Sicurezza e Compliance degli endpoint distribuiti

IBM BigFix garantisce controllo e visibilità globali

In Evidenza

- Identificazione, gestione e report di difformità e anomalie rispetto alla policy grazie a strumenti di sicurezza e conformità basati su analytics
- Utilizzo di una singola infrastruttura e console per la gestione di tutti i dispositivi - smartphone, tablet, desktop, computer portatili e server
- Protezione in tempo reale per gli endpoint nei confronti di virus, Troyan horses, spyware, rootkit e altro malware
- Gestione automatica delle patch per sistemi operativi e applicazioni multipli
- Applicazione delle policy di sicurezza attraverso data loss prevention integrate e controllo dei dispositivi

Negli ambienti moderni, caratterizzati da una forte crescita di server, desktop, computer portatili, apparecchi mobili ed equipaggiamenti specializzati come le soluzioni point-of-sale (POS), ATM e i chioschi self-service — definiti complessivamente "endpoint"— gli schemi tradizionali di protezione quali firewall e soluzioni anti virus non sono più sufficienti. La rapida crescita del numero di lavoratori in remoto e di apparecchi mobili ridefinisce i confini da proteggere. Tali confini sono necessariamente gli endpoint stessi.

Gli endpoint sono, per le loro caratteristiche intrinseche, estremamente vulnerabili agli attacchi - compresi danni al sistema causati da malware, furti dovuti al phishing, violazioni della privacy nei social network o problemi di produttività in seguito a spam, interruzioni e instabilità del sistema. Le suddette vulnerabilità possono comportare un serio rischio inclusa la perdita di controllo sull'endpoint e la perdita di dati preziosi. Per ogni endpoint della vostra impresa la gravità del rischio varia continuamente.

La maggior parte dei problemi sono legati a endpoint che presentano lacune a livello di patch critiche o con errori di configurazione e che dunque sono scoperti al momento dell'attacco. Ad esempio gli attacchi epidemici con il virus Stuxnet hanno colpito vulnerabilità ben note legate all'uso di drive USB e della funzionalità di "autoplay" di Microsoft Windows quali vettori di attacco; entrambe le vulnerabilità avrebbero potuto essere eliminate con policy coerenti per configurazioni e aggiornamenti in tutta l'azienda.

I problemi di sicurezza tuttavia non vanno ricercati solo negli attacchi di per sé, ma anche nel modo in cui le imprese si proteggono. Le misure di protezione sono spesso costose e complesse e impegnano molte risorse con costi crescenti. Dopo l'implementazione delle misure di sicurezza, numerose imprese devono comprovare la conformità rispetto alle policy aziendali interne, standard di sicurezza e prescrizioni di legge. La "difformità dalla conformità" rappresenta un'ulteriore problema: le imprese devono inoltre garantire di mantenere nel tempo i livelli di conformità richiesti.

IBM BigFix, è in grado di soddisfare tutte queste esigenze, con soluzioni scalabili in base alle dimensioni aziendali. Fornisce visibilità in tempo reale e controllo dello stato di ogni singolo endpoint, correggendo i problemi per garantire sicurezza e conformità adeguate.

La sicurezza si basa su visibilità e controllo

Le organizzazioni possono avere poche centinaia o diverse centinaia di migliaia di endpoint da mettere in sicurezza per gestire efficacemente i rischi, contenere i costi e soddisfare i requisiti di conformità. Le sfide nel gestire diverse tecnologie consistono nel sapere quanti e quali tipi di endpoint si hanno, verificando e aggiornando patch e policy di sicurezza su tutti gli endpoint, e rispettando la conformità nei confronti di policy IT interne e esterne - con una velocità adeguata alla security posture dell'impresa.

Come reagire in un ambiente di grandi dimensioni e complesso, dove le minacce arrivano da diverse direzioni e gli endpoint individuali sono spesso attaccati? Come gestire migliaia di endpoint in movimento, talmente eterogenei da sembrare impossibili da gestire?

La risposta: utilizzare un unico tool che non solo indirizza i rischi legati alle minacce di sicurezza, ma controlla anche costi, complessità operativa e oneri del team IT, soddisfacendo le esigenze di conformità. La soluzione deve essere in grado di generare immediatamente report di conformità per tutta l'impresa, senza impegnare i sistemi per giorni o settimane per garantire la security posture. Le imprese hanno bisogno di una soluzione semplificata, snella, ad alta scalabilità che garantisca visibilità e controllo degli end point distribuiti.

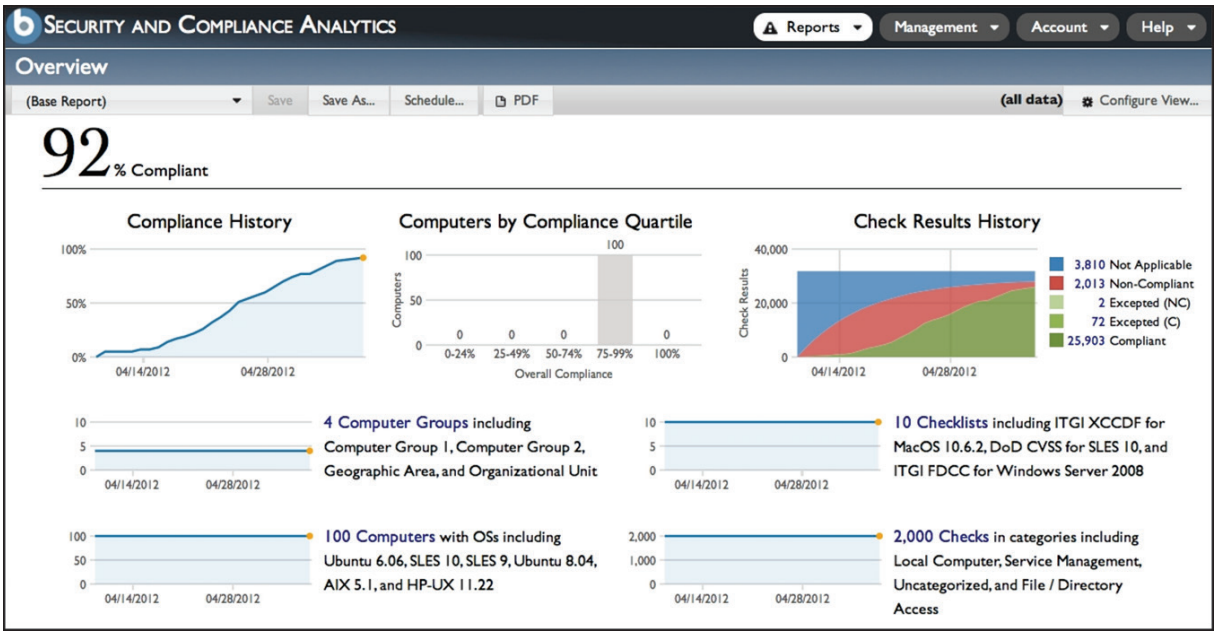
La soluzione ideale di gestione degli endpoint fornisce risorse intelligenti, rapide e automatizzate in grado di adeguarsi alle sfide poste dall'ambiente. Con la giusta soluzione è possibile controllare e proteggere tutti gli endpoint fisici e virtuali della propria impresa, vale a dire smartphone; tablet; PC fissi; portatili in roaming e connessi a Internet; server; point-of-sale (POS), ATM e chioschi self-service. L'ambiente è così protetto e sicuro, indipendentemente che si usi un sistema operativo Microsoft Windows, UNIX, Linux o Mac - o una combinazione degli stessi - utilizzando una sola console e la stessa infrastruttura di gestione.

IBM BigFix fornisce risultati rapidi

IBM BigFix agisce in poche ore o giorni, in base alla complessità dell'infrastruttura, per proteggere gli endpoint in tutta l'impresa. La soluzione univoca gestisce centinaia di migliaia di endpoint con una sola console e un solo server, reagendo rapidamente ai rischi di sicurezza e identificando e correggendo le vulnerabilità in tempo reale.

La soluzione identifica gli endpoint in rete dei quali non si conosce l'esistenza, compresi gli endpoint che non fanno parte della propria rete e altri endpoint non in gestione. L'agent intelligente della soluzione IBM BigFix agisce rapidamente e identifica le patch attuali e i livelli di configurazione, confrontandoli con le policy stabilite. Gli aggiornamenti di sistema operativo e applicazioni sono rapidi e precisi, indipendentemente dall'ubicazione dell'endpoint e dal tipo/stato della connessione, e garantiscono di continuo la conformità alla policy, anche se gli endpoint non sono collegati alla rete. Le capability di gestione della vulnerabilità identificano rapidamente le vulnerabilità, valutando e correggendo gli endpoint gestiti, grazie all'applicazione di policy predefinite.

L'agentt dell'IBM BigFix assicura il continuo rispetto delle policy di sicurezza, indipendentemente dalla connessione o meno dell'endpoint. Le soluzioni tradizionali di gestione degli endpoint utilizzano agent che dipendono completamente dalle istruzioni ricevute da un server centrale di comando e controllo. L'agent intelligente integrato nella soluzione IBM avvia autonomamente gli aggiornamenti e gli interventi di configurazione per mantenere la conformità degli endpoint rispetto alle policy aziendali, contenute nei messaggi IBM Fixlet® e scarica sull'endpoint le patch correlate, la configurazione o altri contenuti solo se necessario, controllando inoltre di continuo la conformità alla policy e inviando aggiornamenti di stato alla console di gestione in caso di modifiche. La console centrale è sempre aggiornata rispetto alla conformità attuale dell'endpoint, configurazione e stato di modifica, permettendo quindi report in tempo reale.



L'attività di reporting tramite console centrale fornisce visibilità in tempo reale sulla configurazione e lo stato di conformità, con vari formati di facile comprensione.

IBM BigFix risponde a molteplici esigenze di sicurezza

IBM BigFix fornisce le seguenti capabilities di sicurezza:

- **Supporto per gli standard di sicurezza**: supporta i benchmark di sicurezza CIS (Center for Internet Security), basati su consenso, e best practice di configurazione di sicurezza, entrambi sviluppati e omologati a livello legislativo, commerciale, industriale e accademico. Fornisce soluzioni best-pratice "out of the box" che implementano gli standard U.S. Federal Desktop Configuration Control (FDCC) e U.S. Government Configuration Baseline (USGCB). La soluzione IT è stata certificata dal National Institute of Standards and Technology (NIST) con il protocollo Secure Content Automation Protocol (SCAP) e dal 2008 viene utilizzata per gli scopi previsti presso le agenzie legislative. Il prodotto supporta anche checklist di sicurezza su piattaforme operative multiple, sfruttando i documenti SCAP, USGCB e la Security Technical Implementation Guide (STIG) della Defense Information Systems Agency (DISA). È in grado di elaborare i documenti di vulnerabilità e alert di sicurezza pubblicati da SANS Institute e nel National Vulnerability Database.
- **Gestione delle patch**: garantisce visibilità in tempo reale e applicazione e gestione delle patch su tutti gli endpoint tramite una sola console. Supporta Microsoft, UNIX, Linux e Mac OS, e applicazioni quali Adobe, Mozilla, Apple e Java. Riduce i cicli delle patch a pochi minuti o ore, con una percentuale di successo fino al 99% al primo passaggio.
- **Gestione della configurazione di sicurezza**: fornisce un'ampia libreria di controlli tecnici che permettono di ottenere la conformità alla sicurezza individuando e applicando le configurazioni di sicurezza. Le librerie di policy consentono un'applicazione continua delle baseline di configurazione; report, correzioni e conferma della correzione degli endpoint non conformi in tempo reale; assicura una vista controllata in tempo reale di tutti gli endpoint.
- **Gestione della vulnerabilità**: valuta gli endpoint in base a definizioni della vulnerabilità per la sicurezza basate sullo standard OVAL (Open Vulnerability and Assessment Language) ed esegue report sulla mancata conformità in tempo reale, per facilitare l'eliminazione di vulnerabilità note negli endpoint.
- **Strumenti di analisi per sicurezza e conformità**: offre strumenti di analytics per controlli e reporting al fine di soddisfare i requisiti di conformità e gli obiettivi di sicurezza IT, compresa la determinazione del progresso e gli andamenti cronologici della conformità della configurazione di sicurezza alla policy; permette di individuare rapidamente esposizioni e rischi, offre report dettagliati sulla conformità alla policy della configurazione di sicurezza; identifica, gestisce ed esegue report sulle difformità rispetto alla policy.
- **Sicurezza dei dispositivi mobili**: protegge e gestisce i dispositivi mobili, compresi i dispositivi Apple iOS, Android, Symbian e Microsoft Windows Phone. Salvaguarda i dati cancellando selettivamente i dati in casi di perdita o furto del dispositivo, configurando e sfruttando policy con password, soluzioni di crittografia, reti virtuali private (VPN) e molto altro. Assicura la conformità identificando automaticamente i dispositivi non conformi e intervenendo negando l'accesso alle email o inviando notifiche agli utenti fino a che non siano state implementate le misure correttive.
- **Gestione della protezione endpoint di vari fornitori**: fornisce uno strumento di controllo centrale e unico per la gestione di prodotti anti virus e firewall di vari fornitori, compresi Computer Associates, McAfee, Sophos, Symantec, Microsoft e Trend Micro, permettendo alle imprese di migliorare scalabilità, velocità e precisione delle soluzioni di protezione. Oltre a garantire che i client di sicurezza degli endpoint siano sempre in funzione e che le soluzioni signature per i virus siano aggiornate, facilita la migrazione degli endpoint tra le diverse soluzioni, permettendo di disattivare e reinstallare il software con un semplice clic.

- **Quarantena automatica in rete**: valuta automaticamente gli endpoint in base alle configurazioni di conformità richieste - e se un endpoint non risulta conforme, la soluzione IT lo configura in modo che risulti in quarantena in rete fino all'effettiva conformità. Il server IBM BigFix è dotato di accesso di gestione, mentre tutti gli altri accessi sono disabilitati.
- **Firewall endpoint**: permette agli amministratori di applicare le policy basandosi sull'ubicazione dell'endpoint, di controllare il traffico di rete in base agli indirizzi IP sorgente e di destinazione, di regolare le comunicazioni in ingresso e uscita degli endpoint e mettere in quarantena gli endpoint se necessario.
- **Asset discovery**: crea una visibilità dinamica relativa ai cambiamenti dell'infrastruttura, compresa una rapida identificazione degli apparecchi in rete non gestiti per favorire ulteriori ricerche o per supportare le installazioni di un agent automatico e riportare così rapidamente sotto controllo gli endpoint.
- **Protezione eccellente contro malware**: protegge da un ampio spettro di malware e controlla i protocolli POP3 email e le cartelle Microsoft Outlook per individuare possibili minacce. Elimina automaticamente dagli endpoint malware, rootkit, spyware elaborando e registrando elementi nascosti o bloccati.
- **Data Loss Prevention**: mette a disposizione una soluzione integrata per consentire alle policy di sicurezza di abilitare gli utenti ad accedere a dati sensibili per lavorare, senza poter perdere o utilizzare non conformemente tali dati, e di sfruttare modelli predefiniti che facilitano il rispetto delle prescrizioni sulla data privacy.
- **Granular device control**: monitora e controlla le porte fisiche sugli endpoint, e può abilitarle o disabilitarle in base al tipo di dispositivo e alle limitazioni di scansione legate al contenuto. Sono disponibili protezioni accessorie per limitare l'accesso a supporti USB.
- **File reputation**: effettua query fino al secondo livello di dati in un database basato sul cloud per stabilire la sicurezza di un file e impedire che gli utenti aprano documenti infetti.
- **Web reputation**: stabilisce automaticamente la sicurezza di milioni di siti dinamici per proteggere gli endpoint da malware basati sul Web, furti di dati, perdite di produttività e reputazione.

Una soluzione univoca è la chiave per gestire con successo gli endpoint

IBM BigFix è in grado di ridurre efficacemente le esposizioni di sicurezza applicando le modifiche rapidamente e con precisione in tutta l'infrastruttura. Elimina il problema di utilizzare vari tools di gestione, che rendono difficile o impossibile controllo e visibilità globale, fornendo invece un'infrastruttura unica di gestione che mette efficacemente in sinergia operazioni IT e di sicurezza su desktop, dispositivi mobili e server, eseguendo le modifiche necessarie, individuando i problemi e rispondendo alle esigenze interne di conformità anche con attività di reporting.

IBM BigFix aiuta a ridurre i rischi per la sicurezza, i costi e la complessità di gestione, aumentando invece velocità e precisione delle correzioni, migliorando produttività e livello di soddisfazione degli utenti. L'agent singolo, la console unica e un solo server di gestione consentono di ottenere processi snelli più affidabili. La soluzione fornisce funzioni come gestione di patch e asset discovery con ROI a lungo termine, aumentando l'efficacia operativa, permettendo un consolidamento dell'infrastruttura gestionale e migliorando la produttività IT.

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**/security/bigfix

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

Si prega di riciclare

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.

WGS03060-ITIT-00