

*Integrating RACF and
distributed Security systems*

M J McNamee

PROGINET CORPORATION



Session Topics

- **Enterprise Security Challenges**
- **What has the marketplace to offer ?**
- **Cutting through the hype**
- **Industry trends**
- **Devising a pragmatic approach**
- **Integrated security in practice**
- **Sample Scenarios**

Enterprise Security Challenges

- **Increasing End User Administration Costs**
 - › Increasing number of systems and users
 - › User add, revoke, resume, change, delete, password reset
 - › **Lack of granular control in off host systems**
 - » *You either have global administration or nothing*
Makes it difficult to delegate

Enterprise Security Challenges

Solaris

Domino/Notes

- **Users have too many credentials to manage**
 - › Reduces productivity
 - › Reduces security

Windows

Oracle

TSO

Novell

Email

CICS

Enterprise Security Challenges

- **Managing Security Policy**

- › **Changing network technologies :**

- › *Easier end user access to data*

DRDA/ODBC : Access DB/2 with Excel etc...

SNA Server, Proginet Legacy Integrator

**DDM & OLE/DB : Access Host data with VB,
Delphi etc ...**

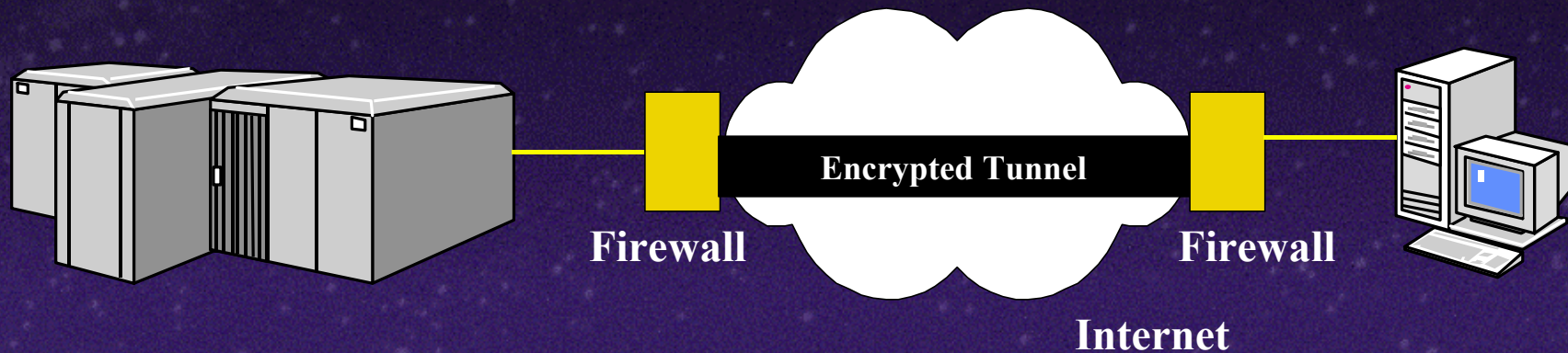
DF/SMS 1.3 and SNA Server 4.0

Meanings change

- **Access to read a dataset means ability to download**
- **Access to write means ability to upload**

Enterprise Security Challenges

- › Expanding the network across public networks



- » *Virtual Private Network*
OS/390 V2R5 NT 4

Provide the ability to securely extend a networks reach

Using public networks e.g. Internet as a transport medium

Beware of opening holes in Firewall

Remote devices can appear to be local

Enterprise Security Challenges

- › **Volume of Critical Business data being exchanged across network increases**
 - » *Integrity must be ensured*
 - » *Data movement must be monitored to detect misuse*
Proginet is developing with a client a file transfer audit system that takes snapshots of data to monitor downloads
 - » *Systems must have a trust relationship - consistent security policy and enforcement required*

Automated tools required as the number of systems increase

What has the marketplace to offer *?*

- **Single Sign On (SSO)**
- **Consistency/Synchronization (CSO)**
Consistent Sign On
- **Distributed Audit**
- **Distributed Administration**
- **Standards**

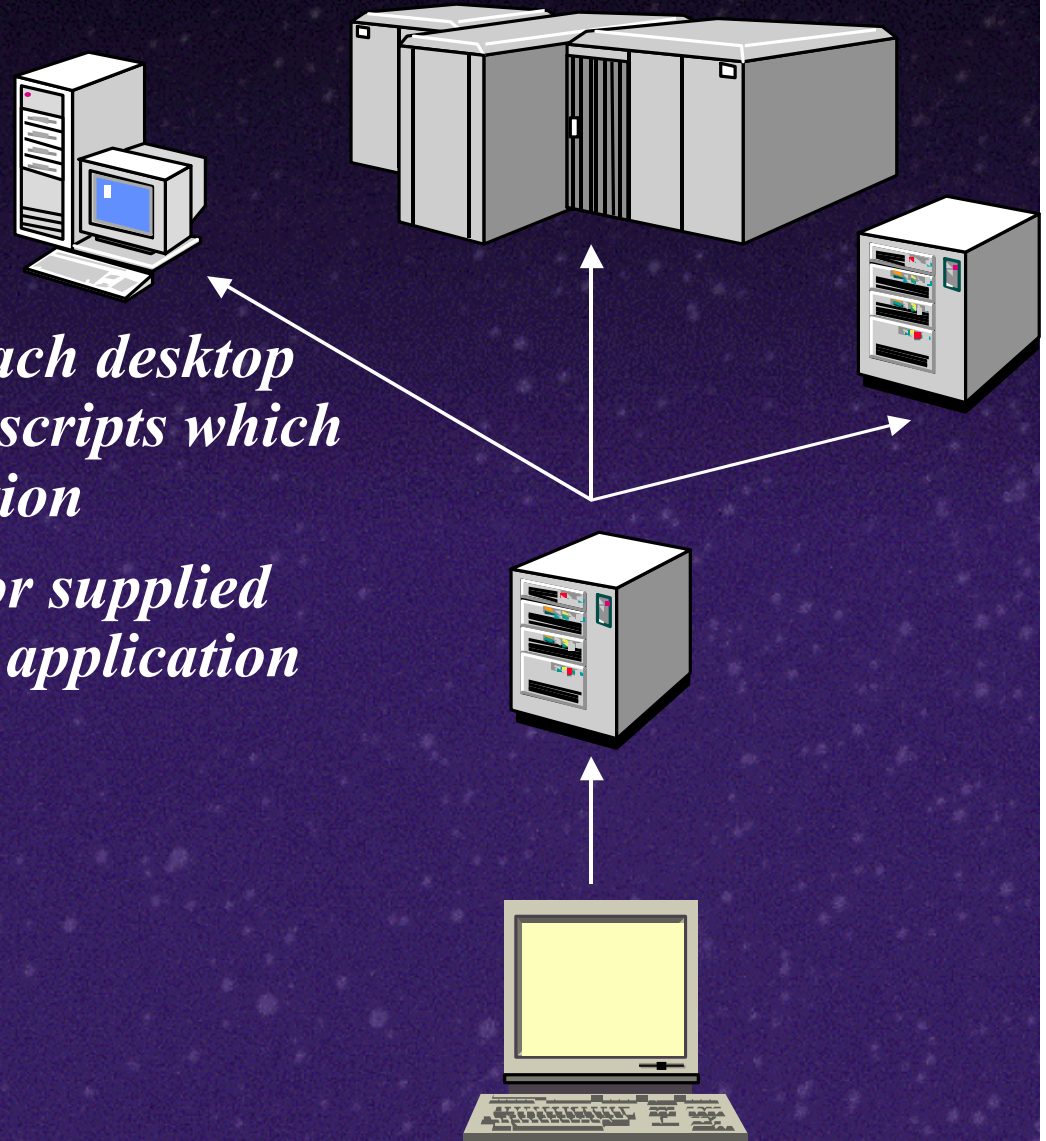
Single Sign On

> Two Types :

- » *Script based : Client on each desktop executing user developed scripts which simulate logon to application*
- » *Agent Based : uses vendor supplied agents which issue native application calls to connect user*

> Advantages

- » *One Sign On !!!!!*
- » *Central Access Control*



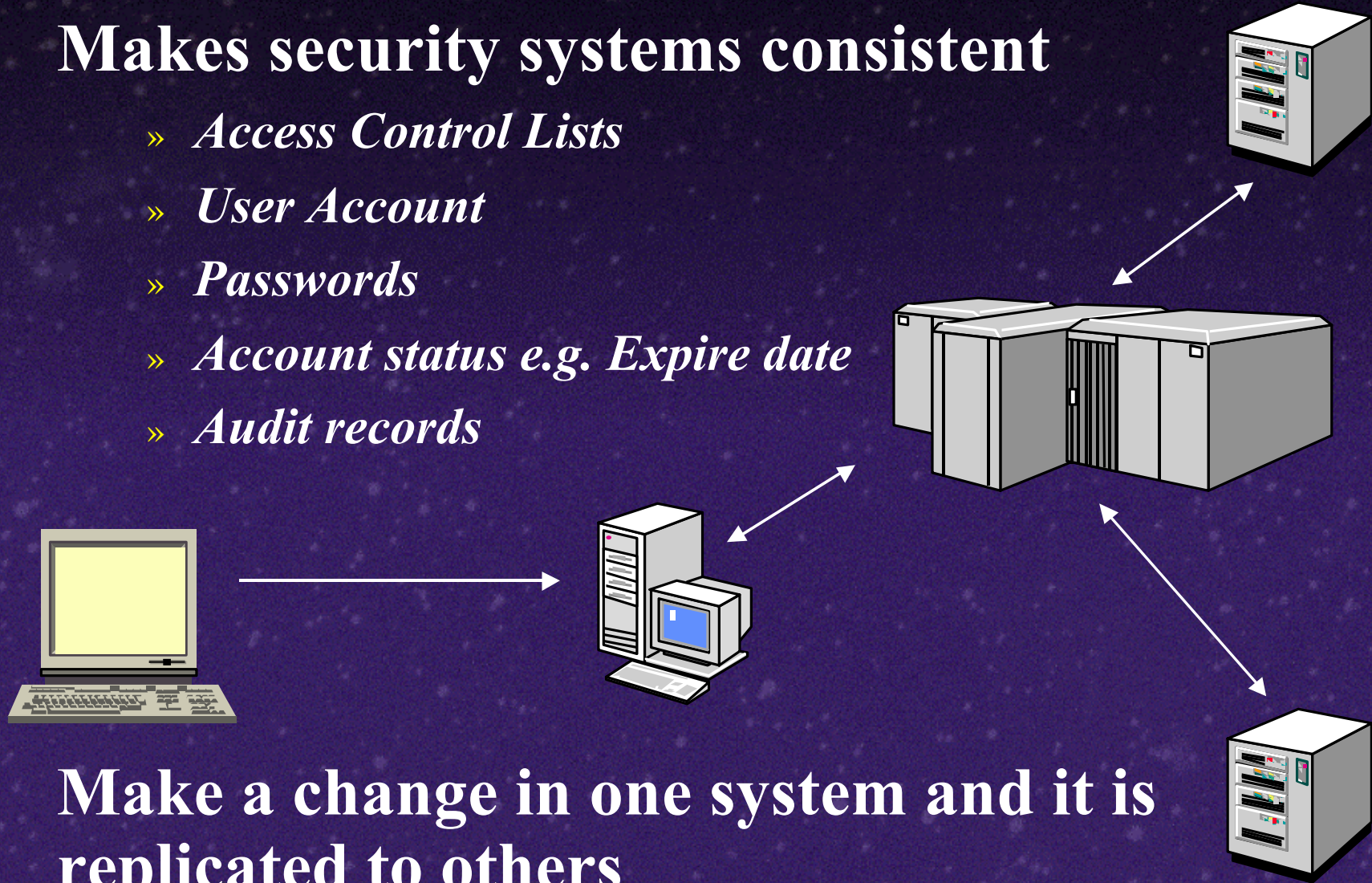
Single Sign On

› **Disadvantages**

- » *Agent Based systems : Application Support is an issue esp. with non standard security systems*
- » *Script Based systems : implementation/maintenance overhead*
- » *Client on every desktop - large implementation cost/elapsed time*
- » *Not quite here yet : Meta (8/1/98) :
“We believe a complete SSO Solution will not appear for at least another two or three years”
“....fraught with problems such as the need for scripting”*
- » *Limited Scope projects seem to be successful*
- » *Authentication Server can be single point of failure*

Synchronization/Consistency tools

- **Makes security systems consistent**
 - » *Access Control Lists*
 - » *User Account*
 - » *Passwords*
 - » *Account status e.g. Expire date*
 - » *Audit records*



- **Make a change in one system and it is replicated to others**

Synchronization/Consistency tools

- **Advantages**

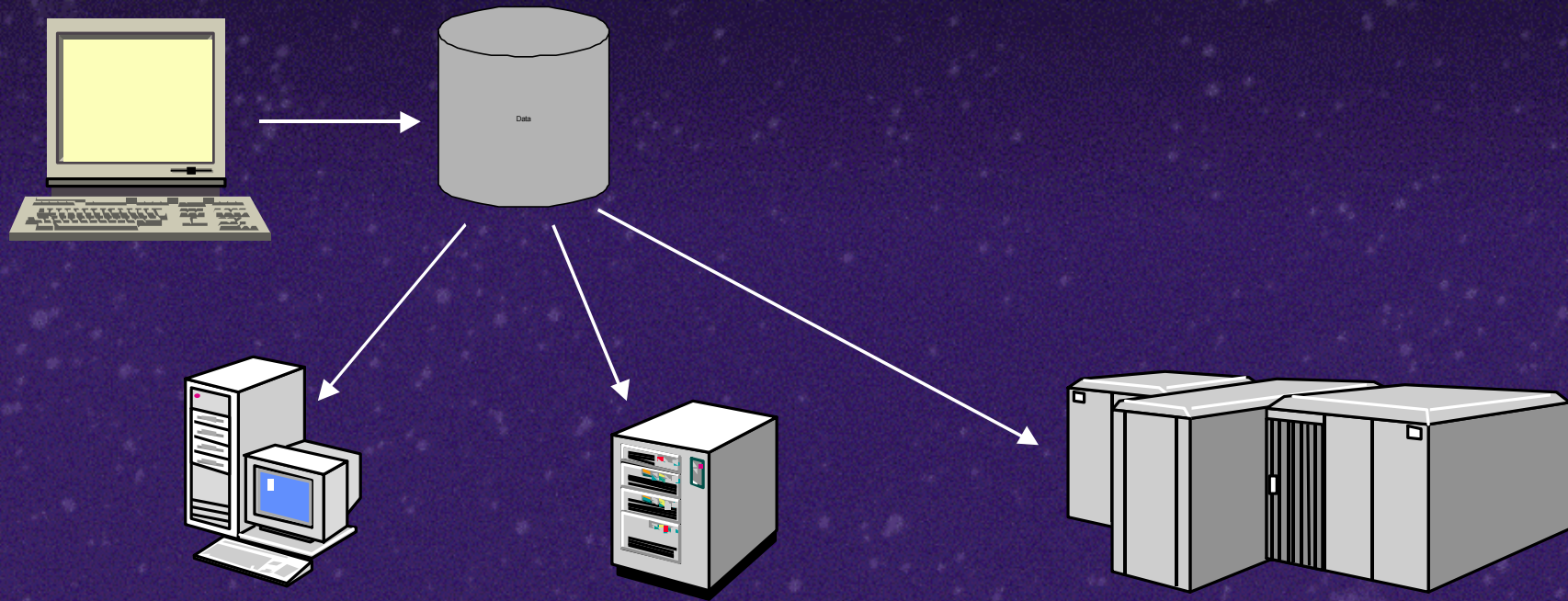
- › **Uses existing user interfaces**
 - » *Little training required*
- › **Implementation is easy/inexpensive**
 - » *Usually installed on existing Authentication Servers so fewer nodes to install*

- **Disadvantages**

- › **Does not take all the end user pain away**
- › **Systems need to be consistent or mapping needs to be defined**
- › **Systems must have some degree of trust**
Policy issues need to be addressed

Distributed Admin

- **Maintain users and Access Control Lists, for the whole network from central database**



- **Changes Pushed to agents on each system for implementation**

Distributed Admin

- › **Advantages**

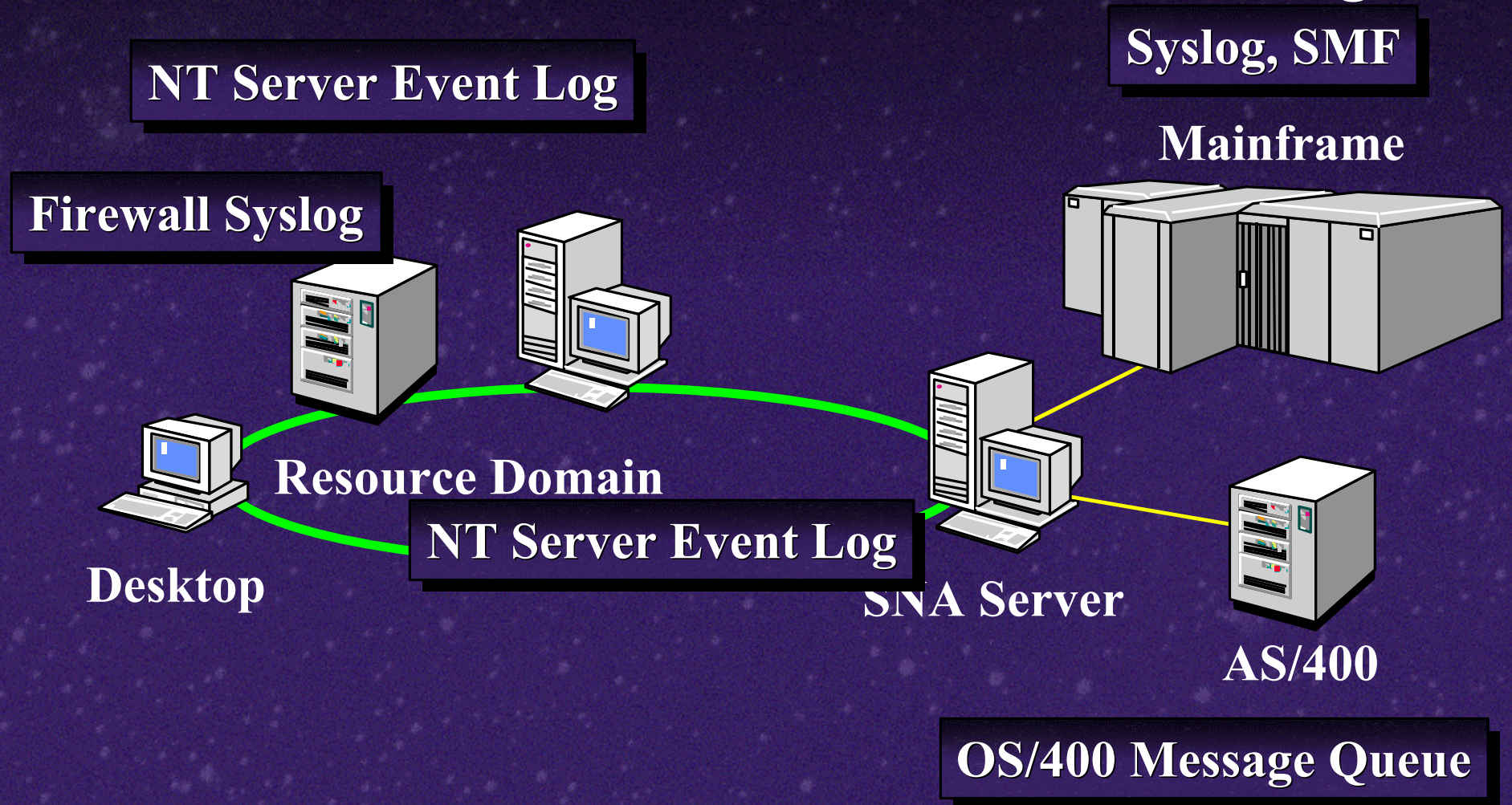
- › *Reduces Admin Overhead*
- › *Allows delegation of admin when operating system cannot - acts as a proxy*

- › **Disadvantages**

- › *Complex to implement and costly*

Distributed Audit

- To audit a users activities in a distributed environment is difficult and time consuming



Distributed Audit

- **Solutions consolidate audit either :**
 - › **In a proprietry repository (typically under a DBMS) with reporting tools**
 - › **In an existing format to allow leverage of existing skills and tools**

Standards

- **Some Standards are becoming readily available and have the potential to evolve into tools to address needs in a multi-vendor environment**
 - › **LDAP (OS/390 V2R5)**
Potentially the glue to join systems together, provide common name space
 - › **NDS (OS/390 V2R7)**
For NDS users
 - › **Kerberos in NT5**
With RACF and OpenEdition/DCE interoperating Kerberos could be a Single Sign On solution.
 - › **Digital Certificates now supported in RACF etc. give the potential of a Single Sign On solution**

Cutting through the hype

- **A game of Bluff :**
 - › **Users are uncertain what they want - so they ask for everything**
 - › **Vendors have everything (Honest !)**
Ask for references and detailed design questions
- **Each class of solution only solves part of the problem**
- **No single vendor has all the answers**
- **Ask for implementation details/costs**

Industry Trends

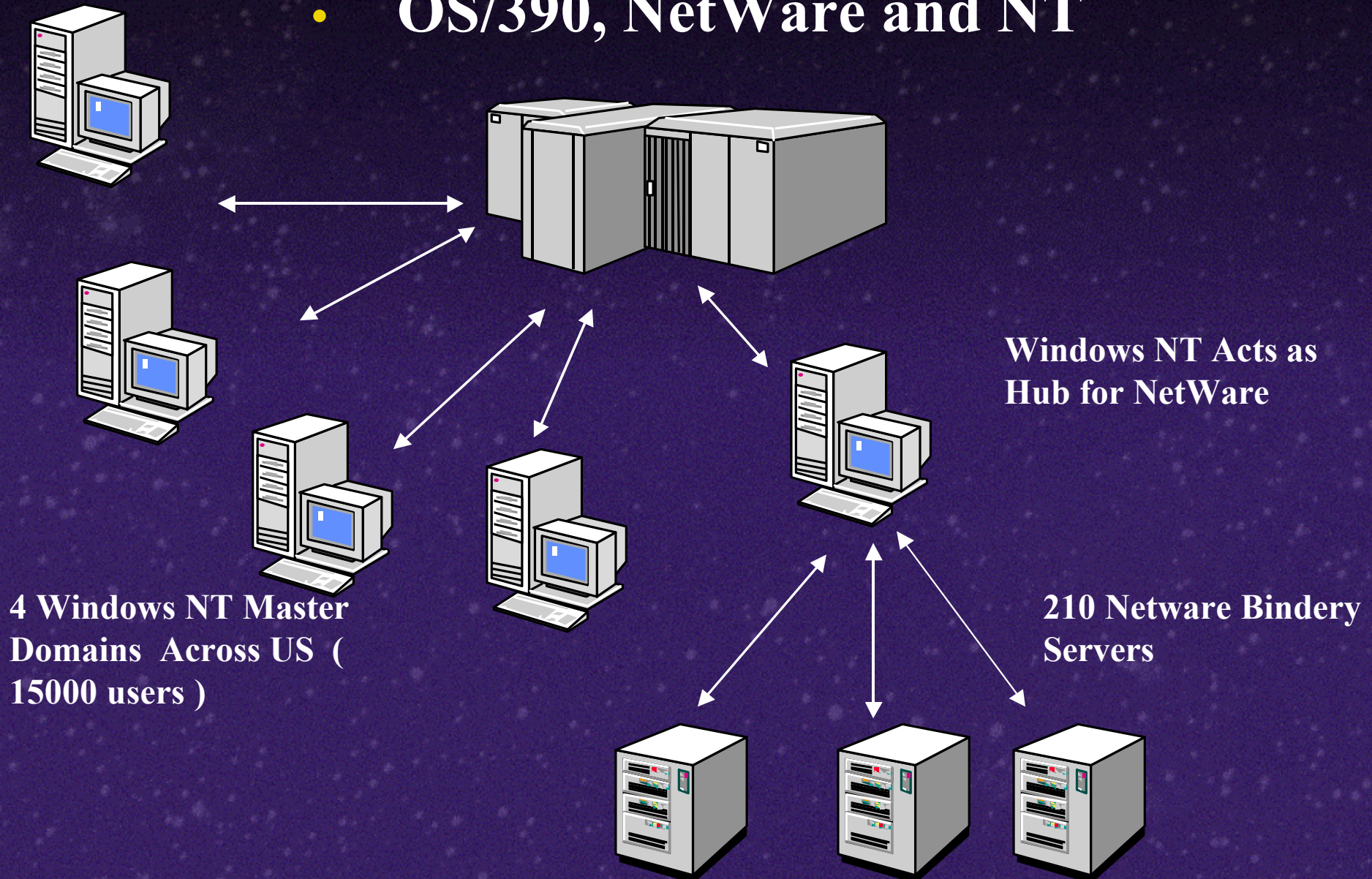
- **Alliances are key**
e.g. Proginet now has alliances with Schumann and Consul
- **Integration between vendor suites could deliver solutions medium term**
- **OS vendors becoming involved**
- **Consolidation ahead e.g. Memco**

Devising a pragmatic approach

- **Identify real needs**
 - › **Consider a tactical approach - technology is still evolving**
- **Devise realistic (achievable) objectives**
- **Identify products**
- **Be prepared to integrate products**

Integrated security in practice

- OS/390, NetWare and NT



Integrated security in practice

- **Password changes, revoke, resume and expiry date synchronized between 2 OS/390, 4 NT Master Domains, 210 NetWare Bindery Servers**
- **NT Audit centralized on OS/390 using RACF SMF 80 records**
- **User Add and Delete automated using RACF as a central hub**
 - › **Add is a batch process using unloaded RACF database**

Questions ?????