Yphise **PROANALYSE**

Evaluations indépendantes de progiciels

Progiciels d'audit de conformité des serveurs

pour répondre aux exigences de disponibilité, de continuité et de sécurité

Volume DECIDER

L'engagement Yphise est de fournir aux décideurs et managers la meilleure recherche indépendante sur les méthodes et solutions pour optimiser l'informatique en Coût, Valeur et Risque. Les résultats constituent un ensemble cohérent et pragmatique pour mesurer et améliorer l'efficacité selon les attentes des grandes entreprises

Yphise est une entreprise indépendante spécifiquement organisée pour conduire des programmes de recherche à l'attention des décideurs et managers de l'informatique. Yphise a une équipe de recherche dédiée pour garantir l'indépendance, la cohérence des résultats et une fréquence de mise à jour suffisante.

Yphise a plus de 900 grandes entreprises clientes à travers le monde. Ils appartiennent à tout secteur d'activité : industrie, banque, assurance, distribution, transport, services, administration, collectivités territoriales.

Yphise mène deux programmes de recherche exclusifs : 1/ L'évaluation des progiciels, 2/ YBRM (Yphise Business Risk Management).

1/ L'évaluation des progiciels

Yphise identifie et certifie les meilleurs progiciels pour accroitre la valeur des systèmes d'information tout en optimisant les coûts et les risques. Yphise couvre tous les domaines d'intérêt des grandes entreprises pour développer, exploiter, maintenir et sécuriser les systèmes d'information nécessaires à leur compétitivité. Yphise évalue 150 progiciels par an depuis 1985. Chaque évaluation est certifiée ISO 9001:2000 pour garantir l'indépendance et le centrage sur les préoccupations des grandes entreprises.

2/ YBRM (Yphise Business Risk Management)

YBRM fournit aux décideurs et managers un référentiel ouvert de meilleures pratiques opérationnelles pour optimiser l'informatique en coût, valeur et risque. YBRM couvre toutes les missions d'une DSI afin de garantir un management opérationnel efficace. YBRM est une approche pragmatique. Il comporte un modèle de scoring pour une autoévaluation périodique aisée. Il permet une amélioration rapide de chaque processus. YBRM est aussi une ligne directrice d'amélioration de l'efficacité opérationnelle d'une DSI qui garantit la cohérence avec la gouvernance.

yphise@yphise.com

6 rue Beaubourg - F-75004 PARIS T 01 44 59 93 00 - F 01 44 59 93 09

PO Box 142, Southbury, CT 06488 U.S.A. T (303) 410-7753 - F (303) 410-4980

AVANT-PROPOS

Le volume DECIDER synthétise les résultats du programme de recherche indépendant Yphise pour le segment de marché évalué.

Ce segment de marché a été sélectionné par le programme permanent de recherche Yphise qui identifie les progiciels méritant l'investissement des grandes entreprises.

- Ce volume résume l'opinion Yphise sur la valeur des progiciels.

- Il identifie la short-list des progiciels qui méritent attention compte tenu des bénéfices attendus par les décideurs informatiques.

- Il score les progiciels de la short-list après leur évaluation approfondie par Yphise certifiée ISO 9001. Le cahier des charges Yphise comporte plusieurs centaines de points de contrôle (volume CAHIER DES CHARGES). Les graphiques agrègent les résultats détaillés sur chaque progiciel (volume COMPARAISON). Les volumes CAHIER DES CHARGES et COMPARAISON sont sur www.yphise.fr.

(Voir le chapitre **LES EVALUATIONS DE PROGICIELS YPHISE**)

Les volumes DECIDER sont accessibles sur www.yphise.fr avec la Licence DECIDER.

La Licence DECIDER fournit aux décideurs informatiques, éditeurs et prestataires de service une compréhension précise des meilleurs progiciels du marché selon les exigences des grandes entreprises.

LE SEGMENT DE MARCHE

Les progiciels d'audit de conformité des serveurs ou SCCA (Server Configuration Compliance Audit) valident, contrôlent et scorent la conformité de la configuration des serveurs et des postes de travail sur des règles de configuration et de sécurité. Ces règles peuvent être spécifiques à l'entreprise ou basées sur des frameworks et best practices standard.

- Premièrement, les solutions de SCCA aident à définir et à personnaliser les points de contrôle des assets informatiques.

- Deuxièmement, elles gèrent la collecte des données sur ces assets. Cette collecte nécessite la découverte des assets, l'interrogation des serveurs et des postes de travail, ainsi que la centralisation des données et la planification des collectes.

- Troisièmement, ces solutions éditent des rapports et mettent à jour des tableaux de bord permettant de superviser, auditer, scorer et démontrer la conformité des assets face aux règles de configuration et de sécurité.

Valeur pour l'entreprise

➢ Diminuer le coût pour le métier des indisponibilités du SI

L'efficacité du métier est liée à la disponibilité du SI (Système d'Information). Une disponibilité continue du SI est nécessaire. Cette disponibilité nécessite la conformité de l'infrastructure à des règles de configuration et de sécurité. Les indisponibilités du SI sont principalement dues à des vulnérabilités non supprimées. Malgré le travail préventif dans les projets de l'industrialisation et de la gestion de la disponibilité métier, l'implémentation en production peut encore contenir des vulnérabilités dues à la non conformité de la configuration. Les entreprises doivent connaître et scorer leurs vulnérabilités afin de les tracer et de les supprimer.

Les solutions de SCCA sont des outils préventifs. Elles aident à anticiper les incidents. Elles réduisent les indisponibilités et dégradations de fonctionnement du SI dues aux non conformités de configuration. Les solutions de SCCA assurent l'alignement des serveurs devant être identiques, comme les serveurs de secours avec ceux en production. Elles s'intègrent aux outils d'orchestration des changements afin de supprimer les vulnérabilités détectées.

➢ Réduire le coût des menaces de sécurité

Les menaces liées à la sécurité sont un coût pour le métier. La perte de confidentialité, d'authentification ou d'intégrité peut dégrader la notoriété d'une entreprise, conduire à la perte de clients et de partenaires ou nécessiter le paiement de compensations.

Une partie des fraudes est rendue possible par les vulnérabilités de configuration du SI, ex. non conformité des droits d'accès, firewall désactivé ou base d'antivirus

obsolète. Malgré le travail de la Sécurité dans les projets, il peut rester dans l'implémentation en production des vulnérabilités aux fraudes.

Les solutions de SCCA contrôlent la présence, l'activation, la mise à jour et la configuration de différents logiciels, incluant des logiciels dédiés à la sécurité, ex. firewall et antivirus. Elles contrôlent l'adéquation entre les utilisateurs autorisés et les mots de passe. Elles aident à prioriser et chercher la solution aux vulnérabilités. Elles s'intègrent avec des solutions d'orchestration de changement afin de supprimer les vulnérabilités détectées.

- **Diminuer le coût pour l'entreprise des non conformités aux exigences légales**

Le SI doit être conforme aux exigences légales ou réglementaires (comme SOX, Basel II et PCI-DSS). Elles incluent des exigences dans le domaine du contrôle des risques opérationnels (ex. chapitre 404 de SOX). Les entreprises doivent démontrer le contrôle des risques liés à l'IT. La non conformité et l'audit sont coûteux. Les solutions DE SCCA aident à réduire ces coûts.

Les solutions DE SCCA lient l'information collectée aux exigences légales et réglementaires et aux meilleures pratiques. Elles scorent la conformité informatique. Elles automatisent et planifient les audits. Cela réduit les coûts et la durée des audits. Cela assure également la reproductibilité des audits (une condition légale).

Valeur sur les processus de l'informatique

- **Change et release management**

Le processus de release management gère le cycle de vie d'une nouvelle release d'un SI, partielle ou totale, jusqu'à sa mise en production. Il gère également le cycle de vie de changements unitaires.

Les projets sont validés dans un environnement de préproduction avant déploiement. L'exploitation peut avoir des problèmes en cas de différences entre environnement de préproduction et de production, ex. différences de paramétrage système ou de droits d'accès. Le processus de release management doit s'assurer que la configuration de de production est conforme aux règles de configuration requises et peut supporter le déploiement. Les solutions de SCCA permettent de comparer et de scorer différents environnements. Elles valident que l'environnement de production est conforme avant le déploiement d'une release.

Il est en pratique impossible de contrôler et d'empêcher toute modification sur un serveur, ex changements d'urgence. Les serveurs peuvent changer dans le temps dès lors que les workflow ne sont pas stricts. Le processus de release management doit comprendre et identifier les changements non contrôlés. Les solutions de SCCA font des audits automatisés à fréquence régulière. Elles conservent la vue de la configuration à un instant t. Elles permettent de retrouver quand un changement a été réalisé.

Le processus de release management doit gérer le cycle de vie des releases. Ceci inclut l'enregistrement de ce qui est configuré, comment et quand. Les solutions de SCCA tracent la configuration.

- **Gestion des environnements**

Le processus de gestion des environnements doit gérer, exploiter et supporter les différents environnements. Il doit s'assurer de la cohérence entre les environnements.

Le processus de gestion des environnements doit savoir fournir des environnements identiques, ex. primaire et secondaire. Il doit également savoir gérer les différences entre environnements - requises, autorisées ou interdites. Les différences doivent être analysées et, si utile, traitées avant la montée d'environnement. Le processus de gestion des environnements assure que la configuration des environnements est conforme avec ce qui est attendu. Les solutions de SCCA aident la gestion des environnements car elles collectent des données de configuration. Elles permettent de mettre en évidence les différences anormales.

Les audits de conformité de la configuration ne doivent pas entraver les choix technologiques. Les solutions de SCCA interrogent des données de configuration de tous les assets informatiques en utilisant plusieurs modes (intrusifs ou non). Ils s'adaptent à l'existant. Ils ne condamnent pas les décisions futures.

- **Industrialisation**

Le processus d'industrialisation vise à garantir l'exploitabilité du SI selon les engagements de service opérationnels utiles au métier. Il doit également s'assurer de l'automatisation des tâches de production.

Garantir le niveau de service délivré nécessite une conformité des serveurs en production avec des règles relatives à la performance, ex. logiciels installés ou paramètres d'un OS. Les solutions de SCCA auditent les serveurs. Elles garantissent la conformité aux paramètres d'installation recommandés. Ces recommandations peuvent être adaptées aux besoins de l'entreprise ou conformes à un organisme externe (ex. CIS Benchmark).

Le processus d'industrialisation définit les services techniques. Ceci inclut la définition des paramètres et les règles de nommage. Le processus d'industrialisation assure le contrôle qualité de la mise en oeuvre d'un serveur. Les solutions de SCCA permettent de définir des règles de configuration. Elles vérifient, contrôlent et scorent la conformité de la configuration. Elles fournissent une vision claire et actualisée de la configuration déployée.

Le processus d'industrialisation doit gérer les solutions techniques pour garantir l'exploitabilité. Les solutions de SCCA savent auditer la configuration des OS, middleware et applications. Elles aident à surveiller l'évolution dans le temps des risques d'exploitabilité du SI. Elles aident à analyser les incidents pour comprendre leurs causes et leurs impacts.

- **Gestion des produits et infrastructure**

  Le processus de gestion des produits (Product Management) et de l'infrastructure garantit l'expertise nécessaire sur les différents produits utilisés - matériel ou logiciel (middleware, progiciels outils ou applicatifs) - pour les administrer et les supporter.

  Les product managers assurent l'administration des produits dans chaque environnement. Les paramétrages peuvent être différents selon l'environnement. Les exigences ne sont pas les mêmes, notamment en terme d'accessibilité. Les product managers créent des règles qui doivent être appliquées selon les environnements. Ils doivent assurer la conformité avec ces règles. Les solutions de SCCA permettent d'auditer les paramètrages sur les environnements cibles. Elles auditent et scorent la conformité des produits par rapport au niveau attendu sur l'environnement ciblé. Elles alertent en cas de non conformité.

- **Sécurité**

  Le processus de sécurité garantit la confidentialité, l'authentification, l'intégrité, la non répudiation et la protection contre la malveillance des données et processus.

  La sécurité cherche à supprimer les vulnérabilités qui rendent les fraudes possibles. Les solutions de SCCA permettent d'agir de manière préventive. Elles contrôlent la conformité du SI avec des règles de sécurité. Elles aident à prioriser et identifier des solutions aux vulnérabilités. Elles vérifient la présence, l'activation et la configuration de logiciels de sécurité (ex. firewall et antivirus). Elles s'interfacent aux solutions d'orchestration de changement afin d'accélérer la suppression des vulnérabilités détectées.

  Le processus de sécurité doit protéger le SI contre les intrusions. Les solutions de SCCA aident à renforcer les produits de sécurité comme les annuaires LDAP ou autres. Par exemple, elles aident à contrôler les mots de passe et l'existence de comptes orphelins.

- **Continuité de service**

  Le processus de continuité de service vise à garantir la reprise d'un SI en cas de panne ou sinistre, selon des délais et des conditions imposées par les processus métier.

  La continuité de service amène souvent à disposer de serveurs de secours identiques aux serveurs de production. Un écart, même minime, peut empêcher les serveurs de secours d'assumer leur rôle en cas de panne du primaire. Les solutions de SCCA permettent de comparer les serveurs. Elles permettent de mettre en évidence les différences et de les scorer. Elles évitent les écarts critiques entre primaires et secondaires.

- **Gestion des incidents et des problèmes**

  Le processus de gestion des incidents vise à résoudre les incidents pour que les utilisateurs puissent reprendre leur activité. Le processus de gestion des problèmes aide à identifier l'origine d'un incident pour éviter sa récurrence.

  Les solutions de SCCA permettent d'agir de manière préventive. Elles auditent les serveurs et les postes de travail. Elles détectent la non conformité de la configuration actuelle à celle ciblée. Cela réduit le nombre d'incidents. Les audits permettent d'identifier le fossé entre configuration actuelle et attendue. Ils permettent de détecter les serveurs qui sont à risque. Les solutions de SCCA réduisent ainsi la récurrence d'incidents. Elles peuvent également s'interfacer avec des solutions d'orchestration du changement pour améliorer la résolution des vulnérabilités.

- **Contrôle des risques**

  Le processus de gestion des risques informatiques vise à gérer le risque qu'un SI représente pour l'entreprise en lien avec la gouvernance informatique. Les entreprises doivent garantir leur conformité avec des exigences réglementaires (Sarbanes-Oxley ou Bâle II). Elles doivent gérer les risques relatifs aux obligations légales associées à la gestion documentaire.

  Le processus de gestion des risques informatiques exige l'analyse et la supervision de la non conformité du SI par rapport à des solutions ou configurations standard. Les risques doivent être précisément évalués. Les solutions de SCCA vérifient et scorent la conformité des serveurs avec des règles. Elles identifient les non conformités critiques avec les règles de configuration. Elles réduisent le risque informatique en s'interfaçant aux solutions d'orchestration de changement.

- **Test**

  Le processus de test d'un projet doit garantir l'adéquation à la fois technique et fonctionnelle du résultat. Il doit garantir la vérification (Moe) et la validation (ou recette Moa) du SI sur les changements réalisés par les projets.

  Les solutions de SCCA détectent les différences de configuration avec la cible. Elles valident automatiquement les changements informatiques après avoir supprimé les vulnérabilités détectées. Ceci facilite les tests techniques. Les solutions de SCCA automatisent la validation de la configuration des postes de travail. Elles améliorent la consistance du processus de test sans augmenter la charge de travail.

LA SHORT-LIST YPHISE

Positionnement du segment de marché

Le segment de marché évalué est spécifique, avec un positionnement précis et une liste de progiciels déterminée. Pour éviter toute confusion, nous le différencions des segments de marché suivants. Un progiciel appartenant à l'un de ces segments de marché n'est pas approprié pour atteindre les bénéfices listés plus haut.

- **CMDB (Configuration Management Database)**

  Les solutions de CMDB aident à gérer et superviser les CIs critiques (Configuration Items, ex. services, applications, composants informatiques) qui contribuent aux services métier. Les solutions de CMDB aident à comprendre les dépendances entre les CIs avec des fonctions d'analyse d'impact. Elles aident à définir et contrôler les changements requis pour améliorer le SI. Elles inventorient les CIs et leurs dépendances. Les solutions de SCCA analysent en détail la configuration technique des CIs d'infrastructure. Les solutions de CMDB ne fournissent pas des possibilités d'analyse des serveurs et des postes de travail. Elles ne peuvent pas vérifier et démontrer la conformité avec des exigences légales et réglementaires. Les solutions de SCCA se concentrent sur l'audit de la conformité de configuration. Les solutions de CMBD et de SCCA sont des outils indépendants.

  Ex. BMC Atrium CMDB (BMC Software), CMDB 360 (Managed Objects), IBM CCMDB & IBM Service Management Platform (IBM) et HP UCMDB & HP BTO (HP).

- **Gestion des Services Métier (BSM - Business service monitoring)**

  Les solutions de BSM fournissent une vue en temps réel de l'état des services métier et de leur performance. Elles aident à comprendre les relations entre un environnement informatique et les services métier. Elles récupèrent des informations sur les services et sur les composants informatiques associés de la CMDB. Les solutions de BSM récupèrent aussi de l'information de solutions d'APM ou de solutions de découverte pour fournir une vue en temps réel de la disponibilité des services. Les solutions de SCCA ne visent pas à vérifier le statut des services en temps réel ; elles auditent la conformité de la configuration. Elles contrôlent l'activation de logiciels et des services, mais elles ne fournissent pas d'information sur son utilisation instantanée. Les solutions de BSM ne vérifient pas, ne contrôlent pas ou ne scorent pas la conformité de la configuration. Les solutions de BSM et de SCCA sont des outils indépendants.

  Ex. BMC BSM (BMC), Managed Objects (Managed Objects), HP BSM (HP) et Tivoli Business Systems Manager (IBM).

- **Antivirus**

  Les solutions d'antivirus s'appuient sur une base de données cohérente et mise à jour d'antivirus pour détecter en temps réel la présence des virus, des vers et des chevaux de Troie. Elles aident à supprimer les failles ou vulnérabilités dues à ces virus, vers et chevaux de Troie. Les solutions de SCCA ne détectent pas précisément ces vulnérabilités. Elles ne fonctionnent pas en temps réel. Elles ne peuvent contrôler si les logiciels dédiés à la sécurité, tels que les solutions d'antivirus, sont activés et à jour. Les solutions d'antivirus ne peuvent pas détecter la non conformité d'une configuration. Elles sont simplement une protection contre des virus, des vers et des chevaux de Troie. Les solutions de SCCA et d'antivirus sont des outils complémentaires pour assurer la sécurité de l'informatique.

  Ex. Norton AntiVirus (Symantec), McAfee Antivirus (McAfee), Endpoint Security et control (Sophos) et InterScan (TrendMicro).

- **Scan réseau (Network scanners)**

  Les solutions de scan réseau explorent le réseau pour déterminer les machines, services, OS et firewalls. Les solutions de SCCA peuvent importer l'information découverte par des solutions de scan réseau. Certaines solutions de SCCA peuvent elles-mêmes balayer le réseau. Les solutions de scan réseau ne peuvent pas vérifier, contrôler ou scorer la conformité avec des règles de configuration. Ce sont des outils complémentaires.

  Ex. NMap (Open source).

- **Gestion des failles de sécurité (SVM - Security vulnerability management)**

  Les solutions de SVM identifient et suppriment les failles de sécurité du réseau. Elles mesurent et gèrent la sécurité et les risques. Les solutions de SVM sont centrées sur la sécurisation du réseau. Elles ne peuvent pas vérifier ou scorer la conformité de configuration des serveurs. Les solutions de SCCA ne peuvent pas identifier et traiter les failles de sécurité du réseau. Elles détectent des failles de sécurité résultant d'une configuration inadéquate. Elles s'intègrent avec des solutions d'orchestration de changement afin de traiter ces vulnérabilités. Les solutions de SCCA et de SVM sont des outils complémentaires.

  Ex. IBM Internet Scanner Software (IBM), QualysGuard (Qualys) et Vulnerability Manager (CA).

- **Gestion des informations de sécurité et des événements (SIEM - Security information and event management)**

  Les solutions de SIEM gèrent la collecte d'informations en temps réel sur le SI. Elles s'appuient sur des fichiers de logs du SI et centralisent ces fichiers pour l'analyse. Elles corrèlent les données rassemblées afin de déterminer des failles de sécurité et la non conformité avec des politiques de sécurité. Elles sont des outils de sécurité. Elles ne peuvent pas vérifier ou scorer la conformité de configuration. Les solutions de SCCA ne

gèrent pas en temps réel le contrôle de la sécurité du SI. Les solutions de SCCA sont des outils qui permettent la prévention. Les solutions de SIEM ne préviennent pas des incidents ; elles fournissent des alertes en temps réel sur des incidents existants. Les solutions de SIEM et de SCCA sont des outils complémentaires.

Ex. Enterprise Security Manager (Arcsight), EnVision (EMC), nFX Open Security Platform (netForensics), NetIQ Security Manager (Attachmate) et Security Operations Manager (IBM Tivoli).

- **Audit et supervision des utilisateurs privilégiés (PUMA - Privileged-user monitoring and audit)**

Les solutions de PUMA supervisent, rapportent et analysent les activités des administrateurs et d'autres utilisateurs privilégiés. Elles fournissent de l'analyse en amont des comportements d'utilisateur et identifient des comportements anormaux. Elles ne peuvent pas vérifier ou scorer la conformité de configuration. Elles sont consacrées aux contrôles à froid des comportements d'utilisateur. Les solutions de SCCA ne contrôlent pas les comportements d'utilisateur. Les solutions de PUMA et de SCCA sont des outils indépendants.

Ex. Consul Insight (IBM, issu de l'acquisition de Consul).

- **Protection des accès réseau (NAP - Network access protection)**

Les solutions de NAP protègent le réseau privé d'une entreprise en renforçant la conformité avec les règles de sécurité sur les ordinateurs. Elles valident le degré de sécurité d'un ordinateur avant de permettre l'accès ou la communication réseau. Elles peuvent confiner les ordinateurs non sécurisés à un réseau restreint jusqu'à ce qu'ils deviennent sécurisés. Les solutions de NAP ne gèrent pas l'infrastructure informatique. Les solutions de SCCA vérifient, surveillent et auditent la conformité des configurations de l'infrastructure informatique. Ce sont des outils préventifs qui ne fonctionnent pas en temps réel, contrairement aux solutions de NAP. Les solutions de NAP et de SCCA sont des outils complémentaires.

Ex. Cisco Trust Agent (Cisco), Microsoft NAP (Microsoft) et Symantec Network Access Control (Symantec).

- **Contrôle des changements (CO - Change control)**

Les solutions de contrôle des changements automatisent, contrôlent et auditent les changements sur les systèmes afin de s'assurer de l'intégrité de l'infrastructure. Elles détectent tous les changements de l'infrastructure informatique. Elles vérifient automatiquement si des changements suivent les règles d'acceptation. Elles génèrent des rapports sur les changements. Elles améliorent le contrôle de la configuration en alertant sur les changements et en permettant des réponses rapides. Les solutions de SCCA vérifient et auditent la conformité actuelle de la configuration de l'infrastructure informatique. Elles n'assurent pas la détection de changements. Elles aident à démontrer la conformité de l'infrastructure avec des règles déterminées, par exemple par rapport à des politiques internes ou des obligations légales. Les solutions de

contrôle des changements et les solutions de SCCA sont des outils complémentaires destinés à garantir la conformité de la configuration dans le temps.

Ex. NetIQ Change Control Solutions (Attachmate), Quest (IBM) et Tripwire Enterprise (Tripwire).

- **Modélisation d'architecture d'entreprise (EAM - Enterprise architecture modeling)**

Les solutions d'EAM aident les architectes informatiques ou métier à modéliser le fonctionnement de l'entreprise et des SI. Elles permettent de représenter graphiquement les processus métier, l'organisation de l'entreprise, les services informatiques, l'architecture d'une infrastructure ou le design d'une application. Elles gèrent la relation et les dépendances entre les composants informatiques et métier. Elles représentent à un instant t une vision de l'organisation, qu'elle soit actuelle ou future. Les solutions de SCCA vérifient et auditent la conformité de la configuration de l'infrastructure informatique avec celle attendue. Les solutions d'EAM ne valident pas la configuration technique des éléments d'infrastructure. Les solutions de SCCA ne valident pas la structure architecturale du SI. Les solutions d'EAM et de SCCA sont des outils indépendants.

Ex. ARIS Business Architect (IDS Scheer), Corporate Modeler (Casewise), MEGA Modeling Suite (Mega) et System Architect (Telelogic).

- **Orchestration du changement (COM - Change orchestration management)**

Les solutions de COM exécutent les changements afin de maintenir opérationnels les serveurs et les postes de travail. Elles aident les entreprises à configurer et maintenir les serveurs, les middleware, les applications, les unités de stockage et le réseau. Les solutions de SCCA auditent et vérifient la conformité réelle de la configuration de l'infrastructure informatique. Elles n'exécutent pas ou ne contrôlent pas les changements. Ce sont des outils de prévention qui aident à identifier les vulnérabilités. Elles ne traitent pas ces vulnérabilités. Certaines solutions de SCCA retenues en shortlist s'interfacent aux solutions de COM afin de traiter les vulnérabilités détectées. Les solutions de COM et de SCCA sont des outils complémentaires.

Ex. Tivoli Provisioning Manager (IBM).

- **Décisionnel (BI - Business intelligence)**

Les solutions de BI aident à analyser une activité pour prendre des décisions. Elles fournissent des fonctions faciles à utiliser pour interroger et obtenir des rapports sur les données gérées dans des datamarts ou des systèmes opérationnels. Certaines analyses décisionnelles sur le risque peuvent avoir besoin des données fournies par les solutions de SCCA. Les solutions de BI permettent d'analyser ces données, mais elles ne peuvent pas les collecter. Les solutions de BI et de SCCA sont des outils complémentaires.

Ex. BusinessObjects (BusinessObjects), Cognos BI (Cognos), DBA Alphablox (IBM) et SAS Business Intelligence (SAS Institute).

- **Gestion des engagements de niveaux de service (SLM - Service level management)**

  Les solutions de SLM permettent de définir le catalogue de services et de négocier avec les clients les objectifs de niveaux de service et de contractualiser l'accord. Ils mettent à disposition des fournisseurs de service mais aussi des utilisateurs les rapports utiles pour évaluer le service délivré en comparaison avec les contrats (SLAs, Service Level Agreements). Les solutions de SCCA auditent la conformité de la configuration sur des règles déterminées. Elles n'auditent pas la conformité du niveau de service délivré. Les solutions de SLM ne peuvent pas évaluer ou vérifier la conformité de la configuration de l'infrastructure informatique. Les solutions de SLM et de SCCA sont des outils indépendants. Elles ne mesurent pas les mêmes indicateurs.

  Ex. Guarantee (Oblicore), SAS ITSLM (IT Service Level Management, SAS Institute) et ServiceFlow (DigitalFuel).

- **Gestion des accès (AM - Access management)**

  Les solutions d'AM contrôlent l'authentification des utilisateurs. Elles acceptent ou refusent l'accès aux services, selon des règles personnalisables. Elles s'appuient sur les annuaires d'entreprise pour authentifier les utilisateurs. Elles ne contrôlent pas ou n'auditent pas la conformité de la configuration de l'infrastructure informatique. Les solutions de SCCA ne contrôlent pas l'accès aux postes de travail et aux serveurs. Les solutions d'AM et de SCCA sont des outils indépendants.

  Ex. BMC Access Manager (BMC), OpenView Select Access (HP), RSA Access Manager (RSA Security), Sun Access Manager (Sun Microsystems) et Tivoli Access Manager (IBM).

- **Gestion des identités (IM - Identity management)**

  Les solutions d'IM contrôlent la définition des utilisateurs et des droits d'accès. Elles créent des comptes dans les annuaires d'utilisateurs des systèmes, en fonction du rôle de chaque utilisateur. Elles synchronisent plusieurs annuaires d'utilisateurs ; les données sur des utilisateurs changées centralement ou localement sont propagées aux autres annuaires d'utilisateurs pour assurer la cohérence des données. Elles accordent automatiquement les droits d'accès appropriés en fonction des rôles métier et sans avoir recours à une autre interface de gestion d'accès. Elles révoquent automatiquement les droits d'accès et suppriment les comptes des utilisateurs supprimés : elles s'assurent qu'aucune suppression d'accès n'est oubliée. Les solutions d'IM ne peuvent pas vérifier, auditer et évaluer la conformité de la configuration sur des règles. Les solutions de SCCA peuvent vérifier la conformité d'un annuaire selon des règles, par exemple les formats de mot de passe. Les solutions d'IM aident à résoudre les non conformités détectées par les solutions de SCCA. Les solutions d'IM et de SCCA sont des outils complémentaires.

Ex. Control-SA (BMC), eTrust Identity Manager (CA) , OpenView Select Identity (HP) et Tivoli Identity Manager (IBM).

- **Gestion des changements applicatifs (ACM - Application change management)**

  Les solutions d'ACM gèrent les versions de code pendant le cycle de vie d'un changement. Elles gèrent les processus de changement, de la demande à l'accomplissement de chaque changement. Elles gèrent les versions d'une série de changements. Elles ne contrôlent pas la conformité de la configuration ou d'un changement dans le temps. Les solutions de SCCA contrôlent la présence d'éléments et de leur conformité aux règles de configuration. Les solutions d'ACM contrôlent les changements nécessaires en cas de fichiers non conformes (ex. versions utilisées). Les solutions d'ACM et de SCCA sont des outils indépendants.

  Ex. ClearQuest/ClearCase (IBM Rational), Dimensions CM (Serena Software) et Synergy (Telelogic).

- **Application des politiques (PE - Policy enforcement)**

  Les solutions de PE gèrent la politique de sécurité d'une entreprise. Elles contrôlent l'exécution des services en temps réel. Elles ne vérifient pas ou n'auditent pas la conformité de configurations. Les solutions d'EP et de SCCA sont des outils indépendants.

  Ex. DataPower (IBM), Forum Sentry (Forum Systems), Layer 7 et Reactivity.

- **Gestion des patchs (PM - Patch management)**

  Les solutions de PM mettent à jour les logiciels et les systèmes d'exploitation. Elles détectent les mises à jour nécessaires et contrôlent leur déploiement. Les solutions de SCCA peuvent détecter la présence du patch le plus récent ou la conformité à une politique de gestion de patchs. Elles ne peuvent pas contrôler le déploiement d'un patch. Les solutions de PM ne peuvent pas détecter la non conformité de la configuration de l'infrastructure informatique. Les solutions de PM et de SCCA sont des outils indépendants.

  Ex. BMC Patch Manager and Tivoli Patch Management (IBM).

La short-list pour le segment de marché évalué

Les progiciels shortlistés par Yphise contrôlent la conformité de l'infrastructure informatique sur des exigences de configuration. Les exigences de configuration peuvent venir d'obligations légales ou réglementaires. Ils fournissent des collecteurs de données multiples et des capacités de reporting.

Yphise a analysé ce marché pour la première fois car jusque récemment il était trop exclusivement centré sur le contrôle de points de sécurité. Il s'agissait d'utilitaires de sécurité. L'offre a évolué. Les solutions de SCCA permettent maintenant de valider la conformité de la configuration sur toute règle de configuration. Ainsi, leur utilisation

dépasse maintenant le simple périmètre de la sécurité. Elles répondent à la diversité des problématiques de conformité de configuration que l'on trouve dans une DSI. Elles permettent en particulier la gestion du risque opérationnel lié à l'infrastructure informatique.

Notre short-list se centre sur les éditeurs qui ont démontré leur engagement pour fournir des solutions efficaces dédiées à ce marché :

- CCS & ESM (Symantec) ;
- NetIQ Secure Configuration Manager (Attachmate) et
- Tivoli Security Compliance Manager (IBM).

- **CCS & ESM (Symantec), Version 8.5 et 6.5.3 respectivement**

  La stratégie de Symantec est double. D'une part, Symantec optimise la sauvegarde, la récupération, le stockage des données et la gestion des serveurs. Sur cet aspect, son offre se base sur l'acquisition de Veritas en 2005. D'autre part, Symantec vise à assurer une protection complète des environnements numériques - de l'infrastructure à l'information. La société fournit des technologies pour la sécurité réseau et pour garantir la conformité des gateways, des serveurs et des postes de travail. Symantec inclut plusieurs business units qui couvrent la disponibilité, la sécurité, la protection des données et les questions de conformité.

  La business unit Compliance inclut quatre produits : Compliance Control Suite (CCS), Enterprise Security Manager (ESM), Security Information Manager (SIM) et Sygate. La solution historique de SCCA de Symantec est ESM. La dernière version date d'avril 2007. Symantec a acquis Bindview en octobre 2005, Altiris en janvier 2007 et 4FrontSecurity en mars 2007. Les trois entreprises sont centrées sur l'amélioration et la gestion de la sécurité. CCS est le produit résultant de l'acquisition de Bindview. La dernière version date d'avril 2007. Cette version inclut l'intégration des technologies 4FrontSecurity. De prochaines améliorations sont programmées au cours des trois années à venir, y compris une fusion de CCS et d'ESM en 2008.

- **NetIQ Secure Configuration Manager (Attachmate), Version 5.6**

  Attachmate, WRQ, OnDemand et NetIQ ont fusionné dans Attachmate. La stratégie d'Attachmate est de contrôler les services critiques tout en assurant la sécurité et la conformité. NetIQ est une business unit indépendante d'Attachmate. L'objectif de NetIQ est d'aider les directions informatiques à fournir des services critiques et à maitriser les risques opérationnels. L'offre de NetIQ se concentre sur la sécurité et la conformité des configurations.

  Le portefeuille de NetIQ inclut la gestion de la performance, la gestion de la sécurité, le contrôle des changements et la gestion des configurations. La solution de SCCA fait partie de la dernière gamme de ces produits. La solution s'appelle NetIQ Secure Configuration Manager. Elle aide à contrôler, superviser et auditer la conformité des configurations des serveurs. Elle s'appuie sur le module Risk and Compliance Center pour fournir les rapports. Son objectif est de réduire les risques opérationnels informatiques.

- **Tivoli Security Compliance Manager (IBM), Version 5.1.1**

  La division Tivoli couvre les logiciels pour la gestion d'infrastructure, incluant la sécurité, la gestion du stockage et la supervision. Un objectif est de supprimer les failles de sécurité et les problèmes de disponibilité qui peuvent se produire à cause de l'infrastructure informatique. Contrôler la conformité de l'infrastructure informatique selon des exigences de configuration est une approche préventive visant à réduire ce type de risque opérationnel.

  La solution s'appelle Tivoli Security Compliance Manager. La dernière version est sortie en décembre 2006. Le produit s'appuie sur DB2 AlphaBlox - la solution de BI d'IBM - pour analyser les données collectées via Tivoli Security Compliance Manager. La dernière version de DB2 AlphaBlox est sortie en septembre 2006.

Tendances du marché

Les progiciels short-listés sont cohérents avec les tendances majeures de ce segment de marché.

- **Améliorer la mesure des risques opérationnels informatiques**

  La non conformité sur une règle de configuration ne représente pas forcément le même risque opérationnel selon la nature ou l'utilisation d'un serveur, ex. la non conformité d'un serveur en production est plus critique que celle d'un serveur de développement. Mesurer le risque opérationnel informatique nécessite de scorer la non conformité. Etablir la priorité de traitement appropriée de chaque risque nécessite d'en évaluer la criticité. La plupart des solutions retenues ne permettent pas un scoring précis de la non conformité. Une perspective d'évolution concerne l'amélioration des possibilités de scoring et, ainsi, l'appréciation précise du risque opérationnel lié à l'infrastructure informatique.

- **Réduire le besoin de personnalisation**

  Les éditeurs s'appuient sur des frameworks standard, des best practices et des exigences légales afin de faciliter l'établissement des règles de conformité. Ils fournissent différents collecteurs de données, requêtes SQL et rapports d'audit. Une perspective d'évolution concerne l'élargissement de la diversité des collecteurs, requêtes SQL et rapports d'audit. Les éditeurs comptent sur des organisations externes pour aider les entreprises à prévenir les principaux risques, ex. CERT (Community Emergency Response Team). Ils fournissent des recommandations de configuration. Le standard OVAL émerge pour décrire les vulnérabilités de configuration. Certaines solutions peuvent déjà traiter les alertes dans ce format. Les évolutions vont continuer à travailler la standardisation des recommandations afin de réduire le besoin personnalisation lors de la mise en œuvre.

- **Sécuriser le réseau de l'entreprise**

  Les menaces de sécurité viennent en partie des terminaux portables. La non conformité des configurations, la désactivation de logiciels de sécurité ou une base

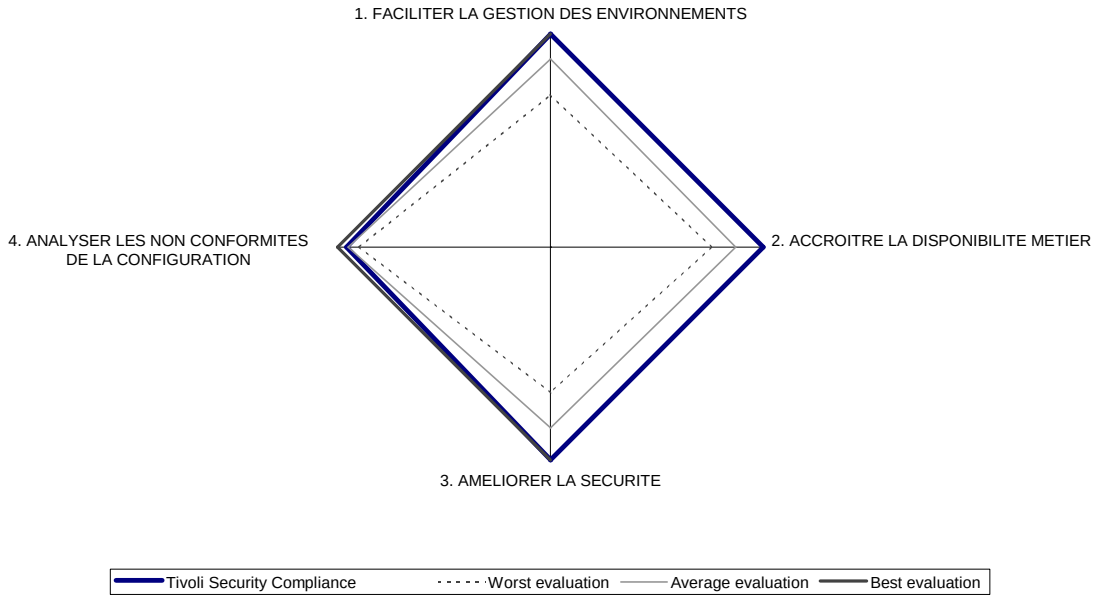
d'antivirus obsolète sont des vulnérabilités qui concernent le SI. Ces terminaux se connectent à de nombreux réseaux externes. Ils représentent un risque élevé de sécurité. Les solutions de SCCA ne mettent pas en quarantaine les terminaux non conformes ou ne corrigent pas les défauts de configuration ; ils vérifient la conformité. L'intégration des solutions de SCCA avec des solutions de NAP (Network access protection) et de COM (Change orchestration management) renforce l'intégrité du réseau. Ces intégrations vont se développer.

- **Faciliter la supervision journalière de l'infrastructure informatique**

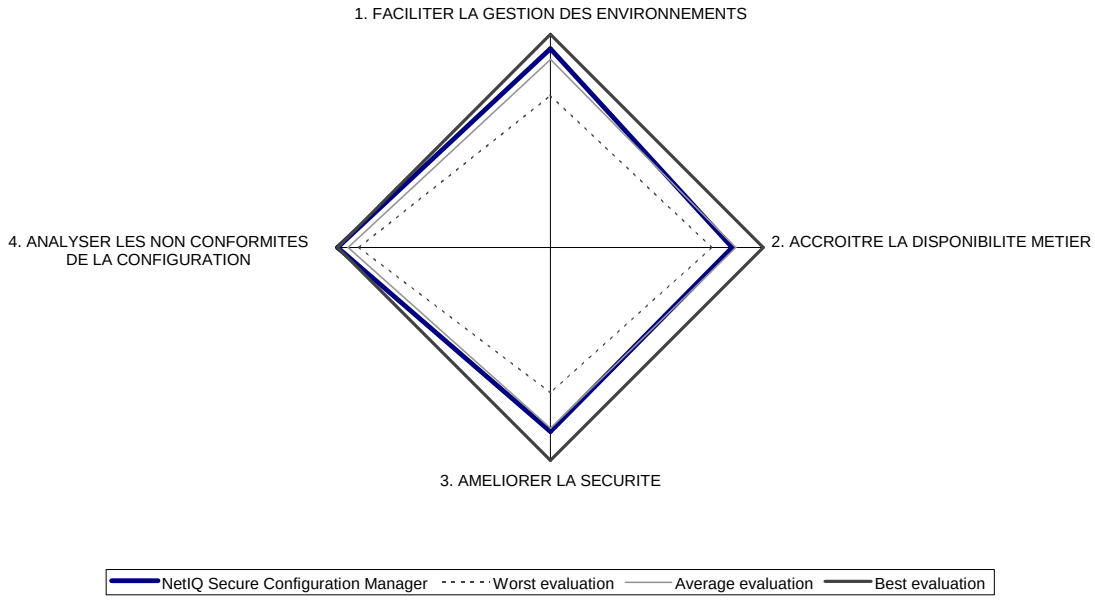
Les solutions de SCCA fournissent des vues et des audits sur les assets informatiques déclarés, classés en groupes. Mais les possibilités de personnalisation sont souvent limitées et complexes. Des évolutions amélioreront la découverte des assets ou leur définition par intégration avec une CMDB. Ceci réduira la charge de travail de mise en oeuvre. Des améliorations sont également utiles sur la personnalisation des groupes d'assets. Elles faciliteront la surveillance quotidienne et complète de l'infrastructure informatique.

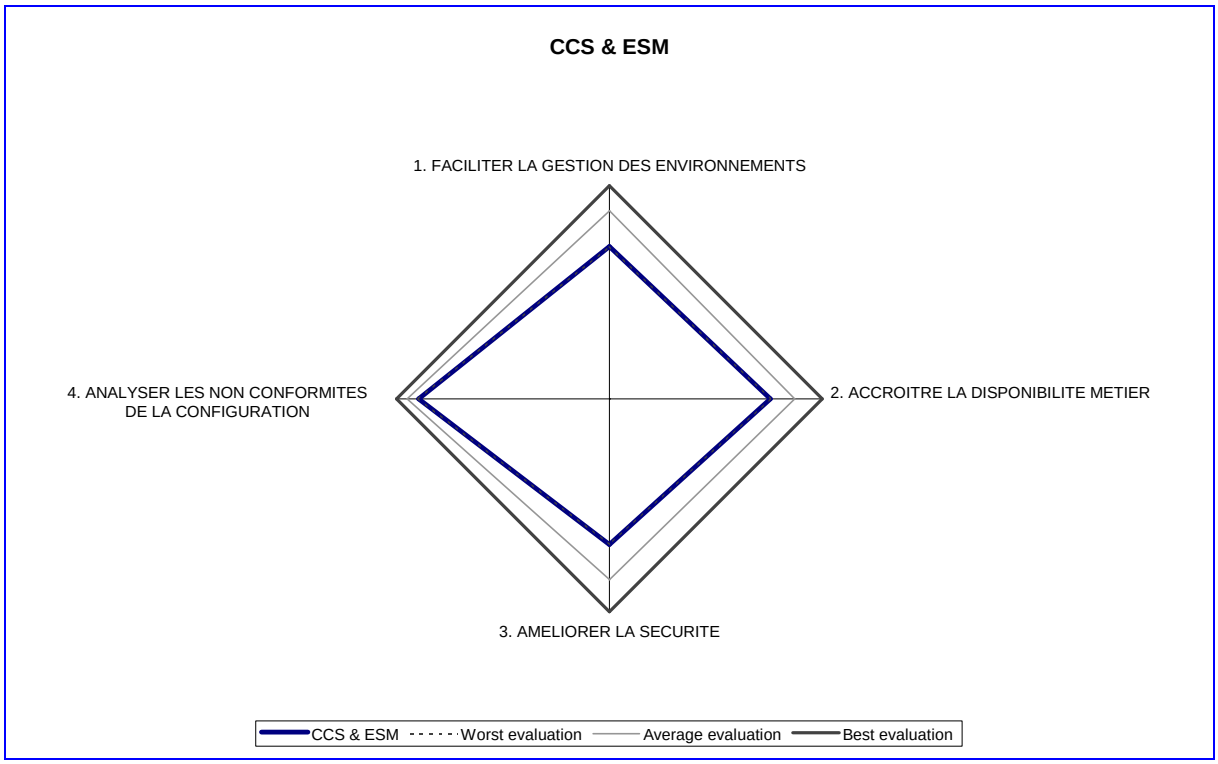
LE CLASSEMENT YPHISE

Tivoli Security Compliance Manager



NetIQ Secure Configuration Manager





Les graphiques ci-dessus sont ordonnés selon le classement final des progiciels short-listés, après leur évaluation approfondie selon la méthodologie Yphise certifiée ISO 9001:2000.

Les quatre axes d'évaluation permettent d'atteindre les bénéfices attendus par les grandes entreprises. Ils agrègent plus de 200 items fonctionnels ou techniques. Ce cahier des charges est concret pour répondre aux besoins actuels. Il est prospectif pour évaluer les perspectives d'avenir.

Commentaires

L'évaluation détaillée des progiciels short-listés démontre que les meilleurs possèdent les forces requises par les grandes entreprises pour investir en confiance.

Les résultats de l'évaluation démontrent que les progiciels short-listés apportent de la valeur. Cependant, il existe des différences significatives entre les progiciels concernant la couverture des différents axes d'évaluation.

Nous vous rappelons que la réalisation d'un prototype dans l'environnement technique ciblé et pour les bénéfices attendus reste nécessaire.

- Tivoli Security Compliance Manager est un produit mature et complet. Il fournit la meilleure couverture sur notre cahier des charges, grâce à ses capacités puissantes pour la collecte et pour l'organisation des audits.

  Tivoli Security Compliance Manager est adéquat pour auditer des SI complexes, incluant des plateformes hétérogènes et diverses applications et logiciels. Le produit

est aussi adapté pour contrôler la conformité de la configuration des serveurs aussi bien que des postes de travail en fonction de règles personnalisables.

Tivoli Security Compliance Manager est prêt à l'emploi, grâce à la gestion en standard de plusieurs collecteurs de données et de rapports d'audit. La personnalisation est simple. L'installation des agents de collecte est gérée de façon précise et l'intrusion est minimale. C'est pourquoi Tivoli Security Compliance est adéquat pour des projets nécessitant une installation rapide et peu de charges de maintenance.

- NetIQ Secure Configuration Manager est un produit mature et complet. Il fournit une bonne couverture de notre cahier des charges et la meilleure couverture sur un des axes d'évaluation.

  NetIQ Secure Configuration Manager convient pour auditer précisément un SI centré sur UNIX ou Windows. La solution se centre sur la vérification des contraintes de sécurité et sur l'audit de la conformité de la configuration en fonction d'exigences légales.

  NetIQ Secure Configuration Manager est prêt à l'emploi et peut rapidement prendre en compte les changements du SI, grâce à ses fonctions de découverte. La solution fournit plusieurs points de contrôle et des capacités de personnalisation. Ces agents nécessitent un seul déploiement. Ainsi, la maintenance et la charge d'installation sont réduites.

- La solution CCS & ESM fournit une couverture correcte et homogène sur notre cahier des charges. Elle convient pour auditer la conformité de la configuration en fonction de standards comme les meilleures pratiques, les frameworks et les exigences légales.

  La solution CCS & ESM est prête à l'emploi. L'éditeur met à jour fréquemment ses points de contrôle. La solution peut fonctionner comme une boîte noire. Cela réduit significativement la mise en place d'un projet et les compétences requises. Cependant, CCS manque de l'ouverture offerte par ESM. La fusion des deux produits, annoncée pour le premier trimestre 2008, devrait améliorer l'ouverture de la solution.

  La solution CCS & ESM permet de collecter de façon correcte les données standard. Elle est performante pour transférer les données collectées à des outils tiers. Ainsi elle convient pour la centralisation des collectes de données du SI et pour les rendre disponibles à des outils tiers.

1. FACILITER LA GESTION DES ENVIRONNEMENTS

1. FACILITER LA GESTION DES ENVIRONNEMENTS

Il faut gérer précisément les environnements informatiques et les configurations de chacun de leur composant pour réduire les indisponibilités. Les vulnérabilités et les écarts entre configurations actuelles et souhaitées sont les causes majeures d'indisponibilités d'un SI. Ces vulnérabilités peuvent se situer sur les postes, les serveurs ou les applications.

Commentaires

Les solutions de SCCA gèrent une base de données qui contient l'information sur les serveurs et les postes de travail. Elles alimentent cette base de données via un outil interne ou externe de découverte, une alimentation manuelle, l'import de fichiers ou l'intégration avec une CMDB. Une fois que la base de données est alimentée, les assets informatiques sont regroupés pour faciliter l'audit de leur conformité. Les solutions shortlistées diffèrent dans leurs capacités d'alimentation et dans leur faciliter à créer des groupes personnalisés.

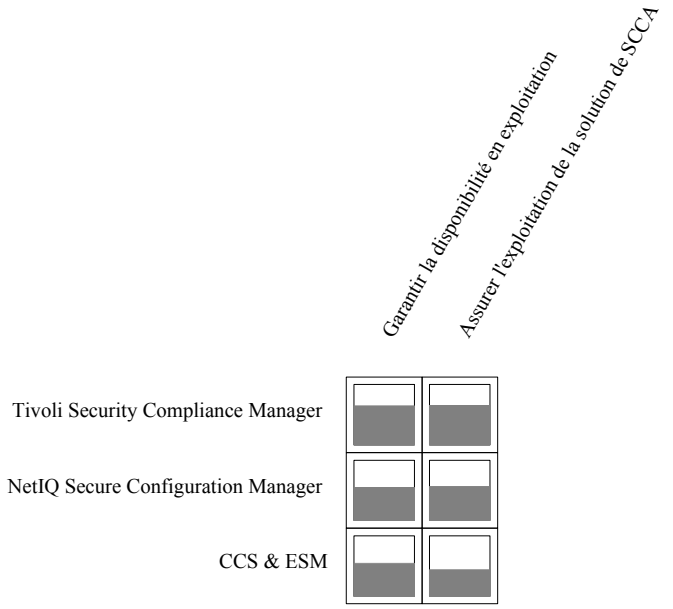
Les assets gérés par les solutions de SCCA incluent des applications métier, des éléments physiques d'infrastructure, des objets systèmes (ex. fichiers, dossiers, ports). Les solutions shortlisées collectent l'information relative aux applications en vérifiant les clés de registre ou à partir des fichiers de configuration. Les applications métier, les collecteurs de données disponibles pour les éléments physiques d'infrastructure et l'agilité à étendre la collection des données diffèrent.

- Tivoli Security Compliance Manager se distingue sur l'axe "Faciliter l'interrogation des environnements". C'est le seul qui couvre l'intégralité des OS requis. La création et la gestion de groupes personnalisés est simple. Le produit se distingue également sur l'axe "Assurer la capacité à interroger l'intégralité du SI". C'est le seul qui permet de créer facilement des collecteurs de données et de vérifier la configuration des éléments physiques d'infrastructure.

- NetIQ Secure Configuration Manager se distingue sur l'axe "Assurer la capacité à interroger l'intégralité du SI". Premièrement, il peut définir des requêtes complexes et personnalisées sur des composants du SI. Deuxièmement, la vision de la conformité par composant est claire. Seul NetIQ Secure Configuration Manager fournit ces deux fonctions. Il se distingue également sur l'axe "Faciliter l'interrogation des environnements". Il fournit sept manières d'alimenter la base de données avec des serveurs et postes de travail, incluant un outil de découverte embarqué. Cela assure la complétude et la richesse de l'information collectée.

- La solution CCS & ESM fournit une couverture correcte de nos exigences sur ce chapitre. Elle fournit des collecteurs de données variés pour vérifier les configurations de bases de données.

2. ACCROITRE LA DISPONIBILITE METIER



2. ACCROITRE LA DISPONIBILITE DU METIER

L'indisponibilité et les dégradations de fonctionnement du SI dues aux non conformités de configuration doivent être réduites. Ces non conformités sont aussi des causes importantes de difficulté de reprise sur incident ou sinistre. Les solutions de SCCA aident à garantir la continuité de l'exploitation. Elles doivent enfin ne pas dégrader le niveau de service délivré par la charge qu'elles génèrent.

Commentaires

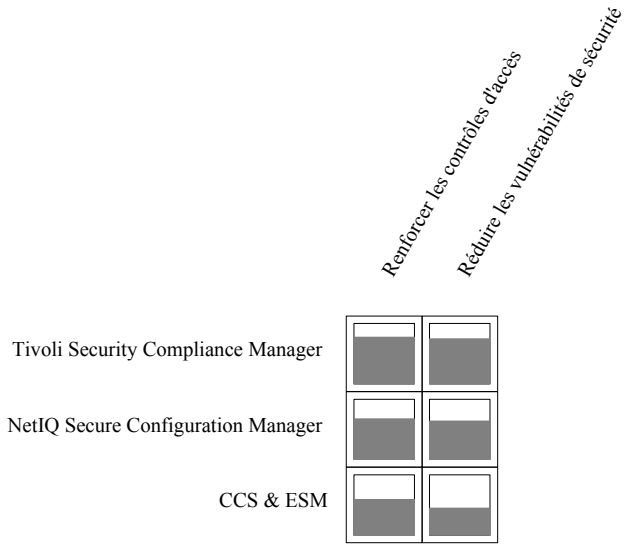
Les solutions de SCCA vérifient et scorent la conformité des serveurs de secours aux serveurs en production. Elles évitent les écarts de configuration qui peuvent poser des problèmes de disponibilité. Elles aident à trouver les causes d'incidents et à alerter des outils tiers ou des responsables. Elles accélèrent la résolution d'incidents. Elles s'intègrent avec des solutions dédiées à la performance pour permettre un contrôle précis de la conformité de configuration. L'intégration des produits shortlistés avec des solutions de gestion de la performance ou de gestion des incidents diffère. Les produits diffèrent également dans leur agilité à comparer deux serveurs.

Les solutions de SCCA collectent les données requises sur la configuration des serveurs et des postes de travail à partir d'agents distribués et stockent ces données dans des bases. Le mode de collecte dépend de la sécurité, de la performance ou de politiques internes à l'entreprise. Les solutions de SCCA aident à organiser la collecte des données via l'installation d'agents performants, supportant plusieurs protocole de communication à distance et permettant une planification de la collecte. Ces capacités varient selon les produits shortlistés.

- Tivoli Security Compliance Manager se distingue sur l'axe "Garantir la disponibilité en exploitation". La solution s'intègre avec de nombreuses solutions tiers, incluant celles d'IBM et de Cisco. Il alerte les responsables de façon adéquate et transfère l'information requise aux outils tiers. Seul Tivoli Security Compliance Manager fournit une bonne couverture des deux fonctionnalités. Il se distingue également sur l'axe "Assurer l'exploitation de la solution de SCCA". Il fournit des fonctions complètes pour planifier et tracer la collecte des données. Il fournit aussi des agents performants qui embarquent leur propre JVM (Java virtual machine).

- NetIQ Secure Configuration Manager se distingue sur l'axe "Garantir la disponibilité en exploitation". Il gère précisément la recherche des causes d'incidents. Il peut aussi scorer automatiquement la conformité de la configuration d'un serveur de secours. NetIQ Secure Configuration se distingue également sur l'axe "Assurer l'exploitation de la solution de SCCA". Il supporte des protocoles de communication variés et utilise des agents performants.

3. AMELIORER LA SECURITE



3. AMELIORER LA SECURITE

Une partie des fraudes est rendue possible par les vulnérabilités du SI, ex. droits d'accès inappropriés, firewall désactivé, antivirus obsolète. L'audit de la configuration permet d'identifier ces vulnérabilités pour les surveiller ou les supprimer.

Commentaires

Les solutions de SCCA réduisent les vulnérabilités de sécurité du SI. Elles s'appuient sur des alertes CERT et des benchmarks CIS pour fournir des points de vérification à jour. Elles identifient les éléments critiques non conformes aux règles de sécurité. La collecte des données sur la configuration de tous les assets informatiques, incluant les serveurs critiques, peut représenter un risque de sécurité pour l'entreprise. Les solutions de SCCA assurent l'intégrité et la fiabilité des communications. Elles sont basées sur des protocoles de communication sécurisés standard. Les logiciels de sécurité fournis par les solutions de SCCA diffèrent ; ce peut être des firewalls ou des antivirus, voire des annuaires. Les groupes CERT et CIS avec lesquels les solutions travaillent sont aussi différents. Enfin, la sécurité des communications varie.

Les solutions de SCCA aident à renforcer les contrôles d'accès. Premièrement, elles gèrent la sécurité des accès à l'information via leur propre console. Les progiciels shortlistés gèrent précisément les autorisations relatives aux produits et bases de données ; cependant la gestion des utilisateurs et de l'authentification varie. Deuxièmement, les solutions de SCCA vérifient les droits d'accès au SI. Leur capacité à récupérer cette information d'annuaires diffère.

- Tivoli Security Compliance Manager se distingue sur l'axe "Réduire les vulnérabilités de sécurité". Le produit fournit plusieurs collecteurs de données pour vérifier la configuration des firewalls et des antivirus. Il assure la consistance des d'alertes sur la non conformité et l'intégrité des informations collectées. Il se distingue également sur l'axe "Renforcer les contrôles d'accès". Il assure l'intégrité des agents installés sur les serveurs. Cela améliore la fiabilité des informations reçues des serveurs.

- NetIQ Secure Configuration Manager se distingue sur l'axe "Renforcer les contrôles d'accès". Il fournit une couverture homogène sur nos exigences sur cet axe. Le produit peut gérer les utilisateurs via une intégration avec un annuaire LDAP. Il fournit aussi une bonne couverture sur l'axe "Réduire les vulnérabilités de sécurité". Le produit s'appuie sur un partenariat pour mettre à jour fréquemment les points de contrôle de sécurité. Grâce au support de standards, il peut utiliser plusieurs sources d'alertes concernant la vulnérabilité.

- La solution CCS & ESM obtient un faible résultat sur l'axe "Réduire les vulnérabilités de sécurité". Cependant, elle fournit des fonctions efficaces pour gérer la sécurité des communications. La solution démontre une bonne couverture de l'axe "Renforcer les contrôles d'accès". Elle fournit des collecteurs de données variés dédiés à l'analyse de la configuration d'annuaires et à la vérification de la conformité d'UIDs et de mots de passe avec des règles de sécurité.

4. ANALYSER LES NON CONFORMITES DE LA CONFIGURATION

4. ANALYSER LES NON CONFORMITES DE LA CONFIGURATION

Le SI doit contribuer à la conformité de l'entreprise par rapport aux exigences réglementaires ou légales (ex. SOX, Bâle II, PCI-DSS). Cela inclut des exigences sur la maîtrise des risques opérationnels (ex. Sarbanes-Oxley, Chapter 404) associés à l'informatique. L'entreprise doit démontrer sa maîtrise des risques que l'informatique peut faire courir au métier.

Commentaires

Les solutions de SCCA aident à superviser la conformité du SI. Après la collecte des données sur les assets informatiques, elles stockent les données et scorent la non conformité. Elle supervisent la conformité par serveur ou groupe de serveurs. Elles identifient les assets les plus critiques via des tableaux de bord personnalisables. Les produits diffèrent dans leur agilité et leur flexibilité à scorer la conformité de la configuration. Pour suivre la conformité dans le temps, des rapports d'audit doivent être stockés. Les solutions de SCCA génèrent et enregistrent les rapports.

Les solutions de SCCA aident aussi à démontrer la conformité du SI par rapport aux règles de configuration. Elles aident à créer des requêtes, à les utiliser pour les audits, à planifier les audits et à créer des rapport d'audits. Pour assurer la cohérence des audits avec des frameworks, des best practices ou des exigences légales, les solutions de SCCA mettent à jour fréquemment leurs outils d'audit. Les produits varient dans la facilité à créer des requêtes et à mettre à jour des audits.

- Tivoli Security Compliance Manager se distingue sur l'axe "Surveiller la conformité de la configuration du SI". Il gère précisément le stockage des données collectées dans la base de données. Il fournit des fonctions standard et peut aussi s'appuyer sur Tivoli Storage Manager pour améliorer les capacités de gestion du stockage. Tivoli Security Compliance Manager fournit aussi une bonne couverture de quatre des cinq exigences liées à l'axe "Démontrer la conformité réglementaire du SI". Le produit fournit des fonctions efficaces pour créer des requêtes personnalisées et des collecteurs de données.

- NetIQ Secure Configuration Manager se distingue sur l'axe "Surveiller la conformité de la configuration du SI". Le produit fournit des fonctions complètes et efficaces pour scorer la non conformité de la configuration des assets informatiques. Il permet une personnalisation des règles de scoring. Il se distingue également sur l'axe "Démontrer la conformité réglementaire du SI". Il fournit des fonctions efficaces pour créer les audits et mettre à jour les outils. C'est le seul à fournir les deux fonctions.

LES EVALUATIONS DE PROGICIELS YPHISE

Le programme permanent de recherche Yphise

Yphise identifie et certifie les meilleurs progiciels du marché selon les attentes des grandes entreprises.

Le programme de recherche Yphise a trois objectifs.

1. **Il sélectionne chaque année les segments de marché** sur lesquels de bons progiciels possèdent les forces nécessaires aux grandes entreprises pour investir en confiance. Yphise sélectionne les segments de marché selon les préoccupations et priorités des décideurs informatiques.

2. Pour chaque segment de marché, **il identifie la short-list des progiciels** qui méritent attention compte tenu des bénéfices attendus par les grandes entreprises.

3. **Il évalue chaque progiciel en short-list et certifie les meilleurs**. L'opinion Yphise se fonde sur une évaluation précise de chaque progiciel afin d'apprécier leur capacité à apporter le retour sur investissement attendu. La méthodologie Yphise, certifiée ISO 9001, permet d'obtenir un score rigoureux sur chaque progiciel. Yphise certifie les progiciels qui possèdent les forces requises.

L'expérience unique Yphise

Plusieurs milliers de décisions d'investissement en grandes entreprises ont utilisé la recherche indépendante Yphise.

1. **Yphise évalue 150 progiciels par an depuis 1985**. Yphise possède une expérience inégalée pour distinguer les stratégies gagnantes des éditeurs de celles vouées à l'échec.

2. **La recherche Yphise couvre les domaines d'intérêt des grandes entreprises** pour développer, exploiter, maintenir et sécuriser les systèmes d'information nécessaires à leur compétitivité. Yphise a une expertise sans équivalent pour apprécier les priorités d'investissement parmi les familles de progiciels selon les préoccupations des grandes entreprises.

3. **Yphise est certifié ISO 9001 en évaluation de progiciels**. Cette norme internationale de la qualité garantit l'indépendance et le centrage sur les préoccupations des grandes entreprises.

4. **L'opinion Yphise est fondée sur une évaluation approfondie** des progiciels. Chacune comporte plusieurs centaines de points de contrôle, conçus pour répondre aux besoins des grandes entreprises.