



Vanguard Security Solutions for the Mainframe



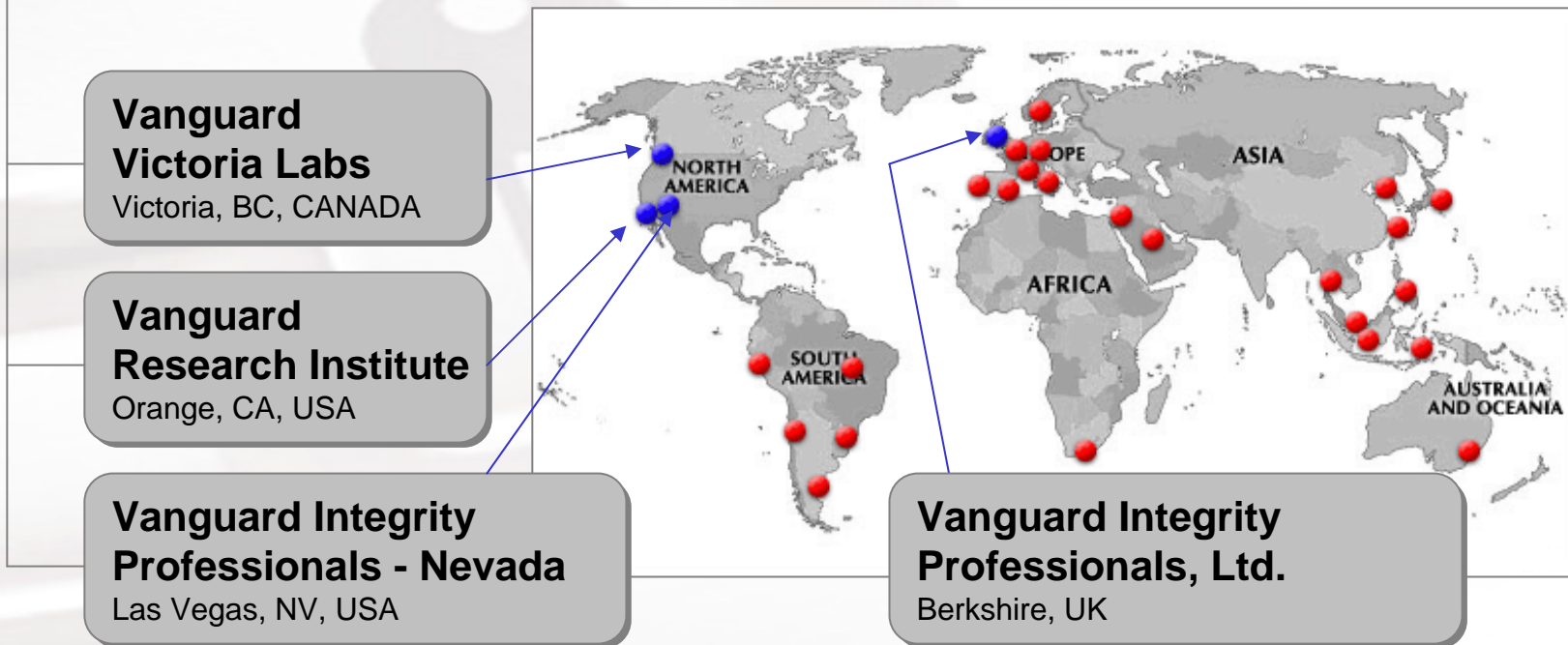


- **Vanguard Credentials**
- **History of Mainframe Security**
- **Vanguard Security Solutions for the Mainframe**

About Vanguard



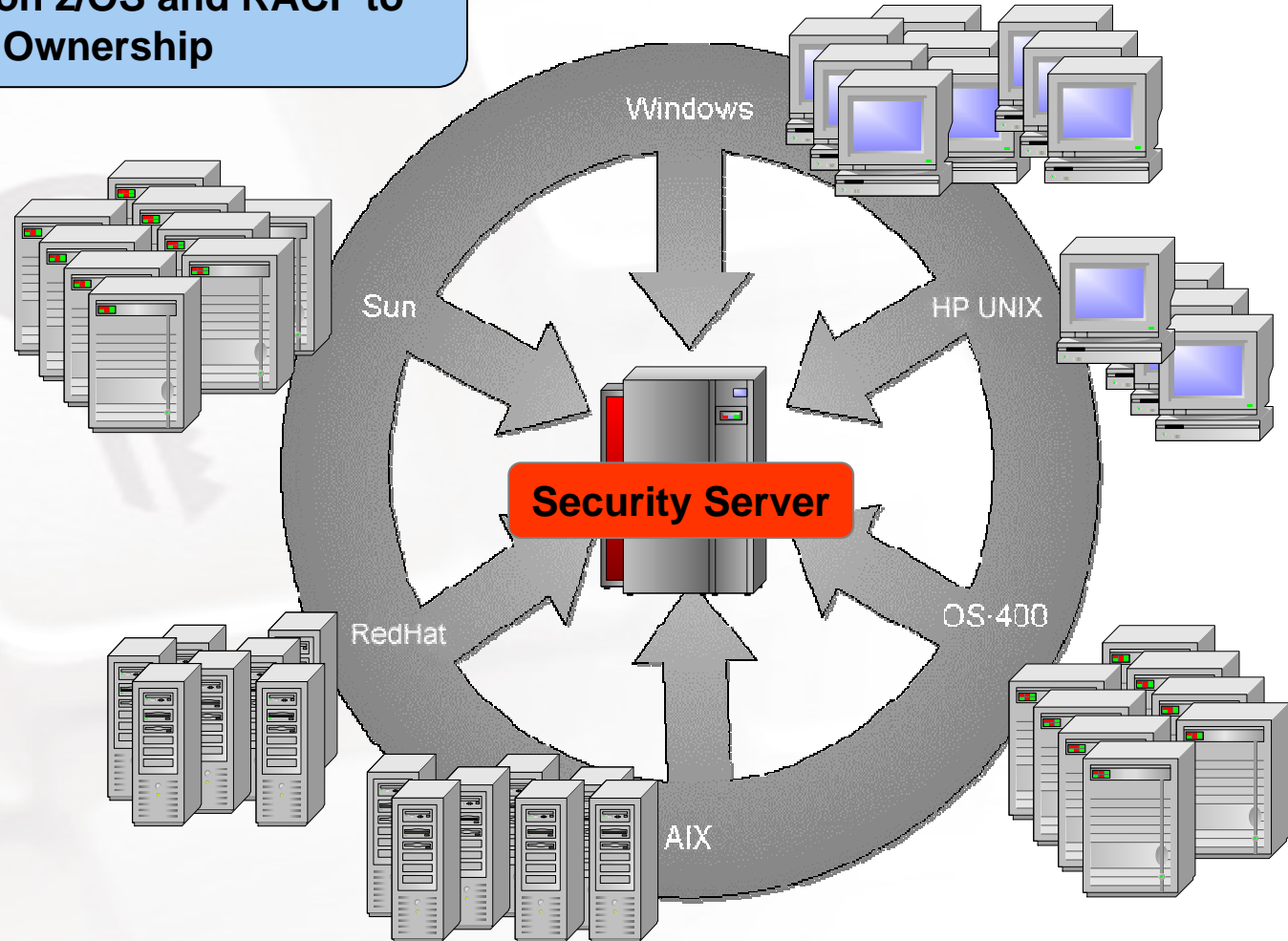
Founded: 1986
Ownership: Privately held
Business: Information Security Software, Training, Services, & Solutions
Customers: 600 domestic and abroad, 1,400 software licenses



More than 20 distributors/resellers servicing 50+ countries worldwide

Corporate Agenda

Centralization of Security Services and Administration built on z/OS and RACF to reduce Total Cost of Ownership



Vanguard Offerings






RACF-L archives -- May 2000 (#262) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://listserv.uga.edu/cgi-bin/wa?A2=ind0005&L=racf-l&D=0&X=4202CB3CD9A834E0F4&Y=racfuser@hotmail.com&P=2> Go



www.listserv.uga.edu
The University of Georgia

Home | Browse | Manage | Request | Manuals | Register

Navigation icons: back, forward, home, search, etc. Username: jkl jkl

Date: Fri, 12 May 2000 13:14:58 PDT
Reply-To: RACF Discussion List <RACF-L@LISTSERV.UGA.EDU>
Sender: RACF Discussion List <RACF-L@LISTSERV.UGA.EDU>
From: Rodolfo Landa <rudy_land@HOTMAIL.COM>
Subject: RACF in Vancouver, BC, Canada
Content-Type: text/plain; format=flowed

Hi there everybody.

I just moved from Mexico City to Vancouver, BC, Canada.

I worked 6 years with RACF in my country and I want to keep working in Security Information up here.

My problem is how to know which companies are using RACF in Vancouver so I can contact them. Do you folks can advice me on my job search?

Regards

Rodolfo Landa
e-mail : rudy_land@hotmail.com

Get Your Private, Free E-mail from MSN Hotmail at <http://www.hotmail.com>

Back to: [Top of message](#) | [Previous page](#) | [Main RACF-L page](#)

Done Internet



Search Results - Microsoft Internet Explorer

Address <http://lists.go2vanguard.com:81/read/search/results?forum=vanguard-l&words=RACF+help&in=:> Go

LYRIS ListManager You are: id

Messages Search Conference My Account My Forums All Forums About

Search Results

Your search for 'RACF help' found more than 100 results. Returning the first 10 results.

Date	Subject
2005-08-17 08:00:00	RE: How to get LRD of dataset profile in batch
2005-08-17 05:35:00	RE: How to get LRD of dataset profile in batch
2005-08-17 01:38:00	How to get LRD of dataset profile in batch
2005-08-16 10:29:00	RE: Cloning multiple rules in one step
2005-08-15 06:50:00	RE: Inconsistency in RB and CL for grouping class
2005-08-15 05:45:00	RE: Inconsistency in RB and CL for grouping class
2005-08-12 13:04:00	RE: Vanguard Administrator - How To Produce A User Summary and Installation-Data Combined Report
2005-08-12 10:28:00	RE: Inconsistency in RB and CL for grouping class
2005-08-12 09:50:00	Re: Error message trying to resume user that is hard revoked
2005-08-11 12:23:00	Re: Advisor Extract of RACF Commands

[previous](#) [next](#) [show more](#)

Internet

Over 500 members

600 discussion threads

Contributors include Vanguard Consultants, Industry experts, Vanguard Customer Service Reps

Tips & Techniques

Enterprise Security Expo & RACF Users Training



20th Annual Vanguard
**Enterprise Security Solutions
& RACF® Users Training 2006**
Security Solutions, Now!

140+ Educational Sessions

Who should attend?

Security Administrators
IS Management
Security Managers
EDP Auditors
Network Analysts

CIOs/CSOs
Network Administrators
System Technicians
System Programmers
IT Professionals

"There is nowhere else you can get this level of knowledge in one place. You are sorely pressed to make decisions on what sessions to attend."

- Casey Parker, Consultant
Parker Consulting

IBM Partnership



IBM Software Development Partner

IBM Early Support & ETP Programs

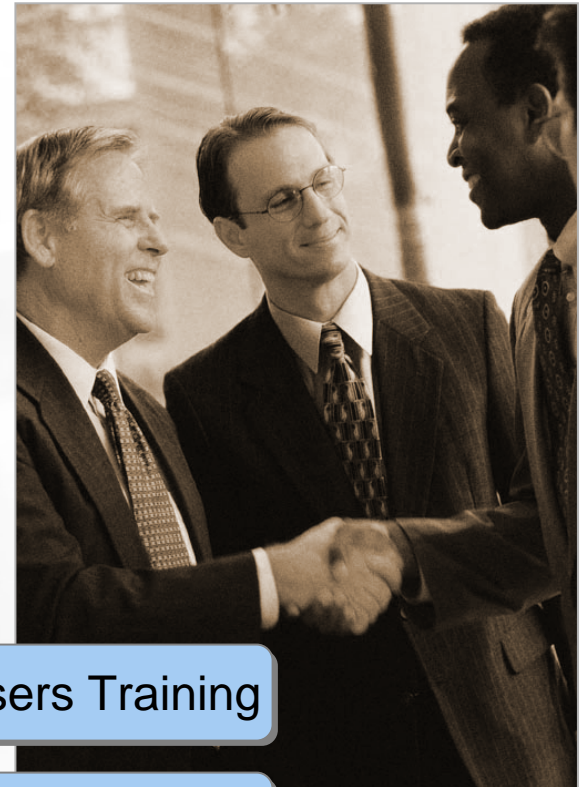
Perform Security Server training for IBM

Security Server (RACF) User Requirements

Certified IBM RACF Migration Tool User

Vanguard Enterprise Security Expo - RACF Users Training

5/9/05 Press Release – IBM signs Reseller Agreement





Vanguard Security Solutions for the Mainframe

Presented by

Art Hatfield-Mihelic

History of Mainframe Security



In the beginning there was DOS, and OS/MFT,
and OS/MVT on System 360sand



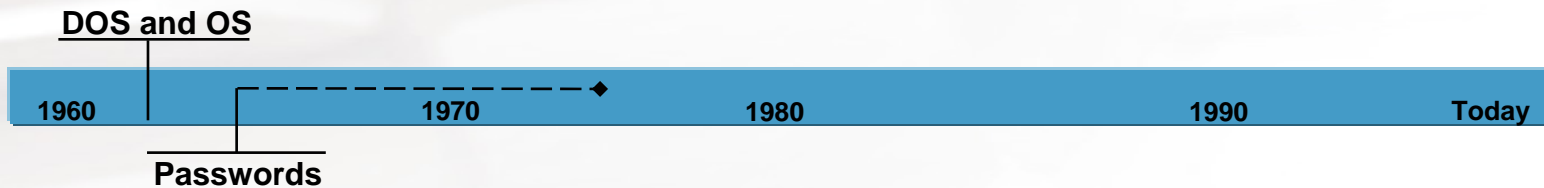
DOS and OS



History of Mainframe Security



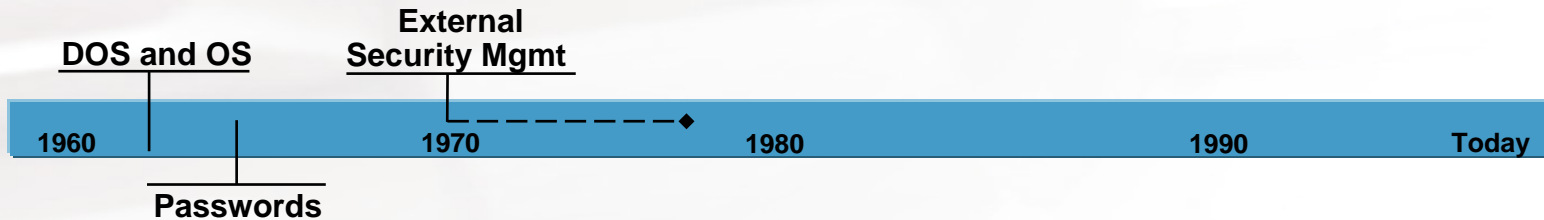
Security was Password Protection for Data Sets



History of Mainframe Security



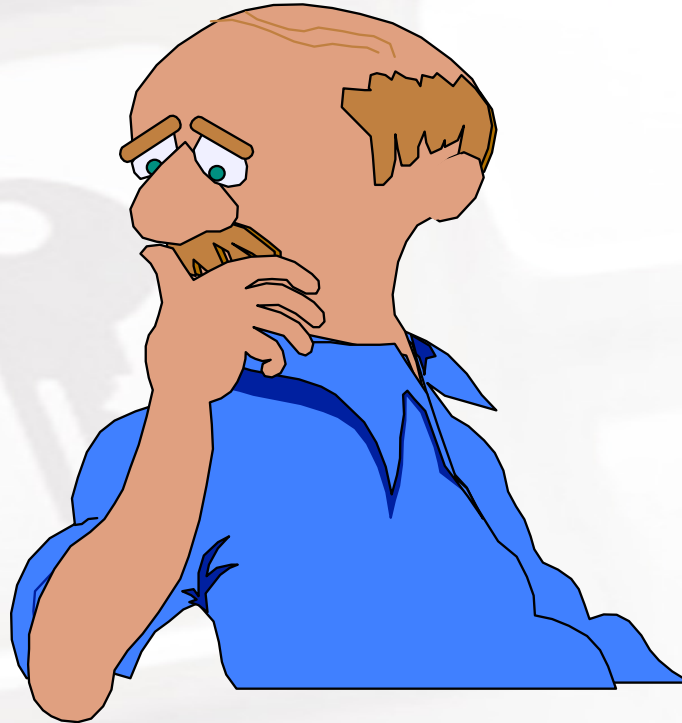
Then came the vision of the “External Security Manager”



History of Mainframe Security



And the decision to build or buy



Wait, there's a Systems Programmer with his own security application to protect his SYS1 data sets!

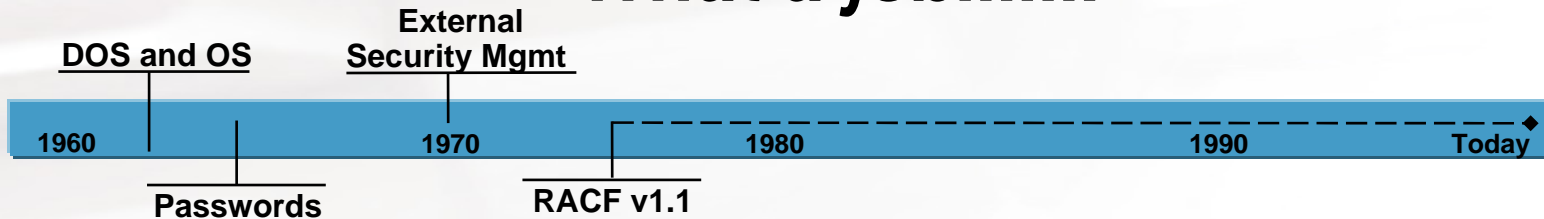
History of Mainframe Security



And hence came forth the Resource Access Control Facility (RACF)



What a job.....



History of Mainframe Security



It's genesis was technical in nature

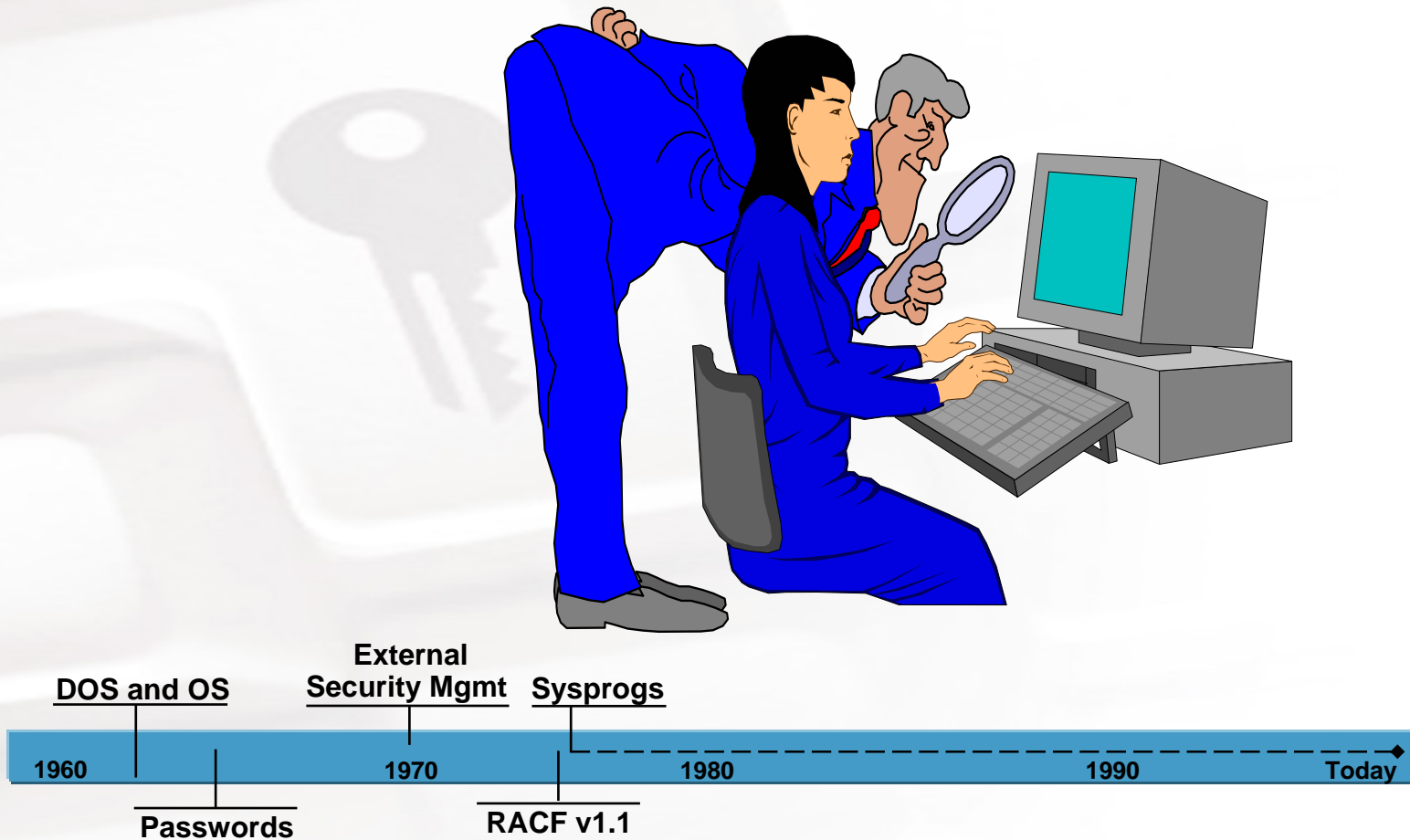


And it has retained that image over the decades

History of Mainframe Security



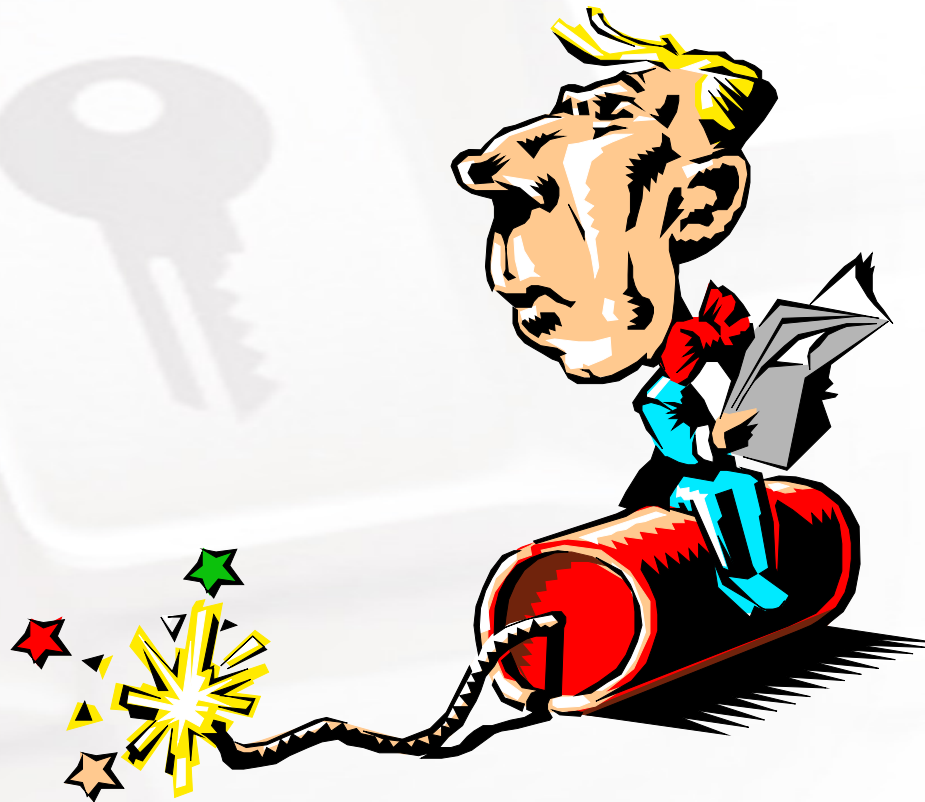
Initially there were no mainframe
“Security Administrators” or “Auditors”



History of Mainframe Security



Systems Programming was responsible for security and using RACF was not difficult for them

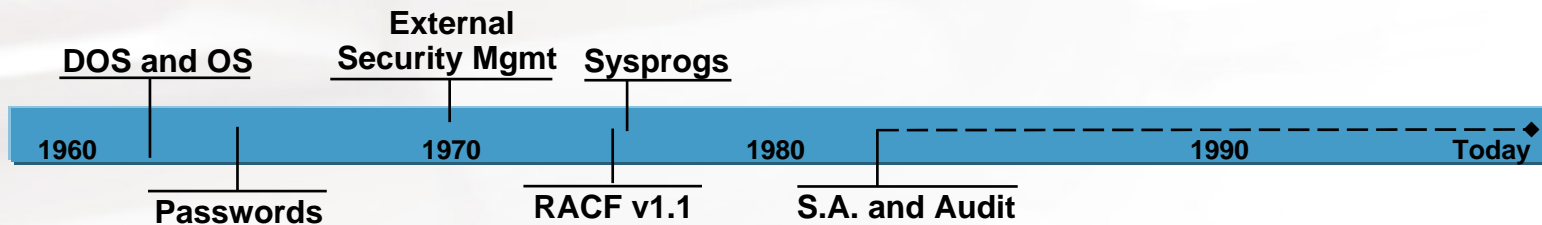
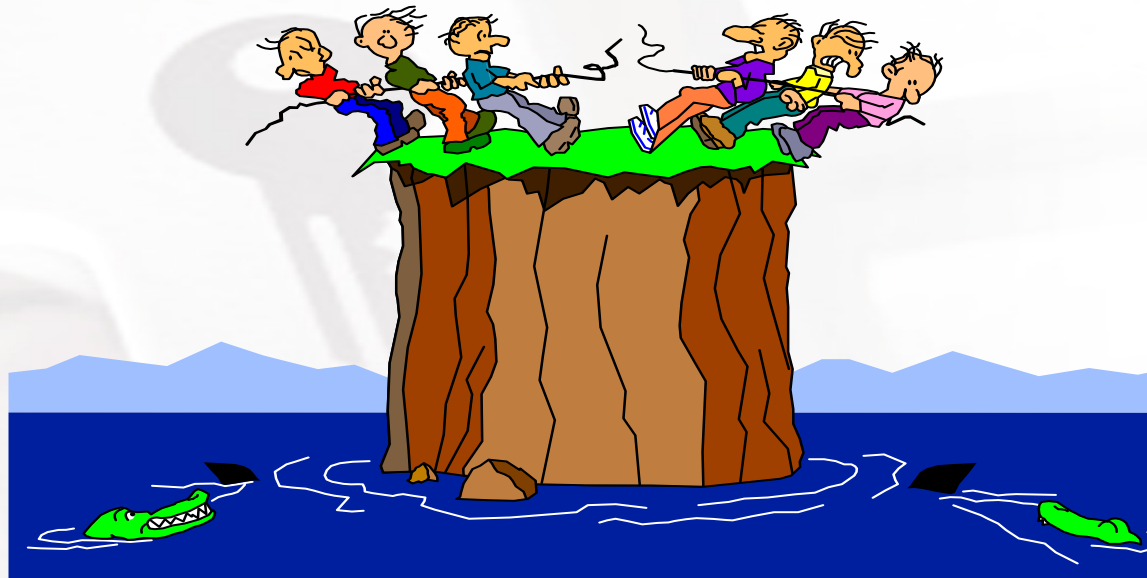


History of Mainframe Security



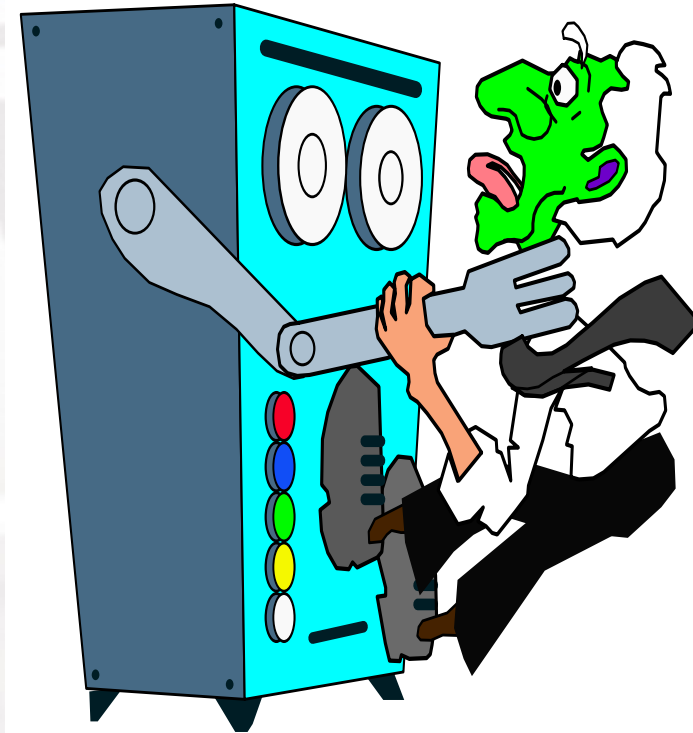
Then came separation of duties and two whole new professions were introduced

- IT Security Administration and Auditing





RACF was not as User-friendly for these professions





Training was made available





But the difficulties continued





Vanguard recognized the need and in 1989

V6.1
OPTION ==> ■

VANGUARD ADMINISTRATOR

Date: 05/10/19

Time: 11:04

ADMINISTRATOR MAIN MENU

- | | |
|-------------------------------------|------------------------------|
| 0 Initialize ADMINISTRATOR Options | 9 Vanguard Analyzer |
| 1 Task Oriented Administration | 10 Vanguard Advisor |
| 2 Security Server Commands | 11 Data Services |
| 3 Security Server Reports | 12 User Data Management |
| 4 On-line Access Analysis | 13 Connect Manager |
| 5 Command Scheduler | 14 Unix File Manager |
| 6 Vanguard Identity Manager | 15 Registration Manager |
| 7 Installation Data Management | 16 PasswordReset Reg Reports |
| 8 Information and Analysis Services | 17 Vanguard Enforcer |
| X Exit | ST Extract Statistics |

Active Extract Files: Small ==> VANGUARD.V6R1.SVSAM
Medium ==> VANGUARD.V6R1.MVSAM

Please consult the help text for this panel
regarding new feature information and contact information.

Copyright 1989-2005 Vanguard Integrity Professionals - Nevada.
All rights reserved.



The Administrator's initial purpose was

Data: Extract
COMMAND ==> ■

VANGUARD ADMINISTRATOR

Date: 05/10/19
Time: 11:08

TASK ORIENTED ADMINISTRATION

User

- 1 Clone
- 2 Delete
- 3 Notify
- 4 Transfer

User/Group

- 11 Owner
- 12 Remove
- 13 Replace

Group

- 21 Clone
- 22 Delete

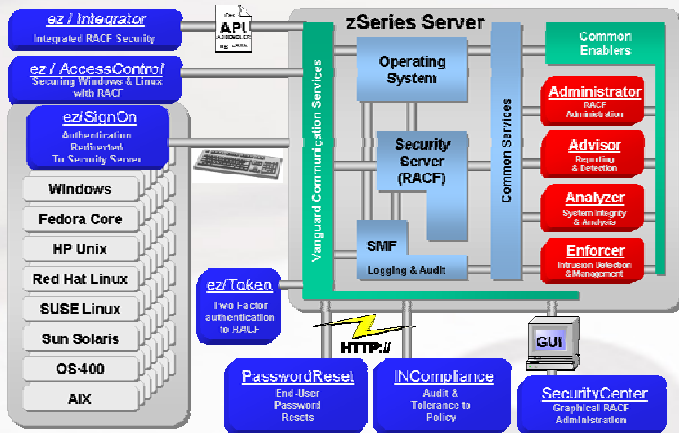
Data Set

- 31 Clone
- 32 Delete

General Resource

- 41 Clone
- 42 Delete

Vanguard Administrator - Today



Automated administration, data mining, reporting and analysis tool that enhances IBM's z/OS Security Server to become a mainframe policy and role-based user-provisioning tool.

Example: The Clone User task created a new functional user account in 27 seconds with 19 keystrokes - generating 190 commands consisting of 9549 keystrokes.

Done manually this would have taken two hours simply to type, not including necessary research time.

```

VANGUARD
Data: Extract
COMMAND ==>
CLONE
Generate OWNER Keyword => Y
Generate User DataSet Profile -> Y
Model generic DSN profile use
'N' will generate profile as:
Process User Segments, RACLINK and
DFP Y TSO Y CICS
WORKATTR Y NETVIEW Y RACLINK
KERB N PROXY N
Generate AT/ONLYAT Keyword
From User ID 1 To User ID 2
USER ID TO BE CLONED NEW USER ID ==>
Installation Data: ==>
Installation Data: ==>
Installation Data: ==>
Installation Data: ==>
EDIT
Command =
***** **
==MSG>
==MSG>
==MSG>
==MSG>
000001 AU
000002 PW
000003 AL
000004 AL
000005 AL
000006
000007
000008 CO
000009 CO
000010 AD
000011 PE
000012 PE
DITTO.* CLASS(FACILITY) ID(BOBA1) ACCESS(ALTER)
000013 PE
VIP$.NOEDIT.COMMANDS CLASS(FACILITY) ID(BOBA1) ACCESS(ALTER)
000014 PE
VRAS.*.* CLASS(FACILITY) ID(BOBA1) ACCESS(READ)
000015 PE
VRAS.ACSTASK CLASS(FACILITY) ID(BOBA1) ACCESS(READ)
    
```

Daily Security Administration Tasks

- Administrate individual profile data
- Perform password administration
- Create new Users, Groups, and Resource Profiles
- Transfer Users between departments
- Produce reports such as access list reports
- Analyze and resolve access violations

RACF Database Management Tasks

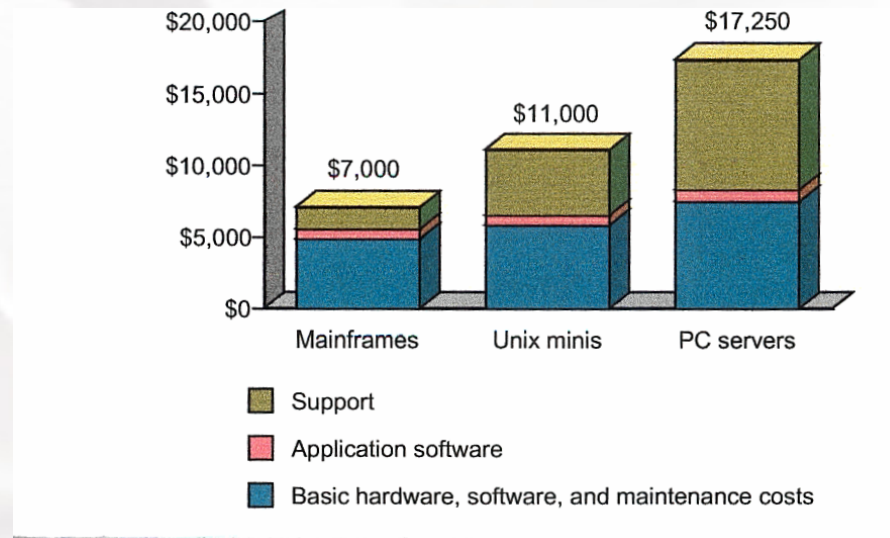
- Correct profile ownership definitions
- Replace users with groups in profile definitions
- Remove obsolete user and group references
- Remove redundant access definitions
- Identify unprotected datasets
- Produce complex reports to support the above tasks

Vanguard Security Solutions



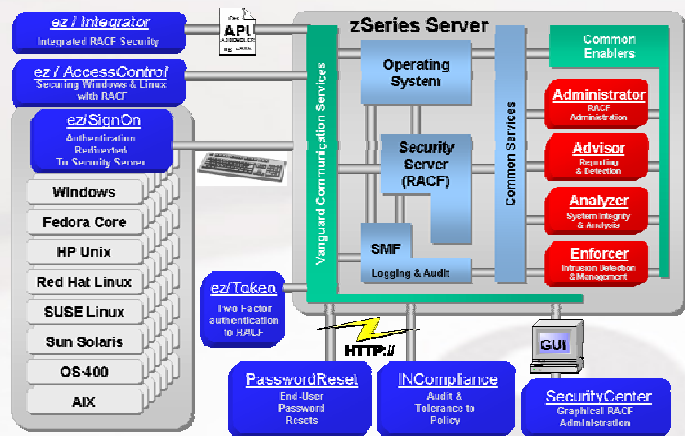
Over the years

- Decentralized Security Administration has evolved
- Security focus has shifted to distributed computing resulting in
- Security Administration staff levels with less technical knowledge



- Vanguard responds in 1998 with SecurityCenter

Vanguard SecurityCenter - Today



A windows-based interface to IBM's z/OS Security Server.

Class	Resource
DATASET	U16JED.***

Security personnel can administer RACF with no knowledge of native RACF commands.

Decentralized administrators can administer only those users, groups and resources within their responsibility.

SecurityCenter allows security administrators to perform routine tasks quickly, giving them time to concentrate on more important tasks, such as overall security strategy.



There's more to the story

Internal Audits

External Audits

Compliance to Internal IT Controls

HIPAA

SOX

GLBA



Again, Vanguard recognized the need and in 1993

VANGUARD Analyzer

Option ==> ■

Online Displays

MVS Options:

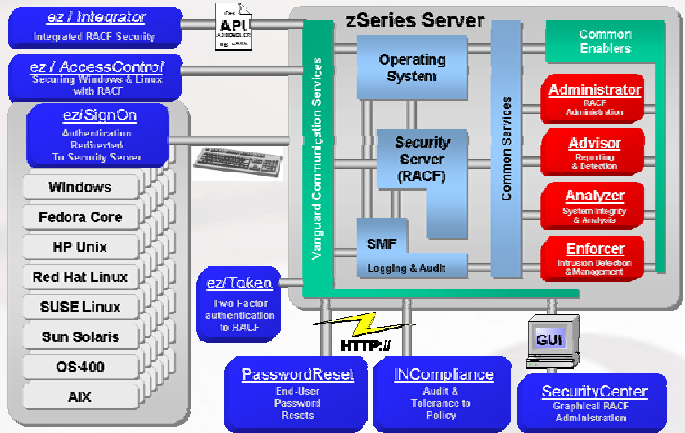
- | | |
|---|---------------------------------|
| A Program Properties Table Analysis | G System Environment Analysis |
| B Sensitive/Critical Data Sets Analysis | H SMF Environment Analysis |
| C Authorized TSO Tables* | I Link Pack Area Analysis |
| D SVC Table Analysis | J Operating System Exits Search |
| E User I/O Appendages | K JES2 Analysis |
| F Subsystem Name Table Analysis | L PARMLIB Analysis |
| | M Filebaseline Capture ** |

RACF Options:

- | | |
|-----------------------------------|---------------------------|
| 1 Class Descriptor Table Analysis | 5 Authorized Caller Table |
| 2 Router Table Analysis | 6 RACF/SAF Exits Analysis |
| 3 Database Analysis | 7 SETROPTS Analysis |
| 4 Started Procedures Analysis | |

- * - not available as a Batch Report
**- not available as an Online Report

Vanguard Analyzer - Today



A system integrity, assessment, risk identification, threat analysis and problem remediation solution for IBM's z/OS environment.

```

Session A: [24 x 80]
File Edit View Communication Actions Window Help
Program Properties Table Analysis Row 1 to 12 of 80
Command ==> _
General Audit Review Message(s)
Primary commands: CAPTURE, GM, L(ocate), SORT, STATS, PRNT, EMAIL
Primary sort sequence: M,ENTRY

Next to one or more entries:
S Display detail information
M Display message text

Opt M Entry Byp Sys Spec Prot CPU CPU AFF Orig Description
-----
M AKPCSIEP No Yes Yes 01 FFFF IBM ISP
R ANFFIEP No Yes Yes 01 FFFF USER z/OS Infoprint
R APSPPIEP No Yes Yes 01 FFFF IBM PSF
    
```

```

Program Properties Table Analysis Row 1 to 2 of 2
Command ==> _
Entry: BPXVCLNY Prot Key: 08
Byp Pwd: Yes CPU AFF: FFFF
System Task: Yes Orig: USER
Spec Key: Yes Description: Unix System Services
No DSI: No
Found in: SYS1.LINKLIB on Z5RES1

Next to one or more entries:
S Display extended message information

Opt Messages
_ VSA391I This entry was originally an IBM entry and has been changed.
S VSA392R This entry is allowed to bypass password protection.
***** Bottom of data *****
    
```

Program Properties Table Analysis Row 1 to 2 of 2
Scroll ==> PAGE

Command ==> _

Entry: BPXVCLNY
Byp Pwd: Yes
System Task: Yes
Spec Key: Yes
No DSI: No
Found in: SYS1.LINKLIB

Next to one or more entries:
S Display extended message information

Opt

```

_ Message: VSA392R
More: +
Risk
RACF checking for datasets is
bypassed.

Explanation
This entry in the PPT grants the
bypass password attribute to the
program.

User Action
The user should verify that the
module in question is an IBM
module for which this attribute
is necessary. Otherwise, check
    
```

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



- **RACF Report Writer “stabilized” in 1992**

“The report writer is no longer the recommended utility for processing RACF audit records.

The RACF SMF data unload utility is the preferred reporting utility.

The report writer does not support all of the audit records introduced after RACF 1.9.2.”

z/OS Security Server RACF Auditor’s Guide

Vanguard Security Solutions



In 1997 Vanguard filled the reporting void

VANGUARD Advisor

Date: 05/10/20

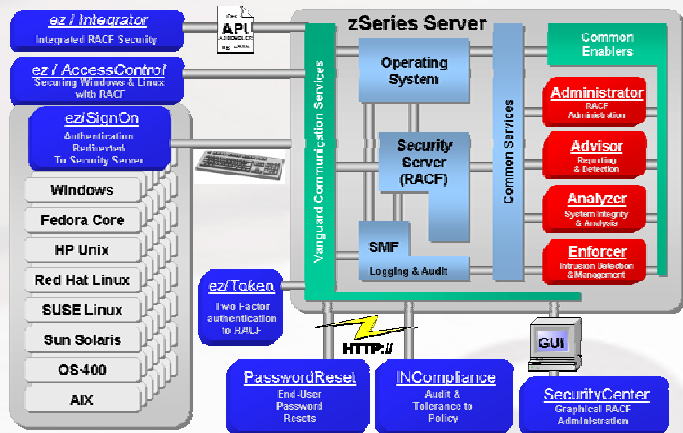
Option ==> ■

Time: 07:44

Standard Reports

- | | | | |
|----|------------------------------|----|-----------------------------|
| 1 | Resource Access Summary | 11 | User Activity Summary |
| 2 | Resource Access Detail | 12 | User Activity Detail |
| 3 | System Entry Summary | 13 | Data Set Activity Summary |
| 4 | System Entry Detail | 14 | Data Set Activity Detail |
| 5 | RACF Command Summary | 15 | TCP/IP Summary |
| 6 | RACF Command Detail | 16 | TCP/IP Detail |
| 7 | Unix System Services Summary | 17 | Sensitive Libraries Summary |
| 8 | Unix System Services Detail | 18 | Sensitive Libraries Detail |
| 9 | Violation Summary | | |
| 10 | Violation Detail | | |

Vanguard Advisor - Today



IBM z/OS Security Event detection, analysis, real-time alerts, reporting and electronic report distribution.

- Detect and alert on intrusion attempts from unauthorized users
- Perform data analysis and compliance reporting from historical or live SMF data
- Create custom report formats for ad-hoc reporting
- Generate JCL and submit jobs for extracts, reports, command generation, and remove OPERATIONS utility
- Supports advanced features such as report filtering, immediate command execution support, and much more

Data: Extract Violation Summary Sort complete
 Command ==> Scroll ==> PAGE

Next to one or more entries:
 S - all detail report M - multiple detail report

Summary Totals: 421 806 268 57 1552

CMD	Userid	User name	Resource Access	System Entry	RACF Commands	Open Edition	Total
___	KEEGANO	KEEGAN	100	55	1	2	158
___	BOBS	BOB SPITZ	10	45	1	29	85
___	ARTM	ART HATFIELD-MIHELIC	44	26	5	0	75
___	DOUGB	DOUG BEHREND	60	10	0	5	75
___	U@01JED	J.E. DOE	1	19	39	0	59
___	U@12JED	J.E. DOE	31	7	16	0	54
___	WINUSER		0	51	0	0	51
___	EZRACF1	#####	0	50	0	0	50
___	JIMM	JAMES MCNEILL	19	29	0	0	48
___	U@03JED	J. E. DOE	6	22	20	0	48
___	U@05JED	J. E. DOE	6	12	27	1	46
___	EZRIGTS	EZRIGTS DEMO ID	40	0	0	0	40
___	EZTEST1	#####	0	37	0	0	37

Current State of the Mainframe



- **Evolution to the z/Series Servers and z/OS**
 - From Closed Legacy System only image
 - To Open E-Business and E-Commerce image
 - Began in 1996 with first release of OS/390
- **Continues Legacy System Support**
- **Exploding Open Server Enhancements**
 - Unix System Services
 - Web Server
 - Lightweight Directory Access Protocol - LDAP
 - Cryptography and Secured Socket Layers
 - Kerberos Authentication

Current State of Mainframe Security

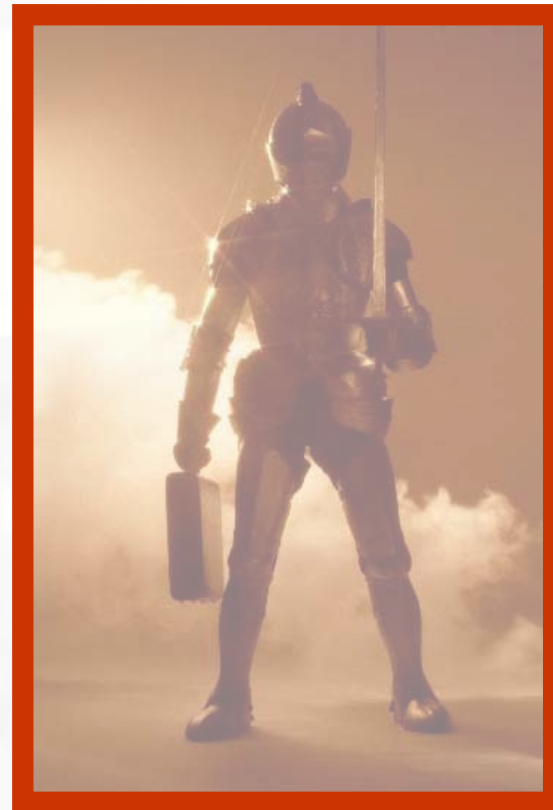


- **Number of valid users exploding**
- **Access paths and threat agents multiplying**
- **Types and numbers of resources to be protected increasing constantly**
- **Multiple security systems must work together**



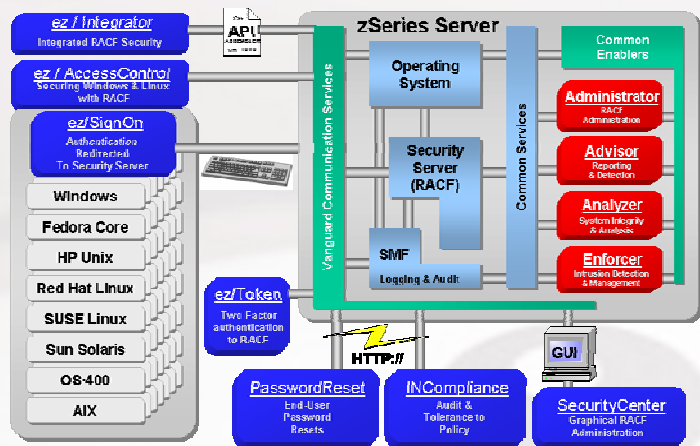


*In addition to
Analyzer and
Advisor, what's
needed now is a real
time 24x7
Intrusion Detection
System!*
*So in 2000 Vanguard
announced...*



The Enforcer

Vanguard Enforcer - Today



A proven z/OS intrusion detection and management solution to protect critical corporate assets and ensure information privacy.

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

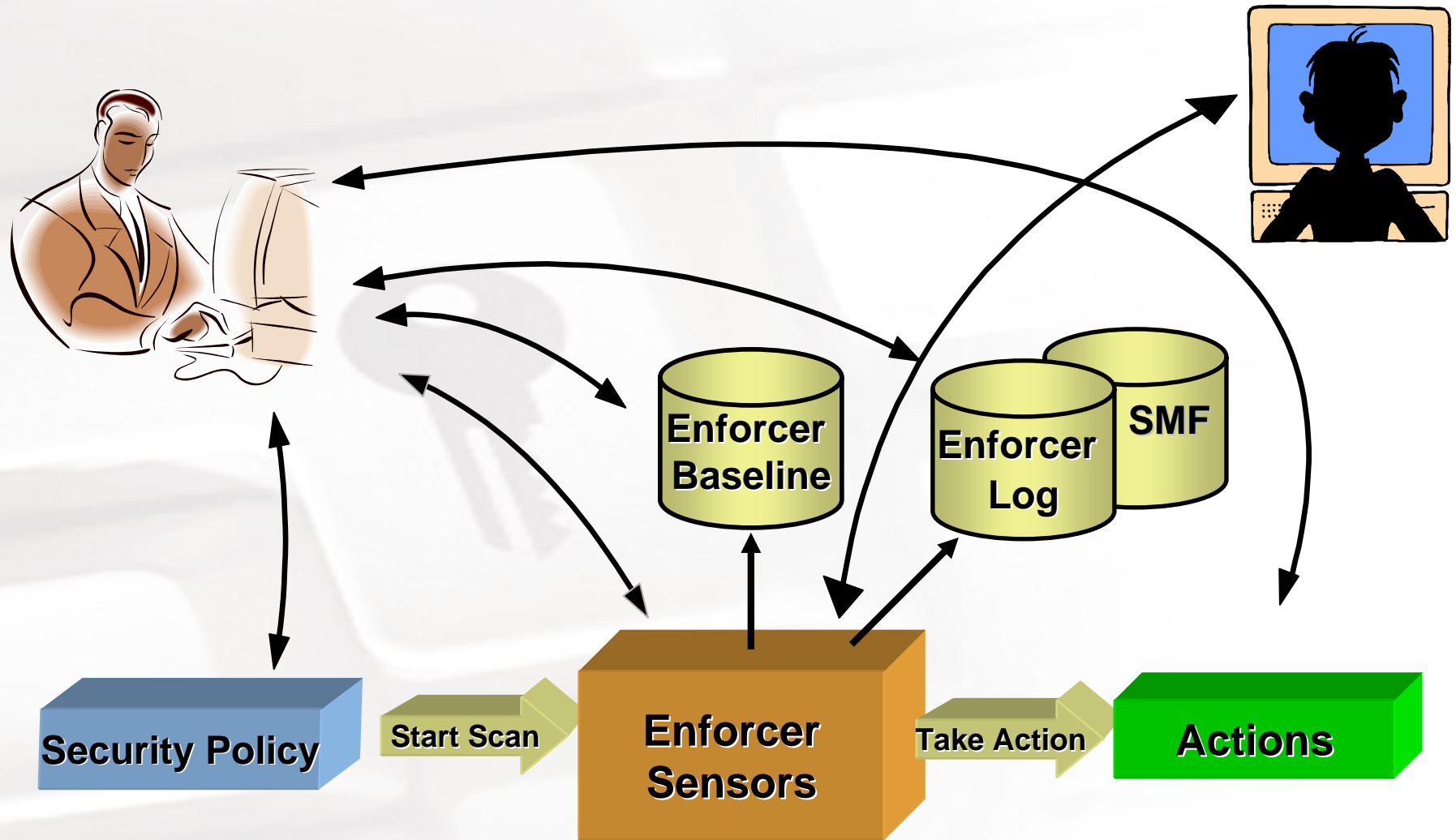
1. User makes unauthorized changes to the permissions of a critical file.



3. Data guardian receives the call and takes appropriate action.

2. Vanguard Enforcer detects the event, automatically puts the permissions back and sends an alert to the data guardian's cell phone with details of the event.

Vanguard Enforcer Flow



Vanguard Enforcer – Baseline and Sensors

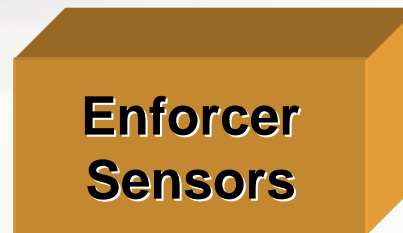


- Baseline
 - Capture of current system state
 - Granular to specific Sensors
- Sensors continuously compare current state to baseline



RACF Extraordinary Users
User Specified Critical RACF Groups
RACF System Wide Options
User Specified Critical DASD Volumes
Profile Access List Entry Expiration
Started Task Security
Supervisor Call (SVC) Security

Authorized Programs (APF) Security
Program Properties Table (PPT)
User Specified Critical Data Sets
RACF Profiles For Critical Data
Critical General Resources
LNKLST Security
Restricted Utilities In The LNKLST
LPA List Security



Vanguard Client Base



Customers: 600+ worldwide

Software Licenses: 1,400+



Vanguard Sampling of Customers



"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



“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 their 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 their 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™



“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 Defence*

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™

RACF-L Inquiry Posting



Hi,

We currently administer RACF without using any third party product.

It is not that bad, by the way!!

You are obliged to learn RACF command syntax, use of standard utilities, and how to make some processes and reports the hard way (cloning a user, for instance). All this knowledge is useful, IMHO.

That said, any tool to simplify administration is of course welcomed!

Some days ago we had, at our office, a presentation of Vanguard products.

They look fine.

What is your experience with them?

I want to know any positive or negative experience you had.



We use the Vanguard product suite extensively. In the IT industry, we, the security professionals, are expected to do more with less. The Vanguard product suite fills that hole completely.

Tasks that were once time consuming can now be done on the fly.

My command syntax days are gone, Vanguard makes me look good in the eyes of management.

I also can say that their support and professional services staff are second to none!

Contact me anytime offline.

RACF-L Response



We have the Vanguard Administrator, Advisor, and Analyzer. We are very happy with all three products, especially the Administrator.

We have a huge volume of data and I am very pleased with the way Vanguard has performed.

The support we get is fantastic to say the least, problems are generally solved the same day. I highly recommend their products and if you need more detail just drop me an email.





Our experience with the Vanguard products has been excellent in general and we've used them for many years.

It saves us huge amounts of administrative time and is very easy to use and eliminates a lot of custom code we developed to handle the tasks - saving on maintenance also.

We've had one problem lately because the audit portion of the product does not accommodate a new FTP SMF record number and there's no fix - we'll have to wait for an upgrade that includes it.

Otherwise, I can't imagine doing this job without the Vanguard products.

New Features and Enhancements in Vanguard Advisor 6.2 – 9/2005

New TCP/IP Telnet Reports. Telnet Server and Client Summary and Detail reports have been added to the TCP/IP category of records.

Vanguard Security Solutions Available from IBM



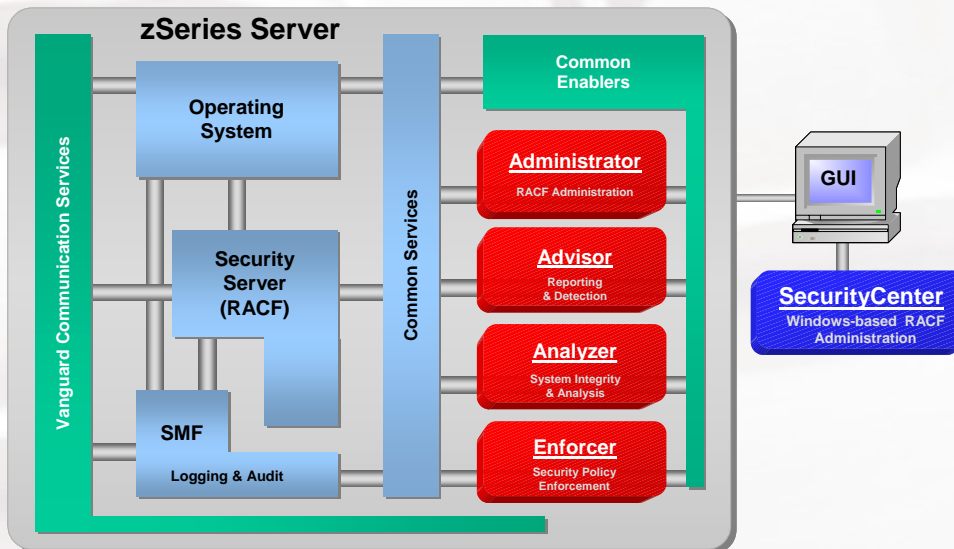
IBM strengthens IT Service Management strategy with efficient security administration and compliance management solutions from Vanguard Integrity Professionals

Complete Security Management Solution

- Security administration, integrity auditing, and intrusion detection and management
- Helps address the most stringent security rules and regulations
- Reduces complexities of RACF security administration and enforce best practices

Vanguard Security Solutions

- **Vanguard Administrator** provides advanced security server management and analysis with automation and power utilities
- **Vanguard Security Center** offers an easy-to-use graphical user interface for RACF and DB2 security administration on z/OS
- **Vanguard Analyzer** assists with security system snapshots or full-scale System z9 security audits
- **Vanguard Advisor** provides event detection, analysis and reporting capabilities for z/OS and RACF
- **Vanguard Enforcer** manages and enforces security policy on z/OS and RACF





- More information
 - <http://www.go2vanguard.com/>
 - art.hatfield-mihelic@go2vanguard.com

