Multicloud Defense Controller の機能および機能拡張

バージョン 25.01（2025 年 1 月 6 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- UI のルックアンドフィールが向上します。
- 全体的なパフォーマンスが向上します。

バージョン 24.12（2024 年 12 月 2 日）

機能

このリリースには、次の機能が含まれています。

アクティブセッションと定期セッションのトラフィック概要の改善

以前は、イベントは接続セッションが閉じられたか、終了された場合にのみ利用可能でした。トラフィックの概要で、セッションがアクティブな5分ごとにイベントを投稿するようになりました。この機能は、一度にいくつのセッションが進行中であるかを調べるのに役立ちます。概要ページの [すべてのイベント（All Events）] チェックボックスを選択して、開いている接続のリストを展開し、チェックボックスをオフにすると、閉じているセッションだけが表示されます。

AI Defense（プライベートプレビュー）

Multicloud Defense は、生成 AI アプリケーションを検出して保護するための AI Defense のプライベートプレビューをサポートするようになりました。詳細については、シスコまでお問い合わせください。

バージョン 24.10（2024 年 10 月 29 日）

このリリースには、次の機能と機能拡張が含まれています。

機能

AWS CloudWAN

Multicloud Defense で、サービス VPC とネットワークセグメントと組み合わせて AWS CloudWAN を使用するオプションが提供されるようになりました。AWS CloudWAN は、お客様のデータセンター、分散拠点、クラウドリソースを接続するグローバルネットワークを構築、管理、監視するプロセスを簡素化します。詳細については、「Create a Service VPC or VNet」を参照してください。

ウェブフックを使用したログ転送プロファイル

汎用ウェブフックを宛先として使用してログ転送プロファイルを作成できるようになりました。ウェブフックは、リアルタイムのデータ転送を可能にし、イベント駆動型アーキテクチャまたは集中型ロギングに最適であるだけでなく、自動化や他のサードパーティサービスとの統合もサポートします。詳細については、「Webhook」を参照してください。

拡張機能

Cisco Talos インテリジェンスとの統合

Multicloud Defense では、FQDN および URL のルックアップに Cisco Talos インテリジェンスを使用するようになりました。Cisco Talos は、世界中で最も信頼できる脅威インテリジェンス調査チームの1つであり、世界クラスの研究者、アナリスト、インシデント対応者、およびエンジニアで構成されています。詳細については、「Intelligence Categories」を参照してください。

ダッシュボードとナビゲーションの表示

バージョン 24.10 以降、Multicloud Defense Controller が更新され、ダッシュボードの外観の一般的なルックアンドフィールと、Magnetic を使用した特定の機能へのナビゲーションが改善されています。これにより、ダッシュボードを他のシスコ製品と統合し、全体的に合理化された表示を作成できます。これは継続的な取り組みです。

バージョン 24.09（2024 年 9 月 30 日）

このリリースには、次の機能と機能拡張が含まれています。

機能

ベータ版：AWS CloudWAN のサポート

拡張機能

ネットワークの可視性レポート

ネットワークの可視性レポートに、アクティビティの概要が含まれるようになりました。

GCP ロードバランサ

GCP では、TCP トラフィックと UDP トラフィックの両方に単一のロードバランサが使用されるようになりました。作業を単一のロードバランサに合理化することで、構成およびメンテナンスタスクが簡素化され、ネットワークインフラストラクチャの複雑さが軽減され、リソース使用率が向上します。

バージョン 24.08（2024 年 9 月 3 日）

修正

このリリースには、次の修正が含まれています。

- FQDN オブジェクトの照合機能が改善されます。
- 全体的なパフォーマンスが向上します。

バージョン 24.07（2024 年 8 月 17 日）

機能

このリリースには、次の機能が含まれています。

- OCI リアルタイム検出イベントのサポート。

修正

このリリースには、次の修正が含まれています。

- ページネーションで最大 250K をサポートするためのイベントバッチ処理でのレポート生成が改善されました。

- **ログなしアクション**に設定されたセッションサマリーイベントが、ログ記録ありのイベントを生成し続ける問題を修正します。この修正により、この設定が選択されている場合、イベントはログに記録されません。
- syslog 転送にすべてのロギングタイプが含まれていない問題を修正します。
- OCI アカウントに接続するために必要な権限のリストを更新しました。

バージョン 24.06（2024 年 6 月 26 日）

機能

このリリースには、次の機能が含まれています。

サイト間 VPN トンネル接続

次のクラウドサービスプロバイダーとプラットフォームを使用してサイト間 VPN トンネル接続を作成できるようになりました。

- Amazon Web Services（AWS）
- Microsoft Azure
- Google Cloud Platform（GCP）
- （旧 Cisco Defense Orchestrator）により管理される Cisco ASA

  Multicloud Defense Gatewayについて
- エクストラネットデバイス

Multicloud Defense Gateway をいずれかのエンドポイントとして使用するか、Multicloud Defense Gateway が両方のエンドポイントとして機能する環境を作成します。BGP または IPSec プロファイルのいずれかでゲートウェイを保護し、特定の環境に合わせて構成を微調整します。詳細については、「Site-to-Site VPN Tunnel Connection」を参照してください。

ダイナミックオブジェクト共有

異なるプラットフォームで共有されるオブジェクトを共有、作成、展開、および変更し、すぐに変更が識別されて更新されるようになりました。詳細については、「Shared Objects」を参照してください。

Azure NAT ゲートウェイ

出力 Azure 展開のネットワークアドレス変換（NAT）ゲートウェイに接続することを目的として、サービス VPC を作成できるようになりました。詳細については、「Egress Gateways」を参照してください。

ゲートウェイでの Azure ロードバランサの使用

ゲートウェイを作成するときにMulticloud Defenseが提供するロードバランサの代わりに、Azureダッシュボードで作成されたロードバランサの使用を選択できるようになりました。詳細については、「Advanced Gateway Configuration: Use Your Own Load Balancer」を参照してください。

その他

- パフォーマンスの向上.
- 運用の改善。
- バグ修正と安定性の改善。

バージョン 24.02（2024 年 2 月 26 日）

機能

このリリースには、次の機能が含まれています。

ハイブリッド クラウド

- （プライベートプレビュー）サイト間 VPN（Multicloud Defense Gateway バージョン 24.02 以降が必要）。

オーケストレーション

- クロスサブスクリプション スポーク VNet 保護（Azure）。
- スポーク VPC/VNet 保護のためのルートテーブルの作成。
- LB ヘルス チェック セキュリティ グループのオーケストレーション。

ゲートウェイ（Gateway）

- すべてのゲートウェイ インスタンス タイプのディスクサイズが削減されました。
- ゲートウェイ SSH アクセスを有効または無効にします。
- [詳細（Details）] ページからゲートウェイをアップグレードします。
- ゲートウェイのアップグレードをキャンセルします。
- インスタンスレベルのアクション（保護の終了、インスタンスの置換、データパスの再起動）。

統合

- クラウド サービス プロバイダー証明書の変更を動的に追跡します。
- Azure Active Directory によるユーザー管理。

その他

- パフォーマンスの向上.
- 運用の改善。
- バグ修正と安定性の改善。

拡張機能

このリリースには、次の機能拡張が含まれています。

- （プライベートプレビュー）サイト間 VPN のサポートを追加しました。これには、IPSec および BGP を含む VPN トンネルの設定が含まれます。VPN は、VPN を通過するトラフィックを処理および保護するために、ゲートウェイで直接終端されます。この機能拡張には、Multicloud Defense Gateway バージョン 24.02 以降が必要です。
- スポーク VPC および VNet でルートテーブルを調整するためのサポートが追加され、トラフィックがスポーク VNet/VPC から送受信され、Multicloud Defense Gateway を含むサービス VPC/VNet にルーティングされるようにします。この機能拡張には、ルートテーブルとルートエントリを作成するワークフロー、およびルートテーブルとサブネットの関連付けが含まれています。
- スポーク VNet ピアリングをオーケストレーションして、スポーク VNet から Multicloud Defense を含むサービス VNet にトラフィックをルーティングすることにより、クロスサブスクリプション スポーク VNet 保護のサポートが追加されます。これにより、Azure のオーケストレーションが AWS および GCP の同様のオーケストレーションと同等になります。
- クラウド サービス プロバイダーのロードバランサ（Azure、GCP、OCI）またはヘルスチェックサービス（GCP）からのヘルスチェックに関連するセキュリティグループ、ネットワーク セキュリティ グループ、およびファイアウォールルール CIDR をオーケストレーションするためのサポートを追加します。
- テレポートを使用したリバース SSH に対応するために、[ゲートウェイの詳細（Gateway Details）]ページから SSH を有効または無効にするためのサポートを追加します。テレポート統合をサポートする Multicloud Defense Gateway バージョン 23.10 以降が必要です。
- [ゲートウェイの詳細（Gateway Details）] ページから Multicloud Defense Gateway をアップグレードするためのサポートを追加します。
- Multicloud Defense Gateway のアップグレードをキャンセル（中止）する機能を追加します。
- ゲートウェイのインスタンスレベルのアクション（保護の終了、インスタンスの置換、データパスの再起動）を追加します。
- すべてのクラウド サービス プロバイダーのすべてのインスタンスのディスクサイズを 256GB から 128GB に削減します。
- 秘密キーがクラウドサービス プロバイダーに保存されて Multicloud Defense Gateway によって取得される、証明書オブジェクトへの変更を動的に追跡するためのサポートが追加されます。クラウドサービスプロバイダーのリソースに変更があった場合、コントローラは、ゲートウェイに対して、クラウド サービス プロバイダーのリソースの秘密キーを再読み

取りして、アクセス可能であること、および更新されたコンテンツが使用されることを確認するように指示します。証明書へのアクセスで問題が発生した場合は、システムログメッセージが生成されます。

- ゲートウェイ展開用のリージョンを選択する場合、すべてのリージョンのリージョンフレンドリ名を実際のリージョン名（小文字の名前）とともに表示する必要があります。この機能拡張により、すべてのリージョンがリージョンフレンドリ名と実際のリージョン名の両方で表示されるようになります。
- 認証のために Azure Active Directory と統合するように Multicloud Defense Controller を設定するためのサポートが追加されます。
- さまざまなリソースビューページのパフォーマンスを向上させ、API コールの数を減らし、全体的な読み込み時間を改善します。
- パフォーマンスを向上させるために、[トラフィックの概要（Traffic Summary）] ページにページネーションのサポートを追加します。
- パフォーマンスを向上させるために、[統計（Stats）] ページにページネーションのサポートを追加します。

修正

このリリースには、次の修正が含まれています。

- リージョンにゲートウェイの展開が含まれていない場合、インベントリビューと検出ビューにアセット情報が表示されない問題を修正します。
- 入力ポリシー規則セットが空の場合、イングレスゲートウェイ Azure の展開が成功しない問題を修正します。
- ログ転送プロファイルがグループのログ転送プロファイルで使用されている場合、S3 バケットへのログ転送が機能しない問題を修正します。
- UI からゲートウェイを削除しても、バックエンドのゲートウェイが完全に削除されず、同じ名前の置換ゲートウェイの展開を妨げる問題を修正します。
- Azure に展開されたゲートウェイに対するパブリック IP アドレスの割り当てを無効にすると、青色/緑色ゲートウェイの置換が実行されても、引き続きパブリック IP が割り当てられる問題を修正します。
- FQDN フィルタプロファイルの最初のカテゴリと FQDN 行を削除できなかった問題を修正します。
- ゲートウェイフィルタ内のゲートウェイ名がアルファベット順にソートされるように問題を修正します。
- アカウントおよびゲートウェイリソースの Terraform へのエクスポートで、エクスポートされた Terraform が空になる問題を修正します。

- ゲートウェイポリシーの [ステータス（Status）] が [更新（Updated）] と表示されているにもかかわらず、ポリシー規則セットの [ステータス（Status）] が [更新中（Updating）] と表示される問題を修正します。
- インスタンスが正常であっても、ヘルスチェックが失敗したためにスケールアウトが失敗する問題を修正します。
- ヘルスチェックが異常とする期間を 120 秒に変更します。新しいゲートウェイが展開されると、ロードバランサのヘルスチェックまたはヘルスチェックサービスがオーケストレーションされ、2 分（120 秒）の期間でインスタンスの正常性が評価されます。以前のオーケストレーションは 20 秒の期間で評価されました。
- タイムゾーンの選択がデフォルトで [UTC] ではなく [ローカル（Local）] になるように問題を修正します。
- CPU メトリックが表示されるはずの値よりも常に小さい値で表示される [統計（Stats）] ページの問題を修正します。
- スポーク VPC が削除されない、GCP でのスポーク VPC ピアリングの削除に関する問題を修正します。この問題は、セルフリンクの代わりに VPC ID が使用された場合にのみ発生します。
- リソース全体での [最終変更日（Last Modified）] 情報の表示に関する一貫性の問題を修正します。
- リンクがリンク先のリソースにリダイレクトされない、さまざまな UI 関連のリソースリンクを修正します。
- 詳細検索に関するさまざまな UI 関連の問題を修正します。
- さまざまな UI ワークフローを適切に動作するように修正します

バージョン 23.12（2023 年 12 月 14 日）

機能

このリリースには、次の機能が含まれています。

オーケストレーション

- GCP でのゲートウェイ作成用にユーザーが指定した NLB IP。
- データパスファイアウォール規則の GCP ヘルスチェック CIDR。

ポリシー

- クラウド サービス プロバイダー全体のゲートウェイに ICMP ポリシーを適用します。

統合

- ログ転送グループ内の複数の Syslog サーバー。

ユーザビリティ

- フィルタリングおよび詳細検索用の追加フィールド。
- ポリシー規則セットの SNAT 設定の表示。

その他

- パフォーマンスの向上.
- 運用の改善。
- バグ修正と安定性の改善。

拡張機能

このリリースには、次の機能拡張が含まれています。

- 最初は使用できなかったフィールドを詳細検索に追加します。
- GCP でのゲートウェイの作成を強化し、ユーザーが提供する IP リソースをロードバランサのフロントエンド IP として使用できるようにします。Terraform を使用している場合にのみ指定できます。
- ポリシー規則セットビューにサービスオブジェクト SNAT 設定の表示を追加します。
- クラウド サービス プロバイダーに展開されるゲートウェイに ICMP ポリシーを適用するには、そのクラウド サービス プロバイダーが ICMP をサポートする必要があるという厳しい要件を緩和します。ICMP ポリシーを含むポリシー規則セットは、クラウド サービス プロバイダーが ICMP をサポートしているかどうかに関係なく、任意のクラウドサービス プロバイダーに存在するすべてのゲートウェイに適用できるようになりました。
- ログ転送グループで複数の Syslog サーバー設定のサポートを追加します。
- データパスファイアウォール規則をオーケストレーションするときに、GCP ヘルスチェック CIDR を追加します。

修正

このリリースには、次の修正が含まれています。

- Splunk エンドポイントが到達可能であるにもかかわらず、Splunk のログ転送プロファイルが到達不能と表示されていた問題を修正します。
- AWS サービス VPC のオーケストレーションを解除しても、VPC 自体を含むすべての VPC リソースが完全にクリーンアップされない問題を修正します。
- ユーザーがリバース プロキシ サービス オブジェクトを作成または編集しているときに、すべてのアドレスオブジェクトが表示される問題を修正します。リバース プロキシ サービス オブジェクトだけが表示されるようになりました。

- ゲートウェイを GCP 共有 VPC シナリオにオーケストレーションするときに、コントローラが誤ったプロジェクト ID を使用していた問題を修正します。
- グループ アドレス オブジェクトを作成または変更するときに、アドレスオブジェクトのリストがドロップダウンに表示されない問題を修正します。
- ゲートウェイ作成ワークフローでのクラウド サービス プロバイダー アカウントの先行入力検索を修正します。
- ポリシー規則セット内で規則を追加する際の問題を修正して、パフォーマンスを向上させ、操作を迅速に行えるようにします。
- [Security Cloud Control] ページ（旧 Cisco Defense Orchestrator）から AWS アカウントを追加すると、タイムアウトが発生する可能性がある問題を修正します。
- FQDN一致およびFQDNフィルタリングオブジェクトのカウントの問題を修正します。カウントは、各ビューの両方のタイプのオブジェクトを表していました。
- さまざまな高度な検索とフィルタの問題を修正します。
- Azure に利用可能なキャパシティがない場合に Azure にゲートウェイを展開すると、展開が失敗し、作成されたリソースがクリーンアップされない問題を修正します。Azureにキャパシティがなくても、仮想マシンとその関連リソースの作成が妨げられることはありません。VM は作成されますが、エラーメッセージを表示して障害状態で VM が起動されます。このシナリオが認識され、リソースをクリーンアップするための適切なアクションが実行されて、システムログメッセージを通じてクラウド サービス プロバイダーの問題がユーザーに通知されるようにするには、特定の方法で処理する必要がありました。
- Azure にゲートウェイを展開するときに、クラウド サービス プロバイダーのリソースとキャパシティの情報が表示されない問題を修正します。
- ポリシー規則セット内の規則のリストを表示するパフォーマンスが向上します。
- GCPベースのアカウントを削除しても、インベントリ検出に関連するすべてのインベントリオブジェクトが削除されない問題を修正します。
- ゲートウェイインスタンスのゾーンごとの行で、ユーザーが最初の行を削除できない問題に対処します。これは、ゲートウェイがユーザー管理の VPC または VNet に展開されるシナリオにのみ適用されます。
- ゲートウェイを GCP に展開しても、オーケストレーションされたサービス VPC への出力ルートがオーケストレーションされない問題を修正します。
- スポーク VPC 保護のオーケストレーションが失敗する可能性がある問題を修正します。
- リバース プロキシ サービス オブジェクトの編集時に SNI および L7 DOS プロファイルが表示されない問題を修正します。
- パブリック IP の割り当て設定の UI 変更操作により、不要な青色/緑色ゲートウェイの置換がトリガーされる可能性がある問題を修正します。

- 複数の GCP リージョンへのゲートウェイのオーケストレーションにより競合状態が発生し、ゲートウェイがアクティブになるのを妨げる可能性がある問題を修正します。
- 内部エラーが原因で新しいゲートウェイの展開がすぐに非アクティブになる問題を修正します。
- Terraform によって作成された転送または転送プロキシポリシー規則セットがリバースプロキシ規則として UI に表示される問題を修正します。
- ポリシー規則セットの編集時にルールの順序を変更できない問題を修正します。
- 20 を超える行を含むサービスオブジェクトが受け入れられてゲートウェイにプッシュされると、ゲートウェイがクラッシュする問題を修正します。サービスオブジェクトは 20 行に制限されました。この制限の検証は、コントローラとゲートウェイの両方で実行されます。
- [ゲートウェイの詳細（Gateway Details）] ページにデータの作成時刻と変更日が表示されるように問題を修正します。
- 複数のページにまたがるオブジェクトとプロファイルを含むビューの適切なソートに関する問題を修正します。
- さまざまなオブジェクト作成ページのパフォーマンスが向上します。
- UI 全体の修正と機能拡張により、ユーザー体験が向上します。
- ユーザー指定のローカルまたは UTC の時間設定がビュー全体で適用され、ポータルの呼び出し全体で保持されるようにします。ポータルの呼び出し全体での永続性は、この設定をブラウザのキャッシュに保存することによって実現されます。
- カスタム管理対象の暗号キーゲートウェイ設定のツールチップ情報が欠落していた UI の問題を修正します。
- クラウド サービス プロバイダーのエラーが原因でゲートウェイがアクティブになることができなかった場合に、コントローラがシステムログメッセージを生成するようにします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。