VANGUARD Configuration Manager TM

Vanguard Configuration Manager automates review of current z/OS Security Server configurations against prevailing standards to include DISA STIG, NIST, and DB2 hardening standards and Vanguard Best Practices dramatically reducing personnel cost and time to verify compliance.

Key Features

- Vanguard Configuration Manager is designed to provide the fastest, most cost-effective and accurate method to verify that security configuration controls are in accordance with published prevailing standards for z/OS systems.
- Configuration Manager allows organizations to easily move to continuous monitoring from periodic compliance reporting.

Vanguard Takes The Target Off Your Back

If you look at any best practice guidance, regulation or standard around effective IT security today, you´ll quickly recognize that it advises organizations to ensure their computing systems are configured as securely as possible and monitored continuously for changes.
To avoid unnecessary I/O overhead, data already contained in the History Master File is automatically updated with the latest time stamp, records are automatically aged and those records beyond a user-defined purge date (usually at least 400 days) are removed.

Today, the Security Technical Implementation Guides (STIGs) from the Defense Information Systems Agency (DISA) are the gold standard given their exacting dictates for configuration and monitoring, which prevent cyberattacks for both governments and commercial organizations.

To put things in perspective, following the guidelines laid out in the STIG is essential in eliminating the easy vectors hackers often use to launch attacks. One such breach at MBIA, the nation’s largest bond insurer, was perpetrated due to system misconfiguration.

VANGUARD Configuration Manager TM

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.

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

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 Configuration Manager TM

Vanguard Configuration Manager: Technical Features

- Creates summary and detailed reports To provide the proper information required.
- Executes in both batch and online environments.
- Supports parallel collection and execution of checks to enable reporting to be completed quickly.
- Architected to prevent failure of one check from affecting reporting on another check.
- Consistent look and feel across all DISA STIG categories.
- Users do not need to be an expert on the DISA STIG to complete checks and report on compliance.
- Vanguard always supports the latest DISA STIG versions, including versions for the past two years.

VANGUARD Configuration Manager TM

Why Vanguard Configuration Manager?

VANGUARD CONFIGURATION MANAGER has a built in DB2 Compliance module

Vanguard built into VCM a set of DB2 checks based on their best practices and posted to the NIST NCP site as the set of standards for auditing DB2 security for RACF.
These checks are automated in VCM and can be easily executed in a continuous monitoring methodology that ensures that any deviations from the standards are captured and reported.

VANGUARD CONFIGURATION MANAGER has a built-in Best Practices Compliance module

Vanguard built into VCM a set a comprehensive set of Best Practice checks based on their Professional Services Auditing requirements.
These checks are automated in VCM and will significantly reduce the amount of time it takes for Vanguard Professional Services to complete a comprehensive audit on a given target mainframe system.
Please contact Vanguard Professional Services on how to enable this functionality.

VANGUARD CONFIGURATION MANAGER has a built-in Best Practices Compliance module

Vanguard has automated a number of PCI checks and walks the end user through an entire set of PCI checks for the mainframe.
Please contact Vanguard Professional Services on how to enable this functionality.

Key Differentiators

- Organizations can perform tests and report findings in a few hours each quarter instead of the hundreds or thousands of hours required when using published standards.
- Creates summary and detailed reports to provide the proper documentation required.
- The ability to compare multiple occurrences of the reported results for historical reporting.
- Users do not need to be an expert on the published standards to complete checks and report on compliance.
- Supports implementing the z/OS Security Server and RACF configuration checklist from the National Checklist Program (NCP) of the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS).
- Automates more than 300 z/OS Security Server checks and produces accurate compliance reports in minutes.
- Provides update for all DISA levels and checks within 30 days of posting.
- Delivers the ability to match wildcard resources to profiles.

VANGUARD CleanUp ™

Virtel et ses partenaires

L’assurance d’un expert, la garantie de solutions logicielles efficaces

Depuis 1993, la société Virtel représente des éditeurs majeurs en France et dans les pays francophones. Elle offre ainsi des solutions logicielles novatrices et fiables destinées tant aux grandes entreprises qu’aux PME.

Contact

302 Bureaux de la Colline
92213 Saint Cloud
Tél: 01 46 02 60 42
Email: **info@syspertec.fr**
Site: **www.virtelweb.fr**