



Capturing key strokes, mouse actions and screen activities



Real Time Session Logging and event playback For key strokes, Mouse Movement and Screen updates For Microsoft Platforms

Enterprise AdminGuard™ (EAG)はシステム管理のアクティビティをキャプチャーしレビューする製品です。このユニークな製品は管理者による潜在的な誤用・悪用から複数のマイクロソフトWindowsサーバを監査し、保護します。加えてこの製品は完全な監査証跡の有用性を通じ、誤操作のリカバリーにおいても有益な手段であると言えます。

ファイル削除やデータベース更新、ハードディスクのフォーマットなどといった意図的または事故によるエラーは主要な業務を中断させ顧客の信用を失うことにもなりえます。全てのマウスクリックやキーストロークを記録して、セッションベースの監査証跡を提供することによって、EAGはシステム管理者、オペレータ、データベース管理者などサーバにアクセスするあらゆるシステムユーザの説明責任を確立します。管理者によって実行される全てのアクティビティを記録し、独立した第三者が監査証跡をレビューするバーチャルビデオレコーダとしてのこの機能は、多くの組織で必要とされる監査能力を大幅に拡張しました。

EAGのもつ3つのコンポーネントーホストレコーダ、オーディットサーバ、ログレビューア

ホストレコーダ

全てのキーストローク、マウスアクション、スクリーン更新といった活動をログインセッション毎に記録する機能です。ログファイルサイズを最小限におさえる為に更新差分だけを記録し、完全性を保障する為にログファイルを連続させて記録します。

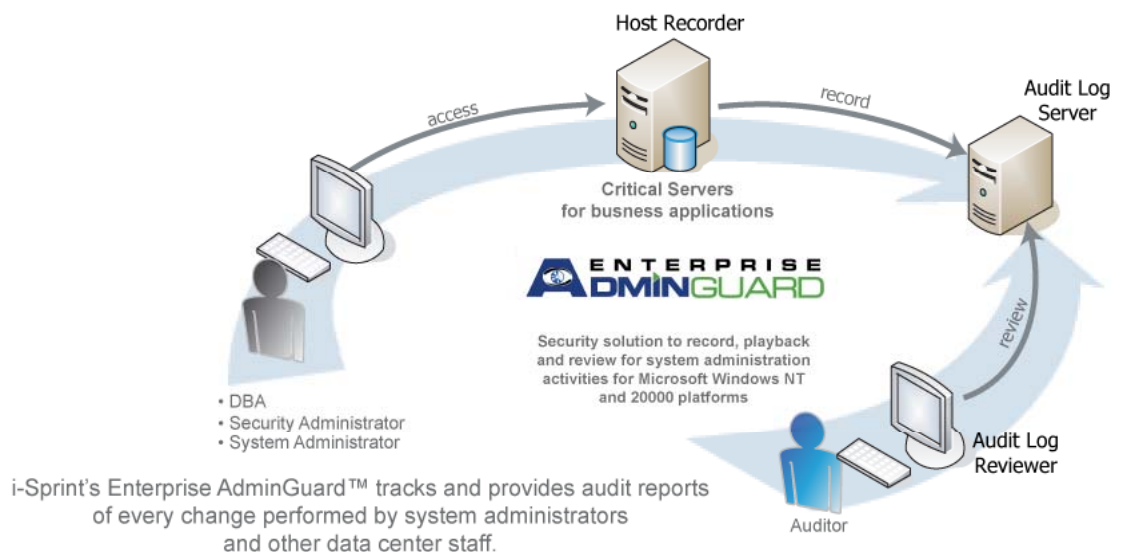
ターミナルサーバやCitrix環境へインストールする際、ホストレコーダをプロキシとして構成することによって、ユーザのアクティビティとしてバーチャルアプリケーションへのアクセスをキャプチャすることができます。

オーディットサーバ

オーディットサーバは専用マシン上で動作し、自動的にログファイルをファイリングすることによって設定管理の煩わしさを最小限に抑えます。また、オーディットログファイルの保存管理機能を有しています。

ログレビュー&オーディットログプレイヤー

ログのビデオプレイバックコントロールや複数オーディットサーバの管理、柔軟性のある検索機能などを有しています。



ホストレコーダ

機能	利点	サポートプラットフォーム
セッション毎のロギング	検索や管理を容易にする為、各ログインセッション毎に別ファイルへ記録。	<ul style="list-style-type: none"> •Windows NT 4.0 SP5 以上 •Windows 2000 SP3 以上 •Windows XP SP2 以上 •Windows 2003 SP1 以上 •Windows Terminal Services •Citrix Metaframe
キーボードエコー記録	パスワードのような機密情報漏洩を避けるため、キーボードエコーのみを記録。	
マウス動作の記録	全てのマウス動作を記録。	
スクリーン更新記録	全てのスクリーン動作を記録。	
オーディットログ最適化	画面更新差分のみを記録。	

オーディットログサーバ

機能	利点	サポートプラットフォーム
サーバの冗長性	高可用性のためのクラスタリング機能を提供。日時もしくはストレージサイズでの保存ポリシーに従ったログ記録管理。	<ul style="list-style-type: none"> •Windows NT 4.0 SP5 以上 •Windows 2000 SP2以上 •Windows 2003 SP1 以上
自動ファイリング	コンフィグレーション設定の必要なく、ファイルサーバ上にログを保存。	

オーディットログレビュー

機能	利点	サポートプラットフォーム
ツリー構造ビュー	複数のオーディットログサーバを管理。	<ul style="list-style-type: none"> •Windows NT 4.0 with SP5 以上 •Windows 2000 SP3以上 •Windows XP SP2以上 •Windows 2003 SP1 以上
閲覧記録	オーディットログの閲覧記録機能。	
プログラムリスト	閲覧者はセッション毎に実行されたプログラムやコマンドのリストを監査することが可能。	
ログファイル検索	独自の検索機能。	
VCRライクなセッションブレイヤ	パスワードのような機密情報漏洩を避けるため、キーボードエコーのみを記録。	