Securing the path to your information assets

Data Sheet

Universal SSH Key Manager

SSHの公開鍵をコントロール

SSHプロトコルの開発元であるSSHコミュニケーション・セキュリティ社は、様々な規模の企業・組織の情報資産の通信経路をセキュアにします。Universal SSH Key ManagerはTectiaおよびOpenSSHの管理者が行ってきた、複雑で手作業が要求される企業環境の管理の時間やコストを削減する互換性及び拡張性の高いソリューションです。又これにより外部及び内部からの承認されないアクセスからのリスクを削減し「見える化」やコンプライアンスも併せて向上させるソリューションです。

困難への挑戦:

今日の複雑な企業環境では、個々のユーザー、システム・アカウント及びアプリケーションIDとそれぞれのターゲットとなるSSHサーバー間の信頼関係を正しくマップする事は不可能といっても過言ではありません。一般的に、企業はユーザー用のIMS (ID管理システム)を展開していますが、すべてのシステムへのSSHアクセスを視野にいれておらず、又企業全体のアカウントも管理出来ていない場合が大半です。更に企業の最も重要な情報資産にアクセスするユーザーの鍵に対する可視化、いわゆる見える化は一切提供していません。ユーザーの鍵を管理する従来の方法は時間がかかりコストもかかります。それでありながら自動化や監査性を提供する方法は今までほとんどありませんでした。

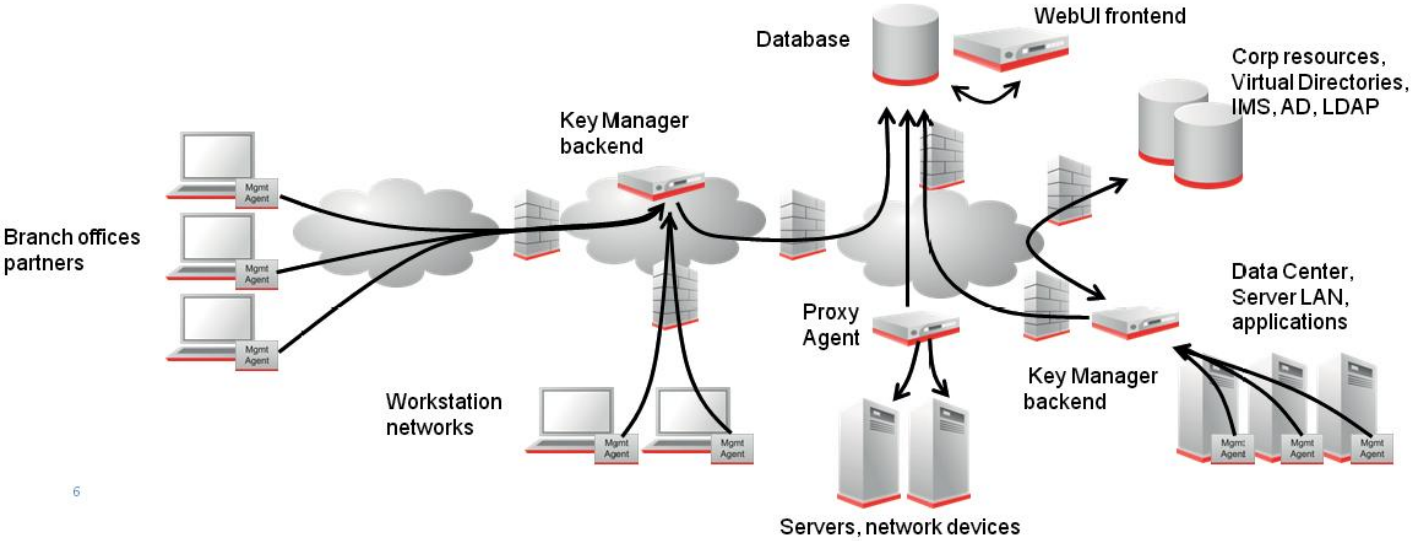
ソリューション:

SSHコミュニケーション・セキュリティー社のUniversal SSH Key Managerは、企業レベルでSSHのユーザー鍵管理を行うことができる唯一のソリューションを提供します。本ソリューションは一般的なFortune 1000レベルの企業の鍵管理に係るコストを平均で1～3百万ドル削減し、セキュリティーチームの負担を減らします。これにより従来対応がおろそかになっていた他のより生産的な仕事にリソースを割り当てることが可能となります。又重要なビジネスに係る情報への権限がないアクセスのリスクを削減することでコンプライアンスに準拠し、更なるセキュリティーレベルを達成します。

セキュリティー投資回収率(ROSI)

セキュリティーでのメリットのみならず、一般的なFortune 1000企業では、本システムを導入することで5年間で75%のIT費用を回収できるだろうと予想しており、セキュリティーリスクの改善を考慮に入れた場合5年で投資が回収できると想定しています。

- **コスト削減**:時間および費用がかかる手作業による管理プロセスを削減します。
- **リスクの削減**:企業全体のネットワークでどのSSHサーバーに誰がアクセスしているかが明確になることでセキュリティーを強化し、セキュリティーインシデントによる企業の価値の失墜を防ぎます。
- **コンプライアンスへの対応**:単一、簡便な監査ソリューションでSSHのユーザー鍵管理を実施することで、コンプライアンスの遵守を確実なものにします。



費用、リスク、コンプライアンス

今日まで、ユーザーの鍵を作成し、展開し、設定するプロセスは手作業で行われており、また管理できないプロセスでした。

環境の複雑さや作成しなくてはならない鍵ペアの数が増加するにつれ、セキュリティ管理者は、誰がどのSSHサーバーへのアクセス権を持っているかに関する可視性を失っていくこととなります。組織の変化、従業員の異動さらに吸収合併などによりサーバーのアクセス権を失効させる必要が発生した場合に問題はより悪化します。

結果として、企業ではSSHユーザーの鍵の設定管理に多大なオーバーヘッドが発生するだけでなく、鍵の更新や削除が十分に行なわれないというリスクが増大する一方で、鍵管理のベスト・プラクティスに対応しコンプライアンスに準拠するというプレッシャーに立ち向かうこととなります。

あなたのIT環境をコントロール下におくには

既存のSSH環境に変更を加えずコネクションの信頼関係を検出する。

- 管理対象環境にある公開・秘密鍵の情報を自動的に収集すること。
- SSH環境にある鍵に関するデータを生成し、信頼関係に関する可視性を提供すること。

収集されたアカウントへのユーザーとIDを整理する

- 収集した情報をIMS(ADまたはLDAP等)へ接続しユーザー/IDにマップする。
- 誰がどのサーバーへ、どのアカウントを使用してアクセスする権限を持っているかに関する、既存の信頼関係を可視化する。
- ユーザーとホストをグループ化し(ローカル及びAD/LDAPを基準にして)、これらのグループを利用して誰がどのSSHサーバーにアクセスすることができるかに関する権限付与規則を作成する。

SSHのユーザー鍵環境を管理、制御する。

- 権限付与規則を強制し、鍵環境の管理を有効にする。
- 公開鍵の管理(配布、更改、削除)を自動化する。
- 秘密鍵のライフサイクル管理(生成、更新、削除)を自動化する。
- 鍵の展開に関する、要求及び認可等の承認された鍵管理プロセスを強制する。

サポートするTectia 及びOpenSSHプラットフォーム:

HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)
HP-UX 11iv2, 11iv3 (IA-64)
IBM AIX 5.3, 6.1, 7.1 (POWER)
Microsoft Windows XP, 7
Microsoft Windows Server 2003, Server 2008, Server 2008 R2
Red Hat Enterprise Linux 4, 5, 6 (x86)
Red Hat Enterprise Linux 4, 5, 6 (x86-64)
Oracle Solaris 9, 10 (SPARC)
Oracle Solaris 10 (x86-64)
SUSE Linux Enterprise Desktop 10, 11 (x86)
SUSE Linux Enterprise Desktop 10, 11 (x86-64)
SUSE Linux Enterprise Server 10, 11 (x86)
SUSE Linux Enterprise Server 10, 11 (x86-64)

検出機能

- 鍵のサイズ、種類、パスフレーズの有無。
- ユーザー/ユーザー・グループを基準とした鍵の所有者。
- ホスト/ホスト・グループを基準とした鍵の場所。
- ユーザー及びホスト・グループ毎の全ての管理対象ホストの有効な信頼関係。
- 承認されていないもしくは不正な公開・秘密鍵。
- 生成、承認、受け付けられた鍵へのリクエスト。
- 設定時の鍵の作成状況。
- 失効または削除された鍵。
- 鍵の要約(展開済みの鍵の数、作成されたが展開されていない鍵の数等)
- 管理者のいない鍵。
- Eメール及びSNMPでのリアルタイムでの警告。

構成

- 様々なソースから収集したユーザー・アカウントを人及びグループへマップ。
- ユーザー及びその他グループをLDAPと同期またはLDAPからインポート。
- 収集したホストをホストグループに展開。
- ホスト及びホストグループをLDAPと同期またはLDAPからインポート。
- 権限付与規則を定義 (どのユーザー/グループがどのホスト/グループへのアクセスをするか)。
- 信頼関係と定義した有効な権限付与規則を比較。

管理

- 権限付与規則(権限付与規則に従い、鍵を展開又は失効する)。
- ウェブ・ベースのインターフェースから鍵の展開を承認するための認可の手続きを実施。
- 現存の認可プロセスに対応するための鍵インターフェースの処理・/統合。
- クライアント・システムでの新しいプライベートの鍵の生成。
- 秘密鍵のライフサイクル及び更新管理。
- 指定したホストへの公開鍵の配布。
- Eメールでの通知及び警告。
- リアルタイムモニター及び環境のメンテナンス。
- 中央集中管理及び分散管理アーキテクチャーのサポート。
- バーチャルアプライアンス、ハードウェアアプライアンス、ソフトウェアでの提供。
- 鍵及び構成情報を中央のデータベースで保管。
- 環境の要求に柔軟に対応可能な中央もしくは分散アーキテクチャーを使用した機能性。
- 複数の鍵マネージャーをバックエンドに配置しフロントエンドにWeb UIの展開を可能にするモジュール式のアーキテクチャー。
- 仮想ディレクトリー、AD、LDAPへの接続。
- 既存のSSHサーバーにエージェント無しで接続可能なプロキシー・エージェントモデル

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