precisely

La sécurité sur l'IBM i : est-ce un enjeu ou une mode ?

Florence Rabuel, Head of IBM Infrastructure Sales, SEMEA
Aurélie Godec, Senior Director, Customer Support

18 Novembre 2021

precisely

Le leader mondial de l'intégrité des données

Faites confiance à vos données. Construisez vos possibilités.

Nos logiciels d'intégrité de données et nos produits d'enrichissement de données offrent la précision et la cohérence nécessaires pour prendre des décisions en toute confiance.

12 000
clients

90
du Fortune 100

Des clients dans plus de
100 pays

2 000
employés

Les marques auxquelles vous faites confiance nous font confiance

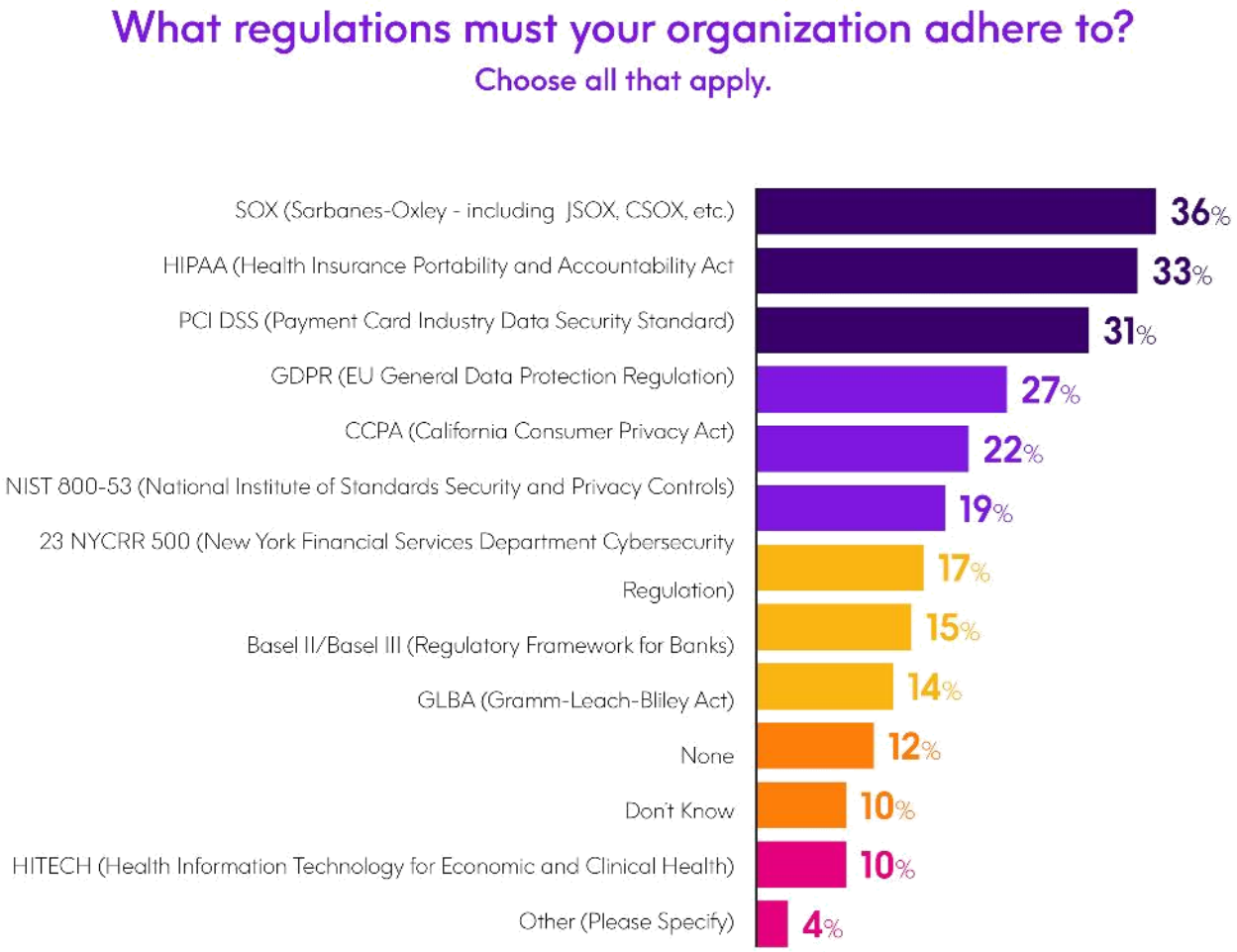
Les partenaires leaders de la Data s'associent à nous

La Sécurité sur IBM i - 2020

- Les Sujets
  - Confiance et Challenges de la Sécurité
  - La mise en conformité aux différentes réglementations
  - Audits
  - Violations de sécurité
  - Les investissements prévus
- Profil des Sondés
  - Responsabilité quant à la sécurité sur IBM i
    - 48% sont les responsables directs
    - 52% partagent cette responsabilité
  - Taille des sociétés
    - 78% travaillent dans des compagnies de plus de 100 employés
    - 57% travaillent dans des compagnies de plus de 500 employés
  - Verticaux
    - 10% dans le domaine de la Santé
    - 10% dans les Services Financiers
    - 10% dans les Services Informatiques
    - 9% dans la Banque

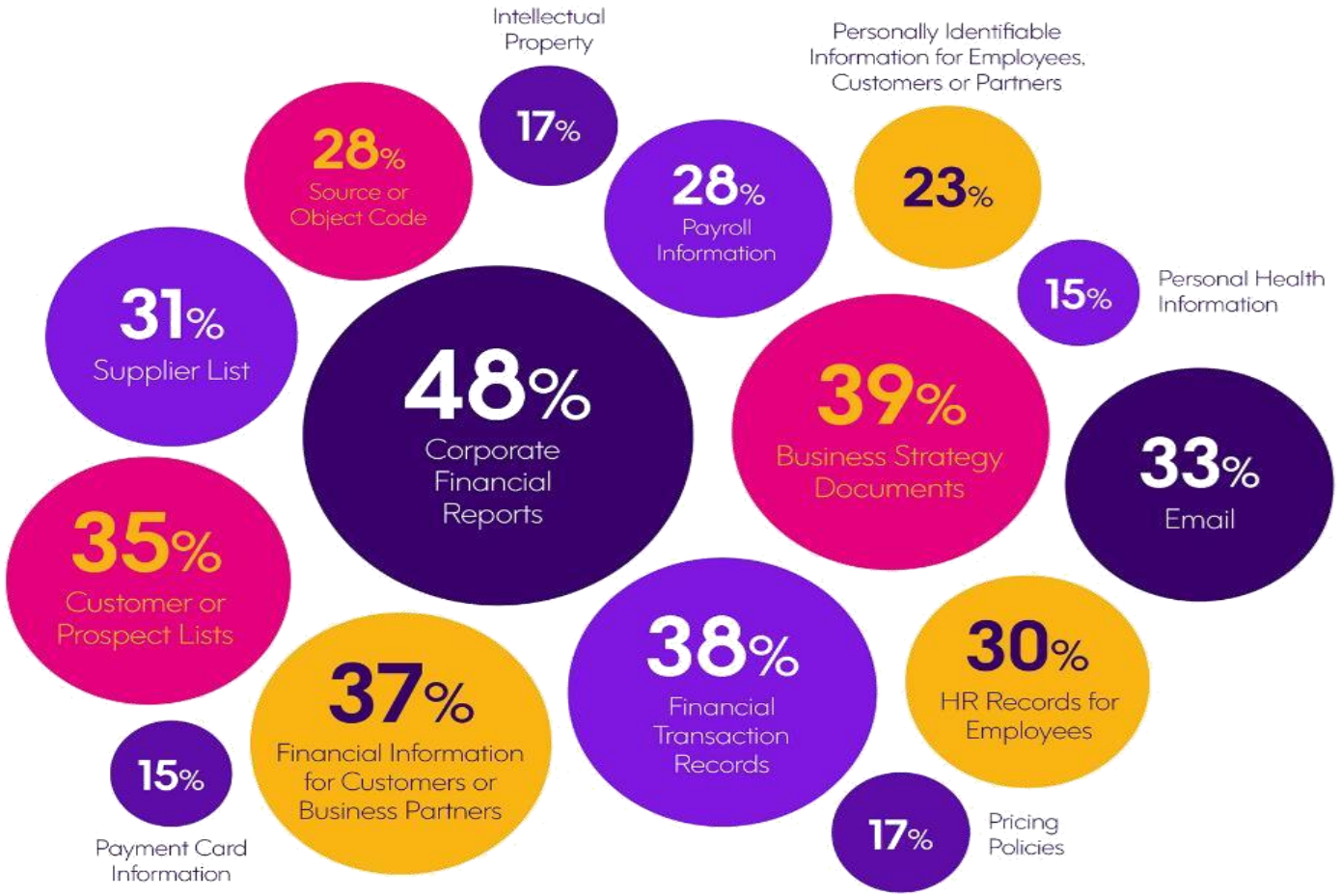
Les Réglementations

- 80% des personnes interrogées dans le cadre de notre enquête sont tenues de se conformer à une ou plusieurs réglementations
- Près de 90% des sondés ont déclaré avoir des données sensibles sur leurs serveurs IBM i:
  - 48%, notamment, ont des rapports financiers internes
  - 39% possèdent des informations business stratégiques
  - 38% ont des enregistrements de transactions financières



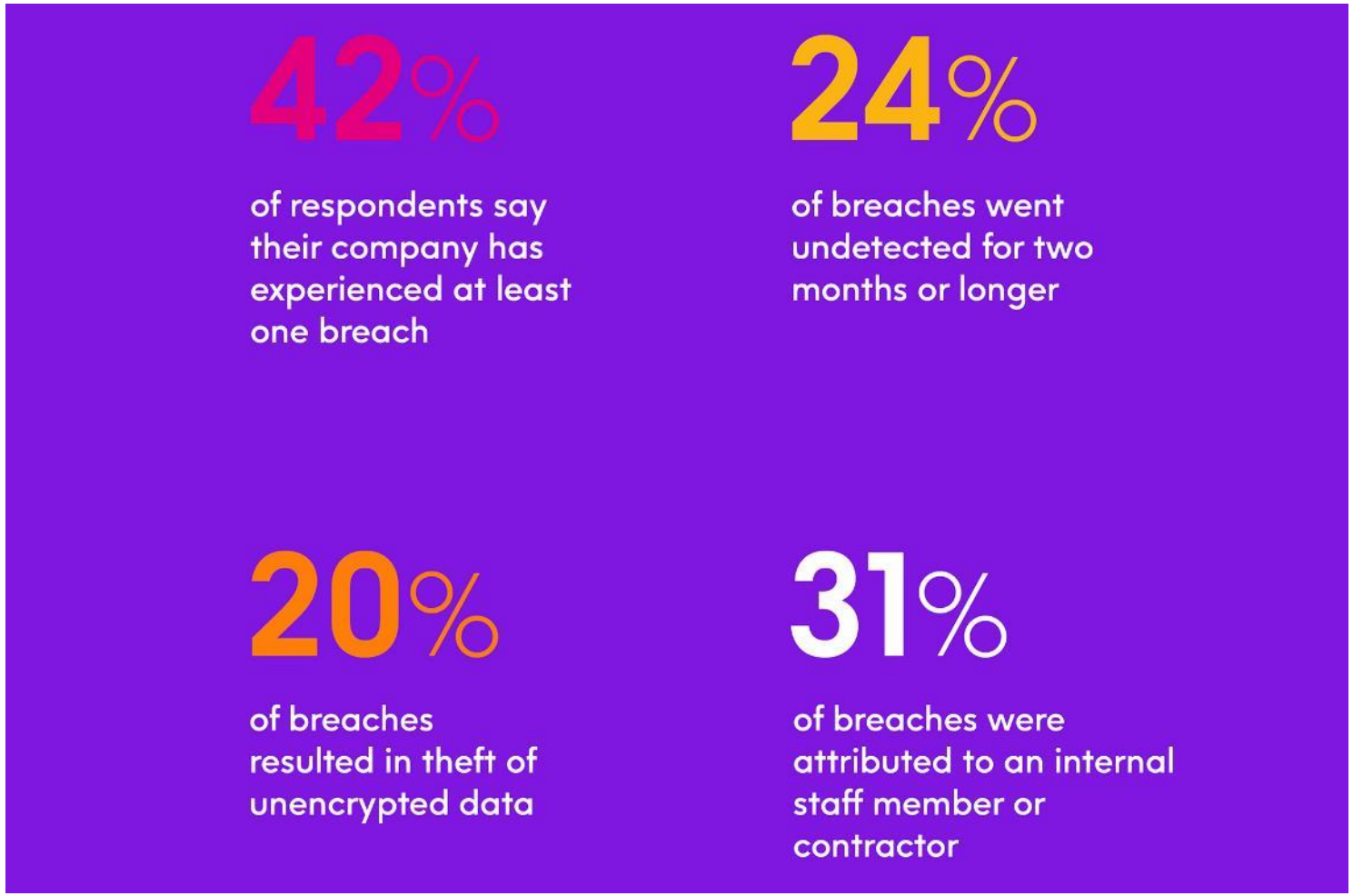
Note: Respondents were asked to "select all that apply;" therefore, figures don't total to 100%.

Types des Données présentes sur l'IBM i



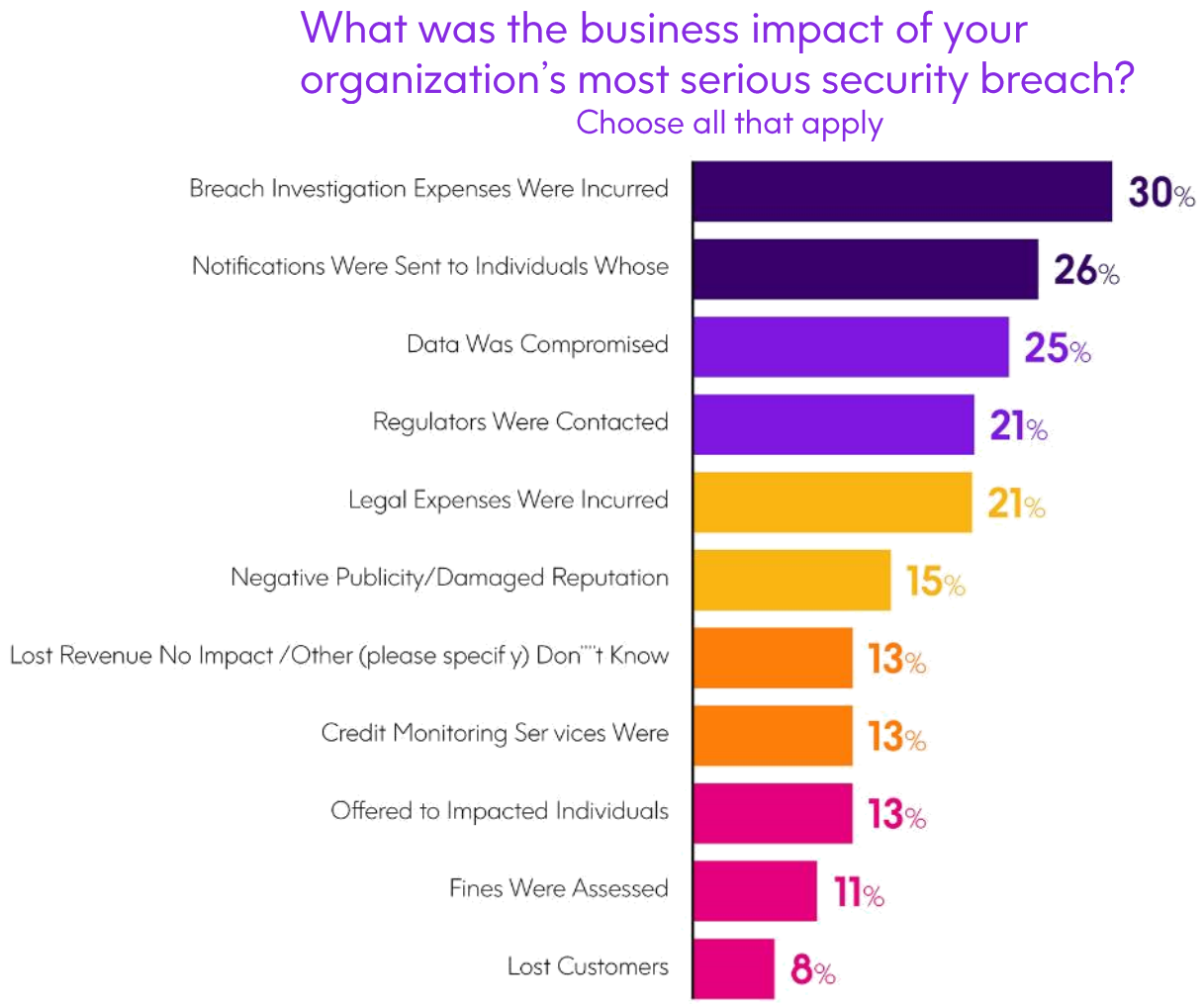
Note: Respondents were asked to "select all that apply;" therefore, figures don't total to 100%.

Les Violations de Sécurité en Chiffres



Les Impacts des Violations de Sécurité

- Rechercher l'étendue d'une violation est onéreux
- Il faut prévenir les personnes impactées ainsi que les autorités de réglementation
- Cela compromet l'image de marque



Note: Respondents were asked to "select all that apply;" therefore, figures don't total to 100%.

Vos préoccupations en 2021

Aujourd'hui le scope s'est élargi à d'autres préoccupations que la conformité à la réglementation.

Trois problématiques se détachent

1. Détecter une menace (intrusion)
   Solution: Assure SIEM integration
2. Se défendre contre le vol d'un mot passe
   Solution: Assure MFA
3. Monitorer et Contrôler les accès des utilisateurs privilégiés
   Solution: Assure EAM

Les axes de sécurité 2021

Détecter une menace (Intrusion) c'est tout l'enjeu du SIEM

Qu'est-ce qu'un SIEM et pourquoi devrait-on intégrer l'IBM i avec ?

- Security information et event management (SIEM) consolide l'information provenant de différentes sources .. Dont l'IBM i.

- Les SIEMs permettent une analyse en temps réel des alertes de sécurité générées par les applications et le matériel réseau

- Détecter très tôt une menace (intrusion), c'est la clé !

- Occulter l'IBM i de cette collecte d'événements, c'est omettre des alertes qui ne seront pas analysées.

Solution: Assure Security SIEM Integration

Les bénéfices de l'Intégration d'Assure Security dans un SIEM :

- Très facile à configurer de manière à ce que les SIEMs ne soient pas submergés d'informations

- Fonctionne avec la plupart des SIEMs comme QRadar, Splunk etc.

Se défendre contre le vol d'un mot de passe

Pourquoi se défendre contre le vol d'un mot de passe?

- Des méthodes telles que le phishing permettent de récupérer des logins et mot de passe pour pirater des comptes et accéder à votre système d'information.
- Ajouter l'authentification multi-facteurs à la combinaison login/mot de passe c'est accroître sa sécurité.
- Les applications mobiles l'utilisent, les données de l'IBM i sont-elles moins précieuses?
- Solution: Assure Security MFA

Les bénéfices d'Assure Multi-Factor Authentication (MFA)

- Fonctionne avec de multiples acteurs– Okta, RSA, Duo, etc
- Supporte différents protocoles: Telnet, FTP et ODBC

Monitorer et contrôler les accès des utilisateurs privilégiés

Pourquoi les entreprises doivent surveiller les accès des utilisateurs privilégiés?

- Il s'agit des administrateurs du système et des programmeurs par exemple.

- Les auditeurs requièrent un process pour monitorer et contrôler les accès des utilisateurs privilégiés.
- Idéalement, ces droits seront alloués pour une période donnée, automatiquement et manière auditable.

- Solution: Assure Security Elevated Authority Manager

Les bénéfices d'Assure Elevated Authority Manager (EAM):

- Des traces et des alertes personnalisables
- Supporte Telnet, FTP, SSH, ODBC

Architecture et Fonctionnalités

Assure Security

Le meilleur de la suite de sécurité Precisely

Assure Security contient

- Le meilleur des capacités de sécurisation de l'IBM i acquises de Cilasoft et Townsend Security
- Un même package pour les nouvelles installations et les mises à jour
- Une interface disponible en Français, Anglais ou Espagnol

Pour les clients Cilasoft et Townsend, Assure Security

- Est leur prochaine mise à jour
- Prend en charge de manière transparente les capacités actuelles (ou plus)
- Facilite l'adoption de nouvelles capacités de sécurisation

Assure Security

c'est la réponse aux problèmes des administrateurs et responsables de sécurité IBM i

Compliance Monitoring

Avoir de la visibilité sur toute l'activité de votre IBM i et optionnellement envoyer les événements vers un SIEM

Access Control

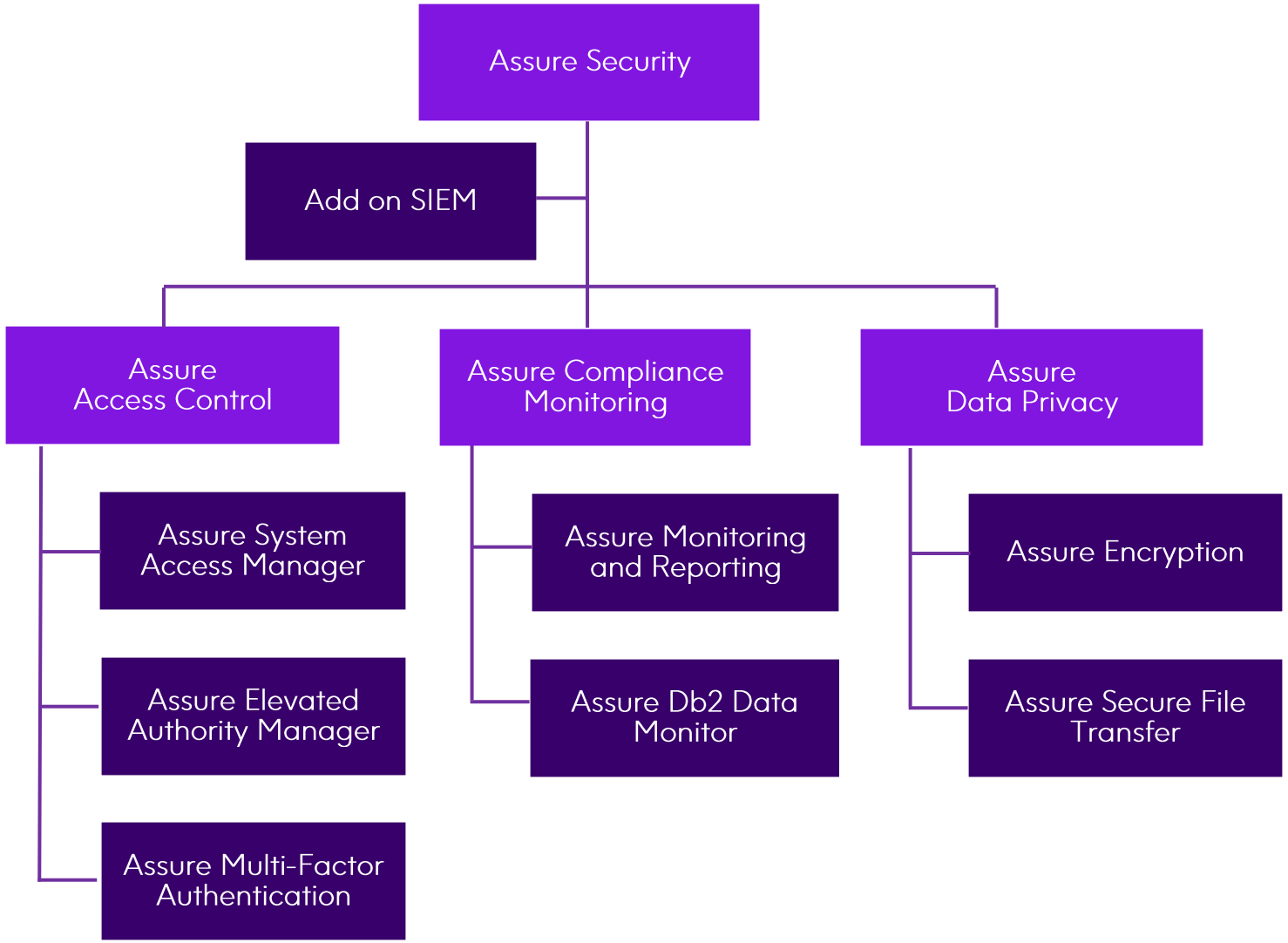
Assurer le contrôle des accès et pouvoir tracer toute activité, suspicieuse ou non

Data Privacy

La protection des données au repos et en mouvement

Security Risk Assessment

Evaluer vos risques et vulnérabilités



Choisissez le produit complet

Choisissez un bundle de fonctionnalités

Ou une fonctionnalité en particulier

Assure Security
Détail des Fonctionnalités

Assure Access Control

System Access Manager

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.

Multi-Factor Authentication

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

Elevated Authority Management

Augmentez automatiquement les droits de l'utilisateur selon les besoins et de façon limitée.

Assure System Access Manager

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, 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 aide à la conformité réglementaire

- Supporte les exigences réglementaires pour SOX, RGPD, PCI-DSS, HIPAA, et autres.
- Satisfait les responsables de la 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 Elevated Authority Manager

Contrôle complet et automatisé des élévations d'autorités

- Les administrateurs peuvent accorder manuellement des droits aux utilisateurs, ou des règles peuvent être configurées pour les gérer automatiquement
- Des règles peuvent être définies pour les profils 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 et la date, le nom du travail, l'adresse IP, etc.
- Les méthodes *SWAP ou *ADOPT sont utilisées pour élever l'autorité
- Gère les processus se connectant via ODBC, JDBC, DRDA et FTP

Surveillance complète des profils élevés

- Surveille les utilisateurs élevés et la durée de l'élévation à partir de l'interface graphique ou des écrans 5250
- Tient à jour une piste d'audit de l'activité élevée à l'aide des jobs logs, des captures d'écran, des exit points 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

Contribue à la conformité réglementaire et aux meilleures pratiques en matière de sécurité

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

Assure Multi-Factor Authentication

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 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
  - Precisely authenticator (gratuit)
  - Serveurs basés sur RADIUS
  - RSA SecurID (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

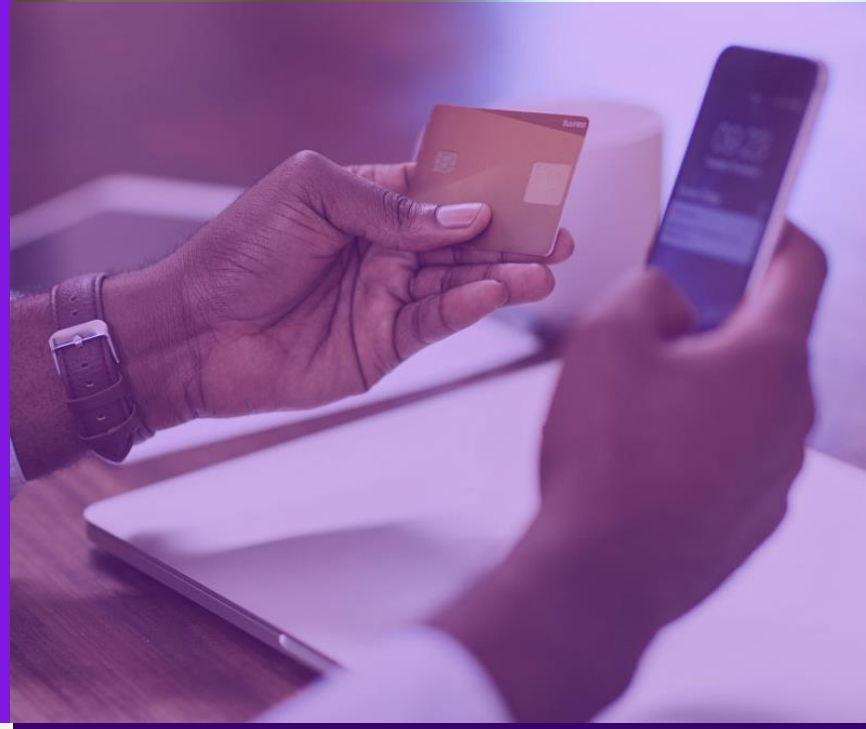
Renforce la sécurité des connexions et aide à la conformité

- 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 Data Privacy

Chiffrement

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



Transfert de fichier sécurisé

Transfert sécurisé de fichiers sur des réseaux internes ou externes à l'aide de chiffrement

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.

Assure Encryption

La seule solution certifiée NIST pour le chiffrement IBM i

- Chiffrement automatique des données Db2 à l'aide des Field Procedures IBM i (IBM i 7.1 ou supérieur)
- Les algorithmes de chiffrement AES sont optimisés pour la performance
- Masquage intégré des données déchiffrées en fonction de l'utilisateur ou du groupe
- Audit d'accès aux données intégré
- Inclut des commandes de chiffrement pour SAVF, IFS, et bien plus encore
- APIs 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
- Assurer 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

Contribue à la conformité réglementaire et aux 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 grâce à la validation du NIST

Assure Secure File Transfer

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
- Gère 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

- Empêche 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 fonctionnent avec toutes les autres solutions PGP

Assure Compliance Monitoring

System & Database Auditing

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

Db2 Data Monitoring

Surveillez les vues des données sensibles Db2 et bloquez la consultation des données

SIEM Integration

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

Assure Monitoring and Reporting

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

- Simplifie le processus complexe d'analyse des journaux
- Surveillance des modifications apportées au système et à la base de données disponibles 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 RGPD
- 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 Precisely.

Permet la conformité réglementaire et les meilleures pratiques en matière de 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 RGPD, SOX, PCI DSS, HIPAA et autres
- Satisfait aux exigences d'une piste d'audit basée sur un journal.
- Assure une véritable séparation des tâches et respecte l'indépendance des auditeurs.

Assure Db2 Data Monitor

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 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

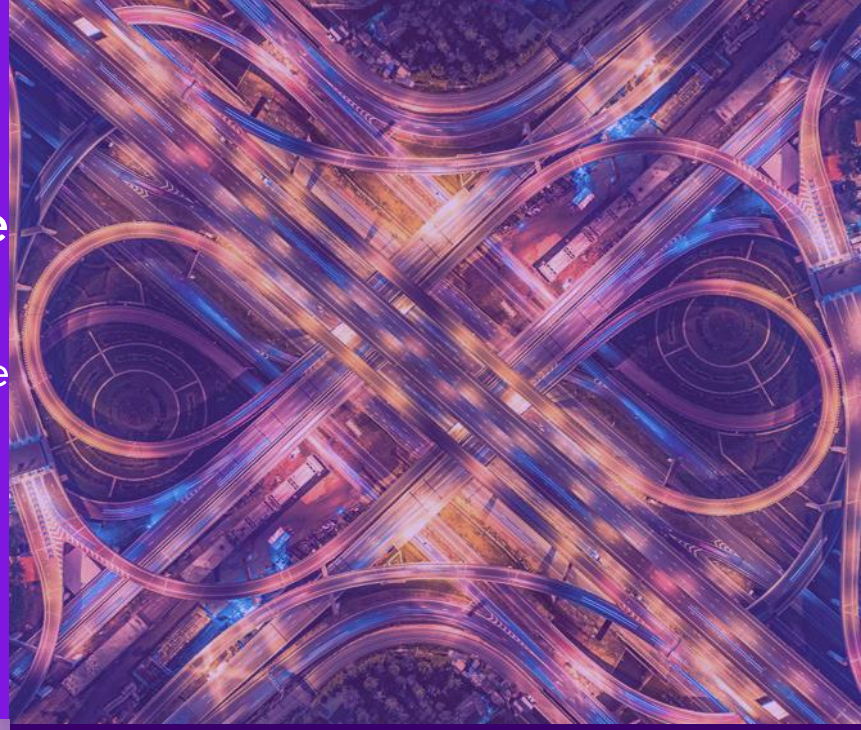
Répond aux exigences les plus strictes en matière de conformité et de sécurité

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

Risk Assessment

Outil d'évaluation des risques de sécurité

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



Security Risk Assessment Service

Laissez l'équipe d'experts en sécurité Precisely ou nos partenaires effectuer une évaluation approfondie des risques et fournir un rapport avec des conseils de remédiation

Security Risk Assessment

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 exécutif de l'évaluation 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

Les Avantages d’Assure Security

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

Supporte la conformité avec:

RGPD
PCI-DSS
SOX
HIPAA
GLBA
HITECH
23 NYCRR 500
CCPA

Et plus encore

Q&R

precisely

Merci!

precisely

frabuel@precisely.com
aurelie.godec@precisely.com