ランサムウェア被害の拡大と IDセキュリティの重要性： Active Directory/Entra ID防御の最前線

東京エレクトロン デバイス株式会社

CN技術本部
カスタマーサクセスデザイン部
第4グループ
飯田 唯

本日のゴール

ID保護の必要性

- 近年のランサムウェア攻撃が、なぜID基盤を起点に事業停止まで至るのか

ITDRの役割

- EDRやバックアップ等の既存対策だけでは防ぎきれないID/権限まわりのリスク
- ITDRの役割

ITDRのベストプラクティスをSemperisで実現

- Semperisによる、具体的な予防 → 検知・自動修復 → 復旧のイメージ

ID保護の必要性

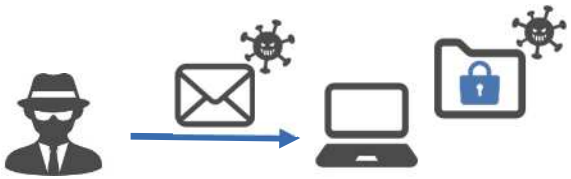
Ransomware攻撃の進化

攻撃者もROIを重視し、ターゲットの事業そのものを停める攻撃へ高度化

1 ファイル暗号化 型

不特定多数にばらまき

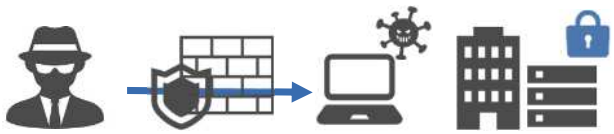
- PC1台のファイルを暗号化
  個々の被害者から身代金
  （1人=数万円～数十万円）
- 業務停止規模：小



2 法人標的 型

組織全体を狙い侵入

- 組織全体のサーバーを暗号化
  企業から高額身代金
  （1社で数千万円～数億円）
- 業務停止規模：中



3 AD制圧＋事業停止 型

営業停止を目的に脅迫

- データの暗号化＋公開を脅迫
  「二重/三重脅迫型」
  （数十～数百億円の損害）
- 業務停止規模：大

国内 ランサムウェア インシデント例

国内でも業務停止型の攻撃が急増、社会的なインパクトも大きい

国内でのインシデント例

- ネットワーク機器を経由してデータセンターのネットワークに侵入
  パスワードの脆弱性を突いて管理者権限を奪取
- アクセス権を認証するサーバーからランサムウェアが一斉に実行される
  起動中の複数のサーバーや一部のパソコン端末のデータが暗号化
- 約2カ月にわたりランサムウェア攻撃の封じ込め対応、システムの復元作業および再発防止を目的としたセキュリティー強化を実施
- 業務停止による多額の損害

ランサムウェア攻撃の傾向と対策

- 一般的に認証・権限基盤が狙われる
- AD/Entraを含むID基盤の防御が重要

（ADを守れない＝クラウドも含めた認証基盤が崩壊）

2025年に猛威を振るったランサムウェアグループ「Qilin」の犯行手口

▶ 内部侵入後にADを掌握し、基幹システムなど重要資産を暗号化する手口

Step1
初期侵入

▶ NW機器などから内部へ侵入
・漏えいしたID/PW、脆弱性から内部へ侵入
※フィッシングなどでIDを窃取されて販売されている

▼

Step2
権限昇格

▶ 特権ID偵察/AD掌握
・認証情報を取得
・ハッカーID作成や、特権昇格をさせられるか試行
→ドメイン構成やユーザー情報を偵察し、権限や稼働プロセス把握

▼

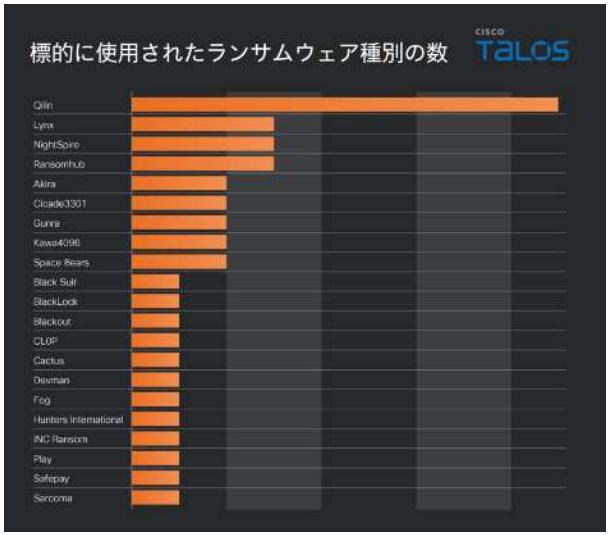
Step3
侵入拡大

▶ 攻撃範囲の拡大
・取得した認証情報を利用して対象システムへアクセス
・管理者権限を利用してEDRなどのセキュリティ製品を無効化

▼

Step4
データ盗取・暗号化

▶ システム・バックアップ・デバイス暗号化/身代金要求
・ダークウェブに情報公開、暗号化の二重脅迫が標準化



2025年上半期から被害件数が1.4倍
国内で最も被害を出しているのは「Qilin」
管理者権限を掌握されるケース増

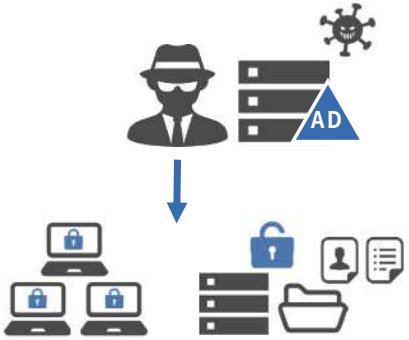
出展：
・https://gblogs.cisco.com/jp/2025/08/ransomware_incidents_in_japan_during_the_first_half_of_2025/
・https://rocket-boys.co.jp/security-measures-lab/qilin-ransomware-tactics-and-profile/

なぜADが狙われるのか？

ID基盤は、攻めるに易く甚大な被害を与えられるため、非常に狙われやすい

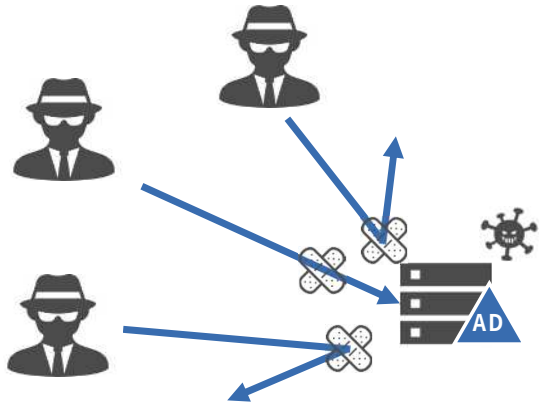
ADを狙う理由

- 認証・権限・アプリ・システムを統括する中枢基盤
- 一度攻撃者が管理者権限を得ると「企業全体の神」に
- 攻撃成功時のリターンが極めて大きい



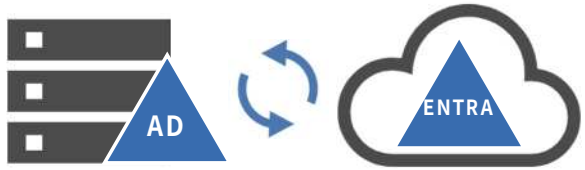
ADを取り巻く現状

- 2000年代の設計思想が現在も残存
- Kerberoasting / DCSync / Relay など攻撃手法は高度化
- パッチや設定のみでは防ぎきれない領域が存在



ハイブリッドの落とし穴

- 多くの企業は AD → Entra を同期
- ADが攻撃されると、Entraが踏み台になるケースも
- Entraが健全でも漏洩は防げない構造
- オンプレの脆弱性がクラウドまで波及する

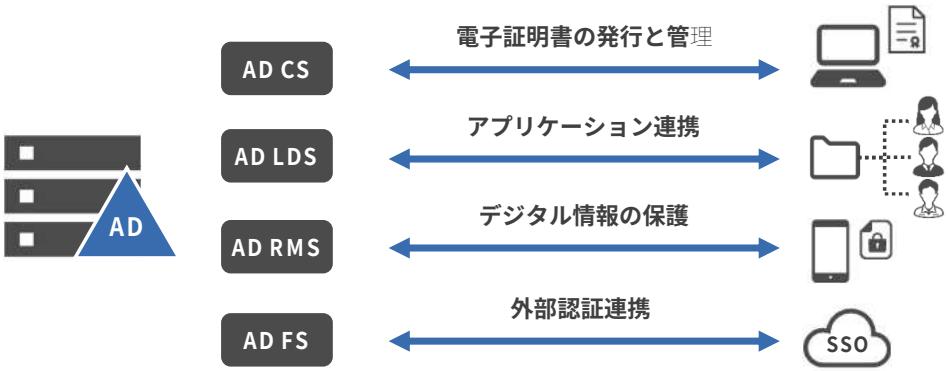


ADが抱える課題

既存対策に加え、ID基盤そのものを守る仕組みが必要

ADをなくせない理由

- 多くのシステムがオンプレADに依存し続けている
- Entraへの完全移行はコスト・改修が膨大
- レガシー資産・工場設備・Wi-FiなどもAD前提で動作
- 結果：ADは「なくせないもの」として存続し続ける



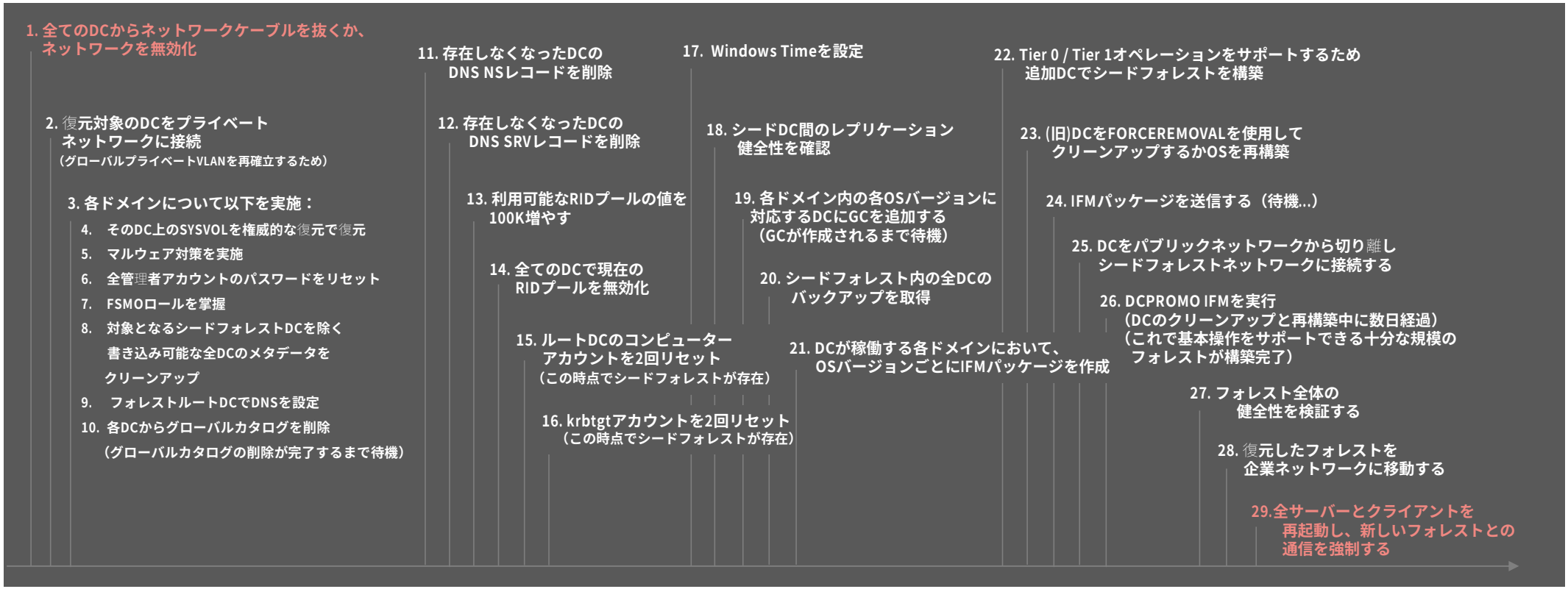
既存対策では止めきれない理由

- 中継攻撃・フィッシングが高度化しMFAを突破
- 正規IDを使われるとEDRでは異常検知が困難
- AD制圧後、EDRを無効化されるケースも
- IDそのものを守る基盤が必要

MicrosoftのAD復旧手順

業務復旧の足枷になる難解なAD復旧

- Microsoftが公開する汎用手順(29ステップ)、間違えると1からやり直し
- 復旧ステップを踏んでも、IDの整合性が取れず、復旧できない場合も多い
- ランサムウェア感染後、ADの復旧だけで3 ~4か月以上必要となる場合もあり



ADが止まる＝事業停止　その被害額は？

年商500億円規模の企業のケース

項目	内容	1 日あたりの影響額
① 売上損失	1日売上2億円×影響率（30～60%）	0.6～1.2 億円
② 人件費損失	従業員1,000名規模想定（中堅企業） 稼働40～80%停止	0.3～0.5 億円 （3,000～5,000万円）
③ 復旧・外部対応コスト（按分）	IR支援・復旧対応コスト：数千万円～ ※1日換算	0.2～0.4 億円 （2,000～4,000万円）
ブランド・法務（参考）	データ漏えい対応・顧客補償	案件依存（数千万～数億円）

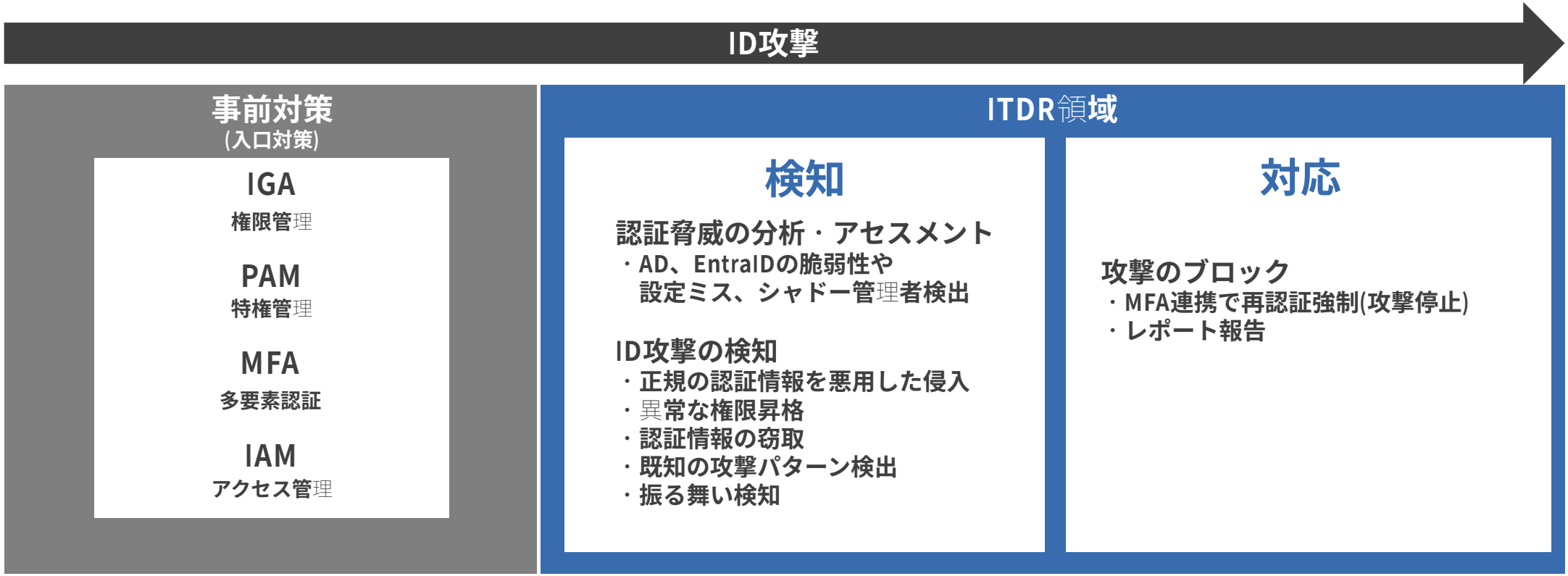
総損失額
（①＋②＋③）　**1.1 ～ 2.1 億円/日**

事業継続性担保のためにもID基盤の防御・即時復旧は必須

ID基盤を守る ITDR

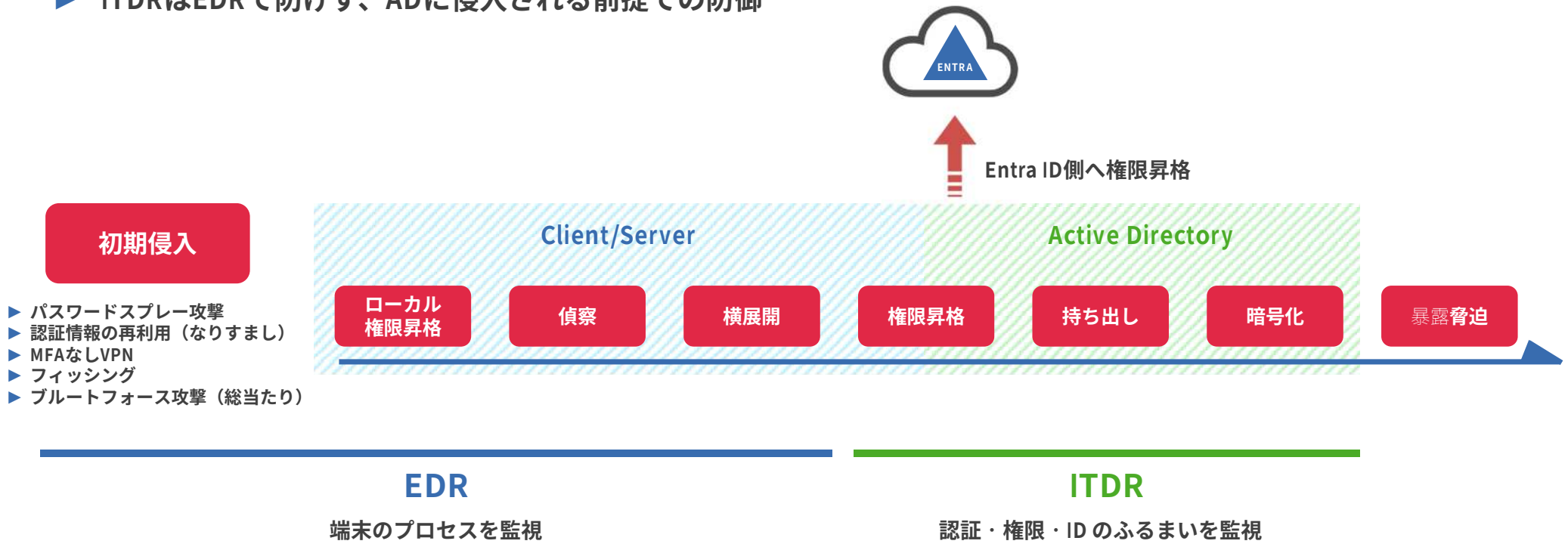
ITDRとは？

- ITDR (Identity Threat Detection and Response)
  - ADやEntra IDなどのIDインフラ上における認証トラフィック等の振る舞いを検知し、対応する新たなカテゴリー
  - ADなどに侵入されてしまったことを前提に、振る舞い検知＆対応するソリューション



EDRとITDRの違い

- EDRとITDRは併用する(互いに補完する)ソリューション
  - EDRとITDRは監視しているフェーズが異なる
  - EDRは境界型防御(FW)で防げず、端末に侵入される前提での防御
  - ITDRはEDRで防げず、ADに侵入される前提での防御



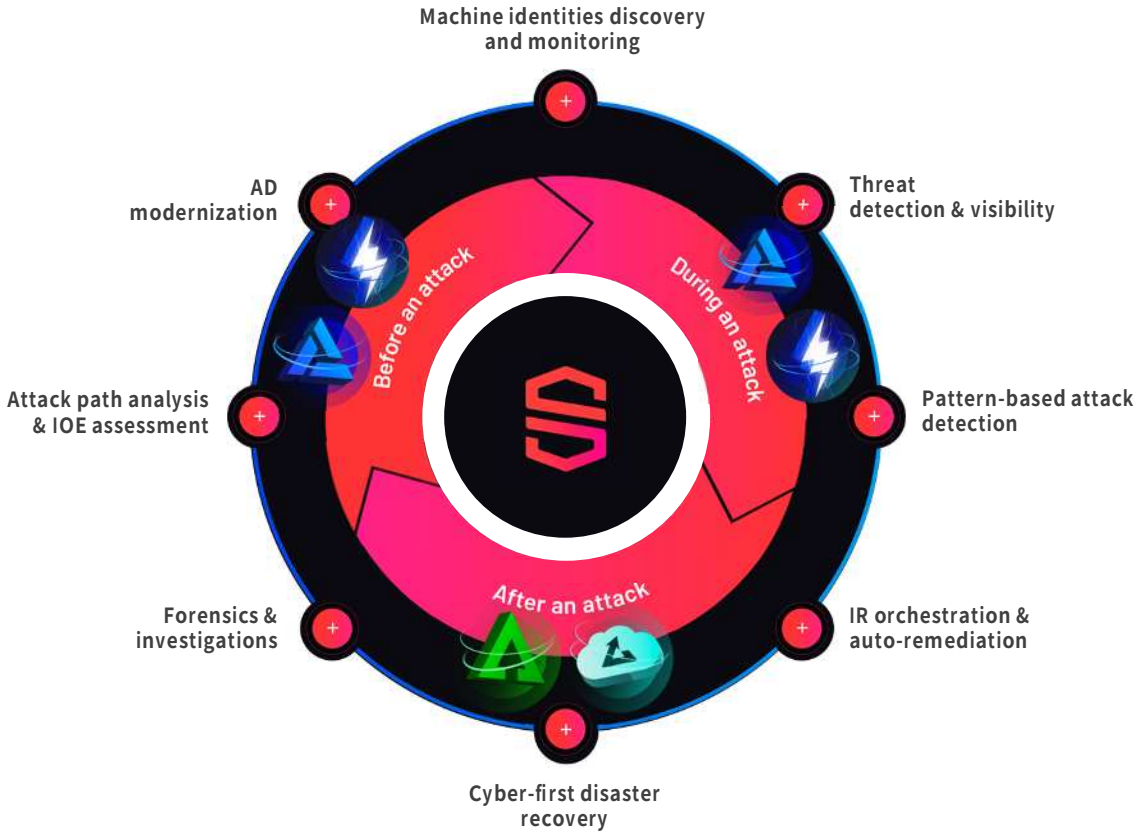
Semperis はITDRではなく “ITDRR ”

- AD/Entra IDの攻撃検知から復旧までを網羅するプラットフォーム

- ITDRR
  =Identity Threat Detection and Response, Recovery
  「アイデンティティ脅威の検知と対応＋復旧」

- AD/Entraの改ざん修復・暗号化時のリストアまで対応

- 攻撃を受けても「業務停止を回避」する設計



Semperis

Semperis 会社概要

社名	Semperis Inc.
本社住所	米国ニュージャージー州　ホーボーケン
設立	2014年
代表者	Co-Founder & CEO Mickey Bresman
従業員数	550+
主要株主	KKR, INSIGHT, TENELEVEN, PALADIN CAPITAL GROUP, AtriumHealth, WORLD TRADE VENTURES, SILVERTECH VENTURES, TPF TECH PIONEERS FUND
受賞その他	サイバーセキュリティ企業の成長率トップ5 4年連続で二桁成長を達成 Fortune「Cyber 60 2024」リストに選出

アイデンティティセキュリティ基盤への採用

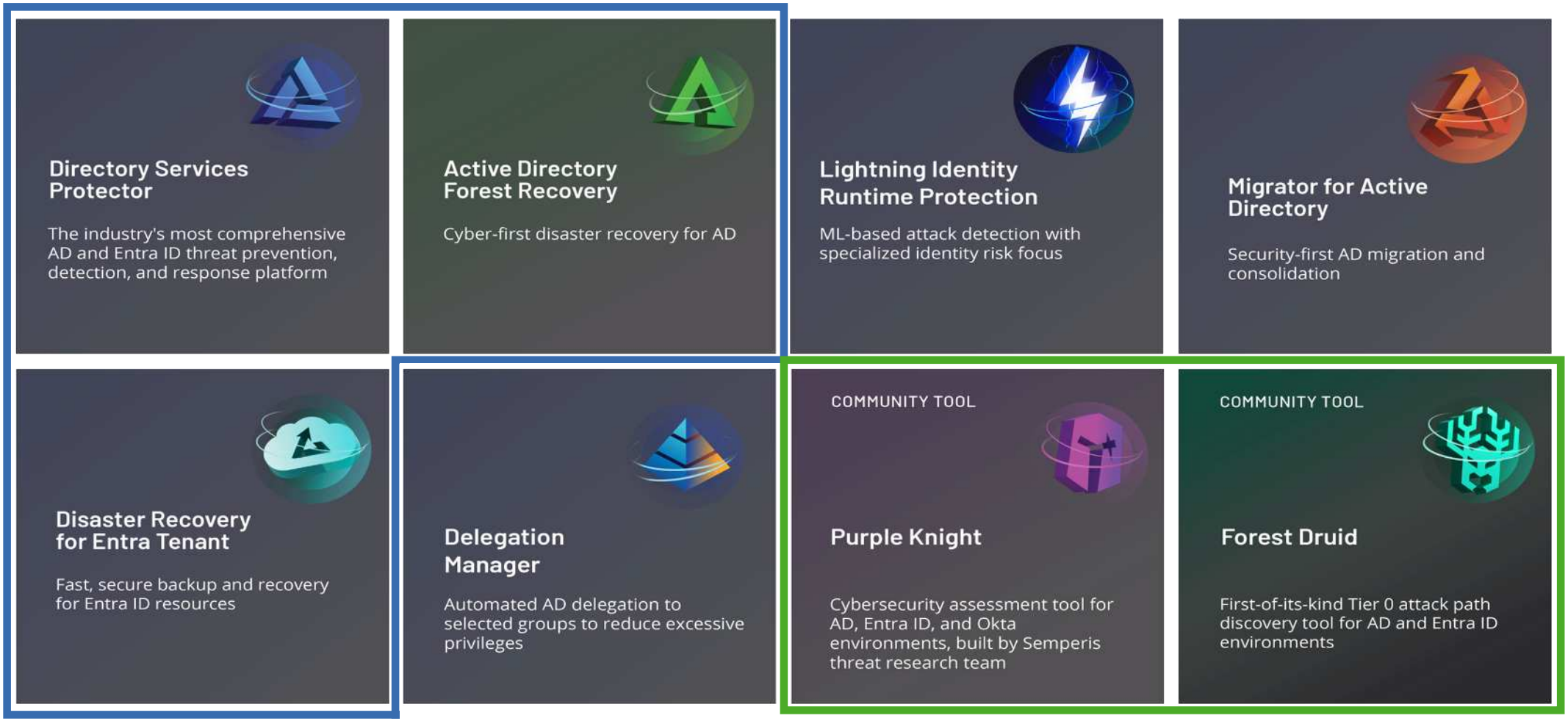
200+ million

アイデンティティをSemperisが保護

- #1 health system in the US, top 5 in the world
- 2/3 top consulting firms in the world
- 2/3 top airlines in the world
- #1 and #5 big box retailer in the world
- #1 bank in Europe. #2 bank in the U.S.
- Top 5 property insurer in the U.S. #2 auto insurer

Semperis 製品一覧

Connect Beyond



東京エレクトロン デバイス

Purple Knight

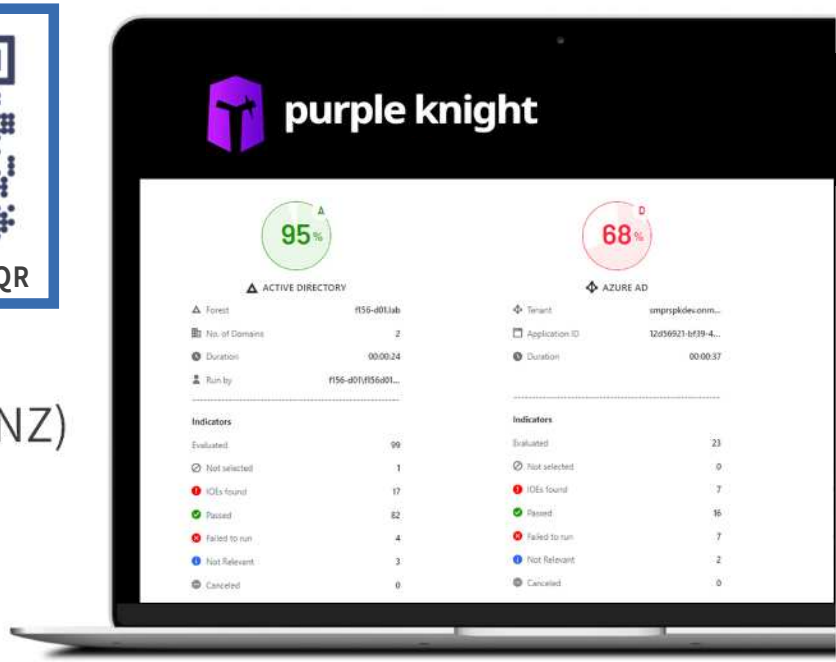
Connect Beyond

攻撃ベクトルに対して包括的なテストを実行
ハイブリッドID環境内の危険な構成とセキュリティ脆弱性を可視化

PURPLE KNIGHT

- ダウンロード無料
- AD/Entraの脆弱性を180+項目で診断
- 高速評価＆スコアリング
- 48,000以上ダウンロード
- ADアセスメントサービスとしてFive Eyes(米・英・豪・加・NZ)諸国政府が本サービスを推奨

ダウンロード用QR



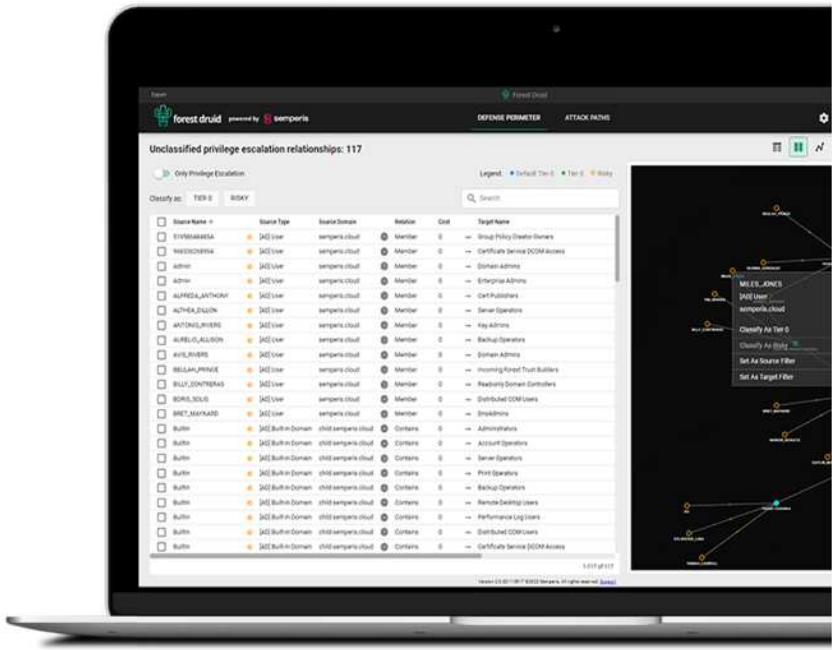
東京エレクトロン デバイス

Forest Druid

Tier 0を狙う攻撃パスをグラフで表示し、防御境界の再設計を支援

- ダウンロード無料
- Tier 0までの攻撃経路の可視化
- 攻撃パスの列挙と優先度付け
- ゾーニング／境界設計

FOREST
DRUID



DSP

Active Directory＋ Entra IDの常時監視、変更検知、修復

- ▶ 継続的脆弱性評価
- ▶ 改ざん防止・追跡
- ▶ リアルタイムセキュリティアラート
- ▶ 自動修復（悪意ある変更からのロールバック）
- ▶ コンプライアンスレポート報告
- ▶ 高度な振る舞い検知

DIRECTORY SERVICES PROTECTOR

東京エレクトロン デバイス

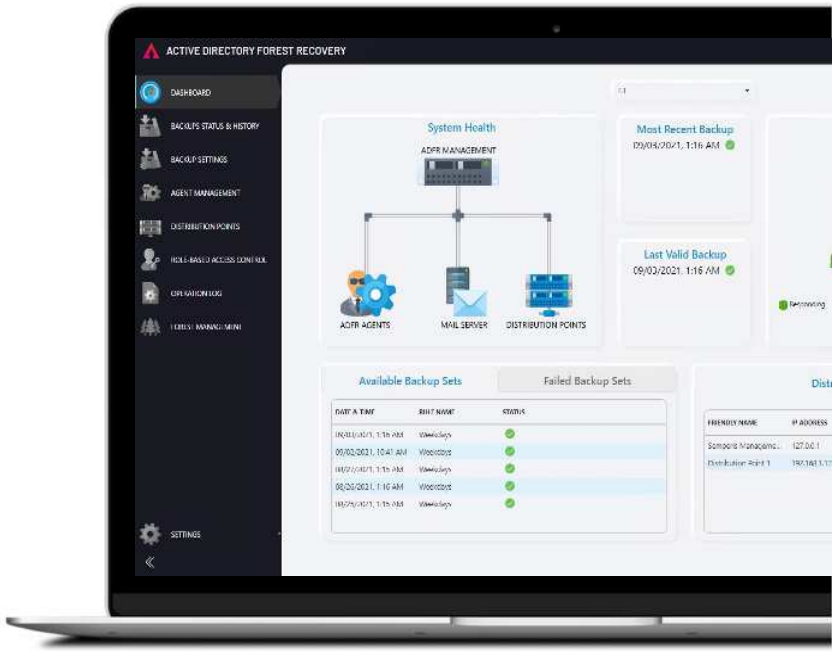
ADFR

Connect Beyond

ACTIVE DIRECTORY FOREST RECOVERY

Active Directory Forestを迅速かつマルウェアフリーでリカバリー

- クリーンな復元（マルウェアフリー）
- 迅速＆どこからでも復旧
- 高度な自動化
- 攻撃後のフォレンジック（ADのアンチウイルス機能）



東京エレクトロン デバイス

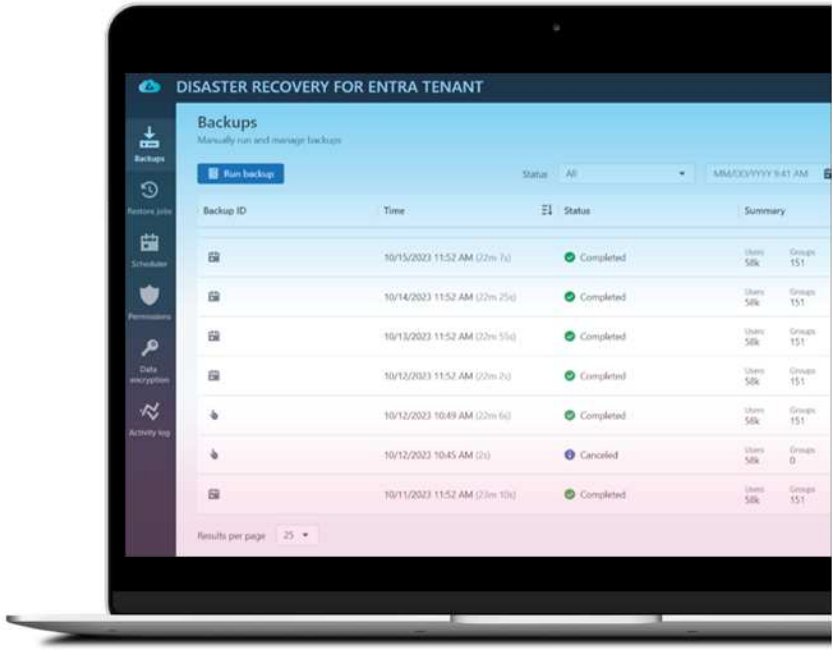
DRET

Connect Beyond

DISASTER RECOVERY FOR ENTRA TENANT

Entra IDをSaaSで迅速かつ柔軟にリカバリー

- Entra ID の構成・設定・ロール・アプリを自動バックアップ
- 誤設定・攻撃・破壊に対して柔軟にロールバック
- SaaSのため運用負荷が低い
- Entraの復元ポイントを常時保持
- コンプライアンス報告



東京エレクトロン デバイス

ITDRの各フェーズをSemperisでカバー

IDを守るための重要事項

- 社内の中核を担うAD・Entra IDを保護するための4ステップ
- 正規IDによる「なりすましログイン攻撃」への対策
- AD内の権限変更を検知・対応＆即時修復
- 企業の業務継続性を維持するための即時復旧機能

平時のアセスメント	攻撃のリアルタイム検知	改ざんされた特権IDの修復	AD/Entra IDのリカバリー
Purple Knight/Forest Druid	DSP		ADFR/DRET

ITDRのベストプラクティスをSemperisで実現

※DSP上位エディションでは継続的なアセスメントも提供

もしSemperisがあれば――
攻撃を受けても‘止まらない’ID基盤

Qilin型のランサムウェア攻撃

Qilin型のランサムウェア攻撃 VS Semperis

Connect Beyond

従来の対策

・入口対策
・EDR
・バックアップ

一部のみ検知

正規ID悪用は
見えにくい

AD制圧後
EDR無効化

長期の手作業復旧

semperis

脆弱性・攻撃パスを
事前に可視化

権限昇格・ID改ざん
を検知

悪意ある変更を
自動ロールバック

AD/Entraを短期間で
クリーン復旧

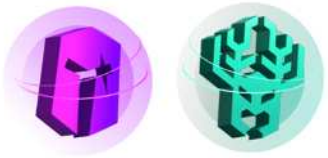
東京エレクトロン デバイス

まとめ

まとめ

- ✓ ID保護の必要性
- ✓ ITDRの役割
- ✓ ITDRのベストプラクティスをSemperisで実現

1 AD/Entra IDのリスク棚卸



Purple Knight/Forest Druidで
AD/Entra IDを診断
現状の脆弱性・攻撃面を可視化

2 認証・権限監視の強化

DSPで認証・権限のふるまいを
常時監視/自動修復

3 AD侵害前提の復旧シナリオ策定

ADFR/DRETでの即時復旧を
前提としたAD/Entra IDの
DR計画を具体化

各種情報・展示ブースのご案内

▶ Semperisに関する情報

▶ Semperisの概要
https://cn.teldevice.co.jp/maker/semperis/

▶ TED Blog (Semperis)
https://cn.teldevice.co.jp/maker/semperis/

▶ Semperis カタログ資料

▶ 展示ブース