Intellinx
Insider Threat Intelligence

Soyez proactif,
gérez les menaces internes

Une révolution dans la détection et la prévention des menaces internes

De récentes enquêtes ont montré qu'environ deux tiers des cas de fraude et d'usurpation d'identité sont commis par des employés des sociétés et d'autres éléments internes. Le rapport 2006 de l'Association of Certified Fraud Examiners estime que les sociétés américaines perdent, en moyenne, 5 % de leurs revenus annuels en fraude interne. Face à ce phénomène, les sociétés, dans le monde entier, s'efforcent de trouver des solutions aux menaces internes qui vont au-delà de la simple protection de leurs installations.

Intellinx présente un système de surveillance multi-plateforme, unique en son genre, pour une visibilité inégalée de l'activité de l'utilisateur final sur les applications d'entreprise.

Soyez proactif, gérez les menaces internes

La solution Intellinx fournit une infrastructure stratégique permettant de lutter contre les fraudes internes et les fuites d'information et de répondre, de façon proactive, aux menaces internes, au lieu de réagir a posteriori. Grâce à un système complet d'enregistrement, de surveillance et d'analyse des activités autorisées de l'utilisateur sur toutes les plateformes principales existantes, les responsables de la sécurité informatique peuvent agir sur des comportements suspects lorsqu'ils se produisent et utiliser les renseignements recueillis pour anticiper les futures fraudes.

1 Tenir les utilisateurs responsables

Intellinx permet une visibilité complète de l'activité de l'utilisateur final grâce à la reconstitution visuelle de chaque écran, de chaque frappe sur clavier et de tout flux d'écrans sur chacune des applications des principales plateformes existantes. Intellinx permet aux responsables de la sécurité informatique de savoir qui a fait quoi, quand et où. L'activité de tous les utilisateurs finaux, des utilisateurs standard, ainsi que du personnel IT, est enregistrée, quel que soit leur niveau d'autorisation.

2 Enquêter sur les comportements suspects

Intellinx capture une piste d'audit très détaillée de l'activité de l'utilisateur avec une recherche poussée d'activités en multi-plateforme. Il vous permet de rechercher, par exemple, tous les utilisateurs qui ont eu accès à un numéro de compte donné, durant une période donnée, sur toutes les applications et toutes les plateformes de l'entreprise. Puis, vous pouvez faire un zoom sur des sessions d'utilisateur spécifiques et reconstituer, visuellement, leurs actions, écran par écran. L'enquête peut être menée en temps réel, alors que l'activité suspecte se produit, ou rétroactivement, par le biais de l'examen des données historiques enregistrées.

3 Réagir immédiatement

Intellinx génère des alertes en temps réel qui permettent le ciblage instantané d'un comportement suspect et des délais de réaction appropriés pour éviter tout dommage. Des règles configurables suivent des modèles de comportement de l'utilisateur, au niveau de l'application, et génèrent des alertes en temps réel en cas d'irrégularités. Il permet aux auditeurs de se concentrer immédiatement sur les suspects. Par exemple, une alerte sera automatiquement générée si un utilisateur final vérifie des comptes client, par nom de client, plus de cinq fois dans la même heure, alors que la moyenne est de deux fois par heure.

4 Empêcher et anticiper les fraudes futures

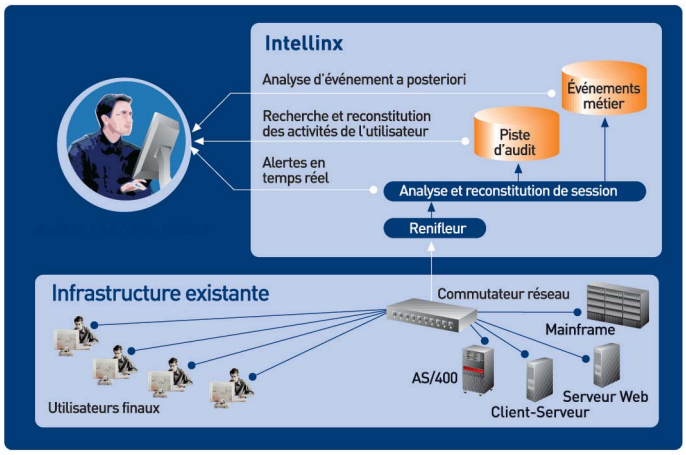
La fraude n'est pas un fait du hasard. Elle suit certains modèles comportementaux et opérationnels et les fraudeurs correspondent à des profils particuliers. Intellinx vous permet d'effectuer des analyses à posteriori du comportement des utilisateurs en appliquant de nouvelles règles à des données pre-enregistrées. De nouvelles connaissances en termes de détection des fraudes peuvent s'appliquer à des informations pré-enregistrées de l'entreprise. Combiné aux renseignements internes de l'entreprise, Intellinx peut être utilisé pour prévoir et anticiper les futures fraudes.

Valeur métier "out-of-the-box"

Intellinx propose une valeur métier prête à l'emploi d'une qualité exceptionnelle. Immédiatement après son installation (qui ne prend en général que quelques heures), Intellinx commence à effectuer des captures des activités des utilisateurs dans toute l'entreprise, permettant ainsi aux auditeurs internes d'effectuer des enquêtes approfondies grâce à une relecture complète des écrans. Les responsables de la sécurité informatique peuvent immédiatement rechercher tous les écrans d'utilisateurs sur lesquels ont été affichées certaines valeurs, durant une période donnée, sur toutes les applications et toutes les plateformes de l'entreprise. Les entreprises tirent immédiatement profit de la technologie Intellinx, sans avoir à effectuer une longue intégration à leurs systèmes ou à leurs configurations d'applications.

Implémentation à risque zéro

- La technologie en instance de brevet d'Intellinx permet d'intercepter les communications entre les utilisateurs finaux et les serveurs de l'entreprise en reniflant les transmissions réseau par le biais des commutateurs réseau. Intellinx n'affecte **donc en aucune manière les résultats des ordinateurs hôtes ou des réseaux.**
- Il n'est pas nécessaire d'installer un logiciel ou du matériel sur l'ordinateur hôte ou client.
- Intellinx suit l'activité de l'utilisateur sur toute application des principales plateformes, y compris mainframe, iSeries, Application Client/ Serveur, Web (Intranet), etc.
- Les entreprises tirent profit du processus d'installation rapide (quelques heures), sans aucun risque pour les opérations IT en cours.
- L'architecture Intellinx est souple et extensible, proposant une solution rentable aux entreprises comptant entre 500 et 100 000 employés.
- Les enregistrements sont stockés dans un format très condensé, permettant la surveillance de dizaines de milliers d'utilisateurs finaux à l'intérieur d'une entreprise sans qu'il n'y ait d'effet notable sur l'espace disque.
- Les fichiers d'enregistrement sont chiffrés et comportent une signature numérique, les rendant ainsi potentiellement recevables auprès des tribunaux.



La différence Intellinx

- **Visibilité inégalée de l'activité de l'utilisateur final** – Visibilité complète de l'activité de l'utilisateur final grâce à la reconstitution visuelle de chaque écran, de chaque frappe sur clavier et de tout flux d'écrans sur chacune des applications des principales plateformes existantes. Toute action est visible, y compris les mises à jour et les actions en lecture seule.
- **Piste d'audit complète** - Intellinx enregistre toutes les activités des utilisateurs, 24 heures sur 24, 7 jours sur 7, et non pas uniquement les événements suspects en temps réel. Cela est essentiel pour rendre les utilisateurs responsables de leurs actes. Que des règles appropriées soient en place ou non au moment d'un événement, la relecture post-événement permettra, ultérieurement, une enquête judiciaire.
- **Recherche sur multi-plateforme y compris sur système patrimonial** - Intellinx propose une solution unique de suivi de l'activité de l'utilisateur sur toutes les plateformes principales existantes, y compris sur les systèmes patrimoniaux. Il vous permet de rechercher une valeur donnée affichée sur un écran d'utilisateur multi-plateforme à partir d'un simple écran de recherche. Les règles Intellinx suivent les processus métier multi-plateforme. Par exemple, un processus métier suivi par Intellinx peut commencer sur un mainframe, continuer sur une application client-serveur et finir sur le Web.
- **Suivi du comportement de l'utilisateur au niveau de l'application** - Intellinx est la seule solution du marché qui analyse l'activité de l'utilisateur au niveau de l'application (et non au niveau du réseau). Les règles d'Intellinx suivent toutes les frappes sur clavier et le flux d'écrans auxquels a accédé l'utilisateur, en détectant le processus métier approprié, y compris chaque valeur de champ atteinte ou mise à jour. Ces informations sont reliées, en temps réel, à l'activité d'autres utilisateurs finaux, à d'autres activités et à d'autres types d'informations.

A propos d'Intellinx

Intellinx Ltd. a été créée par Sabratec Ltd., leader des solutions d'intégration de systèmes patrimoniaux, fondée en 1997. En 2003, Sabratec a commencé à développer la technologie Intellinx, perfectionnant ses vastes connaissances des technologies d'intégration et répondant ainsi à la demande croissante de ses clients pour un système de protection de leur actif informationnel contre le danger des menaces internes. A la suite de l'acquisition de Sabratec Ltd. par Software AG, en janvier 2005, la division Intellinx, qui ne faisait pas partie de l'acquisition, a été recréée en société indépendante, Intellinx Limited. Le centre de Recherche et développement d'Intellinx se trouve en Israël. Dans sa filiale de New York, sont installés les services du marketing et de l'assistance technique pour la région Amérique du Nord. Intellinx est reconnu par les plus grands cabinets d'analyse tels que Gartner et IDC, comme une technologie novatrice, chef de file dans le secteur des solutions de lutte contre les menaces internes. En 2006, Intellinx a été nommé « Cool vendor » par Gartner, dans 2 catégories: Sécurité et vie privée et Développement d'application.

Intellinx
Insider Threat Intelligence

Intellinx Software Inc.
156 William St.,Suite 806, New York
NY 10038, USA
Tel: 212 513 0977 Fax: 212 513 0979

Intellinx Ltd.
1c Yoni Netanyahu St. P.O.B. 1035
Or-Yehuda 60200, Israel
Tel: +972 3 538 5555 Fax: +972 3 634 9230

www.intellinx-sw.com
E-Mail: info@intellinx-sw.com