IBM Tivoli zSecure

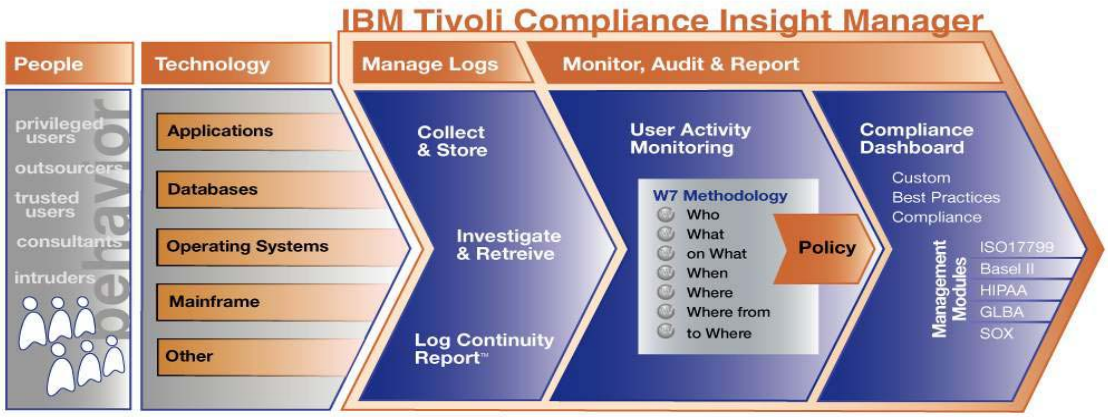
Soluzioni per l'auditing
e la compliance

Da oltre 20 anni Consul si occupa di soluzioni per l'*auditing* e la *compliance* ed ha sviluppato una piattaforma tecnologica unica sul mercato per completezza ed efficacia. Oggi Consul è un'azienda IBM ed i suoi prodotti sono entrati a far parte del portafoglio Tivoli, con conseguente rinomina di Consul Insight in IBM Tivoli Compliance Insight Manager e di Consul zSecure in IBM Tivoli zSecure.

IBM Tivoli Compliance InSight Manager

La gestione della sicurezza informatica vede coinvolte persone e tecnologie che devono essere controllate attraverso specifiche politiche di sicurezza. Fondamentale nella gestione di questo processo continuativo è la possibilità di ricavare informazioni di audit in modo continuativo ed omogeneo.

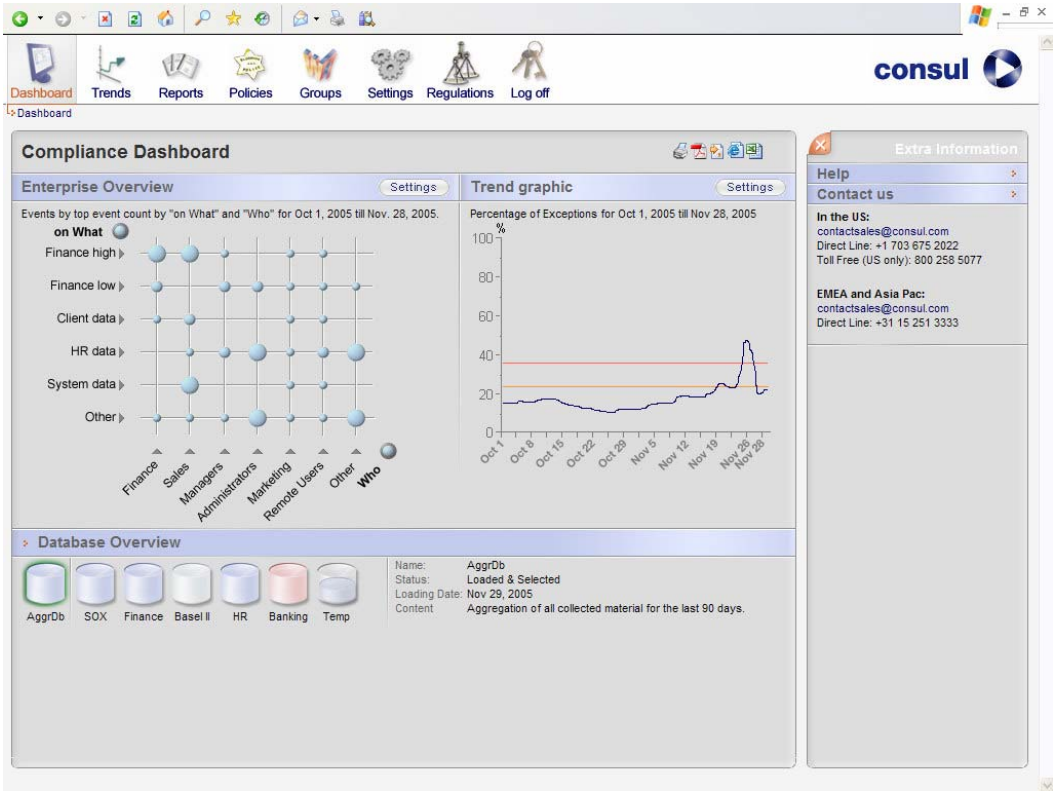
In questo contesto è fondamentale riuscire a correlare tra di loro i dati relativi alla sicurezza provenienti dai sistemi, distribuiti ed eterogenei, normalmente di difficile interpretazione poichè basati su sintassi sempre molto diverse.



IBM Tivoli Compliance Insight Manager (ex Consul Insight) è un prodotto attualmente unico sul mercato ed è composto da un sistema molto efficace di aggregazione dei log. Il modulo di *log management* è opera su ogni tipo di log ed è in grado di controllare che tutti i dati siano correttamente acquisiti e non ci siano manipolazioni degli stessi. Il tutto viene esaminato mediante una dashbord console a più livelli che permette di semplificare le attività di analisi e controllo delle compliance.

Insight è in grado di controllare che tutte le attività fatte dagli utenti, dai sistemi di rete fino al mainframe, dal sistema operativo alle applicazioni e database, siano conformi alle regole aziendali o alle specifiche normative oggi esistenti (ISO17799, Sarbanes-Oxley,

GLBA...). Inoltre la tipologia di presentazione dei dati di tipo giornalistico, denominata W7 ed attualmente sottoposta a standard internazionale, permette anche a chi non è esperto di poter sapere chi (WHO) ha fatto cosa (WHAT) su quali sistemi, a che ora (WHEN) cosa ha cambiato.



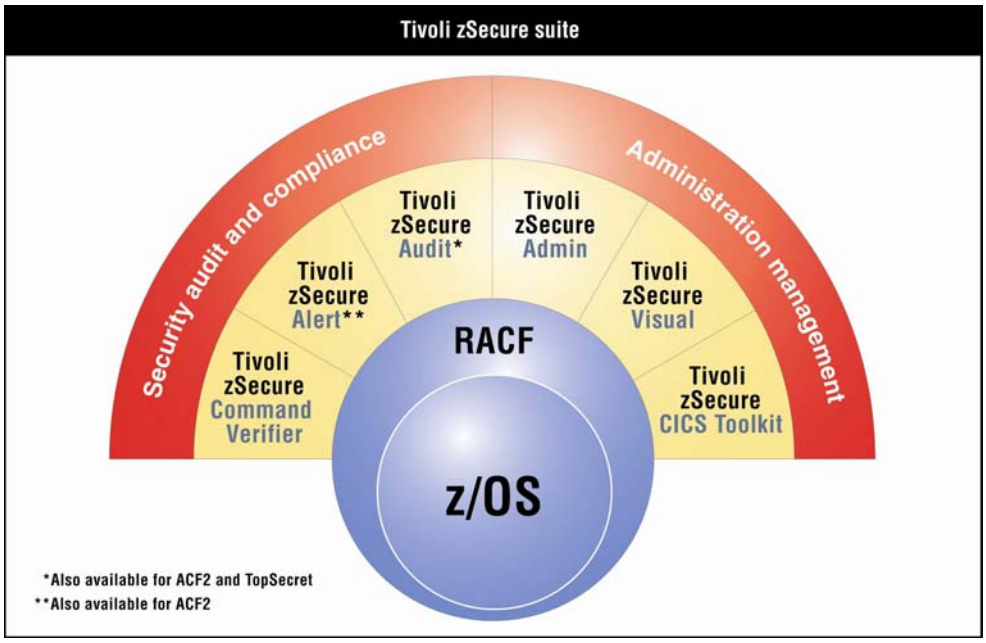
Insight quindi permette di risolvere tutte le esigenze di tracciamento, monitoraggio, reportistica, ricerca ed investigazione di attività non conformi alle politiche di sicurezza aziendali. I principali campi di utilizzo sono:

- Centralizzazione ed automazione delle attività di controllo dei log: *log management*
- Verifica delle attivià degli utenti privilegiati: *privileged user monitoring and audit* (PUMA™)
- Auditing sulle fonti dati critiche aziendali (RDBMS)
- Capacità di generare report comprensibili a persone non tecniche, es. Auditor, e per soddisfare le numerose mormative (ISO 17799, SOX, Basilea II...)

L'architettura su più livelli permette di sposare ambienti anche molto complessi, quali prima non si pensava fosse possibile, come grandi realtà finanziarie e di telecomunicazioni.

IBM Tivoli zSecure

Tivoli zSecure è una suite integrata di specifici strumenti per l'amministrazione, l'audit e la compliance dell'ambiente zSeries. Centinaia di clienti nel mondo usano zSecure per facilitare la gestione del mainframe e aumentare le capacità di controllo e di analisi.

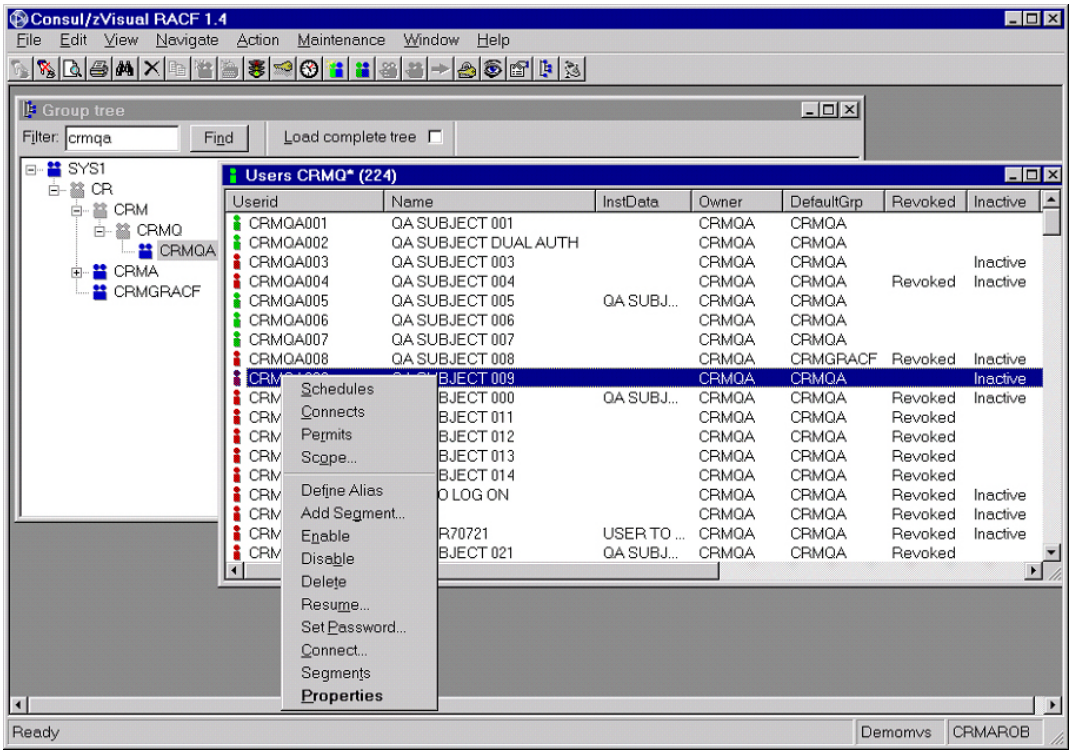


La suite zSecure, perfettamente integrata con InSight a cui fornisce le informazioni necessarie per popolare il dashbord, dà una modalità user-friendly di operare con la sicurezza mainframe, permettendo di scegliersi l'interfaccia utente più adatta a chi deve amministrare il RACF (ISPF, Windows based o CICS) e consentendo attività correlate di alert e monitoring.

IBM Tivoli zSecure Admin è il diffusissimo strumento della suite zSecure che permette di semplificare e velocizzare in maniera esponenziale l'amministrazione del RACF, evitando di usare complicati comandi nativi, ed automatizzare le attività quotidiane che hanno carattere ripetitivo prevenendo così l'errore umano. zSecure Admin potenzia la capacità di autorizzazione degli accessi e di delega del RACF. La gestione della sicurezza del mainframe è particolarmente semplificata, visto che con zSecure Admin è necessario un numero di risorse sensibilmente ridotto rispetto a quello normalmente utilizzato per

gestire il RACF nativamente. Rappresenta l'interfaccia utente classica verso il RACF via TSO-ISPF.

IBM Tivoli zSecure Visual rappresenta una delle tre possibili interfacce suddette e precisamente quella Windows based, con la quale è possibile demandare l'amministrazione del RACF a utenti con conoscenze meno specialistiche. Questo limita la necessità di investire in education costosa e specialistica sul RACF, in quanto la maggior parte degli utenti oggi è in grado di utilizzare un'applicazione di tipo Windows. Nella figura di seguito infatti possiamo notare come si presenta questo tipo di interfaccia e quale feeling di semplicità essa dia.



IBM Tivoli zSecure CICS Toolkit è la terza possibile interfaccia utente per l'amministrazione del RACF, quella CICS based. User-friendly anch'essa, visto che utilizza metodologie all'avanguardia e SOA compliant come quelle CICS, molto usate a livello utente finale, consentendo quindi di demandare le azioni ripetitive di gestione della sicurezza mainframe a utenti già avvezzi a un quotidiano utilizzo del CICS. In questo modo le complicate routine RACF diventano semplici strumenti di amministrazione. Una delle funzionalità fondamentali dello zSecure CICS Toolkit, che

lo rende SOA compliant, è la possibilità che esso dà alle applicazioni Web di potersi connettere direttamente al RACF.

IBM Tivoli zSecure Audit è il modulo per implementare una soluzione di audit e compliance in ambiente System z. Esso permette di misurare e verificare il livello di sicurezza del proprio mainframe e fornisce una vista accurata di quali sono gli scostamenti rispetto alle politiche definite, visualizzandoli per ordine di importanza. E' un potente strumento di reportistica che analizza gli eventi e i log RACF e SMF sia di tipo online che storico. In questo modo, anche tramite il supporto dell'Insight che evidenzia e raccoglie tutti gli eventi di security più rilevanti, permette di identificare e quindi analizzare quelle inconsistenze che generano rischi di esposizione all'intera sicurezza mainframe, garantendo in questo modo la massima integrità. Una grossa potenzialità di zSecure Audit è quella di poter generare report anche via XML, consentendo quindi di servirsi di qualsiasi strumento di analisi fra cui anche Microsoft Excel o Lotus 123.

IBM Tivoli zSecure Alert è uno strumento di monitoraggio real-time delle intrusioni e delle attività indesiderate, specifico per ambiente mainframe, che va ben oltre ad un tradizionale sistema di Intrusion Detection. Infatti è in grado di bloccare le azioni prima che queste abbiano effetto, come un vero sistema di Intrusion Prevention. zSecure Alert monitorizza lo z/OS, il RACF e lo Unix System Services, permettendo di inviare allarmi SNMP alla dashbord console di Insight e a quella IBM Tivoli, di generare WTO, email e messaggi di testo a cellulari e pager.

IBM Tivoli zSecure Command Verfier (ex zLock) permette di effettuare *policy enforcement* in modo che il sistema mainframe risulti protetto da operazioni accidentali o volute ma comunque dannose, limitando quindi le abilitazioni e le autorizzazioni degli utenti. Il modulo possiamo quindi paragonarlo a uno standardizzatore della security mainframe a quelle che sono le politiche di sicurezza decise in azienda, garantendo una compliance a livello di compagnia massimizzando il controllo, minimizzando i rischi dovuti a una sicurezza fuori standard e abbattendo i costi causati dal dover costantemente ripulire autorizzazioni non consentite o situazioni rimaste sporche all'interno del RACF.