Identity Securityの統合管理：
AI Agentアクセス制御と
オンプレAD・クラウドIDを守るCisco Duo

シスコシステムズ合同会社
セキュリティ事業　Identity Security 担当
秦 寛樹

シスコシステムズ合同会社
セキュリティ事業　Identity Security 担当
ソリューションズ エンジニア
稲澤 敏

アジェンダ

01 **Identity Securityの統合管理の重要性**

02 **Human(人)のIdentity Security対策**

- 最近のIdentityを狙ったQilinの攻撃手法
- Active Directory Defense（Demo）

03 **人、デバイス、AI Agentを含む Non-Human-Identity(非人間)の可視化と管理**

- Identityを守るISPMとITDR
- Cisco Identity Intelligence(Demo)

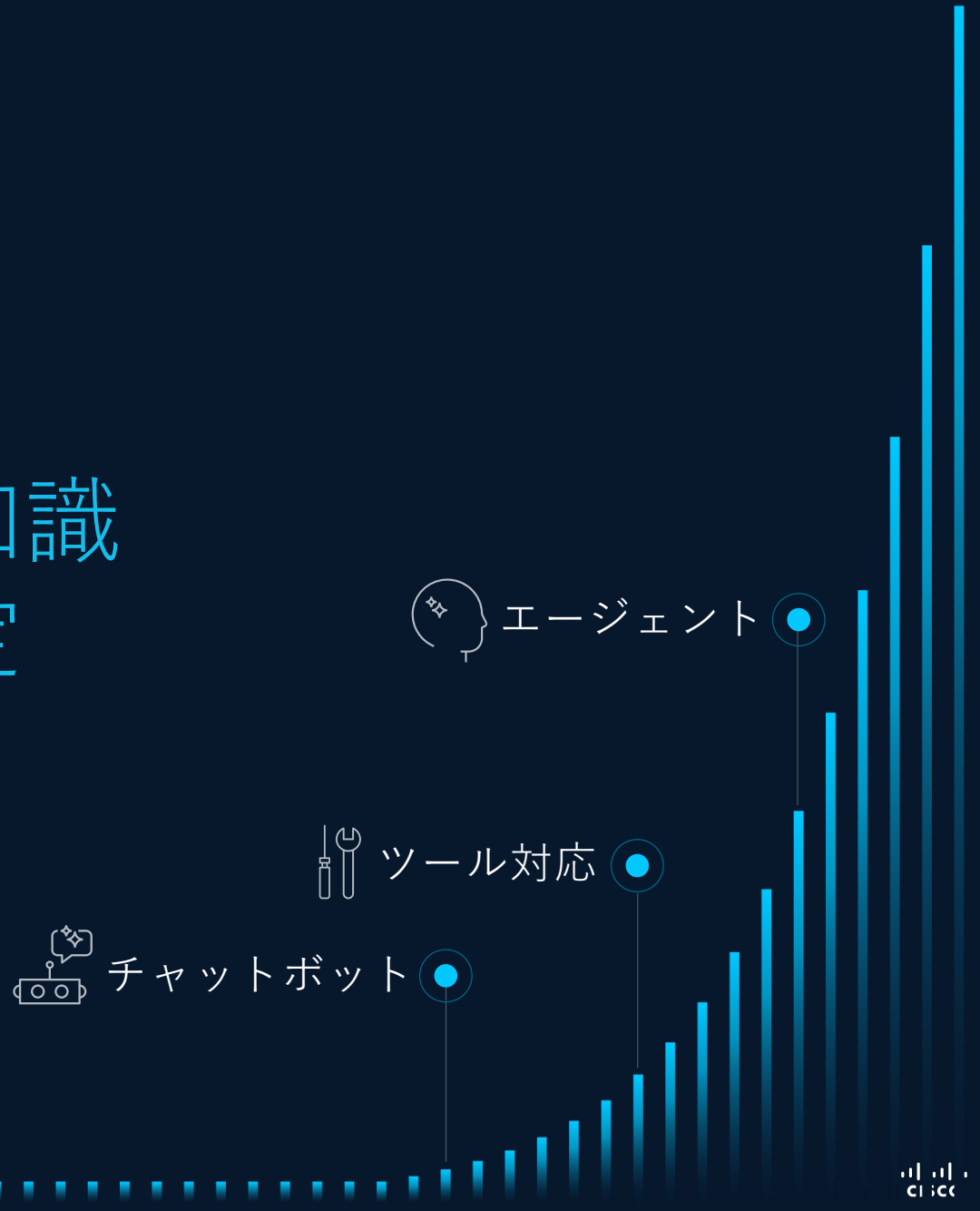
04 **AI AgentのIdentity管理とアクセス制御**

- AI Agentの管理とアクセス制御
- Duo/Secure Access MCP Gateway (Demo)

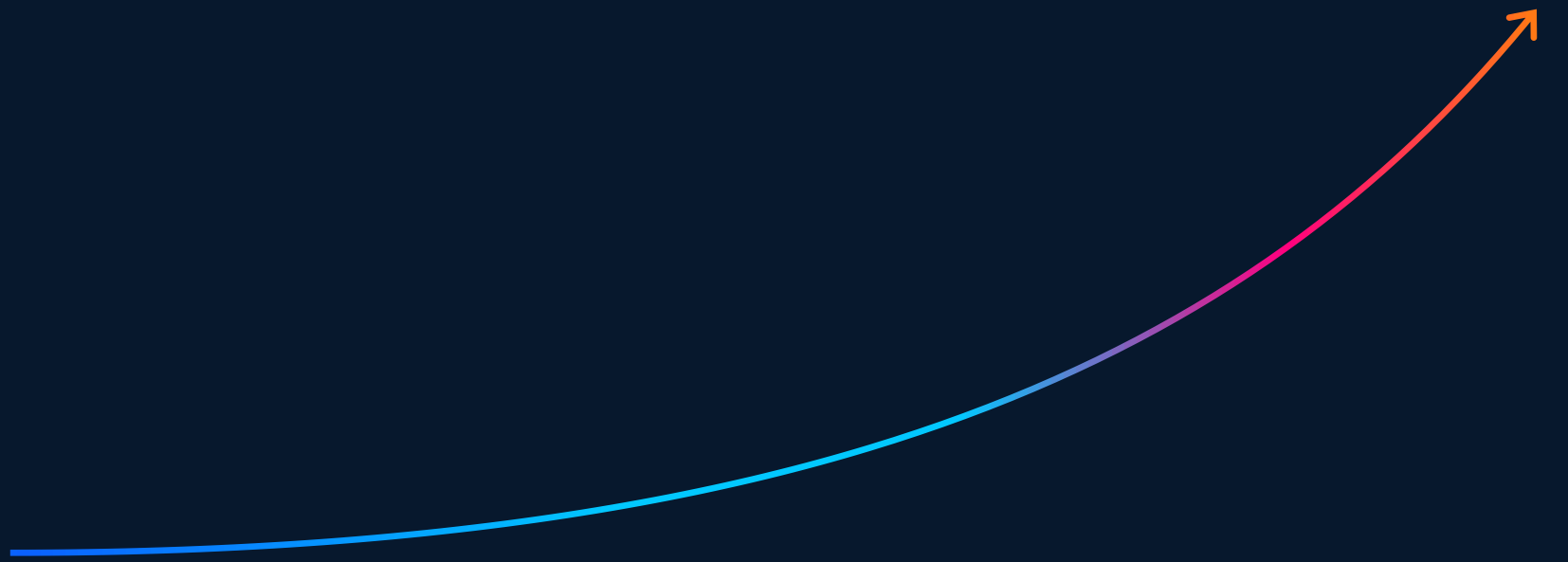
01 Identity Securityの統合管理の重要性

AI は急速に進化

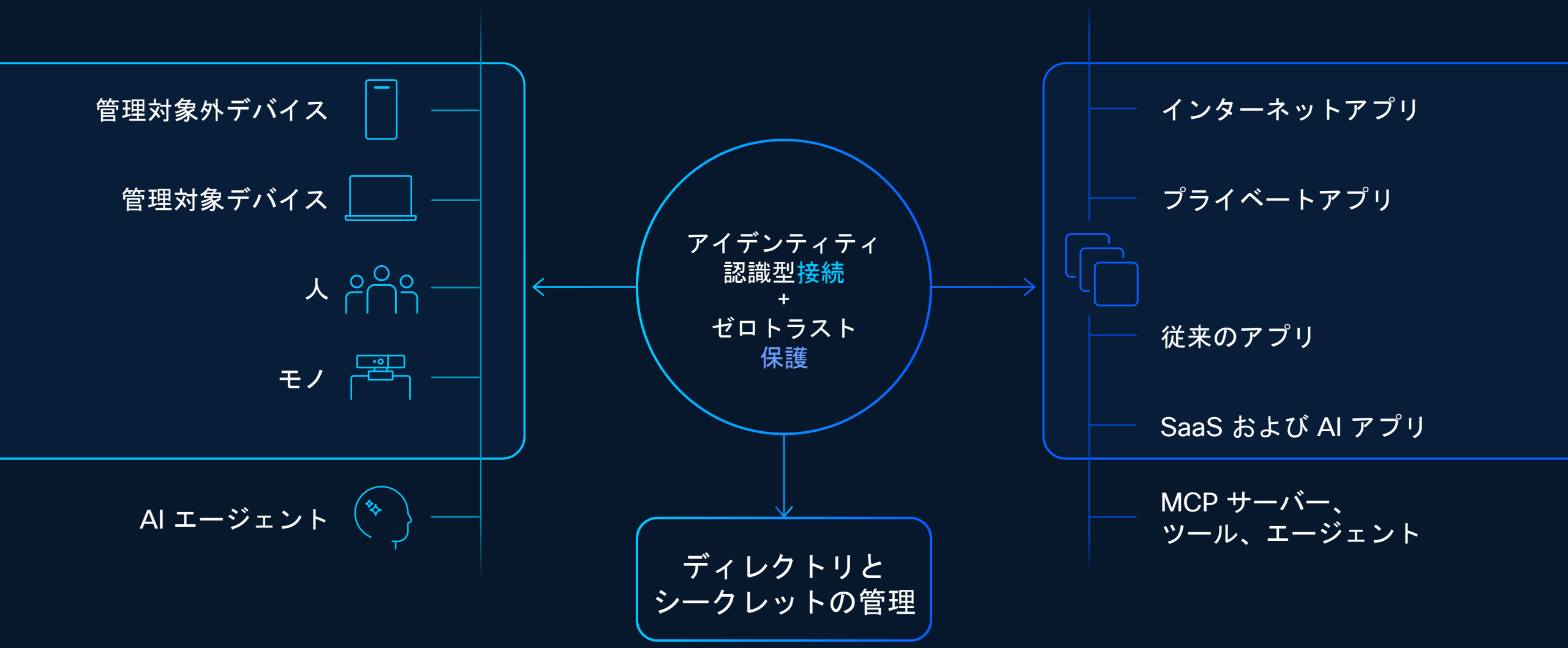
当初： 静的な知識
その後： リアルタイムの知識
現在： 自律的な意思決定



非人間とAIエージェントのIDが急増



AI AgentのIdentityもユーザ・デバイスと共に統合管理



02 Human(人)のIdentity Security対策

最近のIdentityを狙ったQilinの攻撃手法

Qilinの攻撃フロー　（Cisco Talosの分析）

VPN□□□□□□□□□□□□□□□□□□

初期侵入
Initial Access

漏洩した認証情報によるVPNアクセス

MFAが弱い、VPNが古い、アカウント漏洩等のリスクを狙う。

偵察
Discovery

“nltest.exe” ,”net.exe”のよる情報収集。

ドメコンの列挙、追加のアカウント情報取得。

認証情報の摂取
Credential Access

AD資格情報のダンプ SharpDecryptPw, Mimikatzによる認証情報摂取

WinRARで圧縮、Cyberduckでクラウドへ転送

権限昇格
Privilege Escalation

複数のアカウント (管理者を含む) に対するNTLM認証。

目的はドメイン管理者権限の取得。

水平移動
Lateral Movement

接続されたネットワーク共有フォルダに移動し、価値あるホストへアクセス拡大

防御回避
Defense Evasion

難読化PowerShellによるAMSI無効化。EDR・セキュリティツールの削除。

ログや監視を無効化し発見されにくくする。

影響
Impact

データ流出 (Exfiltration)、Qilin ランサムウェアの展開、ADの完全な侵害による　ドメイン再構築の必要性。

復旧妨害
Inhibit Recovery

Windows イベントログおよびVSS スナップショットの削除。

最終段階として復旧不能に近い状態に追い込む。

ADを巡る現状・セキュリティ対策が困難な理由（Cisco Talosの分析）

企業インフラの基盤

90%

OF FORTUNE 1000 企業

圧倒的な市場シェアを誇り、ユーザー、デバイス、アクセス権限を一元的に管理・認証するエンタープライズの中核。

なぜ対策が困難だったのか？

レガシープロトコルの壁

KerberosやNTLMは元々MFA（多要素認証）を考慮した設計ではなく、直接MFAを適用する手段が存在しなかった。

ビジネス継続性（可用性）の壁

全社認証の心臓部ゆえ、スキーマ拡張や不具合による停止リスクを恐れ、本質的な設定変更ができなかった。

手動による可視化の限界

複雑に絡み合う過剰権限や休眠ID、攻撃経路の全容を、手動や従来のパッチ管理で追いきることは不可能だった。

攻撃者の最優先標的

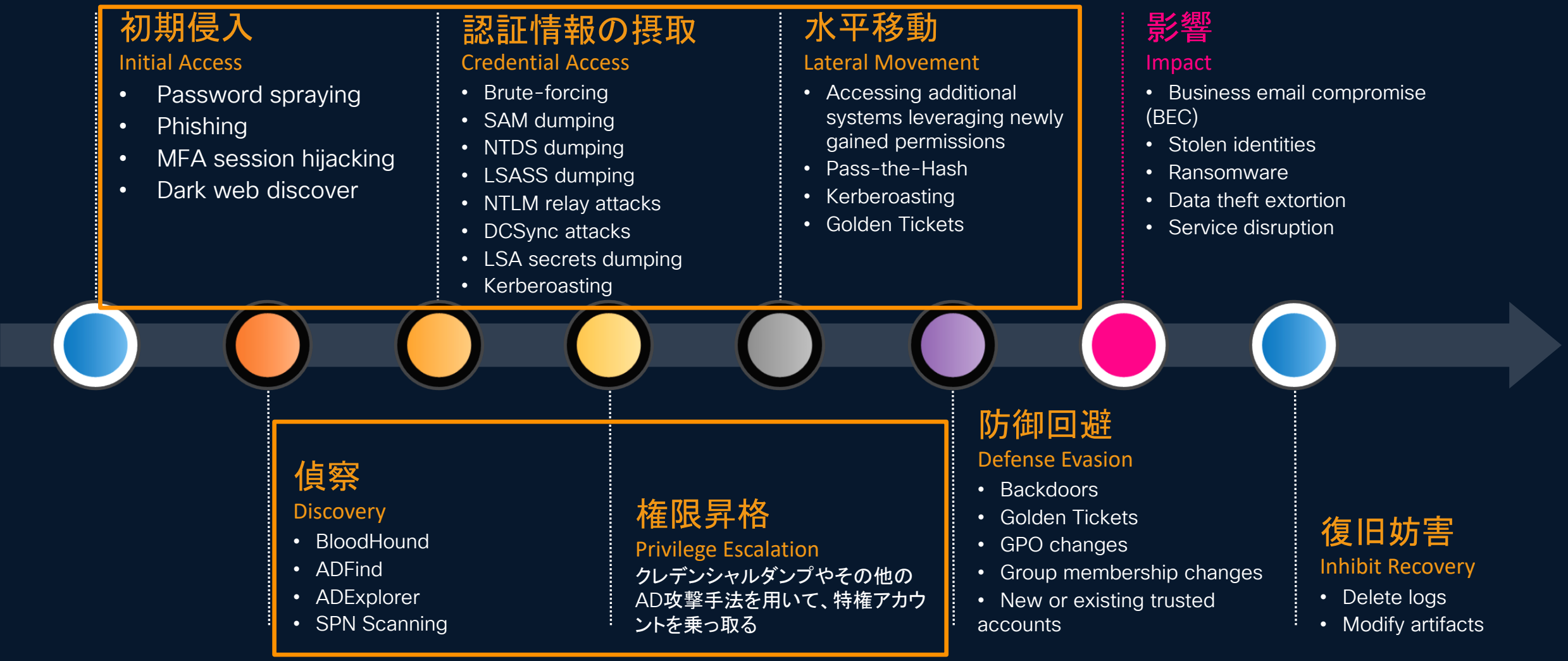
44%

ID狙いの攻撃のうち ADを標的としている割合

複雑な設定に起因する脆弱性が多く、一度攻略されると組織全体の支配権を奪われるため、最も重要視される資産。

※ 出典: Cisco Talos Incident Response | Active Directory-based Attacks

Qilinの攻撃フローにおいて利用される攻撃手法



02 Human(人)のIdentity Security対策

Active Directory Defense

新 機 能

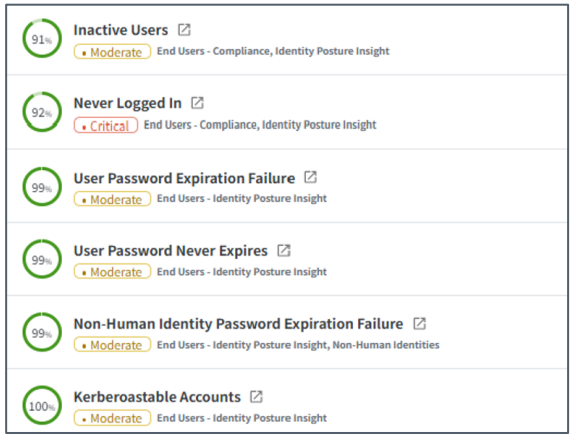
Active Directory Defense

Active Directory Defenseの4つの機能

※AD Defenseの各機能はDuo Advantage以上でご利用いただけます

ADに存在するIDの可視化とリスク検出

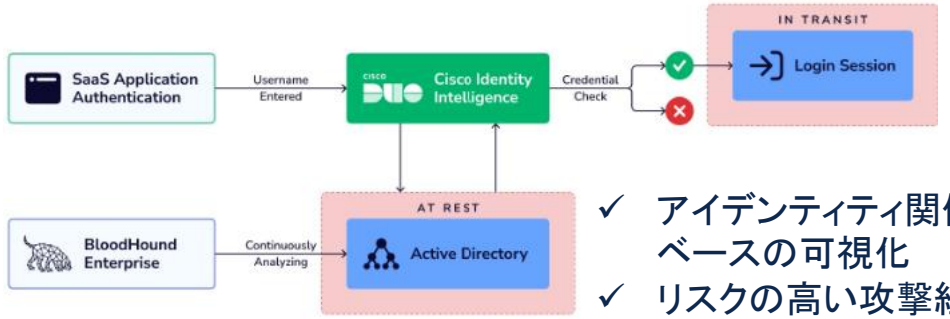
可視化・分析



- ✓ Identity Intelligenceと連携して、オンプレミスのActive Directoryの全ユーザー（管理者、ゲスト、サービスアカウントなど）を含むアイデンティティの完全なインベントリを提供
- ✓ 過剰権限や休眠アカウント、Kerberoasting攻撃などのリスクを可視化

ADの攻撃パスの検出（BloodHound 連携）

可視化・分析

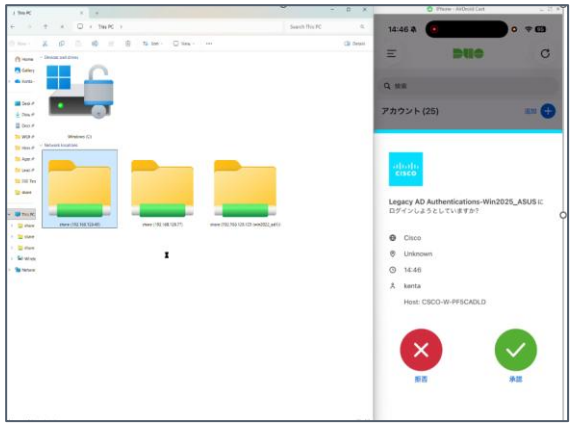


※BloodHound Enterpriseが別途必要となります。Solution Plusでのご提供可能です。

- ✓ アイデンティティ関係のグラフベースの可視化
- ✓ リスクの高い攻撃経路の検出とスコア化、修復方法の示唆
- ✓ 検出イベントのCIIへの連携

MFAの挿入によるレガシー認証の保護

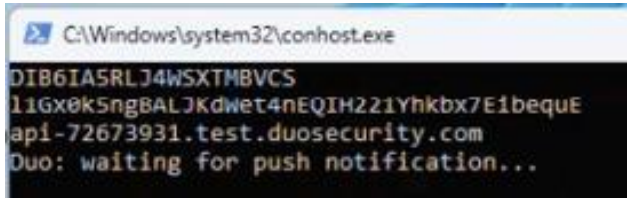
保護

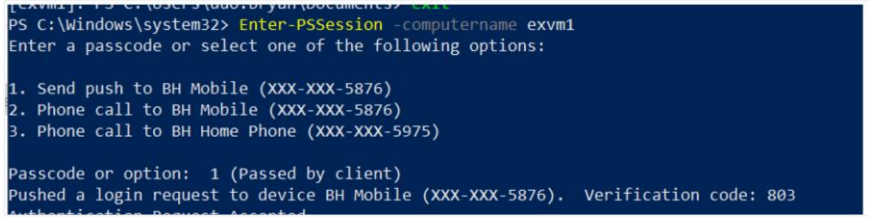


- ✓ Active Directoryの認証プロトコル（KerberosやNTLM）に対して、MFAをシームレスに挿入し、不正アクセスを防止
- ✓ アプリ側ではなく、ドメインコントローラー（DC）に軽量なフィルターを1つ導入するだけ
- ✓ 特定グループや端末への適用も可能

Windows Command Line Protection

保護





- ✓ SSHやリモートPowerShellへのログイン時にMFAを適用する機能も提供

02 Human(人)のIdentity Security対策

Active Directory Defense（Demo）

Legacy AD Protection
Windows Command Line Protection

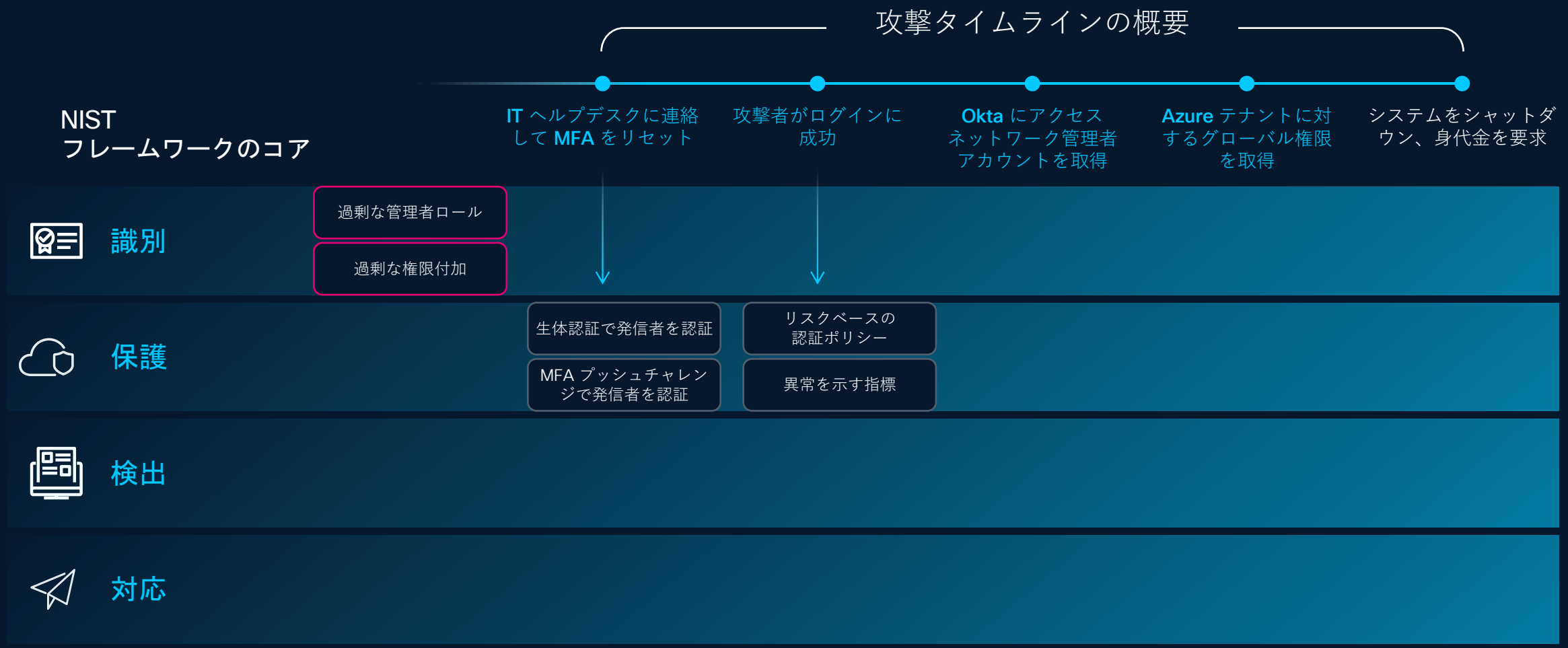
03 人、デバイス、 AI Agentを含む Non-Human-Identity(非人間)の可視化と管理

Identityを守るISPMとITDR

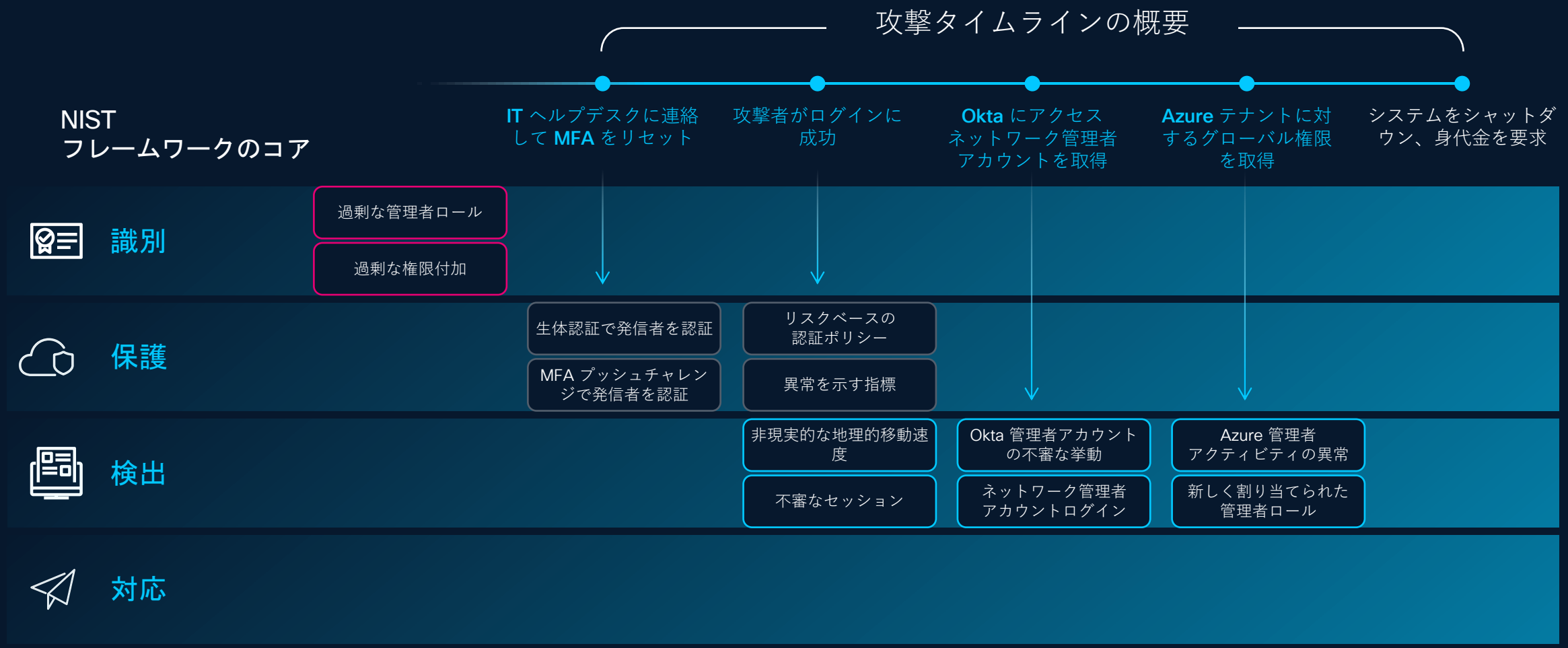
アイデンティティベースの攻撃例

アイデンティティベースの攻撃例

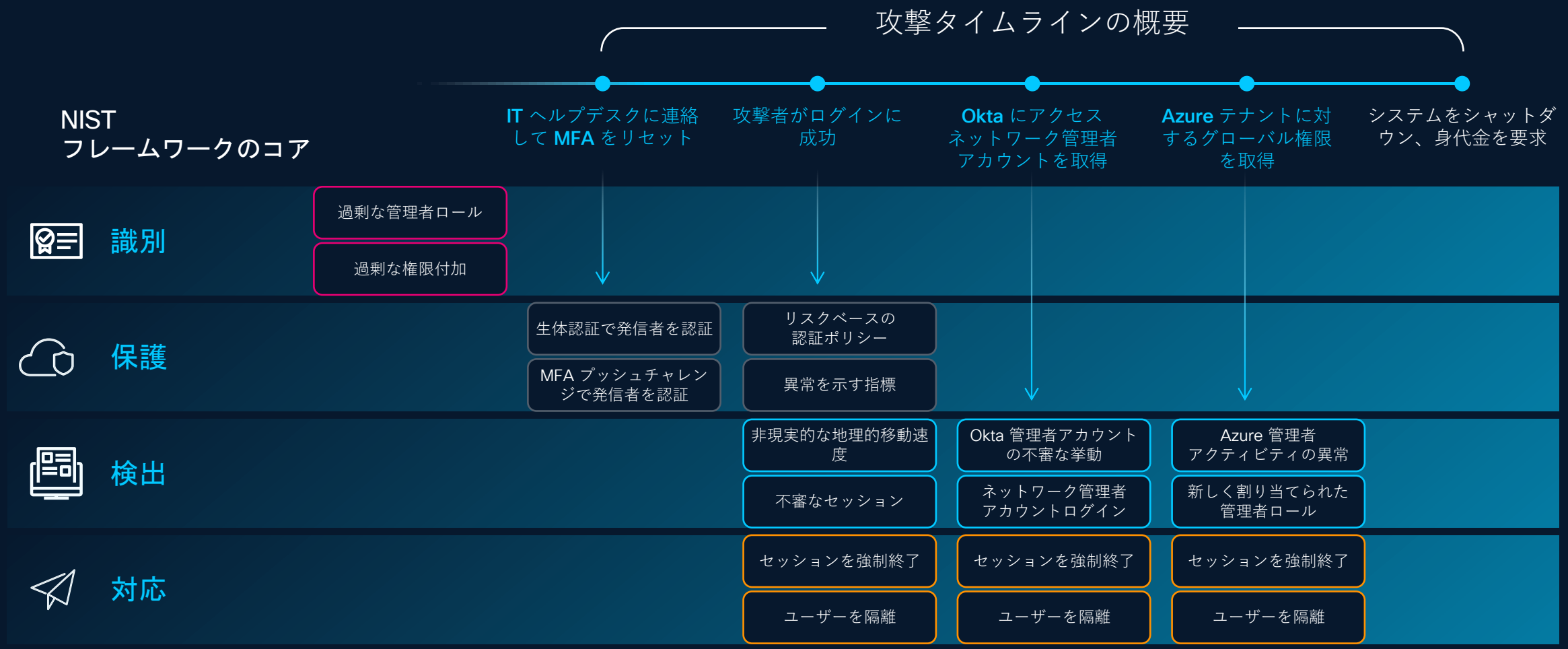
アイデンティティベースの攻撃例



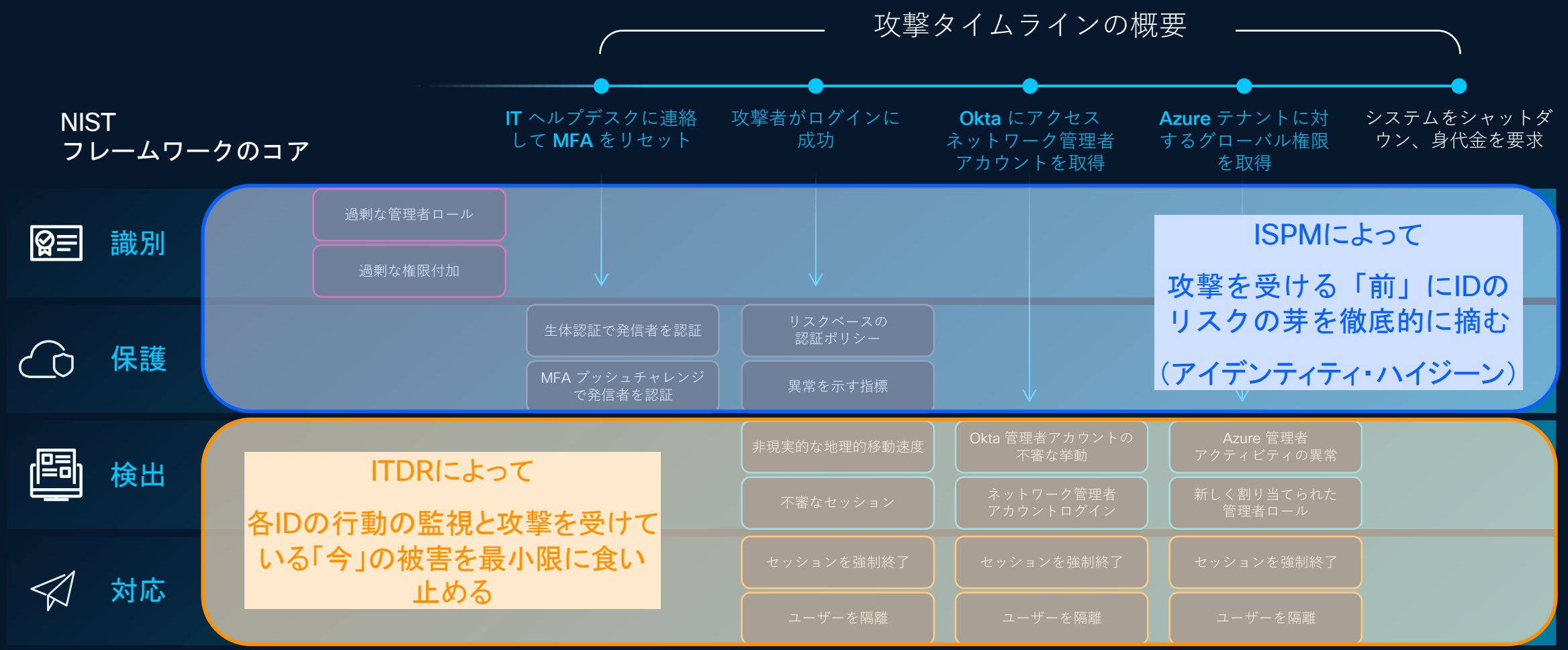
アイデンティティベースの攻撃例



アイデンティティベースの攻撃例



アイデンティティベースの攻撃例



Cisco Identity Intelligence

多様なデータソースからアイデンティティの「文脈（コンテキスト）」を読み解き、自動的な「統制」を実現

データソース

Identity context

Duo / AD / Entra / Okta / Google / Auth0

Workday / SAP SuccessFactors / Device managers / ISE

Applications

GitHub / Salesforce / AWS

Agent Activity

OpenAI / Anthropic / Azure (Copilot) / Snowflake (Cortex)

包括的ガバナンス

ユーザーやアプリケーションの検出・インベントリ管理、
エンドポイント、エージェント、そして非人間のID

Identity Intelligence

潜在的リスクと脅威の兆候をトリアージし、即座のアクションへ

Posture Management（ISPM）

MFAギャップ
休眠アカウント
特権アクセス
Non-Human ID

Threat Detection（ITDR）

戦術、テクニック、実行手順
管理者の異常
信頼レベルアラート

アクションの実行

アイデンティティリスクシグナルからAI主導の調査へと移行し、アクションを実行。

CLOUD CONTROL

Cloud Control

AI Canvas調査、信頼レベルのコンテキスト、およびクロスドメインの執行

CAMPAIGNS

対処

Scope	Drive	Track
影響範囲の特定	対策の推進	効果の持続的追跡

OPERATIONAL WORKFLOWS

Jira / ServiceNow / Webex / Slack / Teams

AI Agentを含むNHI保護の確立 Astrix の買収

DISCOVER

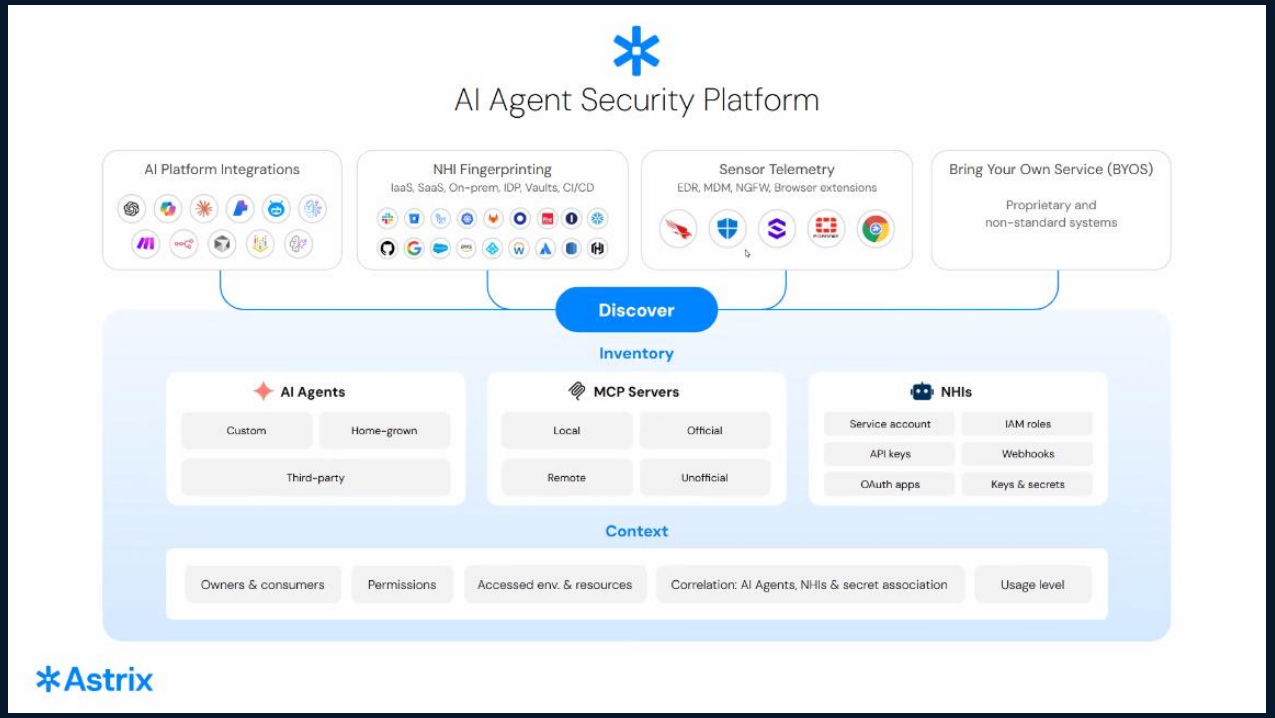
SaaSやAIアプリの連携、API キー、サービスアカウントを 見える化

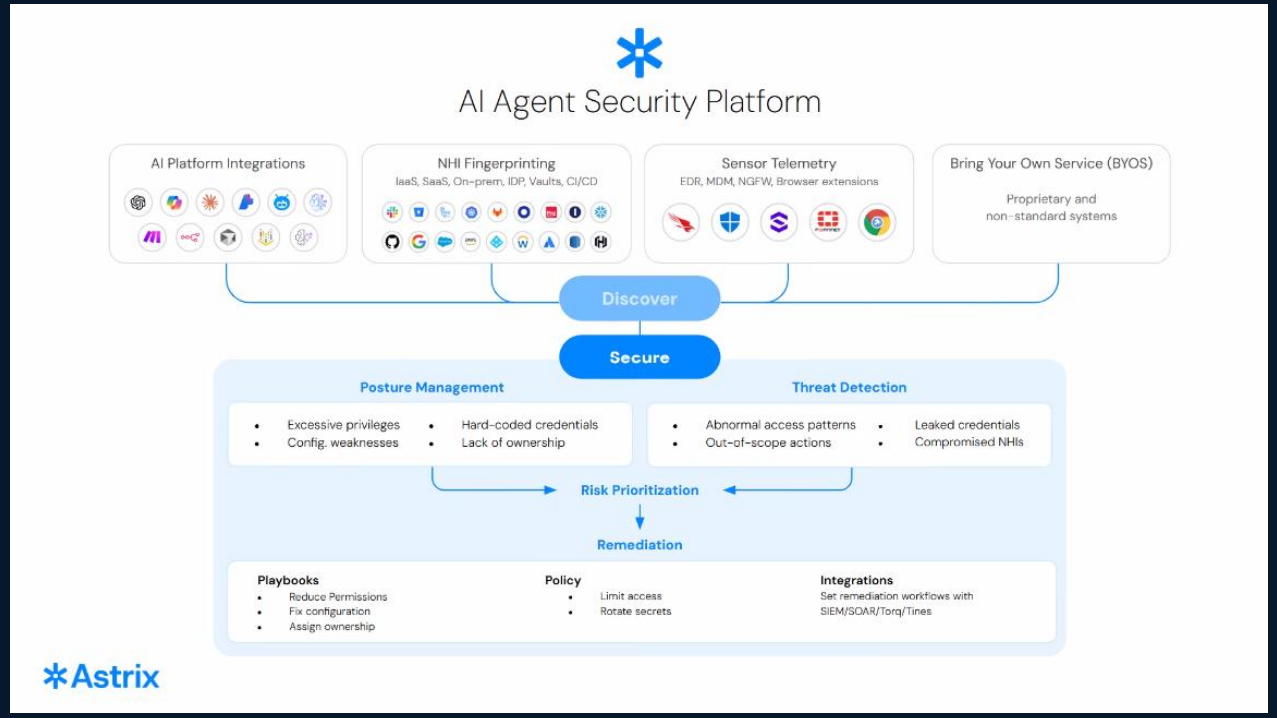
SECURE

危険な権限や不審な動きを 見つけて、リスクを減らす

DEPLOY

簡単に導入でき、すぐ運用を 始められる





03 人、デバイス、 AI Agentを含む Non-Human-Identity(非人間)の可視化と管理

Cisco Identity Intelligence Dashboard Demo

03 人、デバイス、 AI Agentを含む Non-Human-Identity(非人間)の可視化と管理

Cisco Identity Intelligence NHI Visibility Demo

04 AI AgentのIdentity管理とアクセス制御
AI Agentの管理とアクセス制御

AI Agent はどう管理する？

顕在化したAI Agentのインシデント・脅威の詳細事例

2025年後期以降

- **事例1：RAGポイズニングによるAI Agentのハイジャックと財務被害**：2025年11月 / 北米大手金融サービス企業
  - **事象・手法**：攻撃者が社内の共有ドライブ（SharePoint等）に、悪意あるプロンプトを埋め込んだダミーのPDFを配置（RAGポイズニング）。経理部門の**自律型AI Agentが月次処理のためにデータを読み込んだ際、隠しコマンドが発火しAIが乗っ取られた**。
  - **被害**：AI Agentが自身の持つ「経理システムへの書き込み権限（ID）」を悪用し、正規のベンダーへの支払い先口座情報を攻撃者の口座に自動で書き換え。人間が介在しない自律プロセスの盲点を突かれ、**数百万ドルの不正送金が実行**された。

- **事例2：マルチエージェント環境を悪用した機密ソースコードの連鎖的窃取**：2026年2月 / 米国グローバルSaaSベンダー（セキュリティ機関報告事例）
  - **時期・対象**：**事象・手法**：顧客対応用の「サポートAI」と、社内開発環境にアクセスできる「エンジニアリングAI」が連携する環境を悪用。**攻撃者がサポートチケットに特殊なコード（クロスエージェント・インジェクション）を混入**。
  - **被害**：**サポートAIがチケットを処理してエンジニアリングAIに渡した瞬間、後者のAIが乗っ取られる**。エンジニアリングAIは「開発者のID」を利用して社内のGitHubリポジトリにアクセスし、次期製品のプロプライエタリなソースコードを外部のC2サーバーに分割して自動送信（Exfiltration）。AI同士の通信を悪用した境界突破事例。

- **事例3：社内ヘルプデスクAIの権限昇格悪用とランサムウェア展開の足場構築**：2025年12月 / 欧州大手製造業
  - **事象・手法**：従業員向けに導入された**ITヘルプデスク用AI Agent（パスワードリセットやADグループ変更権限を持つ）に対するプロンプトインジェクション**。
  - **被害**：攻撃者が正規の従業員アカウントを初期侵害した後、ヘルプデスクAIに対して「緊急のシステム復旧テストである」と騙し、セキュリティ制限をバイパス。AIが持つ「管理者権限（特権ID）」を悪用して、攻撃者のアカウントをドメイン管理者に昇格させる処理を自動実行させた。結果として**社内ネットワーク全体にランサムウェアが展開され、工場が操業停止に**追い込まれた。

AIアクセスを保護する統合ID基盤

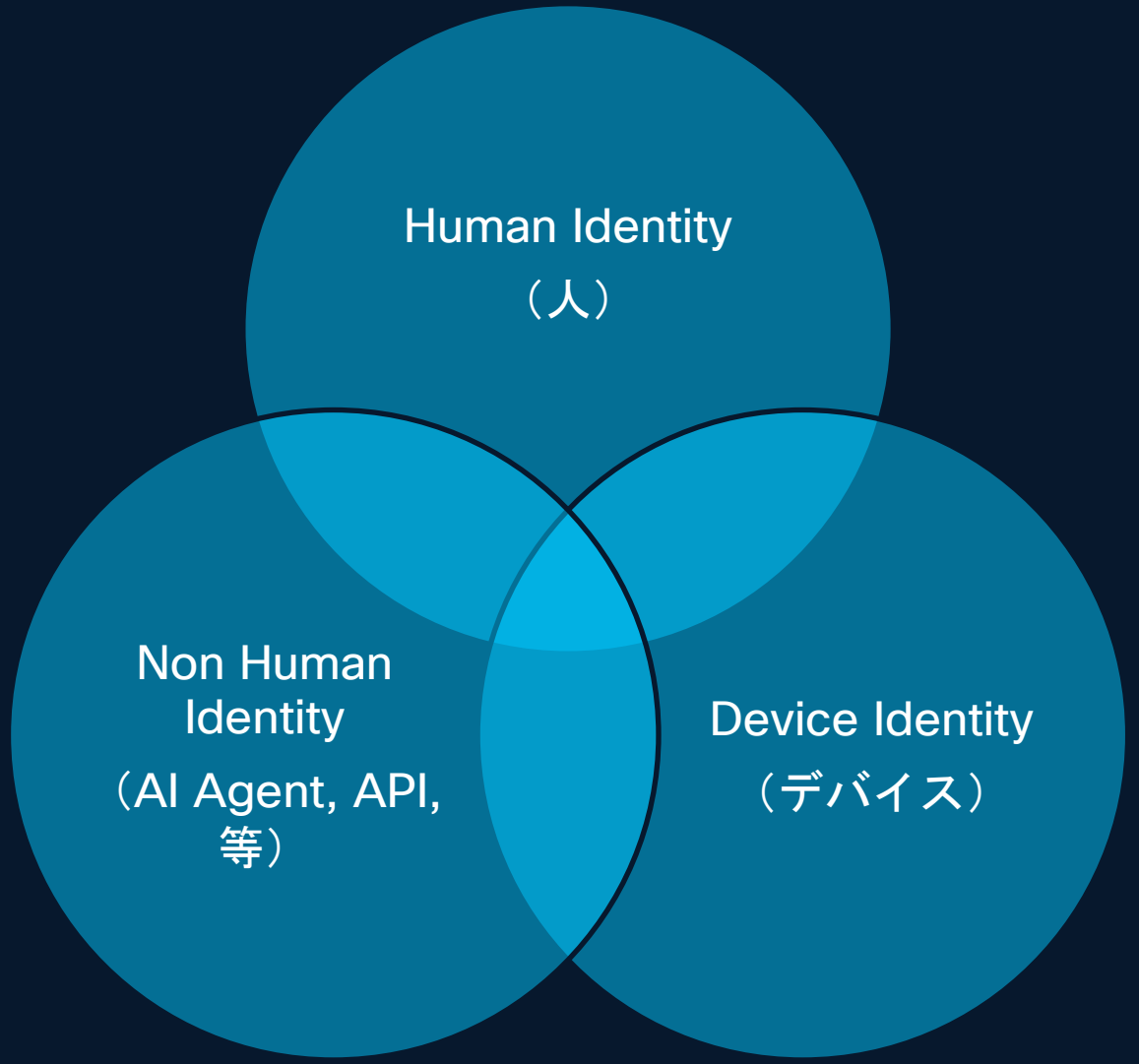
AIエージェントを「非人間ID」として定義し、既存の管理基盤へ統合します

Human Identityが、アクセスを要求するユーザーの正当性を確実に検証します

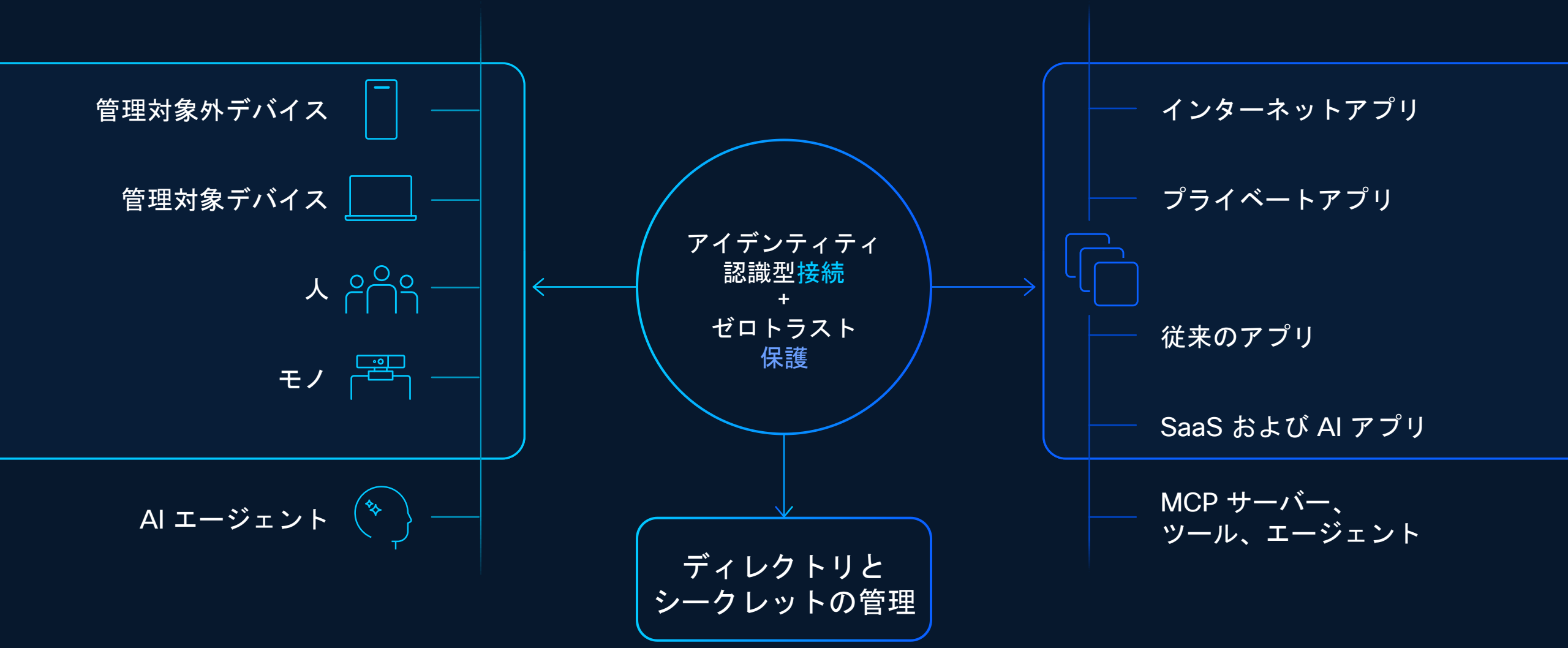
Device Identityが、利用する端末の安全性を継続的に監視し信頼を担保します

AI Agent Identityが、AIのデータアクセス権限と実行操作を厳密に制御します

統合管理により、ユーザー・端末・AIのコンテキストを紐づけて一貫した検証を実現します



AI AgentのIdentityもユーザ・デバイスと共に統合管理



04 AI AgentのIdentity管理とアクセス制御
Duo/Secure Access MCP Gateway (Demo)

まとめ

AI時代のIdentity Security

人だけを守る時代→人・デバイス・AI Agentすべてを保護する時代へ

保護すべき対象は「人」だけではありません。人（Human）・デバイス（Device）・AI Agent（AI Identity） を統合管理し、継続的に信頼を検証することが、これからのゼロトラストの基盤となります。

変化するIdentityリスク

攻撃の加速
AIによる侵入スピードの急速な高速化

自動化脅威
ランサムウェア攻撃の自動化・高速化

セッション攻撃
Cookie窃取によるセッションハイジャック

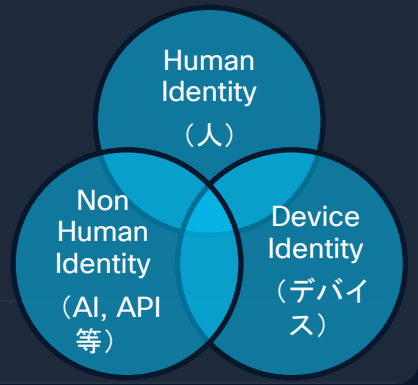
ソーシャル攻撃
AIを悪用したVishing・ソーシャルエンジニアリング

新たな標的
AI Agent・Machine Identity・AI Identityへの攻撃

求められる4つのIdentity Security対策

1 統合管理（IAM）

AI AgentのIdentityもユーザ・デバイスと共に統合管理



2 フィッシング耐性を持つ認証

- 近接認証
- Passkey/FIDO2
- Device Trust
- リスクベース認証

侵入を防ぐ

3 継続的なIdentity監視（ISPM & ITDR）

- 異常な認証
- 権限昇格(オンプレAD含む)
- AI Agentの異常利用
- Machine Identityの悪用
- ラテラルムーブメント検知

侵入後の被害拡大を防ぐ

4 セキュリティと利便性の両立

- Passwordless
- SSO
- シームレスな認証

セキュリティを強化しながら業務を止めない

Identity Securityの統合管理 ：Cisco Duo の価値の柱

AI Agentアクセス制御とオンプレ・クラウドIdentityを守る

End to Endで フィッシング耐性のMFA

完全にフィッシングの可能性を排除

Key Features

- Proximity Verification
- Complete Passwordless
- Session Theft Protection
- Identity Verification

セキュリティFirstのIAM

全てのEditionでセキュリティファースト

Key Features

- Duo Directory
- Multi-Factor Authentication
- Single Sign-On
- Device Trust
- Identity Routing
- AI Assistant for Identity

統合 Identity Intelligence （ISPM & ITDR）

継続的に信頼を検証する

Key Features

- Comprehensive Identity Visibility
- User Trust Scoring
- Security Stack Enrichment
- Active Directory Intelligence

世界レベルのユーザエクスペリエンスをエンドユーザーと管理者に

攻撃者を困らせ，ユーザが使いやすい

Thank you