IBM Tivoli Endpoint Manager for Security and Compliance

Un'unica soluzione per la gestione della sicurezza degli endpoint all'interno dell'intera organizzazione aziendale

Punti principali

- Visibilità e controllo in tempo reale tramite un'unica console di gestione.
- Un unico agente multifunzionale e intelligente che valuta e risolve i problemi, contribuendo a garantire una sicurezza e una conformità costanti.
- Capacità di gestire centinaia di migliaia di endpoint, fisici e virtuali, indipendentemente dall'ubicazione e dal tipo o stato di connessione.
- Identificazione, gestione e notifica sulle eccezioni e deviazioni della politica con le analisi sulla conformità e sicurezza.
- Gestione automatica delle patch per più sistemi operativi e applicazioni.

Con la crescita estremamente rapida sia del numero di endpoint che delle minacce atte a comprometterne la sicurezza, IBM Tivoli Endpoint Manager for Security and Compliance offre ai clienti una visibilità in tempo reale unificata e la protezione dell'ambiente complesso e altamente distribuito.

Progettato per garantire la sicurezza degli endpoint all'interno dell'intera organizzazione aziendale, Tivoli Endpoint Manager for Security and Compliance consente alla vostra organizzazione sia di proteggere gli endpoint che di dimostrare alle autorità di controllo l'aderenza agli standard di sicurezza previsti dalla normativa vigente. Una soluzione facile da gestire e rapida da implementare, che supporta la sicurezza in un ambiente costituito da una grande varietà e quantità di endpoint: server, PC desktop, laptop connessi ad Internet "in roaming", smart phone e altri dispositivi mobili, come anche apparecchiature destinate ad usi specifici, come dispositivi POS (Point-Of-Sales), ATM e chioschi self-service.

Tivoli Endpoint Manager for Security and Compliance consente di ridurre i costi e la complessità della gestione IT, aumentando l'agilità operativa, la rapidità dei rimedi e la precisione delle operazioni. L'impatto minimo sull'operatività degli endpoint permette di incrementare la produttività ed offrire agli utenti un'esperienza più soddisfacente. Assicurando costantemente l'adozione di politiche di sicurezza conformi alle normative vigenti, Tivoli Endpoint Manager for Security and Compliance contribuisce a ridurre il rischio ed aumentare la visibilità di verifica. La velocità e l'efficienza di un agent intelligente permettono la conformità di cicli automatici di verifica calcolati in minuti invece che in settimane.

Gestire le esigenze di sicurezza all'interno dell'intera organizzazione aziendale

Tivoli Endpoint Manager for Security and Compliance risponde ai problemi di sicurezza associati agli ambienti desktop, mobili e distribuiti. Offrendo funzionalità per la gestione e la sicurezza degli endpoint in un'unica soluzione, questo prodotto contribuisce ad assicurare una protezione e una conformità continua. Ad esempio, consente di ridurre drasticamente il divario tra le condizioni di sicurezza esistenti e quelle ottimali, applicando le patch software in pochi minuti. E permette di diminuire il divario tra le varie funzioni come quelle che definiscono ed attuano strategie e politiche, quelle che gestiscono i dispositivi in tempo reale e quelle che generano report sui problemi di sicurezza e conformità.

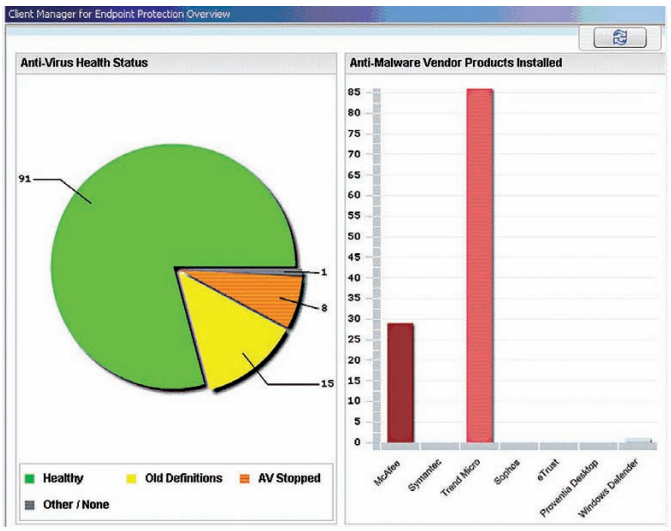
Le funzionalità di Tivoli Endpoint Manager for Security and Compliance offrono:

- Visibilità accurata ed estremamente aggiornata e applicazione continua delle configurazioni e delle patch di sicurezza.
- Gestione centralizzata di prodotti anti-malware e firewall di terze parti.
- Best practice immediatamente utilizzabili, conformi alle regole stabilite nello U.S. FDCC (Federal Desktop Configuration Control) e alle metodologie definite nelle STIG (Security Technical Implementation Guide) della DISA (Defence Information Systems Agency).
- Supporto del protocollo SCAP (Security Content Automation Protocol); Tivoli Endpoint Manager è il primo prodotto certificato dal NIST (National Institute of Standards and Technology) sia per la valutazione che per la risoluzione dei problemi di sicurezza.
- Trasmissione sicura delle istruzioni tra gli endpoint, come dimostrato dalle certificazioni NIAP CCEVS EAL3 e FIPS 140-2, Livello 2.
- Supporto dello standard OVAL (Open Vulnerability and Assessment Language), per promuovere la libera diffusione di informazioni sulla sicurezza pubblicamente disponibili.
- Capacità di ricevere e intervenire in base ad avvisi sulle vulnerabilità e sui rischi per la sicurezza, pubblicati dal SANS Institute.
- Visualizzazione dell'andamento e analisi delle modifiche apportate alla configurazione di sicurezza attraverso un reporting analitico di sicurezza e conformità avanzato.
- Utilizzare soluzioni analitiche per migliorare le proprie conoscenze e di reporting per rispettare obiettivi in materia di conformità e sicurezza IT compresa la determinazione di progressi e andamenti cronologici per il continuo rispetto delle disposizioni in termini di configurazione della sicurezza, la rapida identificazione di rischi ed esposizioni della sicurezza a cui sono esposti gli endpoint, la facile creazione e condivisione di report di riepilogo e dettagliati sul rispetto delle disposizioni in termini di configurazione della sicurezza, nonché l'identificazione, la gestione e il reporting di eccezioni e di deviazioni dalle politiche.

Le funzionalità aggiuntive disponibili per tutti i prodotti della famiglia Tivoli Endpoint Manager, basati sulla tecnologia Bigfix, consentono di:

- Rilevare e identificare endpoint, della cui esistenza le organizzazioni possono non essere consapevoli: fino al 30 per cento in più, in alcuni casi.
- Utilizzare un'unica console per le funzioni di gestione, configurazione, rilevamento e sicurezza, semplificando le operazioni.
- Eseguire azioni mirate a un tipo specifico di configurazione degli endpoint o di utente, utilizzando qualsiasi prodotto hardware o software.
- Utilizzare un'infrastruttura di gestione unificata, per coordinare le operazioni IT, di sicurezza, sui desktop e sui server.
- Raggiungere gli endpoint, indipendentemente dall'ubicazione e dal tipo o stato di connessione, con un ampio supporto per tutti i principali sistemi operativi, applicazioni di terze parti e patch basate su linee guida.

Tivoli Endpoint Manager for Security and Compliance consente di eseguire processi automatizzati e altamente mirati, che garantiscono il controllo, la visibilità e la rapidità per effettuare modifiche e documentare la conformità dell'ambiente endpoint agli standard di sicurezza previsti dalla normativa vigente. I cicli di correzione sono brevi e rapidi, e i problemi associati a malware e virus vengono affrontati con una gestione rapida delle patch.



Tivoli Endpoint Manager for Security and Compliance consente di creare e distribuire report che aiutano le organizzazioni a visualizzare i problemi che incidono negativamente sull'efficacia delle iniziativa mirate a garantire la sicurezza e la conformità dell'ambiente endpoint.

Un'ampia serie di potenti funzioni di sicurezza

Tivoli Endpoint Manager for Security and Compliance include le seguenti funzioni principali e vi offre la possibilità di aggiungere facilmente altre funzioni in base alle vostre specifiche esigenze, senza aumentare i costi dell'infrastruttura o di implementazione.

Gestione delle patch

La gestione delle patch comprende un'ampia serie di funzionalità che consente di installare patch per sistemi operativi Microsoft® Windows®, UNIX®, Linux® e Mac e per molte applicazioni di terze parti, come Adobe, Mozilla, Apple e Java™, su endpoint distribuiti, indipendentemente dall'ubicazione e dal tipo o stato di connessione. Un singolo server di gestione è in grado di supportare fino a 250.000 endpoint, riducendo i tempi di implementazione delle patch senza compromettere la funzionalità degli endpoint, anche su reti con poca larghezza di banda o globalmente distribuite. La reportistica in tempo reale consente di acquisire informazioni su quali patch siano state installate, dove siano siano state installate e chi le abbia installate, nonché di confermare in modo automatico l'avvenuta applicazione delle patch, offrendo una soluzione completa per il relativo processo di gestione.

Gestione delle configurazioni di sicurezza

Certificate dal NIST, le funzionalità offerte da questa soluzione per la gestione delle configurazioni di sicurezza forniscono un'ampia libreria di controlli tecnici che facilitano l'osservanza dei requisiti di sicurezza prescritti dalla normativa vigente, rilevando le configurazioni di sicurezza e assicurandone l'applicazione. Le librerie di politiche di sicurezza supportano l'applicazione costante della configurazione di riferimento; documentano, eseguono e confermano in tempo reale la correzione delle configurazioni sugli endpoint non conformi e assicurano una visione certa e in tempo reale di tutti gli endpoint.

Questa funzionalità fornisce informazioni importanti sul funzionamento e sulla sicurezza degli endpoint, indipendentemente dall'ubicazione, dal sistema operativo, dalla connessione (che si tratti di computer connessi via cavo o di dispositivi mobili connessi in modo intermittente) e dalle applicazioni installate. Contribuisce a consolidare e unificare il ciclo di vita della conformità, riducendo il tempo necessario per definire e correggere le configurazioni degli endpoint.

Gestione delle vulnerabilità

La gestione delle vulnerabilità consente di rilevare, valutare e correggere le vulnerabilità prima che gli endpoint vengano compromessi. Grazie a questa funzionalità, è possibile verificare la presenza di eventuali vulnerabilità nei sistemi utilizzando le definizioni OVAL (open source security language) e documentare le regole non conformi agli standard di sicurezza in tempo reale. Ciò consente una maggiore visibilità e una completa integrazione in ciascuna delle fasi di identificazione, analisi e correzione che compongono il processo.

Il personale IT può identificare ed eliminare le vulnerabilità note esistenti su tutti gli endpoint, eseguendo azioni automatizzate o manuali. Utilizzando un unico tool sia per rilevare che per correggere le vulnerabilità, gli amministratori sono in grado di operare con maggiore rapidità e precisione, riducendo il tempo necessario per installare le patch, aggiornare il software e rimediare alle vulnerabilità. Gli amministratori possono impostare allarmi per identificare rapidamente i sistemi pericolosi e adottare le misure necessarie per localizzarli, allo scopo di correggere le vulnerabilità riscontrate o rimuoverli. Gli amministratori possono estendere la gestione della sicurezza ai clienti mobili connessi o meno alla rete.

Rilevamento dei dispositivi

Con Tivoli Endpoint Manager for Security and Compliance, il rilevamento dei dispositivi non è più una raccolta di informazioni statiche. Questo prodotto consente di rilevare dinamicamente le modifiche che si verificano nell'infrastruttura. La possibilità di scansionare frequentemente l'intera rete aumenta notevolmente la visibilità e il controllo, contribuendo ad assicurare che le organizzazioni individuino rapidamente, con un impatto minimo sulla rete, non solo gli endpoint, ma tutti i dispositivi identificabili tramite un indirizzo IP, comprese le macchine virtuali (VM), i dispositivi di rete e le periferiche, come stampanti, scanner, router e switch. Questa funzione contribuisce a garantire una visibilità costante di tutti gli endpoint esistenti nell'organizzazione, compresi i laptop e i notebook mobili ubicati all'esterno della rete aziendale.

Gestione di soluzioni multivendor per la protezione degli endpoint

Questa funzionalità consente agli amministratori di gestire da un unico punto di controllo le applicazioni di terze parti per la sicurezza degli endpoint, fornite da aziende come Computer Associates, McAfee, Sophos, Symantec e Trend Micro. Grazie a questa gestione centralizzata, le organizzazioni sono in grado di aumentare la scalabilità, la rapidità e l'affidabilità delle soluzioni di protezione. I sistemi vengono monitorati per assicurare che i client per la sicurezza degli endpoint siano sempre funzionanti e le firme dei virus siano aggiornate. Oltre a fornire una visione unitaria di tecnologie eterogenee, questa funzionalità facilita la migrazione da una soluzione di protezione ad un'altra sui singoli endpoint, grazie alla possibilità di rimuovere e reinstallare software con un semplice clic. La verifica "a circuito chiuso" assicura che gli aggiornamenti e le altre modifiche vengano completati, potendo essere eseguita tramite Internet anche sugli endpoint disconnessi dalla rete aziendale.

Quarantena automatica della rete

Tivoli Endpoint Manager for Security and Compliance verifica automaticamente che le configurazioni degli endpoint siano conformi agli standard di sicurezza e, in caso di difformità, consente di isolare gli endpoint dalla rete fino a quando tale conformità non venga ottenuta nuovamente. Tivoli Endpoint Manager mantiene l'accesso all'endpoint, ma non degli altri tipi di accesso che vengono disabilitati.

La linea di prodotti IBM Tivoli per la gestione degli endpoint

Questi prodotti consentono di consolidare ulteriormente gli strumenti utilizzati, diminuire il numero degli agenti e ridurre i costi di gestione estendendo l'investimento in Tivoli Endpoint Manager for Security and Compliance ad altri componenti della famiglia Tivoli Endpoint Management. Poiché tutte le funzioni vengono gestite utilizzando la stessa console, un unico server ed il medesimo agente endpoint, l'aggiunta di nuovi servizi richiede semplicemente la modifica della chiave di licenza.

- **Tivoli Endpoint Manager for Core Protection** – offre funzionalità anti-malware e firewall personali integrati per proteggere endpoint fisici e virtuali attraverso l'interrogazione in tempo reale di informazioni sulle minacce raccolte in ambiente cloud computing per eliminare quasi completamente la necessità della presenza sugli endpoint di file contenenti le firme del codice malevolo.
- **Tivoli Endpoint Manager for Power Management** – permette di assicurare l'applicazione delle politiche di risparmio energetico nell'organizzazione, con la granularità necessaria per consentire l'applicazione delle politiche in un singolo computer.
- **Tivoli Endpoint Manager for Lifecycle Management** – soddisfa l'attuale esigenza di convergenza IT consentendo di conoscere in tempo reale lo stato di funzionamento degli endpoint, offrendo agli amministratori funzionalità avanzate per la gestione degli stessi.
- **Tivoli Endpoint Manager for Software Use Analysis** – consente di rilevare e analizzare le applicazioni installate su desktop, laptop e server. È possibile acquisire informazioni progressivamente più dettagliate su chi ha pubblicato il software, i titoli e gli applicativi, fino a individuarne il livello di versione, includendo anche dati statistici aggregati sull'utilizzo.

Tivoli Endpoint Manager: soluzioni basate sulla tecnologia BigFix

L'elemento che rende tutti i prodotti Tivoli Endpoint Manager estremamente funzionali consiste in un approccio peculiare, basato su un'unica infrastruttura che consente di applicare politiche uniformi su tutti gli endpoint da gestire, rendendo l'intera linea di soluzioni estremamente vantaggiosa, grazie a caratteristiche che includono:

- **Un agente intelligente**: le soluzioni Tivoli Endpoint Manager utilizzano un approccio all'avanguardia che colloca un agente intelligente su ogni endpoint. Questo agente svolge più funzioni, tra cui autovalutazione e applicazione delle policy, con un impatto minimo sulle prestazioni del sistema. A differenza delle architetture client-server tradizionali, che richiedono l'invio di istruzioni da un punto di controllo centrale, questo agente inizializza le attività in modo intelligente, inviando messaggi al server centrale di gestione ed estraendo le patch, le configurazioni e le altre informazioni necessari per rendere conforme l'endpoint alla politica da applicare. 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.
- **Reportistica**: la singola console unificata, integrata nelle soluzioni Tivoli Endpoint Manager, coordina le attività eseguite sui singoli endpoint, consentendo di raggiungere un alto livello di visibilità, che include la documentazione e l'analisi continue eseguite in tempo reale dagli agenti attivi sugli endpoint dell'organizzazione.
- **Funzionalità di trasmissione**: l'architettura scalabile e leggera delle soluzioni Tivoli Endpoint Manager consente di configurare qualsiasi agente come un relay per gestire lo scambio di informazioni tra gli altri agenti e la console. Questa funzione consente l'utilizzo dei server e delle workstation esistenti per trasferire i pacchetti di dati tra i vari nodi della rete, riducendo la necessità di nuovi server.
- **Messaggi IBM Fixlet**: Fixlet Relevance Language è un linguaggio comandi di pubblico dominio che consente a clienti, business partner e sviluppatori di creare politiche e servizi personalizzati per gli endpoint gestiti attraverso le soluzioni Tivoli Endpoint Manager.

Soluzioni Tivoli più attente alla sicurezza

Tivoli Endpoint Manager for Security and Compliance rientra nell'ampio portafoglio di soluzioni IBM per la sicurezza, semplificando la gestione dei problemi di sicurezza all'interno dell'intera organizzazione aziendale. Supportando le operazioni IT complesse, interconnesse e intelligenti necessarie per realizzare un pianeta più intelligente, le soluzioni di sicurezza garantiscono visibilità in tempo reale, controllo centralizzato e maggiore sicurezza dell'intera infrastruttura IT, compresi gli endpoint globalmente distribuiti che ne fanno parte.

La linea di prodotti Tivoli Endpoint Manager in sintesi

Requisiti server:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Requisiti console:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Piattaforme supportate per l'agente:

- Microsoft Windows, compresi XP, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded e Embedded POS
- Mac OS X
- Solaris
- IBM AIX
- Linux su IBM System z
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Oracle Enterprise Linux
- CentOS Linux
- Debian Linux
- Ubuntu Linux

Ulteriori informazioni

Per ulteriori informazioni su IBM Tivoli Endpoint Manager for Security and Compliance, contattare il vostro rappresentante commerciale o Business Partner IBM oppure visitate 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.

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

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

Tivoli software

TID14075-ITIT-02