# McAfee Database Activity Monitoring

## Protezione conveniente dei database per soddisfare i requisiti di conformità


Le organizzazioni conservano i dati più preziosi e sensibili in un database, ma la protezione del perimetro e la sicurezza di base fornita con il database stesso non tutelano dai sofisticati hacker di oggi o dalle minacce potenzialmente derivanti da insider malintenzionati. Una ricerca[1] mostra che oltre il 96% dei record violati includeva un database, e che il 66% delle violazioni rimane nascosto per molti mesi o ancor di più. McAfee® Database Activity Monitoring rileva automaticamente i database in rete, li protegge con un insieme di difese preconfigurate, agevolando la creazione di una policy di sicurezza personalizzata per il proprio ambiente. Ciò rende più facile dimostrare la conformità ai revisori e migliorare la protezione delle risorse dati critiche.

### Vantaggi principali

- Massima visibilità e protezione da tutte le fonti di attacco.
- Monitoraggio delle minacce esterne, del personale interno con privilegi e delle minacce sofisticate provenienti dall'interno del database.
- Rischi e responsabilità ridotti bloccando gli attacchi prima che provochino danni.
- Risparmi in termini di tempo e denaro con un'installazione più rapida e un'architettura più efficiente.
- Flessibilità di un'installazione facile sull'infrastruttura IT scelta.
- Integrazione con i principali prodotti McAfee, come la piattaforma di gestione McAfee® ePolicy Orchestrator® (McAfee ePO™) e McAfee Vulnerability Manager for Databases.

Con McAfee Database Activity Monitoring le aziende guadagnano in visibilità su tutte le attività legate al database, compresi gli accessi privilegiati locali e i sofisticati attacchi provenienti dall'interno dello stesso database. McAfee Database Activity Monitoring li aiuta a proteggere i dati più preziosi e sensibili da minacce esterne e personale interno pericoloso. Oltre a fornire un'affidabile processo di revisione, McAfee Database Activity Monitoring previene le intrusioni terminando le sessioni che violano le policy di sicurezza.

Con McAfee Database Activity Monitoring le aziende possono:

- Creare rapidamente una policy di sicurezza personalizzata per soddisfare le normative del settore o gli standard di governance IT interni.
- Registrare l'accesso ai dati sensibili per scopi di verifica, compresi i dati completi delle transazioni.
- Terminare le sessioni che violano le policy e mettere in quarantena gli utenti sospetti, evitando che i dati vengano compromessi.
- Mantenere separate le mansioni come richiesto da molte normative.

McAfee Database Activity Monitoring protegge a un costo conveniente i dati da tutte le minacce, monitorando localmente l'attività in ogni server database e allertando o interrompendo il comportamento dannoso in tempo reale, anche quando opera in ambienti virtualizzati o di cloud computing.

### Protezione da tutti i vettori di minacce per il database

Gli attacchi che prendono di mira i preziosi dati memorizzati nei database possono provenire dalla rete, da utenti locali che accedono al server stesso e anche dall'interno del database, tramite procedure o attivatori memorizzati. McAfee Database Activity Monitoring utilizza i sensori basati sulla memoria per catturare tutti e tre i tipi di minacce con una singola soluzione non intrusiva. Queste informazioni possono essere quindi utilizzate per dimostrare la conformità a scopo di verifica e per migliorare la sicurezza complessiva per i dati più importanti di un'azienda.

### Identificazione delle minacce mentre si concretizzano, riducendo rischi e responsabilità

Diversamente dalle verifiche di base o dall'analisi dei log, che rivelano solo ciò che si è verificato dopo un evento, il monitoraggio in tempo reale e le funzioni di prevenzione delle intrusioni chiudono le brecce prima che provochino danni. Gli allarmi sono inviati direttamente alla dashboard di monitoraggio con i dettagli completi della violazione delle policy, allo scopo di eseguire gli interventi correttivi. In caso di violazioni ad alto rischio la configurazione può terminare automaticamente sessioni sospette e mettere in quarantena gli utenti malintenzionati, dando tempo al personale di sicurezza di investigare l'intrusione.

## Le patch virtuali proteggono dagli attacchi conosciuti e da molte minacce zero-day

Non sempre è possibile installare immediatamente le patch del produttore, in quanto spesso richiedono di testare le applicazioni, con conseguenti tempi di fermo per applicare l'aggiornamento. Inoltre, alcune applicazioni utilizzano ancora vecchie versioni dei database, per i quali le patch non vengono più fornite. McAfee Database Activity Monitoring rileva sia gli attacchi che tentano di sfruttare le vulnerabilità note, sia i comuni vettori delle minacce e può essere configurato per emettere un allarme o per terminare la sessione in tempo reale. Gli aggiornamenti delle patch virtuali vengono forniti regolarmente per le nuove vulnerabilità scoperte e possono essere applicati senza il downtime del database, proteggendo i dati sensibili finché non viene rilasciata e applicata una patch del produttore del database.

## Installazione rapida e non intrusiva con risorse minime

In quanto soluzione solo software, McAfee Database Activity Monitoring può essere implementato e iniziare a proteggere i database in meno di un'ora, senza bisogno di hardware speciale o server aggiuntivi. Per accelerare ulteriormente l'installazione, McAfee Database Activity Monitoring esamina automaticamente la rete alla ricerca dei database e utilizza modelli con procedure guidate per i vari contesti normativi, guidando l'utente nella rapida creazione di policy di sicurezza personalizzate per soddisfare le esigenze di verifica. Distribuendo la responsabilità di implementare la policy di sicurezza ai sensori autonomi in esecuzione su ciascun server database, McAfee Database Activity Monitoring dimensiona efficacemente i costi per supportare anche le imprese più grandi.

## Supporta l'infrastruttura IT moderna, compresi virtualizzazione e cloud

Altri sistemi per il monitoraggio dei database si affidano all'analisi del traffico di rete per identificare le violazioni delle policy, un'operazione impossibile o inefficiente nelle architetture distribuite e altamente dinamiche utilizzate per la virtualizzazione dei data center e per il cloud computing. Di contro, i sensori McAfee possono essere configurati per iniziare l'attività con ogni nuovo database, richiedere le policy di sicurezza basate sui dati ospitati, quindi inviare gli allarmi al server di gestione. Anche se la connettività di rete viene interrotta, i dati restano protetti dato che il sensore applica le policy di sicurezza a livello locale, e gli allarmi sono messi in coda per essere consegnati quando il server di gestione torna raggiungibile.

## Integrazione con la piattaforma McAfee ePolicy Orchestrator

McAfee Database Activity Monitoring è integrato nel software McAfee ePolicy Orchestrator, fornendo così reportistica centralizzata e informazioni riepilogative su tutti i database, da una singola dashboard. Il software McAfee ePO si collega ad altre soluzioni McAfee per la sicurezza al di fuori della protezione per il database per fornire un'unica visualizzazione per una visibilità completa e una gestione più semplice.

## Soluzioni McAfee per la sicurezza del database

McAfee offre una serie di soluzioni per la sicurezza del database per aiutarti a ottenere una visibilità completa del panorama complessivo del database e lo stato di sicurezza. Per ulteriori informazioni, visita www.mcafee.com/it/products/database-security/index.aspx oppure contatta il rappresentante locale McAfee o il rivenditore più vicino.

## A proposito della protezione per gli endpoint di McAfee

Le soluzioni per la protezione degli endpoint di McAfee offrono protezione su tutti i tuoi dispositivi, sui dati che contengono e sulle applicazioni che eseguono. Le nostre soluzioni, complete e personalizzate, riducono la complessità per raggiungere una protezione multilivello degli endpoint, senza mettere a rischio la produttività. Per saperne di più, visitare www.mcafee.com/it/products/endpoint-protection/index.aspx.

McAfee
An Intel Company

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

[1] *Studio Verizon Business*, 2013.


60603ds_dam_1013_fnl_ETMG