ssh communications security

データシート

UNIVERSAL SSH KEY MANAGER™ 1.7

Secure Shell インフラにおけるID 及びアクセス管理

Universal SSH Key Manager は、SSH 信頼関係に可視性を提供し、Secure Shell 環境に監査とコントロールをもたらす、マルチプラットフォームで拡張性のあるソリューションです。SSH 鍵に関するポリシーがコンプライアンスに対応するようにし、承認されていないアクセスのリスクを削減し、コストを削減します。

問題

多くの大企業は、自動バックアップや日々のファイル転送、ユーザーによるシステム管理の為のインタラクティブなアクセス等のビジネスに欠かせない作業に、安全な認証や機密性（暗号化）を提供するのに、Secure Shell (SSH) にまかせています。しかし、ほとんどの企業では、これら機能を可能にする SSH公開/秘密鍵の生成、設定及び展開を、手作業で行っています。これらの SSH公開/秘密鍵 のクレデンシャルを発行するプロセスを統括する中央管理の欠如は、そのクレデンシャルのライフサイクルを追跡したり、ポリシーに従って生成されていることを確認する手段がないということを意味します。

時間がたつにつれ、コントロールできなくなるほど、認証鍵が拡散していってしまいます。セキュリティ・マネージャーは誰がどのサーバーへのアクセス権を持っているのか、また以前に許可されたアクセス権を取り消していいのかなどの可視性とコントロールを失っていきます。個々のユーザー、システム・アカウント、アプリケーションID及び各宛て先サーバーとの間の信頼関係をマップするのはほぼ不可能な状態になります。

エンド・ユーザーのアクセスを統治する標準の ID 及びアクセス管理ソリューションは一般的に、SSH の鍵を利用した通常システムやアカウントへのアクセスに関しては、対応していません。ガバナンスやコントロールの欠如は、企業をリスクやコンプライアンスの監査に失敗する状況に押し上げ、さらに企業は手動でこれらに対処する必要性から非常に多くの人員を展開する必要性に迫られます。

挑戦

SSH ユーザー鍵の伝統的な管理方法は、時間と管理費がかかり、これを自動化し、監査可能な状態にする手段は一切ありませんでした。ビジネスにおける多くの重要な機能は、SSH を利用して自動化されており、これら機能に影響を与えることなく SSH の鍵を管理することは非常に困難だったからです。間違った鍵を削除すると、日々のオペレーションに高価な混乱をもたらすことになりかねません。多大な経費のかかるを問題は、組織変更、従業員の異動、退職、企業の合併買収の際に、顕著となります。

サポート対象の SSH バージョン

ssh communications security

Centrify

Attachmate

ORACLE SOLARIS

bitvise

UNIVERSAL SSH KEY MANAGER

ソリューション

SSH コミュニケーションズ・セキュリティ社の Universal SSH Key Manager は、エンタープライズレベルの SSH ユーザー鍵管理ソリューションです。Universal SSH Key Manager は、運用環境のシステムに影響を与えることなく、企業が SSH インフラの制御を行い維持することを可能にするアプローチを提供します。企業の生命線である重要作業の変更の必要性や、数百にもおよぶ自動化プロセスを変更する必要もありません。Universal SSH Key Manager による既存の仕組みに影響を与えないアプローチは、以下の五つの原則に基づいています。

- **査定:** SSH に関するポリシーを作成し、それに基づき SSH 環境の検証を実行。
- **検出:** すべての SSH 鍵を検出、信頼関係をマップし、ポリシー違反を検出。
- **監視:** 鍵の使用実績を監視し、日々のオペレーションに影響の無いようにどの鍵を削除できるか確認。
- **修復:** 失効すべき鍵を削除し、有効な鍵のみを使用することにより、コンプライアンスを達成。
- **管理:** 手動操作を削減し、中央管理を行うことで、コンプライアンスを強制、全ての操作を監査。

オプションのユーザポータルを使用すれば、鍵の削除などの行為を、アプリケーションを実際に使用するユーザやその鍵を所有するユーザに委託することもできます。また、ユーザポータルは 中央からセキュリティ・ポリシーに沿ってSSH ベースのアクセスをリクエスし、プロビジョニングを行う簡単な手段を提供します。この行為の監査証跡を取得することも可能です。
Universal SSH Key Manager は、平均的なフォーチュン1000 の企業の諸経費を、平均で 100 万ドルから 300 万ドル節約し、一方で重大なセキュリティ違反のリスクを削減し、未解決のコンプライアンスの問題を解決します。OpenSSH、Tectia やそのほかの SSH 実装のうちどれを使用されていたとしても複雑な問題を解決します。

査定	検出	監視	修復	管理
SSH環境の状況を査定 • SSH 鍵と承認に関するポリシーを作成 • SSH 環境がポリシーに準拠しているかレポート	誰がどこにアクセスできるか • スクリプトを使用して何千ものホストを迅速にスキャンし、SSH 鍵のインベントリを確認。エージェントレスあるいはエージェントベースでも可能。 • 信頼関係をマップし、ポリシー違反を検出 • 使用されていない、または必要のない鍵と承認を検出	承認されていない変更やポリシー違反を検出し、それに対応するための継続的な監視 • 鍵がいつどこから使用されているか追跡 • 鍵が追加・削除・変更されたらアラート通報 • SSH 設定に承認されていない変更があったら、アラート通報	ポリシーやコンプライアンスに対応するため SSH 鍵を変更 • 使用していない鍵の削除 • ルート配下のディレクトリに鍵を移動 • 承認の更新と制限 • コンプライアンスに対応していない古い鍵の更新 • 中央からの一元管理	アクセスに関するライフサイクルを完全に統合し自動化 • 承認手順を既存のチケットシステムと連結 • 中央管理および SSH 設定の強制 • 鍵生成および削除の自動化 • ポリシー違反の検出とアラート

機能と特長

機能	特長
エージェントレスとスクリプトによる検出	迅速で、システムに影響を与えない方法でSSH 鍵のインベントリを確認
SSH ポリシーとレポート	SSH 鍵環境がポリシーに沿っているかどうかのレポートを作成
自動化と統合のインターフェイス	既存の IAM インフラやワークフローへの接続性のための REST API と CLI
リアルタイムアラート	SIEM ツールにアラートを送り、リアルタイムでの違反への対応
SSH 設定の中央管理	ポリシー制御、標準設定を使用することによる強力なセキュリティ、エラー低減
ユーザーポータル	鍵管理を企業内のエンドユーザーにも可能に。ポリシーに従い、中央からのエンドユーザーによるアクセス要求・鍵のプロビジョニング
コンプライアンスへの対応	現時点の要求および PCI、NIST/FISMA、SOX、HIPAA、Basel III への今後想定される遵守要求にも対応

製品仕様

SSH Key Manager Server の対応プラットフォームとユーザーポータル	• VMWare ESX 5.5 仮想マシンとその他のハイパーバイザー • Red Hat Enterprise Linux / CentOS 6.5 と 6.x バージョン以上
対応データベース	• Oracle 11.2 • PostgreSQL 9.2
高可用性	• 複数台のUniversal SSH Key Manager サーバーサポート • 非挿入型 – 運用環境での障害発生点にならない
鍵検出機能	• サイズ及び種類毎の公開鍵と秘密鍵の検出 • パスフレーズの有無 • 不正な鍵 • 鍵オーナー及びその他の属性（場所、許可、鍵コメントなど） • ホスト及びホストグループ毎の信頼関係 • ホスト鍵
監視機能	• SSH 設定への承認されていない変更の検出 • ユーザー鍵の承認されていない追加、削除、変更行為の検出 • SSH 鍵ベースのログインの検出と証跡 • 設定可能なリアルタイムのメールアラート
鍵の強制機能	• ユーザー鍵を中央の管理下に置く(ホストにあるルート権限を持つディレクトリに鍵を移動) • パスワードで保護された鍵の生成・パスフレーズポリシーに従うことを強制 • 承認ポリシーの中央管理 • 鍵制限の管理 (例えば「command」や「allow-from」制限)
鍵管理の自動化	• 鍵生成、展開、更新、変更、削除の自動化 • 中央での SSH ソフトウェアを設定管理 • コマンドライン統合を利用したプロセスの自動化 • 一時アクセスを許可 (有効期限切れの鍵は自動削除)
管理者の認証方法	• ローカル認証 • Active Directory からの外部アカウント • パスワードと証明書ベースの認証
ロールベースの管理	• Key Manager管理者用のRBAC (製品本体及び LDAP 管理者アカウント双方共) • 各管理者の業務に併せてロールを設定可能
ログ、アラート、アラーム	• Key Manager 管理者によって行われた、あるいは管理されるホストでローカルで実行された承認されていない変更による、SSH鍵とSSH設定への変更の包括的な監査証跡 • 鍵や設定への変更に関するメールと syslog アラート • ホスト毎の疑わしい鍵運用のアラート (使用後、鍵は削除)
管理方法	• ウェブ GUI - Firefox の最新版 - Chrome の最新版 - Internet Explorer 10, 11 • リモート コマンド ライン クライアント • REST API
管理接続の種類	• エージェント型、エージェントレス型の双方のホスト管理方式のサポート • スクリプトによる鍵検出のサポート。既存のオーケストレーションツール (例 Chef, Puppet, Ansible) を使用してスキャンを実行し、結果をインポート。管理操作には、エージェント・エージェントレス接続が必要。
サポートする鍵アルゴリズム	• RSA • DSA • ECC/ECDSA • Ed25519
HSM 製品のサポート	• SafeNet Luna SA 5.4 (エージェントレス接続の際の鍵を保存)

UNIVERSAL SSH KEY MANAGER
製品仕様

サポート対象のSSHバージョン	• Attachmate RSIT 6.1, 7.1, 8.1 • Centrify SSH 2013 • OpenSSH 4.x - 6.x • SunSSH 1.1.5, 2.0 • Tectia SSH 6.4 • Tectia Server for IBM z/OS 6.3, 6.4 • Quest OpenSSH 4.x - 5.2 • Bitvise SSH Server 6.24

管理されるホストのサポート対応プラットフォーム	プラットフォーム	エージェントレス型	エージェント型
	HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)	•	•
	HP-UX 11iv2, 11iv3 (IA-64)	•	•
	IBM AIX 5.3, 6.1, 7.1 (POWER)	•	•
	IBM z/OS 1.13, 2.1	•	
	Microsoft Windows Vista, 7, 10, Server 2003, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2		•
	Oracle Enterprise Linux 5	•	•
	Oracle Solaris 9, 10, 11 (SPARC)	•	•
	Oracle Solaris 10, 11 (x86-64)	•	•
	Red Hat Enterprise Linux 4, 5, 6, 7 (x86, x86-64)	•	•
	CentOS 4, 5, 6, 7 (x86, x86-64)	•	•
	SUSE Linux Enterprise Desktop 10, 11 (x86, x86-64)	•	•
	SUSE Linux Enterprise Server 10, 11 (x86, x86-64)	•	•
	Ubuntu Desktop 12.04, 14.04 (x86, x86-64)	•	
	Ubuntu Server 12.04, 14.04 (x86, x86-64)	•