Cisco Secure Endpoint

目次

製品の概要

Cisco ® Secure Endpoint は、クラウドベースの分析機能を活用して、防御、検出、脅威ハンティング、対応機能を統合ソリューションで提供します。Cisco Secure Endpoint は、パブリッククラウドまたはプライベートクラウド環境で Windows、Mac、Linux、Android、iOS デバイスを保護します。

Cisco Secure Endpoint は、包括的な保護、検出、対応、およびユーザーアクセス管理を提供する単一エージェントのソリューションで、エンドポイントを脅威から守ることができます。Cisco Secure Endpoint には SecureX™ プラットフォームが組み込まれており、Extended Detection and Response（XDR）機能も搭載されています。新しく導入された Cisco Secure MDR for Endpoint は、Cisco Secure Endpoint の優れた機能とセキュリティ運用の専門知識を組み合わせて、脅威を検出して対応するまでの平均時間を大幅に短縮します。

利点

急速に進化するマルウェアの世界では、脅威の検出がますます困難になっています。このような脅威の中でも最も高度な 1% については、最終的にネットワークに侵入して大きな混乱を引き起こす深刻な脅威ですが、検出されない可能性があります。ただし、Cisco Secure Endpoint は、その 1% に対する包括的な保護を提供します。Cisco Secure Endpoint は、侵害を防止し、侵入ポイントでマルウェアをブロックし、ファイルとプロセスのアクティビティを継続的に監視および分析して、最前線の防御をすり抜ける可能性のある脅威を迅速に検出し、封じ込め、修復します。

最近導入された Cisco Secure MDR for Endpoint は、Cisco Talos 脅威調査がサポートする統合された脅威インテリジェンス、定義済みの調査、対応プレイブックを利用するシスコのセキュリティ研究者、調査員、対応担当者のエリートチームを活用して、人間とマシンのインテリジェンスを組み合わせることで、さらなる価値を提供します。専用のグローバル セキュリティ オペレーション センター（SOC）から 24 時間 365 日体制で、脅威を特定して阻止し、マルウェアをブロックし、最前線の防御をすり抜ける高度な脅威も封じ込めて修復アクションを推奨できます。

予防

脅威を最も早い時点で阻止することで、エンドポイントへの損害を最小限に抑え、侵害後のダウンタイムを短縮できます。Cisco Secure Endpoint は、マルウェアをリアルタイムで阻止する堅牢な一連の予防技術を採用しており、今日の最も一般的な攻撃や新たなサイバー脅威からエンドポイントを保護します。

ファイルレピュテーション：Cisco Secure Endpoint には、これまでに確認されたすべてのファイルとそれぞれの判定情報（正常か悪質か）の包括的なデータベースが含まれています。そのため、既知のマルウェアは、プロセッサに負荷がかかるスキャンなしに、侵入ポイントで迅速かつ簡単に隔離されます。

ウイルス対策：Cisco Secure Endpoint には、Windows と Mac 両方または Linux のエンドポイントに対応した、絶えず更新される定義ベースのウイルス対策エンジンが含まれています。どのエンドポイントでもカスタム署名ベースの検出を活用できるため、管理者は堅牢な制御機能を提供するとともに、ブラックリストを適用できます。ウイルス対策シグネチャデータベースは、各エンドポイントにローカルに存在するため、クラウド接続に依存せずに動作できます。これにより、エンドポイントはオンラインでもオフラインでも確実に保護されます。

ポリモーフィックマルウェアの検出：マルウェア攻撃者は、一般的な検出手法を回避するために、同じマルウェアのさまざまなバリエーションを作成することが少なくありません。Cisco Secure Endpoint は、ルーズフィンガープリントによってこれらの亜種やポリモーフィックマルウェアを検出できます。ルーズフィンガープリントは、疑わしいファイルコンテンツと既知のマルウェアファミリのコンテンツに見られる類似点を探し、一致する部分がある場合は問題があるものと判断します。

機械学習分析：Cisco Secure Endpoint は、既知のマルウェアの属性に基づいて悪意のあるファイルやアクティビティを特定できるよう、アルゴリズムによってトレーニングされます。Cisco Secure Endpoint の機械学習機能には、より優れた高精度のモデルを実現するために、Cisco Talos™ の包括的なデータセットが提供されます。機械学習を組み合わせることにより、未知のマルウェアを侵入ポイントで検出できます。

エクスプロイト防止：メモリ攻撃がエンドポイントに侵入する可能性があり、マルウェアはアプリケーションやオペレーティング システム プロセスの脆弱性を悪用してセキュリティ防御を回避します。エクスプロイト防止機能は、エクスプロイトベースのメモリインジェクション攻撃からエンドポイントを保護します。

スクリプト保護：Cisco Secure Endpoint は、エンドポイントで実行されるスクリプトへのデバイストラジェクトリの可視性を向上させ、マルウェアで一般的に使用されるスクリプトベースの攻撃を防ぎます。スクリプト制御により、悪用されやすいデスクトップ アプリケーションやその子プロセスによって特定の DLL がロードされることをエクスプロイト防止エンジンで防げるようになるため、保護が強化されます。

動作保護：Cisco Secure Endpoint の強化された動作分析は、すべてのユーザーとエンドポイントのアクティビティを絶えず監視し、脅威の進化に合わせて動的に更新される一連の攻撃アクティビティパターンに次々と生成されるアクティビティレコードを照合することにより、悪意のある動作をリアルタイムで防ぎます。たとえば、きめ細かい制御や、環境寄生型ツールの悪用からの保護が可能になります。

デバイス制御：Cisco Secure Endpoint を使用すると、USB 大容量ストレージデバイスの使用を制御し、これらのデバイスからの攻撃を防ぐことができます。可視性により、エンドポイント管理者は、デバイスの接続/切断イベントやアクセス違反イベントを確認したり、API を使用してデバイス制御の設定やルールを管理したりすることができます。制御により、管理者はデバイスが接続されたときのデフォルトの動作を定義し、これらのデバイスを制御するためのさまざまなアプローチをさらにサポートするきめ細かいルールを作成することができます。

検出

完全な次世代エンドポイント セキュリティ ソリューションにはマルウェア防御技術が不可欠ですが、高度な脅威に対抗するにはさらなる対策が必要です。Cisco Secure Endpoint は、エンドポイントを継続的に監視して、新たな未知の脅威を検出します。

悪意のあるアクティビティからの保護：Cisco Secure Endpoint は、すべてのエンドポイントのアクティビティを継続的に監視し、エンドポイントで実行されているプログラムの異常な動作をランタイムで検出してブロックします。たとえば、エンドポイントの動作からランサムウェアであると示唆される場合は、問題のあるプロセスを終了して、エンドポイントの暗号化を防ぎ、攻撃を阻止します。

クラウドベースでのセキュリティ侵害の兆候：業界をリードするシスコの脅威インテリジェンス組織である Talos は、絶えずマルウェアを分析して新たな種類の脅威を見つけ出し、新たな脅威の動作プロファイルとフォレンジックプロファイルを構築します。侵害の兆候（IoC）としても知られています。フォレンジックデータとは、ファイルの場所やレジストリキー値の変更など、侵害されたシステムを管理者が特定できるよう支援するために Cisco Secure Endpoint で使用できるすべてのデータです。

ホストベースの IoC：管理者は、インシデント対応で使用する独自のカスタム IoC を作成し、エンドポイント環境全体で侵害後の兆候をスキャンできます。カスタム IoC はオープンスタンダード形式（OpenIOC）で記述されるため、既存のインテリジェンスフィードからデータを簡単に活用できます。

脆弱性：Advantage 階層または Premier 階層のお客様の場合、Cisco Secure Endpoint は Kenna Security と統合され、環境内の OS の脆弱性を特定して、攻撃対象領域を削減します。脆弱性のあるエンドポイントにはリスクスコアが付けられ、管理者は修復に優先順位を付けることができます。

低拡散度：Cisco Secure Endpoint は、エンドポイント全体にわたってわずかな数しか存在しない実行可能ファイルを自動的に識別し、クラウドベースのサンドボックスでそれらのサンプルを分析して、新たな脅威を発見します。標的型マルウェアや高度で永続的な脅威は、多くの場合、検出をすり抜けてごく少数のエンドポイントで攻撃を開始しますが、拡散度は高くありません。Cisco Secure Endpoint は、脅威ハンティングを自動的に行い、他の方法では見逃していたはずの 1% の脅威を簡単に発見します。

脅威ハンティング（Threat hunting）

SecureX Threat Hunting 機能は、アナリスト向けのプロアクティブなアプローチを採用し、潜んでいる高度な脅威を検出します。この機能は、Cisco Secure Endpoint 内の新しい Premier ライセンス階層の一部としてのみ提供されます。インシデント対応担当者は、この機能を利用することで、攻撃が発見された経緯や攻撃の進展状況を知ることができ、また、実施すべき次の対応を確認することができます。SecureX Threat Hunting は被害が生じる前に攻撃を発見して阻止することを目的としています。定期的に継続して Threat Hunting 機能を活用することで、組織は、脆弱性やリスクに関する知識を深め、セキュリティ環境をさらに強化できるというメリットも得られます。

SecureX Threat Hunting は、Talos と Cisco Research and Efficacy Team の両方の専門知識を活用して、お客様の環境内で見つかった脅威の特定をサポートします。シスコは、精度の高いアラートを生成するプレイブックに基づいて、人間主導型ながら高度に自動化された検出機能を提供しています。検出プロセスでは、選りすぐりの脅威検出者の専門知識および 20 年に及ぶ業界での経験と、Orbital Advanced Search テクノロジーを独自に組み合わせ、より高度な脅威を積極的に検出します。

Secure Endpoint Premier ライセンスは、世界中のすべての地域で発注できます。ただし、現時点において、お客様のテレメトリを処理して脅威を検出する SecureX Threat Hunting のインフラストラクチャを発注できるのは北米のみです。

Cisco Secure Endpoint での対応

予防策をすり抜けることができる高度な脅威の数と種類が増え続ける状況では、侵害はいつか起こるものと捉える必要があります。そのような考え方に基づいて、感染したエンドポイントの容易な特定や攻撃範囲の把握に役立つ強力なツールセットを展開する必要があります。Cisco Secure Endpoint は、さまざまな防止機能と検出機能に加えて、きめ細かいエンドポイントの可視性と対応ツールを提供して、セキュリティ侵害に迅速かつ効率的に対処します。

ダッシュボードと受信トレイ：レポートは、イベントの列挙と集約に限定されません。Cisco Secure Endpoint に組み込まれた実用的なダッシュボードにより、管理を合理化して対応を迅速化できます。イベントとエンドポイントは優先順位で分類され、調査の進捗状況を追跡するワークフローに関連付けられます。

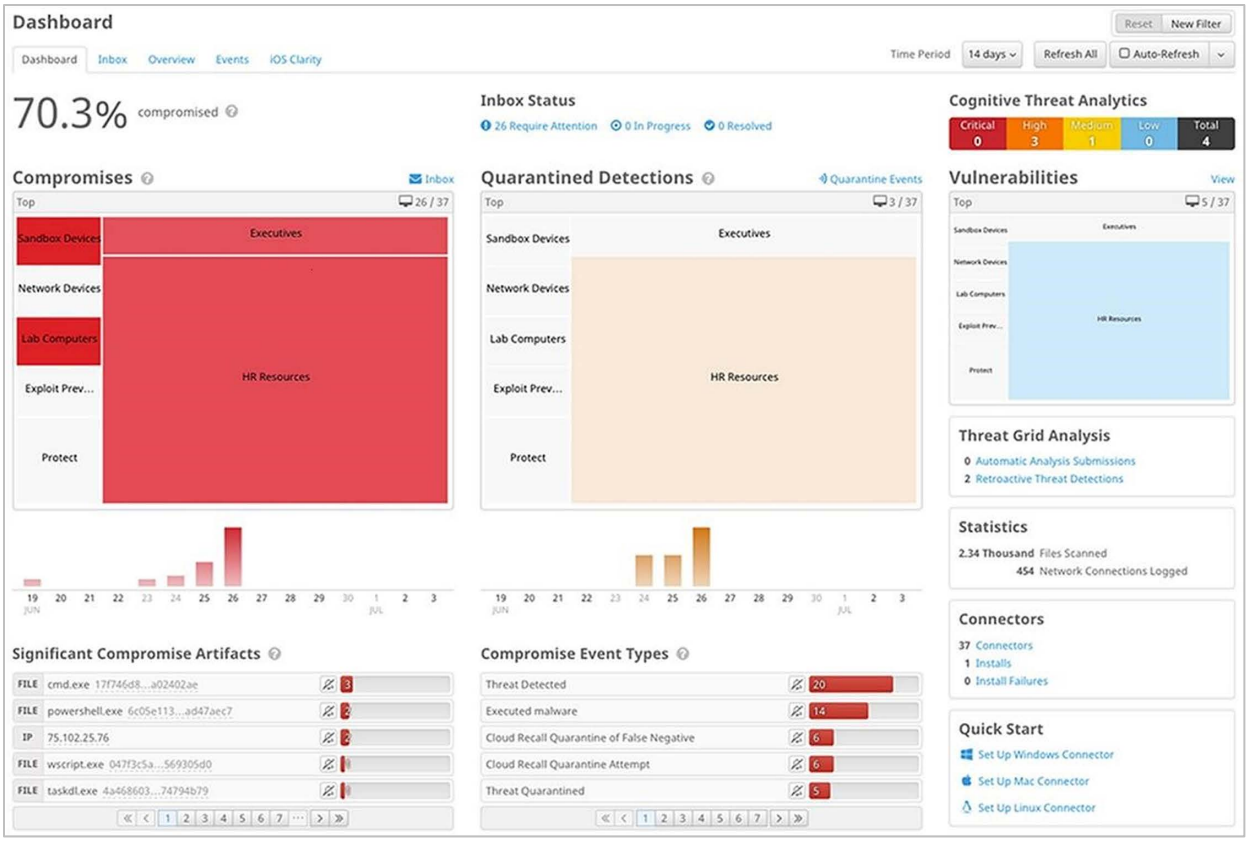

図 1.
Cisco Secure Endpoint のダッシュボード

エンドポイント フォレンジック：ファイルトラジェクトリやデバイストラジェクトリなどの強力なツールは、Cisco Secure Endpoint の継続的な分析機能を使用して脅威の全範囲を示します。Cisco Secure Endpoint は影響を受けるすべてのアプリケーション、プロセス、システムを把握し、最初の侵入を正確に特定すると同時に、侵入方法と侵入ポイントも特定します。これらの機能は、攻撃者が他のシステムへの足がかりを得るために使用しているマルウェアのゲートウェイやパスを特定して、問題の範囲をすばやく把握するのに役立ちます。

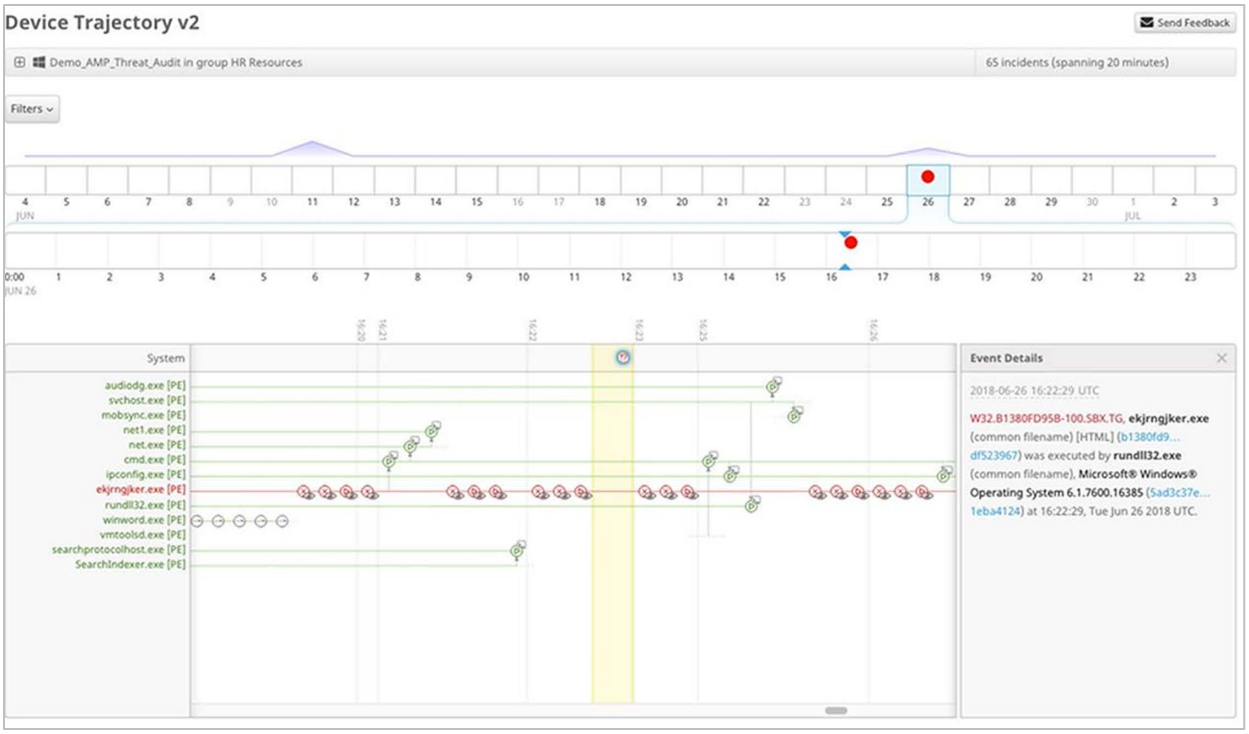

図 2.
Cisco Secure Endpoint のデバイストラジェクトリ

動的分析：Cisco Secure Endpoint には、疑わしいファイルの動作を分析するための、Cisco Threat Grid を搭載した非常にセキュアなサンドボックス環境が組み込まれています。ファイル分析により、動作のシビラティ（重大度）、元のファイル名、実行されているマルウェアのスクリーンショット、サンプルパケットキャプチャなど、ファイルに関する詳細な情報が生成されます。このような情報を入手することで、感染の封じ込めと将来の攻撃阻止に何が必要かをより的確に理解できます。

レトロスペクティブ セキュリティ：Cisco Secure Endpoint は、環境に侵入した高度な脅威を自動的に検出する特許取得済みのテクノロジーを採用しています。Cisco Secure Endpoint は、継続的な監視を利用して、新しい脅威情報と履歴を関連付け、悪意のある動作をファイルが見せ始めた時点でそのファイルを自動的に隔離します。このように最新の脅威への対応が自動化されているため、検出時間が短縮し、マルウェアの拡散が大幅に低減します。

コマンドラインの可視性：コマンドライン引数を可視化し、Windows ユーティリティなどの正当なアプリケーションが悪意のある目的で使用されていないかどうかを確認できます。Cisco Secure Endpoint は、vssadmin を使用したシャドウコピーの削除やセーフブートの無効化、PowerShell ベースのエクスプロイト、特権昇格、アクセス制御リストの変更、システム列挙の試行など、検出が困難な動作を発見できます。

エンドポイントの隔離：侵害されたエンドポイントを隔離して脅威の拡散を阻止し、C&C との通信を防止すると同時に、Cisco Secure Endpoint クラウドなどの信頼できるリソースとの情報交換を可能にすることが重要です。エンドポイントの隔離により、感染したエンドポイントを 1 クリックで隔離するとともに、信頼できるネットワークリソースをホワイトリストに登録できます。エンドポイントの隔離は、管理者なら 1 クリックで解除でき、ユーザーがロック解除コードを入力して解除することもできます。

詳細検索：詳細検索は、Cisco Secure Endpoint の高度な機能です。100 種類以上のクエリがあらかじめ用意されているため、セキュリティの調査と脅威ハンティングが容易になり、あらゆるエンドポイントで複雑なクエリをすばやく実行できます。これにより、現在の状態のスナップショットを取得して、任意の時点でエンドポイントに起きたことを詳細に可視化できます。インシデント対応、脅威ハンティング、IT 運用、脆弱性とコンプライアンスのいずれに伴う調査でも、詳細検索により、エンドポイントに関する必要な情報を迅速に得られます。

Cisco Secure MDR for Endpoint

Cisco Secure MDR for Endpoint は、オプションのエンドポイントの検出および対応（EDR）サービスです。Cisco Security Operations Center（SOC）は、Cisco Secure Endpoint からすべてのイベントを取り込み、調査、エンリッチメント、インテリジェンス収集を実行し、それらをプレイブックとユースケースに照らしてレビューします（広範な自動化と人間によるレビューやエンリッチメントを含む）。これらのインシデントは P1 ~ P4（P1/P2 は直接通信を伴う）として優先順位付けされ、できるだけ早期に軽減策が実施されます。シスコはセキュリティアラートを監視し、最初のイベントから数分以内に適切に対応します。したがって、お客様は組織にとって重要なことに集中できます。

ダッシュボードと受信トレイ：Cisco Secure MDR for Endpoint サービスポータルは、サービスのメインインターフェイスです。このポータルでは、すべてのインシデント、サポート、フィードバック、メトリックなどを利用できます。新しいインシデントまたは既存のインシデントを介して、SOC にすばやく簡単に直接連絡できます。サービスポータルのホームページには、最新のインシデントを案内するウィジェットがあり、すべてのインシデントが優先度順にリストされます。Approval Response Action インターフェイスは、インシデントへのリンクに加えて、推奨される修復措置の拒否または承認のためのポータルを提供します。また、セキュリティニュースのフィード、お客様によるレビュー待ちのインシデント、最新のナレッジベース記事も提供します。

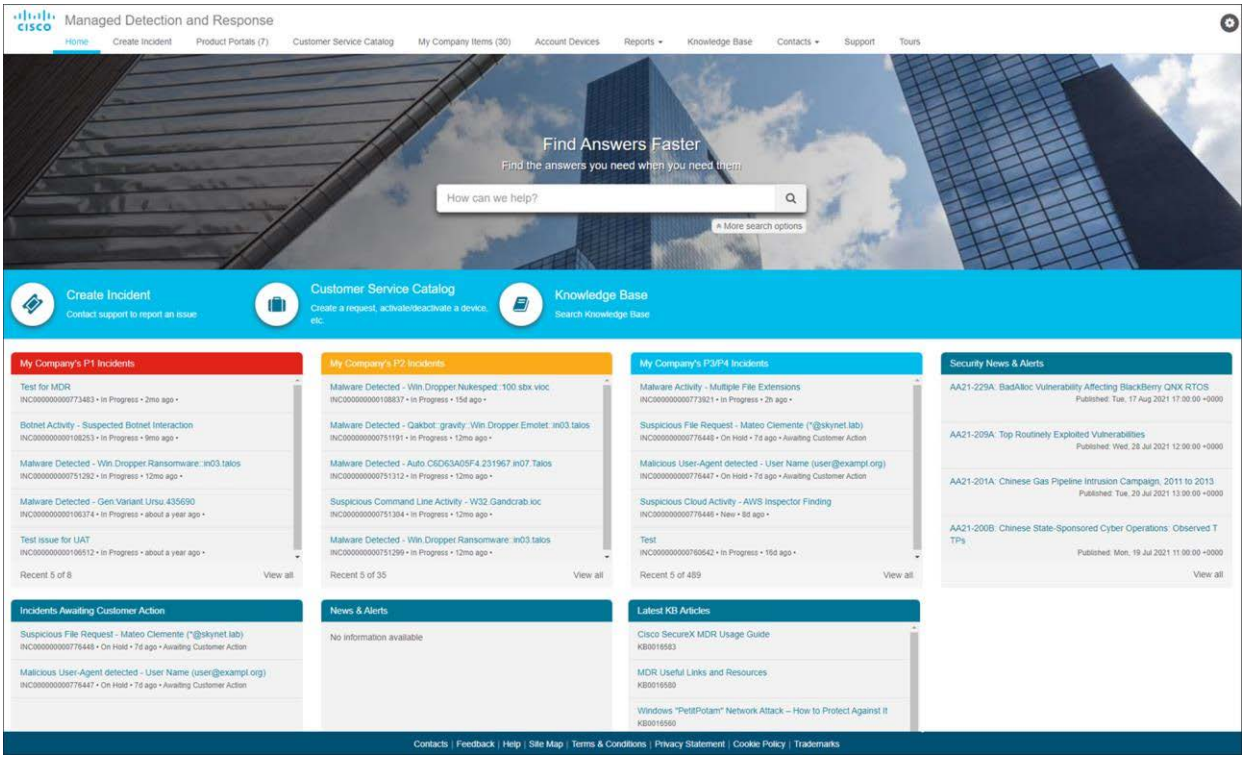

図 3.
Cisco Secure MDR for Endpoint ポータル

サービスカタログでは、フィードバックの送信、サポートのリクエスト、インテリジェンスレポートのリクエストなどを行うことができます。

Cisco Secure MDR for Endpoint のナレッジベースには、サービスとその製品のさまざまな側面に関する有用なガイドやドキュメントが用意されています。Cisco Secure MDR for Endpoint では、リリースノート、製品ガイドとサービスガイド、ベストプラクティス、ライセンス管理情報、専任のインテリジェンスチームから直接提供される詳細なインテリジェンス記事やアドバイザリを利用できます。

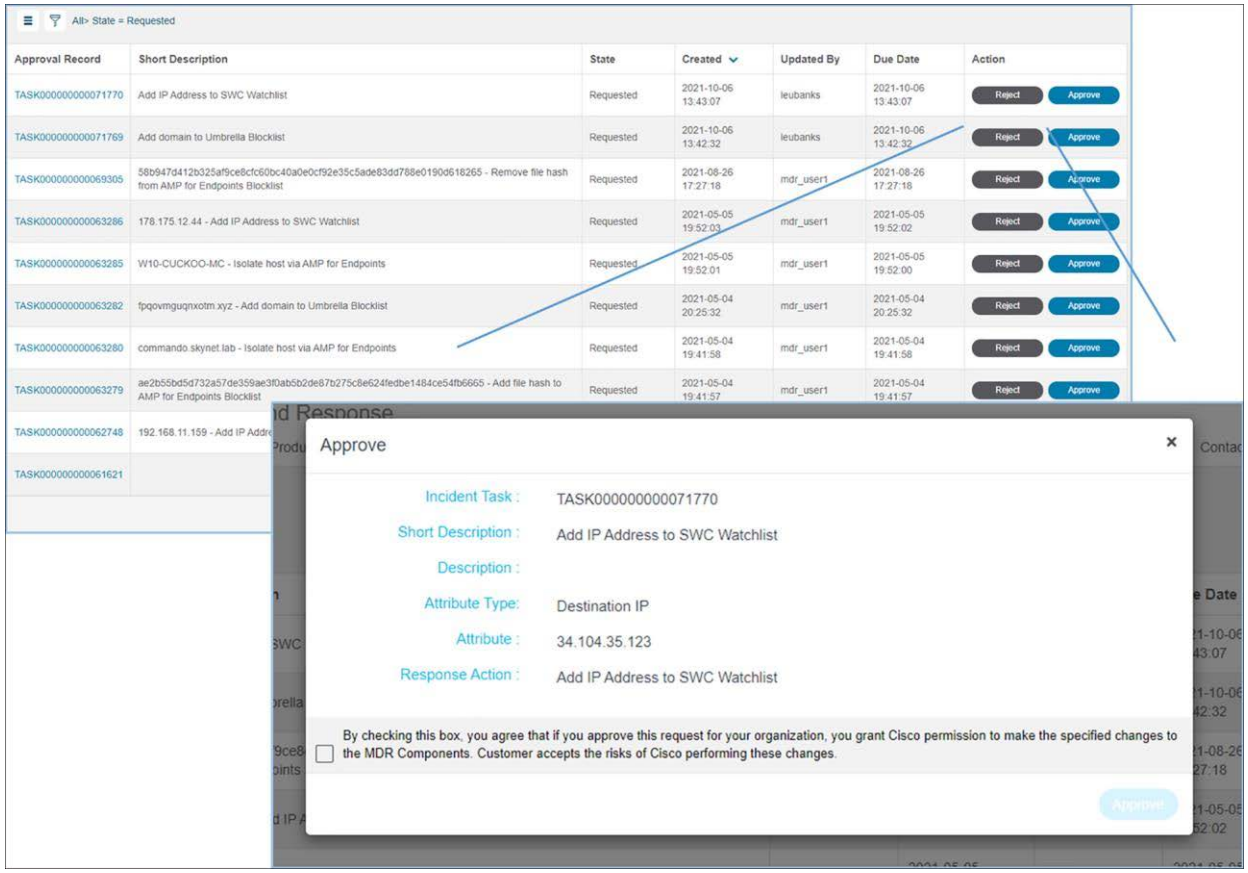

図 4.
Approval Response Action インターフェイス

Cisco Secure Endpoint の独立したサードパーティによる評価

プラットフォームサポートと互換性

Cisco Secure Endpoint は、次のオペレーティングシステムと互換性があります。

- Windows（詳細情報はこちら）
  - Windows 7*（ESU が必要）
  - Windows 8*、8.1*、10、11
  - Windows Server 2008 R2*（ESU が必要）
  - Windows Server 2012、2012 R2、2016、2019、2022
- Linux（詳細情報はこちら）
  - Red Hat Enterprise Linux 6、7、8
  - CentOS 6、7、8
  - Oracle Linux RHCK（Red Hat Compatible Kernel）6、7、8
  - Oracle UEK（Unbreakable Enterprise Kernels）7、8
  - Alma Linux 8
  - Rocky Linux 8
  - Ubuntu Linux 18.04、20.04
  - Amazon Linux 2 – Kernel 4.14 以降
  - SUSE Enterprise Linux 15 / openSUSE Leap 15
  - Debian Linux 10、11
- MacOS および iOS（詳細情報はこちら）
  - macOS 10.13、10.14、10.15、11、12
  - iOS 14.4 以降
- Android
  - Android 8.0（Oreo）以降

*レガシー OS システムへの制限が適用される場合があります

保証情報

保証情報については、Cisco.com の「製品保証」ページを参照してください。

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用、拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

次の表に、環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを示します。

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

発注情報

ご注文ガイドはこちらから入手してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 か国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

詳細については、次のリンクをご覧ください。Cisco Secure Endpoint

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

1019-2023-000-X