semperis

DIRECTORY SERVICES PROTECTOR

業界で最も包括的なハイブリッド Active Directory 脅威検知・対応プラットフォーム

Semperis Directory Services Protector(DSP)は、オンプレミスのADとEntra IDを含むハイブリッドAD環境全体を継続的に監視し、改ざん不可能な変更追跡、サービスアカウント保護、悪意ある変更の自動ロールバックを備えた比類ない可視性によって、ハイブリッドADセキュリティを"自動運転"で実現します。

- オンプレミスのADとEntra IDへの攻撃者のアクセスを阻止
- オンプレミスのADとEntra IDにおける不要な変更を自動で修復
- ADのセキュリティ体制を継続的に検証
- サービスアカウントを検出・監視し、継続的に保護
- サービスアカウントの不正利用を検知し、セキュリティギャップを解消

ハイブリッドADが安全でなければ何ひとつ安全ではありません

オンプレミス/クラウドを問わず、業務アプリケーションはADとEntra IDに依存しており、これらはお客様のITインフラを構成する重要なコンポーネントです。
しかし、ADのセキュリティ確保は、絶え間ない変化、膨大な数の構成設定、人とマシンのアカウントの拡散、そしてますます巧妙化する脅威環境などにより、困難を極めています。

ハイブリッド環境の保護には、さらなる課題があります。多くの攻撃はオンプレミスから始まり、その後クラウドへと横展開していくためです。
Semperis Directory Services Protector(DSP)は、ADとEntra IDの脆弱性を継続的に監視し、オンプレミスとクラウド双方のアクティビティを単一画面で可視化するとともに、ADとEntra IDにおける不要な変更を自動的に修復します。

サイバー攻撃からADとEntra IDを積極的に保護します

攻撃者より先にADとENTRA ID の脆弱性を発見

ハイブリッドAD環境の弱点を狙う攻撃手法は刻一刻と巧妙になっています。
まずオンプレミスADの脆弱性を悪用して環境内に侵入し、その後Entra IDへと横展開していきます。

→ DSPは、Semperis脅威調査チームによって発見された、ADおよびEntra IDを脅かす露出および侵害の兆候を継続的に監視します。

ハイブリッドACTIVE DIRECTORYセキュリティの盲点を排除

脅威アクターは強力な攻撃ツールを使用してバックドアを作成し、ハイブリッドActive Directory内部に永続的なアクセスを確立することで、従来のSIEMソリューションによる検出を回避します。

→ DSPは、ADレプリケーションストリームを含む複数のデータソースを使用して、エージェントベースまたはログベースの検出を回避する変更を

迅速な復旧を実現

侵入者や不正な管理者は、人手では監視・対処しきれない規模とスピードで、システム全体に深刻な被害をもたらす可能性があります。

→ Semperis DSPは、オンプレミスのADおよびEntra IDに対する、悪意のある変更を自動的にロールバックします。Entra IDの変更については手動でのロールバック機能も提供します。さらに、ハイブリッドAD環境全体の変更を相関的に把握できる、統合ダッシュボードを提供します。

semperis

ハイブリッドIDシステムは今まさに攻撃の標的となっています

Active DirectoryとEntra IDの両方を抱えるハイブリッドなIDシステムは、オンプレミス資産とクラウドサービスを最適な組み合わせで活用する企業の増加に伴い、いまや一般的な形態になりつつあります。
しかし、その柔軟性の裏側では複雑性も増大しており、特にMicrosoft環境におけるハイブリッドなIDセキュリティの管理は一層難しくなっています。
Microsoft Digital Defense Report 2023によると、インシデントレスポンスチームが明らかにした代表的なセキュリティギャップとして、「オンプレミス管理とクラウド管理の間に存在するセキュリティ境界の破綻」が挙げられており、これが初期侵入、ラテラルムーブメント(横方向への侵害拡大)、および永続的な潜伏を可能にしています。

ハイブリッド環境では潜在的な攻撃対象領域が拡大します

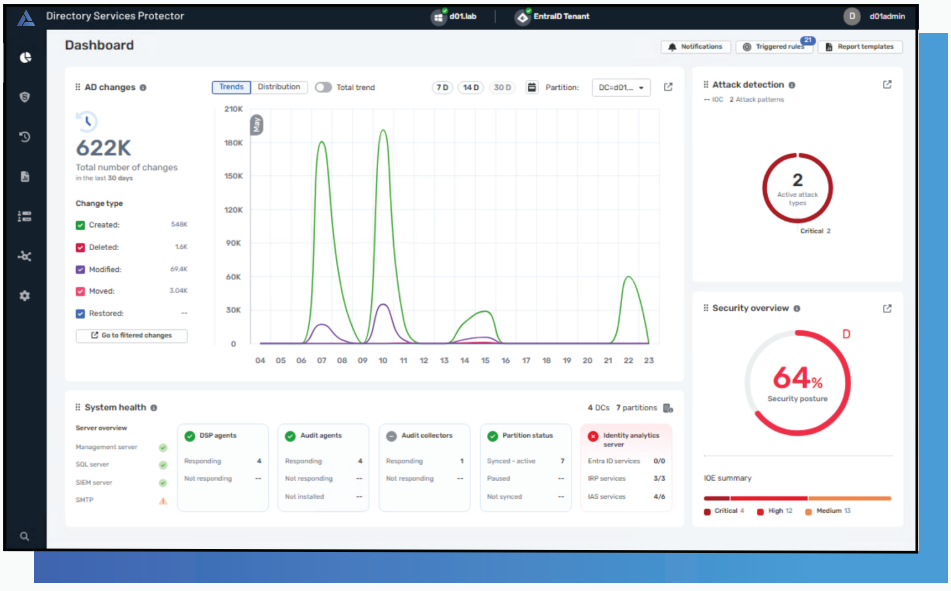
Entra IDはセキュリティ環境の重要な構成要素であるため、ハイブリッドIDモデルを採用する組織は、多種多様な侵入経路の可能性に備えて防御を行う必要があります。
Directory Services Protectorは、Entra IDの変更追跡、不正な変更の自動修復、Entra ID向けのカスタマイズ可能なアラート/レスポンスルール、オンプレミスのADとEntra IDの両方における変更の相関関係を可視化する統合ビューの提供を通じて、ハイブリッドAD環境を保護します。

Directory Services ProtectorによってADとEntra ID 全体のセキュリティ状況を簡単に追跡

ハイブリッドAD全体のセキュリティ状況を明確に可視化し、ADおよびEntra IDに対する脅威検知と対応を管理：

- リスクスコアリングと個々のセキュリティカテゴリへのドリルダウンによる詳細な分析機能により、セキュリティ体制全体を評価・伝達
- サービスアカウント、権限、認証プロトコルの弱点、AD インフラの姿勢、EntraおよびIDの権限など、ADとEntra IDのあらゆる側面をカバーするセキュリティ指標により、重要なインテリジェンスを獲得
- 優先度付けされた修復ガイダンスと自動修復機能を使用し、Entra IDとADの攻撃対象領域を削減
- Entra IDとオンプレミスADの変更を単一のハイブリッドビューで可視化し、相関分析
- SIEMなどの従来のログおよびイベントベースの監視をすり抜ける高度なAD攻撃を検出

オンプレミスのADとENTRA IDの両方に対して1つのソリューションで脆弱性評価/変更追跡/修復



semperis

脆弱性評価

ハイブリッドAD環境のセキュリティ侵害につながる可能性のある曝露指標(IOE)を継続的に監視
セキュリティ研究者コミュニティが提供する組み込みの脅威インテリジェンスを活用

サービスアカウント保護

サービスアカウント向けに特化したセキュリティインジケーターを使用し、ADサービスアカウントを完全に可視化、変更を監視、不正利用を検知し、セキュリティギャップを解消する

自動修復

悪意ある変更の取り消し・削除・無効化・リセットを行う自動レスポンスルールにより、管理作業の負荷を軽減し、手動介入なしで迅速に対応

POWERSHELLサポート

DSPのPowerShellモジュールを使用して各種プロセスを自動化し、既存のツールセットにDSP の運用・管理を統合

きめ細かなロールバック

オンプレミスのADおよびEntra ID内の個々の属性、グループメンバー、オブジェクト、コンテナへの変更を、直前のバックアップだけでなく任意の時点まで復元

改ざん防止トラッキング

セキュリティログが無効化されている場合やログが削除されている場合、エージェントが無効化または停止している場合、あるいは変更がADまたはEntra IDに直接挿入された場合でも、変更を記録

SIEM連携強化

SplunkおよびMicrosoft Sentinelとの標準連携により、セキュリティインシデントおよびイベント管理(SIEM)システムの盲点を排除

委任

堅牢なロールベースアクセス制御(RBAC)と豊富な機能を備えたWeb UIを活用し、管理者は特定の制御範囲において、表示と復元を行うことが可能

フォレンジック分析

不審な変更を特定し、侵害されたアカウントによる変更を切り分けるなど、高度な分析が可能
DSPが収集したデータを活用し、デジタルフォレンジックおよびインシデント対応(DFIR)業務をサポートし、インシデントの発生源と詳細を追跡

リアルタイム通知

ハイブリッド AD 環境で発生する運用上・セキュリティ上の変更を、メール通知でリアルタイムにアラート受信

ENTRA IDの変更監視と対応

ロールの割り当て、グループメンバーシップ、ユーザー属性の変更をほぼリアルタイムで追跡
カスタマイズ可能なアラートルールにより不審なアクティビティを検出し、自動で対応することで、IDセキュリティを強化

強力なレポート機能

ADの専門家が作成した組み込みレポートにより、ハイブリッドAD環境の運用状況、ベストプラクティス、コンプライアンス、およびセキュリティ面のインサイトを獲得
さらに、高度なLDAPおよびDSPデータベースクエリに基づいてカスタムレポートを作成

継続的なセキュリティ検証

自動監視を使用して、構成ドリフト(時間の経過とともに蓄積される、侵害された構成設定、攻撃に対して脆弱な状態)によるセキュリティ態勢の回帰に対処

ENTRA ID変更の追跡

ほぼリアルタイムの変更追跡を使用し、ロール割り当て、グループメンバーシップ、ユーザー属性の変更を監視

セキュリティフレームワークとの整合性

セキュリティ指標を、MITRE ATT&CKやMITRE D3FENDなどを含む業界標準のセキュリティフレームワークにマッピング

ハイブリッドADセキュリティの可視化

Entra IDで発生した変更を簡単に確認でき、ハイブリッドビューを通じてオンプレミスADとEntra ID間の変更を相関して可視化

運用中のハイブリッドAD環境は本当に"安全"ですか？

Microsoft Digital Defense Report 2023 によると、インシデント対応チームは、対応案件の 43% で安全でないAD構成を発見しています

Semperis
ITレジリエンスオーケストレーション

5 ★★★★★

出展：Gartner Peer Insights

DSPは、セキュリティの問題だけでなく、今まではできなかった(もしくは簡単にはできなかった)AD内で行われた変更の監査という点でも、貴重な見識を得るのに役立ちました

大手製造業のAD管理者
(G2では、DSPに関する他のレビューもご覧いただけます)

info@semperis.com
www.semperis.com

Semperis 本社
5 Marine View Plaza
Suite 102
Hoboken, NJ 07030

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)

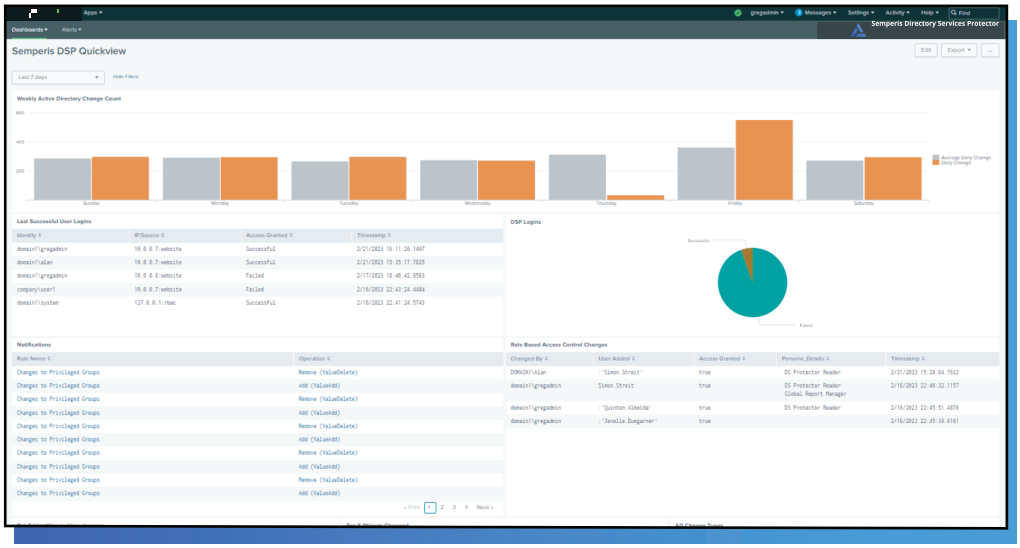
SIEMに可視性を

セキュリティ監査をすり抜ける攻撃の急増

Semperis DSPは、セキュリティログや各DC上のエージェントのみに依存する追跡ツールとは異なり、ADレプリケーションストリームを含む、複数のデータソースを監視します。
ADレプリケーションストリームは、攻撃者がどれほど巧妙に痕跡を隠そうとしても、ディレクトリ上のすべての変更を漏れなく捉えるための、唯一の信頼できる情報源です。
Semperis DSPは、不審なADの変更を意味のあるコンテキストとともにSIEMシステムへ転送するので、セキュリティアナリストの負荷を大幅に軽減します。
Microsoft SentinelやSplunkなどのSIEM/SOAR製品向けに用意された定義済みアラートを利用できるほか、SecOpsツールやServiceNowなどのチケッティングシステム向けにカスタムアラートを作成することも可能です。

標準搭載のSIEM統合

DSPは、標準搭載の統合機能により、これまで見えなかったADセキュリティ情報を、SentinelおよびSplunkユーザーが使い慣れたビューで可視化することで、脅威の検出と対応を簡素化します。



DSPは、ハイブリッドActive Directoryのセキュリティデータを、使い慣れたSplunkビュー上に表示します

splunk> Microsoft Sentinel

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/
本社：〒150-6234 東京都渋谷区桜丘町１番１号 渋谷サクラステージ SHIBUYA タワー 35 階
名古屋：〒451-0045 愛知県名古屋市西区名駅 2-27-8 名古屋プライムセントラルタワー 8 階
大阪：〒530-0001 大阪府大阪市北区梅田 3-2-123 イノゲート大阪 17 階