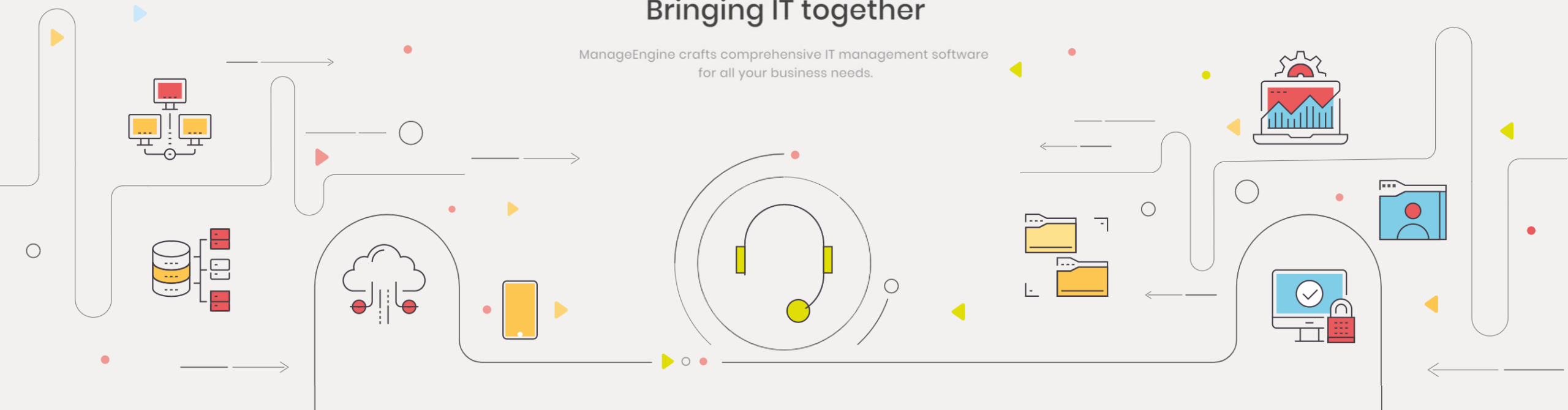


Bringing IT together

ManageEngine crafts comprehensive IT management software
for all your business needs.

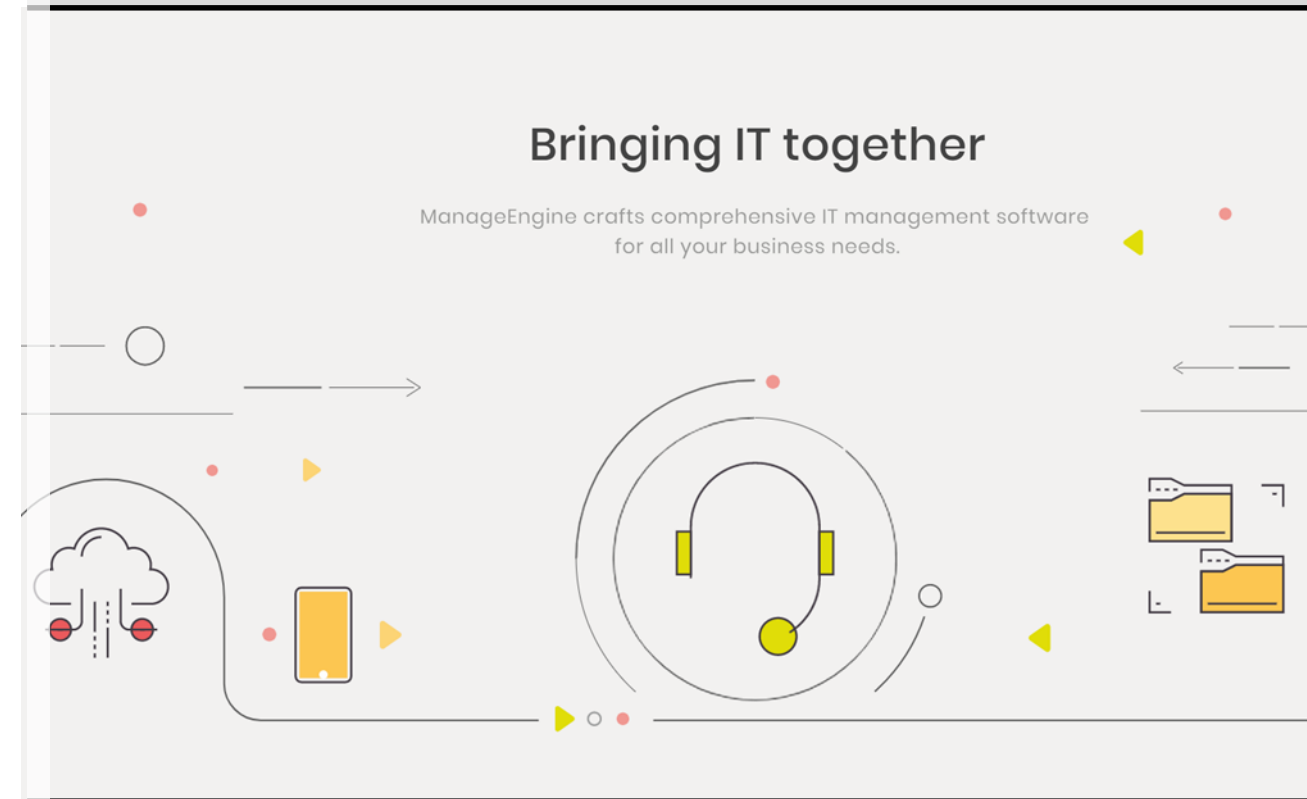


Active Directoryの特権IDに対するセキュリティを強化

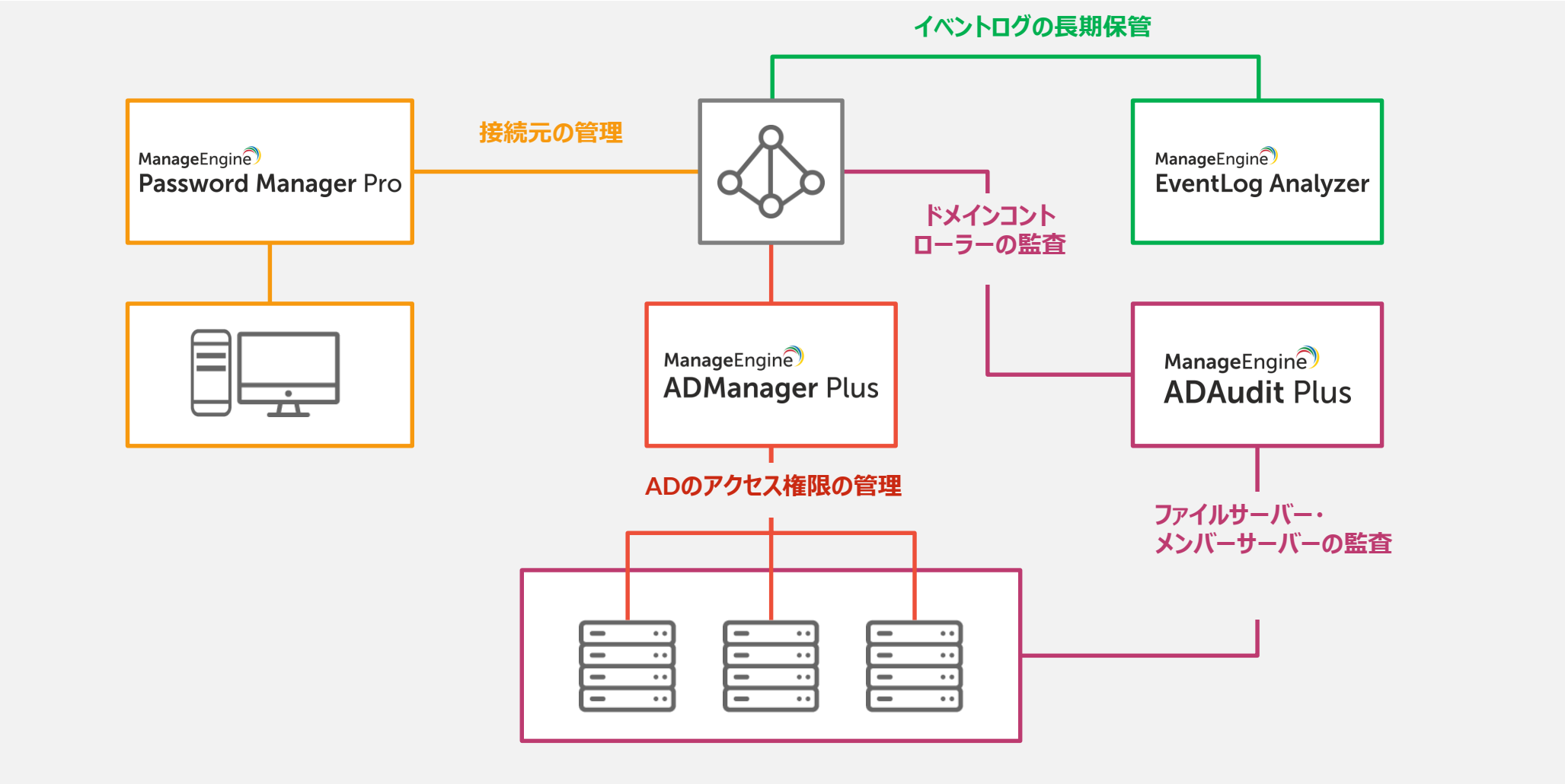
ManageEngine製品を使用した 特権IDの証跡管理とログ監査

目次

- はじめに
- Password Manager Proのご紹介
- ADAudit Plusのご紹介
- EventLog Analyzerのご紹介
- さいごに

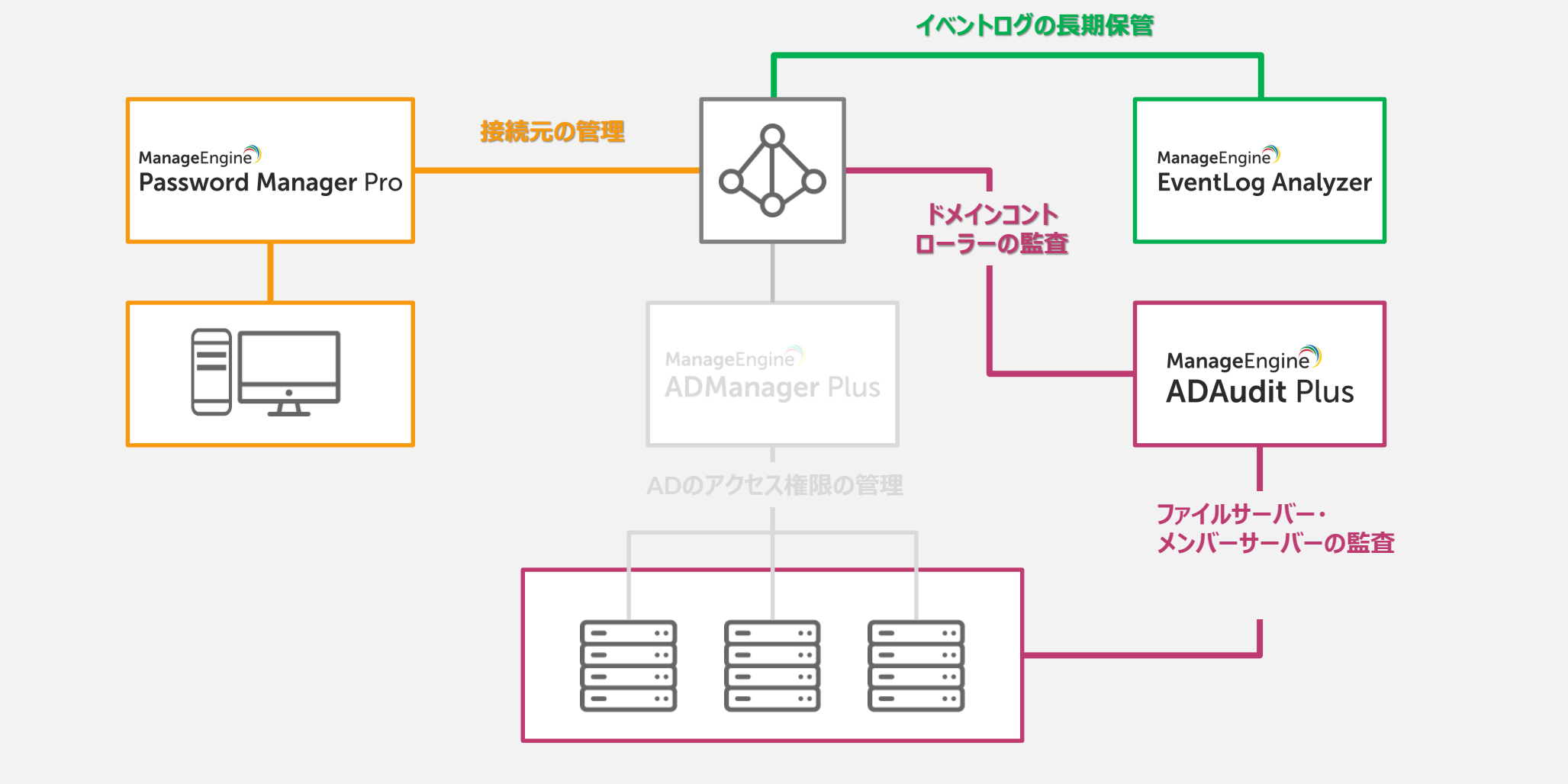


ADの特権ID保護に関連する ManageEngine 製品



Active Directoryのセキュリティをトータルに向上します

ADの特権ID保護に関連する ManageEngine 製品

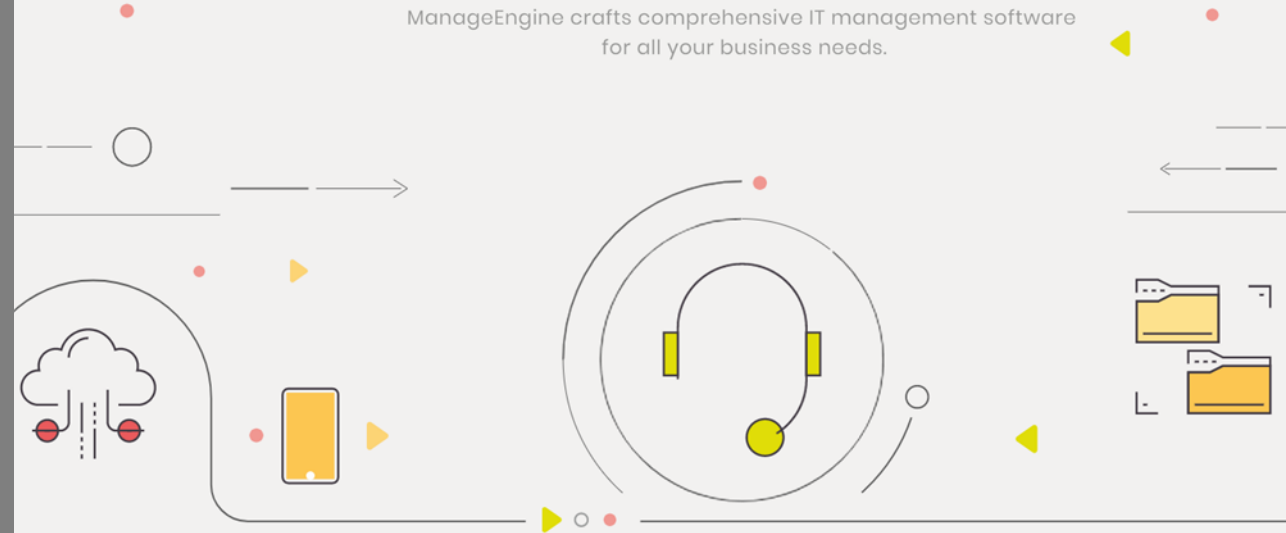


Active Directoryのセキュリティをトータルに向上します

Password Manager Pro のご紹介

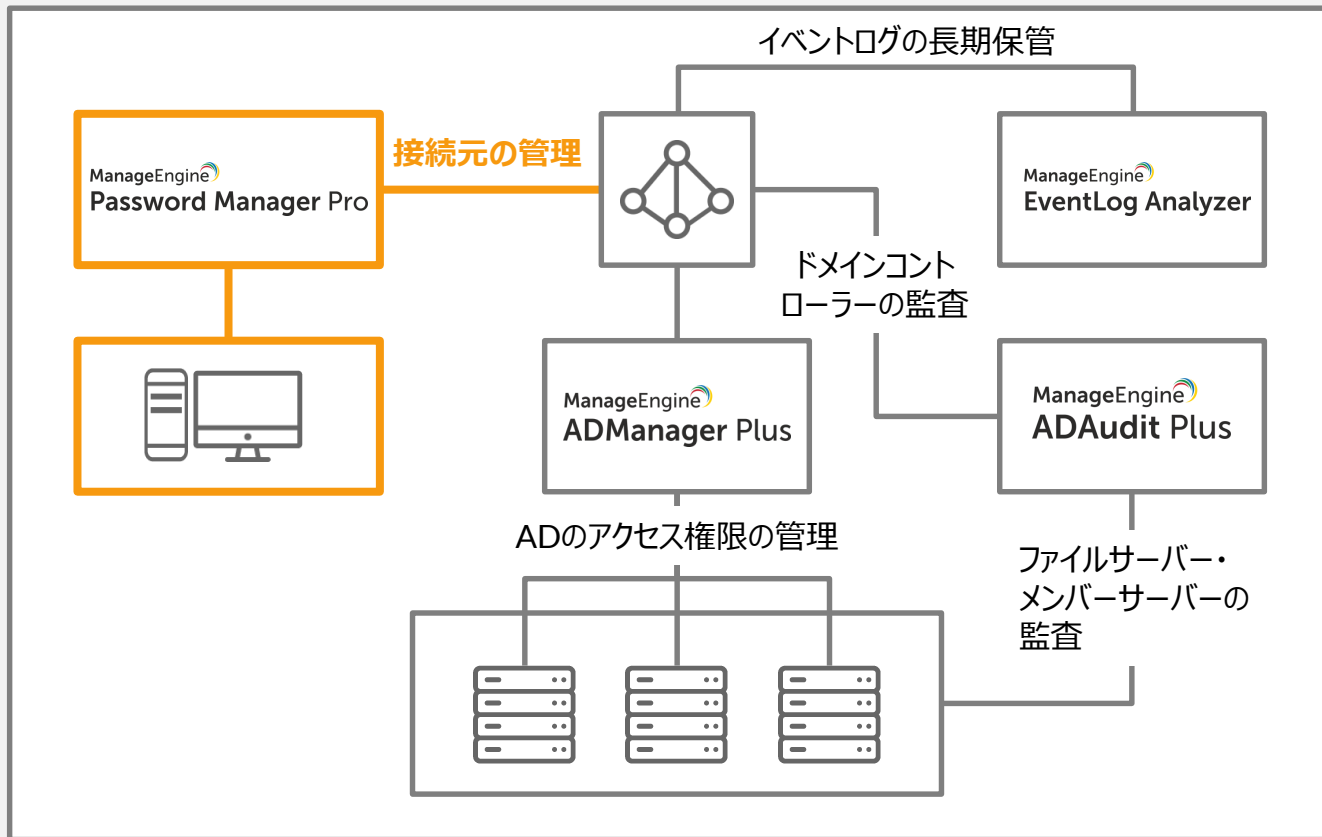
Bringing IT together

ManageEngine crafts comprehensive IT management software for all your business needs.



ADセキュリティ対策製品：Password Manager Pro

ManageEngine



ManageEngine Password Manager Pro

- Active Directoryの特権ユーザーの利用を、踏み台サーバーにて一元管理することで、アクセスを管理



Active Directoryの特権ユーザーのアクセスを管理

特権ID管理に関する注目が高まっています

Windowsの「Administrator」や、
Unix/Linuxの「root」、Ciscoの「enable」
などのIDは、システムに対してあらゆる
権限を持つ特別なID = **特権ID**です

特権ID

Windows :	Administrator
Unix :	root
Linux :	root
Cisco :	enable

不正行為・過失

サイバー攻撃

悪意のある
内部関係者

悪意のある
外部攻撃者

特権IDの不正使用

パスワードの漏洩

特権IDの不正使用やパスワードの
漏洩は、情報漏えいやシステム
障害など、深刻なダメージを
与える恐れがあります

情報漏えい

システム障害

悪意のある内部関係者の不正行為や過失だけでなく、
外部の攻撃を防ぐためにも、特権IDは適切に管理される
必要があります

多くの企業が特権IDの厳格な管理に対する取組みを開始

特権ID管理についてよくお聞きするお悩み事

「誰が」「いつ」
「どのような」操作を
したのかしっかりと
管理できていない

費用が高くて
ツール導入が
ためられる

申請・承認業務が
煩雑で、形骸化
している

多要素認証などで
更にセキュリティを
強化したい

具体的に
どんな作業が
おこなわれたのかが
わからない

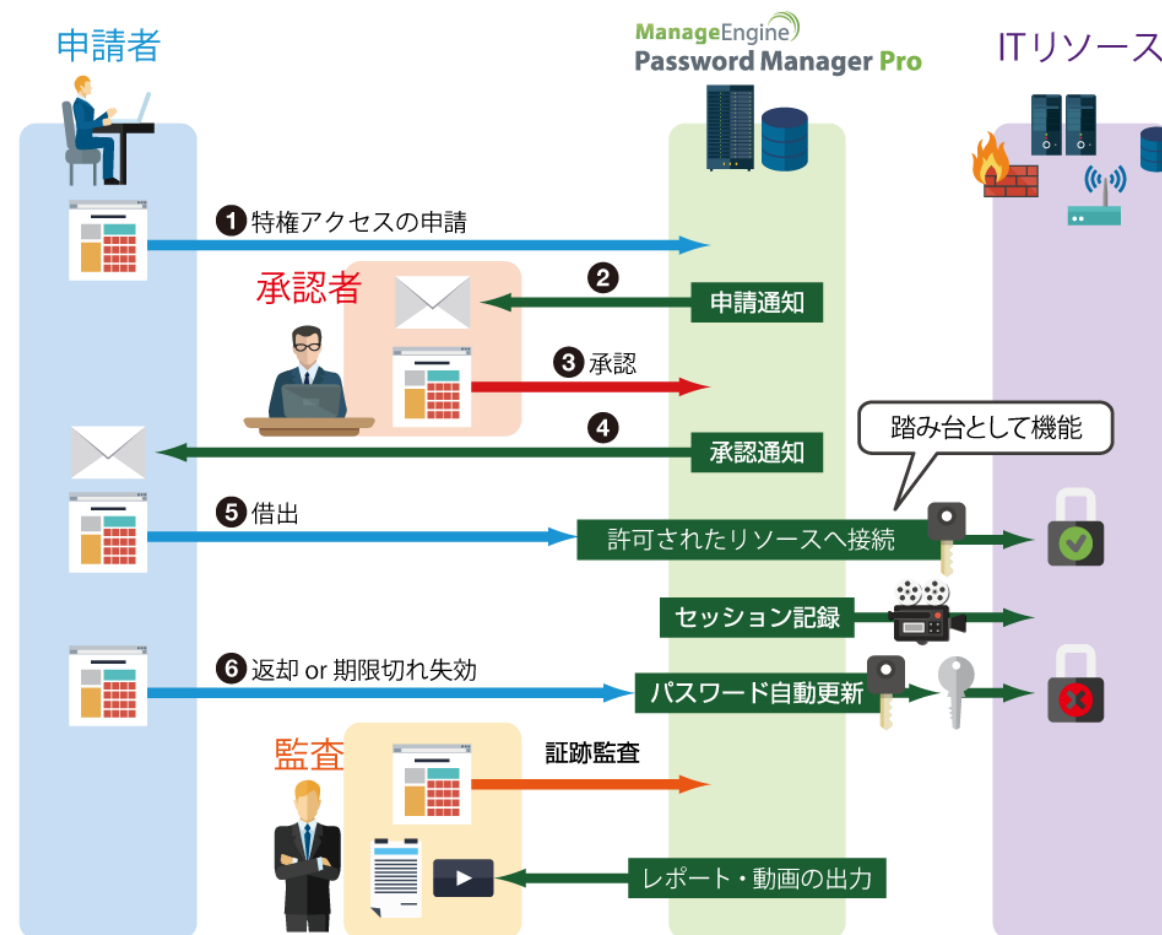
パスワードを教えた後
不正アクセス
されないか心配

多くの企業が特権ID管理に関して苦勞されています

Password Manger Proのフロー全体図

特権IDによるサーバー/NW機器のアクセス利用を管理

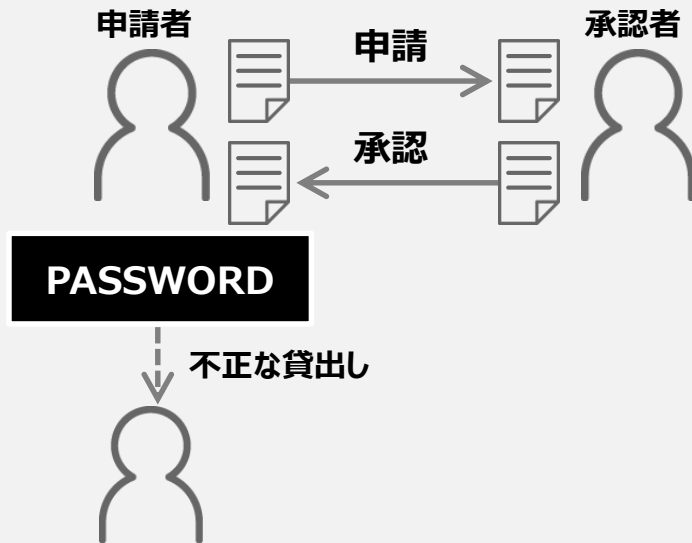
- ワークフロー機能によるパスワードの払い出し
- 踏み台機能による、証跡の管理
- パスワード自動変更によって不正アクセスを抑止



特権IDによるアクセス利用を管理

申請・承認をワークフロー化

Password Manager Pro 導入前



- 申請・承認業務を紙ベースで実施しており、業務工数が多い
- 記入の漏れや事後の記入といった運用上の問題が発生しがち
- 緊急時などは申請・承認を経ずにパスワードの貸し出しなどがおこなわれるケースが多い

Password Manager Pro 導入後

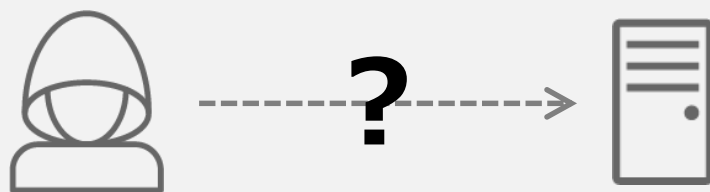


- 申請・承認業務がワークフロー化することで省力化を実現
- 申請・承認業務が行われなければ特権IDが払い出されないため、運用が厳格化

特権IDの運用の省力化と厳格化を実現可能

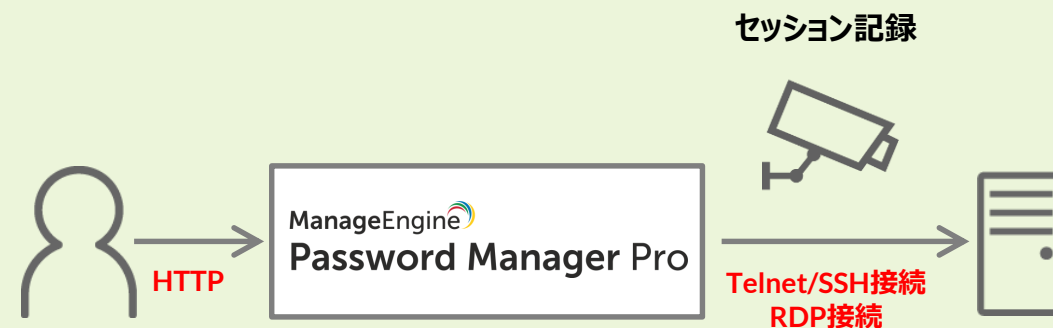
セッション記録によって操作内容を記録

Password Manager Pro 導入前



- 具体的な作業内容は記録されない
- 不正な操作がおこなわれても証跡が残らない

Password Manager Pro 導入後

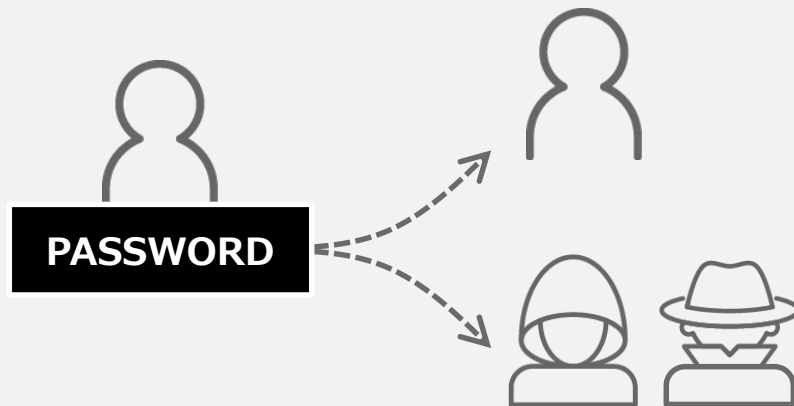


- ITリソースにおいてユーザーの操作画面を全て動画として保存することが可能
- 操作画面の動画保存という運用が、ユーザーの不正操作に対する抑止力を発揮

具体的な操作内容が詳細に動画で確認可能

ITリソースとのパスワードを自動的に変更

Password Manager Pro 導入前



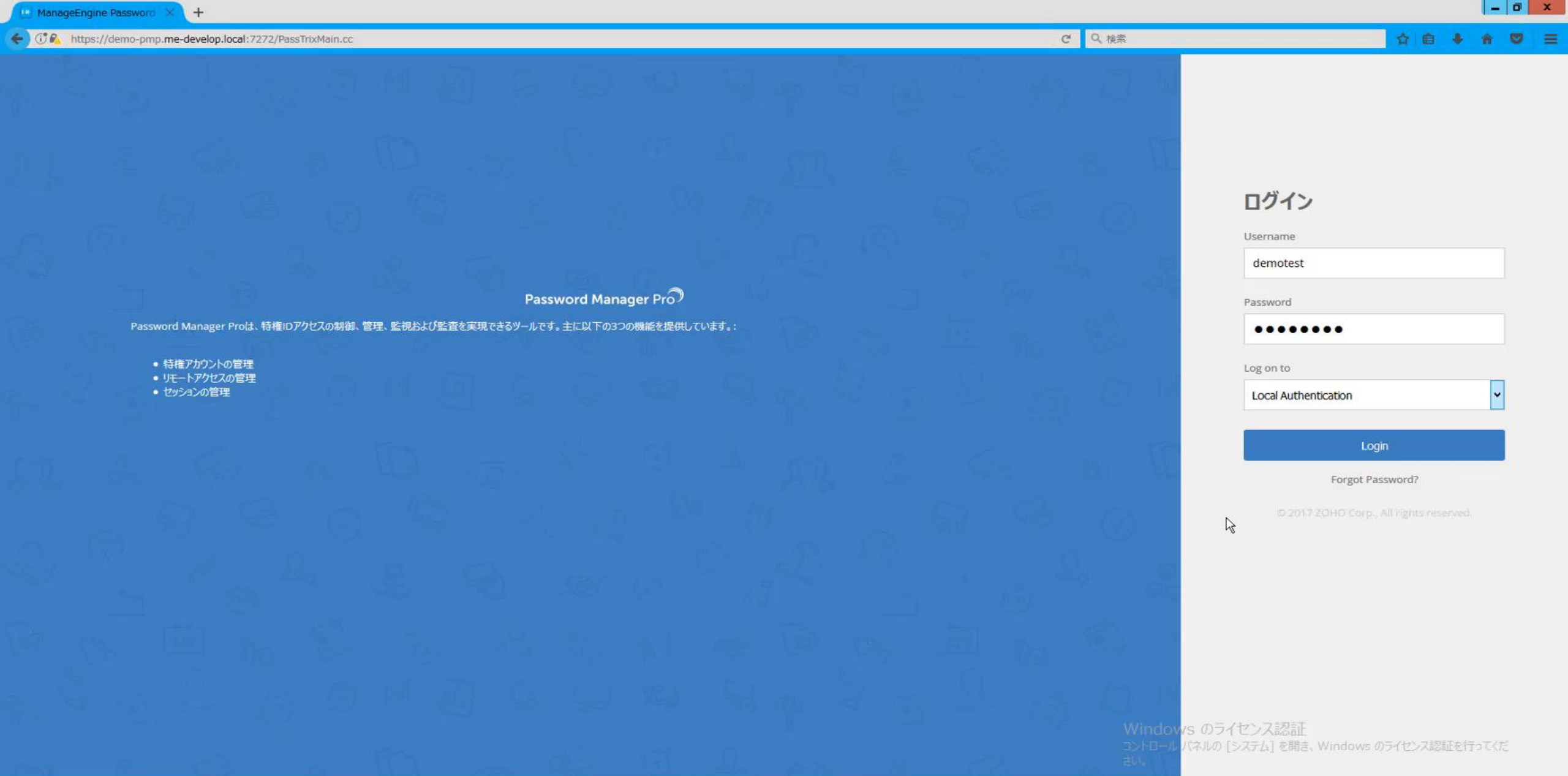
- 特権IDのパスワードが伝わるため、作業後に特権IDの不正利用の危険性が高まる

Password Manager Pro 導入後



- 作業後、Password Manager Pro とITリソースとのパスワードを自動的に変更
- 加えて、特権IDの利用に関わらずスケジュールに従って定期的にITリソースへのパスワードを変更

不正アクセスを防止し、セキュリティ対策としても効果的



申請者側

アクセス履歴の参照

プライマリサーバー セカンダリサーバー

作成

-- すべて --

▼

🔍

☰

操作種別

監査アクション ▼

💡

🔄

表示中 1 - 25 合計

◀ 前の

ページ 1

次 ▶

25

50

75

100

リソース名	ユーザー アカウント	オペレータ	IPアドレス	タイムスタンプ	操作種別	ユーザー名	理由
0 セミナーデモ用	administrator	demotest demotest	192.168.83.150	9 20, 2017 12:03 午後	チェックインしたパスワード	N/A	
0 セミナーデモ用	administrator	demotest demotest	192.168.83.150	9 20, 2017 12:03 午後	パスワードの変更	N/A	リモートでパスワードを変更しまし...
0 セミナーデモ用	demo	demotest demotest	192.168.83.150	9 20, 2017 12:03 午後	チェックインしたパスワード	N/A	
0 セミナーデモ用	demo	demotest demotest	192.168.83.150	9 20, 2017 12:03 午後	パスワードの変更	N/A	リモートでパスワードを変更しまし...
0 セミナーデモ用	demo	demotest demotest	192.168.83.150	9 20, 2017 12:02 午後	パスワードを取得	N/A	Windows Remote Desktop ...
0 セミナーデモ用	demo	demotest demotest	192.168.83.150	9 20, 2017 12:01 午後	パスワードを取得	N/A	Windows Remote Desktop ...
0 セミナーデモ用	demo	demotest demotest	192.168.83.150	9 20, 2017 12:00 午後	チェックアウトしたパスワード	N/A	
0 セミナーデモ用	demo	admin	192.168.83.150	9 20, 2017 12:00 午後	承認されたパスワード	N/A	N/A
0 セミナーデモ用	demo	demotest demotest	192.168.83.150	9 20, 2017 12:00 午後	パスワードアクセス要求	N/A	使用します。
0 セミナーデモ用	administrator	demotest demotest	192.168.83.150	9 20, 2017 11:59 午前	パスワードを取得	N/A	Windows Remote Desktop ...
0 セミナーデモ用	administrator	demotest demotest	192.168.83.150	9 20, 2017 11:59 午前	チェックアウトしたパスワード	N/A	
0 セミナーデモ用	administrator	admin	192.168.83.150	9 20, 2017 11:58 午前	承認されたパスワード	N/A	N/A
0 セミナーデモ用	administrator	demotest demotest	192.168.83.150	9 20, 2017 11:57 午前	パスワードアクセス要求	N/A	使用します。

各機器へ接続した履歴の確認が可能

導入実績

世界**3,300**社以上の企業で導入済

導入業界

- 電機
- 精密機械
- 家電
- 化学
- 繊維
- 鉄鋼
- サービス
- IT
- 通信
- 金融
- 建築
- 不動産
- 電力
- ガス
- 石油
- 外食
- エンターテインメント
- 物流
- 運送
- 食品
- 飲料
- 自動車
- バイク
- 重工業
- プラント
- 建築機械
- 家庭用品
- 製薬
- 化粧品
- アパレル
- 商社
- 小売
- テレビ
- 広告
- 出版
- 印刷
- 地方公共団体
- 学校

導入事例

- 総務省様
- ニッセイアセットマネジメント株式会社様



「Password Manager Pro」の
圧倒的なコストパフォーマンスと
実績を評価

様々な業界、企業規模でご利用いただいております

価格



年間ライセンス

98万円/年～

サポート付

- 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれています。
- 1年ごとに年間ライセンス契約を更新します。



通常ライセンス

245.4万円～

初年度保守サポート付

- 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれています。
- 2年目以降は1年ごとに年間保守サポートサービス契約（40.9万円～）を更新します。
- 4年以上利用する場合は、価格が抑えられます。

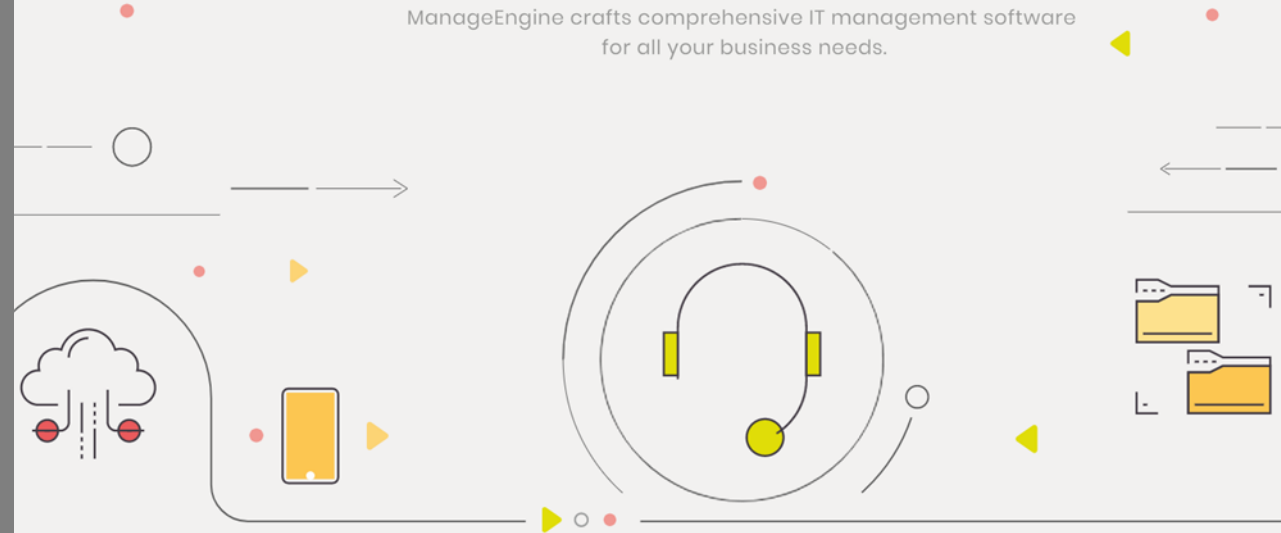
詳細な価格表についてはこちらをご参照ください：<https://www.manageengine.jp/products/Password Manager Pro/pricing.html>

ご要望に応じて、お好きなライセンス体系をお選びいただけます

ADAudit Plusのご紹介

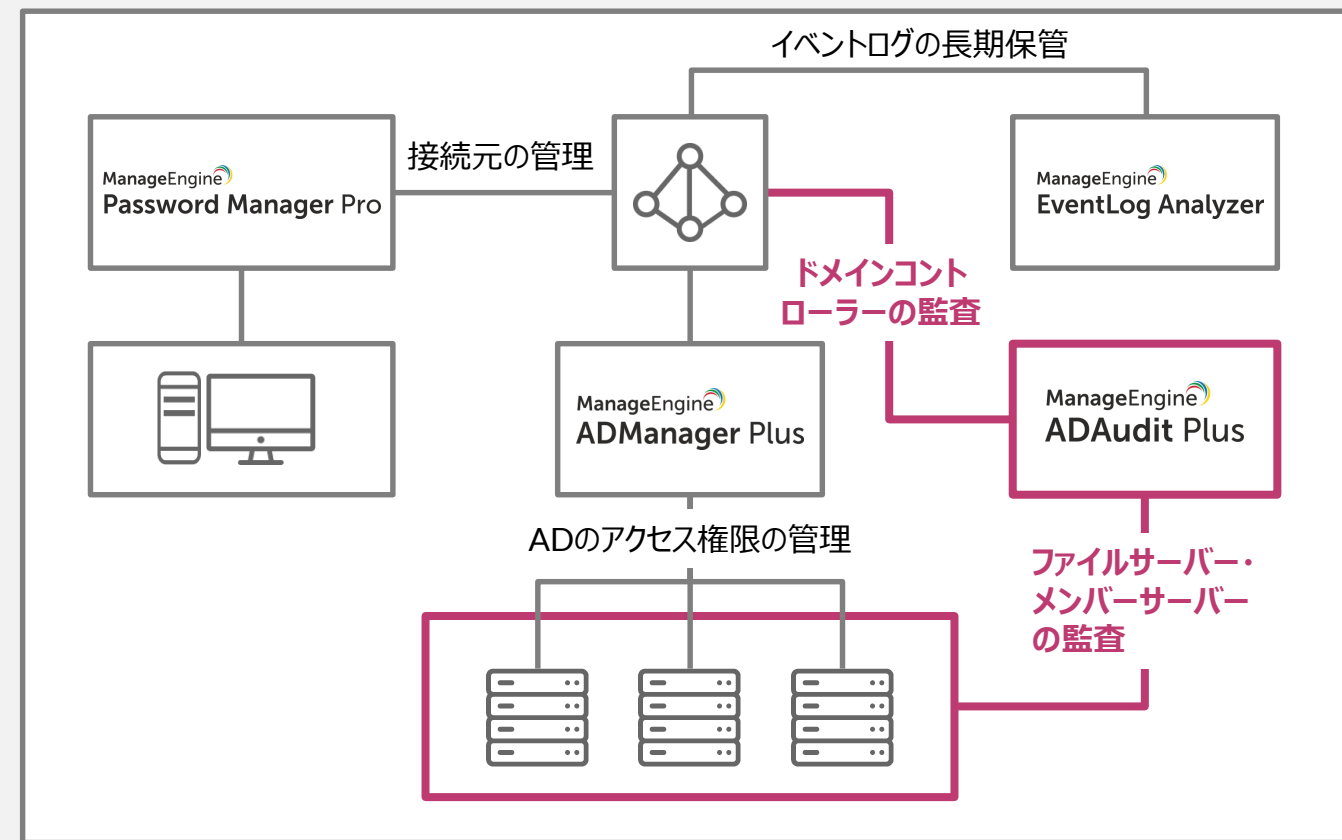
Bringing IT together

ManageEngine crafts comprehensive IT management software for all your business needs.



ADセキュリティ対策製品：ADAudit Plus

ManageEngine



ManageEngine
ADAudit Plus

- ADドメインコントローラーでのログオン失敗・ユーザー/グループメンバー/GPO変更などのログを可視化することで、攻撃を早期検知



Active Directory
監査



ログオン監査



ファイルサーバー
監査



Windowsメンバー
サーバー監査



レポート／アラート機能

Active Directoryへの攻撃を早期に検知

Active Directoryの監査についてよくお聞きするお悩み事

イベントログを
保管しているものの
分析が難しい

Active Directoryと
ファイルサーバーなどを
別々に監査するのは
工数がかかる

様々な観点から
セキュリティ監査を
実施したい

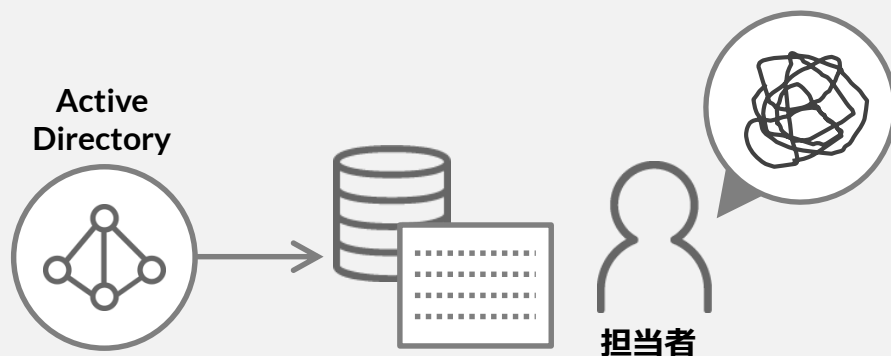
もしサイバー攻撃や
内部不正が発生したら
迅速に対応したい

Active Directoryの
ログも統合して
セキュリティ監査を
おこないたい

多くの企業がActive Directory監査業務に関して苦勞されています

ログの可視化

ADAudit Plus 導入前



- ログは保管してあるが、分析するためには専門的な知識が必要
- 分析するために工数と時間がかかる

ADAudit Plus 導入後



- Active Directoryの重要なセキュリティログを自動で収集／集計
- JPCERT／CCが推奨するイベントログ収集に対応
- 豊富な定義済みレポートにより、外部攻撃や内部不正に関するログを可視化

イベントログの専門的な知識が無くとも、簡単に分析可能

200以上の豊富な定義済みレポート

代表的なレポート

ログオン失敗レポート

ログオンに失敗したユーザーを確認することで、不正なログオン／アクセスを監査

GPOレポート

グループポリシーの変更を確認することで、意図しないグループポリシーの改ざんを監査

ドメインアドミンへの加入ユーザーレポート

特権グループのメンバー変更を確認することで、特権ユーザーを監査

レポートの種類

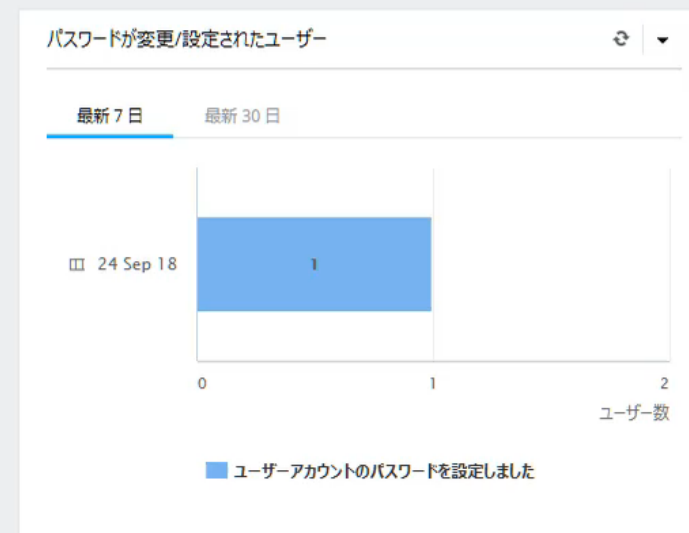
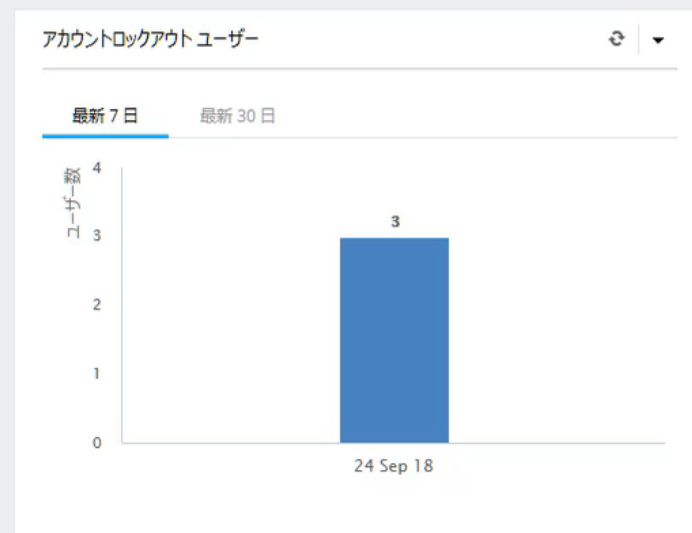
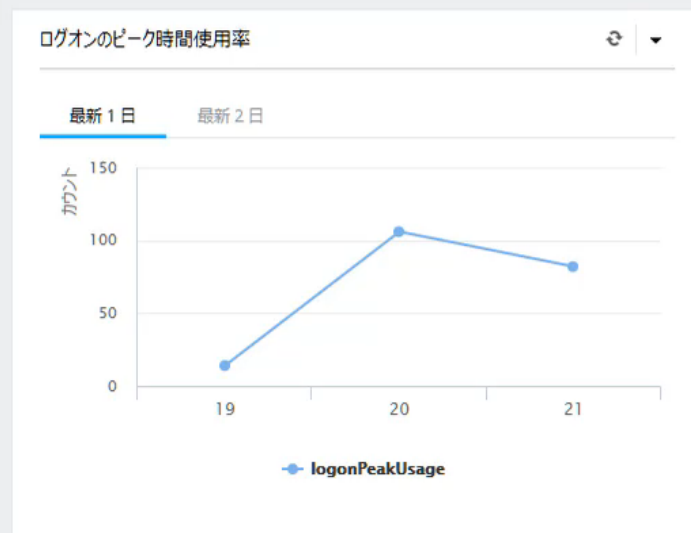
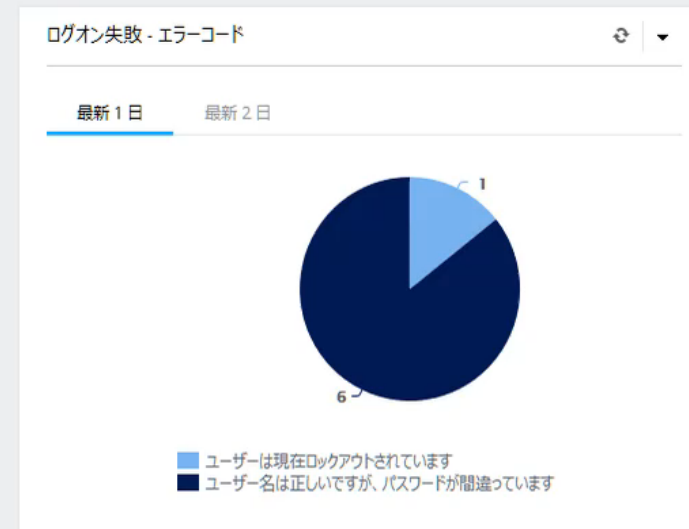
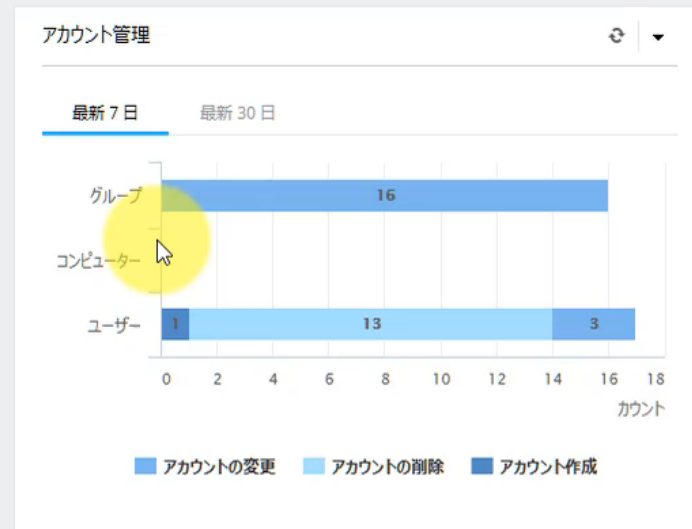
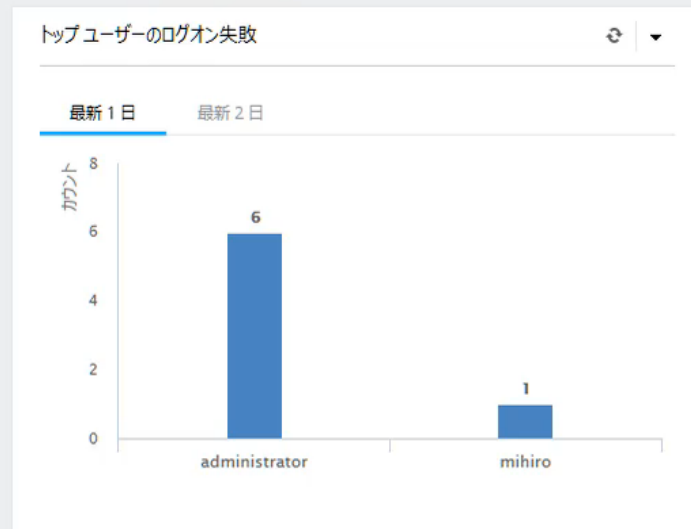
- ユーザーログオンレポート
- ローカルログオン/ログオフ
- ADFS監査
- アカウント管理
- ユーザー管理
- グループ管理
- コンピュータ管理
- 組織単位（OU）の管理
- GPO管理
- 高度なGPOレポート
- その他のADオブジェクトの変更
- アクセス許可の変更
- DNSの変更
- 設定監査
- LAPS監査
- ドメインオブジェクト変更

対応コンプライアンスレポート

- HIPAA
- SOX
- GLBA
- PCI-DSS
- FISMA

多面的な監査や報告を素早く実施

最終スケジュール時刻: 9/24/2018 09:07:03 午後 [すぐに実行する](#)



アラート

更新

重要

4

障害

28

注意

8

最近のアラート

全て見る

METECH\administratorがドメインのローカル セキュリティグループAdministratorsにメンバーCN=前田 美裕,OU=zoho,DC=metech,DC=localを追加しました

9/24/2018 09:05:55 午後

METECH\administratorがドメインのローカル セキュリティグループAdministratorsからメンバーCN=前田 美裕,OU=zoho,DC=metech,DC=localを削除しました

9/24/2018 09:05:05 午後

MIHIRO-SURFACEにおいてユーザーadministratorがログインに失敗しました。理由: ユーザー名は正しいですが、パスワードが間違っています

9/24/2018 08:45:52 午後

MIHIRO-SURFACEにおいてユーザー

特権グループへのユーザー追加を監査

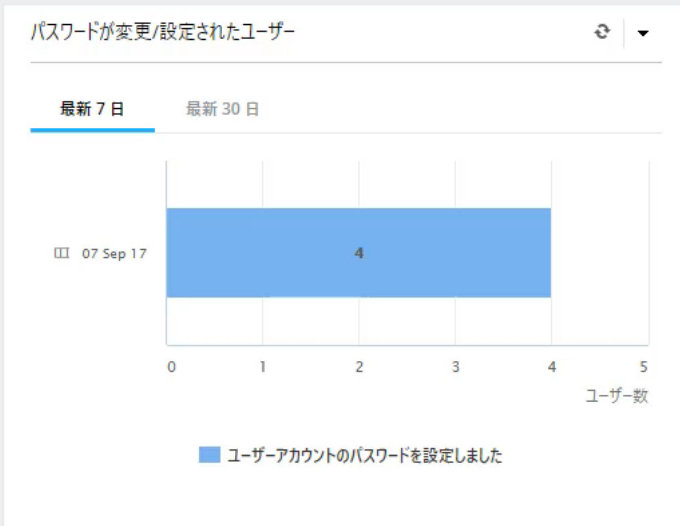
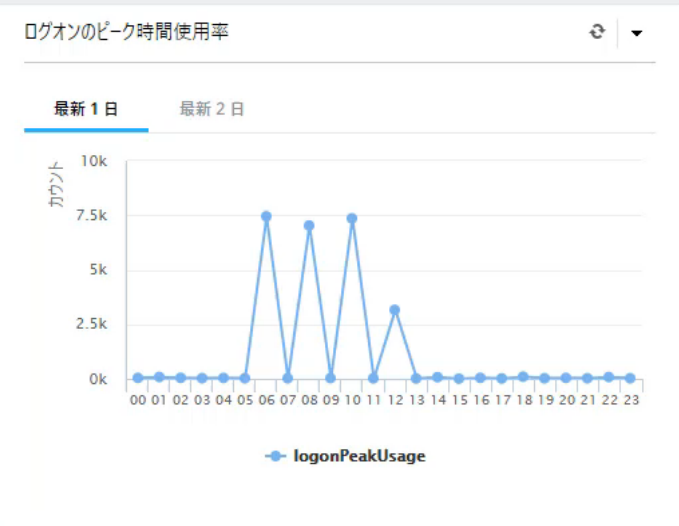
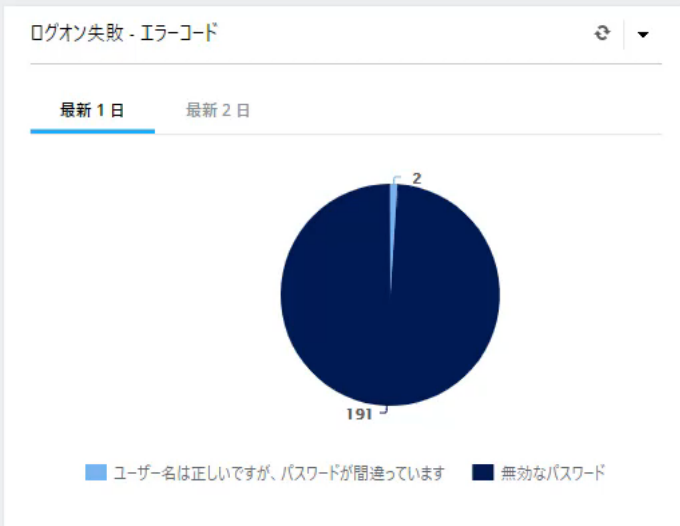
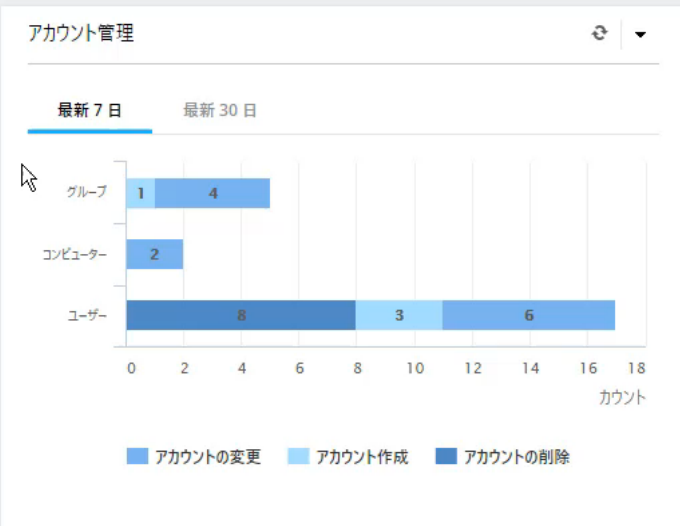
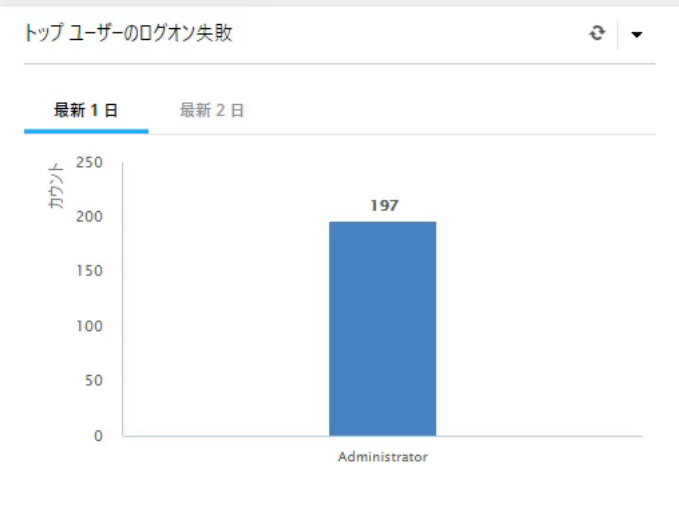
📊 グラフ表示

📄 概要表示

🔍 アーカイブ済みデータの検索

ドメインmetech.local

最終スケジュール時刻: 2017/09/14 6:00:00 [すぐに実行する](#)



🔔 アラート [更新](#)

🚫 重要

🚨 障害

⚠️ 注意

🔔 最近のアラート [全て見る](#)

ローカル管理者アカウントのパスワード変更を監査

グラフ表示

概要表示

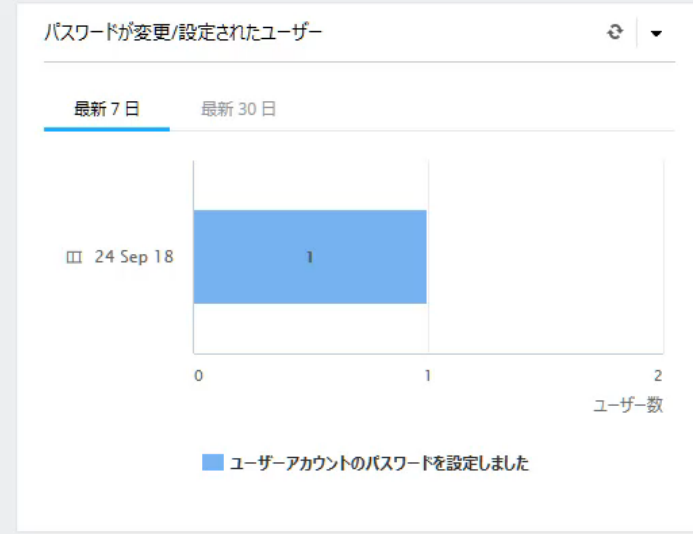
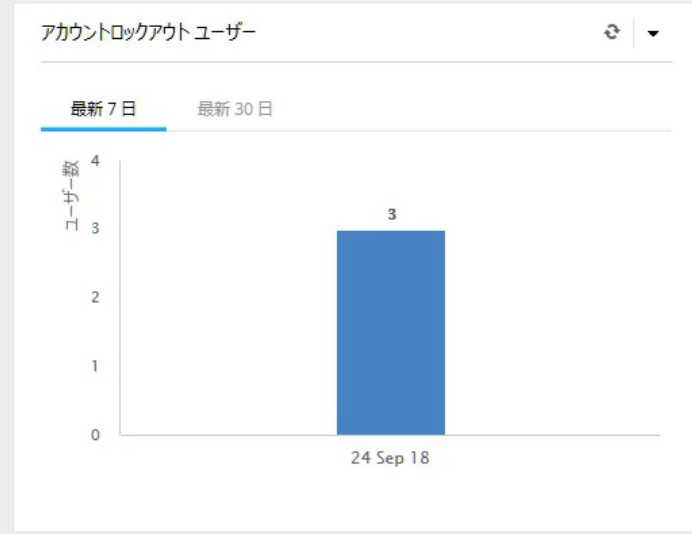
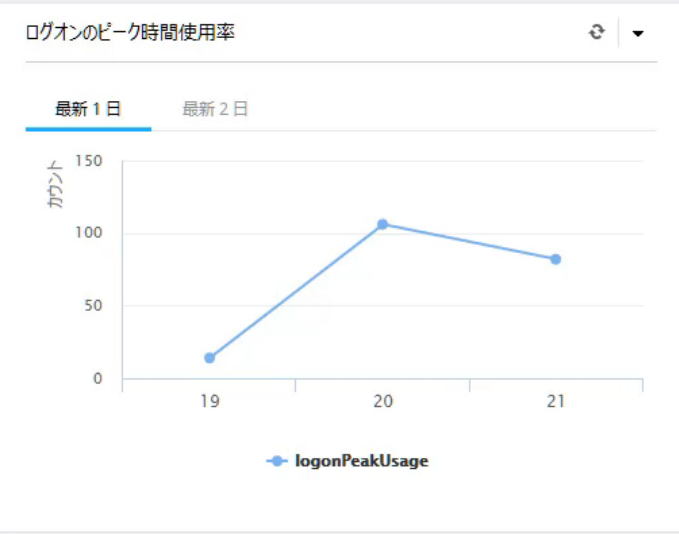
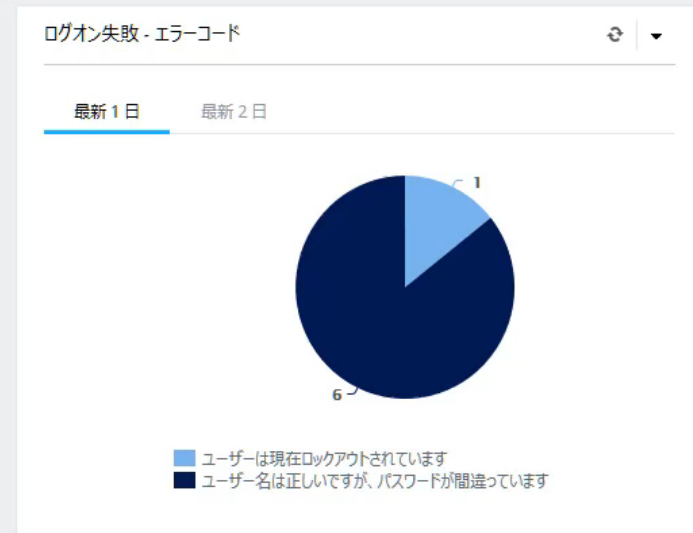
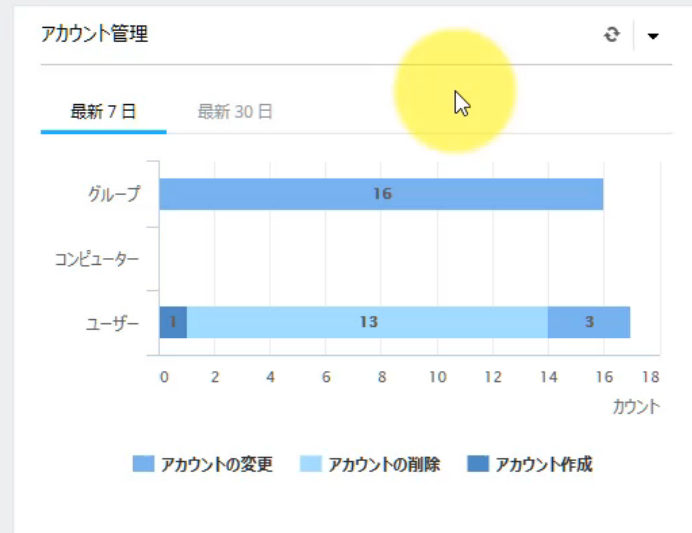
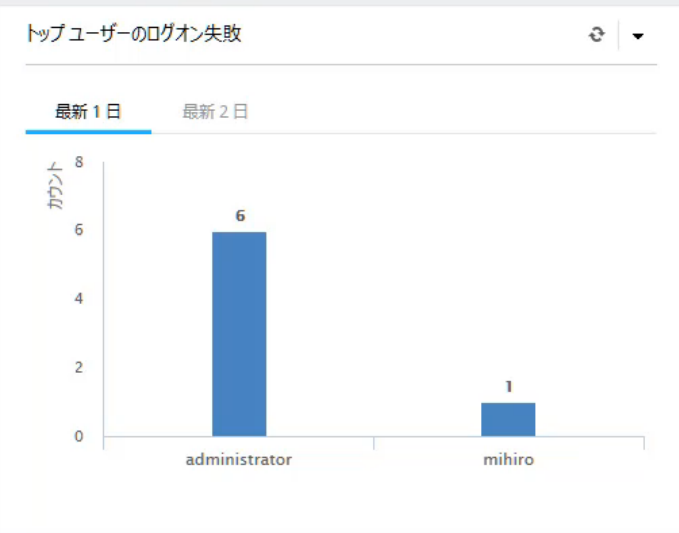
アナリティクス

ディスク使用量を削減

アーカイブ済みデータの検索

ドメインmetech.local

最終スケジュール時刻: 9/24/2018 09:07:03 午後 [すぐに実行する](#)



アラート

重要 4

障害 28

注意 8

最近のアラート

全て見る

METECH\administratorがドメインのローカルセキュリティグループAdministratorsにメンバーCN=前田 美裕,OU=zoho,DC=metech,DC=localを追加しました
9/24/2018 09:05:55 午後

METECH\administratorがドメインのローカルセキュリティグループAdministratorsからメンバーCN=前田 美裕,OU=zoho,DC=metech,DC=localを削除しました
9/24/2018 09:05:05 午後

MIHIRO-SURFACEにおいてユーザーadministratorがログインに失敗しました。理由: ユーザー名は正しいですが、パスワードが間違っています
9/24/2018 08:45:52 午後

MIHIRO-SURFACEにおいてユーザー

Administratorによるログオン失敗をアラート検知

導入事例

累計**3,500**社以上の企業での導入実績

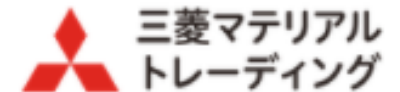
導入業界

- 電機
- 精密機械
- 家電
- 化学
- 繊維
- 鉄鋼
- サービス
- IT
- 通信
- 金融
- 建築
- 不動産
- 電力
- ガス
- 石油
- 外食
- エンターテインメント
- 物流
- 運送
- 食品
- 飲料
- 自動車
- バイク
- 重工業
- プラント
- 建築機械
- 家庭用品
- 製薬
- 化粧品
- アパレル
- 商社
- 小売
- テレビ
- 広告
- 出版
- 印刷
- 地方公共団体
- 学校

お客様の声

三菱マテリアルトレーディング様

- 月次レポート作成時間が半減
- 安定した稼働



様々な業界、企業規模でご利用いただいております

価格



年間ライセンス

39.8万円/年～

サポート付

= 月々約33,170円～

- 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれています。
- 1年ごとに年間ライセンス契約を更新します。



通常ライセンス

98万円～

初年度サポート付

- 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれています。
- 2年目以降は1年ごとに年間保守サポートサービス契約（16.3万円～）を更新します。

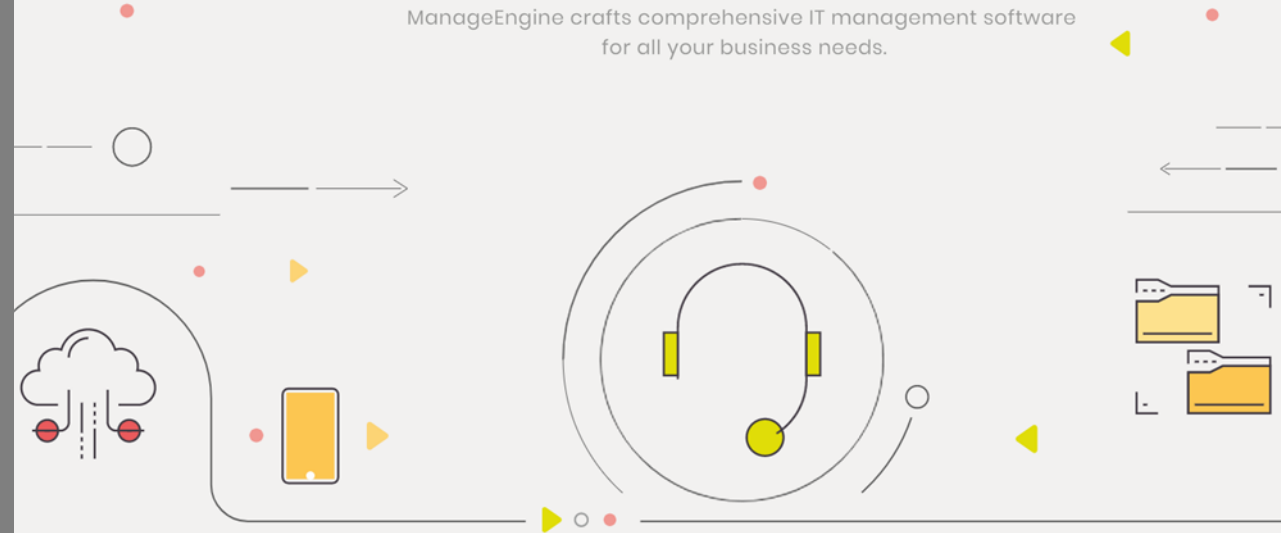
詳細な価格表についてはこちらをご参照ください：https://www.manageengine.jp/products/ADAudit_Plus/pricing.html

ご要望に応じて、好きなライセンス体系をお選びいただけます

EventLog Analyzer のご紹介

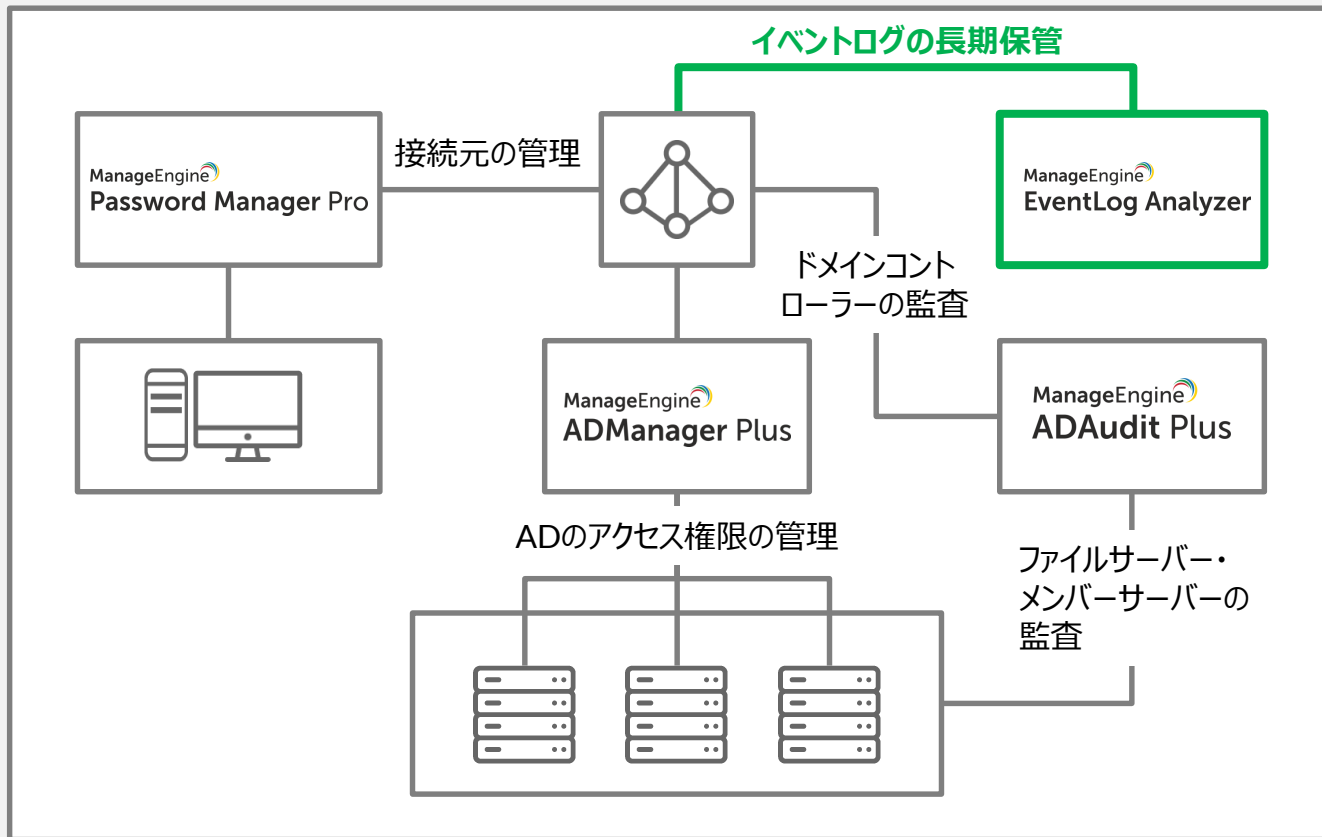
Bringing IT together

ManageEngine crafts comprehensive IT management software
for all your business needs.



ADセキュリティ対策製品：EventLog Analyzer

ManageEngine

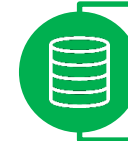


ManageEngine EventLog Analyzer

- Active Directoryへの攻撃時に発生するイベントログの可視化することで、攻撃を早期検知



包括的なイベントログ管理



ログの長期保管

ADAudit PlusとともにActive Directoryへの攻撃を早期検知

イベントログ・Syslogなどの管理についてよくお聞きするお悩み事

エージェントを
インストールせずに
監視したい

異なるフォーマットの
ログをまとめて
管理したい

不正な操作を
把握する
仕組みがない

セキュリティ事故
発生時のログ調査や
原因究明に
時間がかかる

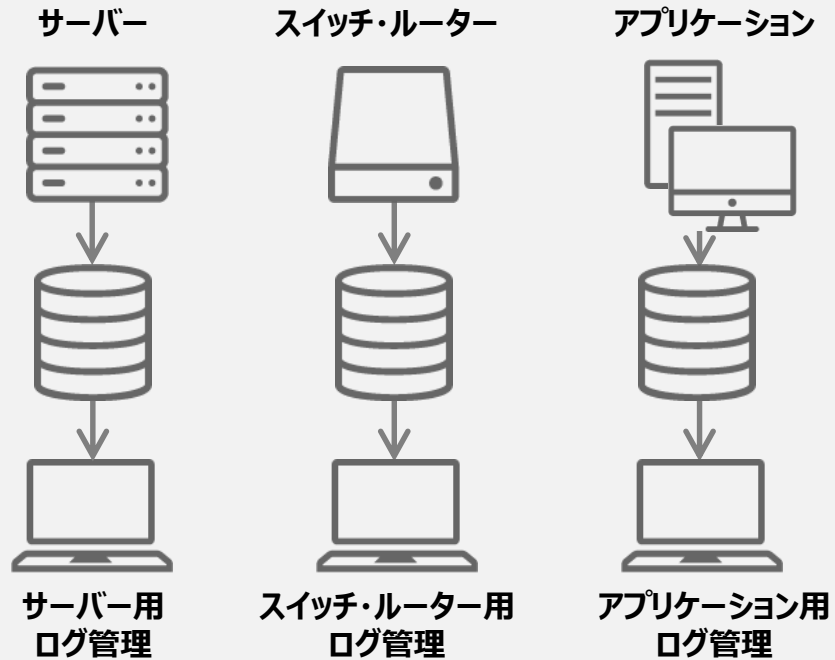
定期報告のための
レポート作成に
時間がかかっている

ログを長期間
保存しておきたいが
容量上難しい

多くの企業がイベントログ・Syslogなどの管理に関して苦労されています

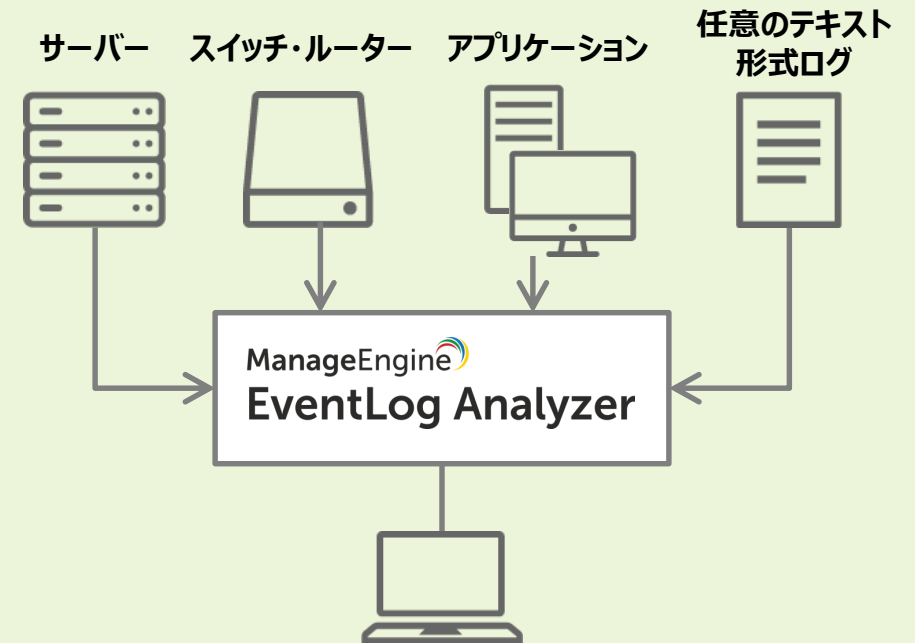
あらゆるログをエージェントレスで一元管理

EventLog Analyzer 導入前



- 機器ごとに個別にログを管理

EventLog Analyzer 導入後



- イベントログ、Syslog、アプリケーション独自のログ、その他任意フォーマットのテキスト形式のログをエージェントレスで一元管理

イベントログ・Syslogなどの管理工数が激減

優れた検索機能

EventLog Analyzer 導入前



- ログの保管機能がメインで、検索する機能がほとんどない
- 報告用のレポートはあるものの、障害の原因追求には適していない

EventLog Analyzer 導入後



- ログの一元管理により、時系列で複数の機器の状態を検索
- イベントIDやメッセージ、接続元や接続先、ユーザー名などを検索可能
- Webベースでわかりやすく、マニュアルを熟読しなくとも直観的に利用できる

セキュリティ事故発生時のログ調査や原因究明の迅速化



導入事例

累計**5,300**社以上の企業での導入実績

導入業界

- 電機
- 精密機械
- 家電
- 化学
- 繊維
- 鉄鋼
- サービス
- I T
- 通信
- 金融
- 建築
- 不動産
- 電力
- ガス
- 石油
- 外食
- エンターテインメント
- 物流
- 運送
- 食品
- 飲料
- 自動車
- バイク
- 重工業
- プラント
- 建築機械
- 家庭用品
- 製薬
- 化粧品
- アパレル
- 商社
- 小売
- テレビ
- 広告
- 出版
- 印刷
- 地方公共団体
- 学校

地方自治体/官庁

- 埼玉県ふじみ野市
- 北海道千歳市
- 内閣法制局 など



企業・組織

- 株式会社ベネフィット・ワン
- ガンホー・オンライン・エンターテイメント株式会社
- 株式会社ジィ・シー企画
- J-PARC（大強度陽子加速器施設） など

様々な業界、企業規模でご利用いただいております

価格



年間ライセンス

16.1万円/年～

サポート付

=ひと月あたり約13,500円～

- 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれています。
- 1年ごとに年間ライセンス契約を更新します。



通常ライセンス

48.3万円～

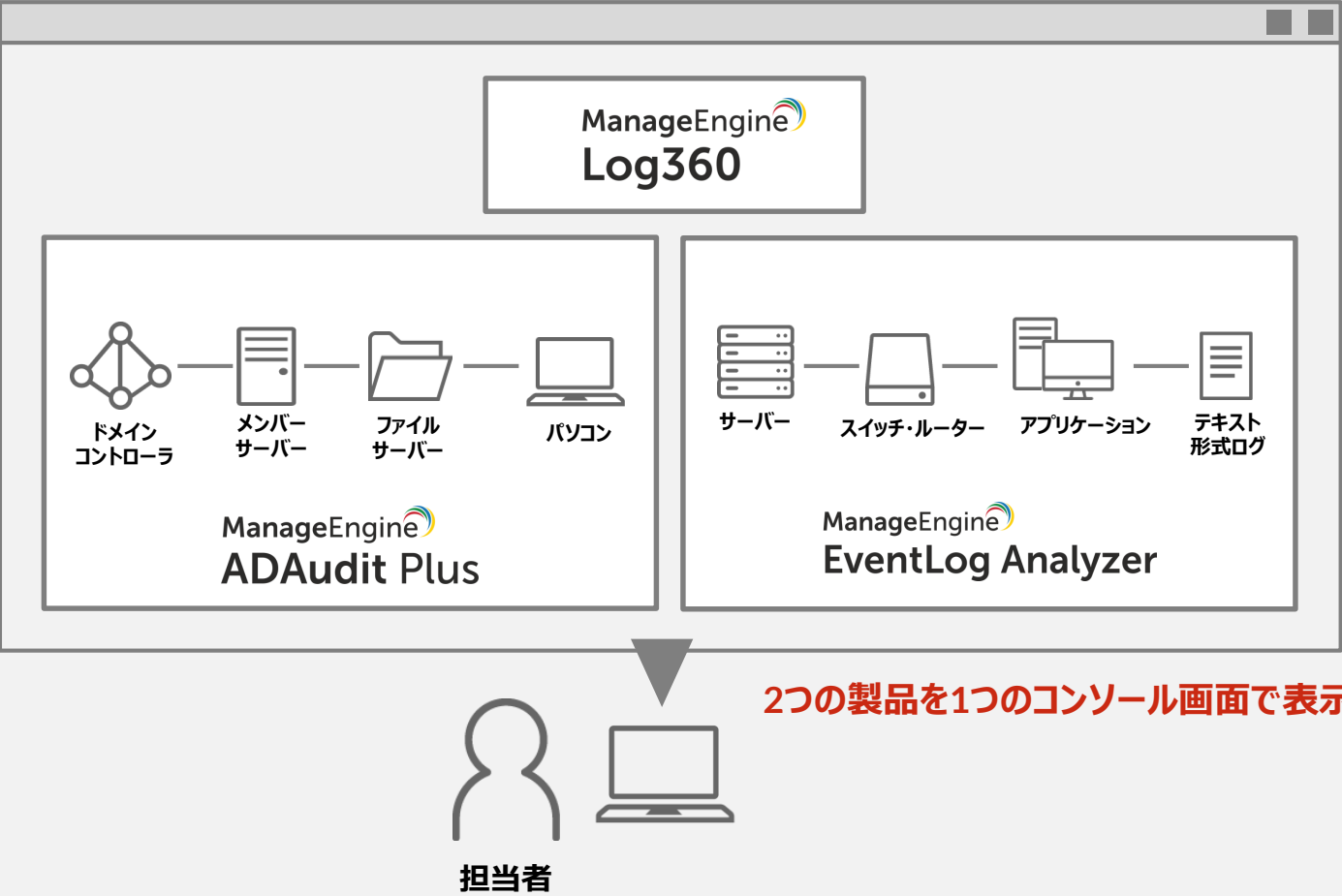
初年度サポート付

- 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれています。
- 2年目以降は1年ごとに年間保守サポートサービス契約（8.2万円～）を更新します。
- 6年以上利用する場合は、価格が抑えられます。

詳細な価格表についてはこちらをご参照ください：https://www.manageengine.jp/products/EventLog_Analyzer/pricing.html

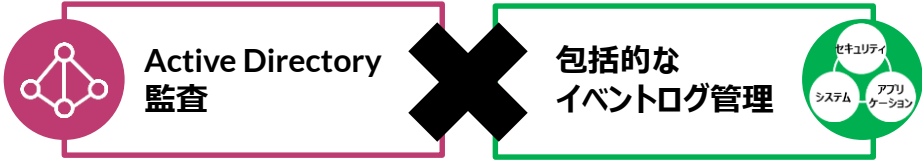
ご要望に応じて、お好きなライセンス体系をお選びいただけます

簡易SIEM製品 : Log360



ManageEngine Log360

- ADAudit PlusとEventLog Analyzerの機能を包括することで簡易SIEMとしての機能を提供

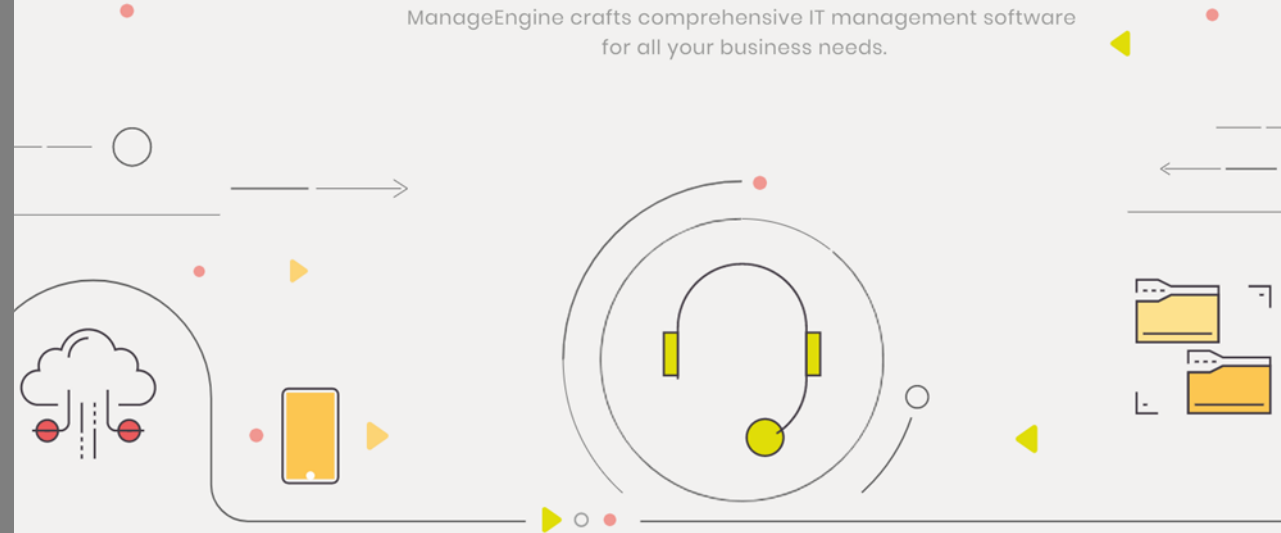


ADAudit PlusとEventLog Analyzerの2製品を統合

さいごに

Bringing IT together

ManageEngine crafts comprehensive IT management software for all your business needs.



さいごに： ADの特権ID保護に関する製品のまとめ



Active Directoryへの攻撃を防止

ManageEngine

ADManager Plus



Active Directoryの特権ユーザーのアクセスを管理

ManageEngine

Password Manager Pro



Active Directoryへの攻撃を早期に検知

ManageEngine

ADAudit Plus

ManageEngine

EventLog Analyzer



製品提供元

ゾーホージャパン株式会社



神奈川県横浜市西区みなとみらい三丁目6番1号
みなとみらいセンタービル13階

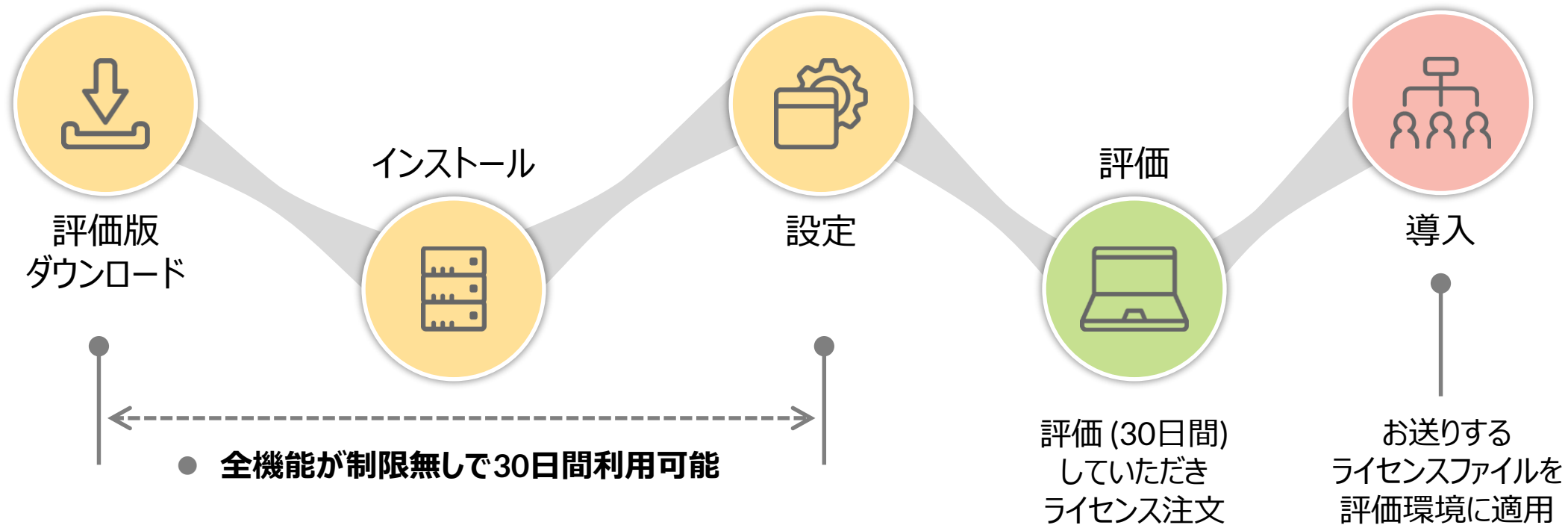
045-319-4612 (ManageEngine 営業担当)

<https://www.manageengine.jp/>

jp-mesales@zohocorp.com

Active Directoryのセキュリティをトータルに向上します

さいごに：導入ステップ°



まずは評価版でお試ください

さいごに：オンライン相談のご案内

製品に関する詳細な説明・デモをご希望の方

オンライン相談

にお申し込みください。

https://www.manageengine.jp/online_meeting/

ManageEngine オンライン相談

検索



購入相談専用窓口 オンライン相談

ManageEngineでは、製品の詳細を知りたい方向けに「オンライン相談」のお申込みを受け付けております。
お気軽にご利用ください。

こんな方におすすめです

製品導入を検討するため、説明を受けたい。

実際の画面や使用感を見てみたい。

口頭で細かいニュアンスの質問をしたい。



訪問説明とほぼ同じ内容をご提供できます！

お申込みフォーム

