データシート

SOX コンプライアンス

Keeperはサーベンス・オクスリー法（SOX法）のコンプライアンスをサポート

2002年に米国連邦法として制定されたサーベンス・オクスリー法（SOX法）は、公開企業や新規株式公開（IPO）を検討している企業に適用される一連の不正防止規制を確立しました。SOX法またはSarboxは、SOX法準拠監査を行う会計事務所だけでなく、米国で株式公開し事業を行う完全子会社や外国企業にも適用されます。

SOX法の目的は、企業の情報開示の正確性と透明性を確保し、会計上の誤りや不正行為から企業の株主と一般市民を保護することです。

リモートワーク時代のSOX法遵守には自動化が不可欠

COVID-19のパンデミックは、INTERPOLが「憂慮すべき」と呼ぶサイバー攻撃の世界的な増加を引き起こしました。サイバー犯罪者は、組織が多数のリモートワーカーを可能にする技術を急速に導入するにつれて増加するセキュリティの脆弱性を利用しています。

このような高リスク環境において、SOX法コンプライアンスの専門家は、既存のコンプライアンス・テクノロジーとプロセスに変更を加えようとしています。

SOX法監査では、組織が5つの主要分野にまたがる内部統制を確立し、これらの統制が効果的に機能していることを示す膨大な文書を提出することが求められています：

1. 統制環境
2. リスク評価
3. 統制活動
4. 情報とコミュニケーション
5. モニタリング

SOX法監査報告書は毎年作成されますが、組織は年間を通じて継続的に統制が機能していることを証明しなければいけません。つまり、監査関連の活動は年間を通じて行われ、すでに過重労働となっているITスタッフにさらなる負担を強いることになります。組織は、可能な限り多くのSOX法コンプライアンス・プロセスを自動化することが極めて重要です。

SOX法コンプライアンスをサポートするためにKeeperを使用する

企業が SOX 法の財務報告・開示要件を遵守するためには、クレデンシャルの保護と財務シス テムへのアクセスが不可欠です。企業ネットワーク内のすべてのユーザーが潜在的なリスク要因となるため、組織のネットワークにアクセスするすべてのデバイス上で、すべての従業員、下請け業者、ベンダーのリスク軽減とデータ保護を確保することが非常に重要です。

Keeperは、カスタマイズ可能な監査ログとイベントレポートにより、IT管理者がデータ環境全体で従業員のパスワード使用とロールベースのシステムアクセスを完全に可視化し、制御することで、SOX法コンプライアンスの監視とレポートを簡素化します。Keeperは、委任管理、実施ポリシー、イベント追跡、監視、およびレポートを通じて、強固な内部統制をサポートします。

IT管理者の洞察

すべての従業員に安全なデジタル保管庫が提供されます。管理者コンソールのセキュリティダッシュボードは、脆弱なパスワード、パスワードの再利用、2FAの実施状況の概要を提供し、ロールベースのアクセス制御（RBAC）により最小権限ポリシーを実施します。部門やチームリーダーごとに管理権限を委譲することができ、フォルダや記録を安全に共有したり失効させたりすることができます。管理者または従業員が退社する場合、その保管庫は自動的にロックされ、安全に譲渡することができます。Keeper データ保管庫へのアクセスログは、コンプライアンスまたはフォレンジックのために監査することができます。

SOX監査報告

Keeper Commander SDKは、管理者と承認されたエンドユーザーがSOXコンプライアンス要件に関連するレポートを実行することを可能にします：

共有アクセスレポート -共有報告コマンドは、組織内のどのユーザーが保管庫内の記録にアクセスできるかの内訳を表示します。このレポートは、現在 Commander にログインしている特定のユーザーに基づいて生成されます。

Keeper Security の高度なレポートとアラートモジュール (ARAM) は、IT管理者にあらゆる規模のユーザーを監視し、危険な行動や異常な行動に関する集中的で要約されたトレンドデータとリアルタイムの通知を受け取り、カスタマイズされたレポートを実行する権限を与えます。例えば、監査レポートコマンドは、ユーザー、レコード、またはシステム全体のレベルで詳細なイベントベースのレポートを提供します。

Keeperは、管理者が簡単にカスタムSOXレポートを定義することができます。このレポートには、誰と情報が共有されたか、アクセスに関連するパーミッションの変更など、情報共有に関連する詳細なイベントが含まれます。ARAMの詳細については、Keeper ARAMデータシートを参照してください。

Eメール自動プロビジョニング

メールアドレスのドメイン一致で、数万または数千のユーザーにKeeperのデジタル保管庫を簡単かつ迅速にプロビジョニングできます。最小限の管理で、既存のメールチャネルまたはポータルを使用して、大規模な展開が可能です。

柔軟なプロビジョニング

Keeperは、SCIMプロトコルを使用して、Microsoft Azure ADまたは他のアイデンティティプラットフォームからユーザーとチームをシームレスにプロビジョニングする機能をサポートしています。Keeperはまた、Keeper Commander SDKを使用することで、APIベースのコマンドラインプロビジョニングをサポートしています。Keeper Commander SDKはオープンソースのPythonコードで、KeeperのGithubリポジトリからダウンロード可能です。

安全なファイルストレージ

従業員のパスワードを保護するだけでなく、Keeperは機密ファイル、ドキュメント、デジタル証明書、秘密鍵、写真、ビデオを安全性の高い暗号化されたデジタル保管庫に保存することで、企業がデータ損失を防ぐことができます。従業員は、意図された受信者だけが共有ファイルにアクセスできることを知って、安心して同僚とファイルを安全に共有することができます。

KeeperはPBKDF2を使用して、ユーザーのマスターパスワードに基づいて認証キーを導き出し、各保存ファイルを暗号化するために、デバイス上でローカルに個々の記録レベルのAES-256暗号化キーを生成します。Keeperのクラウドは各ファイルの暗号化された暗号文のみを保持します。ユーザー間の共有は、共有ファイルの受信者だけが復号化できることを保証するために、PKIを使用して実行されます。Keeperのゼロ知識暗号化方式は、ユーザーだけが保存されたファイルにアクセスし、復号化できることを保証します。

サードパーティベンダーの侵害に対する防衛策

たとえパスワードのセキュリティが強固であっても、ベンダーのいずれかを介して、あなたの会社が危険にさらされる可能性があります。リモートワークが急速に拡大する中、サイバー犯罪者はリモートワークを可能にするために企業が導入している無数のSaaSソリューションを利用しています。Keeperは、管理者が情報および重要なシステムへのサードパーティベンダーのアクセスを制限することを可能にするきめ細かなコントロールをサポートしています。カスタムアラートとレポートを設定し、危険な行動を監視、追跡、管理者に通知することができます。管理者は、サードパーティベンダーのアカウントをロックするなどの措置を講じることができます。

ビジネス向けKeeper BreachWatchは、漏洩した認証情報による侵害から、サードパーティベンダーのアカウントを含む組織を保護します。BreachWatchは、公的な侵害通知に依存しません。ダークウェブフォーラムをスキャンし、従業員のパスワードが漏洩した場合、リアルタイムで組織に通知します。これにより、IT管理者はすぐにパスワードのリセットを強制することができ、サイバー犯罪者がパスワードを使って会社のシステムに侵入するリスクを最小限に抑えることができます。

Keeperについて

Keeper Security (Keeper) は、パスワード関連のデータ漏洩やサイバー脅威を防止するための、市場をリードするトップクラスのサイバーセキュリティプラットフォームです。Keeperのゼロ知識セキュリティと暗号化ソフトウェアは、サイバーセフトのリスクを軽減し、従業員の生産性を高め、コンプライアンス基準を満たすために、世界中の何百万人もの人々と何千もの企業に信頼されています。Keeperは、PC Magazineの年間ベストパスワードマネージャー＆エディターズチョイス、PCWorldのエディターズチョイスに選ばれ、4つのG2ベストソフトウェアアワードを受賞しています。KeeperはSOC-2およびISO 27001認証を取得しており、System for Award Management (SAM)を通じて米国連邦政府による使用にも登録されています。詳細は

https://keepersecurity.com/enterprise.html をご覧ください。