VANGUARD Enforcer ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Monitoring

Provides continuous monitoring of security controls to detect changes to the system

Notifications

ActiveAlerts provide immediate notification of security events

Remediation

Corrects any deviations from the baseline

Continuation

Enforcer captures and baselines current security configurations and profiles for future comparison

Vanguard Enforcer provides continuous monitoring of security controls with an automated process to compare your current z/OS Security Server configuration controls against the previously established baseline. Enforcer has options to notify and or automatically correct deviations from the baseline.

Cybersecurity is an issue causing great consternation in the business world today. With the exponential year-over-year increases in cybercrime, corporations are feeling the heat from customers, partners, Investors, and regulators when breaches transpire.

In 2014, cyber criminals compromised more than a billion data records in more than 1,500 breaches, according to Gemalto. This represents a 49% increase in data breaches and a 78% increase in the number of data records stolen or lost compared with 2013, which works out to 32 records lost or stolen every second. The majority of data breaches occurred in North America (76%), followed by Europe (12%), and then the Asia-Pacific region (8%). Crime rings operating out of Russia or China perpetuated the vast majority of the largest attacks.

Escalating cybercrime creates doubt about the computer defense systems in place today. Deploying the best possible defense system makes it difficult for hackers to enter your company's computer systems and steal critical information.

Key Features

- Vanguard Enforcer detects and corrects changes to the system that would violate security policies.
- Enforcer's active alerts provides immediate notification of security events or combinations of events.
- Enforcer captures and baselines current security configurations and profiles for future comparison.

VANGUARD Enforcer ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Automate Your DISA STIG Assessments And Dramatically Reduce Costs And Time To Verify Compliance

Configuration Manager was designed to provide the fastest, most cost-effective and accurate method to verify that security configuration controls are in accordance with the DISA STIG for z/OS systems.

Vanguard's team of United States-based, z/OS mainframe security experts analyzed all of the DISA STIG z/OS and RACF checks to determine how best to interpret them, test configuration controls for compliance and report findings. This comprehensive intelligence was built into Configuration Manager along with efficient automation capabilities.

The result is that organizations using VANGUARD CONFIGURATION MANAGER can perform System z checks and report findings in a fraction of the time of standard methods. Configuration Manager also allows organizations to easily move to continuous monitoring from periodic compliance reporting.

Improve On The DISA STIG Test Process With Configuration Manager

Verifying that mainframe systems are in accordance with the DISA STIGs can require that more than 300 checks be performed, depending on specific configurations. For each check, from one to hundreds of thousands of control points must be tested.

It can be extremely costly and time consuming to use the standard DISA STIG Checklist process to verify that z/OS systems are configured correctly, even for smaller installations. Organizations that try this method to comply face the following challenges:

- Configuration checks take too long or are impossible to complete.
- Team morale is negatively impacted by the added workload.
- Multiple findings for the same checks are common.
- Ambiguous checks can put teams at risk if interpreted incorrectly.
- DISA STIGS are updated every three months.

With CONFIGURATION MANAGER however, organizations can perform tests and report findings in a few hours each quarter, instead of the hundreds, or thousands, of hours required when using the standard z/OS DISA STIG Checklist process. Once Configuration Manager has identified findings, they can be remediated, as required, to improve an organization's overall z/OS security baseline and increase security levels.

VANGUARD Enforcer ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

The Future Of Security Available Today: Averting Cybercrime With Vanguard's Enforcer

Vanguard Enforcer can detect, correct, and notify your CISO and Security Staff about active threats in less than two seconds. It is the way all security will be done in the future, but it is available right now from Vanguard.

Detect, Correct And Notify With Vanguard Enforcer

Vanguard Enforcer protects critical information and resources hosted on the mainframe by guaranteeing that IBM® z/OS® and RACF® security standards, profiles, rules and settings are not compromised. It responds to deviations from your security baseline with corrective actions that reassert the approved security policy.

Intelligent Security Enforcement With Enforcer

VANGUARD ENFORCER is the result of more than two decades of security expertise, and provides instant access to Vanguard's extensive knowledge base.

Enforcer has built-in signatures of attack behaviors. When Enforcer's auto correction mode is enabled, deviations to a policy will be automatically corrected using the stronger Enforcer Baseline policy, unless the deviation results in stronger security.

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

VANGUARD Enforcer ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Automate Security Measures And Save Time And Money With Enforcer

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

Enforcer Features: 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.
- 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.
- 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 User ID.

Alerts authorized personnel through text messages, cell phones, MVS console, email, etc. — around the clock.

VANGUARD Enforcer ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

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 / 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)
- LNKLST Security
- User Specified Restricted Utilities in LNKLST
- LPA List Security

Key Differentiators

- Enforcer monitors system critical resources including the most privileged data sets and programs.
- Enforcer monitors users with elevated privileges.
- Extensive security checking performed to minimize possible leakage of authentication information.
- Standard z/OS services used to ease installation's migration to a new system, software or enhancement release.

VANGUARD Enforcer ™

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