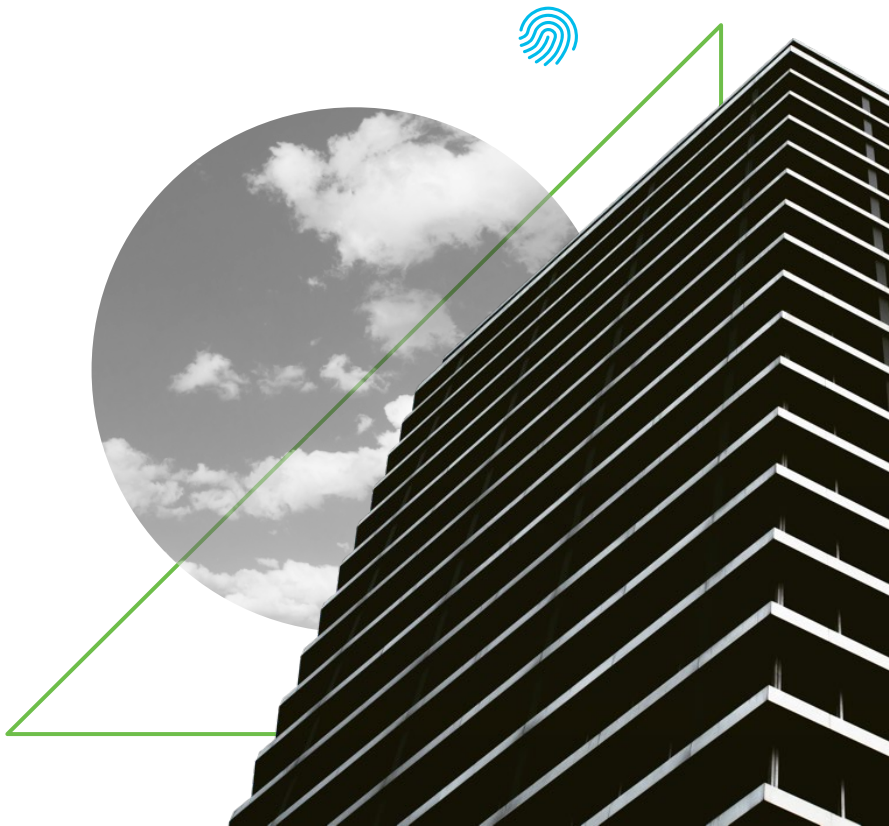
CISCO
SECUREざっくりシリーズ

The bridge to possible

ざっくり
Cisco Secure Endpoint

Agenda

- ターゲットとゴール
- 用語集
- なぜエンドポイントセキュリティが今重要なのか？(背景)
- Cisco Secure Endpointの概要
- ライセンスの概要
- Essentialsライセンス
- Advantageライセンス
- Premierライセンス
- Secure Endpoint Proサービス
- 第三者機関評価
- 事例
- 参考リンク集



ターゲットとゴール

ターゲット:

お客様と対面するプリセールス様、営業様

ゴール:

エンドポイントセキュリティがなぜ今必要か、背景をシンプルに理解する

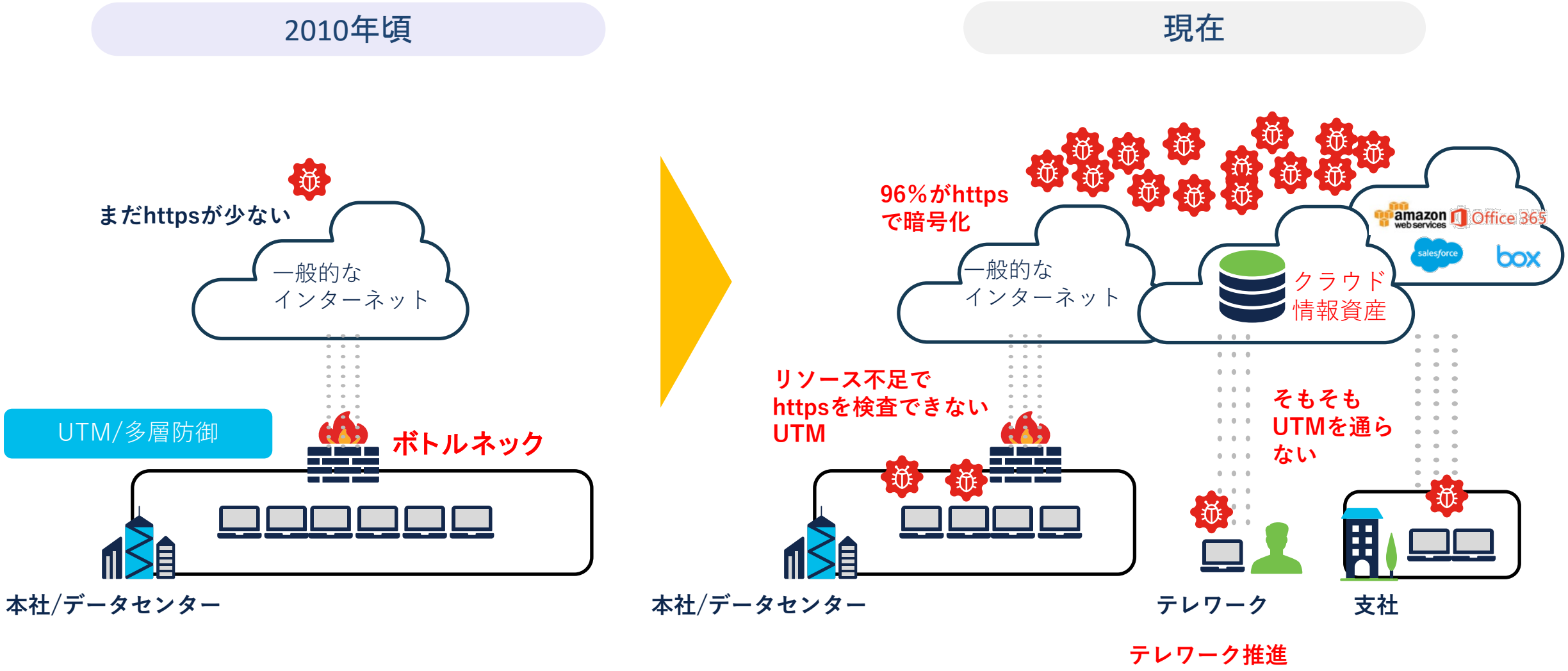
Cisco Secure Endpointが持つEDR/EPP機能を簡単に説明できる

テレワークやクラウド環境で既存のAVやUTMに課題を持つお客様にすばやく提案できる

用語集

用語	概要
EPP	Endpoint Protection Platformの略で、アンチウィルス(AV)のソリューションの総称です。一般的にエンドポイントにソフトウェアをインストールして、マルウェアからエンドポイントを保護します。
NGEPP NGAV	NGEPP:Next Generation Endpoint Protection Platform NGAV:Next Generation Anti-Virus 広義ではNGEPP/NGAVはEPPに含まれます。狭義ではEPPは主に従来のシグネチャ型のパータンマッチング方式を採用して既知のマルウェアを検出・ブロックするものに対して、未知のマルウェアを検出するために振る舞い検知や機械学習(AI)といった技術を用いるものを区別して呼びます。
EDR	Endpoint Detection and Response の略で、エンドポイントの状態を継続的に監視して、侵入された(インシデントが発生) 後に、すばやく影響範囲を分析、マルウェアを封じ込め、システムを復旧するといった脅威の軽減を行うためのソリューションです。
XDR	Extended Detection and Responseの略で、EDRの手法を拡張したソリューションです。エンドポイントだけではなく、サーバやファイアウォール、メールなど様々なネットワークポイントから情報を収集して相互に分析を行い、自動化された対応(プレイブック/ワークフロー)などを実施します。
MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledgeの略で、米国連邦政府が支援する非営利組織「MITRE」(CVEの提供で有名)が実際のサイバー攻撃の手法を分類してまとめたナレッジベースフレームワークです。
AMP for Endpoints	Cisco Secure Endpointsの旧名称。補足までに、CiscoのFirewallやメールセキュリティなど様々な製品にAMPのエンジンが使われている。

なぜエンドポイントセキュリティが今重要なのか？
テレワーク環境における利用の変化



参考情報:情報セキュリティ10大脅威 2021

出典IPA https://www.ipa.go.jp/security/vuln/10threats2021.html

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

- 「ランサムウェアによる被害」が1位
- 「テレワーク等のニューノーマルな働き方を狙った攻撃」が初登場で3位

エンドポイント：最後の防衛ライン

- エンドポイントは最も攻撃されやすい対象の一つ
- 同じくもう一つの最も攻撃されやすい対象である人間が直接触れるデバイス
- 暗号化された通信で可視性が低いネットワークより、エンドポイントでの防御が効果的であり、必要不可欠

Image source: https://commons.wikimedia.org/wiki/File:Soccer_goalkeeper.jpg (public domain)

エンドポイントセキュリティの変遷

侵入を未然に防ぐのが理想だが、EPPやNGEPPの防御では限界があり、すり抜けが発生している現実がある

侵入されることを前提として、感染経路や被害範囲を特定して対応するEDRやXDRが重要

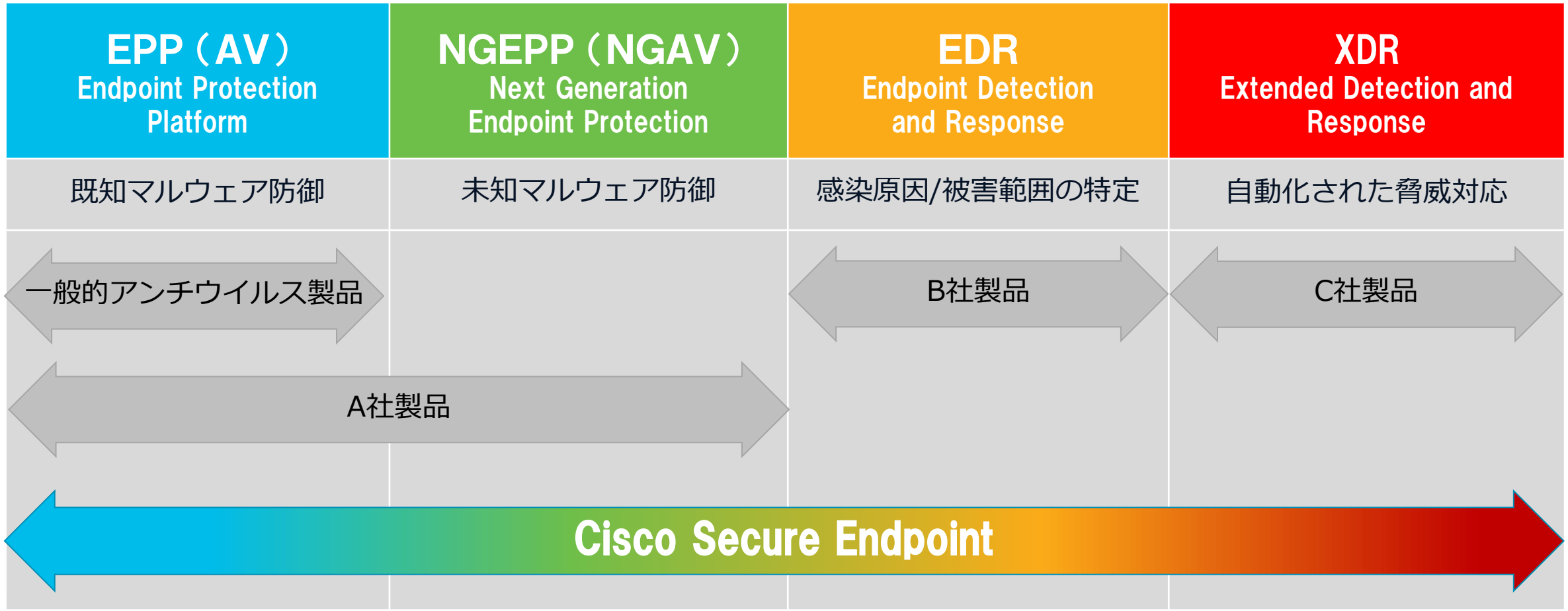
EPP (AV) Endpoint Protection Platform	NGEPP (NGAV) Next-Generation Endpoint Protection	EDR Endpoint Detection and Response	XDR Extended Detection and Response
防御	防御	検知と対応	検知と対応
既知の脅威対策 シグネチャベースの ウイルス対策	未知の脅威対策 シグネチャ非依存の ウイルス対策	インシデント調査活用 感染経路や被害範囲の 特定	自動化された脅威対応 MITRE ATT&CK
パターンマッチング ヒューリスティック	サンドボックス 機械学習（AI）	痕跡（IOC）分析	プレイブック (ワークフロー) 脅威ハンティング

Emotetなどのマルウェアが巧妙な手口でアンチウィルスをすり抜けて被害が拡大
(参考)IPA 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html

今、多くのお客様で採用が進んでいる注目分野

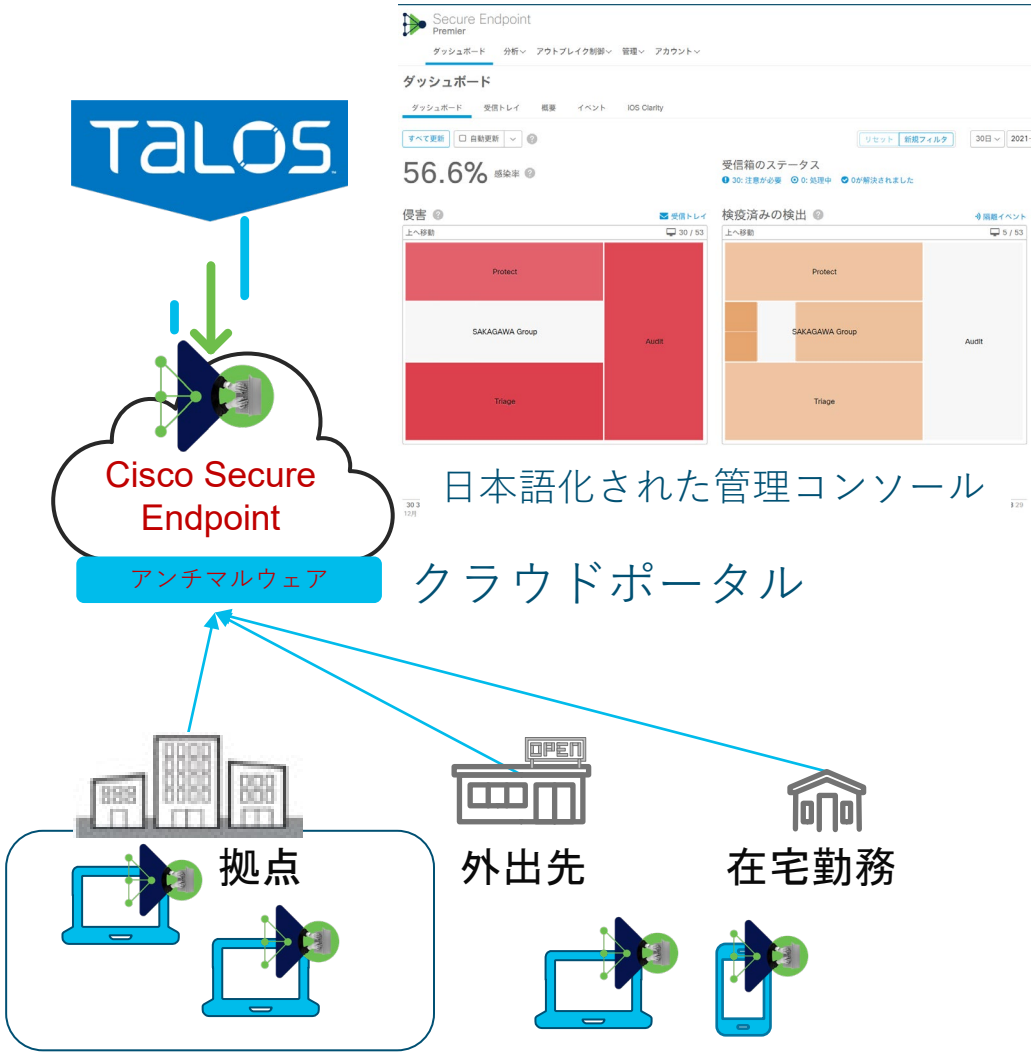
Cisco Secure Endpoint = EPP + NGEPP + EDR + XDR

Cisco Secure Endpointはアンチウイルス機能に、万が一の感染原因を特定するためのEDR機能を統合
（単一エージェントで利用可能）



Cisco Secure Endpoint
クラウド提供型の次世代エンドポイントセキュリティ

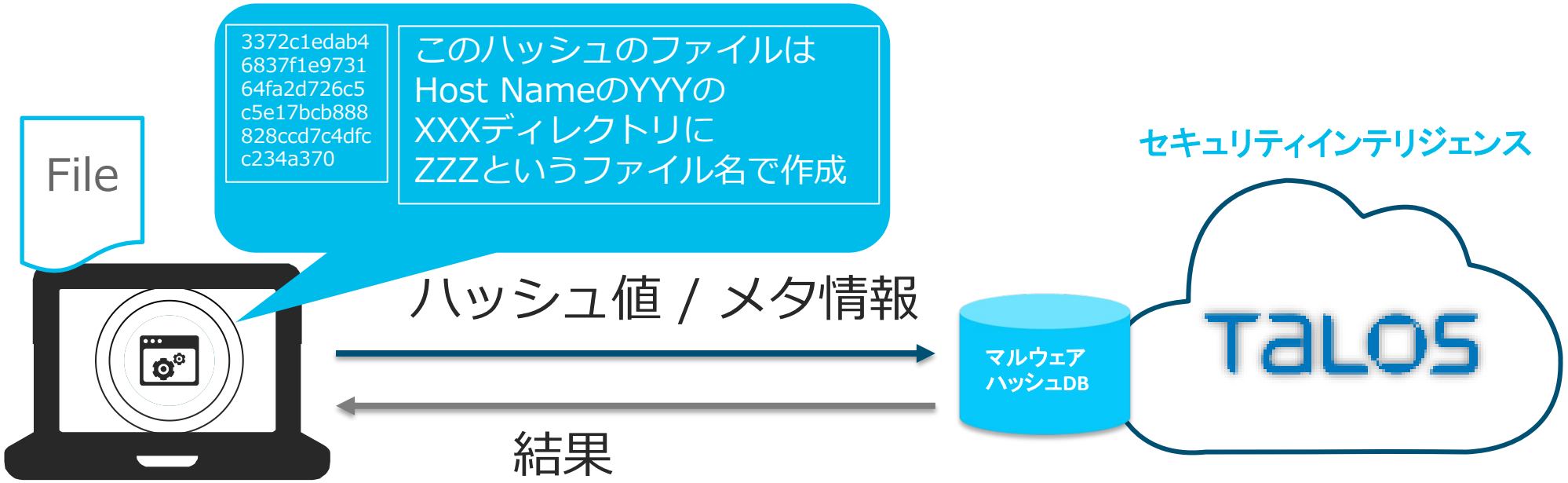
- クラウド管理でマルウェアの検知・隔離・感染の証跡を提供 (オンプレミス構成も提供可)
- マルチプラットフォーム対応
  - Windows/MAC/Android/Linux/iOS(CSC)
- マルウェアの検出・防御（EPP+NGEPP）
  - シグネチャパターンマッチングより高速なハッシュ値をベースにしたマルウェア検知
  - 高度なマルウェア分析と詳細な脅威分析を組み合わせたサンドボックス(Threat Grid)
- 検知をすり抜けるマルウェアの解析（EDR）
  - 後からマルウェアと発覚したファイルを直ちに隔離（クラウドリコール）
  - マルウェアの感染源、ネットワーク内での拡散状況を可視化（トラジェクトリ）



Secure Endpointの基本機能

EPP機能

ファイルのハッシュ値をクラウドデータベースに問い合わせて照合



- Good: ベンダーが作成したファイル
- Unknown: まだ DB に情報無し
- Malicious: マルウェア

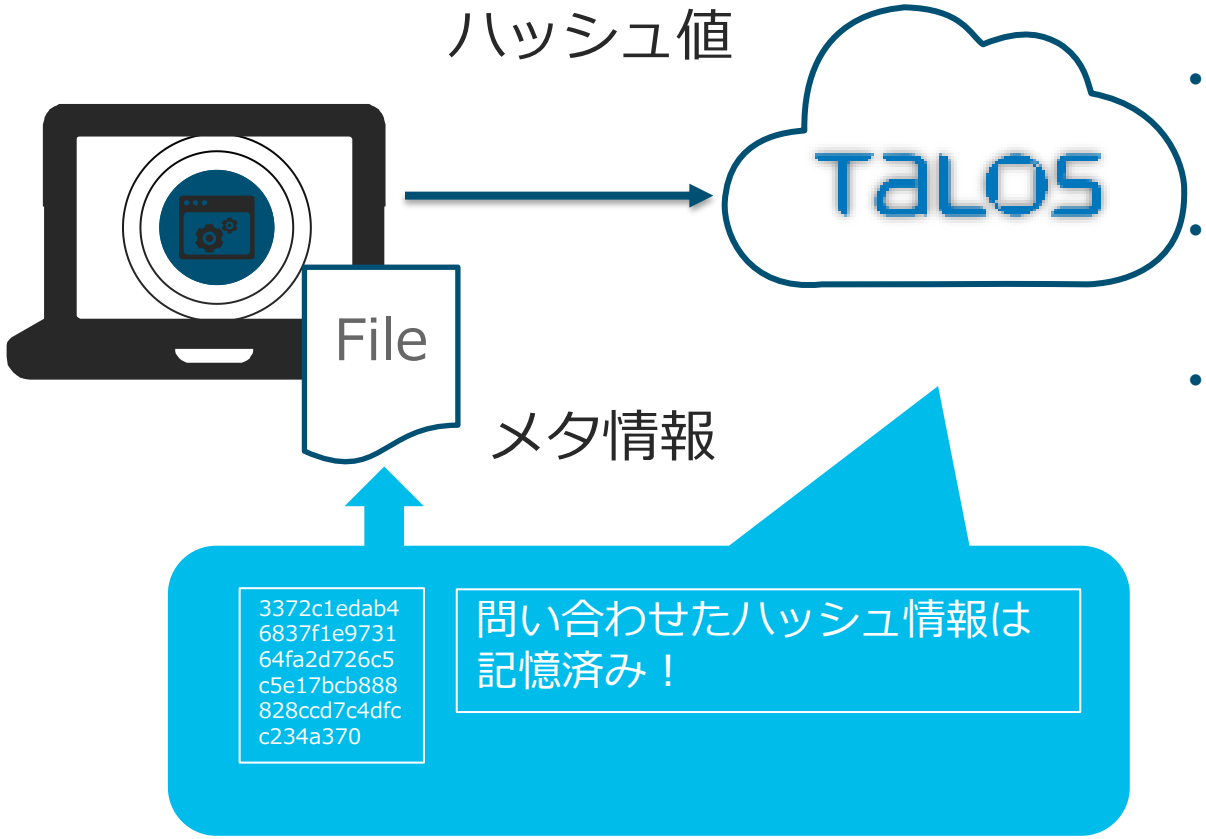
⇨ 検知、隔離、ブロック

クラウドリコール

EPP機能

EDR機能

もし、脅威データベース登録前のマルウェアが侵入してしまっても・・・
後日、脅威データベースが登録された際に侵入済みのマルウェアも自動隔離

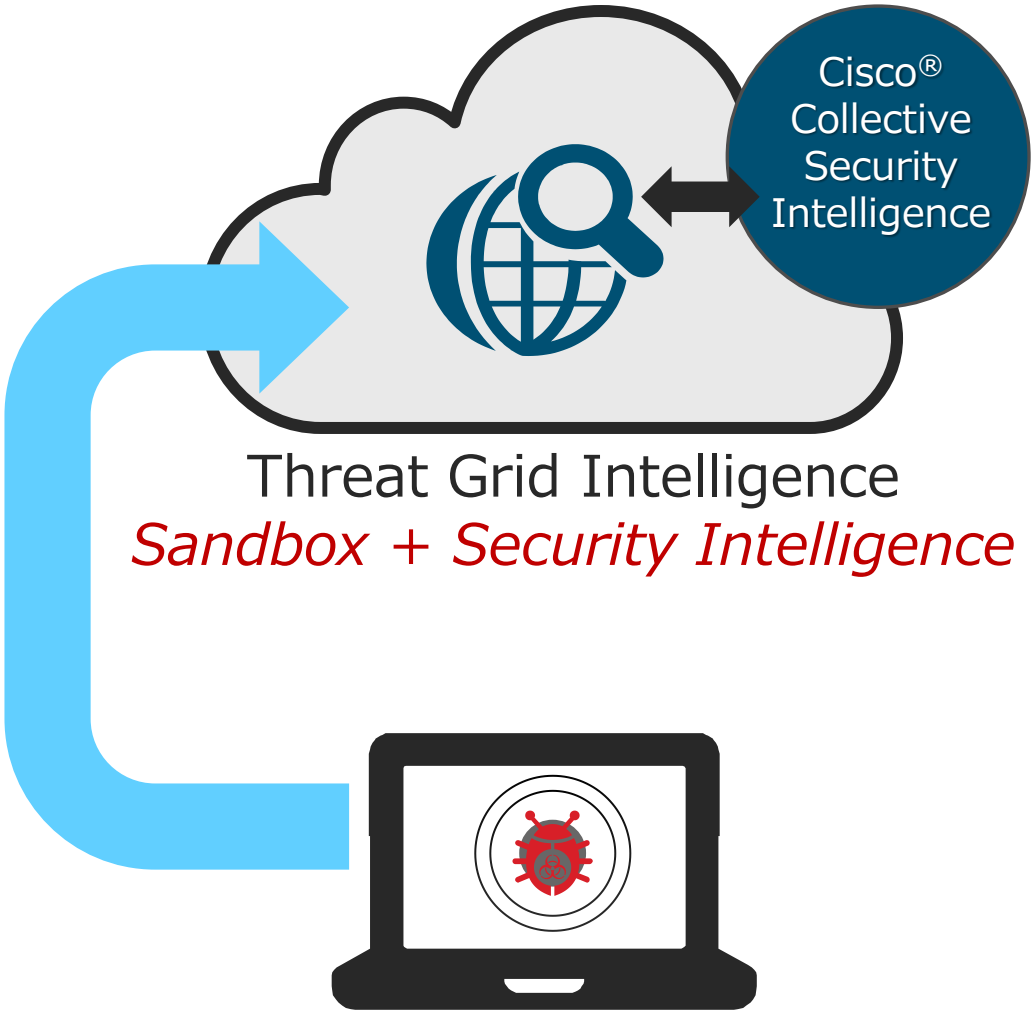


- 一度チェックしたハッシュ値はパスさせた後もクラウド上で記憶
- このハッシュ値がマルウェア判定になった場合、自動的に該当ファイルの隔離を実施
- 定期的なフルスキャンをする必要が無い
  → 他社アンチウイルスをご利用で、フルスキャンが終わらなくて・・・というお客様にご好評

Threat Grid＆セキュリティインテリジェンス

NGEPP機能

脅威データベースに情報がない不審なファイルは、Threat Gridというサンドボックス上の仮想OSで実際にマルウェアを実行



- Threat Gridは、不審なファイルを仮想環境で実行し、関連するプロセスや通信先などを総合的に評価する
- Threat Gridは、クラウド版とオンプレミス版から選択可能
  （クローズド環境でも利用可能）

EDR機能

インシデント・レスポンス
感染原因・範囲の特定(トラジェクトリ)

マルウェアが見つかった場合に、どの脆弱性を元に感染したのか、どのようなルートで感染したのかを可視化

デバイス トラジェクトリ

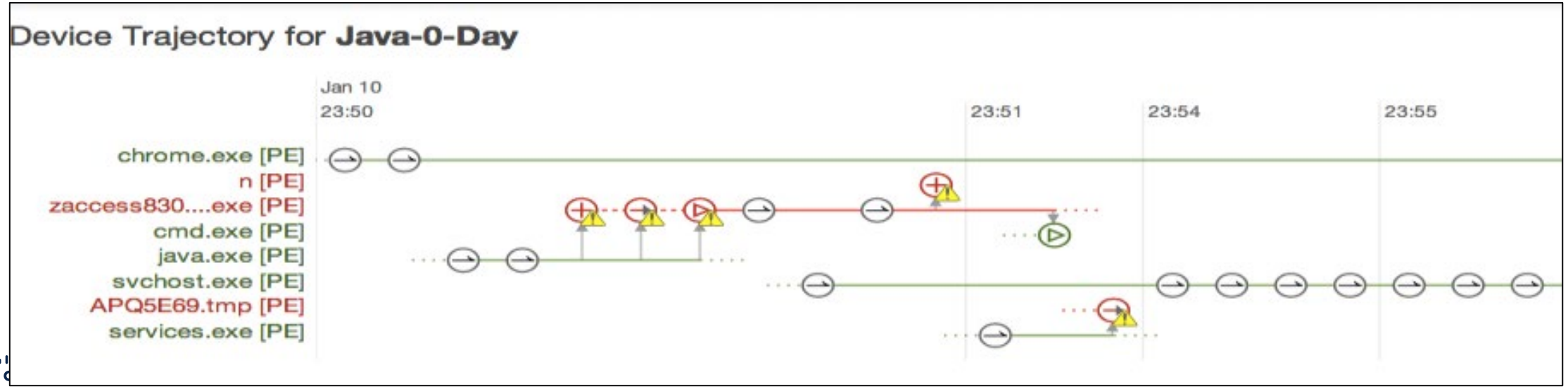
感染**原因**を特定

- マルウェア ファイルはどのようにシステムに入ってきたのか？
- どのような通信をおこなったのか？

ファイル トラジェクトリ

感染**範囲**を特定

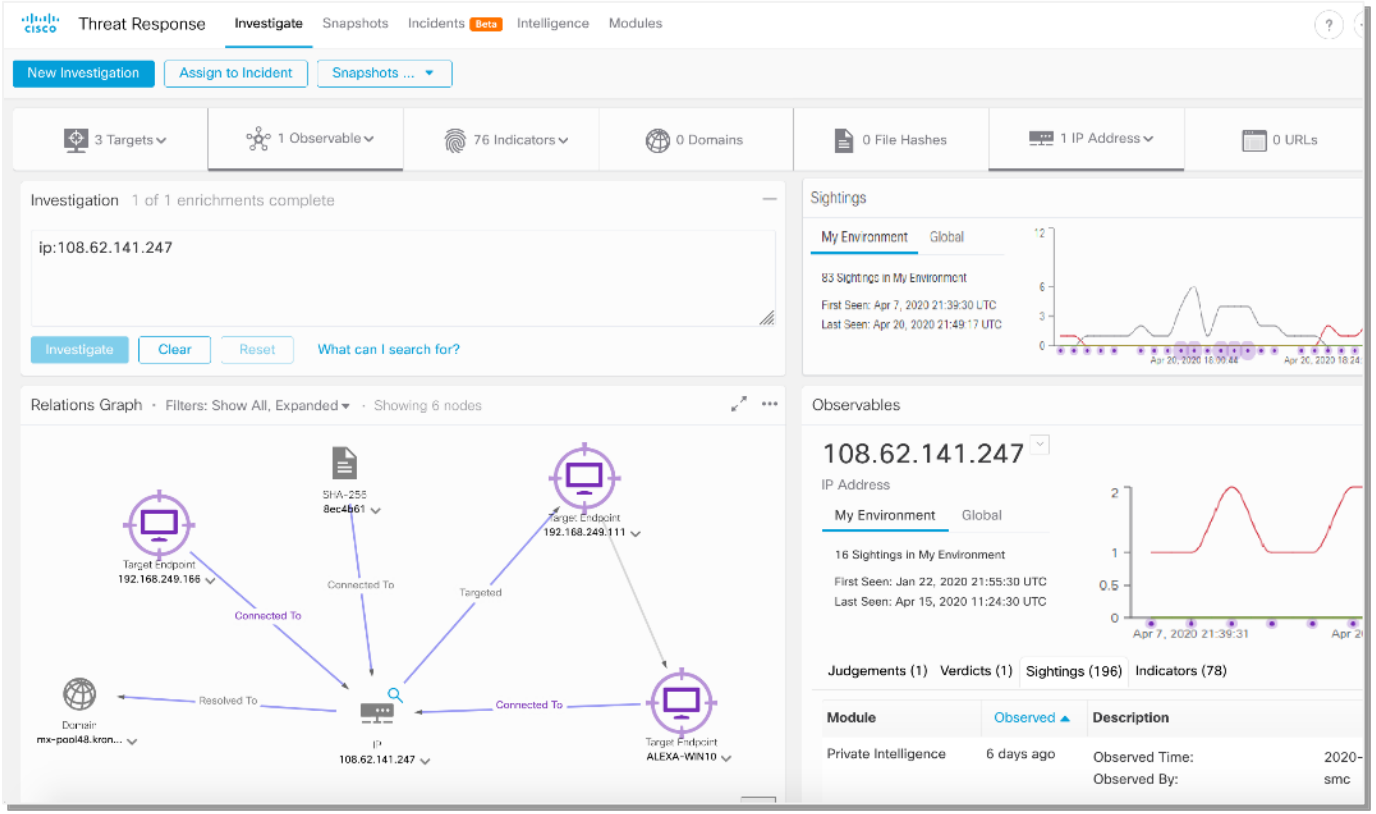
- 最初に感染したのは誰か？
- 現在そのマルウェアは どのシステム上に存在するのか？



Cisco SecureXとの統合
無償で提供されるXDRプラットフォーム

XDR機能

SecureX と呼ばれる無償のクラウドXDRプラットフォームで統合し、ダイナミックな防御とシンプルなクロスコントロールの脅威検知、対応、オーケストレーションを実現することで、自動化された脅威管理を実現します



- クラウドで提供されるインテリジェンスを用いて、複数の製品間でのマルウェアを検知・ブロックを実現
- 一貫したポリシーとカスタムブロック/許可リストにより、リアルタイムで「一度見たら、どこでもブロック」。

ライセンス概要

Security Services for Endpoint

機能	Essentials	Advantage	Premier
SecureX Platform Ciscoとそれ以外のコンポーネントを統合する、セキュリティオーケストレーションを含むCisco XDR プラットフォーム	●	●	●
次世代型エンドポイント 複雑な攻撃シナリオへ対抗する保護を含む、次世代型の保護テクノロジー	●	●	●
継続的なモニタリング 常に最新のエンジンを用いて、エンドポイントの全てのアクティビティを監視	●	●	●
動的なファイル分析 付帯されたサンドボックス環境	●	●	●
脆弱性の識別 環境を横断した脆弱性アプリケーションの迅速な識別	●	●	●
端末隔離 ネットワークから端末を切り離す事で脅威の拡散をストップ	●	●	●
Orbital Advanced Search エンドポイントでのリアルタイム調査によりアクティブハンティングを実現		●	●
Advanced Analytics Cloud access 動的ファイル分析ポータルへのフルアクセス		●	●
Threat Hunting Service 未知の脅威を列挙する拡張ハンティング機能			●
Endpoint Pro Service Advantage、Premier Tier向けの Managed SOC Services		●	●

オプションサービス

Extend Detection

脅威ハンティングサービス

脅威ハンティングサービスは、アナリストを中心としたプロアクティブなプロセスで、見逃していた隠れた高度な脅威を発見します。このサービスには、自動化されたプレイブックと、脅威検知の自動化が含まれています。本サービスは、Premier Tierに含まれます。

Extend Hunting

Managed Endpoint Detection and Response Services (Pro)

イベントが発生した後、調査員とアナリストのチームが調査を開始し、脅威を検出、抑制するための対応時間を短縮します。

Essentials ライセンス
EPP + EDR機能

多面的に防止

クラウドベースのレピュテーション確認

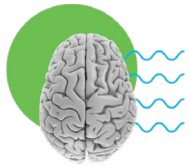
Secure Endpointは、エンドポイントでのファイルI/O操作（コピー、移動、実行など）を監視し、クラウドで配信される評定結果を利用して、ポリシー設定に基づいて悪意のあるアクティビティを自動的にブロック。 また、SHA256ハッシュに基づく1対1の検索に加えて、マルウェアに類似した特徴を検索するエンジンも搭載。また、パブリック クラウドにも、オンプレミス アプライアンスにも対応。

オフラインにおける保護

クラウド検索が利用できない場合（インターネットに接続されていない状態でエンドポイントが動作している場合）に備え、「オフライン」エンジンは、従来のシグネチャベースのアンチウイルス保護も提供し、より深いカバーを実現

メモリ ベース/ファイルレス アタック

最近の攻撃手法の多くは、従来のファイルベースのアンチマルウェア防御を回避するために特別に設計されているが、Exploit Preventionエンジンはメモリベースの防御であり、正当に実行されているプロセスのメモリ空間を操作しようとする試み（インジェクション攻撃など）を検出し、防止。コマンドライン可視化とスクリプト保護は、典型的な防御方法を回避するスクリプトベースまたはインタラクティブな攻撃を捕捉するように設計。



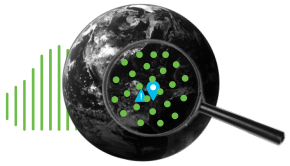
ふるまいベース検知

Secure Endpoint に搭載されているいくつかの検知エンジンは、悪意のある行動パターンの特定に特化。マリシャス アクティビティ防止エンジンは、ランサムウェアのような行動を時間差で検出してブロックすることに重点を置いており、ビヘイビア プロテクション エンジンは攻撃行動のパターンをクラウドからエンドポイントに配信し、マルチステップ攻撃を阻止する柔軟な方法を提供します。

ネットワークフロー相関

DFC（Device Flow Correlation）エンジンは、マルウェアやコマンド＆コントロール活動に関連する IP アドレスへのアウトバウンドネットワーク接続を検索するほか、カスタムのブロックリストや許可リストにも対応

継続的な検知



既知の脆弱性検知

悪意のある攻撃に対して脆弱であることが知られている一般的なソフトウェアアプリケーションのバージョンを実行しているエンドポイントを特定し、MITRE CVE データベースの説明と深刻度ランキングにリンクすることで、パッチが適用されるまで脆弱性のあるバージョンの実行をブロックするなどの事前対応を可能に

プリバレンス分析

プリバレンス分析では、環境内の異常な/一般的でないアプリケーションを特定し、それらを Cisco Secure Malware Analytics に自動的に送信。そこで何千もの行動指標に基づいてこれまでに知られていなかったマルウェア サンプルを特定、レトロスペクティブ イベントとしてエンドポイントに通知して隔離。

IoC (侵害の兆候)

ファイル、テレメトリ、侵入の各イベントは相関関係にあり、潜在的にアクティブな侵害として優先順位付けされるため、セキュリティチームはマルウェアのインシデントを特定し、それらを組織的な攻撃に結びつけることが可能。また、独自のカスタム IoC を作成して追跡することで、環境内のアプリケーションに特化した標的型攻撃を捕捉することが可能。

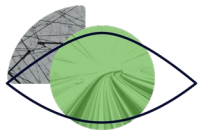
グローバル脅威アラート

グローバル 脅威アラート（旧コグニティブ脅威アナリティクス）は、Secure Endpoint との統合によりファイルレスまたはメモリのみのマルウェアや、Webブラウザのみで動作する感染症を発見。また、エンドポイントに出入りする Web トラフィックを監視することで、コマンド＆コントロールを検出し、攻撃サイクルの初期段階でマルウェアを捕捉。

API 連携

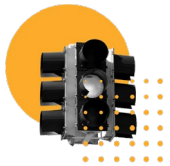
双方向（読み書き）のAPIが有効になったことで、ユーザーはサードパーティのセキュリティツールやSIEMとより簡単に統合することができ、管理コンソールにログインすることなくEndpointアカウントのデータやイベントにアクセスすることが可能 (詳細 https://github.com/CiscoSecurity)

エンドポイントに限らない応答



クラウドリコール (レトロスペクティブイベント)

レトロスペクティブ・セキュリティとは刻々と変化する現実に適応する能力を表し、ある時点での単一の許可／不許可の判断だけでなく、継続的な監視、新たな状況や新たな脅威情報への迅速な対応を提供

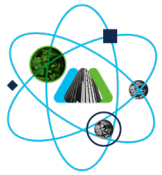


端末の隔離

侵害が疑われる、あるいは確認されたエンドポイントは、トラブルシューティングやフォレンジックを中断することなくワンクリックで、あるいは観測されたイベントの深刻度に応じて自動的に対応し、ネットワークの他の部分から隔離することが可能。問題解決後は簡単に復元することも可能。

自動化されたアクション

エンドポイントの隔離だけでなく、グループごとに異なる前提条件を設定することで他のアクションを自動的に起こすことも可能。他のアクションの例としては、分析用サンプルの提出、フォレンジックスナップショットの取得、影響を受けたシステムを別のポリシーグループへ移動する等。



XDR統合

SecureX によりオペレータはコンテキストを切り替えたり、何度もログインしたりすることなく、Secure Endpoint コンソールからすぐに他の製品での対応アクション（例えば、Umbrella の DNSでブロック）を開始することが可能。また、SecureX のオーケストレーションアクションにより複雑なワークフローを合理化し、自動化された対応を実現可能。

クロス プラットフォームのポリシー適用

同じクラウド・レピュテーション・ルックアップとマルウェア・アナリティクスのインターフェイスを使用するCisco Secure Firewall、Secure Emailなどの他の製品は、Secure Endpointコンソールに接続することができ、ブロックリストや許可リストに何かを追加するのは1か所で完了可能。

Advantage ライセンス
EDRを強化する追加機能

Advantage ライセンスによるアドバンスド サーチ機能

A
Advantage

```
SELECT name, version, install_location,
install_source, language, publisher,
uninstall_string, install_date
FROM programs
WHERE publisher LIKE "%solarwinds%";
```

Advantageライセンスは、Essentialsに加えて2つの機能を提供

1. Orbital Advanced Searchの高度な検索機能
   - レジストリキー、実行中のプロセス、インストールされたライブラリやアプリケーション、ユーザアカウント、ネットワーク接続などの多様な情報をエンドポイントから取得
   - SQLライクな直感的に理解しやすい検索言語(OSQuery)
   - MITRE ATT&CKに関連付けされた豊富なクエリーが用意されていて、簡単・すぐに使い始めることが可能。
   - ユースケースとして、プロアクティブな脅威探索、インシデント対応の迅速化、フォレンジック情報(スナップショット)の取得、IT運用およびコンプライアンスレポートなど
2. セキュア・マルウェア・アナリティクス
   - 任意のサンプルを手動で送信し解析、インタラクティブなサンドボックス上での操作、特定のアーティファクトを対象とした定義済み Orbital クエリが利用可能

https://github.com/Cisco-Talos/osquery_queries

A
Advantage

Orbital Advanced Search により、セキュリティとIT運用の連携強化、脅威ハンティングの簡素化を実現

主な機能

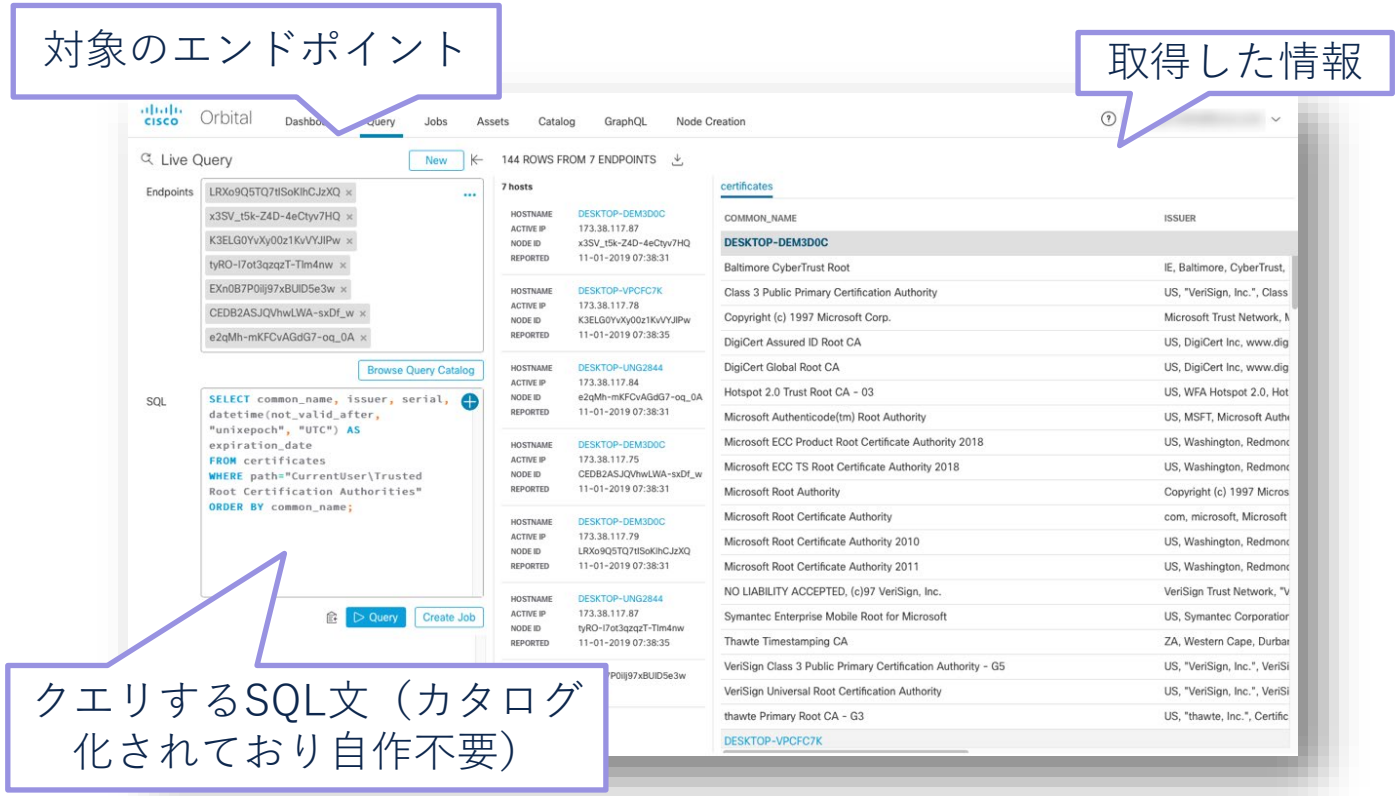
高度な検索、カスタマイズ可能な事前定義されたクエリ、フォレンジックスナップショット

主な使用例

脅威の探索、IT運用の実現、脆弱性とコンプライアンスの追跡

メリット

調査・対応の迅速化、調査・修復のシームレス化



Premier ライセンス
脅威ハンティング

P
Premier

SecureX 脅威ハンティング

Premier ライセンスはEssentialsとAdvantage に加えて脅威ハンティング を提供

- アナリストを中心としたプロセスで脅威ハンティングを実施
- Cisco Talosのリサーチャーの深い経験と豊富なプレイブックを活用
- 調査結果、レポート、アラートを Secure Endpoint コンソールに統合
- 脅威レポートで、詳細な説明とタイムライン、特定された脅威を修復するための推奨ステップを提示

Secure Endpoint Proサービス

Cisco Secure Endpoint Pro

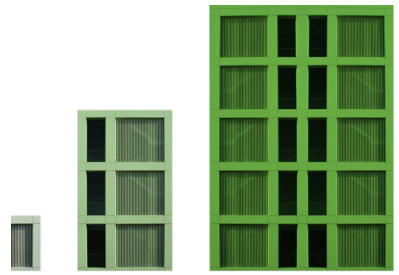
Ciscoが提供するSOCサービス

エンドポイントのセキュリティ確保という重い課題を解決します

シスコのセキュリティ専門家による専任のエリートチームが、24時間365日体制でエンドポイントの監視、検知、対応を行うので、お客様は心配する必要はありません

数時間ではなく、数分で脅威を検知し、対応します

シスコのスペシャリストが、Cisco SecureX プラットフォームによる自動化と高度なプレイブックを使用して、検知と応答時間を劇的に短縮します

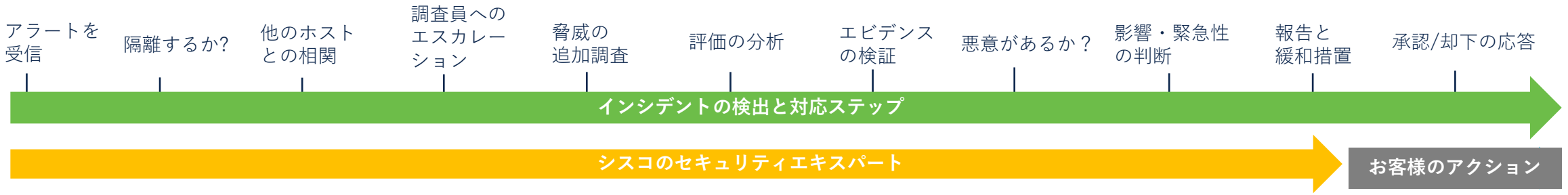


あらゆる脅威を調査し、最も重要なものに優先順位をつけます

すべてのインシデントを詳細に調査し、当社の専門家によるエビデンスに基づき、お客様が改善策を承認または拒否できるようにします

Cisco Secure Endpoint Pro の活用法

ユースケースの例



シスコの主なアクション

- シスコはセキュリティ警告を監視し、最初の事象から数分以内に適切な調査を行います
- Cisco SOCはSecure Endpointからすべてのイベントを取り込み、プレイブックやユースケースに照らし合わせて検証します
- 各インシデントは、24時間365日対応のSOCとIntelの専門チームによって優先順位付けされ、強化されます

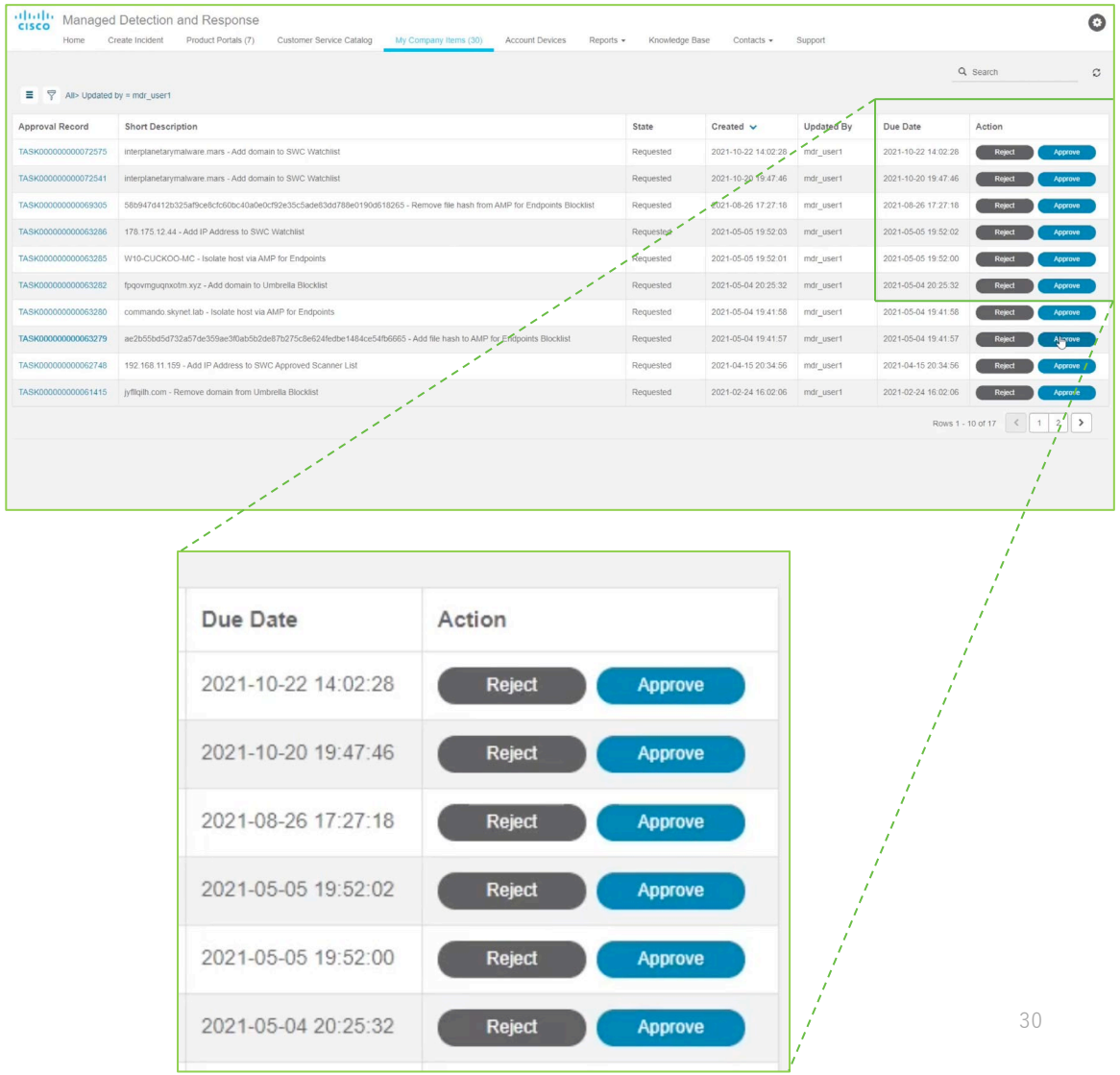
お客様との主なやり取り

- すべてのインシデントを調査・報告 - トップクラスのインシデントには1時間以内に電話連絡
- すべてのサービスインタラクションのための包括的なポータルは、可視化とダッシュボードのステータスを可能にします
- 改善アクションの承認または拒否、インシデントへのリンクの表示を簡単に行うことができます

Cisco Secure Endpoint Pro の活用法

Approval Response Actionインターフェイスでは、改善アクションの承認または拒否、インシデントへのリンクの表示を簡単に行うことができます

Approval Response Action インターフェース



第三者機関評価
事例
参考リンク集

AV-Comparatives によるエンドポイント検知評価

	防止率	誤検知数
マルウェア防止テスト	99.8%	0
リアル ワールド保護テスト	98.5%	1

Secure Endpoint の効果を実証

- 高い防御率
- 低い誤検知数

リアル ワールド保護テストにおける誤検知数
(テストケース数: 751)

	誤検知数
シスコ	1
Microsoft	0
Cybereason	8
CrowdStrike	12

ソース: https://www.av-comparatives.org/tests/business-security-test-march-april-2020-factsheet/

Radicati による Secure Endpoint 評価

シスコの強み

- Radicati は、シスコの包括的なセキュリティ・ポートフォリオとセキュア・エンドポイントに組み込まれた SecureX プラットフォームの統合の両方を、複数のセキュリティ・コントロール・ポイントにわたって広範なカバレッジ、自動的に強化される脅威のコンテキスト、統一された脅威対応能力を提供する最大の強みとして強調
- 同様に Secure Endpoint が Cisco Firewall、Secure Email、Umbrella、その他の Cisco ソリューションと豊富かつネイティブに統合されていることにより、ネットワークエッジからエンドポイントまでユーザーの環境をシームレスかつ包括的に可視化するシスコの能力を高く評価。また、Secure Endpoint の API がユーザーの既存のSIEMと統合できることも、さらなる価値を提供する機能として評価。
- また Radicati は、Secure Endpointが、習得や使用が容易で、EPPとEDRの両方を単一のエージェントで提供し、脅威の防止と修復の両方に対応する効率も高いことを強調。

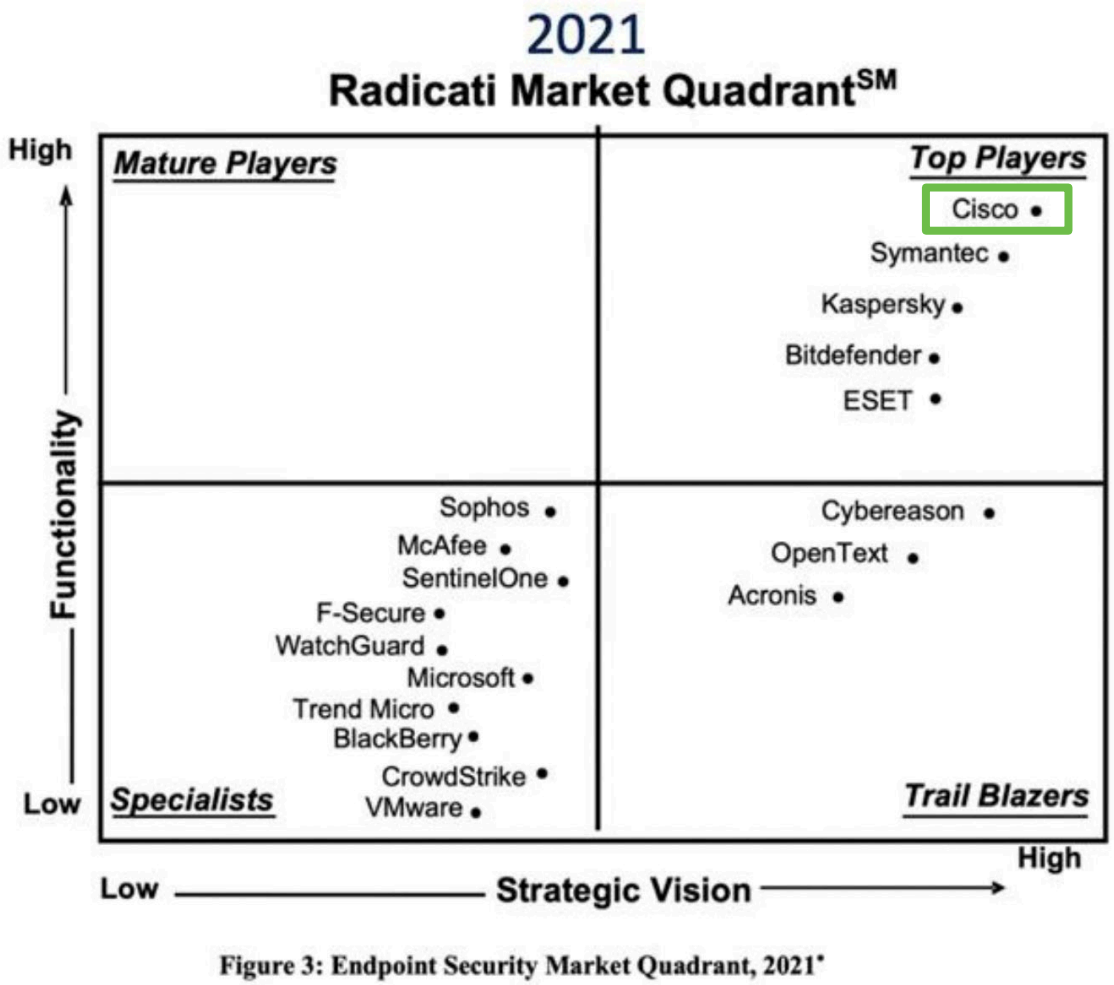
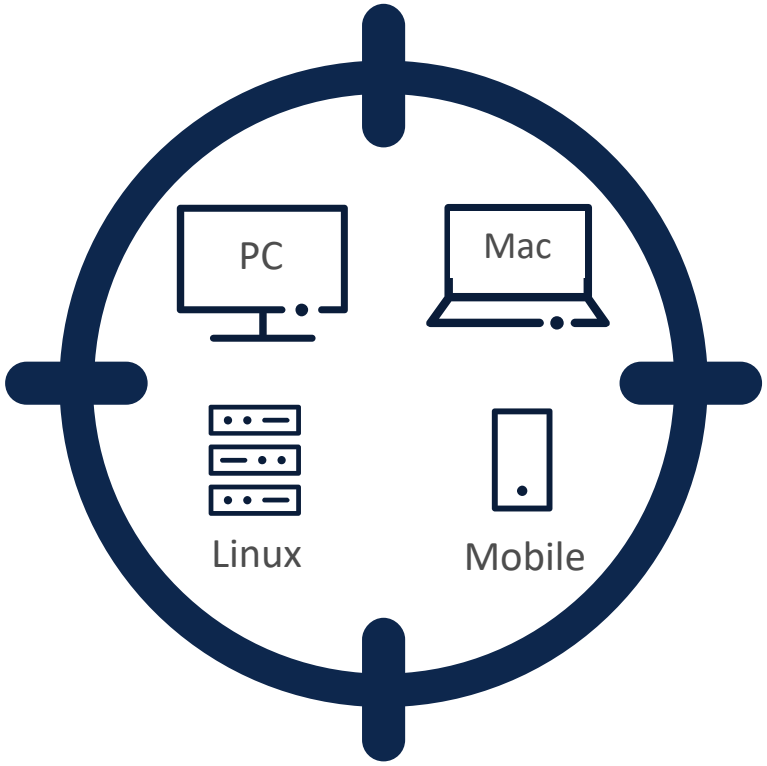


Figure 3: Endpoint Security Market Quadrant, 2021*

ソース https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/licensed-apt-protection-market-quadrant.pdf

Cisco Secure Endpoint導入実績

- グローバル (国内、海外)
  - 6,000 社以上で導入済み
  - 1,500万 以上のコネクタ
  - 最大規模は 14 万コネクタ
  - 数十社が 10 万コネクタ以上で導入
- 国内
  - 官公庁・自治体・大学・研究所・運輸・教育・金融・流通・出版/メディア・製造・小売等

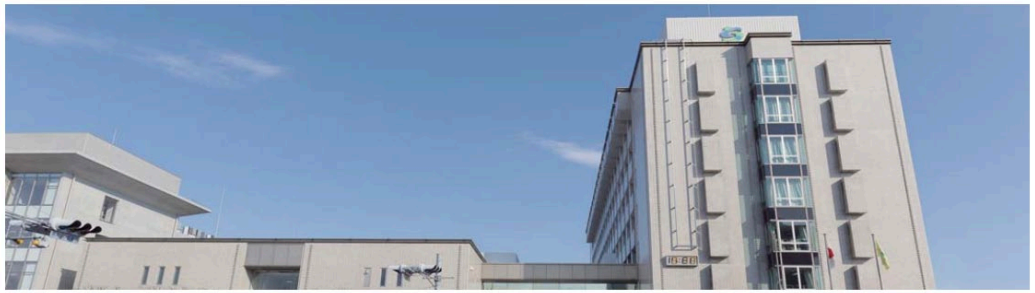


Cisco Secure Endpoint 公開事例 (国内)

シスコ セキュリティ ソリューション導入事例

佐賀市教育委員会

教員と児童生徒の PC を未知の脅威から守るため
クラウドと連携するマルウェア対策ソフトを導入



Cisco AMP はクラウド上に蓄積される最新の情報と常に照合して脅威を判定するという新しい仕組みで、標的型攻撃やゼロデイ攻撃への備えを万全にできる点を評価しました。

—— 佐賀市教育委員会 こども教育部 学校教育課
ICT 利活用教育係 主幹 兼 係長　石橋 秀昭 氏

シスコ セキュリティ ソリューション導入事例

静新SBSグループ

(株式会社 静岡新聞社/静岡放送 株式会社)

多種多様な職種とデバイス、働き方の変化に対応する
新たな統合セキュリティ対策を実現

インシデントが起きてからではなく、未然に防いでいることが可視化されるシスコ セキュリティ ソリューションの満足度は高いものがあります。

—— 株式会社 静岡新聞社 静岡放送 株式会社 システム統括局 システムセンター副部長 松田 武之 氏

Secure Endpoint 事例紹介URL
https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/customer-stories-listing.html

参考リンク集

- Sales Connect セキュリティ資料

  「PSU VoD/個別製品トレーニング」の「Endpoint(AMP)」タブに資料がございます。

製品情報

- PSU-VoD-SEC-AMP4E-01 概要のご紹介-AMP4E-01 Overview
- PSU-VoD-SEC-AMP4E-02 機能のご紹介-AMP4E-02 Function Introduction
- PSU-VoD-SEC-AMP 各種エンジンの解説1-AMP description
- PSU-VoD-SEC-Cisco Secure Endpoint(旧AMP) 各種エンジンの解説2-AMP description
- Secureざっくり CSC-Zakkuri Cisco Security Connector

デモンストレーション

- PSU-VoD-SEC-AMP デモンストレーション-AMP DEMO - Video

30日間フリートライアル

- 30 日間のフリートライアル
- 延長も可能（要申請）
- 案件登録でシスコの製品担当が POV を支援

SECURE