

# NetIQ Security Manager™

## Proteggere i dati critici e razionalizzare la gestione degli incidenti con una soluzione integrata di gestione delle informazioni e degli eventi di sicurezza

### Introduzione

Tramite un'unica struttura integrata e scalabile, NetIQ Security Manager consente il monitoraggio in tempo reale delle modifiche ai sistemi e delle attività degli utenti, l'individuazione di possibili minacce e intrusioni, la gestione degli eventi relativi alla sicurezza e la loro correlazione, la gestione dei log e l'automazione della risposta agli incidenti. NetIQ Security Manager risponde alle più esigenti normative relative alla conformità automatizzando le procedure di analisi della sicurezza, garantendo l'integrità dei file system, monitorando le modifiche e gestendo la risposta alle attività sospette.

### Soluzioni innovative

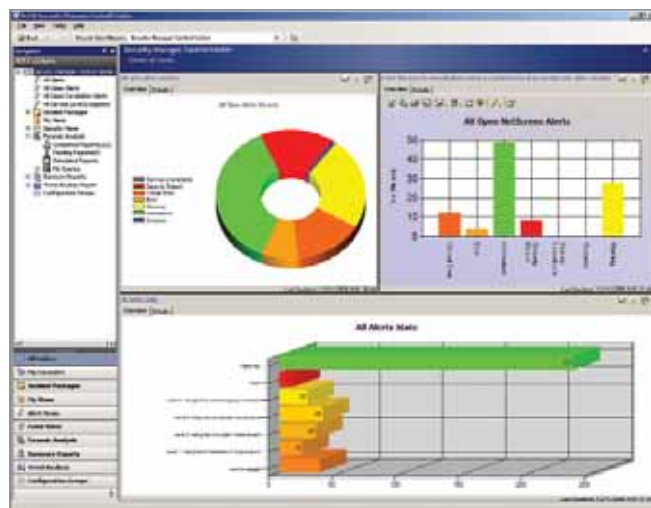
Per soddisfare le continue richieste a livello di sicurezza e disponibilità, le aziende continuano a investire in una vasta gamma di soluzioni per la sicurezza (firewall, prodotti antivirus, sistemi di individuazione delle intrusioni) generando un tale volume di dati da rendere problematica l'individuazione in tempo reale delle violazioni alla sicurezza, nonché la loro raccolta ed analisi.

NetIQ Security Manager massimizza il valore dell'infrastruttura di sicurezza esistente consolidando e archiviando i log e i dati relativi agli eventi di tutta l'azienda. La soluzione include una Knowledge Base completa all'interno della quale sono disponibili tutte le informazioni relative alla sicurezza e che consente di semplificare l'analisi e la soluzione degli incidenti. Grazie alla tecnologia TRACE™ (Trend Reporting, Analytics and Centralized Examination), che utilizza una soluzione proprietaria di archiviazione distribuita basata su file, si ottiene un considerevole miglioramento della gestione dei log rispetto ai database relazionali tradizionali.

### Vantaggi chiave

**Riduzione del tempo di esposizione al rischio** – Ottimizza i tempi di reazione grazie ad una serie di funzionalità avanzate di monitoring in tempo reale dei problemi relativi alla sicurezza, di notifiche e di informazioni e risposte automatizzate.

**Miglioramento della qualità delle informazioni relative alla sicurezza** – Mette a disposizione una Knowledge Base dettagliata che genera automaticamente una vera e propria "security intelligence" ed integra informazioni nuove e aggiornate. In questo modo le conoscenze necessarie per comprendere e rispondere ai problemi vengono rese disponibili esattamente nel momento in cui sono necessarie.



NetIQ Security Manager fornisce una soluzione unica per la protezione dalle intrusioni, per la gestione e la correlazione degli eventi di sicurezza e per l'esecuzione di analisi avanzate in ambito forense e sulle tendenze relative alla sicurezza.

**Ottimizzazione dei livelli di protezione** – Integra e mette in relazione i dati archiviati e quelli generati in tempo reale da tutti i sistemi e i processi di sicurezza. Tenendo traccia dei problemi per verificarne la corretta e puntuale gestione, è possibile ottenere un controllo ottimale del ciclo di vita degli episodi problematici, ottimizzando i livelli di protezione.

**Forte incremento delle performance operative** – Contribuisce ad accrescere il ritorno sugli investimenti (ROI) consolidando le informazioni relative alla sicurezza dell'azienda in un'unico punto, filtrando le informazioni irrilevanti e i falsi positivi ed evidenziando i veri episodi problematici. In tal modo si garantisce un monitoraggio mirato e una capacità di reazione ottimale.

**Garanzia di conformità** – Consente di analizzare e produrre regolarmente dei report sulle informazioni relative alla sicurezza aziendale, di monitorare i controlli sulla sicurezza per validarne l'efficacia e di applicare in tempo reale policy e best practice. In tal modo è possibile soddisfare i requisiti di sicurezza delle normative attualmente in vigore.



## Controllo degli accessi e monitoring degli utenti

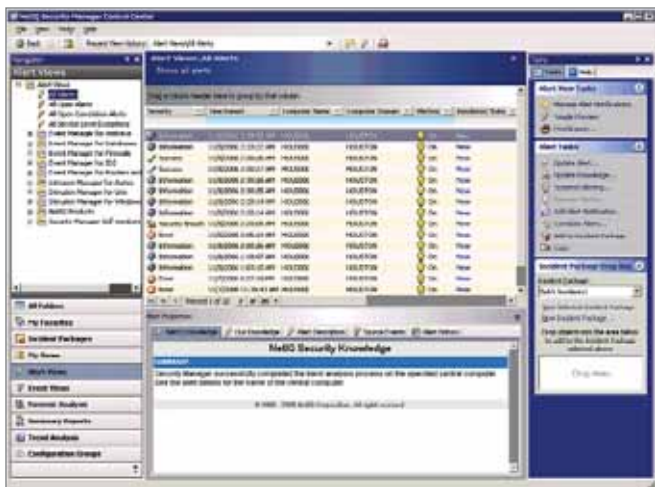
NetIQ Security Manager migliora la disponibilità dei servizi e protegge la proprietà intellettuale dell'azienda grazie a degli strumenti di controllo degli accessi e di supervisione in tempo reale delle attività degli utenti. L'individuazione delle modifiche e la possibilità di segnalarle tramite degli allarmi assicurano l'integrità del file system.

**Abbrevia i tempi di risposta a fronte di incidenti** – notifica immediatamente le violazioni alla sicurezza e alle policy mediante allarmi ed avvisi in tempo reale, consentendo di reagire rapidamente e minimizzare il rischio di eventuali danni.

**Riduce il tempo di esposizione ai rischi** – risponde in tempo reale a fronte dei problemi individuati grazie a dei workflow e a delle risposte automatizzate che consentono di monitorare e risolvere gli incidenti. L'interfaccia guidata consente la creazione e la personalizzazione delle risposte agli utenti privi di particolari conoscenze di programmazione.

**Protegge dalle intrusioni accidentali o intenzionali** – monitora le attività autorizzate o illecite effettuate dagli utenti o dagli amministratori di sistema e di rete sui sistemi aziendali, inviando allarmi in caso di necessità. Le attività monitorate includono: log-in e log-off, modifica delle autorizzazioni, cancellazione dei file di log, modifiche delle autorizzazioni di audit, installazione di software, etc.

**Migliora l'efficacia e la conoscenza delle problematiche relative alla sicurezza da parte dei dipendenti** – include una Knowledge Base integrata per la sicurezza che fornisce informazioni sulle cause che possono aver fatto scattare l'allarme. Questa base dati può essere ampliata con informazioni specifiche dell'azienda (come ad esempio le procedure per la gestione dei problemi), al fine di capitalizzare e riutilizzare tutte le competenze acquisite - senza rischi di perderle ogniqualvolta un dipendente lasci l'azienda.



Knowledge Base integrata e ampliabile per la centralizzazione delle attività di monitoring e di risposta agli allarmi di sicurezza generati da qualsiasi dipartimento dell'azienda.



Security Manager riduce gli eventi di disturbo e i falsi positivi mettendo in correlazione gli eventi generati da diversi sensori per la sicurezza e identificando in modo preciso i problemi critici.

## Correlazione e analisi delle informazioni di sicurezza

Presenta in tempo reale informazioni rilevanti sulla sicurezza, fornendo un quadro realistico sullo stato di sicurezza dell'azienda e distinguendo tra episodi problematici reali e avvisi di disfunzioni o falsi positivi, al fine di razionalizzare la distribuzione delle priorità e le modalità di risposta.

**Ottimizza il valore dell'infrastruttura di sicurezza** – ottimizza le difese e le contromisure adottate dall'azienda attraverso un unico "centro operativo" che gestisce le procedure per la raccolta, la correlazione, l'analisi e la risposta agli eventi generati dalle varie risorse, dai vari specifici prodotti per la sicurezza e dai dispositivi di rete.

**Riduce gli "eventi di disturbo" e i falsi positivi** – riduce il numero delle informazioni non pertinenti grazie ad un potente motore di correlazione che opera in tempo reale semplificando la categorizzazione degli eventi di sicurezza e consentendo ai team responsabili della sicurezza di focalizzarsi sui problemi reali. Tramite un "correlation wizard" viene inoltre semplificata la procedura per la creazione e l'applicazione di nuove regole di correlazione.

**Garantisce l'archiviazione degli eventi relativi alla sicurezza evitando che questi vengano persi o dimenticati** – grazie al workflow interno che consente di tenere traccia dei problemi, è possibile fissarne le priorità e analizzarne lo stato in qualsiasi momento. Possono inoltre essere aggiunte delle informazioni relative alle risposte in modo da fornire un audit trail sulla modalità di gestione dei problemi.

**Garantisce la disponibilità degli aggiornamenti più recenti** – fornisce un meccanismo dinamico di facile utilizzo per ricevere le notifiche sugli aggiornamenti relativi alle funzionalità del prodotto. Facilita inoltre la distribuzione e l'installazione di questi aggiornamenti grazie alla tecnologia NetIQ AutoSync.

# NetIQ Security Manager™

## Riepilogo tecnico

**Console unificata per la supervisione delle operazioni di sicurezza** – Un'unica applicazione Win32 per la gestione degli allarmi in tempo reale, per l'analisi forense dei log e per la presentazione degli incidenti, destinata agli analisti e al personale che opera nell'ambito della sicurezza.

**Motore di correlazione basato su regole** – Correlazione tra gli eventi in tempo reale su sistemi centrali dedicati, in base a regole che consentono di indentificare la sequenza e la tempistica degli eventi a partire da tecnologie eterogenee. Gli eventi generati dai firewall possono ad esempio essere correlati ad eventi riconducibili ai server.

**Gestione sicura e produttiva dei log** – La tecnologia TRACE™ garantisce un'analisi tempestiva e la creazione di report sintetici sul contenuto dei log, una risposta rapida a fronte di incidenti relativi alla sicurezza, analisi e reportistica multidimensionali. I controlli di integrità, garantiti dalle firme digitali, proteggono dalla falsificazione dei dati.

**Monitoring e raccolta dei dati con e senza agent** – Gli agent assicurano la raccolta locale e la gestione dei dati, mettendo a disposizione funzionalità robuste tra le quali il monitoring degli utenti, l'individuazione delle modifiche e le ricerche SID in modo da garantire la flessibilità dei deployment.

**Individuazione delle modifiche** – Gli agent assicurano l'individuazione di modifiche a livello di sistema, quali modifiche di file, modifiche delle autorizzazioni degli utenti, modifiche dei registri Windows, modifiche degli oggetti su iSeries, etc.

**Monitoring degli utenti** – Gli agent offrono delle robuste funzionalità di supervisione degli utenti di server e di altre periferiche. Grazie al sistema interno di tracking degli incidenti le risposte vengono elaborate in tempi rapidi.

## Sistemi e periferiche supportate

NetIQ Security Manager fornisce il supporto necessario per una vasta gamma di sistemi, periferiche e applicazioni, tra cui:

- **Server e workstation:** Microsoft, Linux, Unix e iSeries
- **Servizi critici:** database, Active Directory e infrastruttura VoIP
- **Soluzioni di sicurezza:** prodotti antivirus, firewall, sistemi per il rilevamento e la protezione dalle intrusioni
- **Periferiche di rete:** router, switch. etc.
- **Soluzioni NetIQ:** NetIQ Secure Configuration Manager™, NetIQ AppManager®, NetIQ Change Guardian for Windows™, NetIQ Change Guardian™ for Active Directory, NetIQ Group Policy Guardian™

## Requisiti minimi di sistema

**Per i server Security Manager** (Central Computer, Database Server, Log Archive Server e Reporting Server):

- Biprocesso dual-core (raccomandati AMD/Intel). Processori Quad raccomandati per ambienti di grandi dimensioni.
- 2 GB RAM (minimo). 4 GB RAM (raccomandati).
- Windows Server 2003
- Microsoft SQL Server 2005 SP2 per Database Server e Reporting Server. Enterprise Edition raccomandata per Reporting Server. Reporting Server inoltre richiede:
  - Microsoft SQL Server 2005 Analysis Services con Service Pack 2
  - Microsoft SQL Server 2005 Integration Services (SSIS)
- IIS 5.0, IE 6.0, Office 2003 Web Components ed oltre raccomandati per i report Trend Analysis.

## Contacts

**Sede Centrale**  
**NetIQ, An Attachmate Business**  
1233 West Loop South  
Suite 1800  
Houston, TX 77027  
713.548.1700  
713.548.1771 fax  
888.323.6768 sales  
info@netiq.com  
www.netiq.com

**Sede Centrale NetIQ EMEA**  
+31 71 368 1100  
info-emea@netiq.com

**Sede italiana di Milano**  
+39 02 99060201

**Sede italiana di Roma**  
+39 06 5423281

informazioni.italia@attachmate.com  
www.netiq.com/it

Per ulteriori informazioni sulle sedi locali, sui partner e sui rivenditori NetIQ, visitare il sito [www.netiq.com/contacts](http://www.netiq.com/contacts).

NetIQ® AppManager®, NetIQ Change Guardian™ for Windows, NetIQ Change Guardian™ for Active Directory, NetIQ Group Policy Guardian™, NetIQ Security Manager™, NetIQ Secure Configuration Manager™, NetIQ e il logo NetIQ sono marchi o marchi registrati di NetIQ Corporation o delle sue filiali negli Stati Uniti o in altri Paesi. Tutti gli altri nomi di società o prodotti possono essere marchi o marchi registrati delle rispettive società.

© 2007 NetIQ Corporation, tutti i diritti riservati.

DS10259SMGR EC 0707

