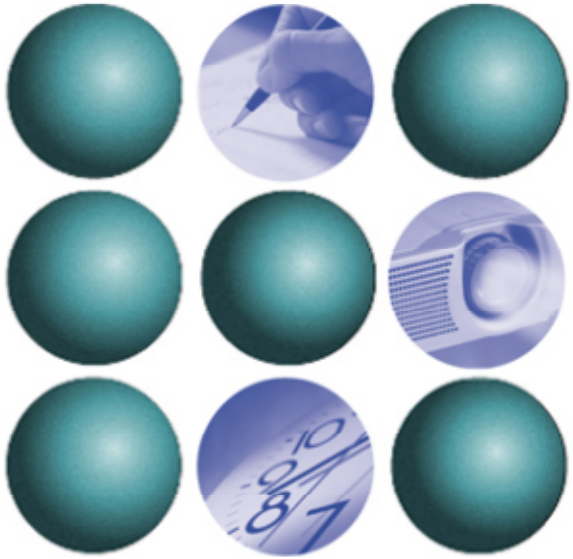


Központi **jogosultság-menedzsment** és **biztonsági felügyelet** megvalósítása nagy felhasználószámú, nagy fluktuációjú szervezeteknél

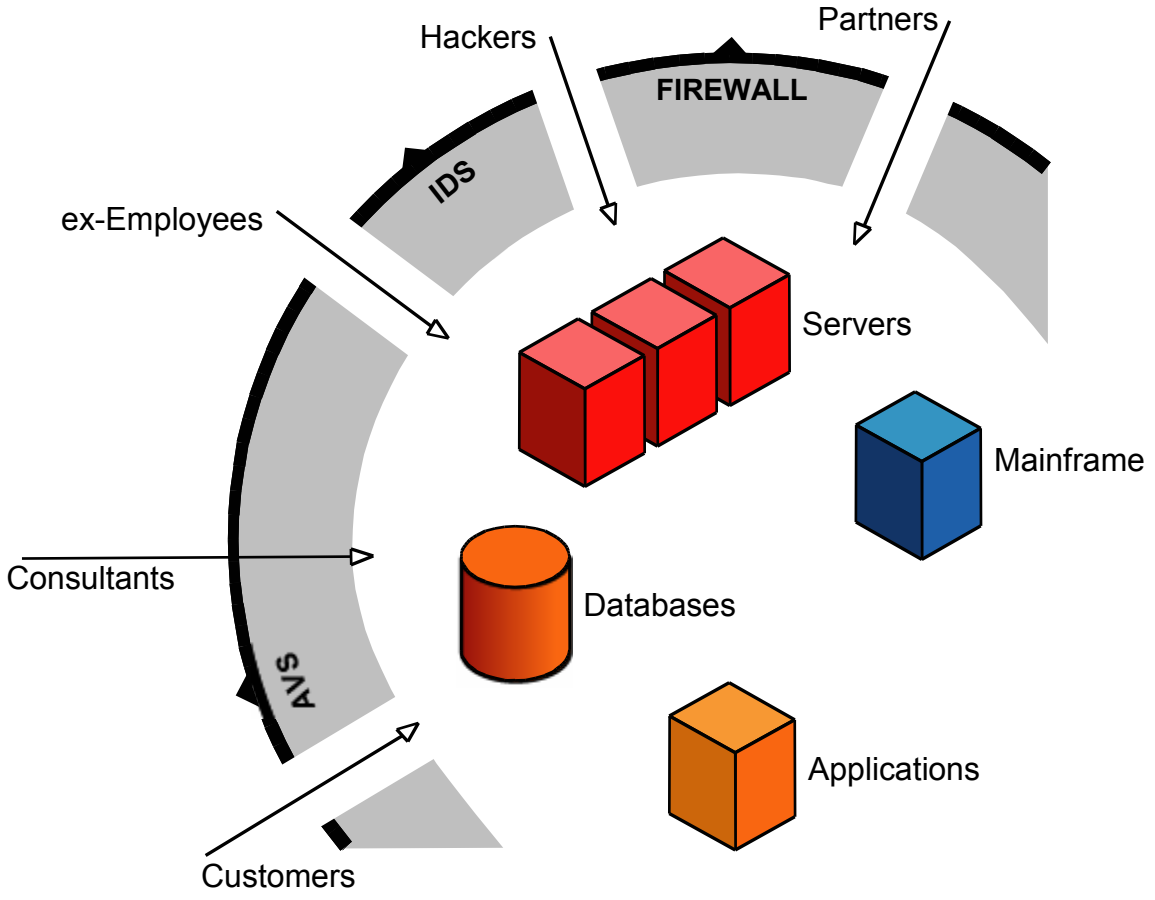
Bartos Zoltán Balázs
bartos.balazs@kfki-lnx.hu

Agenda

- **Miért van szükség jogosultság-menedzsmentre?**
- BMC Control-SA – egy lehetséges megvalósítás
- Control-SA/PassPort – bízzuk a felhasználóra!
- InSight for Control-SA – teljes körű biztonsági felügyelet

A hálózati perem lassan eltűnik

- Nincs többé zárt belső hálózat
- Extranet
- Web szolgáltatások
- Wireless
- Dial-up
- VPN



Az egész informatikai rendszert felügyeljük, vagy csak a határvonalát?

Bevezetés – az Identity Managementről

Identity Management (Jogosultság- vagy hozzáférés menedzsment)

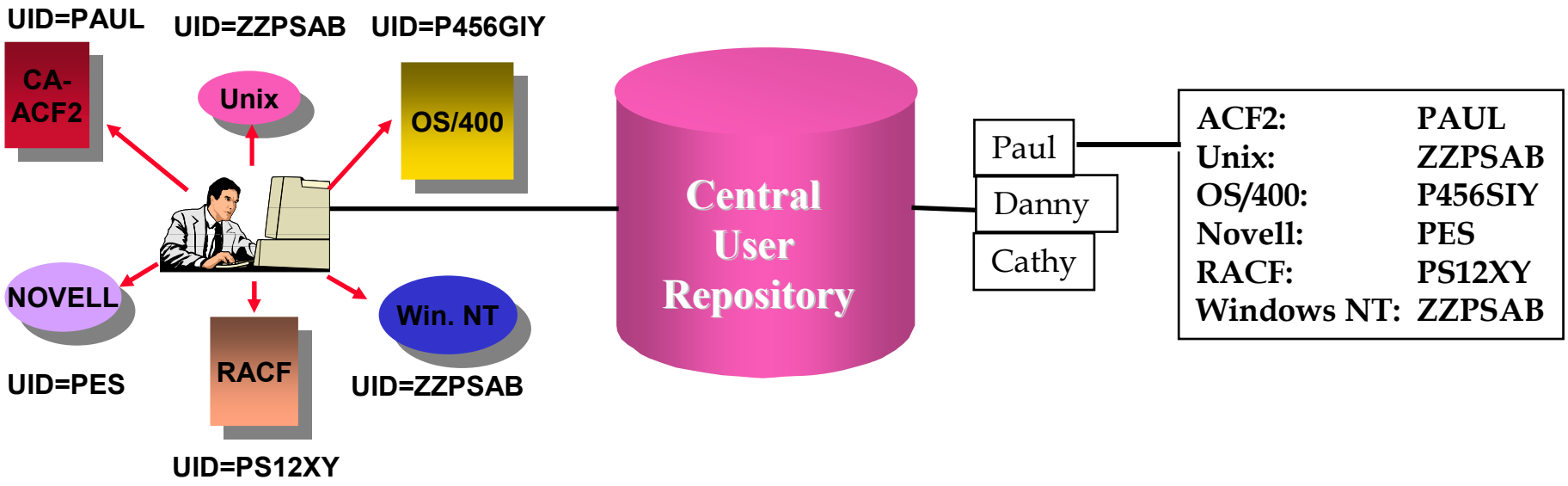
– Felhasználói **hozzáférések** és **jogosultságok** központosított, egységes kezelése heterogén környezetben.

– Hozzáférések központi →
- Létrehozása
- Módosítása
- Megszűntetése

– Felhasználók által önállóan elvégezhető tevékenységek bővítése (password-reset, hozzáférés igénylés).

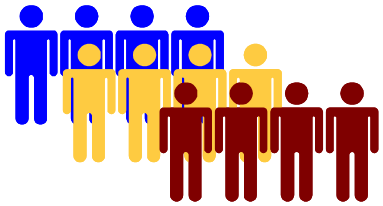
Felhasználók és jogosultságok

- Központi felhasználói adattárház:
  - Felhasználói adatok összevont megjelenítése
  - Átlátható kapcsolat az emberek és a hozzáféréseik között
  - Belső ellenőrzések megkönnyítése



Miért szükséges a hozzáférés-menedzsment?

- **Nagy számú** felhasználó a rendszerben.
- **Heterogén** környezet – különféle platformok, külön felügyelettel.



- Sok újonnan érkező / távozó felhasználó.
- Új felhasználói hozzáférés minél gyorsabban.

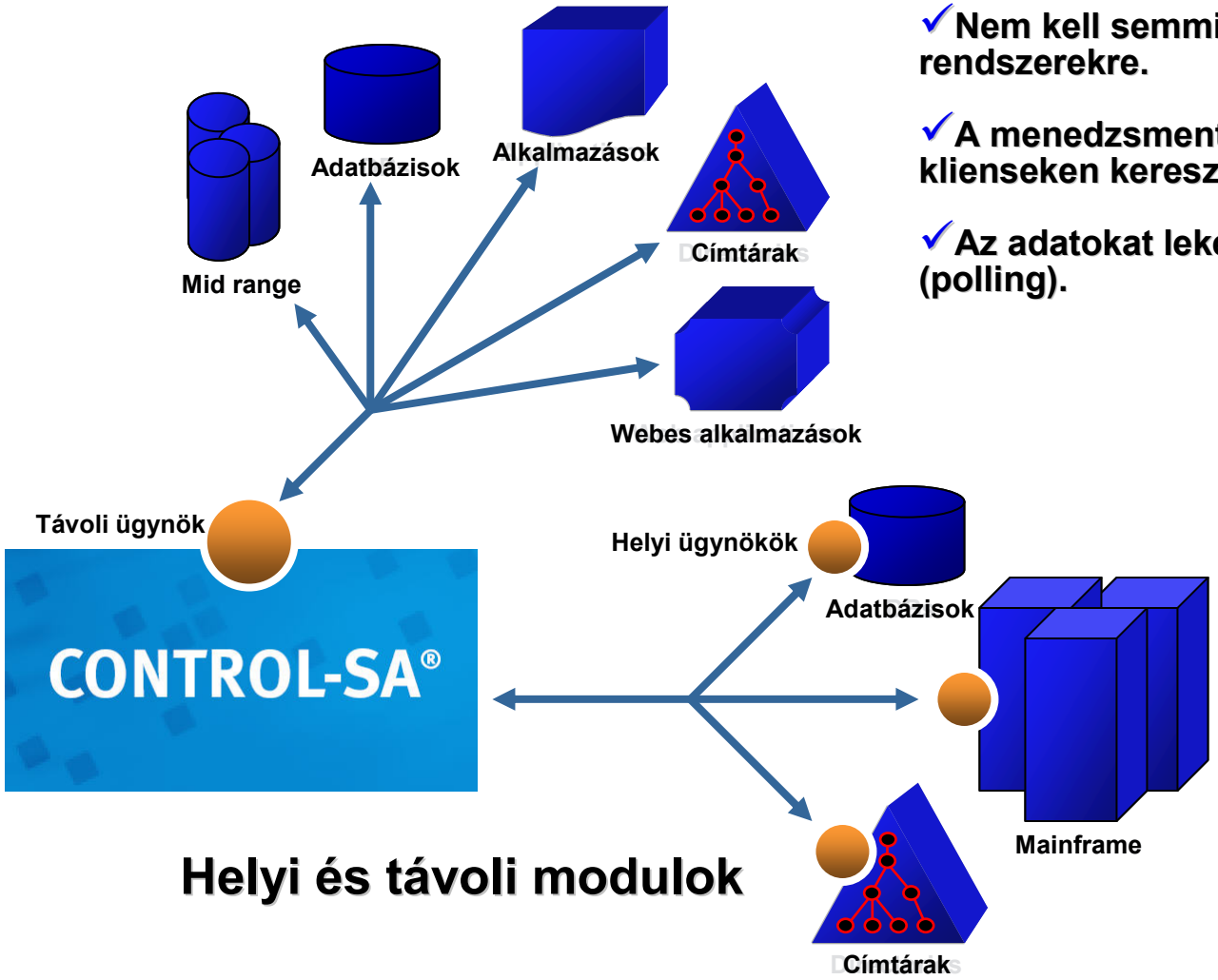
Agenda

- Miért van szükség jogosultság-menedzsmentre?
- **BMC Control-SA – egy lehetséges megvalósítás**
- Control-SA/PassPort – bízzuk a felhasználóra!
- InSight for Control-SA – teljes körű biztonsági felügyelet

A Control-SA jellemzői

- Felhasználói hozzáférések **automatizált** kialakítása.
- **Munkakörhöz** rendelt jogosultság-kiosztás.
- A biztonsági házirend **központi felügyelete**.
- Jelszavak összehangolása.
- Központi riasztás felügyelet.
- **Visszakereshető** biztonsági beállítások és módosítások.
- Fejlett **jelentéskészítés.**
- Egységes felhasználói felület.

A BMC Control-SA modell



Helyi és távoli modulok

Távoli menedzsment

- ✓ Nem kell semmit telepíteni a menedzselt rendszerekre.
- ✓ A menedzsment távolról, vagy alkalmazás-klienseken keresztül történik.
- ✓ Az adatokat lekérdezés útján nyeri ki (polling).

Lokális menedzsment

- ✓ Agent szoftver telepítése a menedzselt rendszerekre.
- ✓ Az agent szoftver a központi rendszer kiterjesztése
- ✓ A változásokat azonnal észleljük.

Lokális menedzsment agent szoftver telepítésével

A megoldás előnyei:

•Valós idejű, kétirányú menedzsment – a központi és a lokális felhasználói adatbázis konzisztens .

•Riasztási lehetőség a biztonsági szabályok megsértésekor.

•Hálózatkimaradás esetén a lokális agent szoftverek továbbra is működnek, helyreállás után adatszinkronizáció.

•Titkosított hálózati forgalom (3DES), csökkentett hálózati terhelés

Hátrányok:

•Időigényesebb az implementáció (telepítés minden rendszerre)

•A helyi agent szoftverek lefoglalják a rendszer erőforrásainak egy kis részét (tapasztalat: 1-3%)

CONTROL-SA Agent szoftverek

- Mainframe
  - RACF
  - CA-ACF2
  - CA-Top Secret
  - VM:Secure
- Network Systems
  - Win NT Server
  - Win 2K A.D.
  - Novell/Netware
  - OS/2 LAN Server
  - LDAP
  - Netscape / iPlanet
  - Netscape NDS
- UNIX
  - Sun/Solaris NCR
  - IBM/AIX
    SGI/IRIX
  - HP-UX Digital Unix
  - NIS Tru64
  - Linux
- Midrange
  - AS400
  - VMS
  - TANDEM

CONTROL-SA Agent szoftverek

- Informix
- Oracle
- Oracle Apps.
- Sybase
- Lotus Notes
- MS-Exchange
- MS-SQL
- Oracle Applications
- SAP/R3
- PeopleSoft
- *Tivoli Access Mgr for eBusiness
- *CA-eTrust Access Cont. & SSO
- Netegrity Sitminder
- Cisco Secure
- DB2
- Entrust/PKI
- Netscape Enterprise Server
- Proxima SSO
- ACE/Server
- SeOS
- Tandem Safeguard
- * Novell GroupWise

** Tanúsított BMC MarketZone partner fejlesztése*

Távoli menedzsment

A megoldás előnyei:

- Egyszerű, gyors implementáció.
- Jó megoldást nyújthat, ha különböző korlátozások miatt nem engedélyezik egy platformra az agent szoftver telepítését.

Hátrányok:

- Adatkonzisztencia (polling) – hálózatkimaradás esetén a változások csak később jutnak érvényre.
- Hálózati terhelés megnövekedhet.
- Biztonsági kérdések – hogyan érzékeljük a szabálysértéseket?
- Gondoskodni kell a hálózati forgalom biztonságáról

Távoli menedzsment – támogatott rendszerek

•LDAP

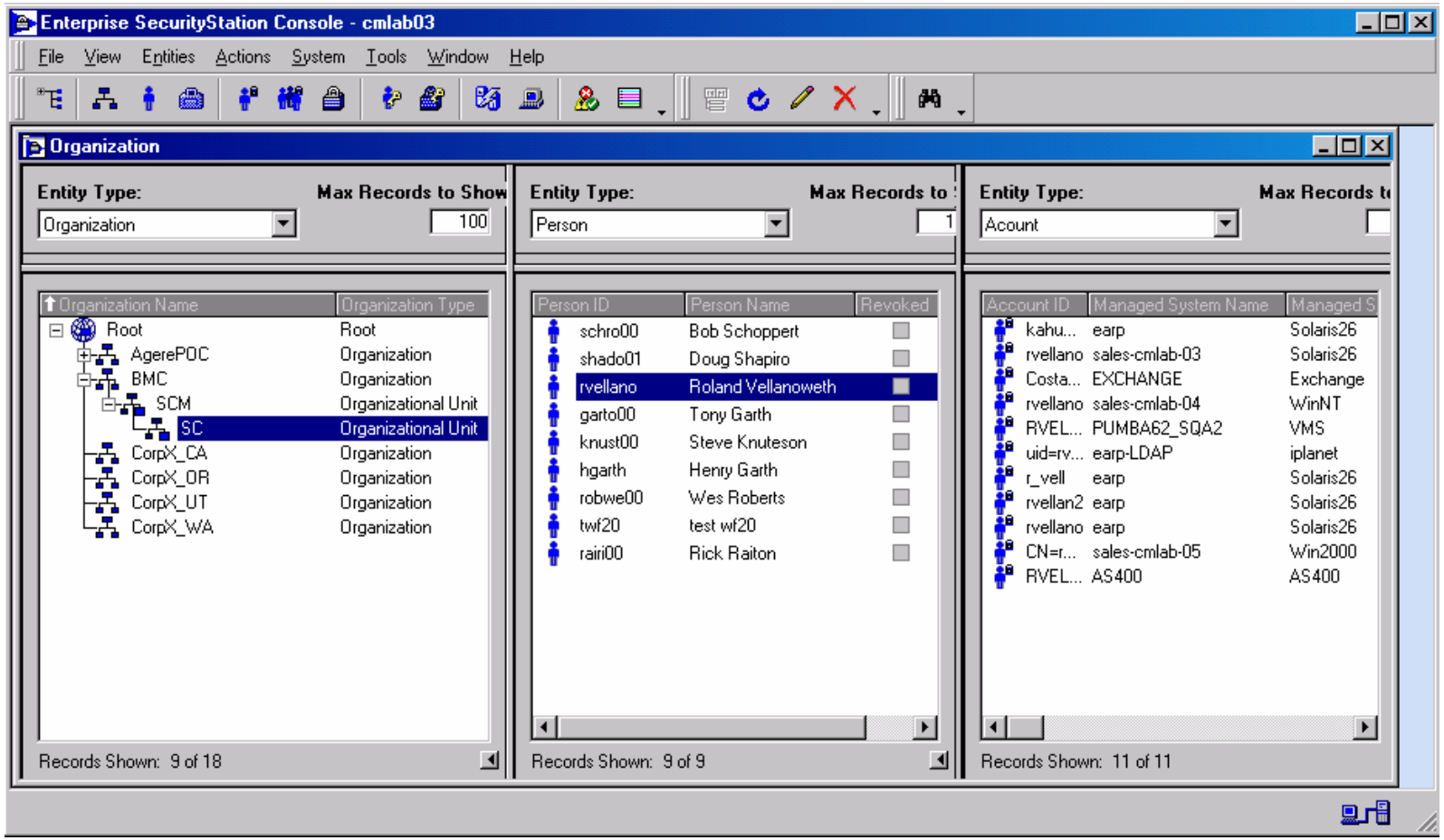
•Adatbázisok – Oracle, Sybase, DB2, Informix, MS-SQL – A Control-SA agentek az adatbázis kliensekkel egy gépre települnek – menedzsment az adatbázis klienseken keresztül.

•Egyéb támogatott rendszerek kliens-szerver alapokon:
- – Lotus Notes
- – SAP R/3
- – PeopleSoft
- – Exchange
- – Entrust
- – Oracle Applications
- – Netware
- – etc.

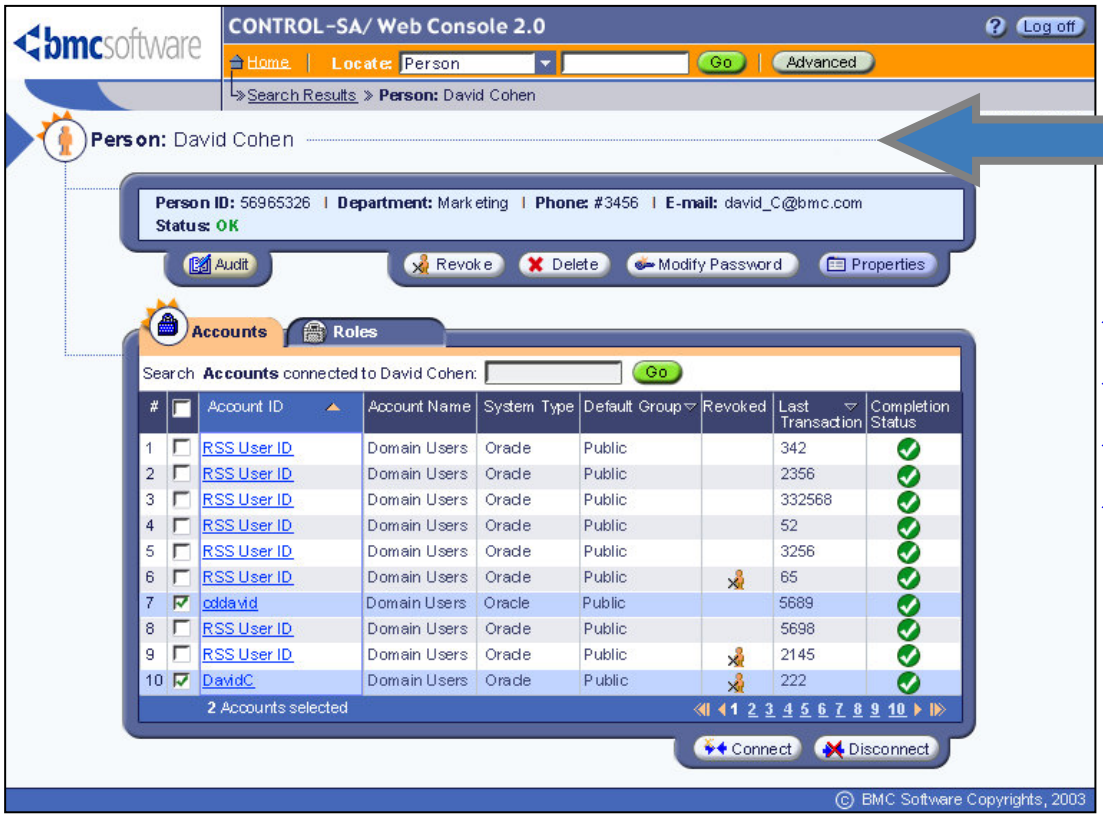
•Windows A.D.
•WinNT Server / Workstation
•Unix

CONTROL-SA Adminisztrátori nézet

- Enterprise SecurityStation Console GUI version 3.8



CONTROL-SA Webes felület



CONTROL-SA®

- ✓ Adminisztráció böngészőn keresztül.
- ✓ Gyorsabb implementáció.
- ✓ Nem szükséges konzolt telepíteni.
- ✓ Bármelyik PC-ről elérhető.

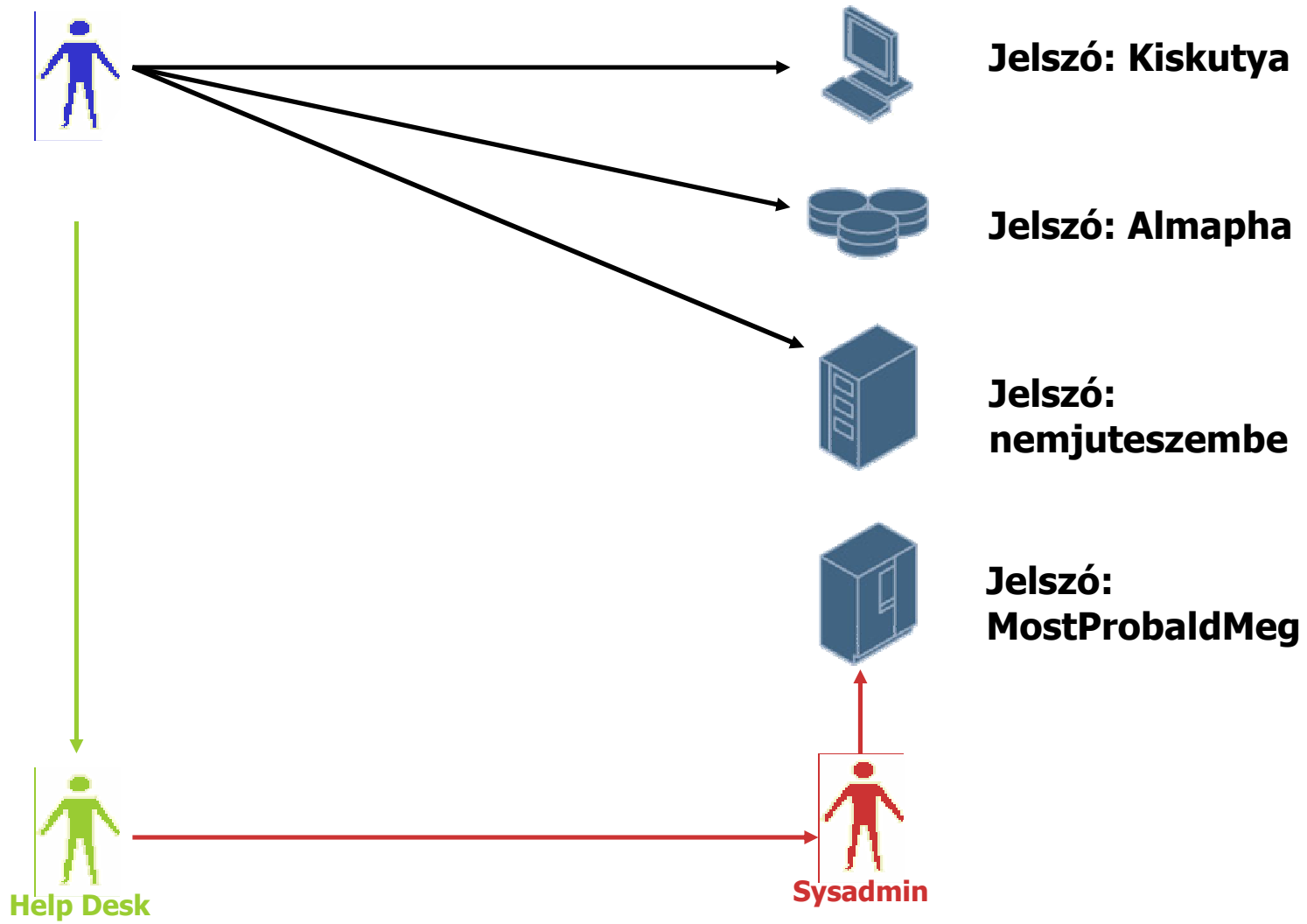
Architektúra:

- **OS: Solaris a központi szerver (ESS) alatt**
- **Web szerver: Tomcat**
- **Támogatott böngészők: IE 5.5 felett**
- **JAVA alapú fejlesztés**

Agenda

- Miért van szükség jogosultság-menedzsmentre?
- BMC Control-SA – egy lehetséges megvalósítás
- **Control-SA/PassPort – bízzuk a felhasználóra!**
- InSight for Control-SA – teljes körű biztonsági felügyelet

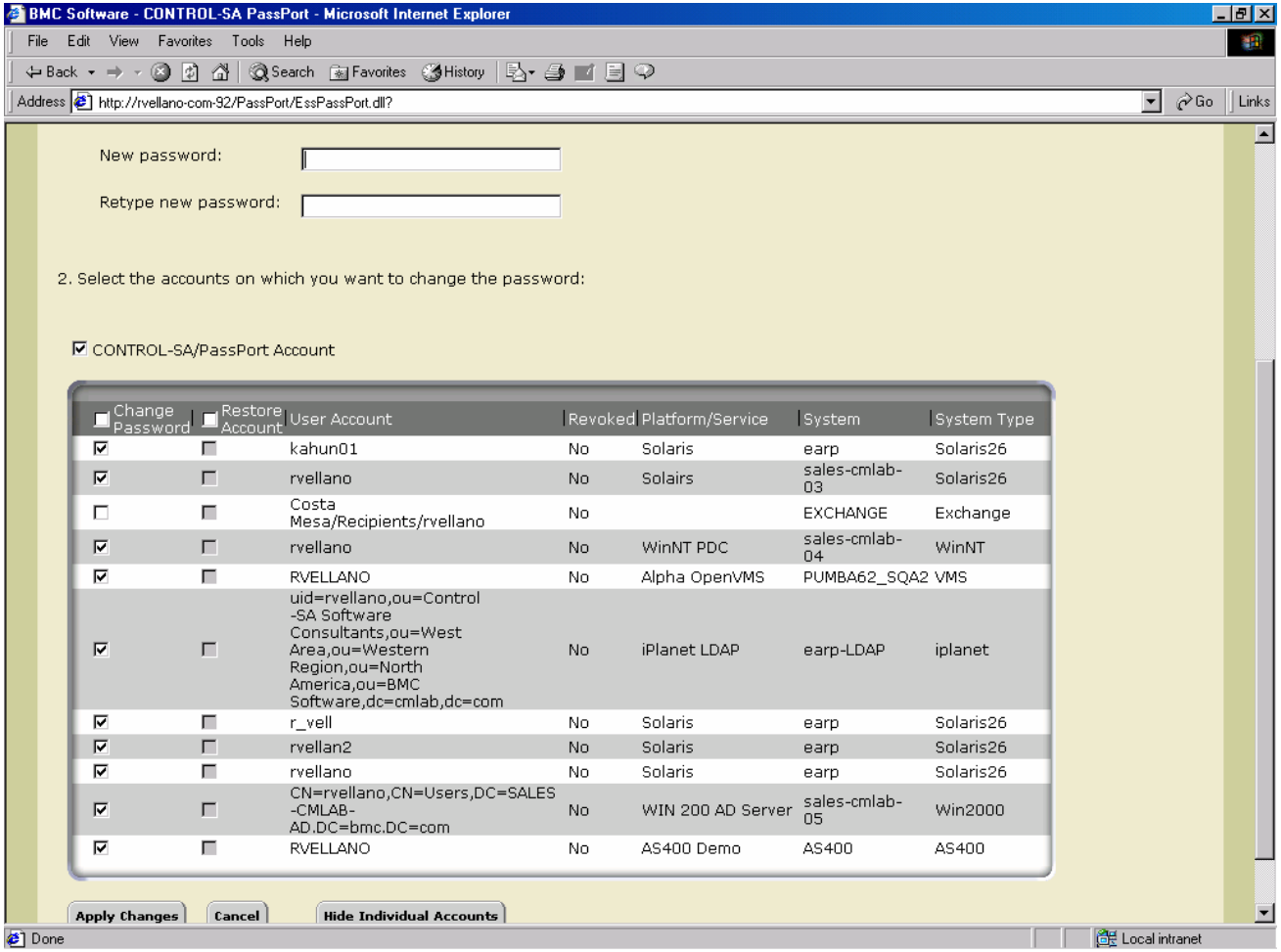
Miért van gond a jelszavakkal?



CONTROL- SA/PassPort

- Lehetővé teszi az „átlagos” felhasználó számára is:
  - Kezdeti regisztráció a PassPort rendszerbe.
  - „Jelszó reset” kezdeményezése.
  - Bejelentkezés a PassPort rendszerbe „kérdés/válasz” jellegű authentikációval.
  - Testreszabott „kérdés/válasz” információk feltöltése.

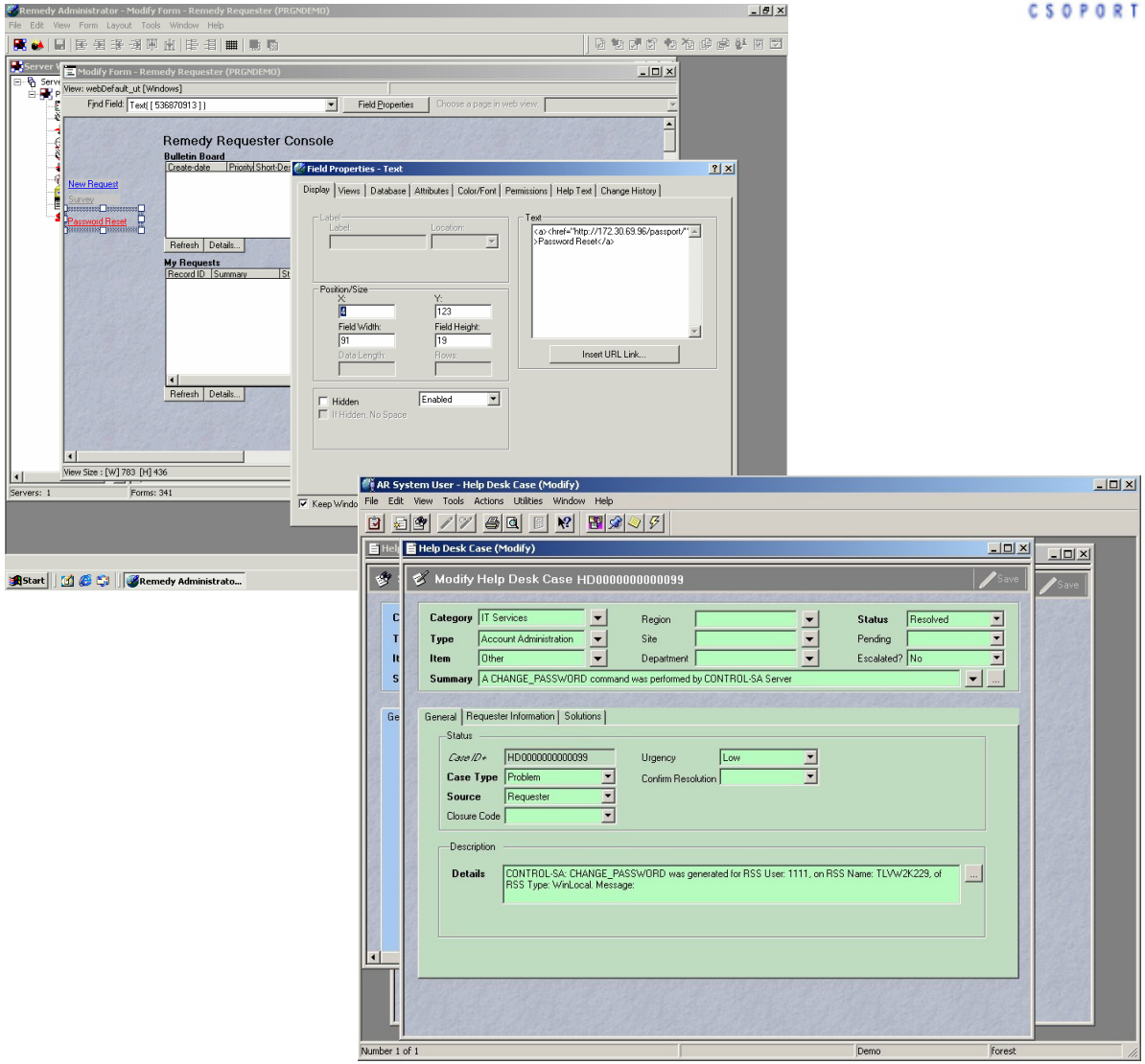
A PassPort webes felülete



További lehetőségek

›Remedy Help Desk integráció

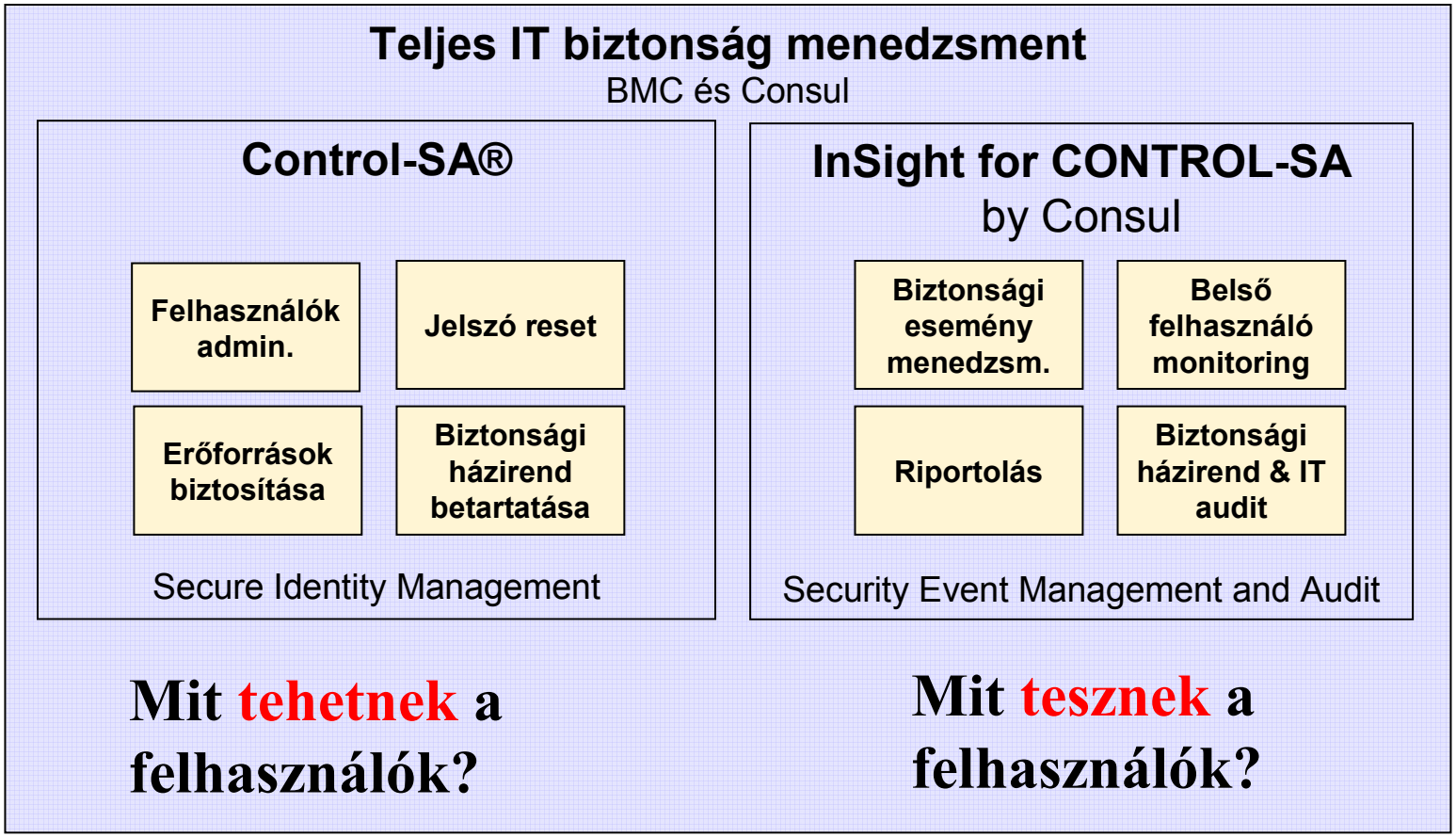
- Automatikus ticket készítés, a reset érvényességének ellenőrzésére.
- Ha nem sikerült a jelszó reset, figyelmeztető ticket készül.



Agenda

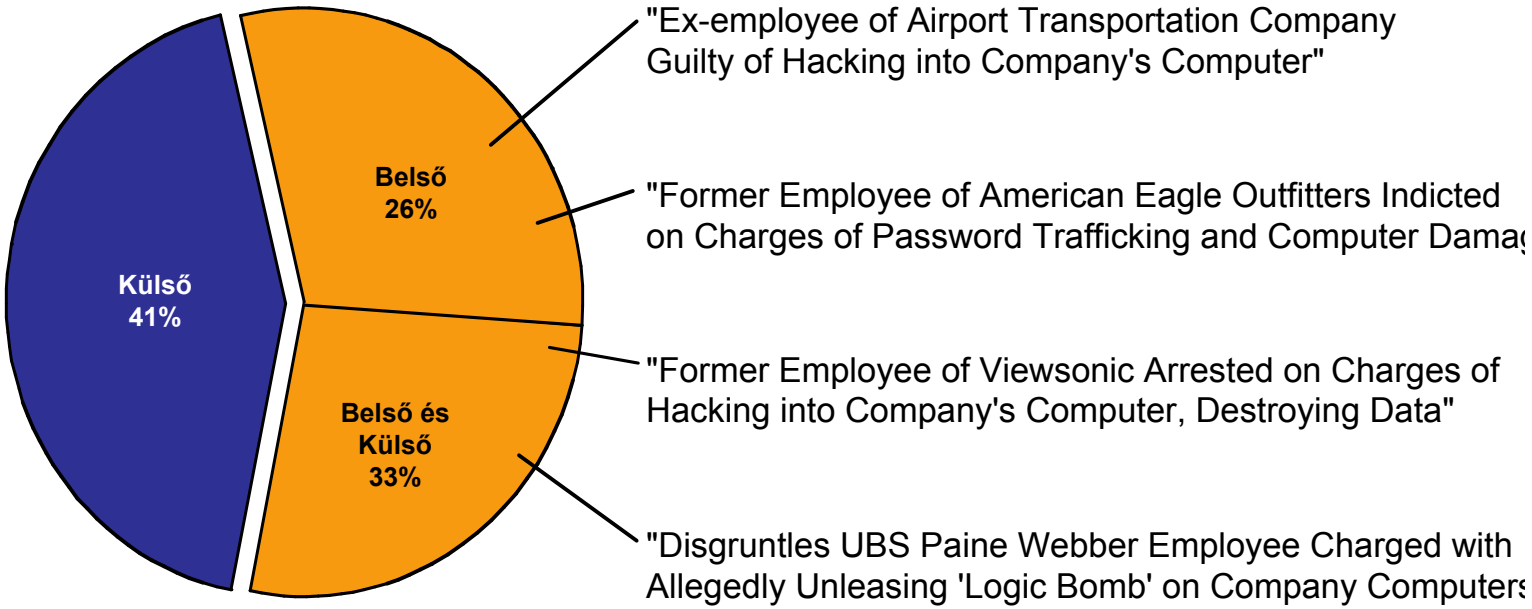
- Miért van szükség jogosultság-menedzsmentre?
- BMC Control-SA – egy lehetséges megvalósítás
- Control-SA/PassPort – bízzuk a felhasználóra!
- **InSight for Control-SA – teljes körű biztonsági felügyelet**

A teljes IT biztonság menedzsment



A „Megbízható Felhasználó” veszélye

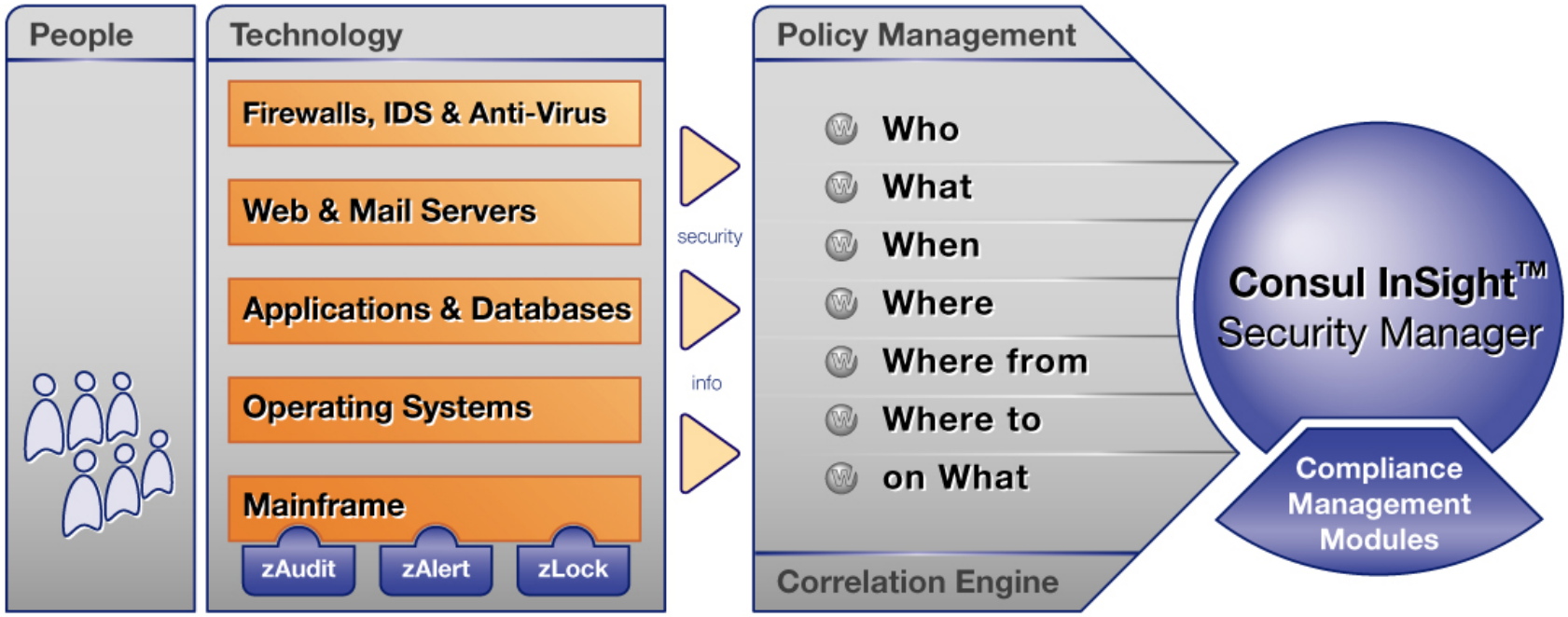
Hálózati támadások forrásai



Forrás:Global Security Survey 2003, Deloitte Touche Tohmatsu

A külső támadások problémákat okozhatnak; a belső támadások tönkretehetik a szervezetet.

InSight for Control-SA by Consul

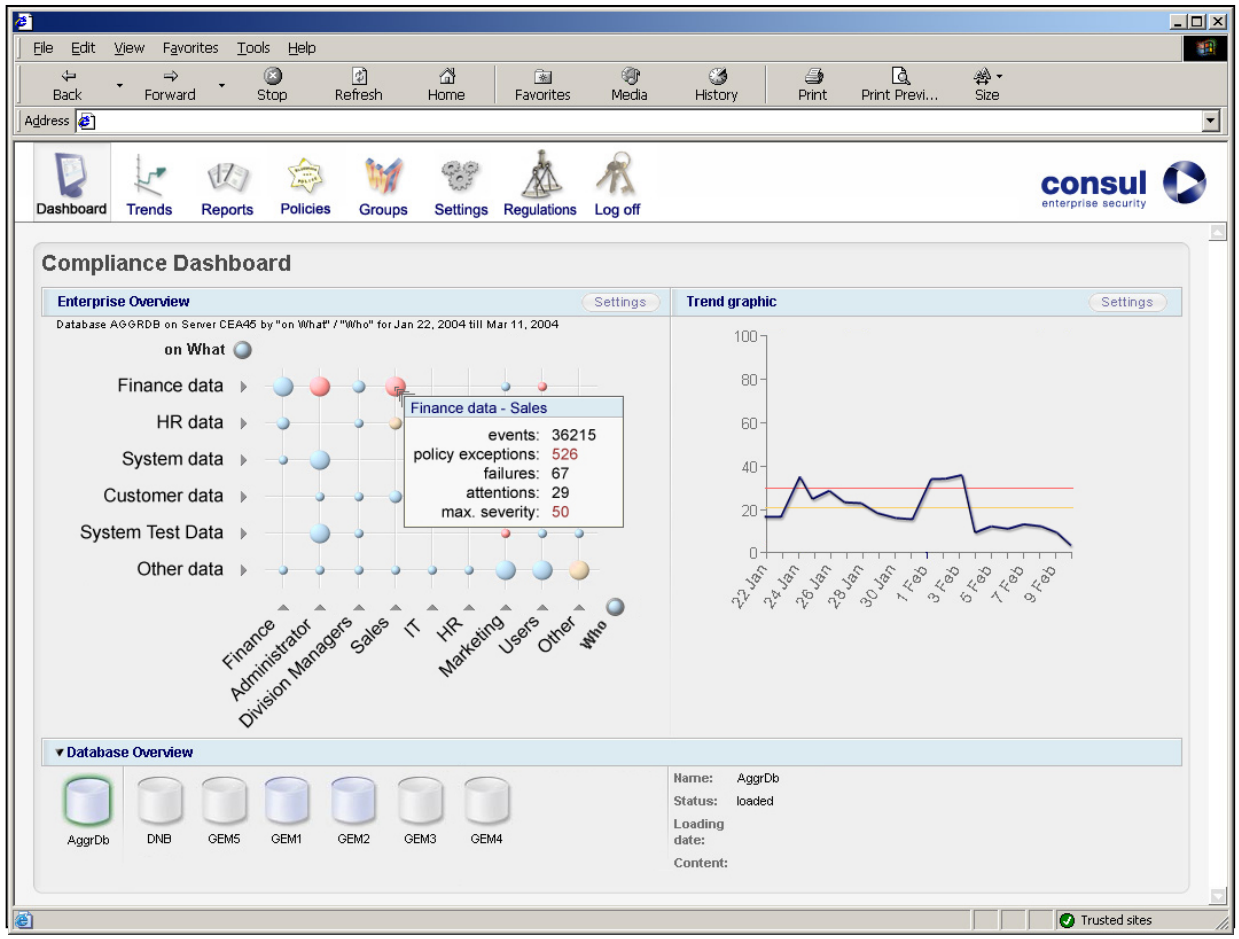


Cél: az IT üzemeltetési és a biztonsági feladatkörök és felelősségek egyértelmű szétválasztása.

Helyi feljegyzések vs. Központi adatgyűjtés

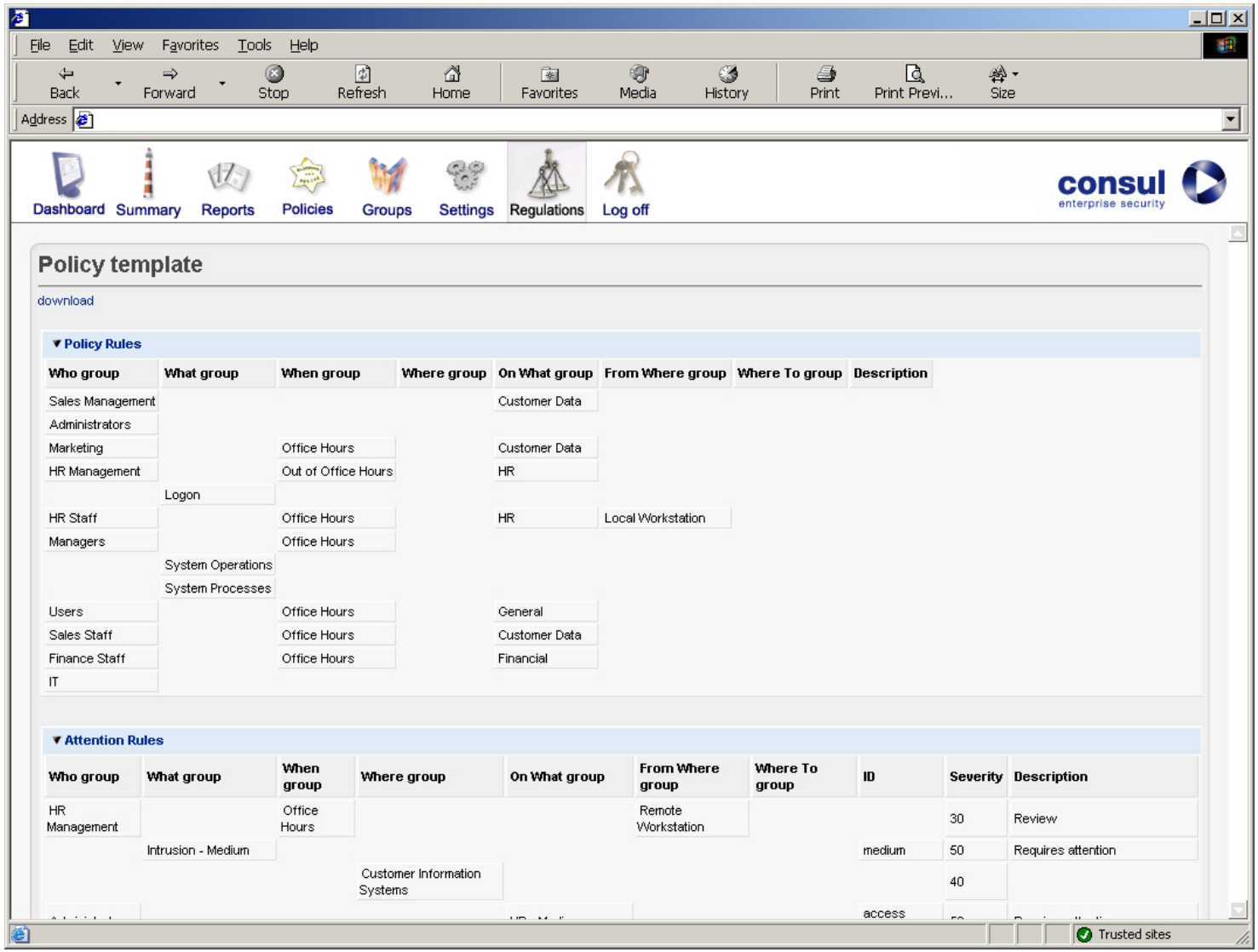
• Lokális megoldás		• Centrális megoldás:
– Csak homogén környezetben	→	– Tetszőleges számú és típusú platformon
– Nagy, gyakran kezelhetetlen adattömeg	→	– Könnyen definiálható szűrési feltételek
– A feljegyzések törölhetőek	→	– Központi tárolás akár évekig
– Reaktív beavatkozás	→	– Proaktív monitorozás és beavatkozás
– IT üzemeltetés részéről erőforrásigény	→	– Üzemeltetés és biztonság szétválasztása
– A felelősség homályos és nehezen bizonyítható	→	– A felelősség egyértelmű és bizonyítható

Az InSight jellemzői

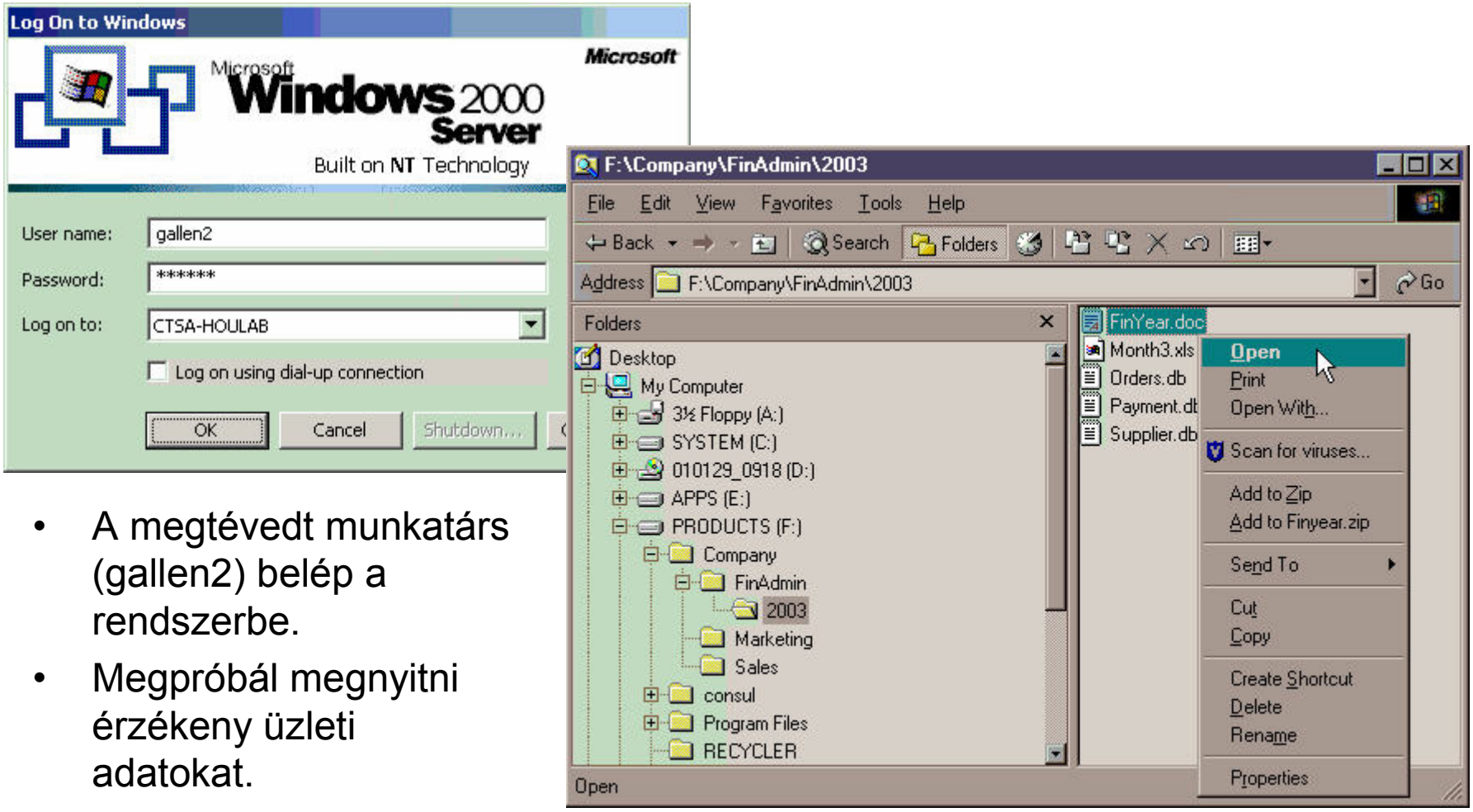


- A biztonsági naplóbejegyzések központi összegyűjtése, rendszerezése és kiértékelése.
- Események közötti összefüggések (Correlation Engine).
- Egyszerű, áttekinthető kezelőfelület.
- Valós idejű riasztás és közbeavatkozás (Control-SA).
- Utólagos vizsgálatok, audit, jelentéskészítés.

Biztonsági házirend definiálása

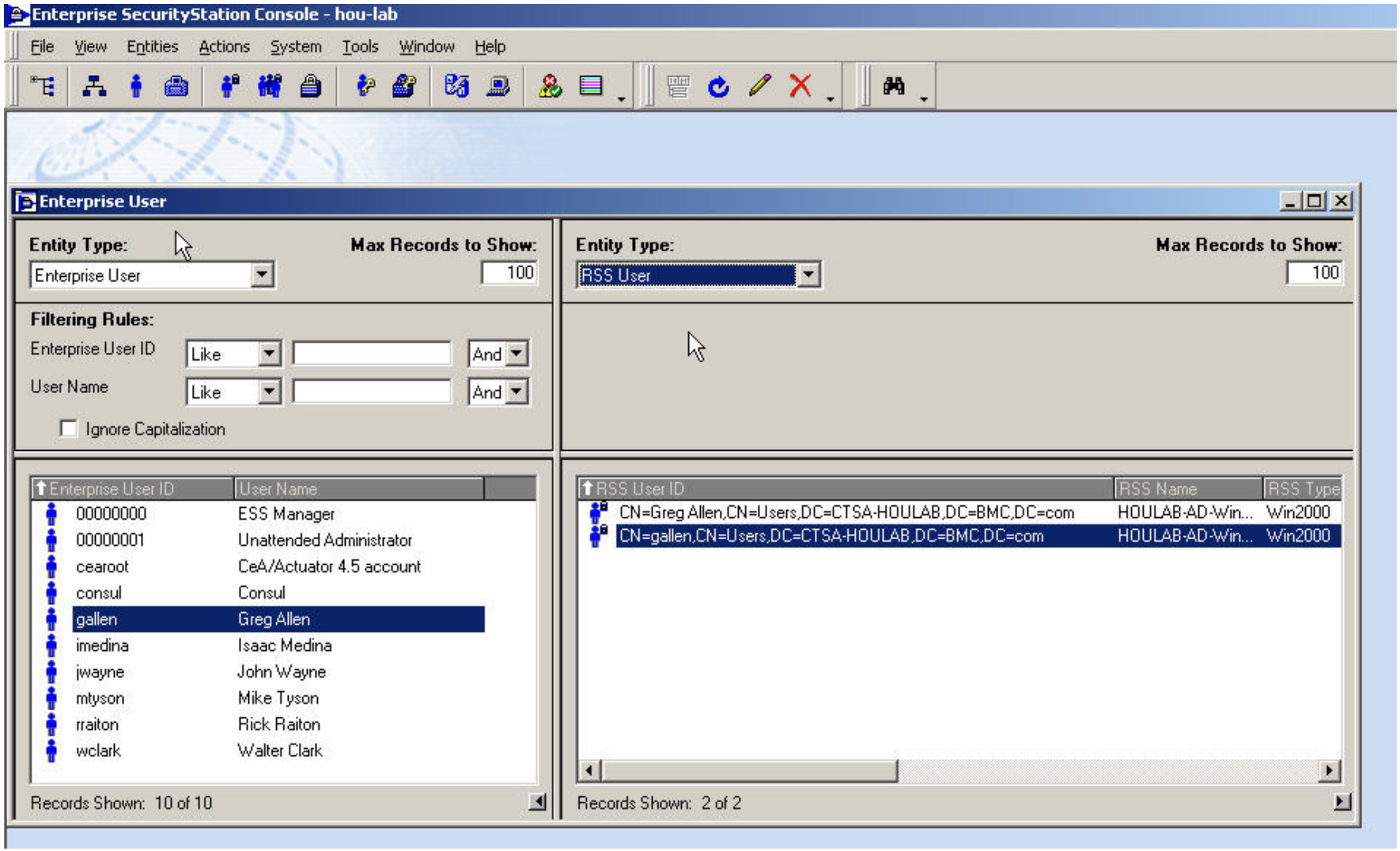


Az InSight működés közben (1.)



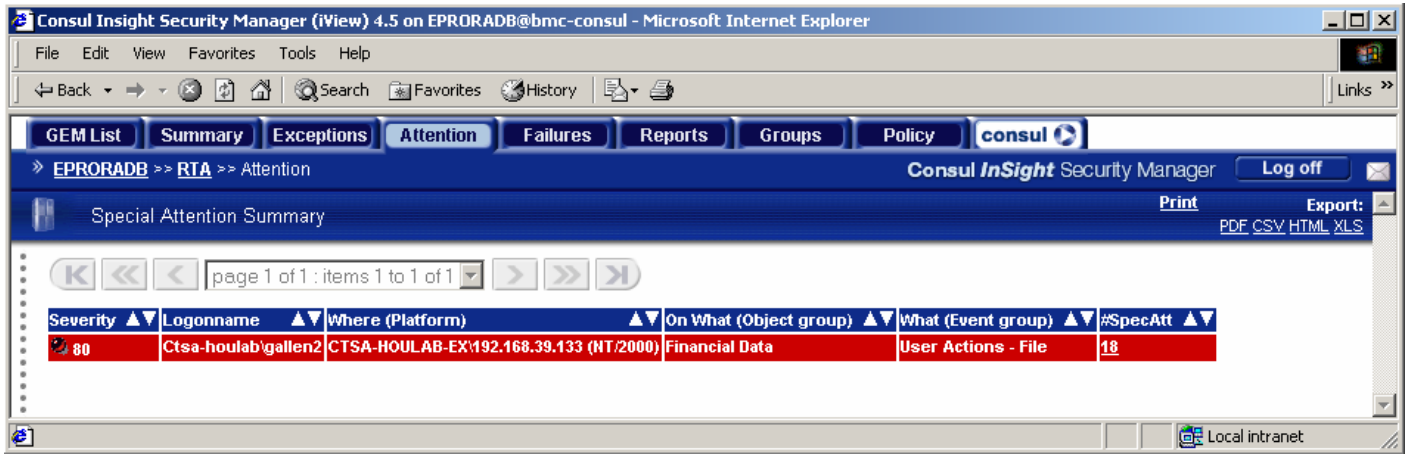
- A megtévedt munkatárs (gallen2) belép a rendszerbe.
- Megpróbál megnyitni érzékeny üzleti adatokat.

Az InSight működés közben (2.)

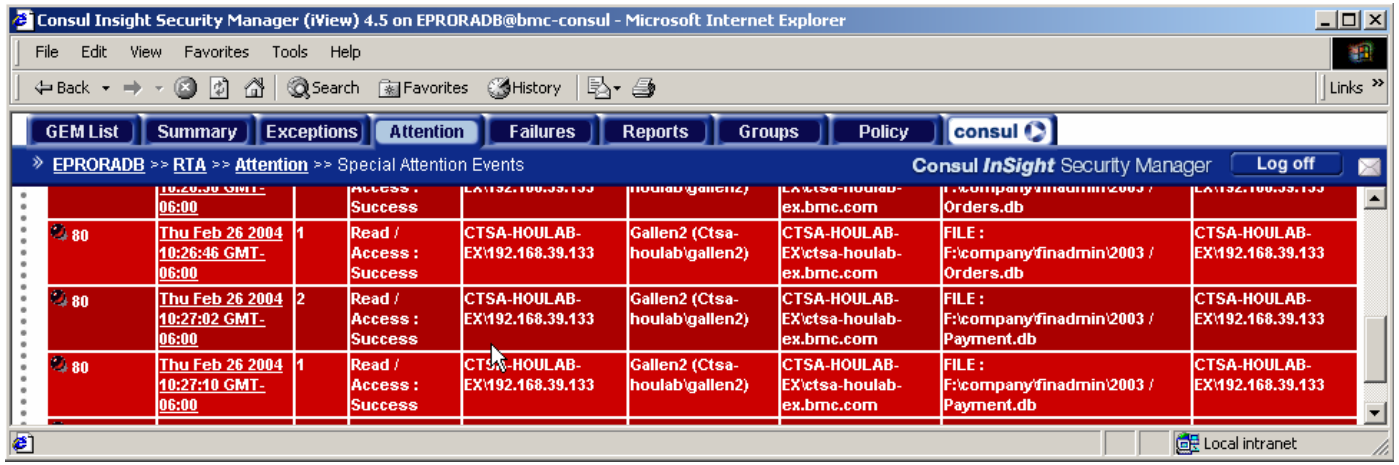


Az InSight működés közben (3.)

- Az InSight szerver érzékeli a szabálysértést és riasztást generál.

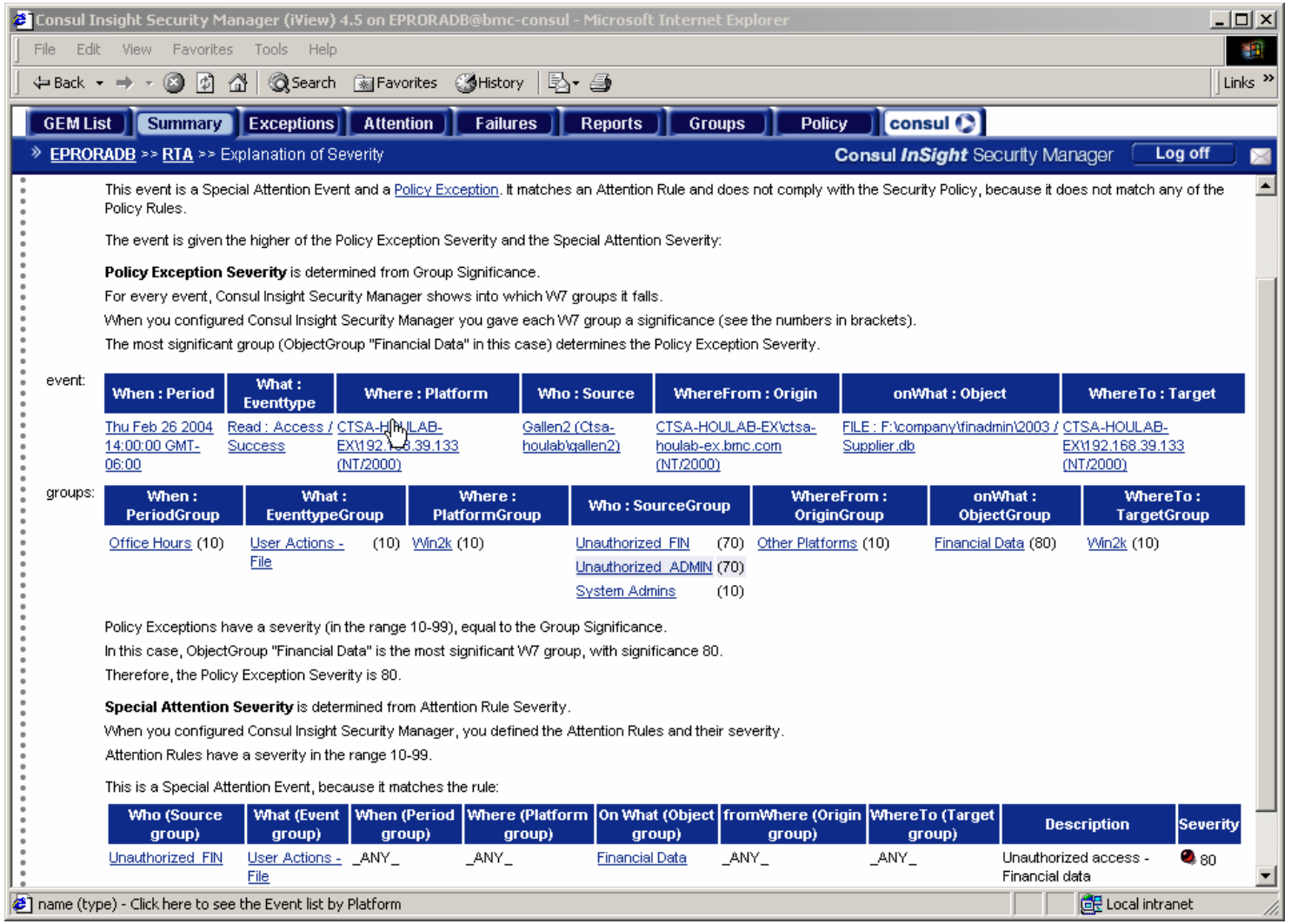


- Mivel *gallen2* munkaköre alapján számára tilos ezekhez az adatokhoz hozzáférni, ezért súlyos riasztás történik.



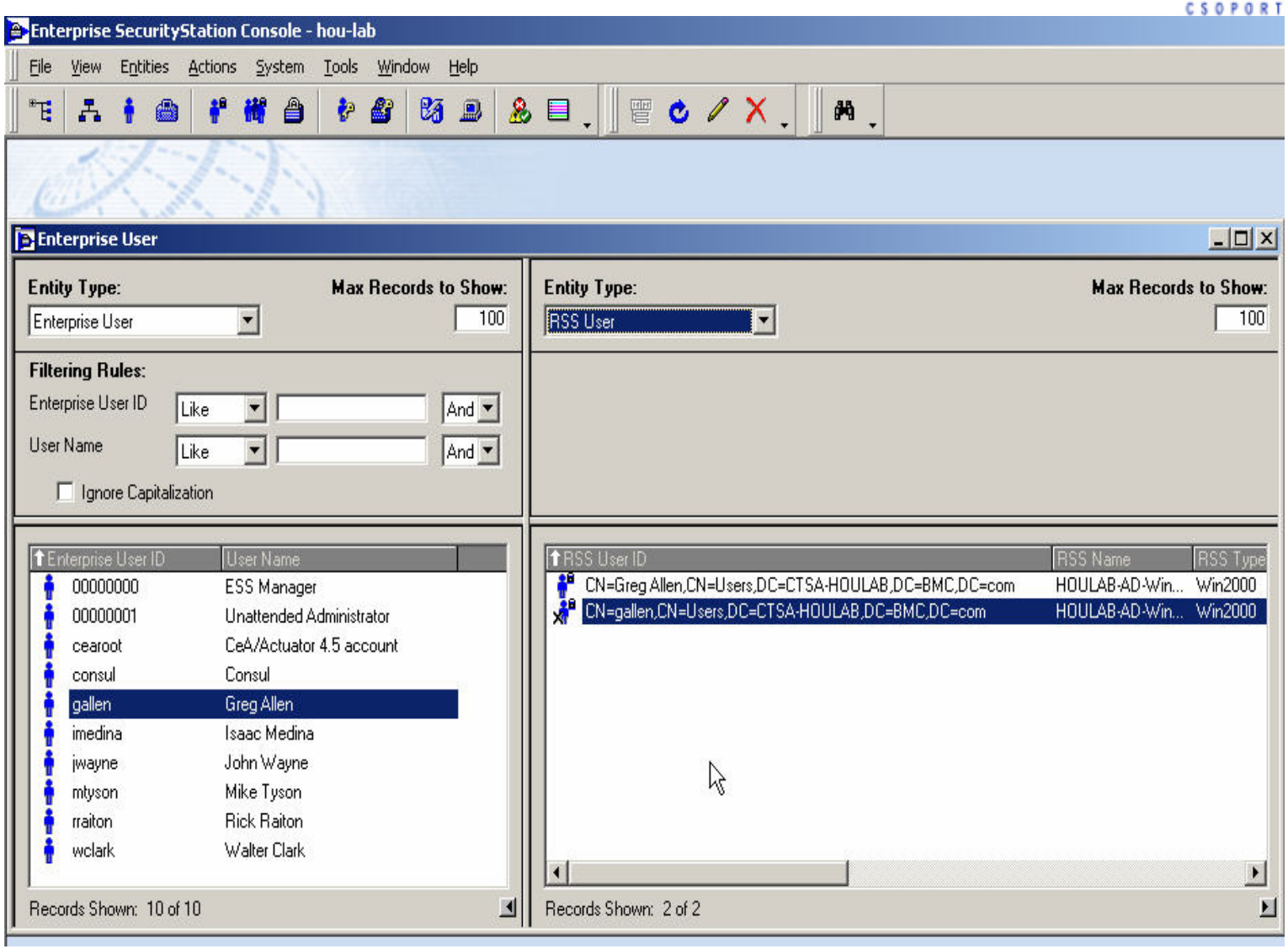
Az InSight működés közben (4.)

Az InSight megmagyarázza a riasztás konkrét okát is.



Az InSight működés közben (5.)

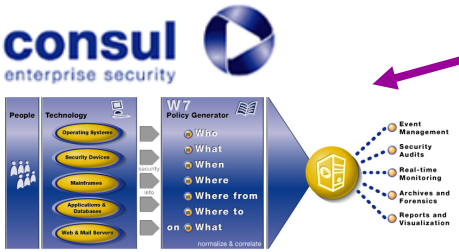
A Control-SA visszavonja *gallen2* felhasználói hozzáférését.



A biztonsági szabályozás betartatása

BSM Identity Management

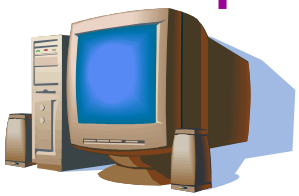
Greg Allen megpróbál hozzáférni az üzleti statisztikákhoz.



A Consul Insight érzékeli a hozzáférési kísérletet.

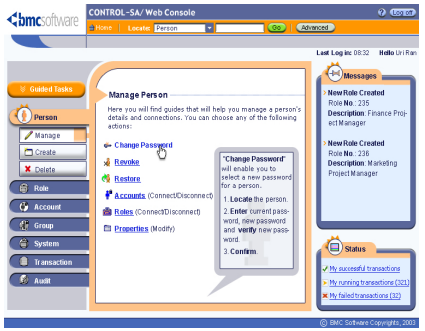
A Control-SA felfüggeszti Greg Allen hozzáférését.

Az integrált InSight jelzi a Control-SA felé a házirend megsértését.



CONTROL-SA

Consul InSight



CONTROL-SA Admin

Itt a vége…

Köszönöm
a figyelmet !