VANGUARD Offline

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Testing

Simulation testing to test and evaluate impact of new RACF commands before implementation

Prevention

Prevents unexpected system errors and lockouts due to changes to RACF and reduces troubleshooting time

Implementation

Security administrators can perform what-if analyses on the 'offline copy' of RACF database

Vanguard Offline is a simulation-testing application that allows security administrators to test and evaluate the impact of new RACF commands before implementing in a production environment.

- Offline provides detailed reporting of how resources are accessed including who, when, where, and what level of authority. This allows for complete and accurate remediation of excessive or inappropriate access to resources.
- Offline will report on the actual security profile used at any given time and provide accurate reporting on existing access.
- Offline evaluates impact of any new RACF commands prior to implementation in a production environment.

Key Features

- Security administrators can execute commands against a copy of their RACF database as if against a production system and analyze the potential impact of the new commands and all consequences thereof.
- Collects and aggregates all security decisions into a database.
- Produces a wide-range of usage reports for auditors and security administrators.

Offline checks Access Previously Granted via SUROGAT SUBMIT Profiles

• Vanguard Offline will record all access that occurs via a SUROGAT ID. When requested Vanguard Offline can provide a report that shows the effect of removing access to a SUROGAT SUBMIT profile.

VANGUARD Offline

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Why An Offline RACF Database?

The use of an Offline RACF database allows testing commands before actually implementing them on an active system. Thus there is no impact of the tests on any other production application, and also no need for a dedicated LPAR just for these types of tests. Sample applications include merging RACF databases from multiple systems, and large reorganizations or cleanup of profiles.

What Is Offline And What Other Benefits Do INFOSEC Pros Derive From It?

VANGUARD OFFLINE is a simulation-testing application that allows security administrators to test and evaluate the impact of new RACF commands before they are implemented in a production environment. By reducing unexpected results from changes to user and production processes, VANGUARD OFFLINE saves time, reduces z/OS Security Server (RACF) errors and increases confidence in the change management process.

VANGUARD OFFLINE also prevents unexpected system errors and lockouts due to changes to RACF and reduces the time required to troubleshoot and resolve them. When VANGUARD OFFLINE detects problems with new commands, security administrators can perform what-if analyses on an ‘offline copy’ of the RACF database to determine how best to resolve them.

A Highly Effective Tool

VANGUARD OFFLINE can also be used as a highly effective forensic and analytical tool that enables users to utilize its History Master File to easily look back at who accessed or attempted to access which resources on z/OS Security Server over long periods of time. VANGUARD OFFLINE provides much more granular reporting than other tools and applications that rely on System Management Facilities (SMF). Because VANGUARD OFFLINE does not use SMF data, the software is able to identify any access to production resources handled by RACF and provide complete reports on the access level allowed and denied to specific User-IDs. VANGUARD OFFLINE makes it easy for security administrators to:

- Determine how users gained access to specific resources
- Remove any previously undetected unauthorized access
- Verify that changes made to user access privileges are complete
- Report complete and accurate user access information to auditors

VANGUARD Offline

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

How Vanguard Offline Works

With VANGUARD OFFLINE, security administrators execute commands against a copy of their RACF database as if they were executing them live. They can test and analyze the potential impact of the new commands on the system by running the same reports they already run against their production database and the following:

- All access that was previously allowed and is now denied
- All access that was previously denied and is now allowed
- All access that was changed
- All access that was changed and unchanged
- All access that was granted via extraordinary privileges such as GAC, UACC, ID(*),

OPERATIONS, TRUSTED and PRIVILEGED

If there are problems with any proposed commands, administrators can easily perform what-if analyses on the copy of the RACF database to determine the impact of new profiles or evaluate how profile additions or deletions should be modified to eliminate potential production problems. When more accurate predictions about the impact of proposed changes on the system are required, Vanguard Offline can conduct an impact analysis using historical data about access activity and which profiles were used to gain access to resources.

VANGUARD Offline

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Vanguard Offline works with Vanguard CleanUp to validate proposed changes before they are made to the production system.

With Vanguard Offline, security administrators can test user, group, connect, permit, dataset, and general resource profiles that have been identified by CleanUp as unused, unwanted or duplicate and report on any potential production access failures that will occur if those profiles are deleted.

Key Differentiators

- Provides complete accounting of all unique authorization requests.
- Provides a simple method for remediation of elevated access and authorities.
- Captures all authentication requests including the ones designated as bypass, Vanguard has the ability to show those liabilities.
- Automates Tests and analyzes how new z/OS Security Server commands will impact users and processes before those commands are executed in a production environment.
- Uses actual z/OS Security Server authorization and authentication requests as input to the verification engine resulting in avoidance of operational disruption while making changes to the z/OS Security Server.

VANGUARD Offline

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Why Vanguard to Secure Your Enterprise?

Almost half of the Fortune 1000 companies in the world spanning banking, retail, insurance, as well as numerous government agencies trust Vanguard with their enterprise security.

About Vanguard Security Solutions

Vanguard offers the most advanced and integrated portfolio of enterprise security products and services in the world. The portfolio was the first to offer fully automated baseline configuration scanner for Mainframe DISA STIGs— the Gold Standard for Security.

For More Information

To learn more about Vanguard Security Solutions please call 702.794.0014 or visit www.go2vanguard.com

Corporate Headquarters

6625 S. Eastern Avenue—Suite 100
Las Vegas, NV 89119-3930