VANGUARD
Integrity Professionals
Information Security Experts

Vanguard プロダクト新機能概要

Version 2.4

2020 年 4 月 2 日 改訂

VANGUARD
Integrity Professionals
Information Security Experts

目次

Vanguard Security Solutions (VSS) 2
1. 複数のデリバリー・モデルが VSS で利用できるようになりました 2
2. VSS と VCM に個別の FMIDs が追加されました 2
3. IBM z/OS 2.4 許容サポート 3

Vanguard ACF2 Access Rule Changes Capture 3
4. ACF2 Access Rule Changes Capture の紹介 3
5. Compare Two Rule Sets 3

Vanguard Active Alerts 4
6. Access Control Facility (ACF2) のサポートを追加 4
7. Access Rule Change Capture のサポートを追加 4
8. Active Alert 17 のサポートを追加 4

Vanguard Administrator 5
9. CA ACF2 のサポート 5
10. 新しいレポート: SURROGAT クラス分析 5

Vanguard Advisor 6
11. CA ACF2 のイベント・レポートのサポート 6
12. CA TSS のイベント・レポートのサポート 6

Vanguard Cleanup および Vanguard Offline 6
13. 様々なインフラストラクチャーの改善 6
14. Vanguard Offline で使用するサロゲート・クラス・コレクションのサポートを追加 7

Vanguard Compliance Manager 7
15. Vanguard Aggregation and Delivery STC™ (VAD) 7
16. VCM Current with Latest Version of DoD DISA STIGs 8
17. 貴社のベスト・プラクティスが Vanguard Compliance Manager で利用可能になりました 8

Vanguard ez/Integrator 9
18. 複数の ESMs のサポート 9
19. TLS のサポート 9

Vanguard ez/PivCard 9
20. PIV-I と PIV–C カードのサポート 9

Vanguard ez/Token 10
21. Vanguard Multifactor Authentication は SAF をサポートするようになりました 10
22. Vanguard Multifactor Authentication は RADIUS をサポートするようになりました 10

VANGUARD
Integrity Professionals
Information Security Experts

Vanguard Security Solutions (VSS)

1. 複数のデリバリー・モデルが VSS で利用できるようになりました

説明

Vanguard 製品の導入は複数のデリバリー・モデルを利用できるようになりました。継続的デリバリーとメンテナンス限定版が利用可能になりました。

利点

継続的デリバリー・モデルには、すべての修正と機能拡張が含まれます。これはバージョン 2.3 での現行のデリバリー・モデルです。Vanguard 2.4 では、メンテナンス限定版を選択できます。メンテナンス専用バージョンは、2.4 のベースからの機能拡張は含みませんが、失敗の修正 PTFs が含まれます。

2. VSS と VCM に個別の FMIDs が追加されました

説明

Vanguard 製品は複数の FMIDs を持ちます。

VSSC240 - Vanguard Security Solutions 継続的デリバリー・モデル

VSSM240 - Vanguard Security Solutions メンテナンス限定モデル

VCMC240 - Vanguard Compliance Manager 継続的デリバリー・モデル

VCMM240 - Vanguard Compliance Manager メンテナンス限定モデル

利点

システムのセキュリティーは構成制御から始まると同時に、これを正しくブランド化することは、適切なセキュリティー構成によりコンプライアンス要件を満たすことができることを認識することです。

VANGUARD
Integrity Professionals
Information Security Experts

3. IBM z/OS 2.4 許容サポート

説明

サポートされているすべてのバージョンの Vanguard Security Solutions は、IBM が現在サポートしているすべての z /OS® リリースをサポートし、IBM Z® オペレーティングシステムを実行しているお客様のセキュリティーとデータ保護を強化しています。

利点

IBM z/OS 2.4 のサポート。

Vanguard ACF2 Access Rule Changes Capture

4. ACF2 Access Rule Changes Capture の紹介

説明

Vanguard ACF2 Access Rule Changes Capture™ を使用すると、ベースラインが確立されてからリソースまたはデータセット・ルールに加えられたすべての変更を確認できます。

利点

ユーザー・インターフェイスにより、アクセス・ルールを以前の状態に簡単に復元できます。

5. Compare Two Rule Sets

説明

この機能はルールの比較パネルを簡単に使用して、比較するルールおよび比較するために使用するルールセットのリストを選択できます。

利点

この機能により、違いが見つかったか、見つからなかったかを示すことができます。セキュリティー管理者が CA ACF2™ のルールセットを決定できるようにします。

VANGUARD
Integrity Professionals
Information Security Experts

Vanguard Active Alerts

6. Access Control Facility (ACF2) のサポートを追加

説明

CA ACF2™ システムで実行するための Vanguard Active Alerts のサポートを追加しました。

利点

Vanguard Active Alerts は、複数の ESMs (RACF® and ACF2) でサポートされるようになりました。

7. Access Rule Change Capture のサポートを追加

説明

Access Rule の変更に対するすべての変更を収集するために Vanguard Active Alerts のサポートが追加されました。

利点

この機能により、ベースラインが確立されてからリソースおよびデータセット・アクセス変更ルールの収集が可能になります。これにより、アクセス・ルールを以前の状態に簡単に復元できます。

8. Active Alert 17 のサポートを追加

説明

USS ファイル・システム・アクティビティに関する通知用の新しい Alert（17） の Vanguard Active Alerts のサポートが追加されました。

利点

この機能は、マウント、アンマウント、特定のファイル・アクセスなどの USS のアクティビティについて警告します。すべての SMF 92 サブタイプが含まれます。

VANGUARD
Integrity Professionals
Information Security Experts

Vanguard Administrator

9. CA ACF2 のサポート

説明

Vanguard IAM™ – Vanguard Administrator™ for ACF2™ は、管理を簡素化し、CA ACF2™ セキュリティー実装の品質と有効性を向上させます。オンラインモードで ACF2 セキュリティー管理、データマイニング、レポート、および印刷機能の幅広い機能を提供します。

利点

Vanguard Administrator for ACF2 は、他の Vanguard ACF2 セキュリティー・ソリューションとのさまざまなレベルの統合に加えて、より高いレベルのパフォーマンスと機能を提供するように設計されています。使いやすいアイデンティティー管理、タスク指向の管理、権限分析、セキュリティー監視を提供するセキュリティー自動化機能により、ワークロードの増加と操作の複雑さの問題を解決します。

Vanguard Administrator for ACF2 を使用すると、経験の浅いスタッフが迅速に対応できる使いやすい環境を提供していると同時に、経験豊富な IT セキュリティー・エキスパートがより効率的に作業できるようになります。

10. 新しいレポート: SURROGAT クラス分析

説明

SURROGAT クラス分析レポートは、Administrator メイン・メニューのオプション 3 である Security Server Reports メイン・メニューのオプション 20 として追加されました。SURROGAT クラス分析オプションは、SURROGAT クラスの構造内で検出された問題、プロファイル・データとアクセス・データに関する情報、各クラスへの直接および間接アクセス、爆発レベル、および Via 情報について報告します。

利点

Vanguard Administrator は、代理ユーザーに関する情報をレポートできるようになりました。代理ユーザーとは、他のユーザーの権限レベルを使用して、他のユーザーに代わってタスクを実行する権限を持つユーザーです。

VANGUARD
Integrity Professionals
Information Security Experts

Vanguard Advisor

11. CA ACF2 のイベント・レポートのサポート

説明

Advisor は CA ACF2™ の SMF イベントについてレポートできるようになりました。

利点

Advisor を使用すると、企業は z/OS システムおよび現在の ACF2 のリスク管理に重要なイベント・ログを監視および分析できます。Vanguard Advisor は情報を収集し、その重要性を認識し、その重要性を説明し、ユーザーが露出を排除するように導きます。

12. CA TSS のイベント・レポートのサポート

説明

Advisor は CA TSS™ の SMF イベントについてレポートできるようになりました。

利点

Advisor を使用すると、企業は z/OS システムおよび現在の CA Top Secret (TSS) のリスク管理に重要なイベント・ログを監視および分析できます。Vanguard Advisor は情報を収集し、その重要性を認識し、その重要性を説明し、ユーザーが露出を排除するように導きます。

Vanguard Cleanup および Vanguard Offline

13. 様々なインフラストラクチャーの改善

説明

レポート間隔の変更。

キャプチャーされる最大イベントが 300,000 に増加しました。

ヒストリー・マスター・ファイル (HMF) 更新処理は、高速バッファリングのために VSAM リソース・プール (VRP) を使用するようになりました。

利点

製品の生産性とパフォーマンスの改善。

14. Vanguard Offline で使用するサロゲート・クラス・コレクションのサポートを追加

説明

Vanguard Offline は、サロゲート・ユーザー・アクセスをキャプチャーしてレポートするようになりました。

利点

サロゲート・ユーザーによるアクセスは、実行 ID ではなく代理のユーザー ID でレポートされるようになりました。さらに、Vanguard Offline Impact Analysis Reports は、実行ユーザー ID のアクセスまたは実行 ID への代理のアクセスに変更が加えられた時にレポートするようになりました。この機能は、Vanguard Offline 処理に固有のものです。

Surrogate Chain レポートは、実行ユーザーID へのアクセスを通じて反映されます。言い換えると、提供される情報は 1 レベルだけの深さになるため、SURROGAT クラスに複数の変更を加える際は十分に注意してください。

たとえば、UserA が UserB としてジョブをサブミットし、それが 3 番目のユーザーである UserC（実行 ID）の下でジョブをサブミットする場合、Offline Impact Analysis に唯一ありそうな反映は、実行 ID（UserC）によるデータセットやリソースへのアクセスが、UserB によるアクセスとなることです。UserA の USERB.SUBMIT プロファイルへのアクセスが修正された場合、それは Offline Impact Analysis にも反映されます。バッチ・ジョブは独立して実行されるため、このシナリオで UserA の影響を追跡する既知の方法はありません。UserB の影響が反映されます。

この制限の原因は、実行時に使用可能なデータです。

新しいレポート：Access Summary by Submitted By レポートが Access History Reports セクションに追加され、Impact Summary by Submitted By レポートが Impact Analysis Reports – Online セクションに追加されました。

Vanguard Compliance Manager

15. Vanguard Aggregation and Delivery STC™ (VAD)

説明

VAD は、一元化されたサイトからソフトウェアおよび構成の配信変更を提供します。また、Vanguard GRC™ – Vanguard Compliance Manager™（VCM）ソリューションの管理者およびユーザーに、新しい VCM 結果情報を収集する機能を提供します。

利点

Vanguard Aggregation and Delivery STC は、企業全体の VCM 展開への一元化されたアクセスを提供することにより、VCM の既存の能力と柔軟性を高めます。固有の z/OS 環境内の脆弱性を評価するためのツールとして、VCM はコンテキスト内の検出結果に関する収集、分析、レポートを行い、VCM が展開および実行される特定の z/OS イメージの範囲を限定します。Vanguard

Aggregation and Delivery STC の導入により、単一の一元化されたサイトから企業全体で実行されている VCM 分析の結果にアクセスして処理できるようになり、管轄区域を越えた個人および機密情報の流れを管理する地域の法律や規制に潜在的に違反しない方法で、そのようにします。

VCM ソフトウェアの現在のレベルにおいて、VCM は実行された各脆弱性チェックに関連する要約情報を生成および記録します。この情報は要約データに過ぎず、地域の準拠法および規制の対象となる可能性のある個人的または機密性のものとして、特徴付けまたは分類できる情報は含まれません。この概要情報は、実行される脆弱性チェックの詳細とともにローカル VCM の「結果」データベースに記録されます。

16. VCM Current with Latest Version of DoD DISA STIGs

説明

現在のセキュリティー技術実装ガイド（STIG）サポートが追加されました。Vanguard Compliance Manager（VCM）は、3 か月ごとに、米国国防総省（DoD）国防情報システム局（DISA）からの最新のチェックで更新されます。

利点

VCM を所有することの大きな利点は、DoD DISA STIG の最新バージョンに絶えず更新および維持されることです。つまり、3 か月ごとに新しい検査のベースラインが作成され、現在のお客様に提供されます。

Vanguard Compliance Manager（VCM）は、DoD DISA STIG に対する最新かつ最も厳格なコンプライアンス製品です。お客様が常にどのバージョンの変更が行われたかを把握したり追跡したりすることなく、DISA STIG の変更の最新バージョンを常に入手できるように、継続的に維持しています。VCM は継続的に更新され、そのインターフェイスは新しいチェックと変更されたチェックを顧客に通知します。

17. 貴社のベスト・プラクティスが Vanguard Compliance Manager で利用可能になりました

説明

Vanguard は、カスタム・ベースラインという名前の新しいセクションの下に Vanguard Compliance Manager に新しい検査を追加しました。カスタム・ベースライン検査は、IBM z/OS の構成設定をお客様が定義したセキュリティー設定と比較します。これらは、貴社が推奨する設定であり、貴社のベスト・プラクティスに成文化されています。

利点

Vanguard Best Practices が Vanguard Compliance Manager に組み込まれました。Vanguard プロフェッショナル・サービスの支援により、VCM のお客様は現在のセキュリティー設定と z/OS 構成設定を Vanguard Integrity Professionals が推奨する設定と比較できるようになりました。

VANGUARD
Integrity Professionals
Information Security Experts

Vanguard ez/Integrator

18. 複数の ESMs のサポート

説明

Vanguard ez/Integrator は、IBM® RACF®、CA ACF2™ および CA TSS™ をサポートするようになりました。

利点

お客様は、複数の External Security Managers (ESM) で ez/Integrator の機能を享受することができます。さまざまな言語への統合を提供します。

19. TLS のサポート

説明

Vanguard ez/Integrator は TLS 通信をサポートするようになりました。

利点

お客様は、TLS を使用した安全な通信を確保できます。Vanguard ez/Integrator がサポートするすべてのトランザクションは、TLS 1.2 で保護できます。

Vanguard ez/PivCard

20. PIV-I と PIV–C カードのサポート

説明

Vanguard ez/PivCard は PIV-I と CIV カードの両方をサポートするようになりました。

利点

アメリカ合衆国連邦政府の PIV プログラムによって作成されたインフラストラクチャーを活用することを目的として、2つの追加の資格情報 ー 個人 ID 検証相互運用（PIV-I）および商用 ID 検証（CIV）資格情報が定義されています。これにより、より多くの企業が PIV カードを活用できるようになります。

VANGUARD
Integrity Professionals
Information Security Experts

Vanguard ez/Token

21. Vanguard Multifactor Authentication は SAF をサポートするようになりました

説明

Vanguard Multifactor Authentication (MFA) は、IBM System Authorization Facility (SAF) と連携するように拡張されました。

利点

このソリューションは、RACF のみのサポートへの依存関係を解消します。Vanguard MFA は ESM に中立になりました。Vanguard SAF インターフェイスでは、CA ACF2™ および CA TSS™ で Vanguard MFA を使用できるようになりました。

22. Vanguard Multifactor Authentication は RADIUS をサポートするようになりました

説明

Vanguard Multifactor Authentication（MFA）は、RADIUS ベースのトークン・プロバイダーと連携するように拡張されています。

利点

このソリューションは、RADIUS プロトコルの通信プロトコルをサポートする多数のトークン・プロバイダーをサポートします。