IBM Software Group

Best Practices for Delivering Value Faster Through Better use of Existing Assets

IBM Americas zSeries Premier Event
Puerto Rico
March 8th 2006

Presented by Ronn Bailey
Vanguard Integrity Professionals

Tivoli software

ON DEMAND BUSINESS

Trademarks

- The following are trademarks or registered trademarks of the International Business Machines Corporation (IBM) or subsidiaries
  - IBM®, CICS®, DB2®, Tivoli®, zSeries®,
  - z/OS®, OS/390®, MVS, MVS/ESA, MVS/XA
  - RACF®, SecureWay®, Security Server
- The following are trademarks and service marks of Vanguard Integrity Professionals (VANGUARD)
  - Vanguard Administrator™, Vanguard Advisor™, Vanguard Analyzer™
  - Vanguard Enforcer™, SecurityCenter™
  - SmartLink™, Find-it-Fix-it-Fast™, RiskMinder™, SmartAssist™, eDistribution™
- Microsoft™, Windows, and the Windows logo are trademarks of Microsoft™
- Java™ and all Java-based trademarks are trademarks of Sun Microsystems, Inc.
- UNIX™ is a registered trademark in the United States and other countries licensed exclusively through The Open Group
- CA-ACF2®, CA- Top Secret® are trademarks of Computer Associates International.
- Other company, product, and service names may be the trademarks or service marks of others in the United States, other countries, or both

Agenda

- Security Management and Compliance
- Vanguard Administrator
- Vanguard Advisor
- Vanguard Analyzer
- Vanguard Enforcer
- Vanguard Security Center
- References
- Related Discussions
  - IBM SOX White Paper
  - A SOX Project Status
  - Other Regulations
  - INCompliance Tool
  - How to Hack z/OS White Paper
  - How to Stop the z/OS Hack
  - A More Correct View of RACF – Meta Data

What's on the Minds of Security Professionals

CEO needs

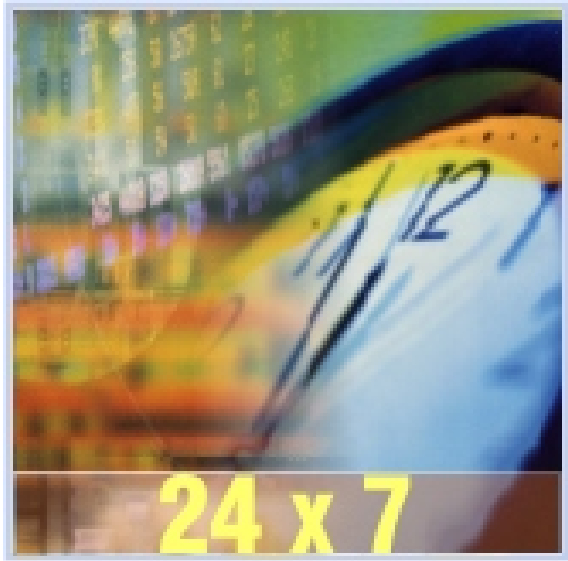
- Revenue growth with cost containment with in a **secure** environment
- Key competency: **responsiveness**
- Critical success factor: enable **effectiveness** of people
- **Compliance** with regulations

Security Manager's challenges

- Aligning IT and business goals to grow revenue with in a secure environment
- Building responsiveness and agility into the organization through security
- How can security help enable people and teams to be more effective
- Efficiently meeting audit requirements

IBM zSeries
a powerful platform for security for the On Demand Business

- The real threat is to your business reputation – failing trust and confidence of your partners, customers and shareholders
- zSeries provides security solutions
  - Authentication
  - Authorization
  - Audit
  - Administration
- via world-class
  - Cryptography
  - Data encryption & decryption
  - Intrusion detection
  - Overall system integrity
  - Common Criteria Security Certification
- Over 80% of corporate data resides and/or originates on mainframes*
- Online criminal attacks of corporate and government networks cost businesses an estimated $666 million in 2003.**



*Source: ITG August 2003

**The survey was conducted by CSO [Chief Security Officer] magazine in cooperation with the U.S. Secret Service and the CERT cyber security center at Carnegie Mellon University in Pittsburgh.

IBM and Vanguard - Partners for Security Management

Offering efficient RACF Security Management, Access Control, Reporting and Compliance Monitoring Across the Enterprise

Process / Service view of IT Security Management

- Security Configuration
- Vulnerability Management
- Security Patch Management
- Access Management
- Privacy Management
- Identity Management
- Security Event Management
- Incident Management
- Threat Management
- Security Controls Definition
- Security Compliance
- Business Risk Management

Protect systems

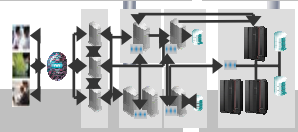
- Security Server (RACF)
- IBM Tivoli Security Compliance Manager
- **Vanguard Enforcer**
- **Vanguard Analyzer**
- **Vanguard Advisor**

NEW!

Manage users

- IBM Tivoli Identity Manager
- IBM Tivoli Access Manager
- IBM Tivoli Federated Identity Manager
- **IBM Tivoli Directory Server & Directory Integrator**
- **IBM Tivoli Security Administrator for RACF**
- **Vanguard SecurityCenter**
- **Vanguard Administrator**

NEW!



Manage threats

- IBM Tivoli Risk Manager
- **Vanguard Advisor**
- **Vanguard Analyzer**
- **Vanguard Enforcer**

NEW!

Establish trust & compliance

- **IBM Tivoli Identity Manager**
- **IBM Tivoli Access Manager**
- **IBM Tivoli Federated Identity Manager**
- **IBM Tivoli Security Compliance Manager**
- **Vanguard Enforcer**
- **Vanguard Advisor**

NEW!

IT Governance – Data Governance (IBM DGC)

IT Governance gives the information needed to continually make – and enforce – high quality decisions that significantly impact business. Lowering costs and raising profits.

The Business of Managing Business Data

- **MRD – Master Reference Data (A centralized data repository)**
- **MDM – Master Data Management (Previously known as MRD)**
- **CDI – Customer Data Integration**
- **ETL – Extract Transformation and Load**
- **EII – Enterprise Information Integration**
- **EAI – Enterprise Application Integration**
- **EDR – Enterprise Data Replication**
- **ECM – Enterprise Content Management**
- **PDM – Predictive Data Management**

A correct view of RACF is to think of it as very important, valuable & critical business data, not simply security stuff.

- The Security Server DB is the most pervasive DB in the Enterprise. Every person, data asset, sub-systems, business transactions, business systems and processes – virtually all units of work depend on it. The transaction throughput is greater than all other data bases combined.
- Enterprise wide - there is no DB more critical to the operational organization.
- Metadata is data about data. The Security Server DB is Enterprise Metadata.
- The actual content goes far beyond user ID's, passwords and ACL's for security. It contains business "policy data." Information that governs actual use, control, authority and classification - of people, data, transactions, business systems and processes.
- The Security Server DB has the same issues and requires the same disciplines of Data Management and Maintenance as other large scale Enterprise data bases.
- Security Server DB is very unique. It has its own access method and format. It is highly specialized. No other data in the Mainframe uses it's access method and format.
- The Security Server (RACF) requires it's own set of tools for DB management, maintenance, analysis, assurance, automation and so on.

Vanguard provides the tools for Security Server (RACF) and extends its capabilities to other systems across the Enterprise.

IT Governance – Data Governance (IBM DGC)

Another view of IT Governance has to do with the external pressures of regulatory compliance. This is very serious and has become very personal for those executives that have fiduciary responsibility.

Violating SOX - Fines up to $5 million or 20 years in prison.

The Business of Managing Business Risk

- IBM Sarbanes Oxley White Paper - Top 10
- A Current Project Status – Real World
- One Customers List of External Regulatory Requirements
- 2005 INCompliance

Vanguard Integrity Professionals - Relevance

More Than Half the Companies In This Room are Existing Vanguard Customers Representing 89 Years of Service – Thank You!

For Rest of the Companies Here:

1 Is Top Secret
1 Is Mixed: Top Secret 90% & 10% RACF – Considering Consolidation (Think RACF)
2 ACF2 Shops, one considering Migration to RACF (Good Idea)
5 Have RACF - 2 with no tools, 2 with home grown tools and 1 using a competitive product

Vanguard Customers and References

"I do not believe I would have been able to survive the SOX audit without the Vanguard tools…ease of use is phenomenal!"

Gary Godek
Information Security Administrator
Eaton Corporation

"With the Vanguard products, productivity has increased. The value of the products has far exceeded the costs."

Ann Fleming
Director of Information Security
Georgia Department of Labor

"The Windows interface on SecurityCenter makes RACF administration a lot easier. You double-click to see the security tree, then click again to drill down into specific permissions for specific individuals."

Greg Sieg
Manager of Technical Development and Support
Princess Cruises

ABN AMRO Bank
U.S. Bancorp
Wachovia
Bank of Montreal
State Street Bank
Capital One Services
Travelers Indemnity
AFLAC
Hyundai Marine & Fire Insurance

U.S. Office of Personnel Management
Singapore Housing Development Board

IBM Global Services
Princess Cruises
America West Airlines

United Healthcare Corporation
Blue Cross Blue Shield of Connecticut
Centra Health
California Health Services
University of Virginia Medical Center
Rite Aid Corporation

Wal-Mart
The Gap
Sears Canada
Winn-Dixie Stores
Dillard Department Stores

Goodyear Tire & Rubber
Pratt & Whitney
Sony Electronics
Nissan North America
Ralston Purina

Depository Trust & Clearing Corp. (DTCC)

"DTCC has become far more proactive in meeting security compliance requirements with the use of the Vanguard technology. Vanguard's solutions help us maintain, track, and perform constant surveillance and enforcement over our environment."

— Paul de Graaff
Vice President
Chief Information Security Architect
The Depository Trust & Clearing Corporation

Business Challenges

- Complex system environment: Sysplex with 15 LPARs & 10 RACF® databases
- Labor intensive security management tasks were stifling IT productivity
- Goal: lockdown the security environment by
  - Fully automating the change control process
  - Continuously monitoring and enforcing policies for critical resources and RACF settings to ensure system integrity
  - Reducing security vulnerability window and costs and expertise required to manage RACF policies

Solution Benefits

- Identifies security policy deviations in real-time
- Immediately escalates policy exceptions
- Establishes new security baseline (re-baseline) or rejects exception by reinforcing existing (approved) policy automatically
- Continuously monitors security posture
- Reduces window of vulnerabilities through real-time detection and alerting

Solutions

- Vanguard Administrator™, Analyzer™, Advisor™, & Enforcer™

Canadian Department of Defense

"Vanguard's products make my job fun! I can now devote most of my time to security oversight activities because we have experienced enormous productivity improvements. The reporting capabilities are outstanding, I maintain visibility across my entire RACF environment, review policy changes, and receive alerts on security events including policy violations. I have transitioned our security operation from reactionary to proactive security management."

Central RACF Administrator

Canadian Department of Defense

Business Challenges

- Management of distributed RACF environment: Sysplex with 14 LPARs & 2 RACF® databases
- Labor intensive security administrative tasks were stifling security officer's productivity
- Frequent job rotations made it difficult to maintain deep RACF expertise
- Internal audit identified too many findings
- Lacked oversight of policy changes

Solution Benefits

- Provides a platform for RACF training; new personnel are productive on day-one.
- Reports across the entire RACF environment improving oversight and control
- Improves responsiveness through real-time alerting on security events
- Automated system auditing proactively identifies vulnerabilities to maintain audit readiness

Solutions

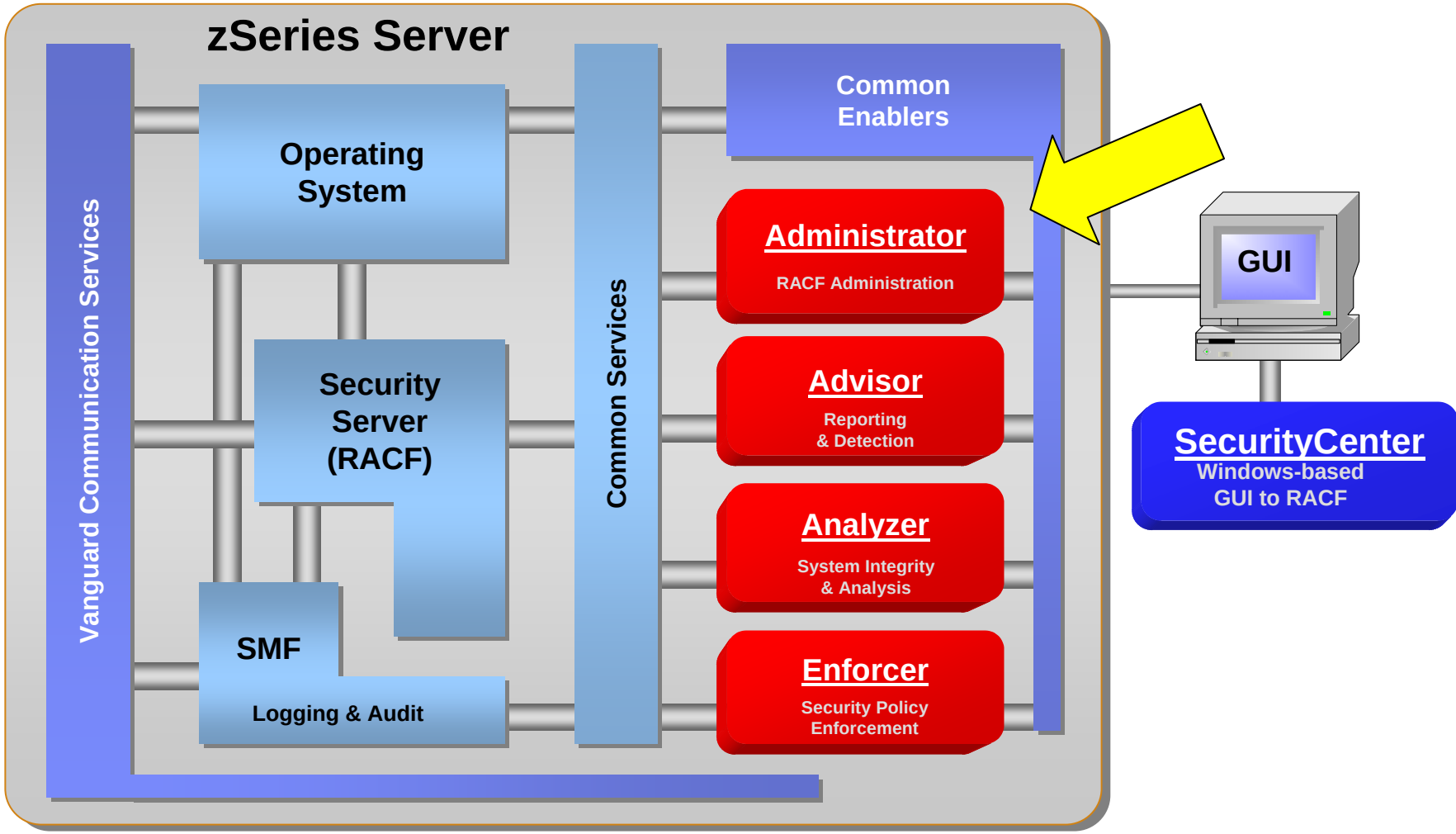
- Vanguard Administrator™, Analyzer™, Advisor™, Enforcer™, & SecurityCenter™

Design Concepts

- Integrate administration, audit, reporting, assessment, intrusion management and compliance
- Provide new ways of working:
  - **Integrated functions and perform concurrently**
  - **Exception analysis and action recommendations**
  - **Same look and feel when ever possible**
- See a problem, correct it immediately
- When possible, let the system do it

(Automatic & Unattended Operation - Core Concepts)

Vanguard's RACF Administration and z/OS Compliance Tools



Administrator – RACF Administration

- Easy RACF Administration
- Simplifies the complexity of RACF administration
- Reduces the amount of Administrative errors
- Allows the same number of Administrators to do more *valued* work rather than tedious repetitive tasks

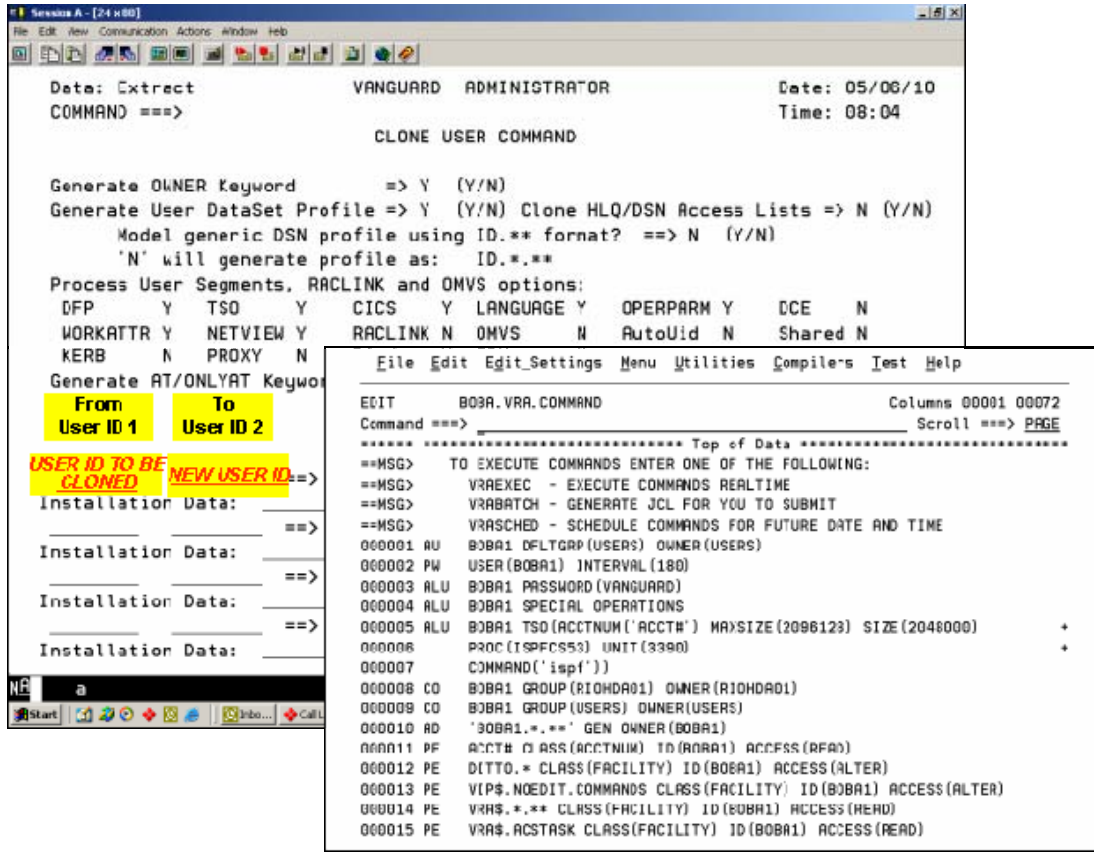
Administrator – RACF Administration

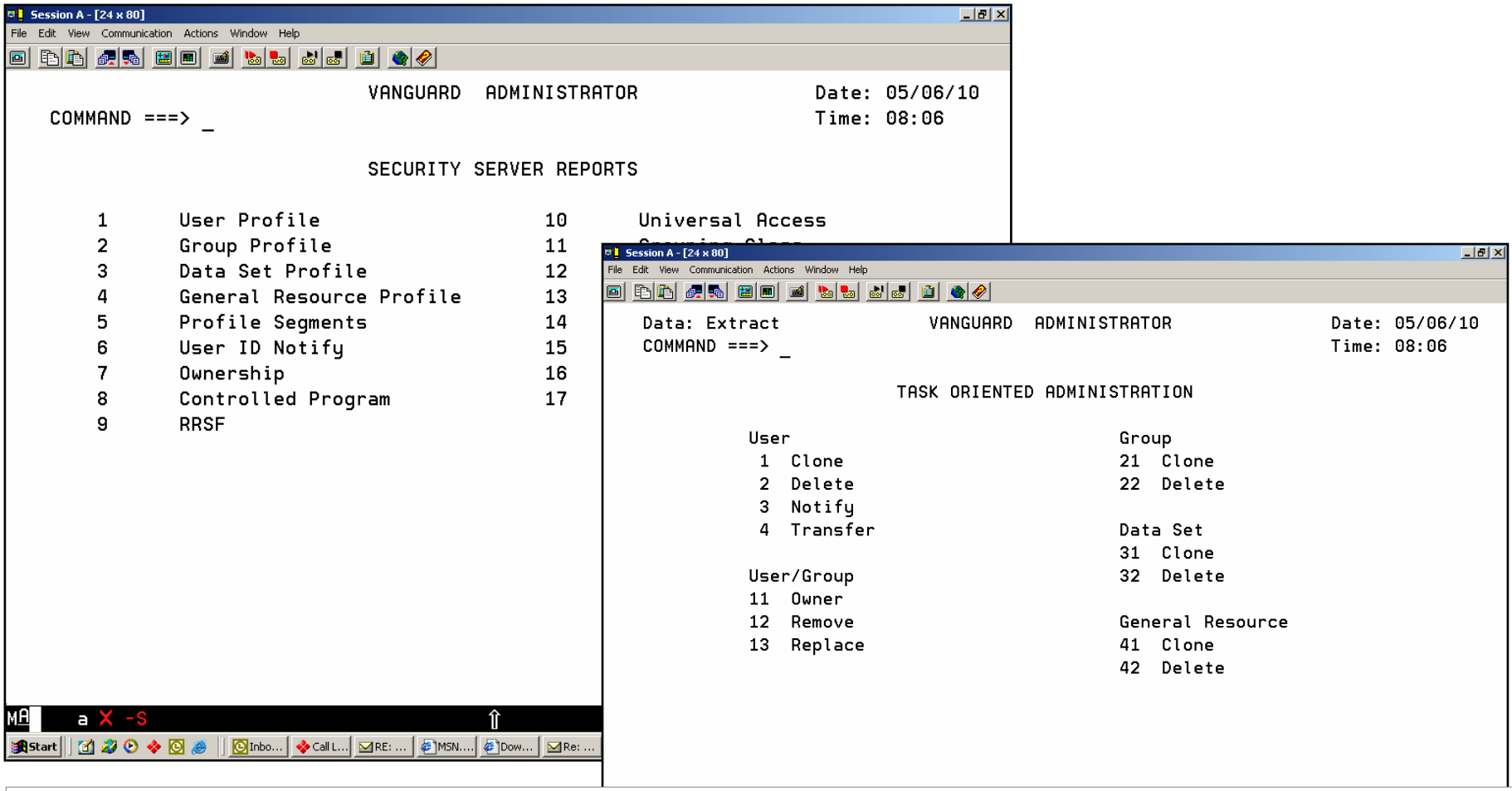
Automated security administration

- Provides a wide range of administration, data mining, and reporting tools.
- Simplifies and enhances security management functions on systems running RACF.
- Handles increased management workloads and complex system administration for either centralized or decentralized RACF environments.
- Provides security automation features such as:
  - Easy-to-use password administration
  - Decentralized administration support
  - Task-oriented administration
  - Authority analysis

Administrator – RACF Administration

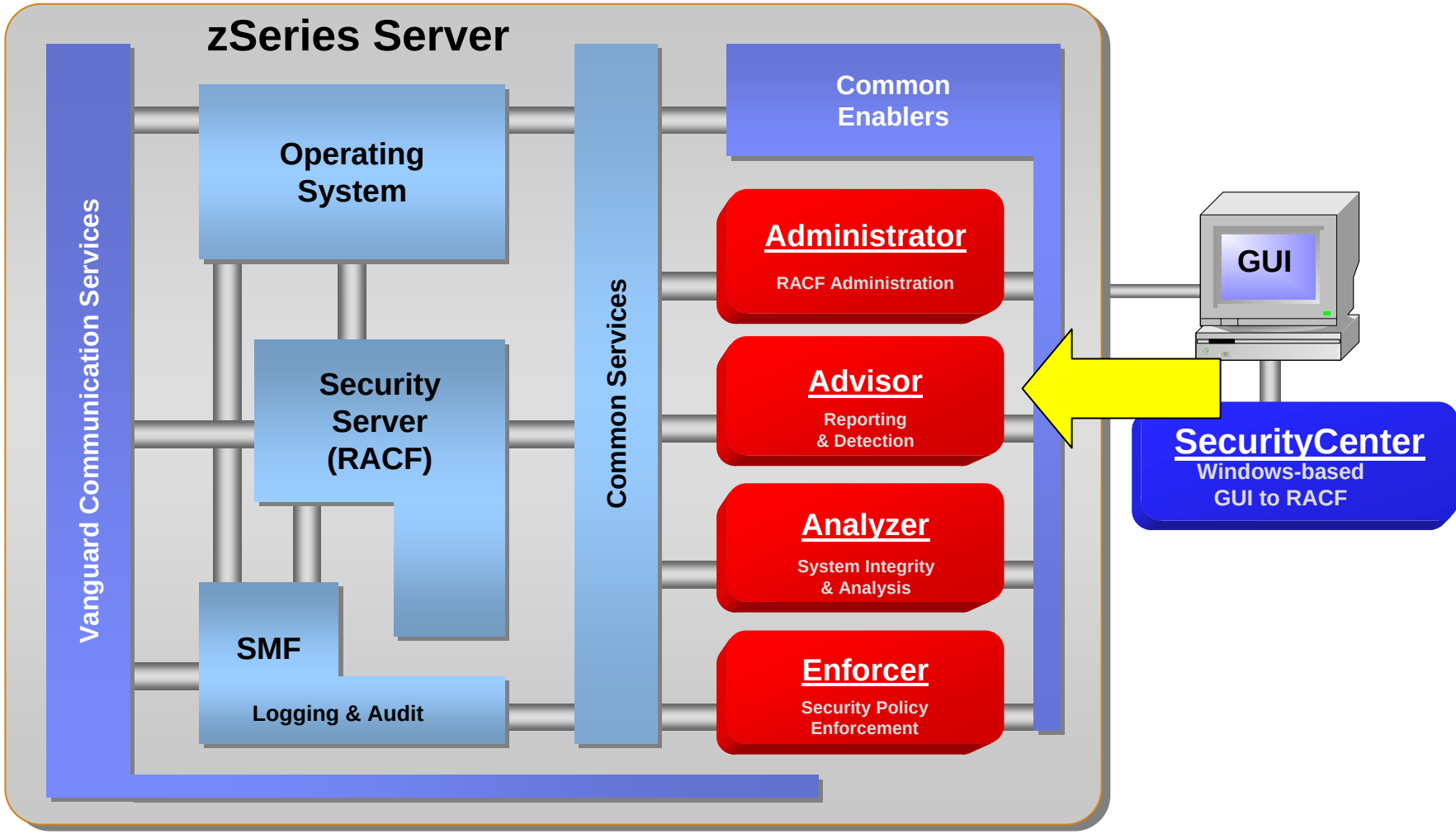
- Simplified administration for RACF
- Reduces the complexities of RACF security administration
- Helps to eliminate user errors
- Enforces best practices
- Reduces the RACF learning curve
- Enhances security through centralized administration





Administrator allows less technical personnel to quickly perform security administration tasks that would normally take hundreds of hours.

Vanguard Products



Advisor – RACF Reporting

- Complete detailed reporting, with an intuitive interface.
- Quick delivery of the needed information to the correct people. (email of important events as they occur).
- Valued information is easy to find. No need for large volumes of data that no human can sort through.
- Quick ramp-up for new Administrators, no need to understand the log record configurations of system data.

Advisor – RACF Reporting

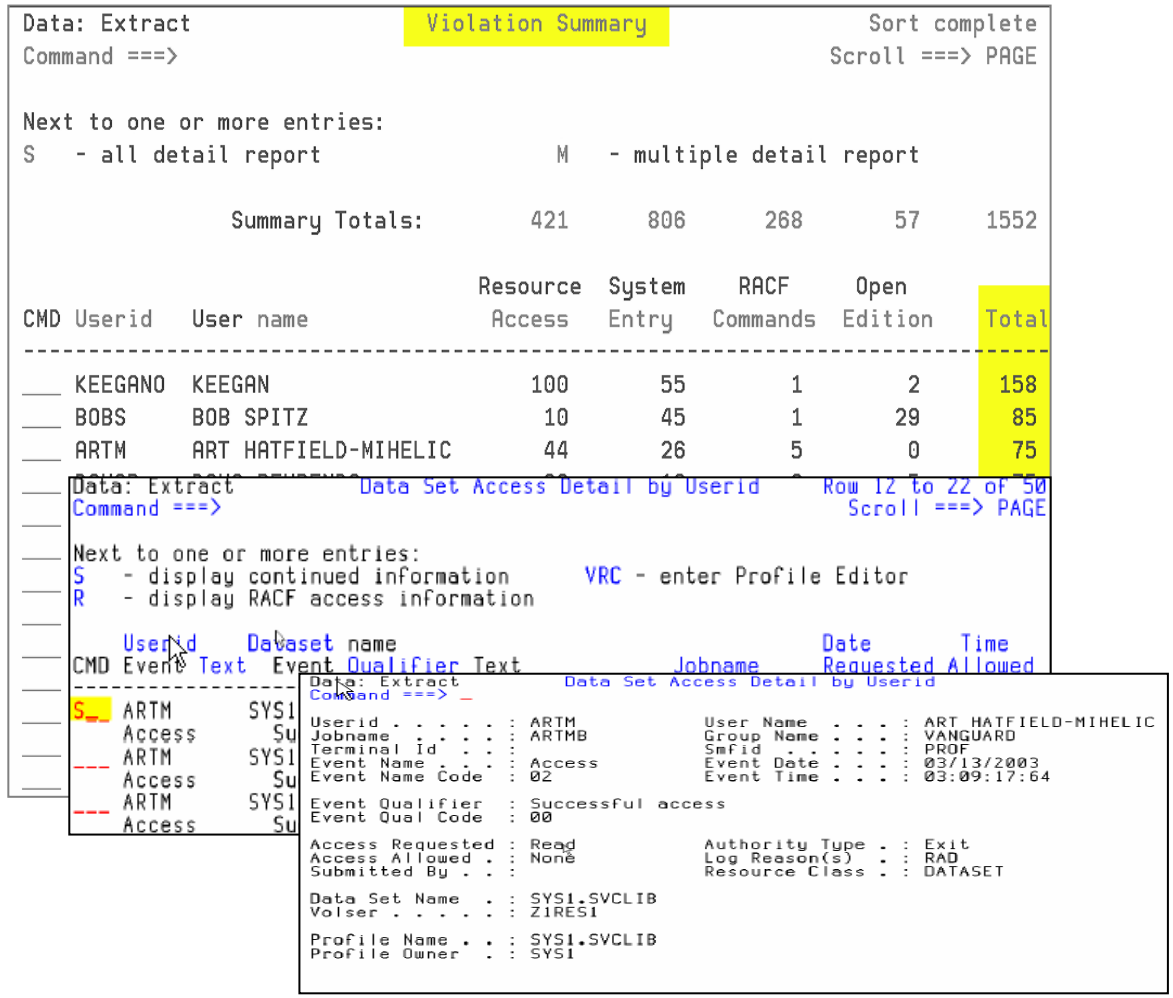
Event detection, analysis and reporting

- Comprehensive event detection, analysis and reporting package for the mainframe environment.
- Works with "live" or collected data from RACF and from the system data (SMF).
- Advisor automatically detects security breaches or malicious patterns 24 hours a day, gathers related information, recognizes the importance, explains the significance, and guides the security administrator through the process of completely eradicating the security exposures.
- Manages summary, detail, and extended-detail information levels.
- No need to learn reporting languages.
- Numerous pre-defined summary or detailed reports provided.
- Custom reports can easily be created.

Advisor – RACF Reporting

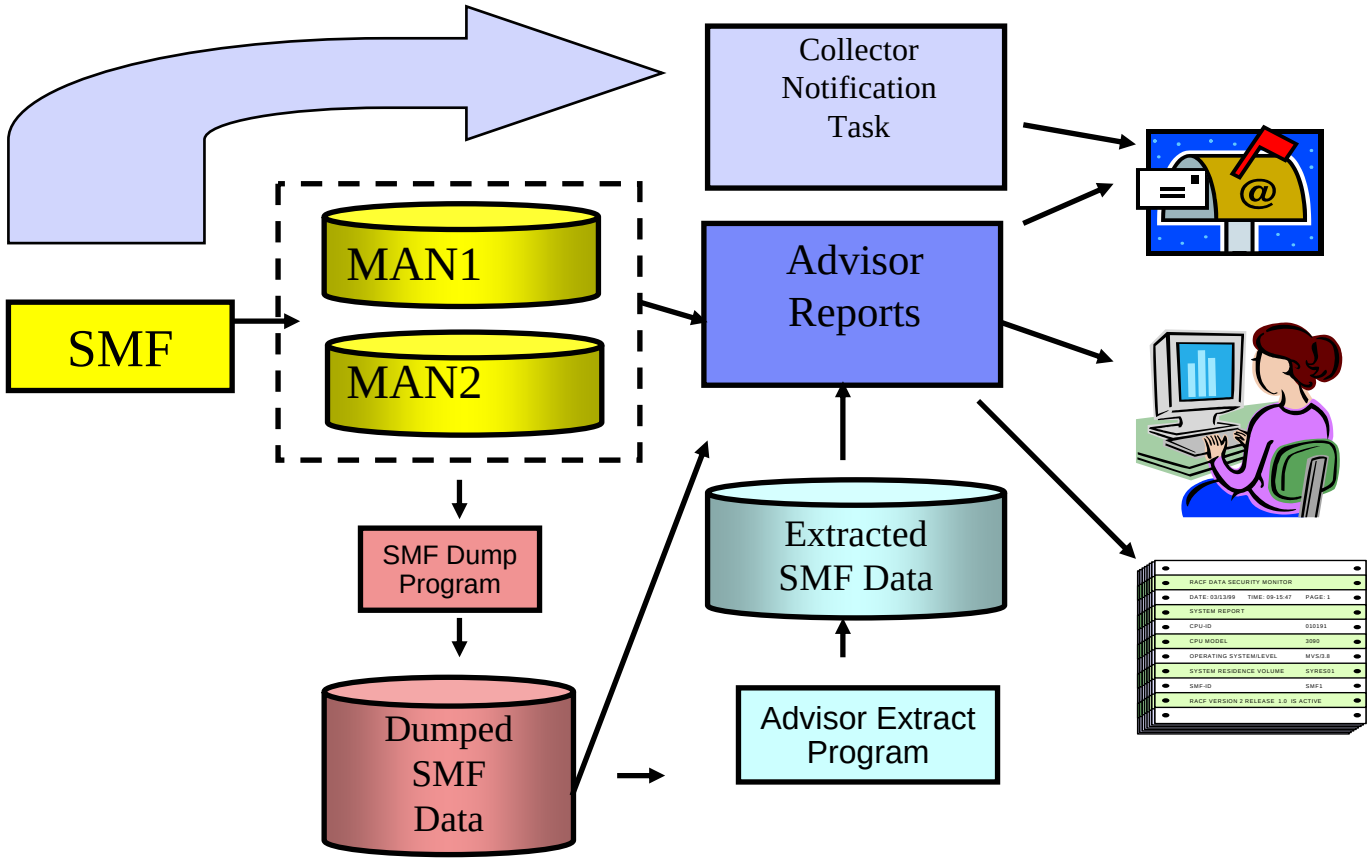
Event detection, analysis, real-time alerts, reporting and electronic report distribution

- A comprehensive security reporting tool for RACF.
- Advisor goes far beyond reporting, is extremely robust and easy to use.
- Data-mining capabilities and is fully integrated with the Vanguard Administrator.
- Helps customers cope with the demands of new compliance and regulatory mandates.

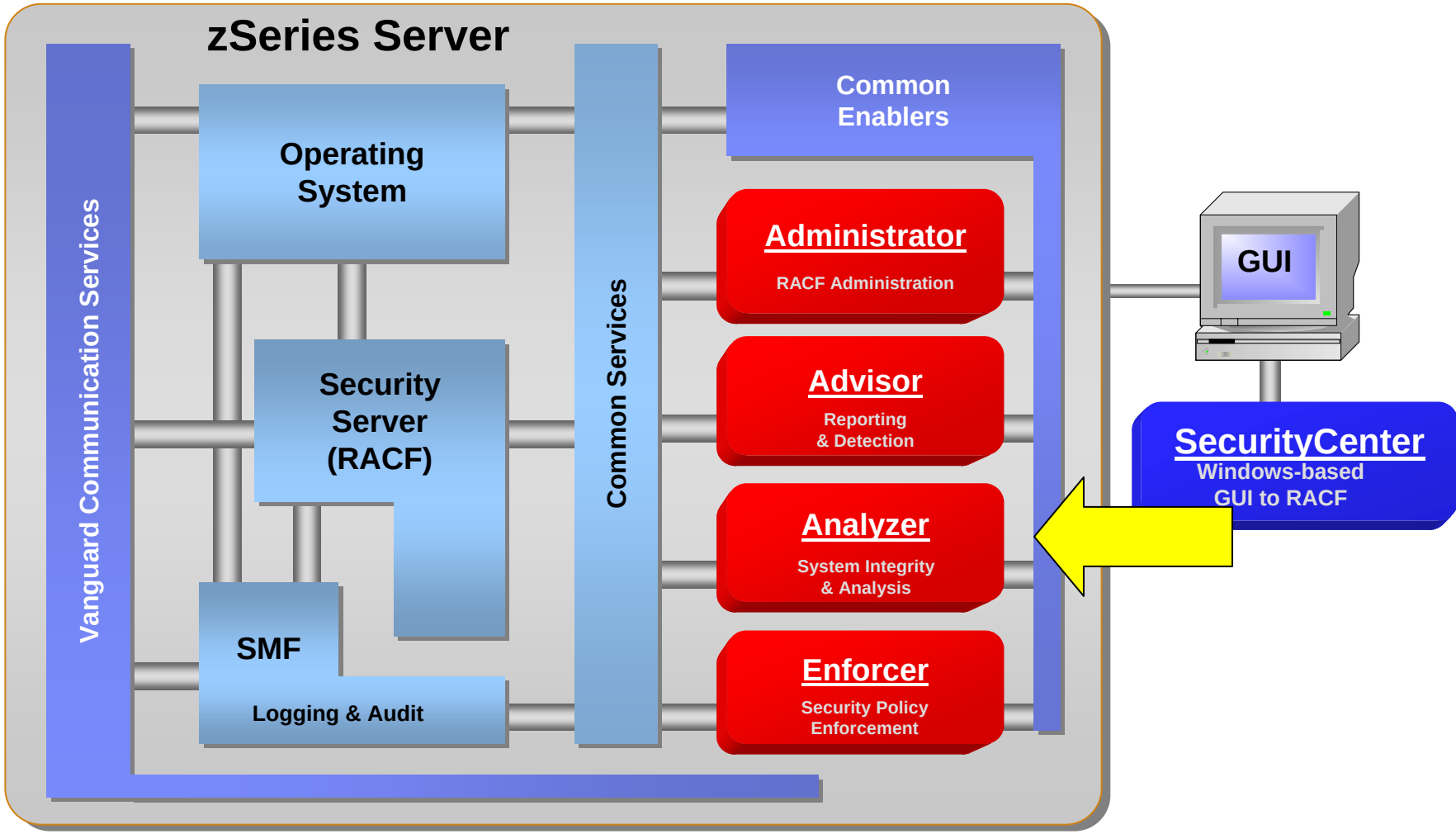


Vanguard Advisor Real Time Notification

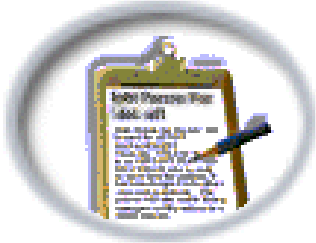
Real time notification is an important Advisor feature that detects security events when they occur and based on parameters specified, automatically notifies interested parties so corrective action can be taken in a timely fashion



Vanguard Products



Analyzer – System Integrity and RACF Analysis



- Easy Auditing of both the z/OS and the RACF environments.
- Less experienced people can review the environment.
- SmartAssist explains the identified risks and recommends how to correct them. You don't need to constantly refer to an audit manual for every finding.
- Far more reliable end results even for an experienced auditor, reduces the number of errors.
- Greater assurance of passing those ‘surprise’ external audits.

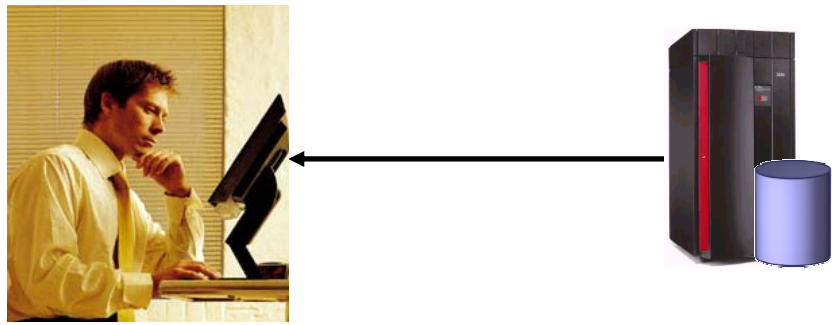
Analyzer – System Integrity and RACF Analysis

Z/OS Analysis Functions

- Program Properties Table
- Sensitive / Critical Data Sets
- SVC Table Analysis
- Subsystem Name Table Analysis
- System Environment Analysis
- SMF Environment Analysis
- Link Pack Area Analysis
- Operating System Exits Search
- JES2 Analysis
- Parmlib Analysis
- Filebaseline Capture

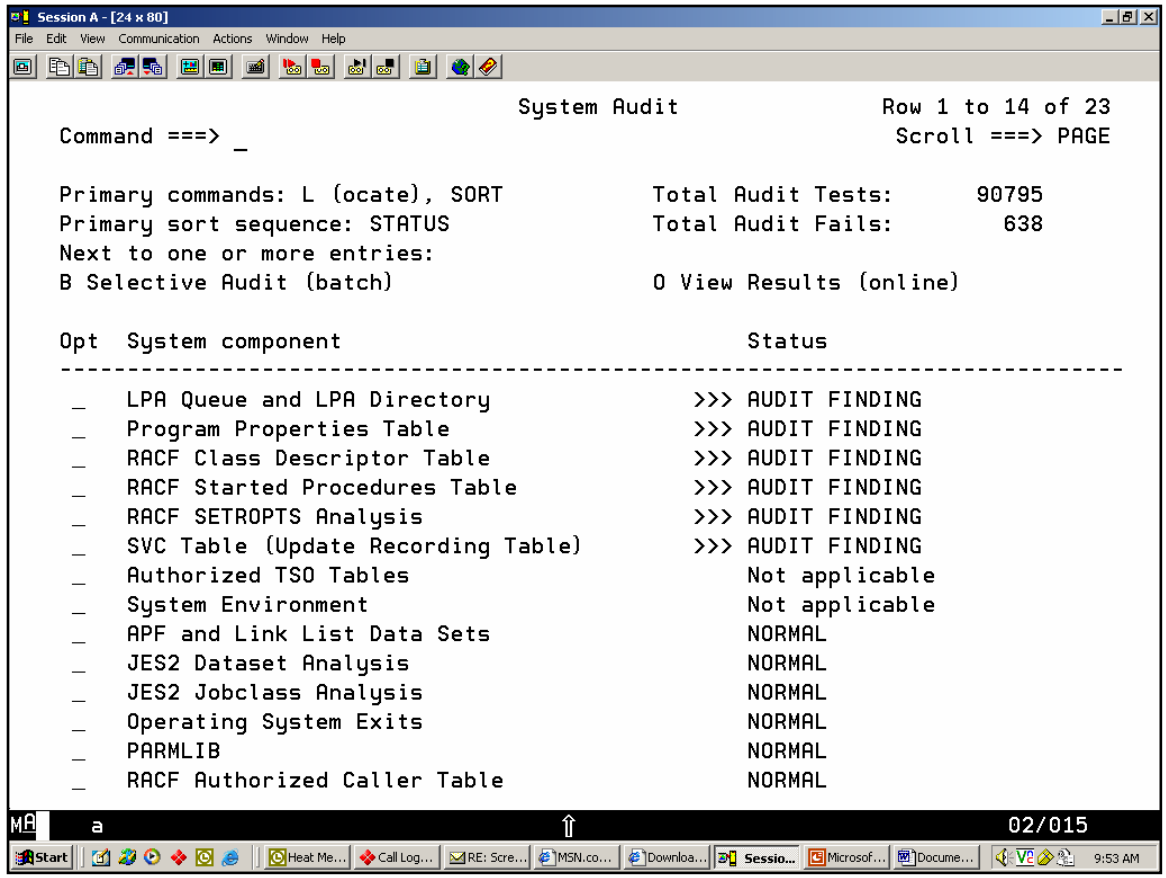
RACF Analysis Functions

- Class Definitions
- MVS Router Table
- Data Base Analysis
- SETROPTS
- Started Procedures Table
- Installation Exits



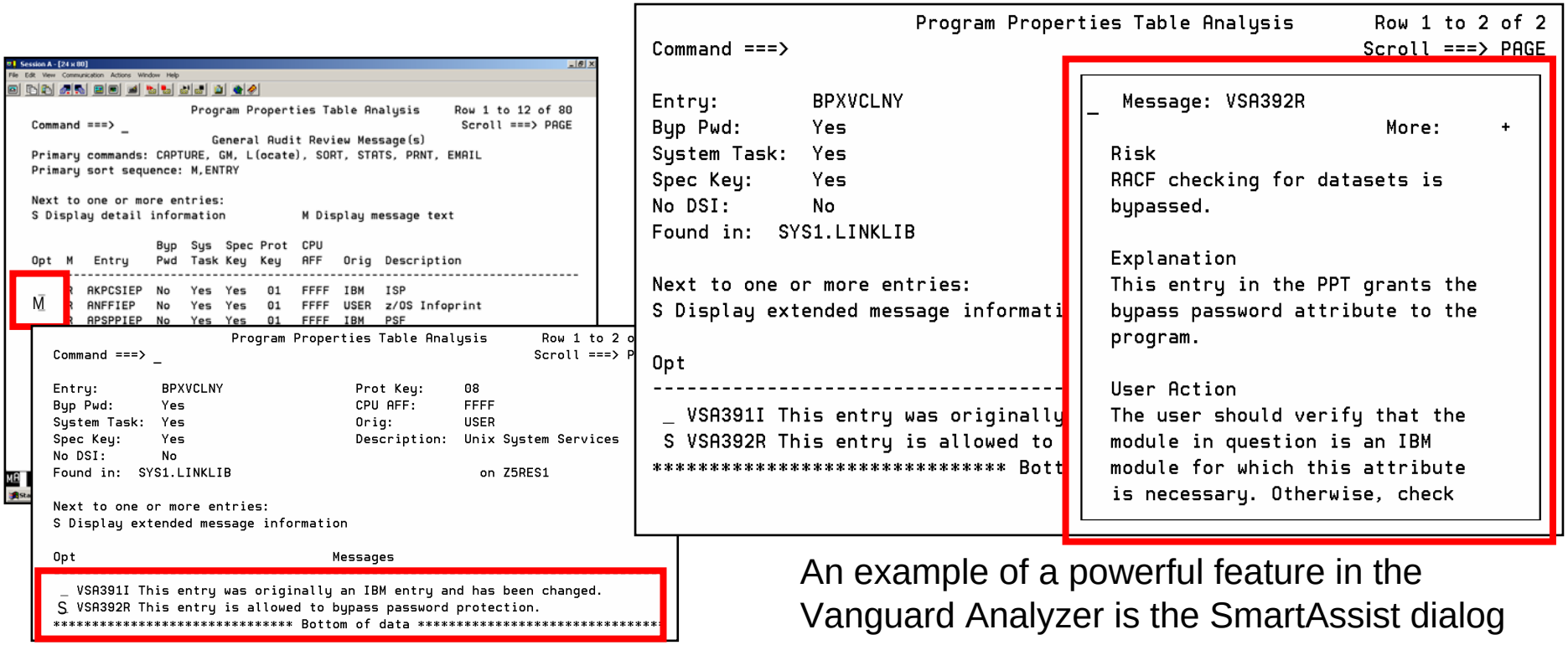
Analyzer - Risk Identification & Assessment

The powerful auditing tool prioritizes and highlights areas to show where a potential security exposure may exist



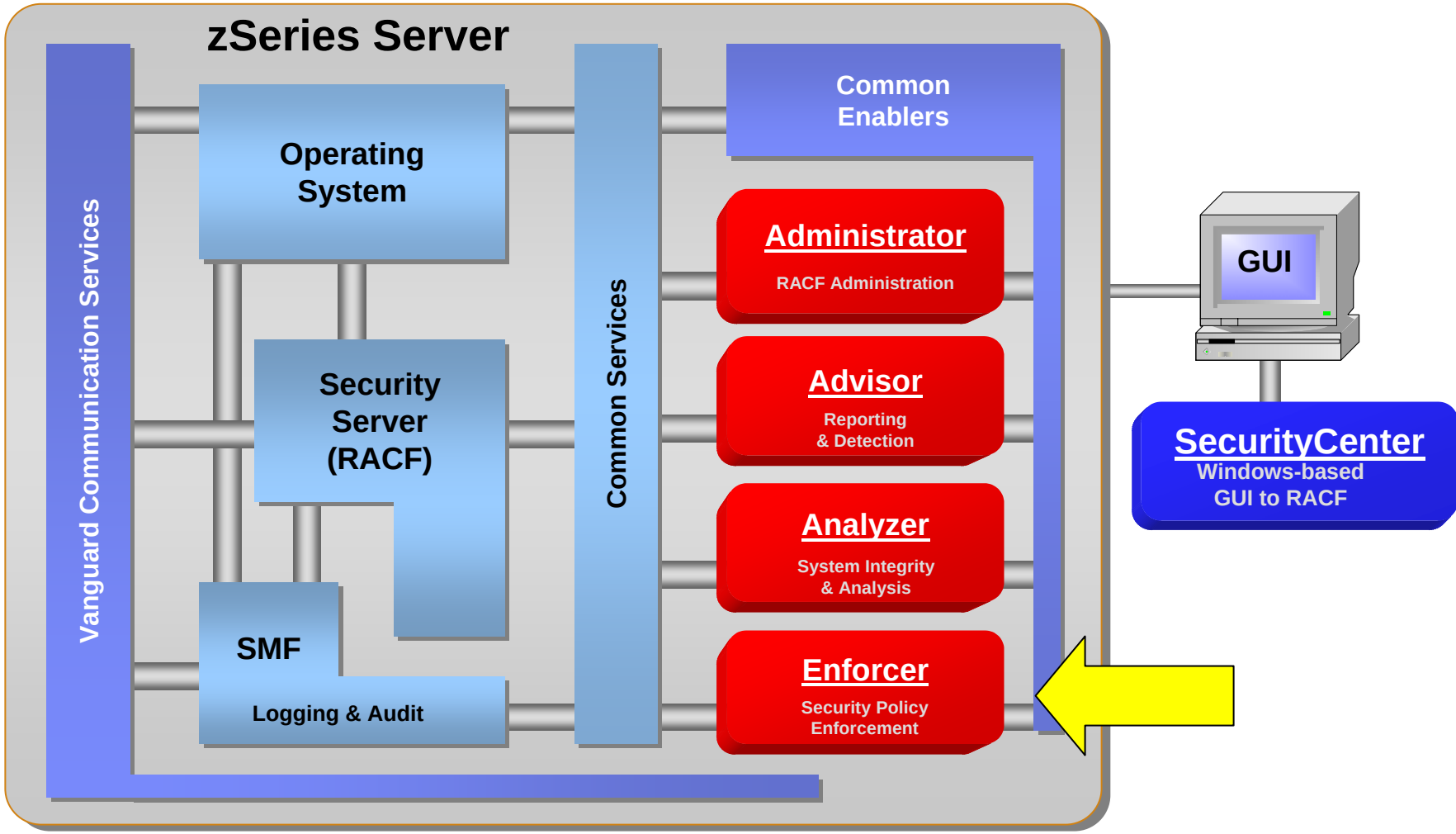
Analyzer – System Integrity and RACF Analysis

A system integrity, assessment, risk identification, threat analysis and problem rectification solution.



An example of a powerful feature in the Vanguard Analyzer is the SmartAssist dialog

Vanguard Products



Enforcer – Security Policy and Rules Enforcement

Intrusion Detection and Management for z/OS

- z/OS based real time security policy enforcer.
- Know immediately if a key asset has been altered.
- Allows for a documented, secured temporary access to a privilege to be granted and automatically revoked.
- Creates a Baseline Security Policy using expert recommendation that you can modify to your companies specifications and enforce in real-time.
- Enhances existing zSeries Security Server (RACF) security policy administration at the enterprise level without requiring additional staff, additional expertise, or ongoing maintenance.
- With Enforcer, organizations can be confident that their security management implementation is effectively protecting their critical resources and continuously adhering to "Best Practices" standards.

Enforcer – Security Policy and Rules Enforcement

Intrusion detection and management solution for the mainframe

- Enforcer protects critical data and other resources by ensuring that the standards, policies, rules and settings defined by an organization's security and compliance experts are in force and stay that way.
- The baselines contain the security policies and implementation rules for the specific system being monitored.
- Enforcer automatically scans the operating system and RACF database at intervals defined by the user and compares what it currently finds against the authorized baselines.
- When discrepancies are found, Enforcer will perform, as defined by the user, operations such as:
  - Log the discrepancy for later analysis and control purposes.
  - Notify predetermined individuals of the discrepancy.
  - Automatically take corrective action to restore the system to the baseline configuration.

Enforcer – Security Policy and Rules Enforcement

A system integrity, assessment, risk identification, threat analysis and problem rectification solution.

1. User makes unauthorized changes to the permissions of a critical file.

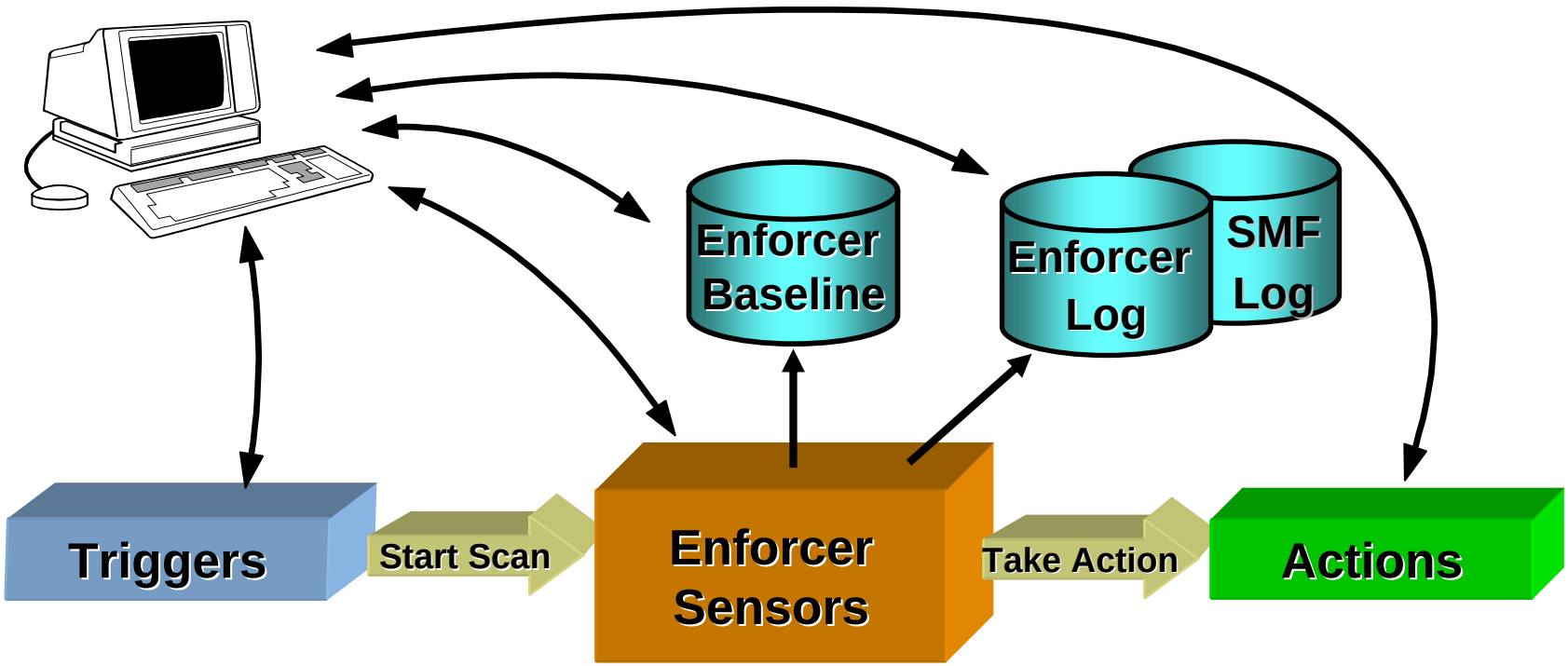
INTRUSION DETECTED

Date/Time: 04/01/05 5:00p
Resource: Payroll Database
User ID: TELLER1

3. Security Administrator receives the call and takes appropriate action.

2. Enforcer detects the event, automatically puts the permissions back and sends an alert to the security administrators cell phone with details of the event.

Enforcer Sensor Task Overview

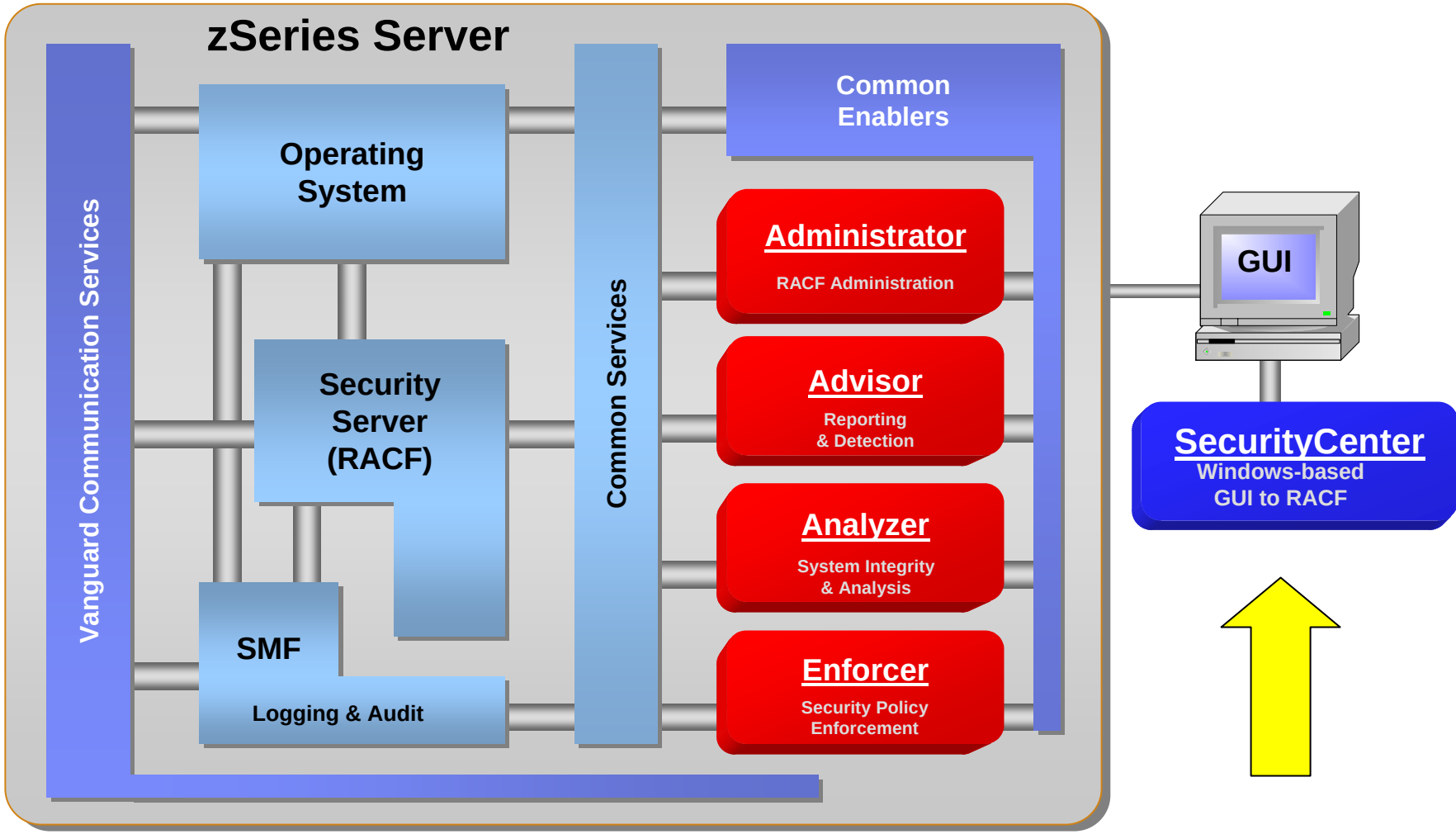


- Startup
- Manual
- Time-Interval

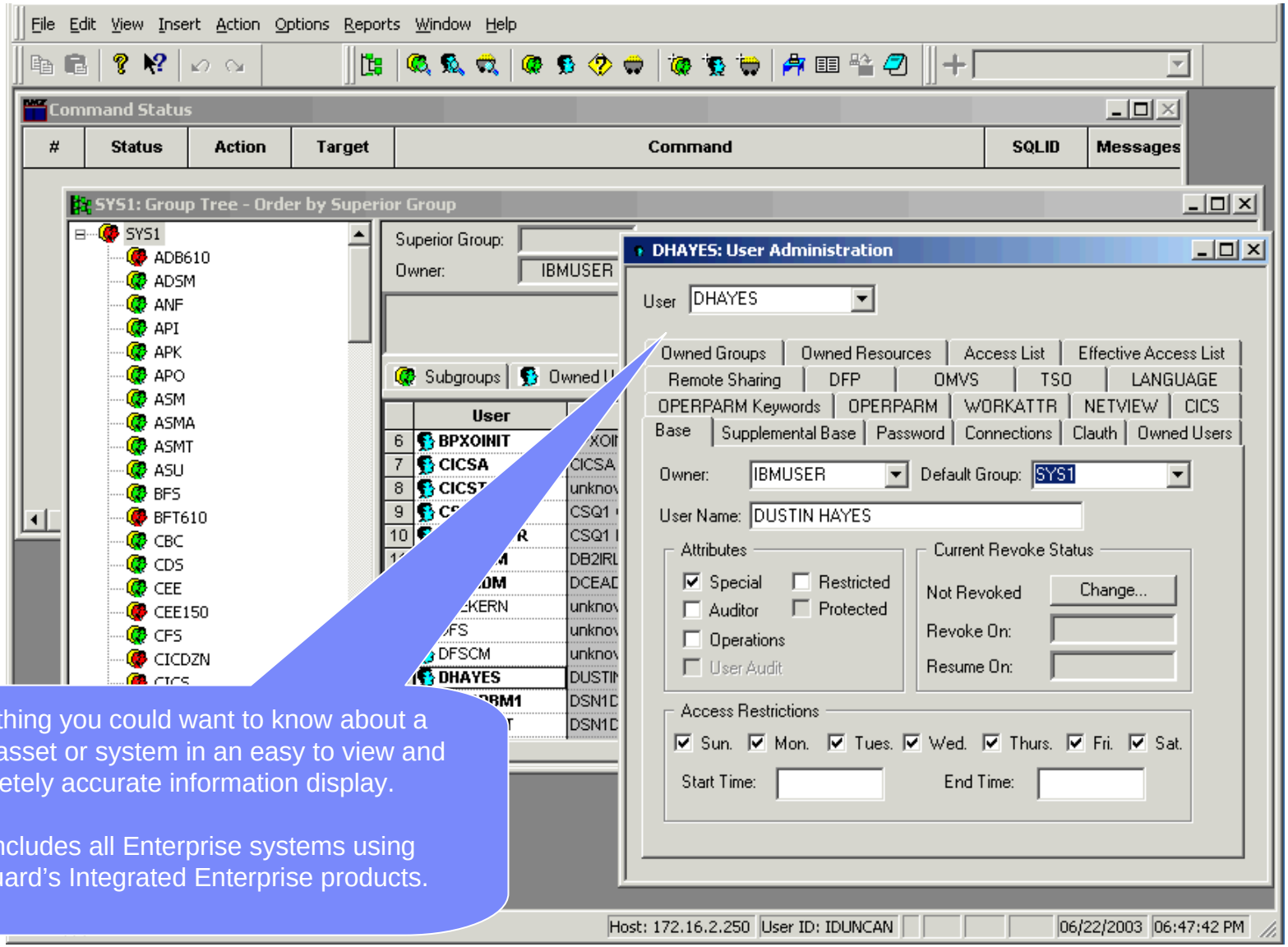
- Critical Data Sets
- Critical Volumes
- Critical Gen'l Res.
- Critical Groups
- Privileged Users
- APF Libraries
- LINKLST Libraries

- RACF Options
- LPA List
- PPT
- SVCs
- Started Tasks
- Restricted Utilities
- Temporary Access

Vanguard Products



SecurityCenter – RACF Like You've Never See It Before



Everything you could want to know about a user, asset or system in an easy to view and completely accurate information display.

This includes all Enterprise systems using Vanguard's Integrated Enterprise products.

SecurityCenter – RACF Visual Based Administration

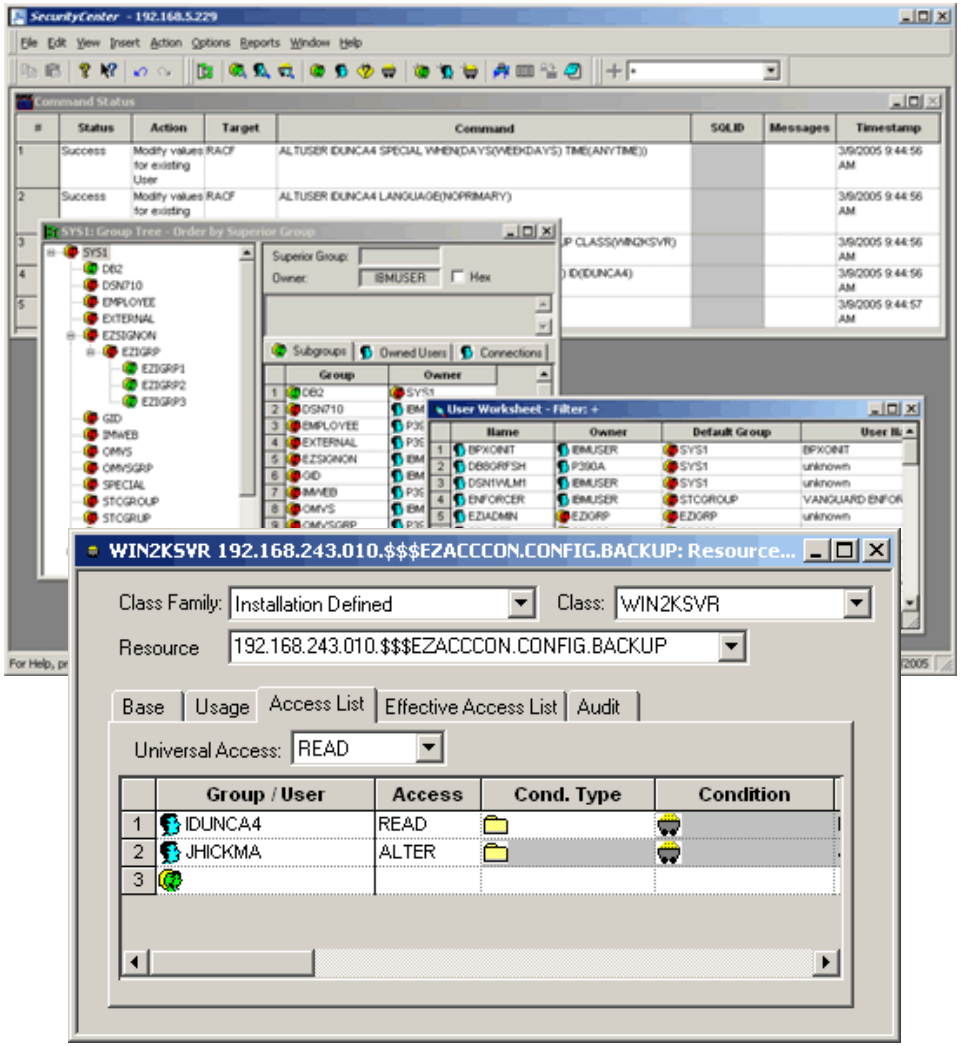
- Easy Graphical User Interface to the RACF Database.
- Ease of use for existing RACF administrators.
- Allows non-z/OS personnel the ability to understand and administer RACF.
- Intuitive Windows based interface, reduces errors especially when doing repetitive administrative tasks
- Help desk password reset functions.

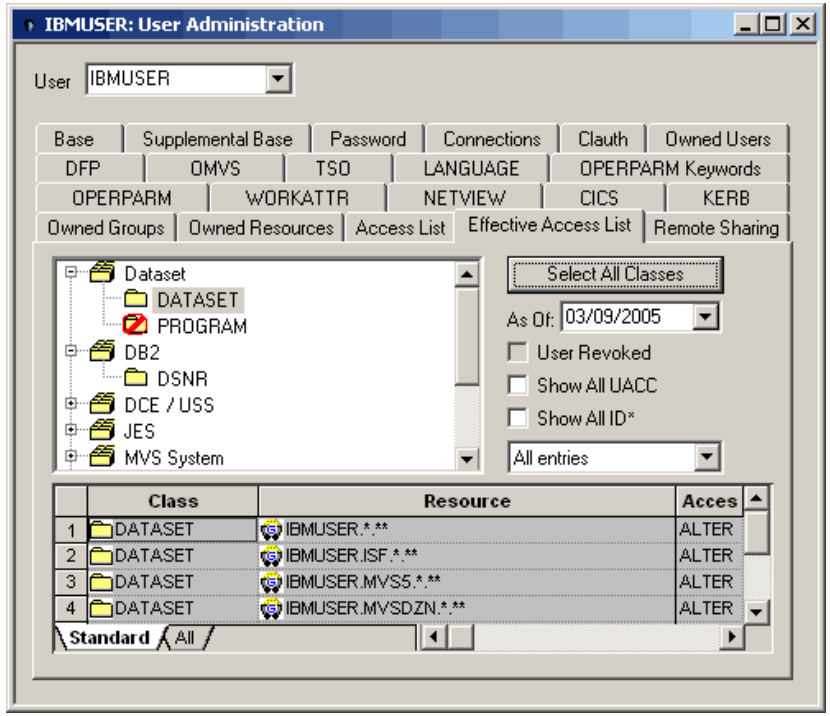
SecurityCenter – RACF Visual Based Administration

Windows-based RACF administration

- SecurityCenter graphically presents hard-to-find security information.
- Point-and-click and drag-and-drop operations replace dozens of native commands.
- Data is entered using familiar Windows-style features such as drop-down lists, radio buttons and check boxes.
- SecurityCenter allows security administrators to decentralize appropriate tasks to departmental level personnel by offering them limited views to their information.
- Enables the experienced security administrator to work more efficiently.
- SecurityCenter provides an easy, intuitive training environment that brings less experienced staff members up to speed quickly.

SecurityCenter - RACF Visual Based Administration

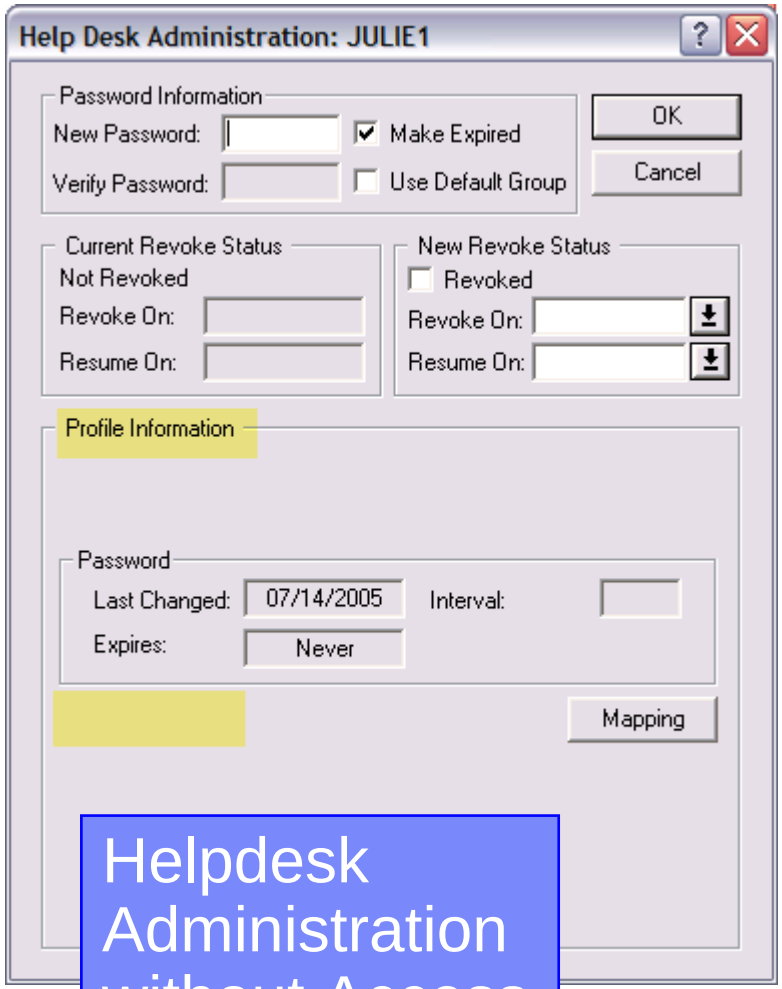




SecurityCenter graphically presents RACF administration in a Windows point-and-click, drag-and-drop interface.

Allowing security administrators of different platforms to administer RACF without having to learn native RACF commands.

SecurityCenter – RACF Helpdesk Administration



Helpdesk Administration without Access

REVOKE

OWNER

NAME

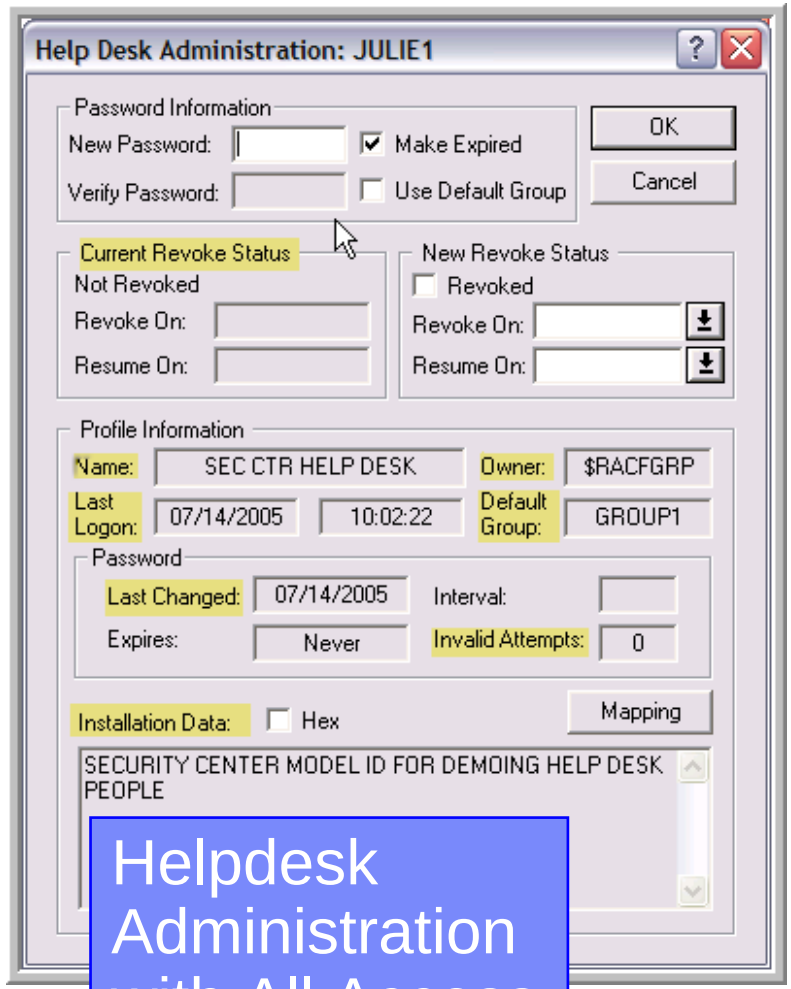
DFLTGRP

LASTUSED

PASSDATE

PASSVIOL

INSTDATA



Helpdesk Administration with All Access

Vanguard's RACF Administration and z/OS Compliance Tools

Summary

- Efficient RACF security management, access control, reporting and compliance monitoring across the Enterprise.
- Reduces the costs of RACF administration.
- Provides a platform for centralized security administration across the enterprise.
- Assists in ensuring security best practices.
- Provides evidence of IT controls for SOX, GLBA, HIPAA and other regulatory mandates.
- Maximizes the productivity of security staff.

Available Services

- Product Implementations
- Training
- z/OS & RACF Health Checks & Remediation
- Migrations from CA-ACF2® and CA-Top Secret® to RACF

An Enterprise Security Problem

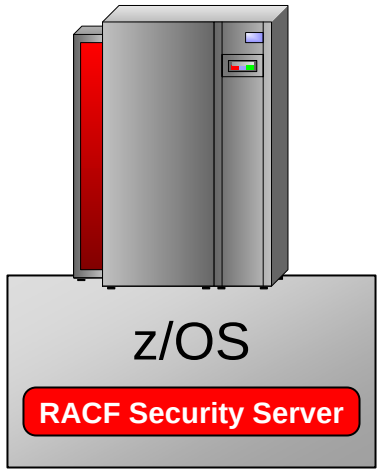
Problem – This Is What Goes On In The Background

Security-on-Demand secure domain concept

Summary

- Ability to administer users and data
- Across dispersed and dissimilar platforms & systems
- Using a single common interface
- Allowing user to sign-on with one password
- With a way to log and report everything from the same place with the same tools
- A solution based on eServer zSeries
  - 99.999% uptime
  - 85% of the critical transactions
  - 80% of the mission critical data

We've Had The ESM Problem Before



CICS Tables
Security

DB2
Security

Applications
Security

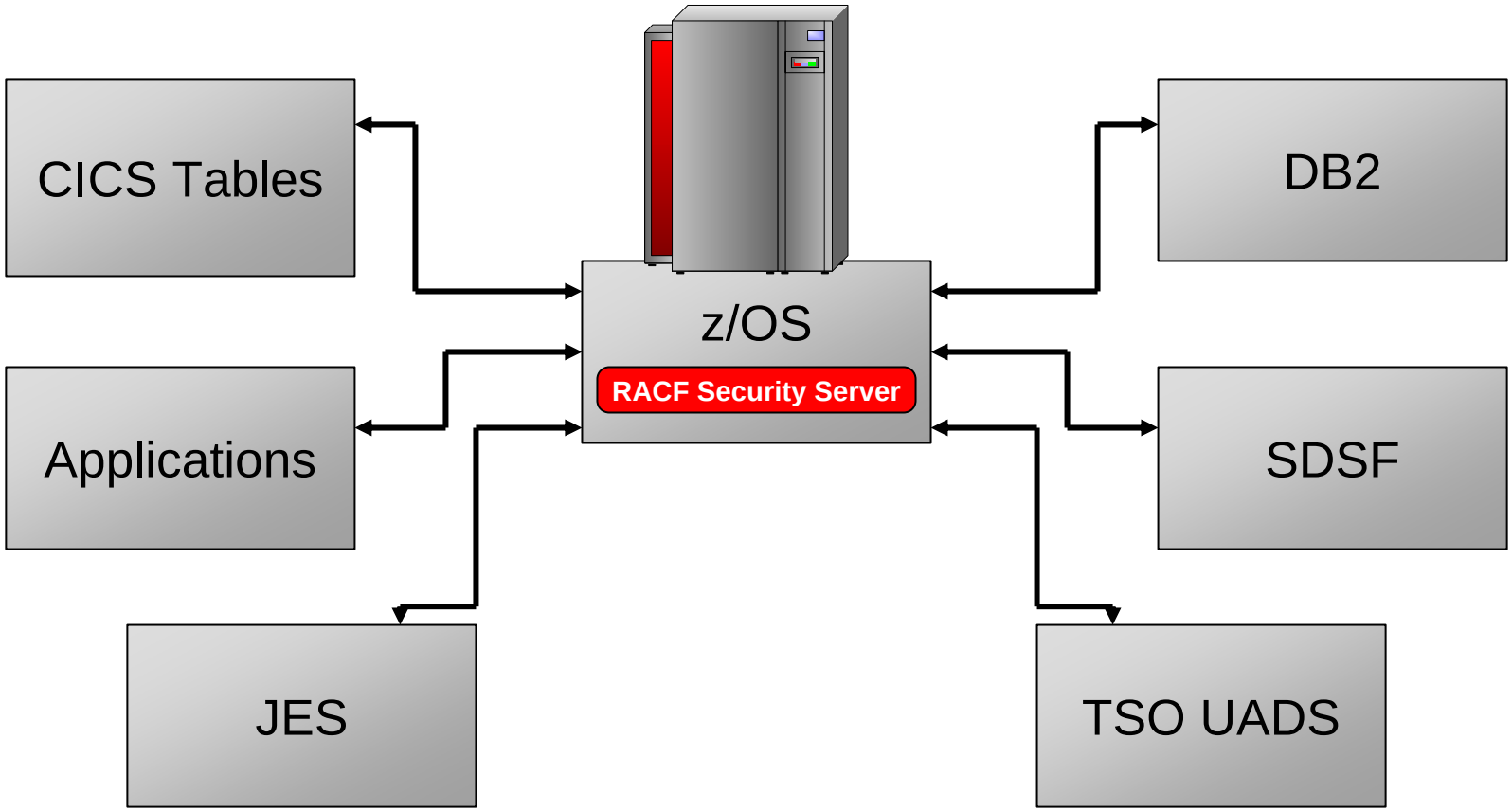
SDSF
Security

JES
Security

TSO UADS
Security

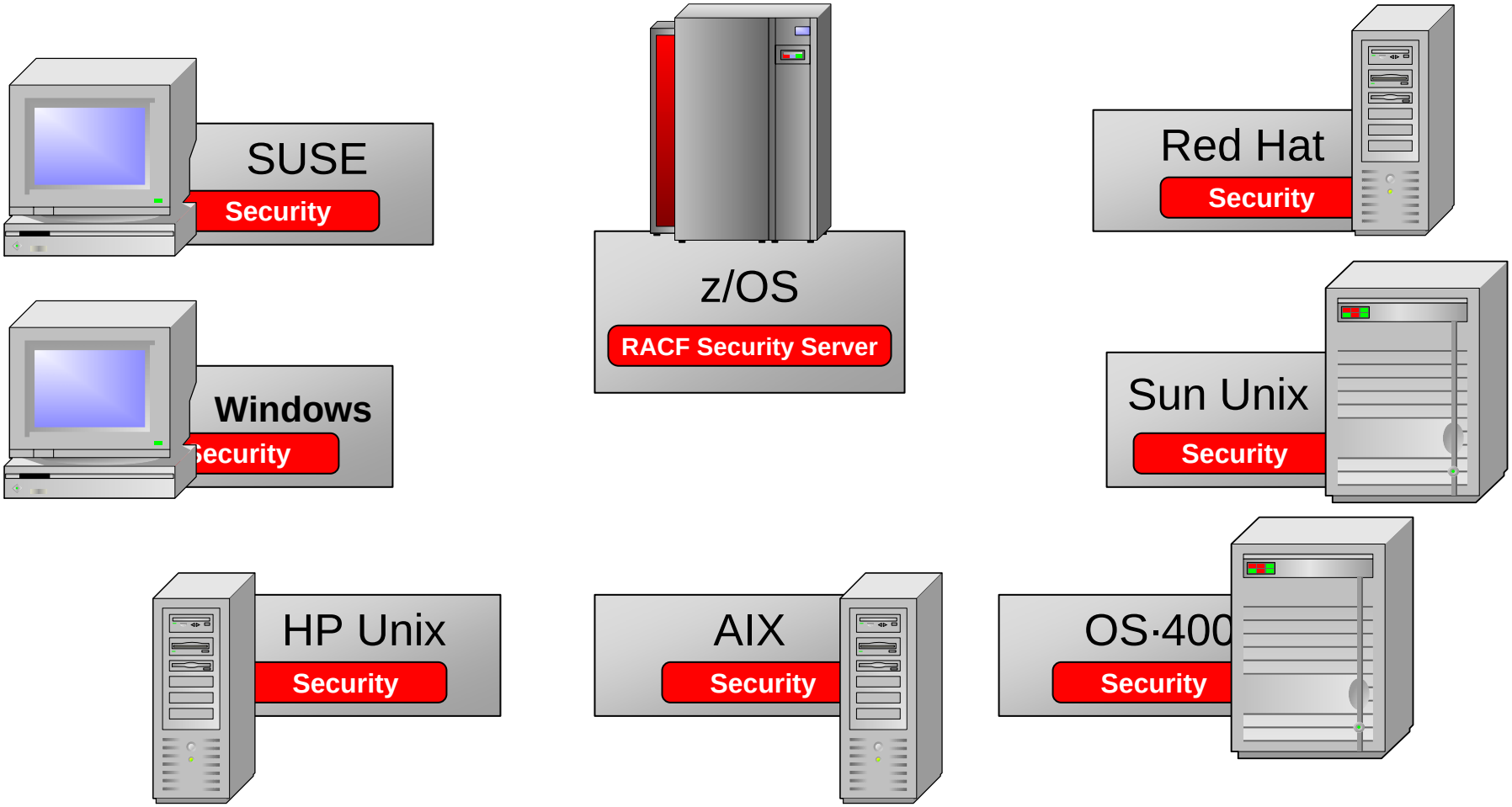
Before distributed computing, each component on a mainframe had its own security system (individual and disconnected secure domains)

IBM's Proven and Simple Solution



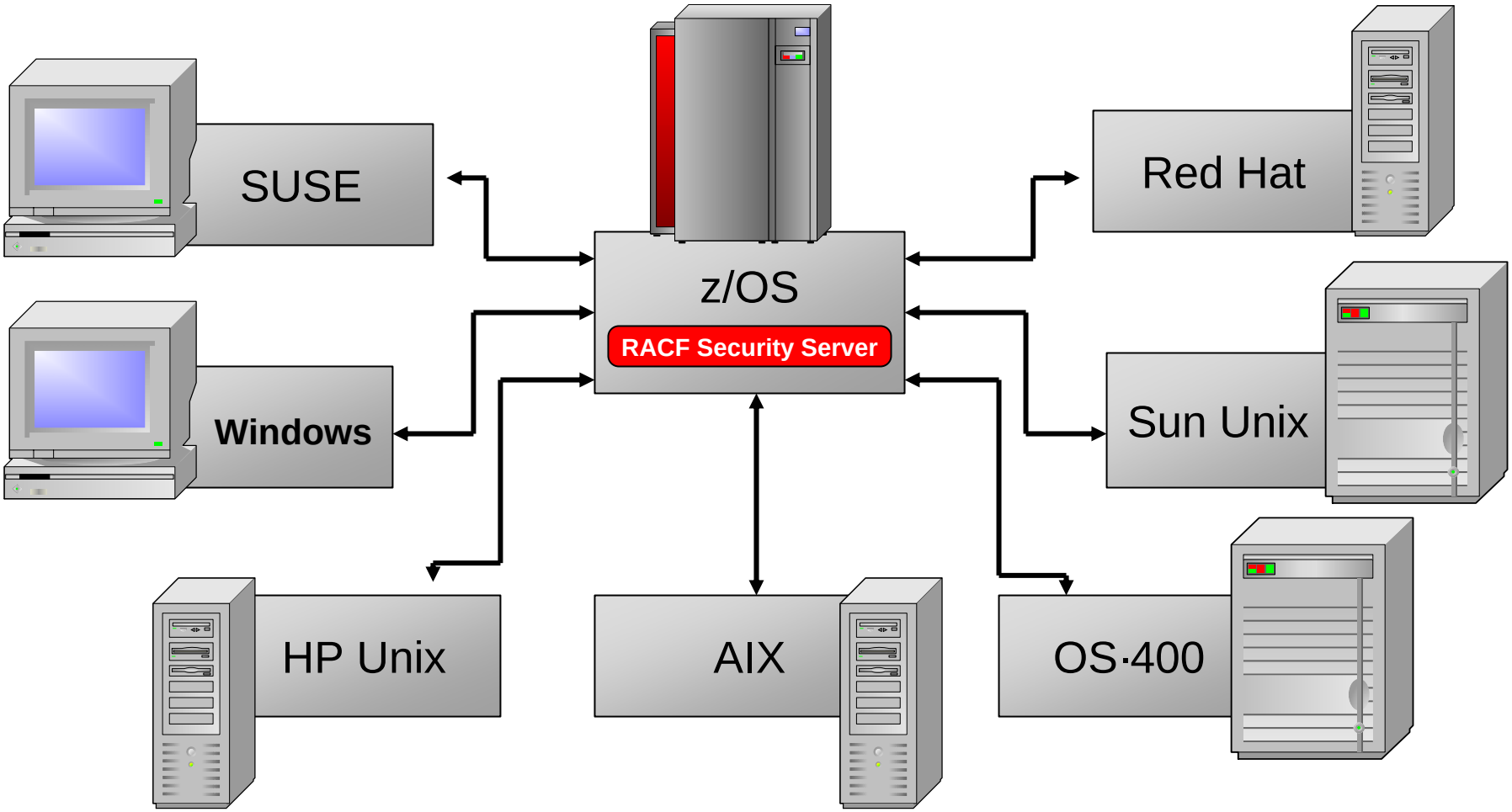
IBM now uses the z/Series Security Server (RACF) as the only security server for each of the different components (single secure domain concept)

Today's Enterprise Problem



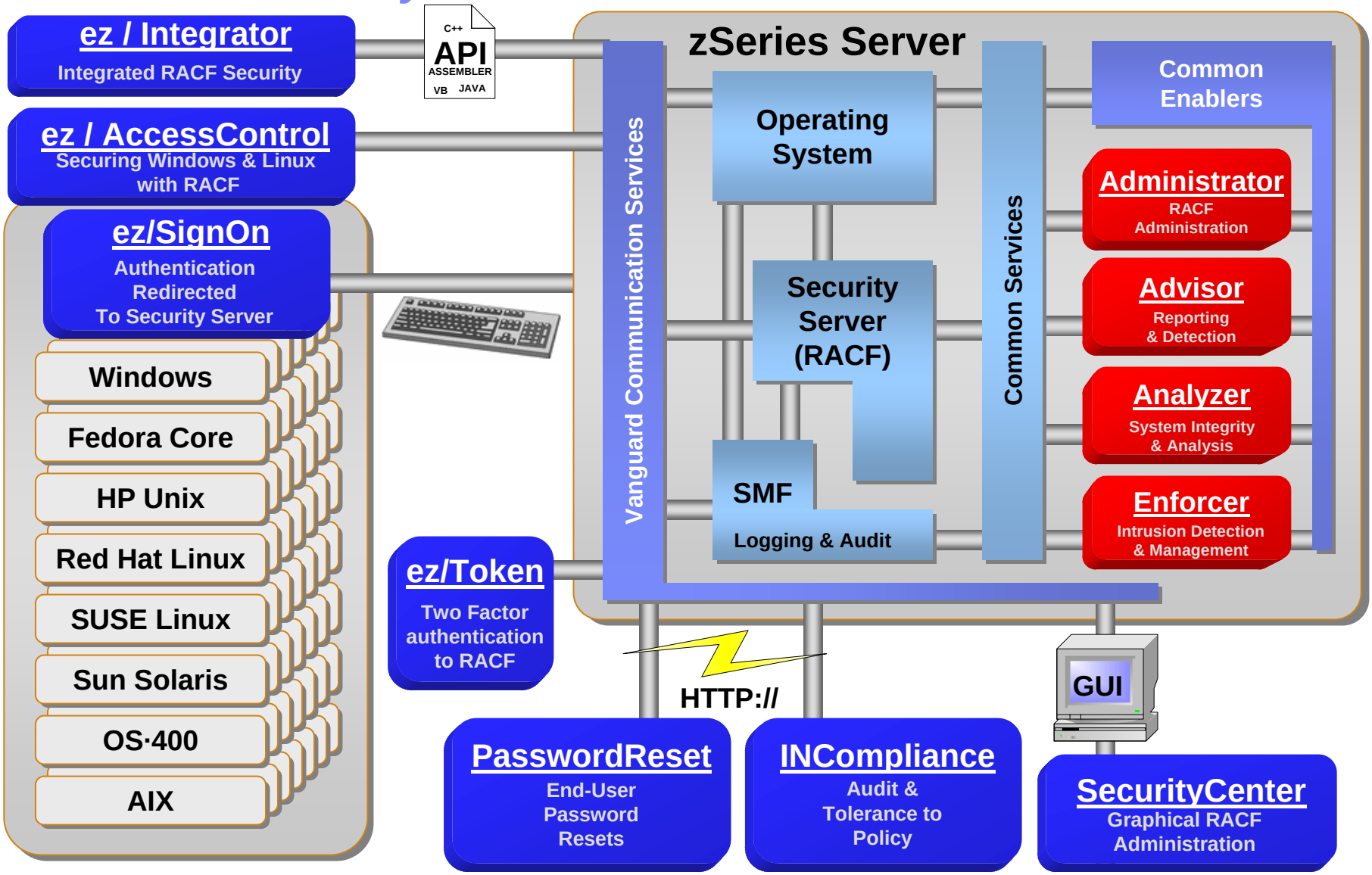
Multiple components in the enterprise each having their own security systems, Individual and disconnected, just like the problem used to be.

Solved With the Same Simple Solution

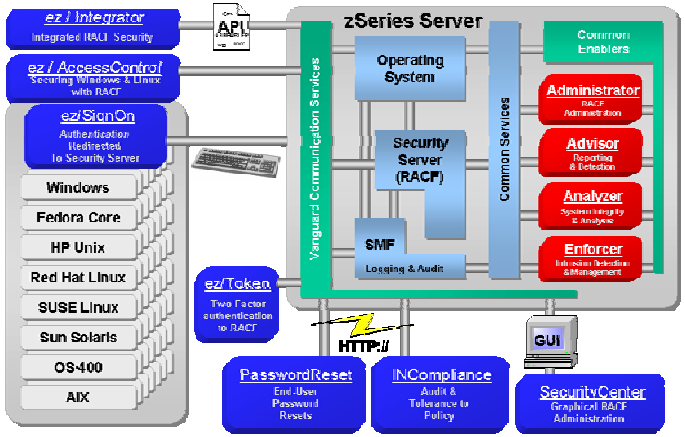


Vanguard extending the power of the z/Series Security Server to distributed components, treating the enterprise as a single secure domain.

Security-On-Demand Architecture



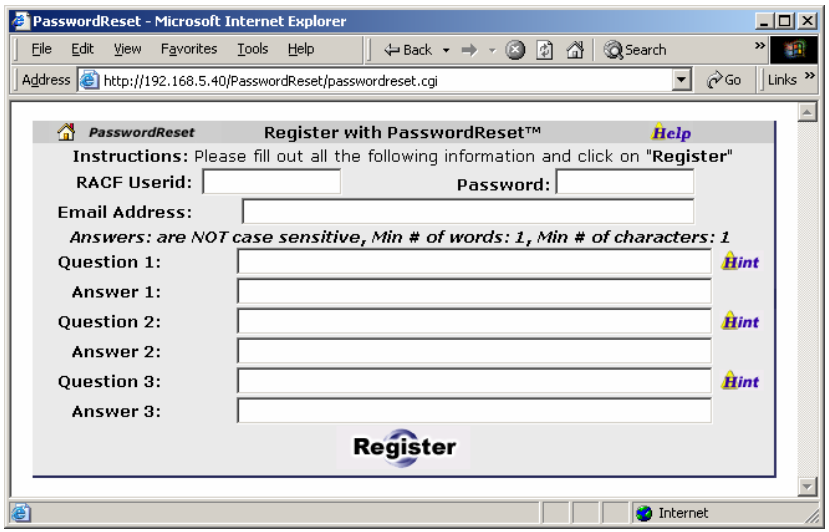
Vanguard PasswordReset



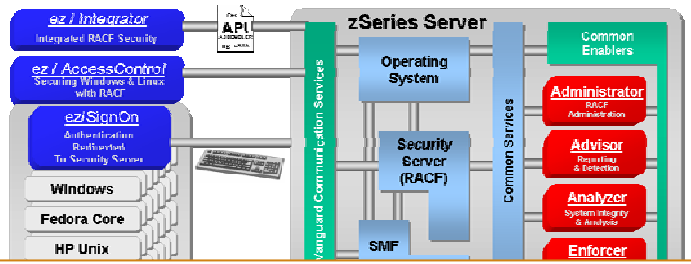
system. An average password reset call to the Help Desk costs $25 to $40. The ROI on this product is less than 12

1. Users self-enroll using a simple web-based interface

2. When a user forgets their password they can click a button at the logon screen, answer their set of questions, reset their password and login



Vanguard ez/SignOn & RegistrationManager



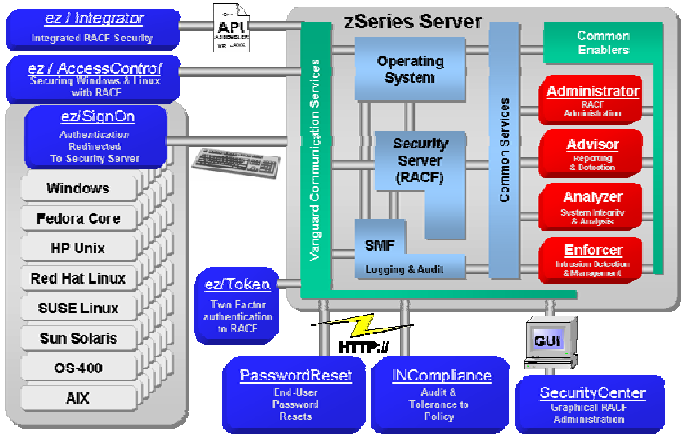
A self-registration, single-password and intrusion detection solution for multi-platform environments.

	ez/SignOn SoD RACF ID	z/OS Server	Windows Server 1	HP UNIX Server 1	Windows XP Workstation	Sun Solaris 1	Windows 2000 Workstation	RedHat 1	
Bill Murray	RACFWIN	RACFWIN	WINUSER		WINUSER	SUNUSR1	WINUSE2		...
Chevy Chase	CCHASE			HPUSER1			WIN2USR	RHUSR1	...
Dan Ackroyd	ZUERT2	ZUSER2	WINUSR2	HPUSER2		SUNUSR2			...
Ted Knight	TKNIGHT		WINUSR3		WINUSER3	SUNUSR3	WIN2USR3	RHUSR2	...

With the Security-on-Demand Federated ID and mapping matrix, one can report and track users/systems and report on user activities across the entire cross-platform enterprise fabric, even when the users platform IDs are different.

With a single command revoking the SoD RACF ID stops all user access to systems and data instantly.

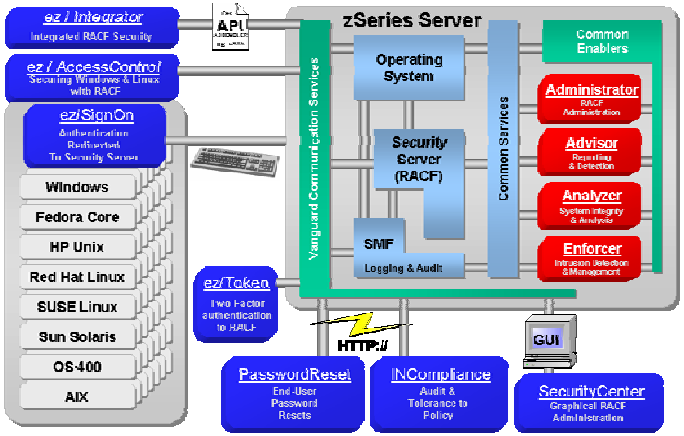
Vanguard ez/Integrator – a.k.a. RACF Anywhere



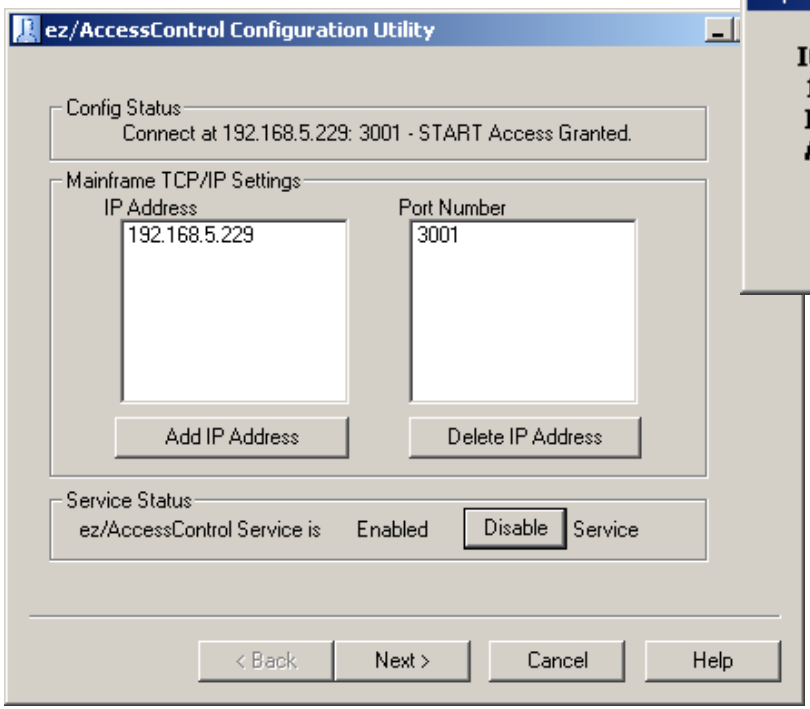
Allows platforms, applications and devices to interface and integrate the proven authentication, authorization and auditing capabilities of IBM's zSeries Security Server.

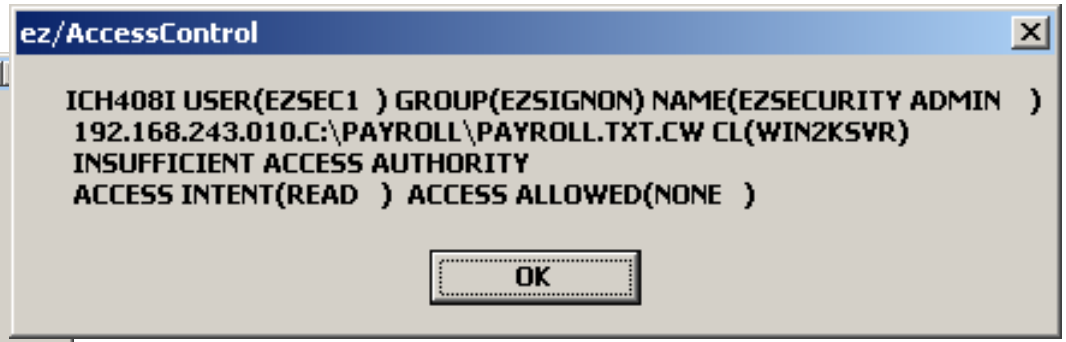
ez/Integrator is an easy-to-use Tool Kit for the IBM zSeries Security Server

Vanguard ez/AccessControl



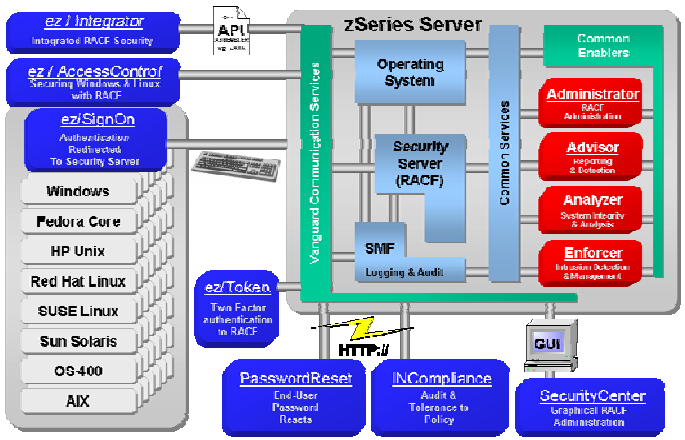
Control Windows® applications and files with the premier security power of the IBM zSeries Server, RACF®





ez/AccessControl provides a single point of access control, routing all requests for access to a drive, file, or directory on a Microsoft Windows 2000 and 2003 platforms through the IBM Security Server™ (RACF®).

Vanguard ez/Token



ez/Token™, a two-factor authentication solution integrated with RACF® for users logging on to the mainframe.

The ez/Token solution provides a more secure alternative than the usual RACF user ID/password combination. With ez/Token, users substitute a new, one-time passcode in place of a password. Passcodes are generated randomly every 60 seconds. For enhanced security, the passcode can be combined with a PIN number.

धन्यवाद

Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

Thank You

English

شكرا

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

Questions

- More information
  - http://www.go2vanguard.com/
  - ronn.bailey@go2vanguard.com