

Una rivoluzione nella prevenzione e individuazione delle frodi interne e delle fughe di informazioni

Sondaggi recenti hanno mostrato che circa i due terzi delle frodi e dei furti di identità sono commessi dagli impiegati delle aziende o da altro tipo di personale interno. Il report del 2006 dell'Association of Certified Fraud Examiners stima che le aziende statunitensi perdono una media del 5% del loro fatturato annuo a causa di frodi interne. Conseguentemente a questo, sempre più aziende al mondo stanno ponendo una maggior enfasi nella ricerca di soluzioni che offrano una protezione contro possibili minacce interne, superando al contempo il concetto di protezione perimetrale.

Intellinx offre una soluzione unica nel suo genere in grado di monitorare le molteplici piattaforme applicative presenti in azienda e permettendo al tempo stesso una visibilità totale sulle attività dell'utente nelle applicazioni corporate.

Difesa proattiva contro frodi e fughe di informazioni

La soluzione Intellinx offre una piattaforma completa per combattere le frodi interne e la fuga di informazioni, ponendosi in modo proattivo nell'individuazione nella prevenzione verso questo tipo di rischi. Grazie a un'azione completa di registrazione, monitoraggio e analisi delle attività dell'utente, i responsabili della sicurezza e gli auditor possono immediatamente intraprendere le azioni opportune riguardo a eventuali comportamenti sospetti e utilizzare successivamente i risultati raccolti per prevenire attività illecite in futuro.

1 Visibilità sulle attività dell'utente

Intellinx offre una visibilità completa sulle attività dell'utente attraverso un replay visuale di ogni schermata, con il dettaglio dei dati e dei comandi inseriti in ogni applicazione sulle piattaforme presenti in azienda. Permette agli auditor e ai responsabili della sicurezza di sapere con certezza chi ha fatto che cosa, quando e dove. Infatti l'attività di tutti gli utenti, inclusi gli utenti IT con privilegi superiori, viene registrata in un apposito database .

2 Individuazione di attività sospette

Intellinx cattura un audit trail* a livello di singolo campo, permettendo una ricerca estensiva delle attività utente su varie piattaforme (AS400, Host, Web, ecc). Individua, ad esempio, tutti gli utenti che hanno avuto accesso a un conto specifico durante un determinato periodo di tempo, attraverso ogni applicazione aziendale, qualsiasi sia la piattaforma utilizzata. Consente di visualizzare la specifica sessione utente per rivederne le azioni, schermata dopo schermata. Questa investigazione può essere condotta in tempo reale mentre l'attività sospetta è in corso o ex-post, attraverso l'esame dei dati storici registrati.

*Audit trail o audit log è una sequenza cronologica di record sottoponibili ad audit , ognuno dei quali contiene evidenze attinenti o risultanti dall'esecuzione di processi di business o funzioni di sistema.

Un valore di business immediato

Intellinx offre un valore di business immediato: appena installato inizia la cattura di tutte le attività utente , permettendo ai responsabili dei controlli di effettuare investigazioni con una visibilità completa. I responsabili della sicurezza e gli auditor possono effettuare ricerche immediatamente all'interno di ogni schermata utente in cui appare un valore specifico in un determinato lasso di tempo, per ogni applicazione utilizzata in azienda. Le aziende cominciano a beneficiare di Intellinx immediatamente, senza la necessità di costose integrazioni nei sistemi aziendali o di configurazioni personalizzate dell'applicazione.

3 Risposte immediate

Intellinx genera allarmi in tempo reale permettendo l'individuazione immediata di ogni attività sospetta e offrendo al contempo una risposta efficace per la mitigazione dei rischi.

Regole configurabili consentono di tracciare i pattern di operatività dell'utente a livello applicativo generando allarmi in tempo reale sulle irregolarità individuate. Intellinx permette agli auditor di focalizzarsi immediatamente sugli eventi anomali: ad esempio, un allarme può essere generato automaticamente se un utente effettua ricerche nominative sui conti dei clienti per più di 10 volte in un'ora, qualora la media di questa tipologia di attività dovesse essere di molto inferiore.

4 Prevenzione da frodi future

Il crimine non è casuale, segue determinati modelli comportamentali e operativi, e l'esecutore di norma corrisponde a un determinato profilo.

Intellinx permette di eseguire analisi a posteriori sui comportamenti degli utenti, applicando nuove regole a dati pre-registrati.

Nuova conoscenza sulle modalità di individuazione delle frodi può essere applicata alle informazioni già registrate dall'azienda. Con i risultati delle analisi interne, Intellinx può essere utilizzato per prevedere e prevenire future attività illecite.

Campi di applicazione ed esempi

Intellinx può portare i suoi benefici a varie tipologie di aziende. I seguenti esempi di rilevazioni non sono esaustivi, ma rappresentano alcune possibilità di implementazione di regole di controllo, suddivise per settore.

Controlli generici

- Transazioni fuori dal normale orario di lavoro
- Login da parte di un utente che non è presente in ufficio perché fuori ufficio per lavoro, malattia o ferie (collegamento di Intellinx con sistema di controllo ingressi/uscite)
- Collegamento con utenti diversi dallo stesso terminale o con lo stesso utente da terminali diversi

Banche

- Un numero eccessivo di ricerche di conti correnti per nome del cliente effettuate dallo stesso utente o postazione di lavoro
- Un numero eccessivo di accessi a conti ad alto profilo effettuati dallo stesso utente o postazione di lavoro
- Cambio dell'indirizzo di un cliente e ripristino del vecchio indirizzo dopo un breve lasso di tempo
- Aggiunta dello stesso indirizzo a conti correnti differenti da parte dello stesso utente o postazione di lavoro
- Aggiunta di nuovi beneficiari a un conto e ripristino della situazione precedente in seguito
- Aggiunta di un nuovo beneficiario seguito da un trasferimento di fondi da o verso lo stesso conto dallo stesso utente o postazione di lavoro
- Aggiunta degli stessi beneficiari a diversi conti da parte dello stesso utente o postazione di lavoro
- Cambiamento dei limiti di credito e ripristino della situazione precedente dopo un breve periodo di tempo

Assicurazioni

- Verifica dell'accesso ai dati personali dei clienti
- Numero eccessivo di polizze temporanee con storno successivo da parte di un agente
- Cambio del conto corrente o dell'indirizzo di un cliente e ripristino della situazione precedente dopo un certo periodo
- Definizione di indirizzi o conti correnti uguali per clienti differenti
- Aggiungere richieste di risarcimento da parte dello stesso impiegato che ha aperto la polizza
- Accesso a dati di clienti che non sono normalmente gestiti da quell'impiegato

Telecom

- Tracciare l'accesso alla lista delle chiamate dei clienti
- Tracciare l'accesso a numeri telefonici che non sono elencati nell'elenco pubblico, specialmente immediatamente dopo che un nuovo numero è stato allocato a un cliente
- Tracciamento dell'accesso alle informazioni sull'instradamento di specifici numeri di telefono

Utenti IT privilegiati in ogni area di business

- Cambiamento di dati in ambiente di produzione con strumenti di query (ad es. SQL/400, DB/2 SPUFI or QMF)
- Cambiamento di codice dei programmi in produzione
- Cambiamento di dati sensibili in ambiente di produzione utilizzando un'applicazione da un terminale del dipartimento IT e/o da parte di un utente IT
- Introdurre una nuova versione di un programma in ambiente di produzione, eseguirlo e ripristinare la versione precedente (per coprire eventuali tracce)
- Introdurre un programma in produzione, eseguirlo e cancellarlo subito dopo
- Eseguire programmi in ambiente di produzione
- Collegamento con un utente di business da un terminale del dipartimento IT dopo il normale orario di lavoro o durante i weekend
- Collegamento con utenti diversi dallo stesso terminale
- Aggiunta di nuovi campi in una tabella contenente dati sensibili

Auditing

- Le azioni dell'utente finale sono estratte e consolidate in un database di audit trail
- È possibile mantenere tabelle di audit trail dedicate a specifiche transazioni, ad esempio per gli aggiornamenti dei limiti di credito che eccedono una certa soglia

Performance e usabilità dei sistemi - Controllo dei livelli di servizio

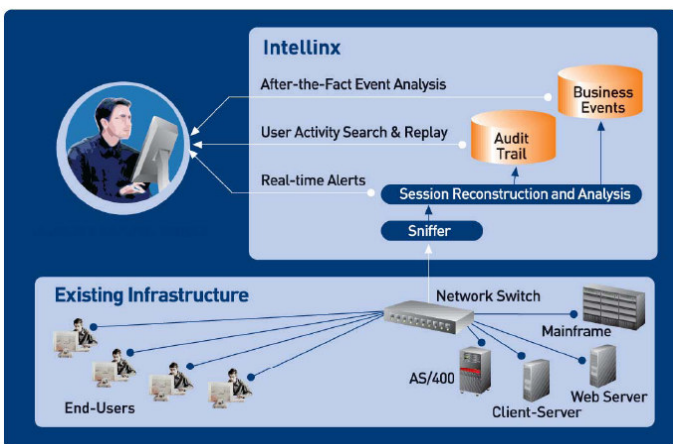
- Monitoraggio della disponibilità dei sistemi e dei tempi di risposta (ad es. Quando il tempo di risposta medio per una transazione specifica supera i 10 secondi negli ultimi 10 minuti, viene istanziato un avviso)
- Monitoraggio di errori ripetuti sulla stessa transazione per utenti diversi. Viene richiesto il supporto se il numero di utenti che ricevono un errore eccede una soglia predefinita
- Quando un utente riceve un messaggio di errore da un'applicazione, viene inviata un'email con i dettagli al team di supporto

Nuovi workflow e funzionalità

- Dipendentemente da determinate azioni dell'utente, è possibile istanziare un'azione (via MQ Series, DB o Web Service, ecc.) per lanciare un processo in un'altra applicazione
- Quando un utente effettua un acquisto di un prodotto finanziario, viene proposto automaticamente al promotore un'attività di cross-selling o up-selling

Implementazione senza rischi

- La tecnologia di Intellinx intercetta le comunicazioni tra utente finale e server corporate "ascoltando" le trasmissioni di rete attraverso gli switch collegati al server. Per questo motivo Intellinx non ha nessun tipo di impatto sulle performance di host e rete.
- Nessun bisogno di installare software o hardware su host o client.
- Intellinx traccia l'attività utente in ogni applicazione sulle maggiori piattaforme, inclusi mainframe, zSeries, AS400, Client/Server, Web ecc.
- L'azienda trae beneficio immediato dal veloce processo di installazione senza alcun rischio per la normale operatività IT.
- L'architettura di Intellinx è flessibile, scalabile e offre una soluzione *cost-effective* a qualsiasi azienda.
- Le registrazioni sono memorizzate in formato compresso, consentendo di registrare le sessioni di decine di migliaia di utenti in uno spazio disco contenuto.
- I file di registrazione sono cifrati e firmati digitalmente. Questo ne permette l'utilizzo a fini giudiziari.



Intellinx fa la differenza

- Visibilità ineguagliabile sulle attività utente – La completa visibilità sulle attività degli utenti è realizzata mediante la replica visuale di ogni schermata, di ogni input, su qualsiasi applicazione. Tutte le azioni dell'utente sono visibili, inclusi gli aggiornamenti e le azioni di sola lettura.
- Audit Trail integrale – Intellinx registra qualsiasi attività degli utenti, non solo quelle considerate sospette, in modalità 24x7. Indipendentemente dall'utilizzo di regole specifiche al momento di un evento, Intellinx permette di applicare nuove regole di controllo anche a dati precedentemente registrati.
- Ricerca su diverse piattaforme – Intellinx offre una soluzione unica per tracciare l'attività degli utenti su qualsiasi piattaforma, inclusi i sistemi legacy. Da un'unica interfaccia di interrogazione è possibile effettuare la ricerca di un dato specifico visualizzato dall'utente in una qualsiasi schermata di ogni applicazione aziendale. Le regole tracciano i processi di business indipendentemente dalla piattaforma: ad esempio, un processo di business tracciato da Intellinx può iniziare su un mainframe, continuare su un'applicazione web e terminare su un'applicazione client-server.
- Tracciamento del comportamento utente a livello applicativo – Intellinx è l'unica soluzione sul Mercato che analizza l'attività utente a livello applicativo (non a livello di rete). Le regole di Intellinx registrano tutto ciò che viene digitato o anche solo visualizzato dall'utente, dai campi utilizzati sino ai processi di business rilevanti. Queste informazioni sono correlate in tempo reale con le attività degli altri utenti, le attività precedenti e con altri tipi di informazioni presenti in azienda.

About Intellinx

Intellinx nasce come divisione di Sabratec Ltd, azienda leader nelle soluzioni di integrazione per sistemi legacy fondata nel 1977 in Israele. Nel 2001 Sabratec inizia lo sviluppo di Intellinx utilizzando la sua profonda conoscenza delle tecnologie di integrazione e con la volontà di soddisfare la crescente domanda dei suoi utenti per la protezione del patrimonio informativo dalle insidie delle minacce interne. Nel 2005 la divisione Intellinx diventa un'azienda indipendente, Intellinx Ltd.

Le principali società di analisi hanno conferito a Intellinx diversi riconoscimenti nell'area delle soluzioni per le minacce interne. Nel 2006 Gartner ha inserito Intellinx nei "cool vendor" di 2 categorie: "Security & Privacy" e "Application Development"



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



About Advanction

Advanction ha l'obiettivo di fornire soluzioni strategiche e ad alto valore, affidandosi alle sue competenze tecnologiche e di business, e attraverso prodotti e servizi innovativi. Advanction è stata selezionata da Intellinx Ltd. Come partner per la Svizzera e l'Italia.

Advanction S.A.

Svizzera

Nucleo
CH-6835 Morbio Superiore
Svizzera
Phone/Fax: +41(0)91 6825094

Italia

Largo Murani, 2
20133 Milano
Italia
Phone: +39 02 40709377

E-mail: info@advanction.com — Web: www.advanction.com