Evidian

Réduire les risques opérationnels des services financiers

Trusted partner for your **Digital Journey**

Contrôler les risques opérationnels grâce au management des identités et des accès

Réduire les risques opérationnels

Dans le secteur financier, la protection des données constitue un véritable enjeu stratégique. Les risques opérationnels ont pris une importance considérable dans un contexte né de la dérégulation, de l'imbrication des acteurs, du volume croissant des capitaux manipulés et de la sophistication des produits financiers.

En rationalisant les accès aux données sensibles et en gérant de manière structurée et cohérente les accès et les identités, les entreprises bancaires et financières peuvent réduire fondamentalement leur exposition aux risques opérationnels.

Dans un contexte sensible, la gestion des procédures de sécurité d'accès aux applications doit être renforcée et simplifiée. Une gestion proactive du risque opérationnel permet un gain de productivité et une sécurité accrue sur l'ensemble de vos domaines financiers.

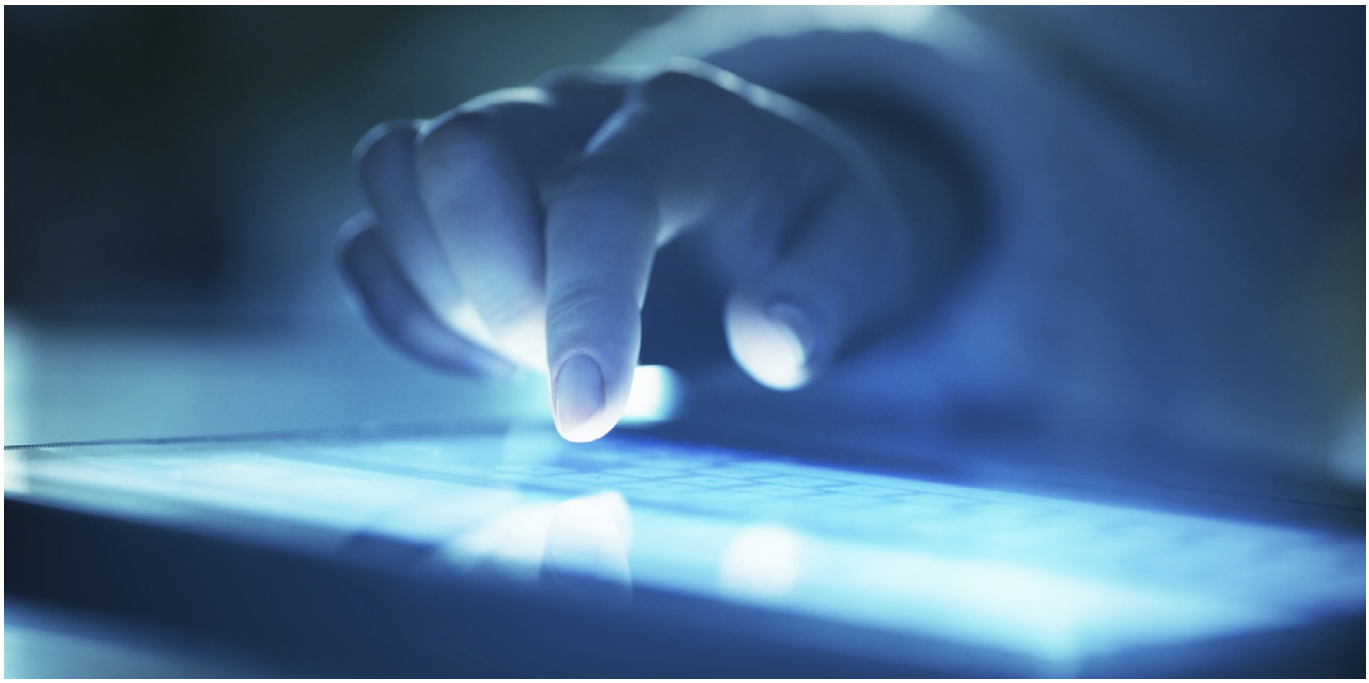
Au niveau de la législation, nous pouvons nous référer à la réglementation de la Federal Reserve's Operations and Systems Risk (Gestion des Systèmes d'Information) – Enquête de Contrôle Interne – Article 2040.4. L'accès aux systèmes automatisés est-il adéquatement protégé ?

- Les droits d'accès, mots de passe et identifiants de connexion protègent-ils les bases de données clés contre la corruption ?
- Les commandes « écrire ou éditer » sont-elles restreintes à un nombre limité d'individus ?
- Des commandes spécifiques sont-elles assignées à un groupe réduit d'individus ? Les droits d'accès sont-ils vérifiés périodiquement ?
- Le système dispose-t-il d'un rapport d'audit pour contrôler les accès des utilisateurs ?
- Les informations liées aux connexions sont-elles stockées dans les rapports pour soutenir les pistes d'audit ?

Des solutions pour diminuer vos risques opérationnels

La gestion des risques bancaires va bien au-delà des domaines classiques de risques de crédits ou risques de marché. Une grande partie des risques opérationnels concerne l'accès à des données informatiques par des personnes physiques.

L'offre modulaire Evidian Access Management facilite la gestion des risques opérationnels en structurant les identités, les rôles et les accès aux applications sensibles utilisées dans les systèmes informatiques bancaires.



Evidian, fournisseur de solutions sécurisées de gestion des identités et des accès

Evidian est le leader européen sur ce segment. Cette offre a été désignée « Leader » par les analystes de KuppingerCole.

Avec Evidian Access Management, une société bancaire et financière peut maîtriser de bout en bout sa chaîne de gestion des accès : des accès utilisateurs internes aux accès utilisateurs externes et des terminaux gérés à ceux non gérés. La solution Evidian permet de faciliter et de contrôler l'accès à l'entreprise « étendue » pour les employés, les partenaires et les clients.

Avec Evidian Identity and Access Governance, il est possible de définir et d'appliquer une politique basée sur les rôles et les modèles de risques qui sépare les tâches, assurant ainsi la confidentialité et l'intégrité des données. De cette manière, l'entité financière s'assure en permanence que seules les bonnes personnes accèdent aux bonnes ressources avec les bons droits et pour les bonnes raisons professionnelles. La solution Evidian offre la possibilité de certifier le respect des réglementations et l'implication des employés utilisant les procédures de l'entreprise.

Contrôler la fraude interne

« L'accord de Bâle III introduit les risques opérationnels dans l'évaluation des exigences minimales de fonds propres des banques ». Evidian offre une gamme complète de solutions pour une gestion optimale des risques dans les banques d'investissement et les salles de marchés, réduisant les risques opérationnels grâce à l'authentification multiple sécurisée –authentification unique– facile à vérifier et aux rapports d'accès.

Salles de marché

Les salles de marché sont inscrites dans un environnement risqué, aussi bien à travers les données et applications « sensibles » en jeu, que par les positions spéculatives prises en salle de marché. Les opérations effectuées sont étroitement surveillées et contrôlées en back office. Mais comment s'assurer de l'identité réelle de ceux qui effectuent ces opérations ?

Le travail des traders constitue un véritable enjeu stratégique pour une banque. Leur rôle clé dans la salle des marchés nécessite une attention constante et une bonne gestion du stress. Leur activité est maîtrisée, pilotée et contrôlée de façon précise. Pourtant, le contrôle des identités est souvent un maillon faible car la multiplication de périphériques d'identification diminuerait la productivité des traders.

Dans les salles de marchés, les bureaux des traders sont caractérisés par la nécessité d'utiliser des « grappes » de stations de travail avec plusieurs écrans leur permettant d'accéder aux applications disponibles localement ou dans le cloud.

Le partage des accès aux applications (les comptes) et aux postes de travail est un comportement courant chez les traders mais il introduit plusieurs risques opérationnels. Les principaux risques opérationnels sont :

- Des mots de passe divulgués entre employés, le libre accès aux sessions de l'utilisateur (bureaux, postes de travail, applications accessibles sans aucune possibilité d'identifier la personne ni de restreindre les privilèges), l'absence de systèmes « préventifs » malgré leur importance capitale pour la gestion des risques.
- Des accès fragilisés par des mots de passe trop faibles : même s'ils sont changés régulièrement, beaucoup de traders dans les banques utilisent encore #Password1 pour se connecter à leurs applications les plus utilisées, et choisir #Password2 ne changera rien à ce risque.
- Une traçabilité insuffisante des accès utilisateurs aux postes de travail, applications et comptes : les outils analytiques utilisent les données en ligne et les historiques pour fournir des KPIs, analysant et contrôlant les processus, et contribuant à l'optimisation des procédures et de la politique de sécurité. Une identification et une vérification personnelles permettent d'établir un audit fiable, sans risque de répudiation.

Professionnels malhonnêtes

Quelles mesures les banques ont-elles prises pour protéger les activités de la salle des marchés contre les opérations frauduleuses ?

Entre autres, les exigences de sécurité les plus courantes concernent la maîtrise des risques et de l'informatique, la ségrégation des tâches, l'examen interne, l'audit et le reporting, la certification périodique des droits, une politique et un contrôle forts, les procédures, ainsi que la supervision de la haute direction.

L'authentification multiple pour contrôler et faciliter les accès des traders

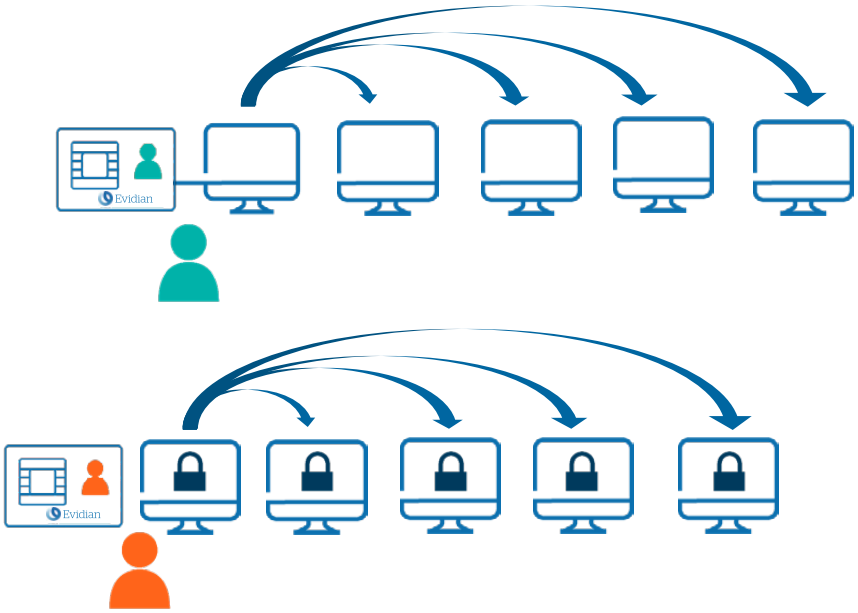
Evidian Access Management pour les salles de marchés est spécialisé dans les solutions d'authentification et de gestion des accès utilisées principalement dans les grandes institutions financières comme les banques, les bourses et les sociétés d'investissement.

Avec la solution Evidian, une seule authentification forte (carte à puce, carte de proximité, biométrie, mot de passe à usage unique, smartphone, etc.) suffit à un trader pour accéder à l'ensemble de ses moniteurs, serveurs et applications financières.

Lorsque le trader s'identifie, toute sa « grappe » d'écrans s'active et lui permet d'accéder à ses applications. Et quand il retire sa carte, ses écrans deviennent inaccessibles.

Cependant, ses applications financières peuvent toujours être surveillées par d'autres collègues grâce au verrouillage transparent.

La solution Evidian offre la même expérience utilisateur avec l'authentification biométrique, l'authentification « tap and go » avec une carte de proximité, et tout autre mode d'authentification compatible avec Windows.



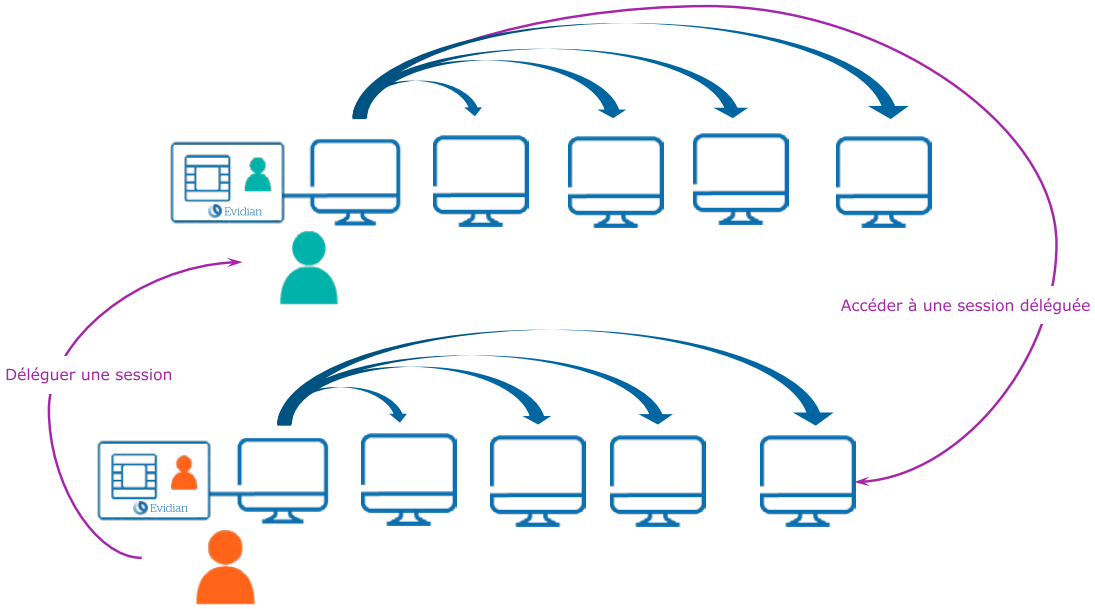
Une seule authentification par mot de passe, carte à puce, biométrie, mot de passe à usage unique, smartphone... est nécessaire pour ouvrir la session Windows. Une seule action est nécessaire pour verrouiller les sessions Windows sur tous les postes de travail.

Une solution conçue pour la productivité des traders

Evidian a élaboré ses solutions de sécurité des accès et de maîtrise des risques avec de nombreuses banques internationales d'investissement et de gestion de patrimoine. L'expérience d'Evidian lui a permis de prendre en compte les scénarios quotidiens de la vie réelle, permettant aux traders de travailler en toute sécurité, tout en augmentant leur efficacité et leur productivité avec une nette amélioration de l'expérience utilisateur.

Ainsi, le logiciel Evidian authentifie l'utilisateur et affiche son environnement applicatif.

Ce système simplifie l'organisation quotidienne du trader et permet un contrôle total de l'utilisateur et du lieu de la tentative d'accès au système et aux applications.



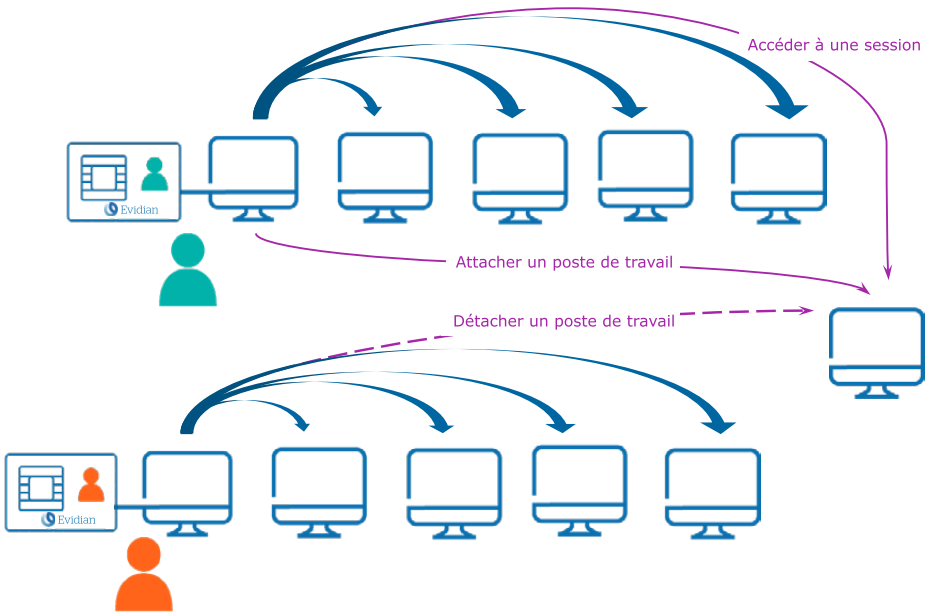
Une seule action est nécessaire pour déléguer une des sessions au sein de la grappe de PC.

De plus, un trader peut déléguer ou partager tout ou partie de sa grappe de PC avec un assistant, un collègue ou le support, sans devoir fermer puis rouvrir sa session Windows.

L'accès à la session Windows et aux applications peut être délégué, de manière permanente ou temporaire, avec des restrictions pour le(s) compte(s) de(s) l'application(s). Aussi, un trader peut détacher en toute sécurité une partie ou l'ensemble de sa grappe de PC. Un collègue peut ensuite attacher les ordinateurs disponibles à sa propre grappe de PC et ouvrir de nouvelles sessions Windows.

Tous les événements d'accès sont stockés dans une base de données, qui peut être utilisée pour vérifier les accès aux ordinateurs de la grappe et aux applications. La solution Evidian contribue à diminuer le nombre d'incidents opérationnels générateurs de pertes. Reposant sur le référentiel de Microsoft Active Directory, la solution est économique et ne nécessite pas de créer un référentiel spécifique.

La solution Evidian est basée sur une configuration standard du logiciel : vous n'avez pas besoin de développer ou modifier des applications, ni même d'introduire des composants matériels et des dispositifs dans votre domaine.



Une seule action est nécessaire pour détacher un poste de travail et permettre à un collègue d'y accéder

Services financiers en ligne et réseaux de succursales

Le nombre croissant de services financiers sur internet et de réseaux de succursales répartis sur plusieurs zones géographiques impose des contraintes en matière de gestion des accès pour les employés, partenaires et clients.

- Comment s'assurer que votre politique de sécurité est bien appliquée ?
- Comment gérer les comptes applicatifs de milliers d'employés ?
- Comment laisser les succursales gérer leurs propres utilisateurs de manière sécurisée ?
- Quelle procédure mettre en œuvre pour sécuriser et simplifier l'arrivée de nouveaux utilisateurs ?

Gérer les accès dans les agences

Le personnel des agences pense souvent que les règles de sécurité, de plus en plus exigeantes, sont contraignantes. En réponse, Evidian Access Management simplifie et rationalise la sécurité d'accès en se substituant à l'utilisateur lors de l'authentification applicative. Désormais, les employés se conforment naturellement à la politique de sécurité.

A partir d'une console centrale, les administrateurs modifient, suppriment ou ajustent les droits d'accès. Ils les attribuent en fonction du rôle des employés dans l'agence, en respectant les contraintes de séparation des tâches.

Un circuit (workflow) d'approbation intégré au provisionnement des applications automatise les autorisations et accélère la disponibilité des applications.

Les événements d'accès sont stockés de façon centralisée pour faciliter les audits.

Services en ligne sécurisés et accès mobiles

Avec Evidian Access Management, les utilisateurs accèdent en toute sécurité à l'entreprise étendue (applications locales, Cloud et SaaS), en utilisant la fédération d'identité basée sur les protocoles standards de l'industrie comme le SAML, l'OAUTH, l'OpenID Connect et l'identité sociale.

La solution permet nativement de définir des politiques d'authentification adaptatives avec des méthodes innovantes améliorant le niveau de sécurité requis pour se connecter aux services sensibles.

Les méthodes d'authentification prises en charge sont : mots de passe, certificats, cartes à puce, cartes de proximité, mots de passe à usage unique délivrés par SMS, par email ou par des applications sur smartphone, Grid card, Evidian QRentry...

Simplifier et renforcer votre politique de sécurité

Avec la suite IAM Evidian, le management des identités devient courant et systématique, ce qui rend les procédures de contrôle plus faciles à maintenir et documenter.

Lors de mouvements de personnel (embauches, mutations, départs), la suite IAM Evidian peut déclencher la création ou la suppression de comptes. Ces derniers sont attribués de telle sorte que la convergence est facilitée entre les droits d'applications et votre politique de sécurité. Les responsables des applications sont soulagés des tâches répétitives et propices aux erreurs.

La suite IAM Evidian met en œuvre des procédures critiques telles que le déprovisionnement de comptes et la séparation des tâches basée sur les rôles. Les comptes inutilisés sont détectés et si nécessaire, supprimés. De plus, l'audit centralisé vous indique précisément qui dans l'agence a utilisé un compte générique.

Lors d'un mouvement de personnel, le circuit d'approbation de la suite IAM Evidian informe par email la hiérarchie. Les responsables peuvent ensuite approuver ou rejeter l'attribution des nouveaux droits en seulement quelques clics. Une fois que le responsable a approuvé la demande, le compte est activé automatiquement pour la période requise.

La solution Evidian permet à l'entreprise d'avoir des utilisateurs finaux, des responsables opérationnels et des agents de sécurité responsables des processus de gestion des identités et des droits d'utilisation.

L'efficacité de la politique de sécurité est mesurable à tout moment, par exemple en déterminant les applications réellement utilisées par un profil d'employés. Par conséquent, vous pouvez régulièrement optimiser vos procédures de sécurité.

Déléguer aux agences et partenaires la gestion de leurs utilisateurs de manière sécurisée

Ouvrir les services financiers en ligne aux agences et partenaires implique de gérer les utilisateurs et leurs droits dans les organisations qui pourront accéder aux services. La suite IAM Evidian vous permet de déléguer cette gestion, de manière sécurisée, aux personnes adéquates dans chaque organisation.

En mettant en œuvre une politique sécurisée de gestion des utilisateurs, chaque requête devra être validée par le correspondant identifié dans chaque organisation et, une fois définie, validée aussi par un responsable central.

Avec cette procédure, la gestion des utilisateurs dans les agences et chez les partenaires peut être déléguée au responsable le plus proche sans prendre aucun risque.

Faciliter l'arrivée de nouveaux utilisateurs de manière sécurisée

Afin de simplifier l'arrivée prévue de nouveaux employés ou utilisateurs dans les agences ou chez les partenaires, les comptes peuvent être créés à l'avance en mode désactivé. A la date prévue d'arrivée, ou même parfois avant, le processus d'activation proposé par la suite IAM Evidian informera cette personne qu'elle doit activer son compte via un lien temporaire envoyé par email. En cliquant sur ce lien, l'utilisateur peut définir son mot de passe pour accéder au système, ce qui active également son compte et ses applications. L'utilisateur est prêt à travailler.

Bien sûr, ce mot de passe doit respecter un format défini par l'entreprise. Par ailleurs, ce processus peut aussi être associé à l'activation d'un dispositif d'authentification forte, auparavant donné à l'utilisateur.

Evidian

Basé sur près de 20 ans d'expérience, Evidian est l'offre de gestion des identités et des accès (IAM) d'Atos.

Plus de 5.000.000 d'utilisateurs actifs se connectent quotidiennement à leurs applications métiers en utilisant une solution logicielle Evidian. Evidian est la solution de gestion des identités et des accès de douzaines de banques et assurances aux Etats-Unis, en Europe, Afrique, Asie et Moyen-Orient. Ces entreprises respectent ainsi leurs exigences légales de confidentialité et d'intégrité, rendent leurs employés efficaces et autonomes et améliorent le service aux clients.

Brochure

À propos d'Evidian

Evidian est la suite logicielle de gestion des identités et des accès (IAM), d'Eviden.

Evidian IAM est le leader européen des logiciels de gestion des identités et des accès, avec une présence en pleine croissance en dehors du continent européen et notamment aux Etats-Unis et au Japon.

Plus de 5.000.000 d'utilisateurs dans plus de 900 organisations dans le monde entier se connectent tous les jours à leur entreprise et gèrent leurs droits d'accès avec les solutions de gestion des identités et des accès d'Evidian.

Plus d'information : **evidian.com**

CT_191021_LPM_Evidian_BR_Finance_Banking_fr