globale, non esiste un modo chiaro per avere una notifica sullo stato della patch nell'organizzazione.

Dopo: le funzioni di notifica web integrata di Tivoli Endpoint Manager consentono agli utenti finali, agli amministratori, agli executive e al management e ad altri di visualizzare dashboard e report aggiornati che indicano quali patch sono state distribuite, quando, chi le ha distribuite e a quali endpoint. Speciali dashboard "cliccabili" mostrano il progresso di gestione delle patch in tempo reale.



I report del dashboard in Tivoli Endpoint Manager mostrano il progresso di gestione delle patch in tempo reale.

Perché funziona

Gli approcci di gestione delle patch tradizionali che utilizzano processi manuali e meccanismi basati su lente tecniche di scan-and-poll sono più rapidi o economici da soddisfare i requisiti aziendali e normativi, lasciando le organizzazioni con costi e rischi elevati inaccettabili. Molte organizzazioni che cercano di utilizzare strumenti di vendor "gratuiti" o a basso costo come ad esempio WSUS rapidamente realizzano che queste soluzioni non sono di classe enterprise. Sono limitati a un vendor singolo, non forniscono controllo dell'organizzazione su quali patch inviare, quando e dove, sono dannosi per l'utente finale e offrono un reporting scarso che non riflette lo stato in tempo reale. WSUS è un esempio perfetto di un prodotto puntuale utilizzato per eseguire solo una fase nel processo di gestione delle patch evidenziato in precedenza e viene utilizzato solo perché è visto come "gratuito".

Microsoft ha introdotto cicli di release di patch regolari, noti come "Patch Tuesdays", che sfortunatamente hanno generato anche "Hack Wednesdays", durante le quali i cyber criminali hanno grandi opportunità di attaccare gli endpoint senza patch senza dover faticare per scoprire nuove vulnerabilità. Gli endpoint a cui immediatamente non sono state fornite le patch diventano un'occasione di accesso per i criminali e rappresentano un rischio per l'organizzazione. Inoltre, le organizzazioni devono gestire gli aggiornamenti per una vasta varietà di prodotti di vendor e hardware form factor – non solo Windows.

Tivoli Endpoint Manager è leader sul mercato in termini di ampiezza di copertura, velocità, automazione ed efficienza di costi e fornisce un sistema operativo completo e patch di applicazioni di terze parti. La soluzione, che include la distribuzione a tutti gli endpoint di un agent a più scopi, semplice e intelligente, supporta un'ampia varietà di tipi di dispositivi che vanno da server a PC desktop, laptop in "roaming" connessi a Internet ed attrezzatura specializzata come ad esempio dispositivi POS (point-of-sale), ATM (automated teller machines) e chioschi self-service.

Un solo server di gestione può supportare fino a 250.000 endpoint, a prescindere dalla loro posizione, tipo di connessione e velocità o stato e server aggiuntivi possono fornire una scalabilità virtualmente illimitata. I controlli basati sulle policy forniscono agli amministratori IT funzioni di gestione delle patch altamente automatizzate e specifiche e e report completi di supporto ai requisiti di compliance. La conformità alle policy è continuamente valutata e rafforzata da un agent intelligente, a prescindere dalla connettività dell'endpoint alla rete. Altri prodotti sono pesanti a livello di back-end, richiedendo quantità massicce di hardware e di personale per supportare le distribuzioni – in molti casi, dozzine, ventine o anche centinaia di server, più agent per endpoint ed un'armata di operatori – per supportare lo stesso ambiente che Tivoli Endpoint Manager gestisce con un server di gestione, un agent di endpoint e con meno di 1/20 del personale.

Un altro aspetto chiave dell'architettura è il supporto agli endpoint che sono attivi e non collegati alla rete aziendale. I dispositivi in roaming come i laptop, ad esempio, possono ricevere patch attraverso una connessione Internet come Wi-Fi o dialup. Il processo di gestione delle patch è virtualmente trasparente per l'utente e i messaggi IBM Fixlet controllano le quantità totali di ampiezza di banda e CPU (central processing unit) consumate dall'agente di endpoint, che è cosciente di dove si trova e della connessione, per ottimizzare l'utilizzo di rete.

Conformità continua

Molte organizzazioni devono stabilire, documentare e provare la conformità con i processi di gestione delle patch per soddisfare le regole governative, gli SLA (service level agreements) e le policy dell'azienda. Le normative come ad esempio Sarbanes-Oxley, PCI DSS e HIPAA/HITECH richiedono che sia messo in opera un processo di gestione delle patch regolare, completamente documentato ed è necessaria una prova di conformità continua per poter superare gli audit. Sfortunatamente, molte organizzazioni sprecano un'enorme quantità di tempo e risorse per la gestione delle patch, e ancora non riescono a soddisfare i requisiti di conformità. La capacità di Tivoli Endpoint Manager di rafforzare le policy e notificare rapidamente la conformità può aiutare l'organizzazione ad essere pronta per gli audit ed a superarli.

Come i clienti lo stanno utilizzando

Le organizzazioni stanno affrontando le sfide della gestione delle patch utilizzando Tivoli Endpoint Manager. Per i clienti, i risultati hanno incluso una distribuzione più rapida, una conformità migliore e hanno ridotto i costi IT ed i cicli di gestione.

Sfida: Distribuzione delle patch in giorni o settimane – non in mesi o anni

- Albany County, NY, ha consolidato un certo numero di strumenti di gestione delle patch e della configurazione in solo due giorni
- I ristoranti O'Charley hanno distribuito patch in oltre 350 ristoranti in soli quattro giorni
- SunTrust Banks ha implementato una soluzione per 50.000 endpoint dislocati in circa 1.800 sedi in tre mesi con solo due persone
- International Islamic University Malaysia ha completato una distribuzione completa su 7.000 computer fissi e mobili in sette campus universitari con ampiezza di banda limitata in solo sei settimane.

Sfida: Raggiungimento della conformità con SLA, policy aziendali e normative

- Purolator ha raggiunto un 100% di conformità con uno SLA di 24 ore dal provider del servizio gestito
- SunTrust Banks ha raggiunto il 98,5% di conformità di patch su 50.000 endpoint
- Concord Hospital ha aumentato la conformità di patch dal 40-60%, al 93%
- Entergy IT, che deve soddisfare gli SLA che richiedono la distribuzione delle patch in più di 22.000 endpoint entro un arco di 10 giorni dalla release, ha distribuito più di 4,9 milioni di patch nell'azienda dal 2004 – e non ha mancato un singolo SLA in questo periodo.

Sfida: Riduzione dei costi IT

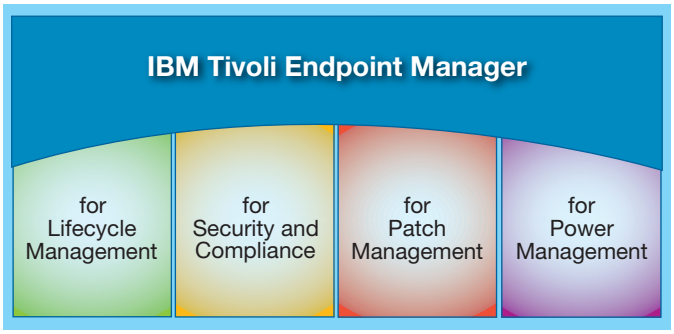
- BGC Partners ha eliminato le spese di viaggio costose alle sedi remote in sei continenti, risparmiando decine di migliaia di dollari
- Tax Tech ha ridotto i FTE (full-time equivalents) della gestione delle patch da 20 a uno
- Stena Lines ha raggiunto un rapporto risparmio di forza lavoro di 12:1 riducendo il tempo di sovraccarico amministrativo per i processi di patch da 240 ore a 20 ore
- Western Federal Credit Union ha riportato una riduzione del 50% nei costi di lavoro attraverso l'automazione e la gestione delle patch unificata.

Sfida: Riduzione dei cicli di gestione delle patch

- Concord Hospital ha diminuito i cicli delle patch da settimane a solo 15 minuti
- SunTrust Banks ha ridotto i cicli di patch da due-tre settimane a due-tre giorni
- Tax Tech ha completamente automatizzato la distribuzione di patch a ciclo continuo in più di 1.000 sedi connesse via VPN (virtual private network)
- Il gruppo di gestione server e desktop di Entergy ha installato 70.000 patch nell'azienda in 24 ore
- Kronos distribuisce aggiornamenti software, policy e patch a tutti gli endpoint idonei entro 15 minuti in tutto il mondo.

Un portfolio completo di soluzioni di conformità e sicurezza

IBM offre funzioni di gestione delle patch attraverso uno specifico prodotto – IBM Tivoli Endpoint Manager per la gestione delle Patch – o come parte integrante di due soluzioni di gestione endpoint più ampie – IBM Tivoli Endpoint Manager for Lifecycle Management e IBM Tivoli Endpoint Manager for Security and Compliance. La famiglia Tivoli Endpoint Manager opera dalla stessa console, server di gestione e agent di endpoint, consentendo alle organizzazioni di consolidare gli strumenti, ridurre il numero di agent di endpoint e diminuire i costi di gestione.



IBM Tivoli Endpoint Manager è una famiglia di prodotti in cui tutti operano dalla stessa console, server di gestione e agent di endpoint intelligente.

Tivoli Endpoint Manager è parte di un portfolio di soluzioni di sicurezza IBM completo, che aiuta le organizzazioni a gestire le sfide relative alla sicurezza per utenti e identità, dati e informazioni, applicazioni e processi, reti, server ed endpoint, incluse le infrastrutture fisiche. Migliorando la visibilità in tempo reale e il controllo e migliorando la sicurezza degli endpoint e la loro gestione, il portfolio IBM supporta i data centre più intelligenti ed in continua espansione per facilitare le operazioni IT intelligenti, interconnesse e dotate di strumenti di un pianeta più intelligente.

La tecnologia Tivoli Endpoint Manager fornisce:

- **Un singolo agent intelligente** – Tivoli Endpoint Manager utilizza un approccio leader nel settore che posiziona un singolo agent intelligente su ciascun endpoint. Questo agent esegue funzioni multiple che includono un'auto-valutazione continua e un rafforzamento delle policy – nonostante questo ha un impatto minimo sulle prestazioni del sistema, utilizzando mediamente meno del due percento della CPU di un endpoint. L'agent avvia le azioni in modo intelligente, inviando messaggi upstream al server di gestione centrale ed estraendo patch, configurazioni od altre informazioni per gli endpoint quando è necessario per essere conformi ad una policy rilevante. Come risultato dell'intelligenza e della velocità dell'agent, il server di gestione centrale conosce la conformità e lo stato delle modifiche degli endpoint, consentendo un report di compliance rapido ed aggiornato.

- **Risposte istantanee** – Se si rileva quante istanze di Adobe Acrobat sono installate o si convalida quali laptop sono influenzati da un richiamo del produttore, Tivoli Endpoint Manager fornisce risposte in pochi minuti – nell'organizzazione. Grazie all'agent intelligente, non c'è necessità di attendere il completamento di lunghe scansioni, con un server centralizzato che si blocchi sui dettagli, o il completamento di migliaia di query SQL prima di creare dashboard e report. Ciascun agent valuta la rilevanza della questione, analizza le informazioni ed esegue una notifica e addirittura agisce sulla base delle analisi, se richiesto.
- **Copertura per gli endpoint in roaming** – Il laptop di proprietà dell'azienda si è spostato ben oltre i confini di un ufficio dell'azienda. Gli utenti si connettono da casa, dagli hotel, dagli aeroporti o anche dagli aerei. Stando sempre un passo avanti, Tivoli Endpoint Manager fornisce la capacità esclusiva di gestire gli endpoint in tempo reale – anche per i dispositivi in roaming.

Conclusione

Tivoli Endpoint Manager gestisce le sfide chiave che molte organizzazioni attualmente affrontano, fornendo un server centralizzato a livello di organizzazione, una soluzione di gestione delle patch dei dispositivi mobili e desktop che automatizza e allevia il dipartimento IT da gran parte del processo di verifica patch. Tivoli Endpoint Manager si configura in pochi giorni ed un singolo server di gestione supporta fino a 250.000 endpoint, aumentando drasticamente i tassi di successo di installazione delle patch, migliorando la conformità alle normative e riducendo le spese.

In un mondo dove i secondi contano, Tivoli Endpoint Manager può essere la differenza tra una strategia di gestione patch corretta e una che mette l'organizzazione a rischio.

Ulteriori informazioni

Per ulteriori informazioni relative a IBM Tivoli Endpoint Manager, contattate il vostro rappresentante commerciale o Business Partner IBM, oppure visitare il sito: **ibm.com**/tivoli/endpoint

Informazioni sul software IBM Tivoli

Il software Tivoli fornito da IBM facilita una gestione efficiente ed efficace delle risorse, delle attività e dei processi IT, consentendo di soddisfare esigenze di business costantemente mutevoli, garantendo una gestione flessibile e dinamica dei servizi IT e contribuendo a ridurre i costi. Il portafoglio Tivoli comprende software per la gestione della sicurezza, della conformità, dello storage, delle prestazioni, della disponibilità, delle configurazioni, delle operazioni e del ciclo di vita dell'infrastruttura IT e si basa sui servizi, sul supporto e sulla ricerca all'avanguardia di IBM.

In aggiunta, le soluzioni di finanziamento di IBM Global Financing (IGF) consentono di gestire la liquidità in modo efficiente, di proteggersi dall'obsolescenza della tecnologia, di ridurre il TCO (Total Cost of Ownership) ed incrementare il ROI (Return On Investment). Inoltre, i nostri servizi GARS (Global Asset Recovery Services) consentono di rispondere ai requisiti ambientali con nuove soluzioni ad alto risparmio energetico. Per ulteriori informazioni su IGF, visitate il sito: **ibm.com**/financing/it

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

La home page di IBM Italia si trova all'indirizzo **ibm.com**

[1] http://cybersecureinstitute.org

TIW14065-ITIT-00