IBM Service Management Roadshow

Risk Management

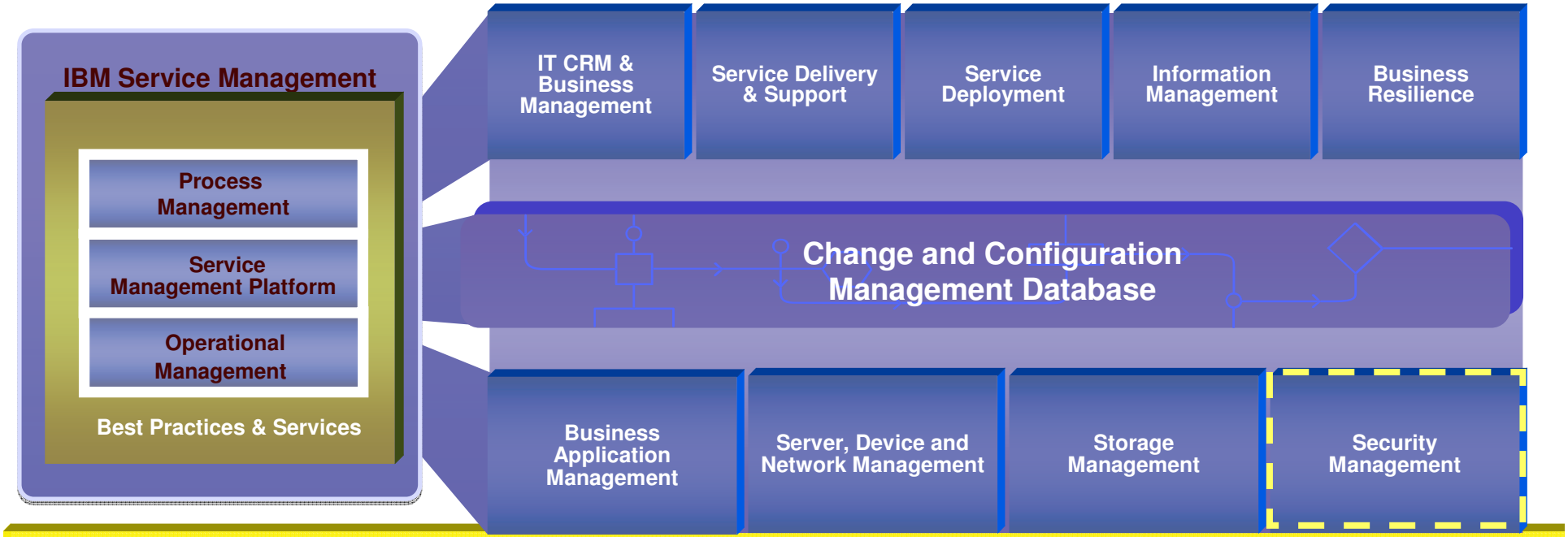
Roma, Palazzo dell'Informazione*, 13 Marzo 2007*

Alessandro Faustini
Tivoli Security Technical Sales

Agenda

- **Service Management & Security**
- **Consul Risk Management**
- **InSight**
- **zSecure**

IBM Service Management e IT Security Management

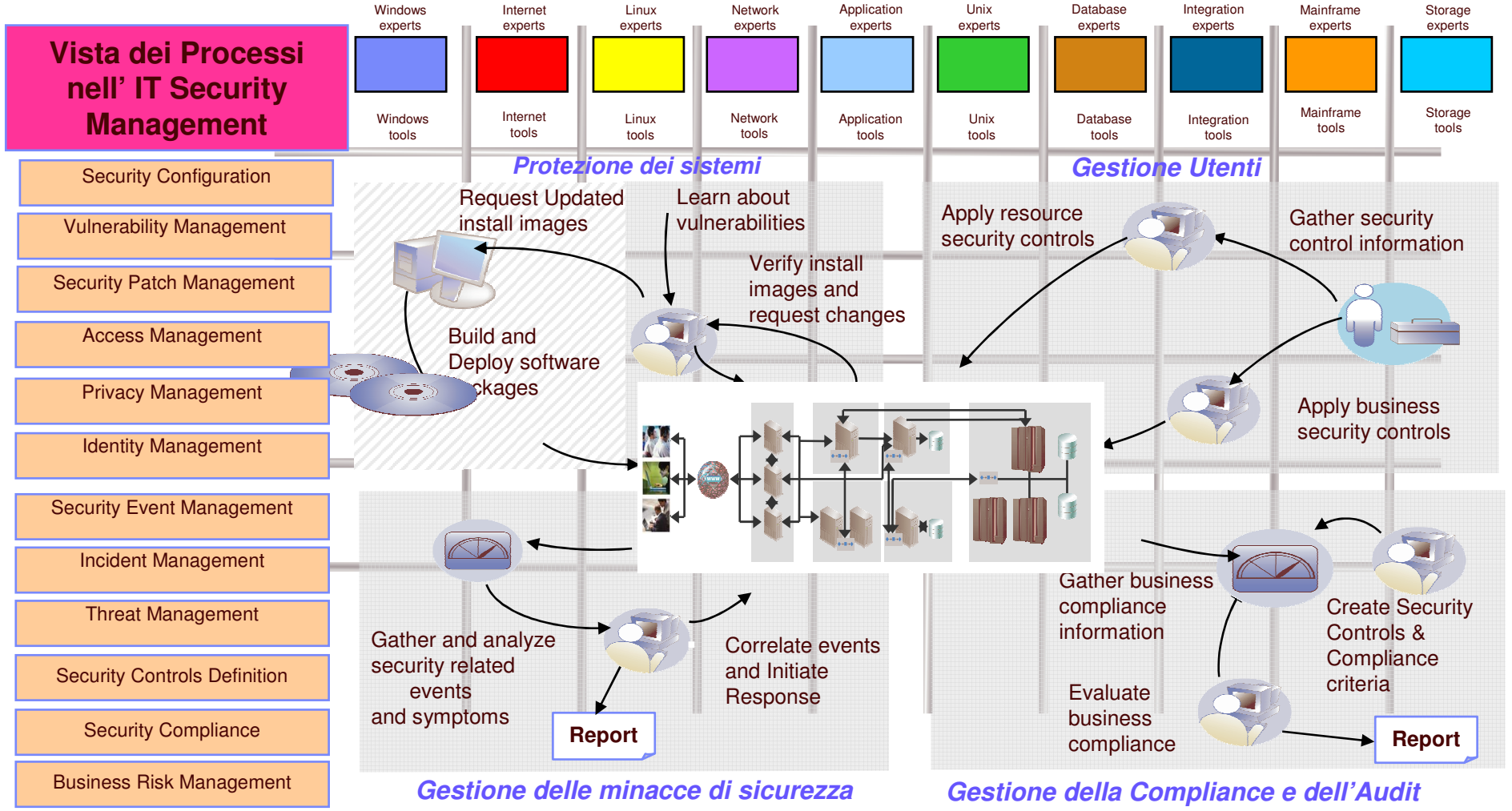


Gestione della sicurezza e della compliance

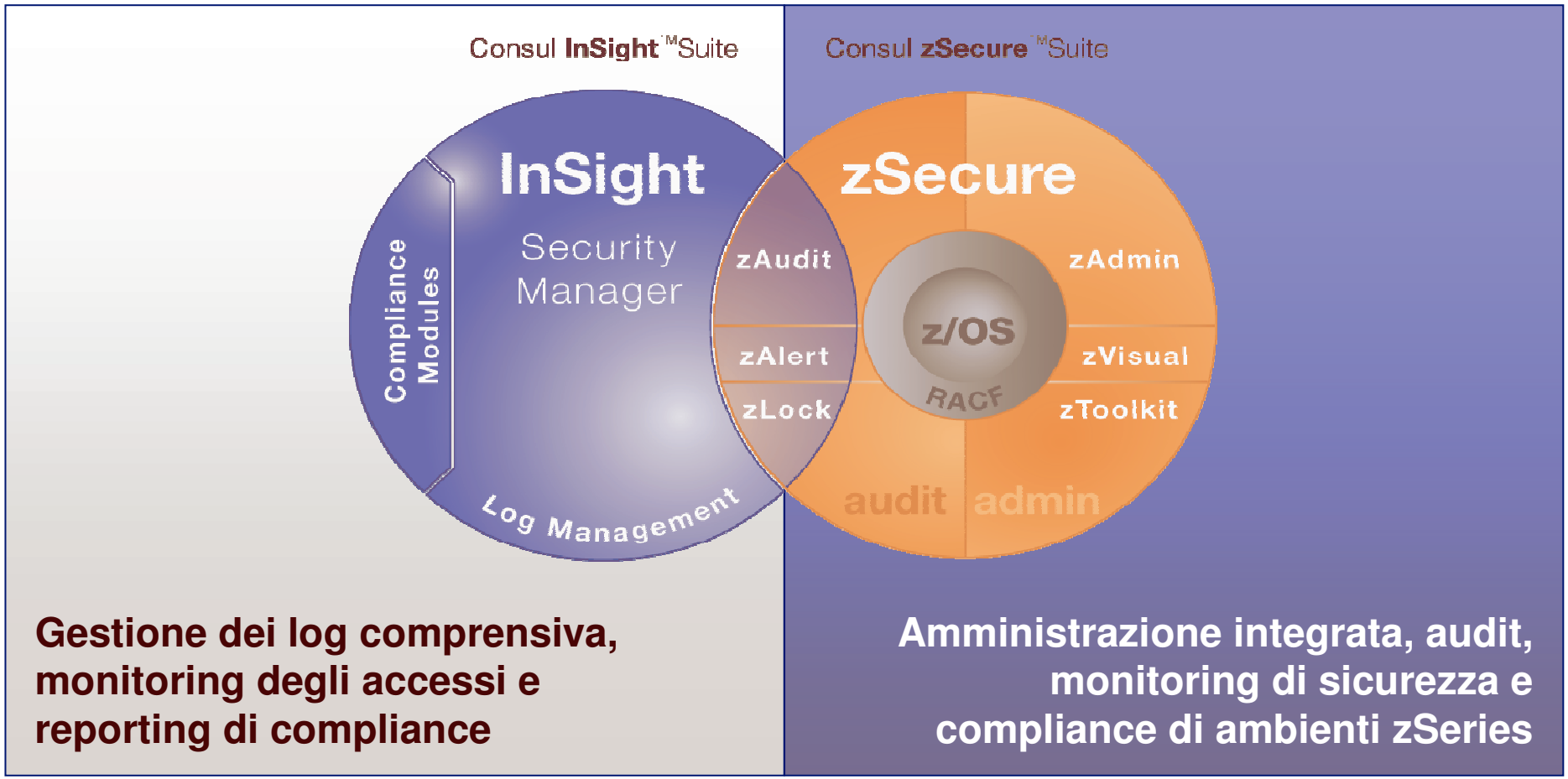
- Gestione della sicurezza IT, dell'audit e della compliance attraverso tutta la compagnia
- Gestione strutturata delle identità e degli accessi
- Gestione centralizzata delle minacce di sicurezza e degli incidenti
- Facilitare la valutazione degli impatti nella gestione dell'IT delle varie leggi e regolamentazioni come la SOX, GLBA, ISO17799, Basel II, Dlg. 196/2003, HIPAA
- Soluzioni comprensive, semplici da usare per gestire e monitorare l'attività utente attraverso tutta l'enterprise

Processi chiave nell'IT Security Management

Le attività ed i processi associati con l'IT Security Management possono essere riassunti in quattro modelli che rimarranno attuali con i cambi della tecnologia.



Consul Risk Management
Audit & Compliance



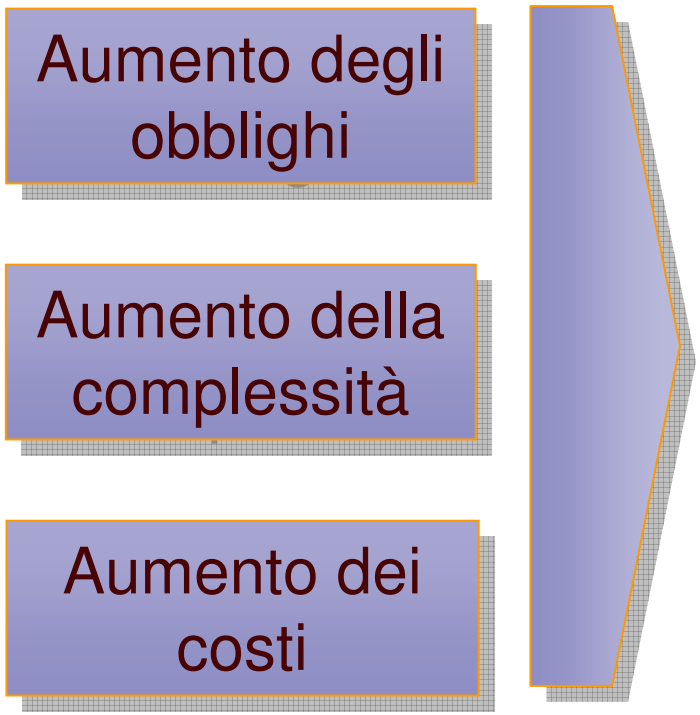
Audit & Compliance

- **Aumento degli obblighi**
  - Le normative sono ormai decine (Basilea II, ISO17799, Dlg. 196/2003, SOX…)
  - Le iniziative di compliance aumentano in ogni settore di industria
- **Aumento della complessità**
  - Le tecnologia e le infrastrutture disparate frammentano ed impediscono gli sforzi per la compliance
  - Il collegamento in termini di compliance tra il livello infrastruttura e il livello business è desiderabile, ma è una sfida spesso onerosa
- **Aumento dei costi**
  - Difficile sapere a priori il costo di un'attività di audit sulle moderne infrastrutture, eterogenee e distribuite
  - La cadenza periodica di un attività di audit impone costi fissi elevati
  - Il fallimento di un audit è nuovamente un costo da ripetere

Il 43% dei CFO pensano che il miglioramento della governance, dei controlli e del risk management sia al top delle loro sfide.

CFO Survey: Current state & future direction,
IBM Business Consulting Services

Audit & Compliance

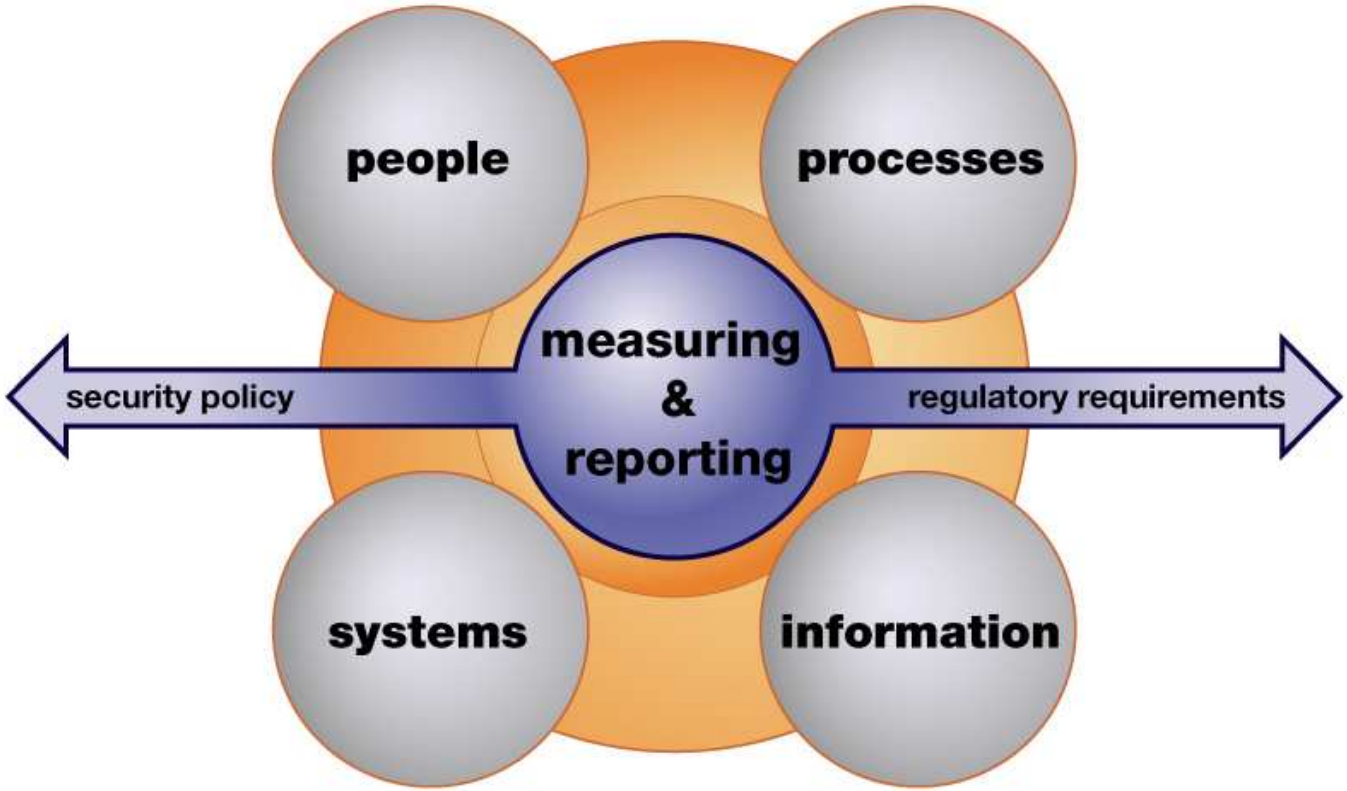


1. Le iniziative di Compliance richiedono processi strutturati e ripetibili
2. L'enfasi è sul controllo delle attività degli utenti privilegiati (*Privileged User Monitoring and Audit*, PUMA)
3. Facilità nel verificare gli accessi ai sistemi e applicazioni
4. Capacità di verificare la compliance degli asset strategici: z/OS, RACF, UNIX, monitoraggio e audit di database

Cosa è importante

- **Violazioni alla Privacy**
  - DBA accedono informazioni riservate?
  - Ci sono usi impropri delle applicazioni HR?
  - Ci sono usi non legittimi di identità?
- **Violazioni alle politiche di sicurezza**
  - Ci sono modifiche ai sistemi non autorizzate?
  - Ci sono utenti root che hanno disattivato il tracciamento delle operazioni?
  - Quando sono stati cancellati i log di sistema?
  - Chi ha fermato quel processo importante senza permesso?
- **Amministratori che violano la separazione delle funzioni**
  - Ci sono utenti privilegiati che hanno effettuato transazioni su applicazioni in esercizio?
  - Ci sono utenti privilegiati che hanno creato e approvato nuove utenze e autorizzazioni sui sistemi?

La Sfida dell'Audit & Compliance



La sfida è misurare e visualizzare il comportamento delle persone sui sistemi e nell'accesso alle informazioni attraverso tutta l'enterprise senza inibire o degradare le performance del business

Persone

the Consul InSight™ Suite

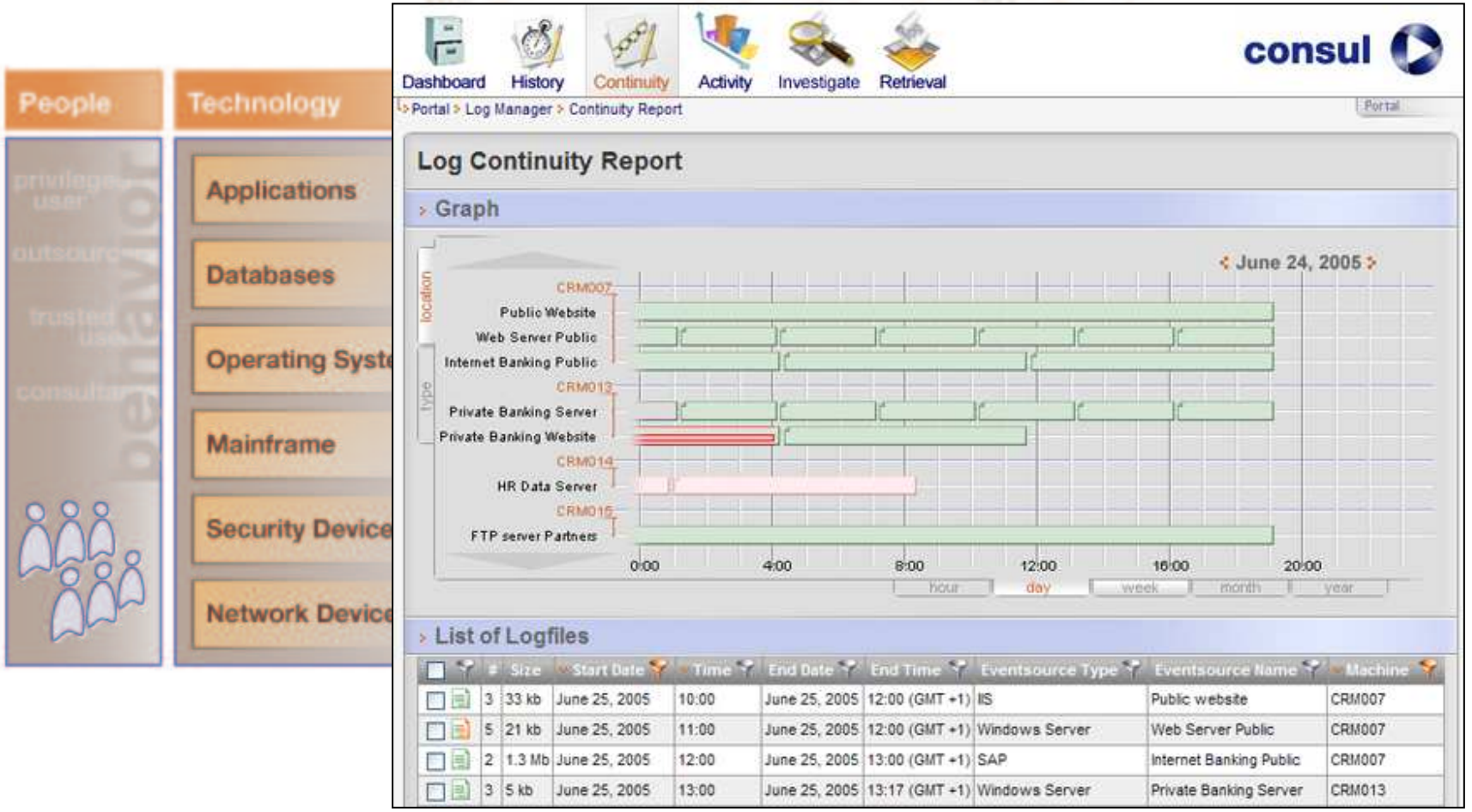
Tecnologie

the Consul InSight™ Suite

Collezionamento dei file di Log

the Consul InSight™ Suite

Log Continuity Report
the Consul InSight™ Suite



Benefici

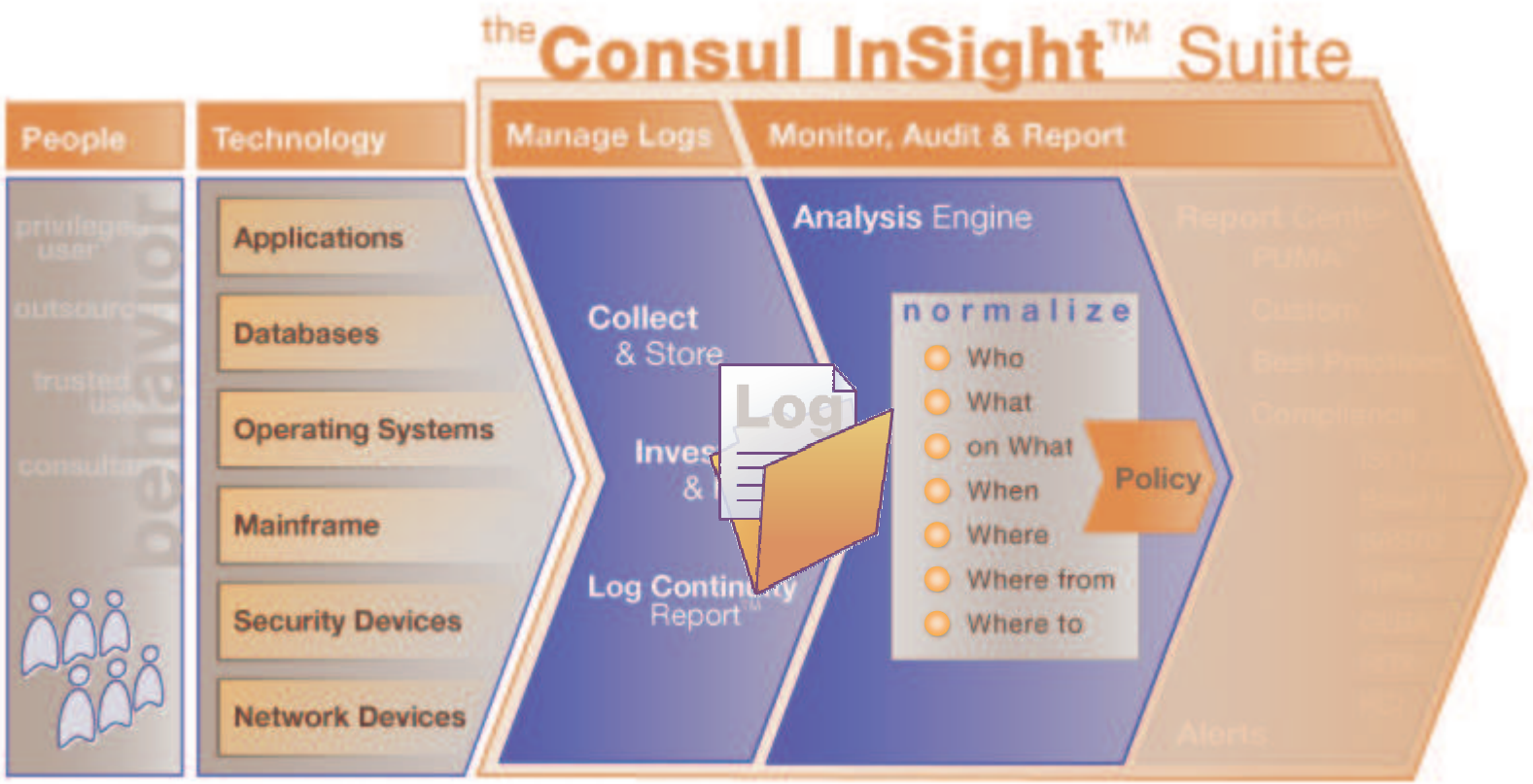
the Consul InSight™ Suite

Elimina le lunghe preparazioni per gli audit

Incrementa l'efficienza del team di audit

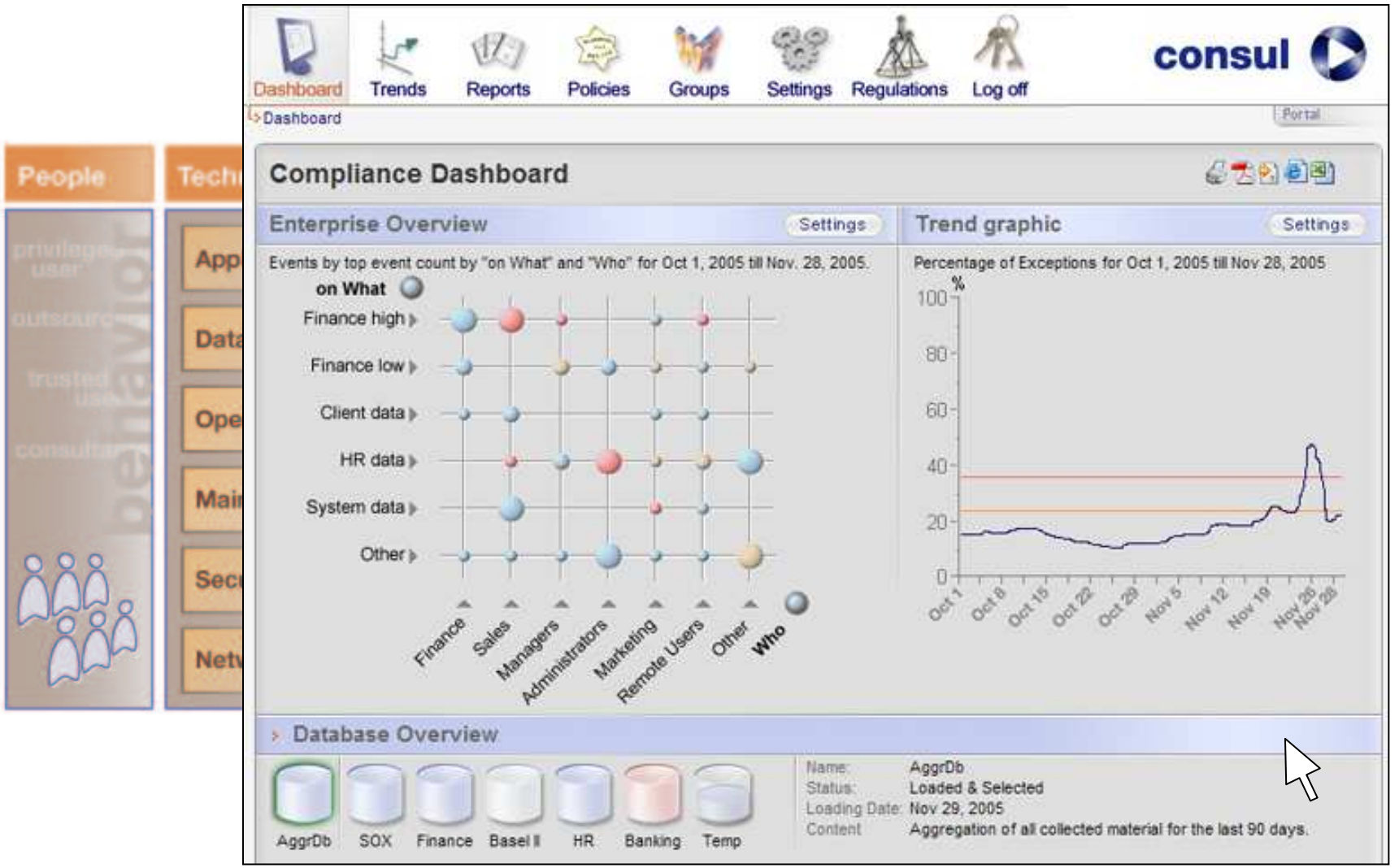
Soddisfazione degli auditor

Normalizzazione

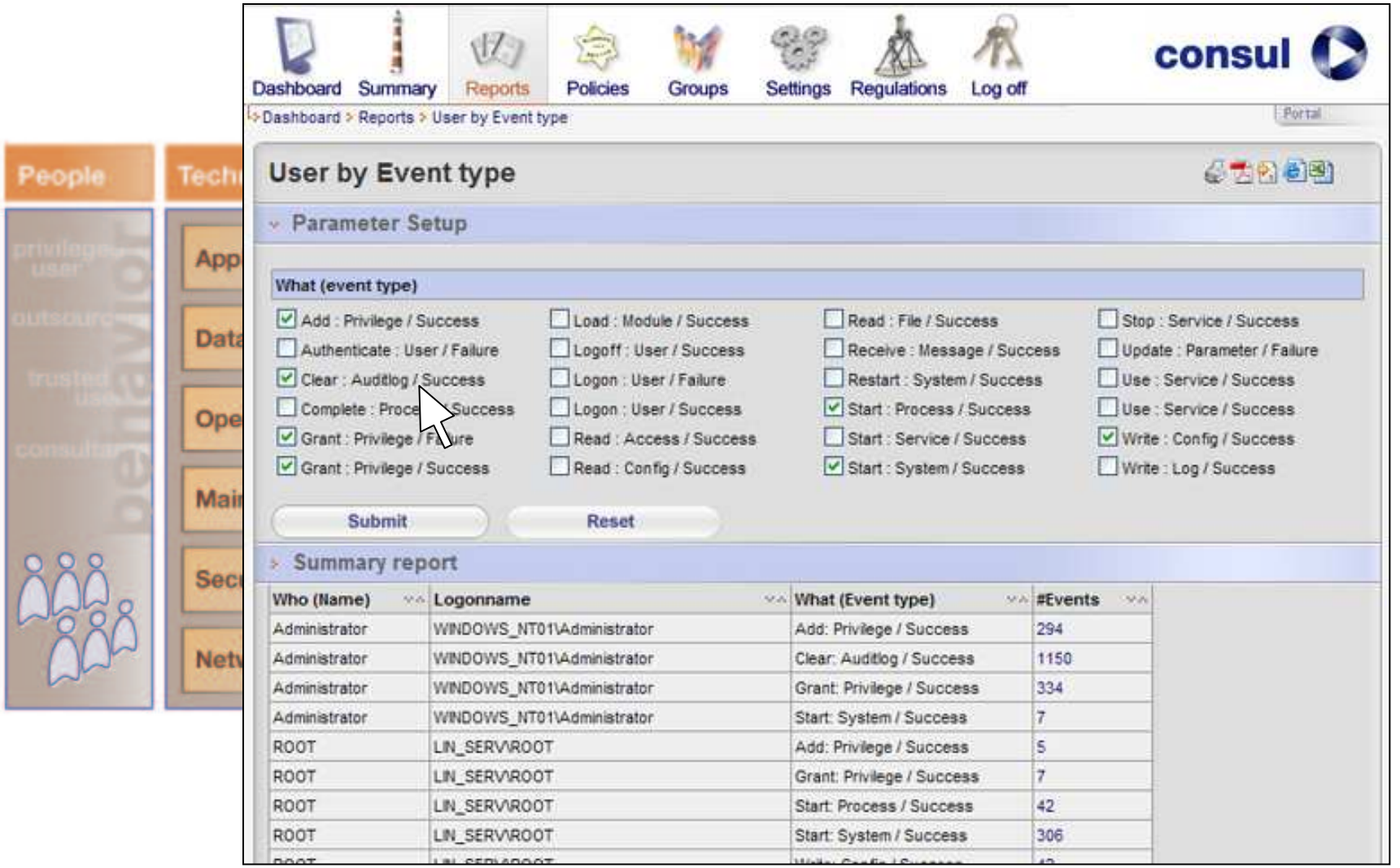


Report Center

Dashboard



Tipo di evento per utente

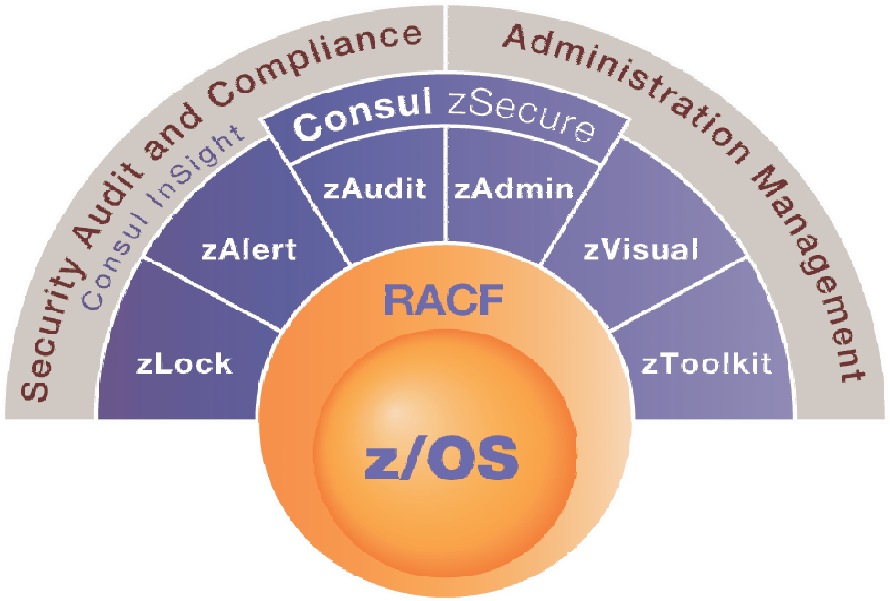


Dettagli sull'evento

Sommario Utente

Consul zSecure Suite

La suite Consul zSecure aggiunge strumenti user-friendly nel mainframe per facilitare l'amministrazione e fornire funzionalità di audit, alert e monitoring per z/OS Resource Access Control Facility (RACF)



Funzionalità chiave

- La suite zSecure migliora la sicurezza del mainframe, migliora l'efficienza dell'amministrazione e consente di far diventare il mainframe l'hub per la sicurezza dell'enterprise.
- **Amministrazione e provisioning:**
  - **zAdmin** facilita e velocizza l'amministrazione del RACF
  - **zVisual** offre una Windows GUI per RACF
  - **zToolkit** è l'intercazccia CICS based per l'amministrazione del RACF
- **Audit, monitoring e compliance:**
  - **zLock** assicura la compliance alle politiche della compagnia e procedure per prevenire comandi errati
  - **zAlert** strumento di monitoraggio real-time delle intrusioni e delle attività indesiderate
  - **zAudit** fornisce strumenti per il detection degli eventi, l'analisi, il report, l'integrità del sistema e l'audit

Benefici

- **Administratione e provisioning:**
  - Riduce il tempo, gli sforzi e i costi di amministrazione
  - Abilita un'amministrazione de-centralizzata
  - Tempi di risposta ridotti, facilitatori del business
  - Riduce il tempo di training necessario per i nuovi amministratori
- **Audit, monitoring e compliance:**
  - Passare audit più facilmente, migliorare la "posture" per la sicurezza
  - Risparmiare tempo e costi attraverso una migliorata gestione della sicurezza e degli incidenti
  - Incrementare l'efficienza operazionale

zSecure: Administration Management

- **zAdmin** – è lo strumento per facilitare e velocizzare l'amministrazione del RACF, evitando di usare faragginosi comandi nativi. zAdmin aggiunge un layer user-friendly sopra i tuoi RACF database. Attraverso questo software è possibile facilitare l'inserimento di comandi amministrativi, generare custom report ed eseguire clean-up di database.
- **zVisual** - è l'interfaccia grafica Windows based per l'amministrazione del RACF, di usare personale non specialistico o abilitare un'amministrazione centralizzata non basata su ISPF/TSO.
- **zToolkit** – Esegue semplici tak amministrativi da un ambiente CICS, liberando risorse con preziose competenze RACF da routine di amministrazione di base.

zSecure: Administration Management

Migliorare la sicurezza del mainframe	**C'è sempre una possibilità per una breccia nel tuo sistema di sicurezza, ma con zAdmin la tua aministrazione più pulita e protetta ridurrà questa probabilità.**
Ridurre i tempi di amministrazione	**Con zAdmin il tempo richiesto per eseguire task di sicurezza è tipicamente ridotto del 50-75% permettendo alle tue ridotte risorse esperte mainframe di focalizzarsi nel miglioramento della qualità della sicurezza.**
Accelerare i tempi di risposta	**Gli utenti in attesa per la creazione di nuove userid ed altri task amministrativi verranno serviti più rapidamente grazie a zAdmin.**
Eliminare la necessità di soluzioni fatte in casa	**Molte compagnie hanno realizzato soluzioni sviluppate in casa per applicare le politiche di sicurezza. Tali soluzioni spesso costano di più per la realizzazione e il mantenimento di quanto le compagnie riescono a realzizare. zAdmin elimina questi costi.**
Abilitare la decentralizzazione delle risorse	**Operatori di Helpdesk e amministratori non-RACF sono generalmente 20-40% più economici. Consul abilita la decentralizzazione dei task amministrativi con minore impatto per l'amminstrazione.**

zSecure: Audit & Compliance

- **zAudit** – Audit e monitoraggio per gli eventi di sicurezza in ambiente mainframe. Analisi automatica delle esposizioni rispetto alle politiche definite. zAudit fornisce report standard e personalizzati, allarmi real-time sulla violazione delle policy.
- **zAlert** – zAlert è uno strumento di monitoring real-time per le minacce di sicurezza in ambiente mainframe che va ben oltre ad un tradizionale sistema di Intrusion Detection poichè è in grado di bloccare le azioni come un vero sistema di Intrusion Pevention. Gli allarmi sono scritti in un linguaggio di reporting semplice da utilizzare (CARLa), dando ai clienti la possibilità di personalizzare il ”look and feel” delle e-mail e dei messaggi di testo da inviare a telefoni cellulari.
- **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.

Consul z/OS audit, monitoring e compliance

Passare gli audit e migliorare la sicurezza	**Avere i report che gli auditor e le regolamentazioni richiedono. Ridurre le possibilità di avere costose brecce di sicurezza attraverso una più sicura amministrzione del mainframe.**
Risparmiare tempi e costi	**zAudit può far risparmiare preziose ore-uomo necessarie per l'audit, la reportistica ed il clean-up dei database amministrativi. Realizzare significativi risparmi nell'utilizzo della CPU dovuti all'efficiente motore di reporting.**
Incrementare l'efficienza operazionale	**zAudit mostra quali JCL, parametri e moduli caricati sono stati cambiati, quindi riduce il downtime delle applicazioni causate da modifiche inaspettate o improprie.**
Velocizzare la reazione agli incidenti di sicurezza	**Grazie ai dettagli presenti nelle e-mail di alert gli amministratori possono muoversi più rapidamente per diagnosticare e rimediare a failure o esposizioni.**
Eliminare la necessità di soluzioni fatte in casa	**Riduce o elimina la necessità di applicazioni home-made per forzare la compliance.**

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Gracias
Spanish

Thank You
English

شكراً
Arabic

Obrigado
Brazilian Portuguese

多谢
Simplified Chinese

Danke
German

Grazie
Italian

Merci
French

நன்றி
Tamil

ありがとうございました
Japanese

감사합니다
Korean