SentinelOne

セキュリティ担当者の運用負荷を解放する

Singularity Platform

EPP + EDR

IT管理

- USB制御
- パーソナルファイアウォール
- ITハイジーン
- 脆弱性管理

エンドポイント保護

- 静的検知
- AIによる振る舞い検知
- Windows MAC Linux
- Cloud Servers Containers
- iOS Android Chrome

インシデント対応・調査

- イベント分析
- 修復 ロールバック
- AIアナリスト
- カスタム検知ルール

ITDR

ID保護

- Active Directoryのリスク低減
- 認証情報の保護

MDR

サービス

- 24/265 監視
- インシデントレスポンス
- リスクアセスメント
- 運用支援

AI SIEM (Data Lake)

- ログの保管
- 可視化・分析
- 3rdParty製品連携

Marketplace

Identity / EMAIL / CASB / SASE / Web / Threat Intel / Sandbox / Firewall

SentinelOneを導入する3つのメリット

EDRに注目が集まる一方で、同製品が発するアラートの分析や対処には専門性が求められ、扱いづらいという課題があります。そうした課題を解消するのが、洗練されたAIを活用した防御と検知、高度な自動対応機能を備える自律型エンドポイントセキュリティ製品であるSentinelOneです。

多段のエンジンで高い検知力を実現

ファイル構造解析（NGAV）、振る舞い検知エンジン（EDR）を標準実装しています。　そのため、近年流行しているランサムウェアやファイルレス攻撃に対しても高い防御力や検知力を有します。第三者評価MITRE　Engenuity ATT&CK　Evaluationsでは検知漏れ0%を示しています。

専門的なスキルがなくても運用が可能

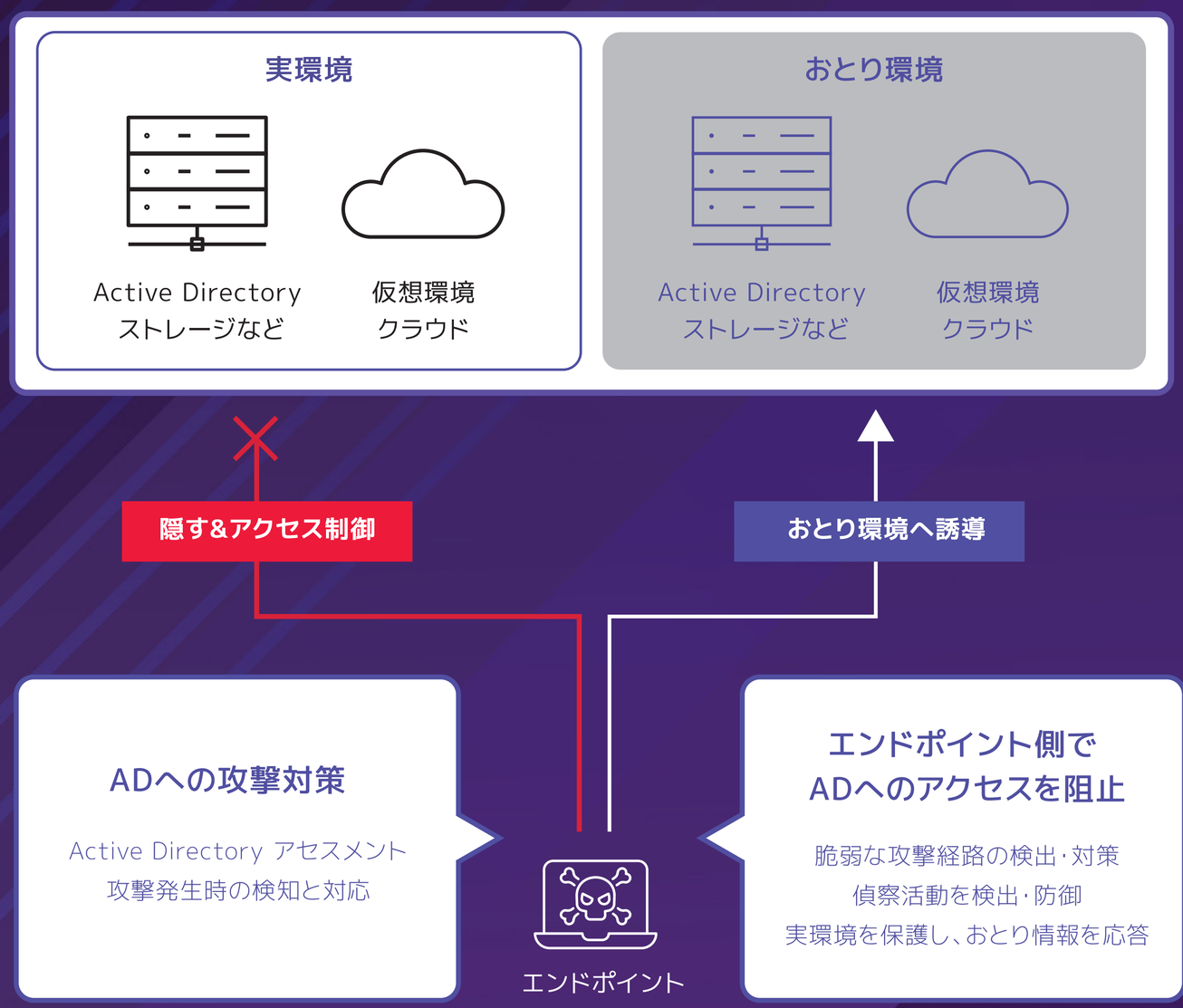
ポリシー設定がシンプルで、複雑なチューニングは不要。インストール後速やかに運用を開始できます。クラウド管理コンソールの利用により、煩雑なサーバー管理やシグネチャの管理が不要です。
また、管理コンソールは日本語表示に対応しています。

人手に頼らないインシデント対応で負荷を軽減

端末内の挙動分析が自動化されているため、高度な攻撃も自律的かつ即時に対応可能。検知・防御・隔離まで一貫して実行します。
さらに万が一、汚染や暗号化をされた場合でもワンクリックで元通りにできる修復機能を実装しているため速やかに業務を継続することができます。

Singularity Identity

「おとり」技術により、攻撃者が侵入を試みる様々な対象を保護



Singularity Identity の特徴

Active Directoryの脆弱性を簡単な操作で修復

パスワードスプレー攻撃などへの対策として、AD の脆弱性や構築ミスの検出を行い、容易な修正手順を提供します。

Active Directoryに対する高度な攻撃を検知し防御

AD アクティビティに対する詳細なモニタリングと行動分析により、Kerberos 攻撃などの高度な攻撃に対して検知・防御が可能です。

「おとり」機能を用いて資格情報へアクセスさせない

エンドポイント内での偵察活動に対して、おとり機能を使用し、実在しない AD に対してアクセスさせます。同時に、実際の認証情報へのアクセス制限を行い、実環境への攻撃自体を抑止します。

統合管理

XDR 製品と同一コンソールによる一元管理が可能です。検知した脅威の駆除、変更されたシステムやユーザーデータを復旧させることができます。

Singularity Data Lake

企業全体の可視化と制御を実現AIでリアルタイムにデータを活用

SentinelOne XDRの特徴

全体像の可視化と分析

エンドポイントやネットワークの活動を詳細に可視化し、攻撃の原因を分析することでインシデントの全体像を把握し、再発防止策を講じることができます

AIによる高度な脅威検知と対応

AIエンジンを用いることで、従来のシグネチャベースでは検知できない未知の脅威も自動で検知し、即座に防御。対応にかかる時間を大幅に短縮し、被害を最小限に抑えます

カスタム検知ルール

組織固有の検知ルールやセキュリティポリシーを設定し、異常な行動を監視することで、潜在的な脅威を早期に発見することが可能です

統合管理

セキュリティイベントをひとつのプラットフォームで一元管理することで運用効率を向上させ、管理の手間を削減します