InTrust®

スマートでスケーラブルなイベントログ管理ツール

皆様の組織の最も貴重な資産は、データと、データへのアクセス権を持つユーザです。ITおよびセキュリティ部門にとって、特にワークステーションやエンドユーザデバイスでユーザや特権アカウントのアクティビティを追跡することは、環境を安全に保ち、各種の業界規制に準拠する上で重要です。ただし、大量のデータがさまざまなシステム、デバイス、およびアプリケーションに分散しているため、これは難しいタスクです。通常の場合、こうしたデータをすべて収集、保管、分析するには、大量のストレージ、長時間を要するイベントデータ収集、および収集したイベントデータに関する社内の専門知識が必要です。

Quest® InTrust®を使用すれば、ログオンからログオフに至るまで、その間のあらゆることを含めてすべてのユーザのワークステーションおよび管理者アクティビティを監視できます。20:1のデータ圧縮によりストレージコストを軽減し、Windows、UNIX/Linuxサーバ、データベース、アプリケーション、およびネットワークデバイスからの数年分のイベントログを保存できます。InTrustのリアルタイムアラートの生成では、疑わしいアクティビティに自動的に対応できるため、脅威に速やかに対応できます。

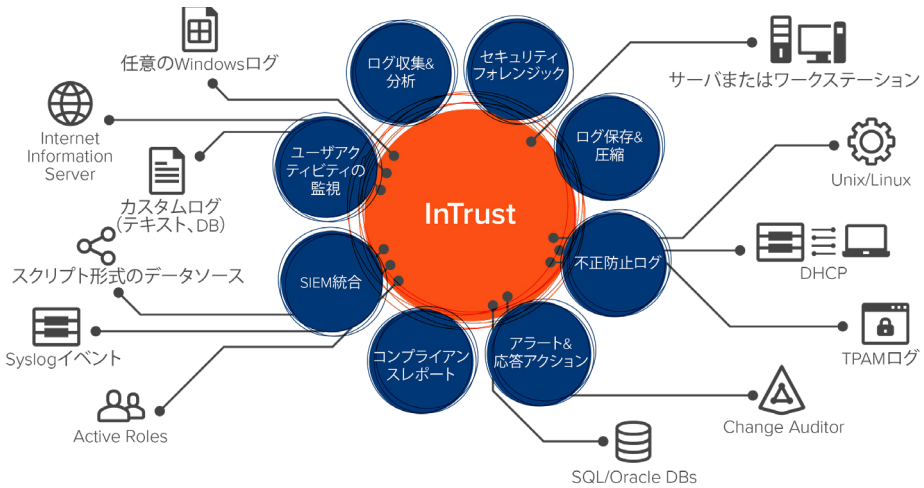
特長

一元管理機能

各種のシステム、デバイス、アプリケーションから収集したすべてのネイティブまたはサードパーティのワークステーションログを、検索可能な1つの場所に保存して、セキュリティおよびコンプライアンスレポートの作成にすぐに利用できます。InTrustは、Windowsイベントログ、UNIX/Linux、IISとWebアプリケーションのログ、PowerShell監査証跡、エンドポイント保護システム、プロキシとファイアウォール、仮想化プラットフォーム、ネットワークデバイス、カスタム・テキスト・ログ、およびQuest Change Auditorイベント。

ユーザ・ワークステーション・ログの監視

ユーザおよび管理者がログオンしてからログオフするまでに行われるすべてのアクティビティを監視して、pass-the-hash、



すべてのユーザワークステーションおよび管理者アクティビティを効率的に監視し、最も貴重な資産であるデータの安全性を確保します。

「私たちは、SOXコンプライアンス監査のためにInTrustを使ってドメインコントローラーからログを収集し、イベントを監視しています。私が気に入っているのはリポジトリビューアです。セキュリティ保護のため、アカウントのロックアウトなどのログインイベントを調査するときに大変便利です。」

エンジニア、S&P 500プロフェッショナルサービス企業

TVID: 726-084-5E5

メリット:

- インデックス付きの高圧縮ログリポジトリにより、ストレージコストの削減および継続的なコンプライアンスを確保
- すべてのエンドユーザおよび特権アカウントのアクティビティを1ヶ所から簡単に検索
- セキュリティイベントを素早くレポート、トラブルシューティング、および調査
- 標準化されたネイティブのイベントログにより、データを容易に把握
- 既存のSIEMソリューションと簡単に統合
- リアルタイムアラートおよび自動化された応答により、脅威に速やかに対応
- イベントを作成時に複製することで、イベント・ログ・データを改ざんまたは破壊から保護

「この製品は、とても貴重なセキュリティレポートとアラート機能を提供してくれると思います。他の製品にも類似の機能がありますが、InTrustは短期間で導入でき、監査とコンプライアンスの分野に即時に価値が得られると感じます。」

シニアITマネージャー、Fortune 500 自動車および輸送企業

TVID: D2B-CDB-505

システム要件

サポート対象プラットフォーム
Microsoft Windowsイベント
Microsoft IISイベント
Microsoft Forefront Threat Management GatewayおよびISA Serverイベント
Microsoft DHCP Serverイベント
Solarisイベント
Red Hat Enterprise Linuxイベント
Oracle Linuxイベント
SUSE Linuxイベント
Debian GNU/Linuxイベント
Ubuntu Linuxイベント
IBM AIXイベント
HP-UXイベント
VMware vCenterイベント
VMware ESXおよびESXiイベント
詳細については、システム要件の文書を参照してください。

フィッシング、またはランサムウェアなどの最新のサイバー攻撃からワークステーションを保護します。アクションを実行したユーザ、アクションの具体的な内容、アクションの対象となったサーバ、アクションが実行されたワークステーションなど、ユーザのアクセスに関する重要な詳細情報をすべて収集し、保存します。

簡単なイベントログ分析

多様なソースから取得した難解なイベントログを、誰が、何を、いつ、どこで、どのワークステーションからどのワークステーションに対して行ったかという標準化された単純な形式に統合することにより、データがわかりやすくなります。特に、Syslogデータはアプリケーションによって大きく異なります。InTrust®なら、Syslogイベント内の構造化データを検知して正しく解析できます。独自のフルテキストインデックス化によって長期にわたるイベントデータを簡単に検索できるようになり、迅速なレポート作成、トラブルシューティング、およびセキュリティ調査が実現します。

スマートでスケーラブルなイベントログ圧縮

大量のデータを収集して高圧縮リポジトリに保存することで（インデックス付きの場合は20:1、インデックスなしの場合は40:1）、ストレージコストを最大60 %削減し、HIPAA、SOX、PCI、FISMAなどとのコンプライアンスを継続的に確保できます。さらに、1台のInTrustサーバで、イベントログを書き込む10,000個のエージェントの場合に最大で毎秒60,000件のイベントを同時に処理できるため、効率性と拡張性が向上し、ハードウェアコストが著しく節減されます。また、さらに容量が必要な場合は、InTrustサーバをもう1台追加してワークロードを分割できます。拡張性は事実上、無制限です。

リアルタイムアラートの生成および対応アクション

しきい値制限を超えるファイル作成、既知ランサムウェアのファイル拡張子の使用、疑わしいPowerShellコマンドなどの、不正または不審なユーザアクティビティを監視します。脅威に対してリアルタイムに警告し、即座に対応します。InTrustでは、アクティビティをブロックする、不正なユーザを無効にする、変更を取り消す、緊急監査を有効にするなど、不審なイベントへの対応を自動的にトリガーすることができます。

ログの不正アクセス防止

作成されたログの複製をキャッシュする場所を各リモートサーバに作成して、イベント・ログ・データの改ざんや破壊から保護します。

SIEM統合

SIEMの年間ライセンスコストは、SplunkおよびIBM QRadar向けInTrustコネクタによって削減することができます。InTrustでは、長期のイベント・ログ・データを保存し、業界のベストプラクティスに基づいて、関連するデータのみをフィルターしてお使いのSIEMソリューションへ転送することで、リアルタイムのセキュリティ分析を行うことができます。

IT Security Searchによる状況分析の強化

すべてのQuest®セキュリティおよびコンプライアンスソリューションから得られる貴重な状況分析を1ヶ所で利用できます。IT Security Searchを使用すると、InTrust、Change Auditor、Enterprise Reporter、Recovery Manager for AD、およびActive RolesからのデータをGoogleのようなIT検索エンジンに関連付けることによって、セキュリティインシデントへの迅速な対応とフォレンジック分析を行うことができます。ユーザの資格とアクティビティ、イベントのトレンド、不審なパターンなど、さまざまなデータを豊富な可視化機能やイベントタイムラインを使用して簡単に分析できます。

ベスト・プラクティス・レポートの自動作成

調査内容を、HTML、XML、PDF、CSV、TXTだけでなく、Microsoft Word、Visio、Excel形式などの複数のレポート形式に簡単に変換できます。レポートのスケジュールを決定して、チーム間の配信を自動化するか、または事前に定義された組み込みイベントログ機能付きベスト・プラクティス・レポートの広範なライブラリから選択することができます。データのインポートおよび統合ワークフローでは、データのサブセットをSQL Serverに自動的に転送してさらに高度な分析を行うこともできます。

QUESTについて

Questは、急速に変化するエンタープライズITの世界にソフトウェアソリューションを提供しています。データの爆発、クラウドサービスへの拡張、ハイブリッド・データ・センター、セキュリティ脅威、規制上の要件によって生じる課題のシンプル化を支援します。Questのポートフォリオは、データベース管理、データ保護、統合エンドポイント管理、IDおよびアクセス管理、Microsoftプラットフォーム管理などのソリューションで構成されます。

Quest
quest.com/jp
世界各地のオフィスの情報については、
（quest.com/jp-ja/locations）をご覧ください

DataSheet-InTrust-US-KS-JA-WL-39601