

# System Administrators Monitor



“SA-monitor, la soluzione completa per la gestione degli amministratori di sistema”

Riferimenti normativi:

Garante della Privacy, Provvedimento del 27/11/08 sugli Amministratori di Sistema.



Valutazione delle caratteristiche soggettive

Valutazione delle caratteristiche soggettive degli AdS

Designazioni Individuali

Gli AdS sono oggetto di incarico individuale con l'elencazione analitica degli ambiti consentiti.

Elenco degli amministratori di sistema

L'elenco degli amministratori deve essere riportato nel DPS. Deve essere riconducibile l'identità degli outsourcers. Deve essere nota l'identità degli AdS ai dipendenti dei quali gli stessi trattano i dati personali.

Verifica delle attività

L'operato degli AdS e' soggetto a verifica almeno una volta l'anno

Registrazione degli accessi

Gli accessi degli AdS sono registrati e le registrazioni comprendono i riferimenti temporali e l'evento che le ha generate ogni registrazione viene conservata per un periodo di sei mesi.

## Il Problema

Il Garante della Privacy, con proprio provvedimento del 27 novembre 2008 ha introdotto una normativa volta a regolamentare l'attività degli amministratori di sistema, al fine di garantire un più alto standard di sicurezza per i dati personali. Le prescrizioni sono obbligatorie per tutti i titolari di trattamento di dati personali (Aziende, Enti, Amministrazioni centrali e periferiche) che non sono interessati dal precedente provvedimento di semplificazione.

Le figure professionali interessate sono:

- Amministratori di sistema
- Amministratori di Data Base
- Amministratori di rete
- Amministratori di applicazioni complesse.

## La Soluzione

Per essere conformi al provvedimento del Garante è necessario affrontare sia gli aspetti tecnologici che quelli organizzativi toccati dal provvedimento: soluzioni parziali comportano costi e non risolvono il problema.

La soluzione di ZEROPIU è SA-monitor, un prodotto, basato su tecnologie Oracle, che

- Supporta i processi organizzativi interessati dalla normativa
  - Realizza in modo efficiente e sicuro la raccolta dei log degli accessi da tutti gli ambienti interessati
  - Costruisce un repository e fornisce strumenti di intelligence che consentono di raggiungere standard di sicurezza elevati.
- SA-monitor si inserisce e si integra, per caratteristiche intrinseche di progetto, in qualsiasi contesto tecnologico ed organizzativo.

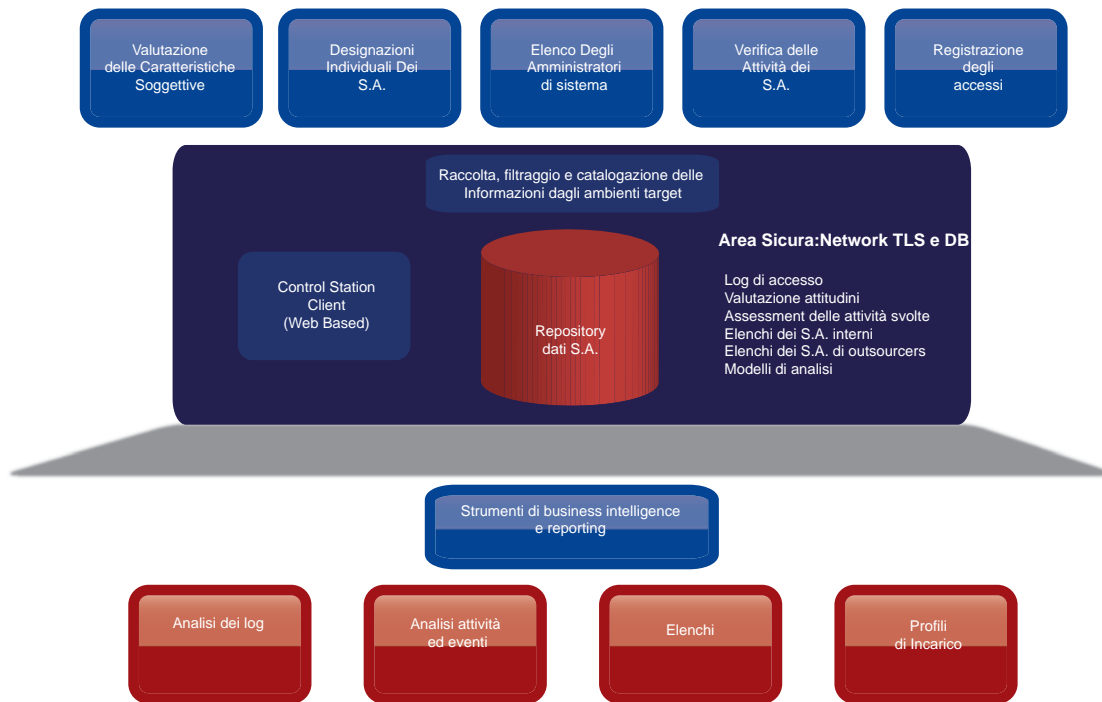
## Qualità

Sa-monitor rende disponibili strumenti evoluti a supporto dei processi organizzativi toccati dal provvedimento:

- la verifica dei profili degli AdS;
- la designazione individuale degli incaricati;
- la tenuta degli elenchi degli AdS;
- la verifica dell'operato degli AdS.

Con SA-monitor, la raccolta dei log degli accessi a tutti i sistemi, i database, le reti e gli applicativi rilevanti è assicurata da una piattaforma tecnologica unica, evoluta e robusta, che garantisce anche il trattamento sicuro delle informazioni (non alterabilità).

Con SA-monitor tutte le informazioni relative agli AdS confluiscono in un archivio unico, su cui operano strumenti sofisticati di analisi dei dati, finalizzati alla individuazione tempestiva delle situazioni di rischio ed alla produzione dei report richiesti dalla norma.



## Architettura

L'architettura funzionale di SA-monitor, riportata in figura, è incentrata su un repository in cui vengono catalogate tutte le informazioni, relative agli AdS, necessarie per la compliance alla normativa sulla Privacy e per la sicurezza dei dati aziendali.

Le informazioni vengono acquisite o catturate dai sistemi operativi in tempo reale o in near real time, in modo trasparente agli utenti.

Per garantire la non alterabilità delle informazioni, l'acquisizione avviene in un ambiente sicuro che include la rete di interconnessione ai sistemi e il DB.

L'accesso all'ambiente sicuro è regolamentato secondo un modello di segregation of duties che impedisce operazioni non lecite sui dati anche agli AdS.

Le informazioni vengono acquisite mediante moduli funzionali specializzati, realizzati per ciascuno dei requisiti obbligatori previsti dalla normativa.

Se il contesto lo richiede, su questa piattaforma possono essere sviluppate delle estensioni così da specializzare i moduli esistenti o crearne dei nuovi dedicati ad una particolare funzionalità.

Il repository contiene informazioni rilevanti per la sicurezza aziendale: l'analisi integrata di queste informazioni è assicurata da strumenti avanzati di business intelligence.

## Tecnologia

SA-monitor è progettato per ambienti target multivendor (ad es. ambienti Unix, Windows, mainframe, apparati di rete, database e applicazioni) e si avvale delle migliori tecnologie disponibili in ciascuno degli ambiti funzionali trattati.

SA-monitor al suo interno racchiude versioni specializzate dei prodotti leader in ciascun ambito tecnologico di riferimento e sfrutta le tecnologie più all'avanguardia nel trattamento dei dati tra queste:

Attestation, reconciliation, ETL, event data correlation, self assessment.

Inoltre offre una flessibilità tale da potersi integrare con qualsiasi fonte dati in maniera nativa.

All'interno della soluzione è anche presente un Log relay che preleva i log tipici di sistema e permette di archivarne una copia esattamente identica all'originale contestualmente alla generazione del log stesso in modo da poter garantire il non ripudio.

Il trasporto dei dati sensibili avviene su canale cifrato in ogni tratto ove sia presente un componente della soluzione.

IL repository centralizzato che sfrutta un modello dati specializzato utilizza un'opzione che ne eleva il livello di sicurezza di accesso e trasporto ai massimi livelli, rispettando canoni di standard internazionali quali PCI-DSS, ISO 27001 e HIPPA.

## Vantaggi

SA-monitor dà una risposta a tutte le esigenze di compliance derivanti dal Provvedimento del Garante sugli amministratori di sistema:

SA-monitor non affronta solo la gestione del log degli accessi.

SA-monitor rende disponibile una piattaforma per affrontare tutte le esigenze di sicurezza connesse a gruppi di utenti privilegiati interni all'azienda caratterizzati da un alto livello di discrezionalità operativa.

Il controllo dell'attività degli AdS non è, infatti, rilevante solo per la tutela dei dati personali ma anche per la sicurezza di diversi insiemi di dati aziendali critici per il business.

SA-monitor è una piattaforma che può integrare tutte gli ambienti tecnologici ed applicativi di oggi e di domani.

**ORACLE**

**ZEROPIU**  
Difference as value

Contatta un rappresentante  
Via Frà Luca Pacioli 3, 20144 Milano  
(+39) 02 - 83102300  
(+39) 02 - 83102310 fax.  
www.zeropiu.it grc@zeropiu.it