Power Week

Université IBM i 2019

22 et 23 mai

IBM Client Center Paris

S05 – Protection des données IBM i : chiffrement, tokenisation et anonymisation

Vincent MUZELLEC
Syncsort
vincent.muzellec@syncsort.com

Protection des données sensibles

La confidentialité des données est attendue

- Les **clients**, **partenaires** et **employés** s'attendent à ce que leurs données soient protégées.
- La divulgation de données et le vol **endommagent** vos relations
- Les atteintes à la protection des données font l'objet d'une **publicité négative**

Les menaces proviennent de sources multiples

- Les intrus criminels **reconnaissent la valeur** des données IBM i
- Les entrepreneurs et les partenaires commerciaux devraient avoir un **accès limité.**
- Les utilisateurs ne devraient voir que les données **dont ils ont besoin** dans le cadre de leur travail.

Les réglementations exigent une protection des données sensibles

- PCI DSS (WW)
- HIPAA (US)
- **RGPD** (EU)
- GLBA (US)
- Lois de l'État sur la protection de la vie privée
- Et plus

Chiffrement - Terminologie

Une clé de chiffrement des données doit être bien **protégée** ou les données seront **exposées**.

- **Une clé** est utilisée pour crypter les données (N° SS, numéros de carte de crédit, etc.) via **l'algorithme de cryptage**, tel que AES (Advanced Encryption Standard).

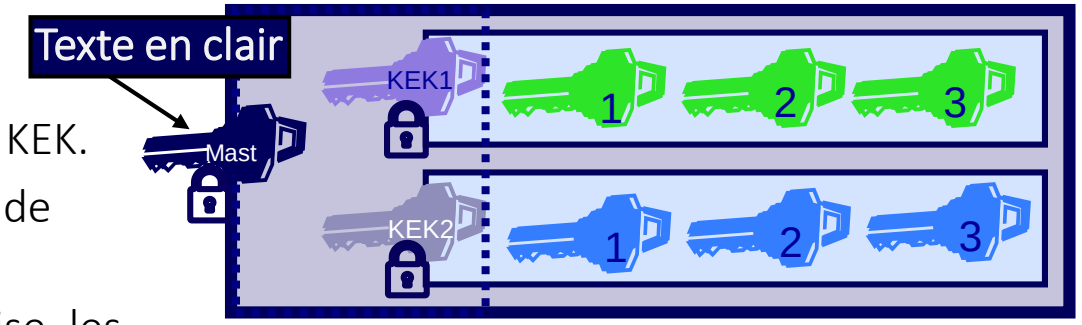
NOTE:
Les algorithmes de chiffrement, tels que AES, 3DES, etc. sont de notoriété publique. Les clés de chiffrement doivent être gardées secrètes et protégées pour assurer la sécurité.

Il est recommandé de crypter la clé de données avec une **clé de cryptage de clé** (KEK).

- Utilisé pour crypter les clés de cryptage des données

Une **clé maîtresse** peut alors être utilisée pour crypter toutes les clés KEK.

- Une clé maitresse est utilisée pour crypter les clés KEK ou les clés de cryptage des données.
- Clé de **niveau supérieur**, en clair ! Si la clé maitresse est compromise, les données sont compromises.
- Comment **conserver** cette clé maitresse en toute sécurité ?



Chiffrement

Qu’est-ce que c’est ?

- Transformation d'informations **lisibles** par l'homme en un format **illisible**
- Le point de sortie IBM i **FieldProc** (IBM i 7.1 ou supérieur) permet le chiffrement des champs sans modification de l'application.
- Nécessite une clé de chiffrement forte en plus d'un algorithme de chiffrement fort.
- La clé de cryptage est **nécessaire** pour renvoyer les données dans un format lisible par l’humain.
- Une solution de **gestion des clés** est recommandée pour assurer la sécurité et la bonne gestion des clés de chiffrement.
- Les **activités** de chiffrement et de déchiffrement doivent être **enregistrées**.
- Les données décryptées doivent être **masquées** en fonction des **privilèges** de l'utilisateur.

Avantages

- Une technologie **éprouvée**
- Les normes offrent une certification **indépendante**
- Les algorithmes sont **continuellement** passés au crible
- **Confiance** dans le respect des exigences de la réglementation qui impose la protection des données confidentielles

Inconvénients

- Selon l'implémentation, le chiffrement et le déchiffrement des données de terrain peuvent avoir une **pénalité de performance**.
- Le chiffrement peut ne **pas préserver le format** original des champs, ce qui peut affecter les processus de validation des champs.
- Les applications peuvent **nécessiter des modifications** pour empêcher l'utilisation d'index chiffrés.

Astuces

- Spécifié par certains **règlements** ; vérifiez les exigences des règlements auxquels votre entreprise doit se **conformer**.
- Meilleure pour les applications nécessitant des **performances supérieures**
- Rechercher une implémentation sécurisée d'un algorithme sécurisé
- Vérifier les **certifications**

Tokenisation

Qu’est-ce que c’est ?

- Remplace les données sensibles par des **valeurs de substitution** ou des "tokens" (Jetons).
- Les jetons sont stockés dans une base de données ou "**coffre-fort à jetons**" qui **maintient** la relation entre la valeur originale et le jeton.
- Les jetons de conservation de format **conservent les caractéristiques** des données d'origine (par exemple, un numéro de VISA ressemblerait toujours à un numéro de VISA et passerait un contrôle LUHN).
- La **cohérence** des jetons permet d'utiliser le même jeton pour chaque **instance** des données d'origine.
- Lorsque les données "jetonisées" sont affichées dans leur forme originale, elles doivent être **masquées** en fonction des **privilèges** de l'utilisateur.

Avantages

- Les jetons ne peuvent pas être **inversés** avec une clé car il n'y a pas de relation algorithmique avec les données d'origine.
- La tokenisation **maintient les relations** avec les bases de données
- La suppression des données du serveur de production réduit le risque d'exposition en cas de violation.
- L'utilisation d'un jeton pour les données d'un serveur peut les retirer du champ d'application de la **conformité**.
- Référencé spécifiquement pour la norme PCI DSS et prend en charge la conformité à d'autres **réglementations**.

Inconvénients

- La tokenisation n'est pas aussi largement reconnue que le chiffrement par les organismes de normalisation.
- La "jetonisation" a un impact sur les performances pour enregistrer les jetons et les récupérer.

Astuces

- Disponible par l'intermédiaire des réseaux de paiement par carte de crédit pour l'utilisation de numéros de carte de crédit à jeton
- Idéal pour la BI et les requêtes puisque la tokenisation **maintient les relations** avec les bases de données.
- Utile pour l'envoi de données à des **services externes** pour traitement lorsque des données sensibles ne sont pas nécessaires - ou pour les systèmes de **développement** et de **test**.

Anonymisation

Qu’est-ce que c’est ?

- Une forme de tokenisation qui remplace de façon **permanente** les données sensibles par des valeurs de substitution.
- Les valeurs de remplacement ne sont pas stockées, de sorte qu'un coffre-fort sécurisé **n'est pas nécessaire**.
- Peut remplacer toutes les instances d'une donnée originale par le même jeton
- **Conserve** les caractéristiques des données d'origine.
- Diverses méthodes d'anonymisation peuvent être utilisées (**masquage**, **mélange**, etc.).
- **PAS une solution** à utiliser sur un serveur de production car les données anonymisées sont **irrécupérables** et les données d'origine sont nécessaires à la production.

Avantages

- **Ne peut pas être inversé** avec une clé car il n'y a pas de relation algorithmique avec les données d'origine.
- Supporte la **conformité** avec le GDPR et d'autres règlementations
- Garde les serveurs hors production hors du champ d'application de la **conformité**

Inconvénients

- L'anonymisation n'est pas aussi largement reconnue que le cryptage par les organismes de **normalisation**.

Tips

- **Pas une solution** pour les données sur votre serveur **de production**
- Idéalement utilisé pour anonymiser des données sensibles sur un système de **développement** ou de **test**
- Bon pour l'envoi de données à des services **externes** pour traitement
- Lorsqu'il est couplé à une solution de haute disponibilité pour la réplication vers des nœuds non-HA, il peut alimenter le système **dev/test** avec des données anonymisées

Présentation d’Assure Security

Une solution complète qui couvre tous les aspects de la sécurité IBM i et aide à assurer la mise en conformité aux réglementations de cybersécurité.

Que votre entreprise ait besoin de mettre en œuvre un ensemble complet de fonctionnalités de sécurité ou que vous ayez besoin de traiter une vulnérabilité spécifique, Assure Security est la solution.

Assure Security

Le meilleur de la suite de sécurité Syncsort

Assure Security contient

- Les meilleures capacités de sécurité IBM i acquises de Cilasoft, Enforcive et Townsend Security.
- Un outil commun pour les nouvelles installations et les mises à niveau
- Une console de monitoring commune avec les produits HA de Syncsort
- Prise en charge de la localisation de l'interface utilisateur en anglais, français et espagnol

Pour les clients Cilasoft et Townsend, Assure Security

- Est le produit de nouvelle génération
- Prise en charge transparente de vos capacités actuelles (ou plus)
- Facilite l'adoption de nouvelles capacités de sécurité

Assure Security

traite les problèmes sur l'écran radar de chaque agent de sécurité et de l'administrateur IBM i

Supervision de la mise en conformité

Gagnez en visibilité sur toute l'activité de sécurité de votre IBM i et alimentez en option une console d'entreprise.

Contrôle d’accès

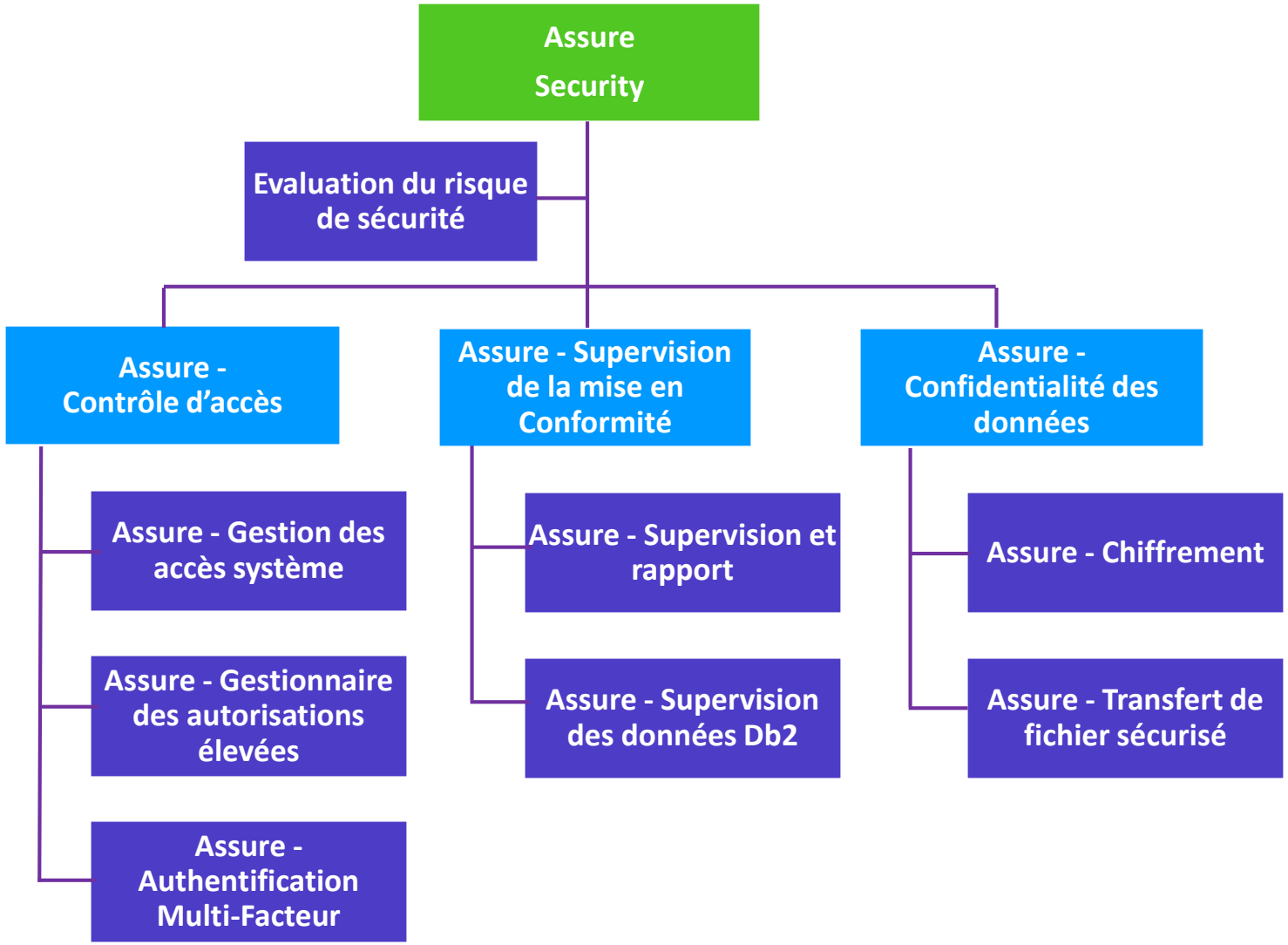
Garantir un contrôle complet des accès non autorisés et la possibilité de retracer toute activité, suspecte ou non.

Confidentialité des données

Protéger la confidentialité des données au repos ou en mouvement pour prévenir les atteintes à la protection des données.

Evaluation du risque de sécurité

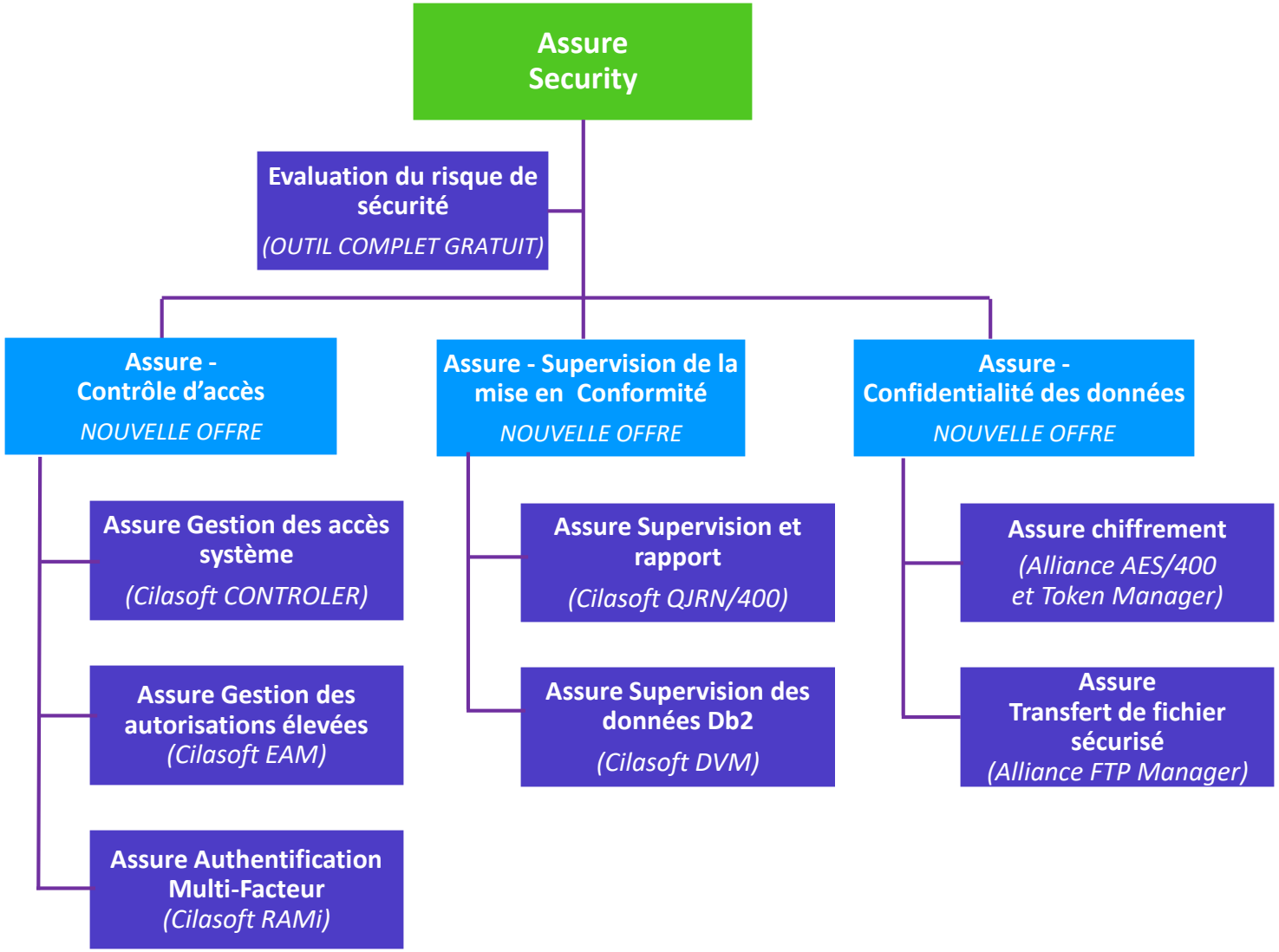
Évaluer vos menaces et vulnérabilités en matière de sécurité



Choisissez le produit complet

Choisissez un ensemble de fonctions

Ou sélectionnez une capacité spécifique



Les meilleures marques acquises par Syncsort s'associent dans Assure Security !

Assure Contrôle d’accès

Contrôle d’accès

Sécurisez tous les points d'entrée dans votre système, y compris l'accès au réseau, à la base de données, à la ligne de commande, etc.

Gestion des autorisations élevées

Augmenter automatiquement le pouvoir de l'utilisateur selon les besoins et de façon limitée.

Authentification Multi-facteur

Renforcer la sécurité des connexions en exigeant de multiples formes d'authentification

Assure - Gestionnaire d'accès au système

Auparavant Cilasoft CONTROLER

Contrôle complet de l'accès externe et interne

- Accès au réseau (FTP, ODBC, JDBC, OLE DB, DDM, DRDA, NetServer, etc.)
- Accès aux ports de communication (ports, adresses IP, sockets - couvre SSH, SFTP, SMTP, etc.)
- Accès aux bases de données (protocoles open-source - JSON, Node.js, Python, Ruby, etc.)
- Accès aux commandes

Puissant, flexible et facile à gérer

- Interface graphique facile à utiliser
- Configuration standard fournie pour un déploiement prêt à l'emploi
- Des règles puissantes et flexibles pour contrôler l'accès en fonction de conditions telles que la date et l'heure, les paramètres du profil utilisateur, les adresses IP, etc.
- Mode de simulation pour tester les règles sans impact sur les utilisateurs
- Fournit des alertes et produit des rapports
- Enregistre les données d'accès pour l'intégration SIEM

Sécurise les systèmes IBM i et permet la conformité réglementaire

- Supporte les exigences réglementaires pour SOX, GDPR, PCI-DSS, HIPAA, et autres.
- Satisfait les agents de sécurité en sécurisant l'accès aux systèmes et aux données IBM i
- Réduit considérablement le temps et le coût de mise en conformité réglementaire
- Permet la mise en œuvre des meilleures pratiques en matière de sécurité
- Détecte rapidement les incidents de sécurité afin que vous puissiez y remédier efficacement.
- A peu d'impact sur les performances du système

Assure - Gestionnaire des autorisations élevées

Auparavant Cilasoft EAM

Contrôle complet et automatisé d'autorisations d'utilisation élevées

- Les administrateurs peuvent accorder manuellement des requêtes aux utilisateurs ou des règles peuvent être configurées pour les gérer automatiquement.
- Des règles peuvent être définies pour les profils source et cible en fonction des profils de groupes, des groupes supplémentaires, des listes d'utilisateurs, etc.
- Les règles déterminent le contexte dans lequel l'autorisation peut être accordée, comme l'heure de la date, le nom du travail, l'adresse IP, etc.
- *Les méthodes SWAP ou *ADOPT sont soutenues pour élever l'autorité.
- Gère les processus se connectant via ODBC, JDBC, DRDA et FTP

Surveillance complète des profils surélevés

- Surveille les utilisateurs surélevés et la durée de l'élévation à partir de l'interface graphique ou des écrans 5250.
- Tenir à jour une piste de vérification de l'activité élevée à l'aide des journaux de travail, des captures d'écran, des points de sortie et des journaux.
- Une option est disponible pour enregistrer simplement l'activité de l'utilisateur sans changer d'autorité.
- Produit des alertes en cas d'événements tels que le dépassement du temps autorisé
- Génère des rapports dans une variété de formats
- Permet l'intégration avec les systèmes de ticketing

Permet la conformité réglementaire et les meilleures pratiques en matière de sécurité

- Génère une piste d'audit des actions par profils élevés pour les auditeurs de conformité
- Facilite la gestion des demandes d'autorité élevée sur demande
- Appliquer la séparation des tâches
- Satisfait les agents de sécurité en réduisant le nombre de profils puissants et en conservant une piste de vérification complète.
- Produire les alertes et rapports nécessaires
- Réduit considérablement l'exposition à la sécurité causée par l'erreur humaine
- Réduit le risque d'accès non autorisé aux données sensibles

Assure - Authentification Multi-Facteur

Auparavant Cilasoft RAMi

Authentification multi-facteur complète pour IBM i

- Vous permet d'exiger deux facteurs ou plus pour l'authentification :
  - Quelque chose que l'utilisateur sait
  - Quelque chose que l'utilisateur a
  - Quelque chose que l'utilisateur "est"
- S'appuie sur les codes des services d'authentification fournis par l'intermédiaire d'un appareil mobile, d'un courriel, d'un jeton matériel, etc.
- Permet de réactiver le profil en libre-service et de modifier le mot de passe en libre-service.
- Appuie le principe des quatre yeux pour les changements supervisés
- Certifié RSA (voir DOC-92160 sur le site communautaire de RSA)

Options de déploiement puissantes et flexibles

- Permet d'activer l'authentification multifactorielle uniquement pour des utilisateurs ou des situations spécifiques.
- Le moteur de règles facilite la configuration lorsque l'authentification multifactorielle est utilisée.
- Prise en charge de plusieurs authentificateurs
  - Syncsort authenticator (gratuit)
  - Serveurs basés sur RADIUS
  - RSA SecureID (local ou dans le cloud)
- Options à lancer à partir de l'écran d'ouverture de session 5250 ou à la demande (manuellement ou à partir d'un programme)
- Options d'authentification multi-facteur ou en deux étapes

Renforce la sécurité des connexions et permet la conformité

- Ajoute une couche d'authentification au-delà des mots de passe mémorisés ou écrits.
- Réduit les risques de coûts et de conséquences liés au vol de données et à l'accès non autorisé aux systèmes et aux applications.
- Réduit le risque qu'un utilisateur non autorisé devine ou trouve le mot de passe d'un autre utilisateur.
- Répond aux exigences et recommandations réglementaires de la norme PCI DSS 3.2, du règlement de cybersécurité du NYDFS, de Swift Alliance Access, de GLBA/FFIEC, etc.

Assure confidentialité des données

Cryptage

Transformez les champs de base de données lisibles par l'homme en texte cryptographique illisible à l'aide de solutions de chiffrement et de gestion des clés certifiées par l'industrie.

Tokenisation

Supprimer les données sensibles d'un serveur en les remplaçant par des valeurs de substitution qui peuvent être utilisées pour récupérer les données d'origine.

Transfert de fichier sécurisé

Transfert sécurisé de fichiers sur des réseaux internes ou externes à l'aide d'un cryptage.

Assure - Chiffrement

Auparavant Alliance AES/400

La seule solution certifiée NIST pour le cryptage IBM i

- Cryptage automatique des données Db2 à l'aide des Field Procedures IBM i (IBM i 7.1 ou supérieur)
- Les algorithmes de cryptage AES sont optimisés pour la performance
- Masquage intégré des données décryptées en fonction de l'utilisateur ou du groupe
- Audit d'accès aux données intégré
- Inclut des commandes de cryptage pour Enregistrer les fichiers, IFS, et bien plus encore.
- API de chiffrement étendues pour RPG et COBOL
- Résout facilement les problèmes d'index cryptés dans les programmes RPG hérités
- Inclut la tokenisation pour remplacer les données sensibles par des valeurs de substitution ou des "tokens".

Prise en charge de plusieurs options de gestion des clés

- Les clés de chiffrement doivent être protégées car les algorithmes de chiffrement sont publics.
- La réglementation en matière de conformité exige une gestion appropriée des clés
- Assurez que la sécurité prend en charge plusieurs options de gestion des clés
  - Magasin de clés local fourni
  - Conçu pour s'intégrer à l'Alliance Key Manager de Townsend Security, conforme à la norme FIPS 140-2, disponible en version:
    - VMware appliance
    - Hardware Security Module (HSM)
    - Cloud HSM (AWS, Azure)
  - Autres solutions de gestion de clés compatibles OASIS KMIP

Permet la conformité réglementaire et les meilleures pratiques en matière de sécurité

- Chiffrement des données sans impact sur les applications
- Protège les données contre l'accès non autorisé par le personnel interne, les sous-traitants et les partenaires commerciaux - ainsi que les intrus criminels.
- Répond aux exigences des réglementations qui imposent la protection des données sensibles telles que HIPAA/HITECH, PCI-DSS, les lois nationales sur la vie privée, etc.
- Renforce la confiance de vos clients en faisant affaire avec vous grâce à la validation du NIST.

Assure - Transfert de fichier sécurisé

Auparavant Alliance FTP Manager

Sécurise les données transférées avec des partenaires commerciaux ou des clients

- Sécurise les données circulant sur les réseaux internes ou externes en les cryptant avant leur transfert et leur décryptage à destination.
- Crypte tout type de fichier, y compris les fichiers de base de données Db2, les fichiers plats, IFS, Save Files et les fichiers spool.
- Prise en charge des protocoles de transfert courants
  - Secure Shell (SSH SFTP)
  - Secure FTP (SSL FTPS)
- Enregistre toutes les activités de chiffrement et de transfert de fichiers pour répondre aux exigences de conformité.
- Offre une option PGP pour crypter les données à la source et à l'emplacement de destination.
- Les fichiers cryptés PGP peuvent être reçus depuis n'importe quel autre système, y compris Windows, Linux et UNIX.

Permet une gestion et une automatisation centralisées

- Application automatique de la protection des données grâce à des stratégies gérées de manière centralisée
- Négocie intelligemment les pare-feu
- Configurable en configuration hub-and-spoke pour gérer automatiquement tous vos besoins de transfert de fichiers
- Fournit des notifications et des alertes par e-mail, SNMP, messages et alertes
- Prise en charge de la confirmation par e-mail du transfert avec la liste de diffusion
- Fournit des API et des commandes pour l'intégration avec les applications RPG, COBOL et les programmes CL.
- Prise en charge des fichiers ZIP et PDF cryptés

Permet la conformité réglementaire et les meilleures pratiques en matière de sécurité

- Protège les données d'être vues en texte clair lorsqu'elles sont transférées d'un réseau à l'autre.
- Répond aux exigences des réglementations telles que PCI, HIPAA et autres qui exigent le transfert crypté et l'enregistrement des activités de transfert.
- L'option PGP offre un cryptage multiplateforme basé sur des normes qui fonctionne avec toutes les autres solutions PGP.

Assure Surveillance de la conformité

Audit Système & Base de données

Simplifier l'analyse des journaux IBM i pour surveiller les incidents de sécurité et générer des rapports et des alertes

Intégration SIEM

Intégrer les données de sécurité IBM i aux données provenant d'autres plates-formes en les transférant vers une console de gestion des informations et des événements de sécurité

Superviser la donnée Db2

Surveillez les vues des données sensibles Db2 et, en option, bloquez les données de la vue

Assure Surveillance et rapports

Surveillance complète de l'activité du système et de la base de données

- Simplifie le processus d'analyse de journaux complexes
- Surveillance des modifications apportées au système et à la base de données disponible séparément ou ensemble
- Puissant moteur d'interrogation avec filtrage étendu permettant d'identifier les écarts par rapport aux meilleures pratiques en matière de conformité ou de sécurité
- Modèles prêts à l'emploi, personnalisables et fournis pour les solutions ERP courantes et la conformité GDPR
- Aucune modification de l'application n'est requise

Produit des alertes et des rapports clairs et faciles à lire

- Fournit des alertes sur les événements de sécurité et de conformité par le biais d'un popup e-mail ou d'un syslog.
- Permet la création facile de rapports personnalisés qui peuvent être générés en continu, selon un calendrier ou à la demande.
- Prise en charge de plusieurs formats de rapport, notamment PDF, XLS, CSV et PF
- Distribue les rapports via SMTP, FTP ou IFS
- Add-on disponible pour envoyer des données de sécurité aux consoles SIEM telles que IBM Qradar, ArcSight, LogRhythm, LogPoint, et Netwrix
- Intégration des données de sécurité dans Splunk pour la surveillance de la sécurité ou l'analyse des opérations informatiques disponibles via la famille de produits Ironstream de Syncsort.

Avantages de la surveillance et pour la conformité et la sécurité

- Identification rapide des incidents de sécurité et des écarts de conformité
- Surveille les meilleures pratiques de sécurité que vous avez mises en œuvre
- Permet de satisfaire aux exigences réglementaires pour GDPR, SOX, PCI DSS, HIPAA et autres
- Satisfait aux exigences d'une piste de vérification basée sur un journal.
- Assure une véritable séparation des tâches et respecte l'indépendance des auditeurs.

Assure supervise les données Db2

Vous donne un contrôle total sur l'accès aux données sensibles

- Surveille les données Db2 pour vous informer de qui a consulté les enregistrements sensibles d'un fichier, quand et comment
- Un riche ensemble de règles permet d'affiner la détection d'accès en lecture et les alertes (par exemple l'accès spécifique à un fichier en particulier).
- Pas besoin de modifier les applications existantes
- Génère des rapports en plusieurs formats et des alertes en temps réel
- Le mode de blocage empêche les utilisateurs de lire les informations spécifiées dans un fichier.
- Mode de simulation disponible pour tester les règles afin de s'assurer que le blocage ne perturbe pas les activités normales avant le déploiement.

Produire des rapports clairs et ciblés sur les vues de données

- Les rapports peuvent montrer les accès à:
  - Salaires des gestionnaires
  - Données médicales
  - Renseignements bancaires
- Les rapports peuvent inclure des informations sur la manière dont les données ont été consultées, telles que :
  - adresse IP
  - Utilisateur actuel
  - Pile d'appels
  - Et plus encore
- Précisez seulement les champs que vous devez voir dans un rapport, et non l'enregistrement entier, pour garder vos données confidentielles vraiment confidentielles.

Auparavant Cilasoft DVM

Répond aux exigences les plus strictes en matière de conformité et de sécurité

- Répond aux exigences réglementaires les plus strictes en matière de données confidentielles
- Réduit le risque de divulgation accidentelle de données
- Déjouent les activités illicites ou criminelles

Evaluation du risque

Outil d’évaluation du risque de sécurité

Vérifier minutieusement tous les aspects de la sécurité IBM i et obtenir des rapports détaillés et des recommandations.

Service d’évaluation du risque de sécurité

Laissez l'équipe d'experts en sécurité Syncsort effectuer une évaluation approfondie des risques et fournir un rapport avec des conseils de remédiation.

Evaluation du risque de sécurité

Ce que c’est

- Une évaluation des risques de sécurité est une vérification approfondie de tous les aspects de la sécurité du système, y compris (mais sans s'y limiter) :
  - Paramètres de sécurité de l’OS
  - Mot de passe par défaut
  - Utilisateurs désactivés
  - Utilisateur de ligne de commande
  - Distribution d'utilisateurs puissants
  - Autorités des bibliothèques
  - Ports ouverts
  - Point d’exit OS
- Les outils ou services d'évaluation des risques fournissent des rapports détaillés sur les constatations, les explications et les recommandations en matière de remédiation.
- Le rapport de l'évaluation pour la gestion non technique résume les constatations.

Avantages

- Aide à satisfaire aux exigences en matière d'évaluation annuelle des risques que l'on retrouve dans les règlements tels que PCI DSS et HIPAA.
- Résultats dans des rapports qui informent la direction et les administrateurs sur les vulnérabilités de sécurité et les remèdes.
- Gagnez du temps en automatisant (outil) ou en déchargeant (service) le processus d'évaluation.
- L'utilisation d'un service ou d'un outil qui englobe une vaste expérience peut combler des lacunes dans l'ensemble des compétences.
- Séparation des tâches entre l'administrateur et le vérificateur

Category	# of checks	Ok	Warning	High Risk
System Values	31	11	14	6
User Profiles	11	2	4	5
Object Authorities	8	1	3	4
Network Access	2	0	2	0

Services professionnels mondiaux

Ajouter de la valeur à votre investissement

Offres de services flexibles pour la sécurité

- Évaluation des risques pour la sécurité
- Services de démarrage rapide
- Services de vérification rapide
- Services de mise à jour de sécurité (installation de correctifs, PTFs, nouvelles versions, etc.)
- Services de mise à jour du système (s'assurer que la solution de sécurité est correctement configurée après un changement d'adresse IP, de version du système d'exploitation, etc.)
- Assistante de l'auditeur (assistant de l'auditeur interne ou externe)
- Services de sécurité gérés
- Conseil à la carte

Tirez parti de l'équipe d'experts en sécurité chevronnés de Syncsort!

Services de sécurité gérés

Protégez votre entreprise avec les plus hauts niveaux de sécurité grâce aux services de sécurité gérés exclusifs de Syncsort. Laissez les experts de l'équipe Global Services de Syncsort se charger de la surveillance, de l'optimisation, des mises à jour logicielles et de l'audit de votre solution de sécurité afin que le personnel puisse se concentrer sur les autres priorités informatiques.

- Réduire les risques d'atteinte à la sécurité ou de violation de la conformité
- Libérez votre personnel informatique pour travailler sur d'autres projets importants
- Bénéficiez de la vaste expérience des experts de Syncsort
- Profitez des dernières fonctions de sécurité grâce aux mises à jour logicielles automatisées.
- Choisissez le niveau qui répond à vos besoins

PLATINUM	Recevez tous les services de niveau Gold plus la surveillance quotidienne de votre solution de sécurité Syncsort qui inclut la détection d'intrusion et nous fournissons des services d'assistance aux auditeurs.
GOLD	Nous effectuons un suivi quotidien de vos paramètres de sécurité, gérons votre configuration de sécurité et fournissons des rapports d'état hebdomadaires. Nous installerons les correctifs de votre solution de sécurité Syncsort, les PTF et les mises à niveau de version.
SILVER	Nos experts procèdent tous les jours à des contrôles de sécurité, examinent les résultats et, au besoin, apportent les ajustements nécessaires en fournissant un rapport hebdomadaire.
BRONZE	Nous vérifions quotidiennement votre environnement de sécurité et fournissons un rapport mensuel sur l'état de vos paramètres de sécurité.

Avantages d’Assure Security

Assure Security offre des capacités innovantes qui dominent le marché sur de multiples facettes de la sécurité :

- ✓ **Contrôle complet** des points d'accès système IBM i, anciens et modernes
- ✓ Cryptage **certifié NIST**, y compris l'intégration avec la gestion des clés hors plate-forme conforme à la norme FIPS de Townsend Security
- ✓ Authentification **multi-facteur** puissante et flexible avec certification RSA
- ✓ Une nouvelle solution unique et innovante pour la surveillance des vues de **données hautement confidentielle**
- ✓ Possibilité de transmettre les données de sécurité IBM i aux principales solutions **SIEM**, y compris la certification QRadar
- ✓ Intégration avec les **solutions Syncsort HA** via un tableau de bord de surveillance et des scripts de basculement

Assure Security est un choix clair

- Vous permet d'atteindre et de maintenir la **conformité réglementaire**
- **Automatise les tâches** courantes de gestion de la sécurité et de la conformité
- **Surveillance** complète de l'activité du **système** et de la **base de données**
- **Détecte** rapidement les **incidents** de sécurité et les **écarts** de conformité
- **Empêche** l'accès non autorisé aux systèmes et aux données
- **Protège** la confidentialité des données au repos et en mouvement pour prévenir les **violations**
- Permet une véritable **ségrégation des tâches**
- Prise en charge des **meilleures pratiques** en matière de sécurité


syncsort
advancing data