

L'impact Intellinx

Intellinx est une révolution dans la détection et la prévention des menaces internes. 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. La solution Intellinx fournit une infrastructure stratégique permettant de lutter contre les fraudes internes et les fuites d'information responsabilisant ainsi les utilisateurs autorisés. Intellinx est la seule solution du marché proposant les fonctionnalités suivantes :

- **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 et de chaque frappe sur clavier sur chacune des applications des principales plateformes. Toutes les actions sont visibles, y compris les mises à jour et les actions en lecture seule. Tous les types d'utilisateurs finaux sont suivis, y compris les utilisateurs finaux privilégiés tels que les administrateurs système et les administrateurs de base de données qui peuvent exposer leur société à des risques majeurs puisqu'ils disposent d'un niveau de permission plus élevé.
- **Piste d'audit complète** - Intellinx enregistre toutes les activités des utilisateurs, 24 heures sur 24, 7 jours sur 7, et non uniquement les événements suspects en temps réel. Cela est essentiel pour responsabiliser les utilisateurs. 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.

Valeur métier unique

Les fonctionnalités décrites ci-dessus permettent aux principales banques dans le monde de réaliser le caractère unique de la valeur métier d'Intellinx.

- **Protéger la marque** et la valeur marché contre les dommages causés par la mauvaise publicité qu'entraînent les cas de fuite d'information et d'usurpation d'identité.
- **Réduire les pertes liées aux fraudes internes** en décelant les fraudes et autre activité malveillante en temps réel. Dans son rapport 2006, l'Association américaine Certified Fraud Examiners estime que les sociétés américaines perdent, en moyenne, 5 % de leurs revenus annuels en fraude interne, commises, pour la plupart, par des employés des sociétés eux-mêmes. Economiser ne serait-ce qu'une partie des pertes dues à ces fraudes grâce à Intellinx, justifie l'investissement lié à l'implémentation d'Intellinx.
- **Réduire le risque opérationnel** en réponse à Bâle 2.
- **Décourager les utilisateurs frauduleux potentiels** juste en les informant que leurs actions sont enregistrées.
- **Renforcer l'efficacité de l'audit interne** en lançant une alerte à la détection d'un comportement suspect et en procurant une visibilité complète aux auditeurs internes de toutes les actions de chaque utilisateur final suspect donné, comme s'ils regardaient par-dessus son épaule.
- **Faire valoir les consignes de sécurité d'entreprise** en diagnostiquant les brèches de sécurité et les exceptions.
- **Améliorer la mise en conformité aux réglementations sur la confidentialité** en créant une piste d'audit complète de toute l'activité de l'utilisateur final, y compris des requêtes qui normalement ne laissent aucune trace dans la plupart des systèmes.

La technologie

La technologie en instance de brevet d'Intellinx propose une infrastructure adaptée à l'entreprise, dotée d'une architecture extensible qui permet une implémentation rentable pour les entreprises de plus de 500 utilisateurs finaux comme pour les entreprises comptant des dizaines de milliers d'utilisateurs finaux.

- **Technologie non invasive, sans risque.** Fondée sur un logiciel de reniflage non invasif et sans agent, la solution Intellinx n'entraîne ni changement dans l'infrastructure de l'entreprise, ni risque, ni temps inactif et ni détérioration des serveurs, réseau ou client.
- **Algorithmes intelligents.** Intellinx intercepte le trafic du réseau de dizaines de milliers d'utilisateurs finaux et reconstitue leurs actions, écran par écran, touche par touche, en temps réel. Les paquets de données brutes, circulant sur les réseaux à une vitesse de millions par seconde, sont analysés par des algorithmes intelligents qui filtrent les paquets du protocole requis provenant du serveur surveillé. Le système gère, en temps réel, des sessions miroir de tous les utilisateurs actifs de l'entreprise. Chaque nouveau paquet est identifié et associé à sa session d'utilisateur miroir, ajoutant ainsi des données incrémentielles pour la reconstitution des écrans et des frappes de touche de l'utilisateur, à l'intérieur du contexte de la session. Le système peut dépendre de différents types d'architectures réseau et gérer des cas dans lesquels les paquets d'un seul écran utilisateur sont transmis à partir d'un serveur sur plusieurs commutateurs réseau différents. Dans d'autres cas, différents serveurs avec répartition de charge transmettront des paquets du même écran.
- **Peu d'espace disque nécessaire.** Bien qu'Intellinx propose une relecture d'écran visuelle des activités de milliers d'utilisateurs finaux capturées en continu, 24 heures sur 24, 7 jours sur 7, l'espace disque nécessaire est relativement petit. Cela est possible grâce au fait qu'Intellinx ne stocke pas d'images d'écran mais plutôt des données brutes de réseau interceptées uniquement, à partir desquelles les algorithmes en instance de brevet reconstituent les écrans et les frappes de touche des utilisateurs, si nécessaire.
- **Architecture extensible.** L'architecture Intellinx est composée de différents serveurs de logiciel : Repository, Sensor, Data Channel Analyzer, Backlog Writer, Action Server, Backlog Viewer et Rule Engine. Tous les serveurs peuvent être exécutés physiquement sur la même machine ou chaque serveur peut être exécuté sur une machine différente, au même endroit ou répartis dans des différents endroits, suivant la taille et la structure de la société. Chaque serveur peut avoir une ou plusieurs instances. Par exemple, plusieurs capteurs peuvent être implémentés ; chaque capteur peut dépendre de plusieurs commutateurs réseau. Plusieurs serveurs Data Channel Analyzer peuvent être utilisés, chacun surveillant un protocole différent, à partir d'un commutateur différent, etc. Les serveurs communiquent par le biais de files d'attente pouvant être implémentées de différentes façons.
- **Piste d'audit fiable.** Essentielle pour capturer un trafic de réseau en temps réel, l'architecture Intellinx est conçue pour être d'une grande fiabilité. Le serveur Sensor effectue uniquement le traitement minimal de capture et de filtrage des paquets du réseau, les plaçant dans une file d'attente pour qu'ils soient analysés par le Data Channel Analyzer. Les différents composants du système vérifient continuellement les files d'attente et leur bon fonctionnement, afin d'assurer qu'aucune donnée ne se perde.
- **Les données enregistrées sont sécurisées.** Intellinx chiffre les données enregistrées. La communication entre les serveurs Intellinx est également chiffrée. De même, les données enregistrées comportent une signature numérique, les rendant ainsi potentiellement recevables auprès des tribunaux. L'accès aux outils d'investigation d'Intellinx est accordé uniquement aux utilisateurs autorisés et authentifiés (en général les agents de la sécurité et les enquêteurs). Chaque utilisateur est affecté de niveaux d'accès particuliers à des données spécifiques, selon les définitions de son rôle.
- **Prise en charge complète du protocole HTTP.** Intellinx prend en charge un large éventail de protocoles, notamment HTTP et HTTPS. Analyser le protocole HTTP et reconstituer les écrans d'utilisateur constituent de véritables défis car il existe de nombreuses façons d'utiliser ce protocole ainsi que de nombreuses méthodes pour bâtir des applications Web (HTML, Javascript, JSP, Servlets, .Net, ActiveX, AJAX, etc.). Intellinx gère également le protocole HTTPS et déchiffre le trafic chiffré en utilisant la même clé privée que celle utilisée par le serveur d'application.
- **Une facilité d'utilisation exceptionnelle et une valeur prête à l'emploi.** Bien que la technologie Intellinx gère des tâches très complexes, elle a été conçue pour « cacher » cette difficulté aux utilisateurs et leur fournir une valeur métier immédiate, dès l'installation. Immédiatement après l'installation (en général, quelques heures seulement), Intellinx commence à capturer les activités de l'utilisateur, permettant aux auditeurs internes d'effectuer des enquêtes approfondies avec une relecture visuelle complète et une recherche multi-plateforme. Les entreprises profitent immédiatement des avantages de la solution Intellinx qui n'exige aucune intégration, souvent prenante en termes de temps, aux systèmes de l'entreprise ni aux configurations de l'application.

En résumé, Intellinx est la seule solution sur le marché qui intercepte, de façon non invasive, des données brutes «sans signification» du réseau, reconstitue les écrans et les frappes de touche de l'utilisateur, identifie le processus métier effectué par l'utilisateur et décèle les exceptions dans les modèles comportementaux normaux.

Etude de cas

La Banque Leumi, principal groupe financier international en Israël, possédant un réseau de 250 succursales dans 19 pays, comptant plus de 1,7 millions de clients et disposant de plus de 100 milliards d'actifs sous gestion. La banque emploie plus de 10 000 employés. A la fin de l'année 2003, la Banque d'Israël décrète une nouvelle réglementation basée sur l'Accord Bâle2 qui exige, entre autre, de toutes les banques de conserver un journal très détaillé de tous les accès aux données de la banque, y compris des mises à jour et des transactions en lecture seule. La Banque Leumi avait prévu d'ajouter un petit composant d'enregistrement à chacun des milliers de programmes de l'unité centrale de manière à générer la piste d'audit nécessaire. La banque avait estimé que 100 programmeurs-mois étaient nécessaires pour accomplir cette tâche, sans compter les coûts de maintenance supplémentaires et les temps d'inactivité sur l'unité centrale. Le coût total avait été estimé à plus d'1 million de dollars. Au lieu de cela, la banque a choisi d'implémenter Intellinx. En installant Intellinx, la banque a pu aussitôt se conformer à la nouvelle réglementation, bien avant toutes les autres banques du pays, enregistrant immédiatement un ROI exceptionnel.

Remerciements aux analystes

Intellinx est rentré dans la liste des « Cool Vendors », catégorie « Sécurité et confidentialité », de l'année 2006, établie par le cabinet Gartner, Inc. Gartner définit comme « Cool vendor » une société offrant des technologies ou des solutions novatrices - permettant aux utilisateurs d'effectuer des opérations qu'ils étaient dans l'impossibilité d'effectuer auparavant - et pertinentes – ayant un impact commercial, présent ou futur, (et non uniquement une technologie au service de la technologie).