Data Sheet

CryptoAuditor™

信頼したインサイダーを食い物にさせるな

SSHプロトコルを発明・開発し、1995年に設立されたSSHコミュニケーションセキュリティー社は、情報資産への経路を保護しようとする様々な業種・規模の企業・組織の負担を軽減することに焦点をあてています。CryptoAuditorは企業・組織が信頼する内部人員のデーター転送に関する操作をリアルタイムで、又管理アクセスに影響を与えずコントロールできる透過的な中央一元管理型の特権アクセス監視・監査ソリューションです。CryptoAuditorは信頼する内部人員によるセキュリティーの脅威を削減し、現在及び今後の法律・業界規制に合致し、既存のネットワーク・アーキテクチャーをそのまま、又は変更を最小限に抑えながら利用できることでコスト効率に優れる実装及び管理を行える製品です。

困難への挑戦:

管理者とは企業・組織の重要なビジネス情報全般に渡りしばしば広範なアクセス権を持つ内部の人員です。実際、これら内部人員は重要な情報資産に対し役員よりも多くのアクセス権を持っています。大多数のこれら内部人員はまさに信頼がおけるとしても、1人の悪行が重大な被害を引き起こしかねません。

管理者がそのような広範囲の情報群にアクセスでき、暗号化して情報を送信できるということは、本質的にセキュリティー及びフォレンジックチームの活動を盲目にし、信頼した内部人員による脅威がステルスとなるということがまさに現実になっています。

さらに、適切な管理者の監査・監視機能が無い場合は、その企業・組織は内部及び外部の法律・業界規制に準拠していないということになり、罰金やその他の責務に対し無防備なままであるということにもなります。

ソリューション:

CryptoAuditorは既存のシステムに大きな変更を加えずに、法律・業界規制に準拠し、さらにその上の基準の達成を助け、内部の人員の脅威に関する潜在的な問題を解決するするソリューションです。過去においては、悪意あるユーザーは暗号化した通信を利用する事でその活動に対する監視の目から逃れてきました。CryptoAuditorはSSH、SFTP及びRDPの通信をリアルタイムで復号化し管理者の操作に影響を与えずにこれを記録します。

CryptoAuditorでのセキュリティー投資回収率

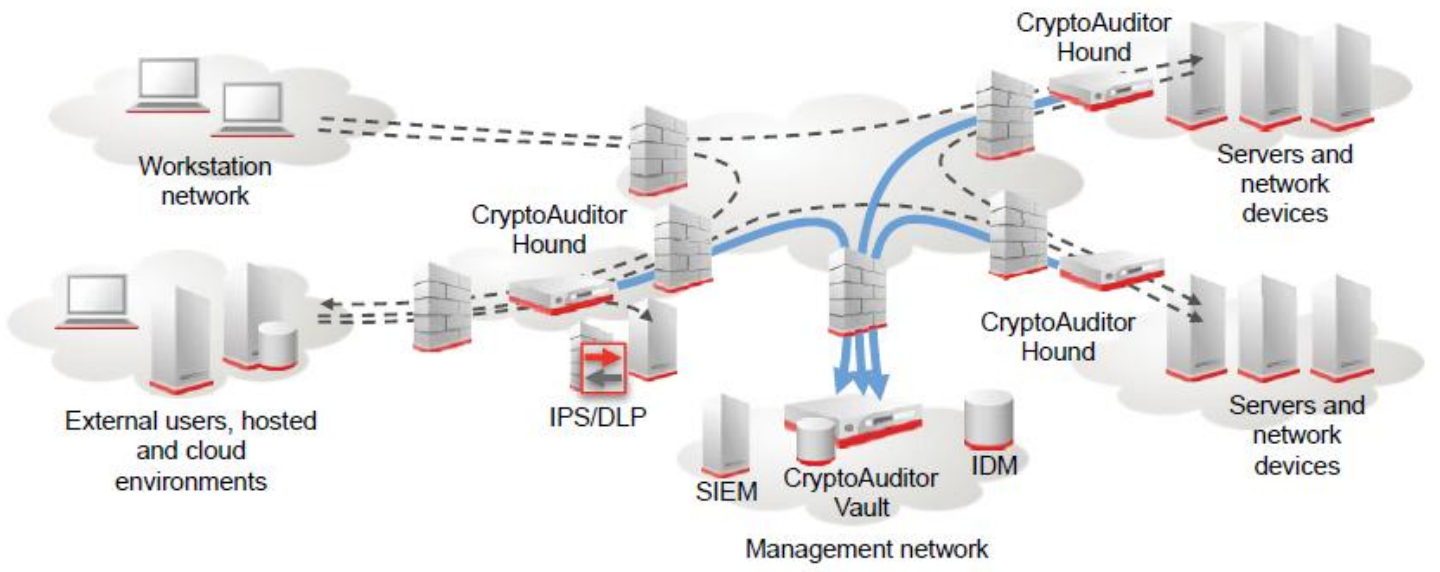
- 信頼された内部の人員からのリスクを削減:
  CryptoAuditorは特権アクセスユーザーに対してたちまち制御及び説明責任を果たすことができます。これにより情報セキュリティーのアーキテクチャーのギャップを埋める事ができます。
- 広範でありながら透過的:既存のシステムへの変更を最小限にするアプローチをとるCryptoAuditorは管理者に対しては透過的である一方で、監査上必要なすべての地点で広範に通信をキャプチャーします。
- 現存のアーキテクチャーに簡単に展開が可能:
  CryptoAuditorは分散アーキテクチャーでも簡単に展開することができあます。単一のコンソールから簡単に管理が行えるアプローチをとっています。

企業内の分散ネットワーク環境において簡単に展開できる、CryptoAuditorは中央で集約型のコンソールから簡単に管理でき、中央に暗号化された監査証跡を保管し、オン・デマンドで、又はリアルタイムでその操作を再生することができます。その上、すべての設定管理は一か所のコンソールから行えるため、時間の節約と利便性の向上も図れます。他の標準のフォレンジックツールと全く異なり、ICAPプロトコルを使用したIDS/DLP連携機能及びSNMP/syslog/ Eメールを利用したコンテンツベースの警告機能は企業外に重要なデータが偶然にまたは悪意を持って転送されないようにするために漏えいに対しセキュリティー・チームが事前にアクションととることを可能にします。

ほとんどの第1世代の監査ソリューションはゲートウエーもしくはフトウェア・エージェントベースで必要な監査ポイントに全てに対して展開するのが困難かつ高価となり、又システムに対しての大きな変更が必要で管理者のワークフローを増大させるものでした。CryptoAuditorは既存のシステムへの変更を最小限にし、管理者にとっては透過的であるため、展開の時間を大幅に削減し、管理者の日々の業務を妨げないため運用コストの増大も防ぎます。

環境をコントロール下に

問題点	CryptoAuditor
転送データーの暗号化を要求し、なおかつ特権ユーザの操作に付いても完全な監査及び個別の説明責任の提供を要求する法律・業界規制の標準（PCI-DSS等）にどのように準拠するのか。	すべてのユーザーの操作、キーストローク、サーバーの出力、データ転送を含む暗号化された接続を監査し、記録を取得します。包括的なレポート及びセキュリティー機能（例、4 eyes認証）があります。
暗号化されたリモートからのシステム・アクセス及びユーザーの操作に対し中央での集約と全般的な可視性がない。	中央集中管理機能、レポート機能、及びSSH、SFTP、RDP（HTTPs及びFTPSはバージョン1.1で対応）に対する可視性を提供します。
暗号化された接続に対するリアルタイムでの情報、警告、侵入もしくはデーター損失に対する保護が無い。	リアルタイムでの監査、コンテンツベースのアラート、SIEMへのSNMPを利用した協調、ICAPを使用してのIP/DLPとの連携を行います。
ITインフラストラクチャー及びシステムに大きな権限を持ち、ログの変更、監査サービスをシャットダウン、その操作を消去又は隠ぺいすることができる管理者(内部/外部)を監査する為のいかなる手段も無い。	ネットワーク・レベルの監視機能は認定された第3者が監査、フォレンジックを行う為の機能を提供します。保護対象のシステムの管理者はCryptoAuditorへの管理者としてのアクセス権や監査証跡へのアクセス権を持ちません。
問題やセキュリティーへの対応、トラブルの解決、フォレンジック、外部からのアクセスに対して監査アクセスを有効にする等のプロセスが複雑で時間がかかり誤りを生じ易い。	監査対象の環境に対し、中央集中方式でのコンテンツベースの監査証跡の検索が可能なため、リアルタイムでの可視性とコンテンツベースのアラート機能を提供します。
監査ソリューションの展開が複雑で時間がかかる。ユーザーにこれまでの業務上での利用方法と異なる利用方法を強いる。	展開、監査、制御に透過的な方法を提供します。
複雑で扱いにくいプロセスやツールにより中間的なIT機器、回避策、他の非公式で承認されていない手段が増える	CryptoAuditorは複雑な操作、作業なしで監査及び制御が可能です。



販売代理店：株式会社ディアイティ

TEL:03-5634-7653　Mail:info@dit.co.jp　URL:http://www.dit.co.jp