

Vanguard Enforcer™

Vanguard Enforcer is a revolutionary intrusion detection management (IDM) solution that is the first IDM solution for the mainframe to receive the difficult to attain Common Criteria certification of EAL3+. Enforcer provides continuous protection of critical z/OS and RACF® policy implementations to ensure that approved IT policies and controls are not compromised.



VANGUARD ENFORCER™

Highlights

- ❑ Effectively protect data through automated security surveillance
- ❑ Ensure the privacy and confidentiality of customer, employee and corporate data
- ❑ Awarded Common Criteria Evaluation Assurance Level 3+
- ❑ Minimize vulnerabilities through automated monitoring and control of your security environment
- ❑ Assure continuous compliance with your security policies and authorized settings

Vanguard Enforcer protects critical data and resources hosted on the mainframe by ensuring z/OS and RACF security standards, profiles, rules, and settings are not compromised.

Enforcer automatically detects and notifies personnel on the occurrence of threat events, and responds to deviations in the RACF security baseline with corrective actions that reinforce the approved security policy.

Intelligent Enforcement

Enforcer recognizes when a deviation from policy results in a weaker security implementation. When Enforcer's auto correction mode is enabled, weaker deviations to a policy will be automatically restored from

the stronger Enforcer Baseline policy automatically, unless the deviation results in strong security. Enforcer is smart enough to tell the difference.

Information Security Compliance

Meeting the demands of regulatory compliance requires a security management solution capable of continuous oversight to ensure that approved IT/IS controls are in place and stay that way. With Enforcer, organizations can be confident that their RACF security implementation is protecting their critical data and resources and continuously adhering to "Best Practices" standards.

Protects Critical RACF Security Profiles

Vanguard Enforcer is a proven z/OS intrusion detection management solution that:

- Provides continuous, periodic scanning of RACF security profiles

looking for deviations from the policy baseline and takes automated corrective action.

- Notifies security personnel on a wide variety of intrusion-related events.
- Manages the security implementation baseline that enforces your security policies.

The automated security measures provided by Enforcer reduce operating expense, and improve the productivity and effectiveness of scarce z/OS security staff.

Active Alerts

Provides automated, unattended 24/7 monitoring and detection of threat-related security events including:

- Access Violations
- Assignment of SPECIAL, OPERATIONS, AUDITOR, PROTECTED, or UID(0)
- Assignment of a Group Attribute or Authority
- Data Set Profile UACC set to greater than NONE
- Data Set Profile UACC set to greater than READ
- Access Granted due to Profile WARNING Mode
- Invalid Passwords within a Time Period
- Password Recycling
- General Resource Class Activation/Deactivation
- SMF Lost Data Detection
- User Id Revoke Due to Invalid Password Attempts
- System Entry Access by a Specific Userid

Alerts authorized personnel through text paging, cell

telephones, MVS console, email, etc... around the clock.

Security Baseline Sensors

Continuously monitor the activities of systems programmers, security administrators, and all other users that impact security. Robust Sensors detect baseline deviations for:

- System and User Specified Critical and Sensitive Data Sets
- User specified critical General Resource profiles
- RACF User with Extraordinary Privileges
- System and User Specified Critical RACF Groups
- RACF System Wide Options
- User Specified Critical General Resources
- User Specified Critical DASD Volumes
- Profile Access List Entry Expiration
- Started Task Security
- Supervisor Call (SVC) Security
- Authorized Programs (APF) List Security
- Program Properties Table (PPT)
- LNKLIST Security
- User Specified Restricted Utilities in LNKLIST
- LPA List Security

Indicate the nature of the violation and corrective action taken with policy deviation alerts.

For More Information

To learn more about the features and benefits of Vanguard enterprise security software solutions, visit www.go2vanguard.com.

Security Management Solutions:

Vanguard Administrator
Vanguard Advisor
Vanguard SecurityCenter

Audit and Compliance Solutions:

Vanguard Analyzer
Vanguard inCompliance
Vanguard Enforcer
Vanguard Policy Manager

Access Management Solutions:

Vanguard Authenticator
Vanguard ez/SignOn
Vanguard ez/Token
Vanguard Tokenless Authentication
Vanguard ez/Integrator
Vanguard PasswordReset

Intrusion Detection Solutions:

Vanguard Enforcer

©2009 Vanguard Integrity Professionals All other copyrights, trademarks and/or service marks are the property of their respective owners.

