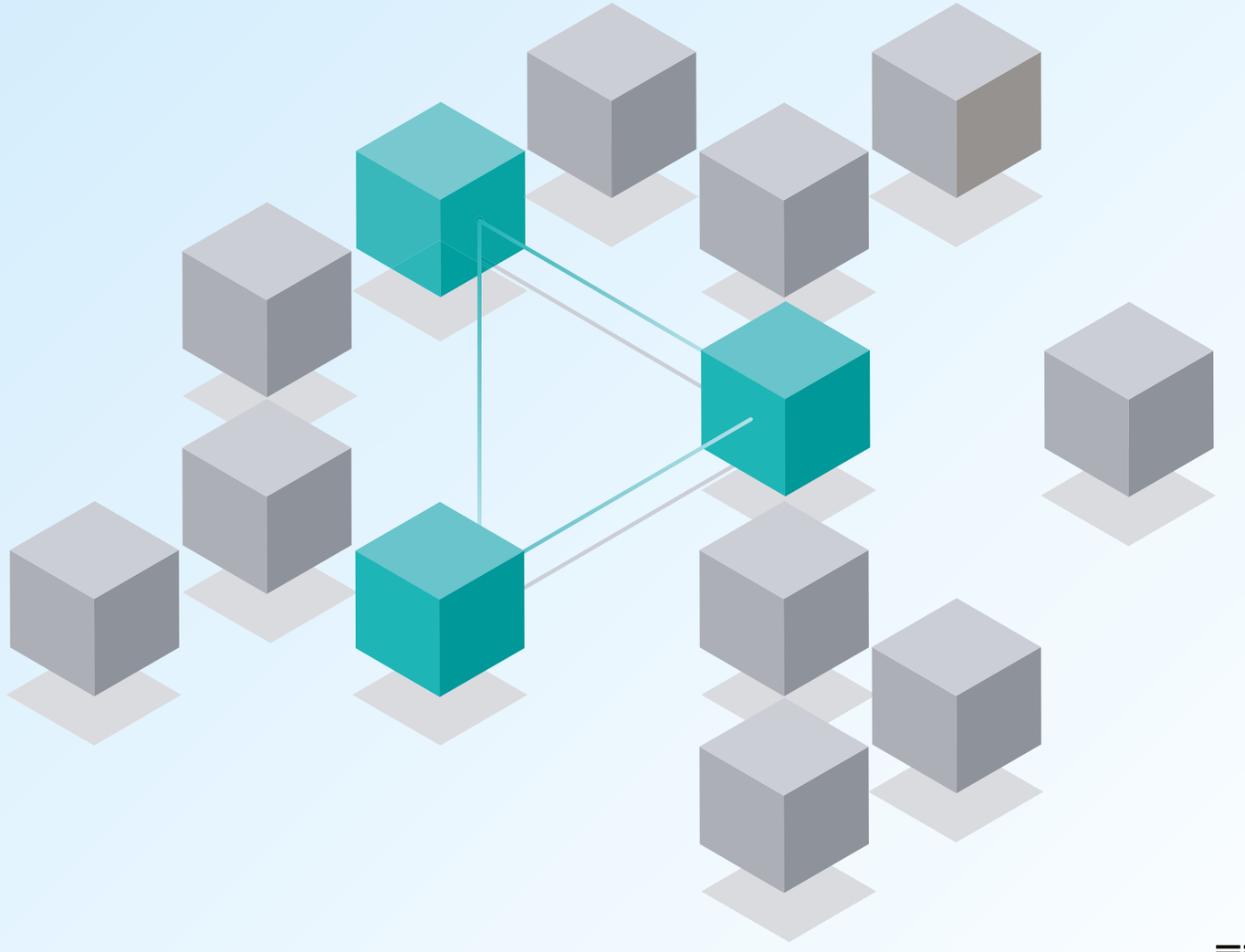
Guida EDR per l'acquirente

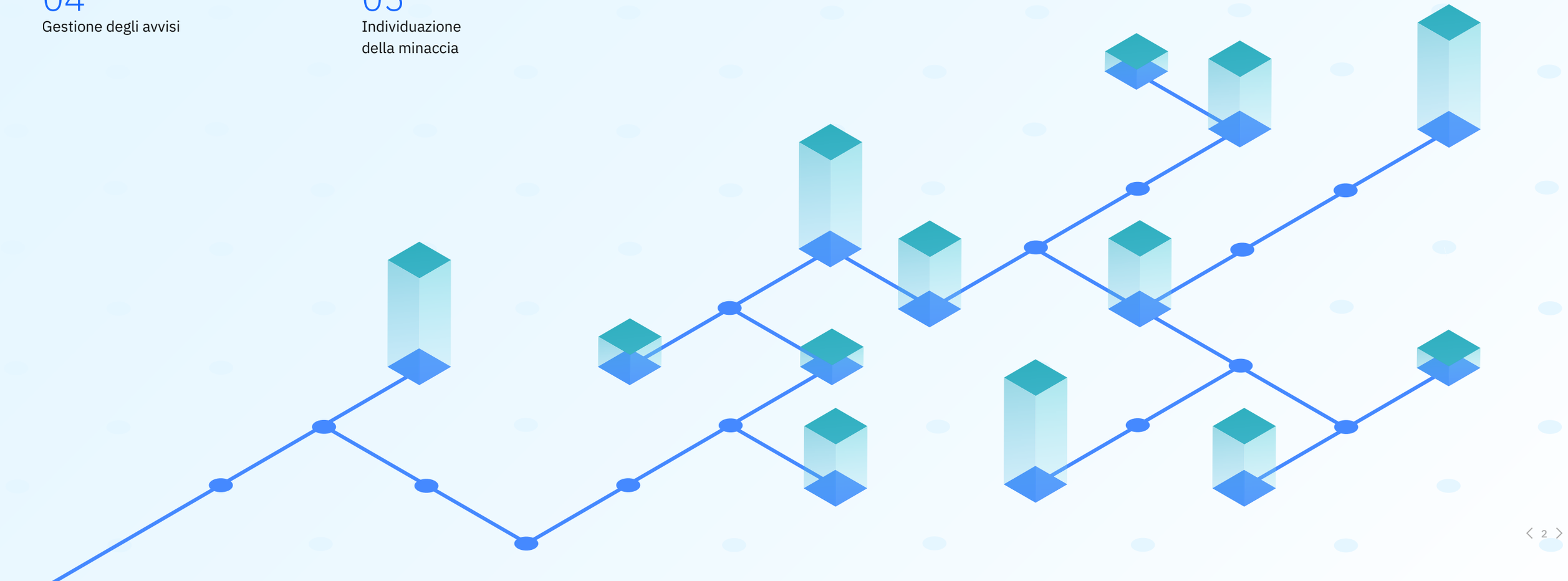
Come scegliere la migliore soluzione di rilevamento e risposta degli endpoint per la tua azienda



REAQTA
an IBM Company

IBM

Sommario



01
Introduzione

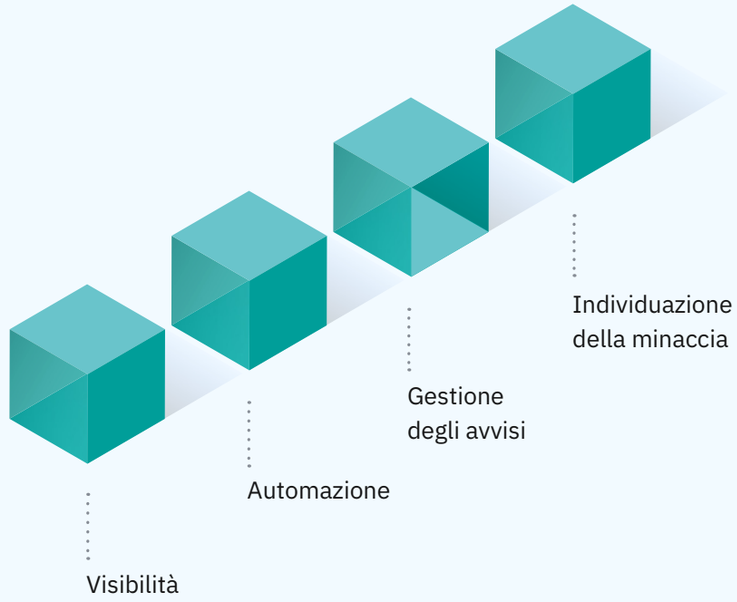
Che cos'è un sistema di EDR e a cosa serve?
Negli ultimi anni stiamo assistendo a una crescente proliferazione e interconnettività di endpoint e dati, di pari passo con l'aumento di attività minacciose da parte di malintenzionati. Queste circostanze hanno determinato una considerevole minaccia alla continuità operativa di piccole e grandi imprese. Sempre più aziende sono vittime di attacchi da parte di criminali informatici e nation state actor.

I tradizionali metodi di protezione combattono le minacce già note, ma sono vulnerabili di fronte a tecniche di attacco sofisticate e sconosciute, e non forniscono visibilità degli asset, il che costituisce uno degli ostacoli principali alla messa in sicurezza dei sistemi. Generalmente, solo le aziende più grandi, o quelle con maggiori disponibilità economiche, possono giovarsi delle competenze di esperti nella protezione degli endpoint. Insieme al fatto che oggi molti attacchi avvengono alla velocità di macchinari con molte componenti mobili, ciò ha portato a una situazione a cui i team composti da persone, che ancora fanno affidamento sulle tradizionali soluzioni per la protezione degli endpoint, non riescono a tener fronte.

Una soluzione per il rilevamento e la risposta degli endpoint (EDR) blocca e isola proattivamente e automaticamente i malware, e allo stesso tempo fornisce ai team della sicurezza gli strumenti adatti ad affrontare questi problemi in modo sicuro. Un EDR moderno può assicurare la continuità operativa limitando con efficacia le crescenti minacce automatizzate, sempre più avanzate, come ransomware o attacchi fileless, senza pesare sul carico di lavoro degli analisti, o richiedere specialisti della sicurezza altamente qualificati.

Devi affrontare uno dei seguenti problemi?
- Fallimento delle soluzioni già adottate
- Visibilità ridotta
- Carenza di personale qualificato
- Alert fatigue (stress da eccesso di avvisi di sicurezza)
- Minacce latenti

Un EDR moderno ed efficace comprende quattro elementi chiave che esamineremo nei prossimi capitoli:



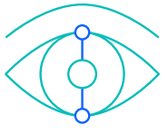
02
Visibilità completa dell’endpoint

Uno degli ostacoli principali alla messa in sicurezza degli endpoint è costituito dalla carenza di visibilità. Una moderna soluzione EDR, in quanto tale, deve fornire una visibilità completa e approfondita all’interno di applicazioni e processi in esecuzione.

Quando viene visualizzata una minaccia, man mano che l’attacco procede devono essere automaticamente creati degli avvisi in tempo reale sul suo comportamento, con una traccia grafica che includa la mappatura MITRE ATT&CK in modo da offrire agli analisti piena visibilità e comprensione di ciò che sta accadendo.

La maggior parte dei software per la sicurezza degli endpoint, se non tutti, operano all’interno del sistema operativo, il che determina un limite per l’agente endpoint. Ciò, infatti, riduce le possibilità e la visibilità dell’agente, mentre si registra un maggiore consumo delle risorse del computer. Avere un agente che opera a livello di hypervisor, ed è progettato per non essere rilevabile, non solo riduce al minimo l’utilizzo delle risorse, ma offre anche un’eccezionale visibilità in grado di monitorare tutti i comportamenti dei processi rimanendo invisibile agli aggressori.

Cosa cercare:
- Visibilità dell’endpoint completa
- Avviso in tempo reale
- Tracciamento
- Agenti liberi
- Workflow unificato



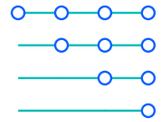
Domande:

→ La tua soluzione fornisce una visibilità completa e approfondita all’interno delle applicazioni e dei processi in esecuzione?

→ Durante un attacco, in che modo la tua soluzione fornisce informazioni importanti e in tempo reale per comprendere meglio la minaccia?

→ Oltre a individuare una violazione e avvisarti, il tuo MSSP fornisce anche una risposta end-to-end e un rimedio?

03
Automazione e facilità d’uso



Con il previsto aumento di minacce e superfici di attacco sofisticate, nel 2022 e negli anni successivi molte aziende subiranno la pressione di dover fronteggiare la criminalità informatica. Un EDR moderno dovrebbe alleggerire il crescente carico di lavoro attraverso l’automazione intelligente e, allo stesso tempo, essere facile da usare in modo da contenere il bisogno di specialisti altamente qualificati.

Per ottenere velocemente valore da un EDR, gli acquirenti devono puntare ad automazione e semplificazione. Grazie all’automazione dell’algoritmo, gran parte del lavoro è lasciata agli algoritmi, riducendo al minimo l’interazione umana. Attraverso tali algoritmi, il software diventa più facile da usare e i team possono essere operativi rapidamente, senza bisogno di lunghe abilitazioni.

In caso di attacco, i tempi di reazione sono fondamentali: il tempo di individuazione delle minacce avanzate dovrebbe rimanere ben al di sotto del minuto, in modo da eliminarle prima che possano provocare danni all’infrastruttura.

Gli acquirenti devono puntare a un EDR capace di funzionare in maniera autonoma e offrire rilevamento automatizzato e capacità di reazione. Ciò fornisce agli analisti una panoramica chiara e in tempo reale di un attacco man mano che si evolve e può suggerire un intervento guidato per tornare rapidamente alla normalità.

Cosa cercare:
- Rilevazione autonoma
- Intervento guidato
- Analitica degli agenti
- Tempi rapidi di reazione
- Facilità d’uso

Domande:

→ Sono richieste competenze avanzate per utilizzare l’EDR?

→ L’EDR è in grado di funzionare autonomamente, in modo da ridurre il carico di lavoro degli analisti?

→ Per quanto concerne i tempi di reazione, le minacce vengono analizzate nel cloud o a livello di agente?

→ Se le minacce vengono analizzate nel cloud, cosa succede se manca la connessione a internet?

04
Gestione avvisi

La principale differenza tra un EDR e un antivirus (AV) tradizionale è che, per quanto riguarda il rilevamento, un AV fa affidamento sulle firme disponibili e deve essere a conoscenza della minaccia per bloccarla. Dall'altra parte, un EDR utilizza un approccio comportamentale per individuare malware e altre potenziali minacce a seconda di come queste si comportano in un endpoint. Inoltre, a differenza di un AV, un EDR è per sua natura leggero e non richiede aggiornamenti frequenti.

Quindi, l'algoritmo utilizzato in un EDR moderno deve essere in grado di individuare rapidamente il pericolo, con grande precisione e alta fedeltà, in modo da mantenere il volume degli avvisi, e il carico di lavoro degli analisti, a un livello minimo. Gli acquirenti dovrebbero cercare informazioni sul tipo di algoritmo e sulle tecniche di apprendimento automatico utilizzati. In confronto agli algoritmi, che per il rilevamento fanno affidamento su analisi e modelli predisposti, un EDR che utilizza un modello iniziale di apprendimento per identificare il normale comportamento di ciascun endpoint consente una maggiore precisione in fase di rilevamento e avvisa in caso di discrepanze rispetto alla normalità.

Per ridurre i tempi di reazione e lo stress da avvisi degli analisti, un moderno EDR deve essere dotato di un solido sistema di gestione degli avvisi, guidato da algoritmi, capace di imparare dall'analista per poi applicarne autonomamente il processo decisionale nella gestione quotidiana degli avvisi stessi. Disporre di un sistema di gestione degli avvisi completamente automatizzato e guidato da algoritmi è fondamentale per affrontare lo stress da avvisi, ridurre il caos tra il personale e tornare a tenere la situazione sotto controllo.

Cosa cercare:
- Alta fedeltà degli avvisi
- Uso di modelli AI
- Prevenzione dello stress da avvisi
- Gestione degli avvisi automatizzaata

Domande:

→ Il tuo sistema fornisce un metodo di gestione e chiusura automatica degli avvisi?

→ In che modo la tua soluzione fa risparmiare tempo agli analisti?

→ In che modo la tua soluzione riduce i falsi positivi?

→ Se un dipendente lascia l'azienda, come verrà mantenuta la sua conoscenza dell'infrastruttura?

05
Individuazione della minaccia

L'individuazione della minaccia è un aspetto fondamentale per una soluzione EDR moderna ed è necessaria per preservare un ambiente ordinato e sgombro da minacce. L'individuazione della minaccia è in grado di rilevare rapidamente l'ingresso nell'ambiente di nuove minacce e di identificare i punti deboli. Il mining dei dati consente di cercare ed eliminare le minacce latenti che altrimenti potrebbero passare inosservate ma che potrebbero risiedere in un ambiente per mesi o addirittura anni, in attesa di essere utilizzate da un utente malintenzionato.

Per loro natura, le minacce in memoria e fileless sono difficili da tracciare e ancora più difficili da seguire quando chi attacca utilizza diverse varianti mentre si muove all'interno di una grande infrastruttura. Un EDR moderno deve automatizzare l'attività di individuazione e utilizzare il mining dei dati per permettere ai team sicurezza di cercare automaticamente le minacce che presentano similitudini con altri casi a livello comportamentale e funzionale, in modo da ottenere risultati in pochi secondi.

Nell'individuazione della minaccia la flessibilità è molto importante. Gli acquirenti non dovrebbero limitarsi a cercare un EDR che offra soltanto una grande libreria di playbook di rilevamento precostituiti da impiegare out-of-the-box, ma anche playbook personalizzati facili da creare, anche senza conoscenze di programmazione, per gli specifici scenari che possono caratterizzare le esigenze di sicurezza di un'azienda.

L'individuazione della minaccia viene spesso assimilata alla ricerca di un ago in un pagliaio. Le ricerche EDR devono ottenere risultati completi e granulari in tempo reale ed essere in grado di scavare all'interno di specifici parametri di individuazione, combinando tali parametri in modo inclusivo o esclusivo. Per aiutare ulteriormente gli analisti e far risparmiare loro tempo, i risultati dovrebbero essere mostrati in un'interfaccia utente grafica (GUI) facile da comprendere, in modo che possano cercare un evento in maniera semplice e intuitiva, da qualsiasi endpoint, in qualsiasi momento.

Cosa cercare:
- Ricerca minaccia latente
- Individuazione automatizzata
- Creazione di playbook personalizzati
- Nessuna conoscenza di programmazione richiesta
- Mining dei dati
- Capacità di agire in tempo reale
- Panoramica grafica

Domande:

→ Gli utenti possono definire strategie di rilevamento e playbook personalizzati?

→ Sei in grado di automatizzare gli scenari di individuazione delle minacce?

→ Ottieni una panoramica grafica di una ricerca delle minacce per un rapido triage?

→ Hai bisogno di conoscenze di programmazione per creare i playbook?

Fasi successive

Scopri di più su IBM Security ReaQta e richiedi una versione dimostrativa.

IBM Italia S.p.A.
Circonvallazione Idroscalo
20054 Segrate (Milano)
Italia

Prodotto negli Stati Uniti d'America
Aprile 2022

Le informazioni contenute nel documento sono aggiornate alla data della prima pubblicazione e potrebbero essere modificate da IBM senza alcun preavviso Non tutte le offerte sono disponibili in ogni Paese in cui IBM opera.

LE INFORMAZIONI FORNITE NEL PRESENTE DOCUMENTO SONO DA CONSIDERARSI "NELLO STATO IN CUI SI TROVANO", SENZA GARANZIE, ESPLICITE O IMPLICITE, IVI INCLUSE GARANZIE DI COMMERCIABILITÀ, DI IDONEITÀ PER UN PARTICOLARE SCOPO E GARANZIE O CONDIZIONI DI NON VIOLAZIONE. I prodotti IBM sono coperti da garanzia in accordo con i termini e condizioni dei contratti sulla base dei quali vengono forniti.

Dichiarazione di conformità alle procedure di sicurezza: La sicurezza dei sistemi IT richiede la protezione di sistemi e informazioni tramite prevenzione, identificazione e risposta agli accessi impropri di origine interna o esterna alle aziende. L'accesso improprio può causare l'alterazione, la distruzione, l'appropriazione indebita o l'uso improprio delle informazioni; può inoltre provocare danni e uso improprio dei sistemi, che possono essere utilizzati per attaccare altri sistemi. Nessun prodotto o sistema IT può essere considerato completamente sicuro e nessun prodotto, servizio o misura di sicurezza è del tutto efficace nel prevenire l'uso o l'accesso improprio. Sistemi, prodotti e servizi IBM sono progettati come elementi di un approccio di sicurezza completo, nel rispetto delle normative, che richiederà necessariamente procedure operative aggiuntive e il probabile impiego di altri sistemi, prodotti o servizi per raggiungere la massima efficienza. IBM NON GARANTISCE CHE SISTEMI, PRODOTTI O SERVIZI SIANO ESENTI DA O RENDERANNO L'AZIENDA ESENTE DA, CONDOTTA MALEVOLA O ILLEGALE DI UNA QUALSIASI PARTE.