機能拡張と修正

次のエントリには、各リリースの時点で各コンポーネントに導入されたすべての機能、拡張機能、およびバグ修正が含まれています。

Multicloud Defense Controllerの機能拡張

バージョン 23.10（2023 年 10 月 31 日）

機能

このリリースには、次の機能が含まれています。

クラウドプロバイダー：

- GCP フォルダのオンボーディング
- AWS ゲートウェイ IMDSv2

ポリシー

- 転送プロキシサーバー証明書の検証

メトリック

- インスタンスごとのメトリック（CPU とメモリを含む）

ユーザビリティ

- すべてのオブジェクトとプロファイルのページネーション
- すべてのオブジェクトとプロファイルのフィルタリングと詳細検索
- 脅威レポートの拡張

- ゲートウェイインスタンスの SSH アクセスのテレポート統合

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、次の拡張機能が含まれています。

- ID に基づいてルールを検索および表示する際の使いやすさを向上させるために、ネットワーク侵入（IDS/IPS）およびアプリケーション保護（WAF）の脅威調査のルール ID 列が有効になりました。
- フォルダ階層構造内に含まれるすべてのプロジェクトのアセットとトラフィックの検出に対応するために、GCP フォルダ階層のオンボーディングのサポートを追加します。GCP フォルダのオンボーディングにより、アセットとトラフィックの検出は許可されますが、完全なオーケストレーションは許可されません。検出は、GCP プロジェクト内で行われた変更にリアルタイムで適応する動的ポリシーを作成するために有益であり、必要です。プロジェクト内でオーケストレーションを行うには、オーケストレーションが必要な各プロジェクトを個別にオンボーディングする必要があります。
- AWS に展開されるすべてのゲートウェイが IMDSv2 を使用して AWS の推奨事項に準拠するようにし、展開されるすべてのインスタンスが IMDSv1 ではなく IMDSv2 を使用するように制限するよう組織のポリシーを設定します。新しいゲートウェイが AWS に展開されると、メタデータバージョンは IMDSv2 のみを使用するように設定されます。
- すべてのプロファイルとオブジェクトにページネーションを追加して、高速で効率的な表示を実現します。
- すべてのオブジェクトとプロファイルにフィルタ機能と詳細検索機能を追加します。
- バックエンド（ゲートウェイからサーバーへ）TLS セッションをネゴシエートするときにサーバー証明書を検証するように、転送プロキシポリシーを拡張します。証明書の検証はデフォルトでは無効になっていますが、すべての TLS セッションの復号プロファイルで、およびドメイン（またはドメインのセット）ごとに FQDN 一致オブジェクトで設定できます。
- 脅威レポートの再設計。脅威レポートの生成は、**[レポート（Reports）]** タブから実行できます。
- 帯域幅、接続レート、アクティブな接続、および HTTP 要求レートのインスタンスごとの統計を表示する機能を追加します。また、インスタンスごとのメモリと CPU 統計も追加されます。メトリックは、**[調査（Investigate）]** > **[ネットワーク（Network）]** > **[統計（Investigate）]** ページに表示されます。

- リバースSSHに対応するためのテレポートとの統合により、特にゲートウェイがパブリック IP なしでオーケストレーションされている場合に、ゲートウェイインスタンス管理インターフェイスへの SSH を容易にします。SSH に対する要件はまれであり、高度なトラブルシューティングを目的とする場合のみ必要です。インバウンド通信は、クラウドサービスプロバイダーの制限（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、ファイアウォールルール）を使用してデフォルトで禁止されます。

修正

このリリースには、次の修正が含まれています。

- Azure のキャパシティの問題が原因で展開に失敗した Azure のゲートウェイがコントローラによって削除されない問題を修正します。
- ユーザー提供の GCP サービス VPC に展開されたゲートウェイからゾーンを削除しても、ロードバランサのターゲットプールからインスタンスが削除されない問題を修正します。
- スケールイン操作中に Azure V5 インスタンスが完全に削除されない問題を修正します。
- さまざまなシステムログメッセージを拡張し、エラーメッセージ情報を改善します。
- X-Forwarded-For（XFF）ヘッダーに複数の IP アドレスが含まれている場合、XFF ヘッダーの IP アドレスの GeoIP 情報の評価が適切に機能しない問題を修正します。
- GCP ロギングへのログ転送を修正し、JSON エンコード文字列ではなく実際の JSON 構造を送信します。
- カスタムタグが適用されている Azure ゲートウェイをアップグレードすると、ロードバランサからの正常性チェックの問題が原因で新しいゲートウェイインスタンスが起動しない可能性がある問題を修正します。
- ログとイベントビューで使用可能なタイムラインの調整が正しく動作しないさまざまな問題を修正します。
- 復号プロファイルなしでセキュアなプロキシ設定を行うと、プロキシが非セキュアなプロキシとして誤って動作する問題を修正します。この修正により、セキュアなプロキシの設定時に復号プロファイルが指定されていることを確認するために、プロキシ設定が検証されます。
- 関連リソースへのアクティブリンクが表示されない、または一貫して機能していないルールセット、オブジェクト、およびプロファイルのさまざまな問題を修正します。
- ログ転送が修正され、すべてのフィールドに列挙値ではなくわかりやすい名前が表示されるようになります。これにより、各ログ/イベントでエクスポートされる JSON は、UI に表示されるのと同じ情報をサードパーティの SIEM で表示します。
- 使いやすさを向上させるために、さまざまなUIおよびUIベースのワークフローのニュアンスを修正します。
- **[調査（Investigate）]** タブのすべてのログとイベントビューからローカル時刻とUTC時刻を選択する機能が再導入されます。

- 詳細検索フィールドで操作し、検索文字列を指定する際のさまざまなユーザビリティの問題に対処します。

バージョン 23.09（2023 年 9 月 30 日）

機能

このリリースには、次の機能が含まれています。

クラウドプロバイダー

- OCI での追加のリージョンサポート。

ポリシー

- GCP の ICMP 転送ポリシー。

ユーザビリティ

- すべてのプロジェクトとプロファイルでのページネーション。
- サービス VPC（VNet）ワークフローでの Azure リソースグループ（RG）の作成。

統合

- Splunk および MS Teams への監査およびシステムログアラート。
- Datadog に転送されるゲートウェイメトリック。

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。

- OCIの追加リージョンである、アムステルダム、ドイツ、ロンドン、フランス（パリ、マルセイユ）のサポートを追加します。
- デフォルトの OCI リージョンを変更するためのサポートを追加します。これは、コントローラが最初に OCI と通信するために使用するリージョンです。現在定義されているデフォルトのOCIリージョンはサンノゼですが、サポートされているリージョンに変更できるようになりました。これを変更するには、サポートに連絡してください。
- トラフィックサマリーログとセキュリティイベントページに、検索をクリアしてログ/イベントを完全に更新できる **[クリア（Clear）]** ボタンを提示します。

- GCP= に展開される Egress/East-West ゲートウェイの ICMP ベースの転送ポリシーのサポートを追加します。
- すべてのオブジェクトとプロファイルでページネーションのサポートを追加します。
- 監査ログとシステムログを Splunk に送信するためのサポートを追加します。これにより、Splunk を新しい宛先として追加することで、アラートプロファイルが更新されます。
- 監査ログとシステムログを Microsoft Teams に送信するためのサポートを追加します。これにより、MicrosoftTeams を新しい宛先として追加することで、アラートプロファイルが更新されます。
- サードパーティ製 SIEM へのゲートウェイメトリックの送信のサポートを追加します。これにより、ゲートウェイメトリックを SIEM に送信するために、設定してゲートウェイに割り当てることができる新しいメトリック転送プロファイルが導入されます。最初の導入では、Datadog を SIEM としてサポートします。他の SIEM のサポートは、今後のリリースで予定されています。
- サービス VPC（VNet）作成の一部として Azure リソースグループ（RG）を作成するためのサポートを追加します。RG は、コントローラによってオーケストレーションされるすべてのリソースを指定した（または新しく作成した）RG 内で関連付けるために必要です。

修正

この更新には、次の修正が含まれています。

- すぐに適用されるゲートウェイ設定を変更すると、パブリック IP の設定を使用するように認識された変更により、不要な青色/緑色のゲートウェイの交換がトリガーされる可能性がある問題を修正します。
- AWS のゲートウェイを無効なクロスアカウント CMEK から有効な同一アカウント CMEK に変更しようとすると失敗する問題を修正します。
- トラフィックサマリーログ、セキュリティイベント、システムログ、および監査ログを表示する際の Investigate ビューの時間範囲セレクタに関するさまざまな問題を修正します。
- ポリシー規則セットからゲートウェイへのページから、ポリシー規則セットに関連付けられたさまざまなリソースページへのアクティブリンクが正しく機能していなかった問題を修正します。
- Valtix アラートルールプロファイルの Terraform エクスポートでシビラティ（重大度）引数がエクスポートされなかった問題を修正します。
- Azure ゲートウェイのデフォルトのインスタンスタイプを AZURE_D2S_V5 に更新します。
- セキュリティおよび非セキュアプロキシを設定する際のさまざまなワークフローの問題を修正します。これらの修正では、ソリューションが共通ポートを自動的に選択するのではなく、ユーザーが目的のポートを明示的に指定する必要があります。

- ユーザーがセキュリティプロキシを設定するときに復号プロファイルが指定されていることを検証することで、プロキシ設定のワークフローを改善する問題を修正します。復号プロファイルは、ゲートウェイが適切な証明書を発行するために必要です。
- UIワークフローを使用してゲートウェイを作成するときにJSONエラーメッセージが発生する問題を修正します。
- 使いやすさを向上させるために、さまざまな UI 関連の動作を修正します。
- ゲートウェイの展開に予想よりも時間がかかる問題を修正します。
- 最小/最大インスタンス設定のユーザー設定に基づいて、コントローラが必要以上のゲートウェイインスタンスをインスタンス化する可能性があるコーナーケースを修正します。
- パブリック IP なしで Azure にゲートウェイを展開すると失敗する問題を修正します。
- 無効化ゲートウェイアクションのシステムログメッセージのシビラティ（重大度）を [高（High）] から [情報（Info）] に変更します。
- さまざまなエラーメッセージをわかりやすくし、あいまいさを軽減します。

バージョン 23.08（2023 年 8 月 21 日）

機能

このリリースには、次の機能が含まれています。

- TCP/TLS 転送プロキシのサポート。
- CPU ベースの自動スケーリングのサポート。
- トラブルシューティングの機能拡張。

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。

- 転送プロキシサービスオブジェクトを機能拡張して、TLS および TCP プロキシ設定を許可します。プロキシは、取得したドメインを使用してバックエンド接続の接続先 DNS 検索を実行するために、トラフィックからドメイン（ホストヘッダーまたはSNI）を取得する必要があるため、HTTP または TLS 暗号化トラフィックでのみ動作します。
- パブリック IP を無効にする設定に変更された場合に、青色/緑色ゲートウェイの置換を実行するようにゲートウェイを拡張します。
- [FQDN] 列を、イーグレス/East-West ポリシー規則セットのデフォルトの表示列にします。
- ゲートウェイ展開 CSP リソース検証チェックに必要な CSP リソース数を追加します。
- 転送プロキシ サービス オブジェクトを作成するときに、HTTP および HTTPS プロトコルの宛先ポートを自動入力します。

修正

このリリースには、次のバグ修正が含まれています。

- 複数のアドレスプレフィックスを含む Azure サブネットが Controller によって適切に処理されない問題を修正します。
- FQDN オブジェクトにより、ポリシーの暗黙的な拒否アクションが原因で、一致するトラフィックが拒否される問題を修正します。
- ページネーションを導入すると、リソースの詳細へのリダイレクトが失敗する問題を修正します。
- ポリシー規則セットからアドレスオブジェクトへのリダイレクトが失敗する問題を修正します。
- ポリシー規則セットの保存後に [ページから移動（Leave page）] ダイアログボックスがポップアップ表示される問題を修正します。
- ポリシー規則セット内から規則を作成しようとすると、無効な JSON エラーメッセージがスローされる問題を修正します。
- ゲートウェイの初期展開時に Controller が必要以上のインスタンスを作成する問題を修正します。
- Azure オンボードアカウントのログイン情報を更新しようとすると、更新されたログイン情報の適用に失敗し、2 回目の試行が必要になる問題を修正します。
- 展開に何分もかかって展開エラーが発生する可能性がある、Azure ゲートウェイの展開に関する問題を修正します。
- マルチテナント導入で、ユーザーがプロファイルを編集してデフォルトのテナントログインを設定できない問題を修正します。
- Easy Setup を介したイーグレス/East-West ゲートウェイの展開が失敗してエラーメッセージが表示される問題を修正します。
- AWS ヨーロッパ（フランクフルト）（eu-central-2）リージョンでインベントリ検出を有効にできない問題を修正します。
- 管理者スーパーユーザーが他の管理者スーパーユーザーを変更または削除できない問題を修正します。
- Multicloud Defense Controller ダッシュボードのログアウトで、完全にログアウトするために複数回のログアウト試行が必要になる問題を修正します。
- 誤った検索結果を生成するさまざまな詳細検索関連の動作を修正します。
- ページネーション導入の結果として、さまざまな詳細検索の問題を修正します。
- [トラフィックの概要（Traffic Summary）] ビューと [イベントログ（Events Logs）] ビューの時間セレクタのさまざまな動作を改善します。

- REST API への呼び出しによって返されるさまざまなエラーメッセージの問題を修正します。
- さまざまな UI 表示の問題を修正します。修正：Controller と UI のパフォーマンスを改善し、安定性を向上させます。

バージョン 23.07（2023 年 7 月 20 日）

機能

このリリースには、次の機能が含まれています。

- パフォーマンスの向上.
- Controller 操作の改善。
- 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。

- アラートプロファイルの Terraform エクスポートの UI に Terraform オプションのサポートが追加されました。
- ページネーションを活用して、多数のリソース（ポリシー規則セット、アドレスオブジェクト、サービスオブジェクト）の表示速度を向上させます。

修正

このリリースには、次のバグ修正が含まれています。

- オブジェクトビュー（アドレスオブジェクト、サービスオブジェクト）にページネーションを導入すると、詳細検索が想定どおりに機能しない問題を修正します。
- UI での監査ログとシステムログの表示が 30 日間に制限される問題を修正します。Controller は監査ログとシステムログを無期限に保存します。過去のログを任意の日数表示できるように UI が更新されました。
- エクスポートされた Terraform に誤ったリソース ID が含まれる、アラートプロファイル Terraform エクスポートの問題を修正します。
- Azure サブスクリプションのアカウントエクスポートに関連した問題を修正して、適切な引数がエクスポートされるようにします。
- アカウントの作成および更新操作に REST API を使用する場合の拡張エラーレポートへの対処に関連した問題を修正します。
- [復号プロファイルの詳細（Decryption Profile Details）] ビューの UI 配置の問題を修正しました。

- ダッシュボードウィジェットの表示に関連した UI の配置の問題を修正しました。修正：Terraform へのアラートプロファイルのエクスポートのサポートを有効にします。
- GCP ロードバランサインスタンスの状態が不明なときに、インスタンス正常性が正常を返す可能性がある問題を修正します。
- 詳細検索を適用すると行の高さが増大する、[調査（Investigate）] -> [ログ（Logs）] の表示の問題を修正します。
- UI テーブルヘッダーの列ラインが表示されず、列幅のサイズ変更が困難になる表示の問題が修正されました。
- インベントリリージョン収集を有効にしようとすると、AWS 接続の問題が原因でエラーが発生する可能性がある問題を修正します。
- CSP を削除しようとするとエラーが生成されるときに表示されるメッセージを修正します。
- アラート サービス プロファイルの表示の問題を修正して、Webex URL が表示されるようにします。
- [ディスカバリ（Discovery）] -> [トポロジ（Topology）] ビューの表示に関する問題を修正し、レンダリングが 1 回だけ実行されるようにします。
- [トポロジ（Topology）] ビューでの [新規作成（Create New）] 操作が正しく機能しなかった問題を修正します。
- ゲートウェイの展開が UI ではブロック操作になっていた問題を修正します。この修正により、ゲートウェイの展開がブロックではない操作になります。
- ゾーンの誤った仕様を使用してゲートウェイを展開すると、ゲートウェイがシステムログメッセージなしで非アクティブとして展開される問題を修正します。
- [検出（Discovery）] ビューの [ルール（Rules）] ボタンと [アクション（Actions）] ボタンの位置のずれを修正します。
- REST API を使用してゲートウェイを展開した結果、エラー状態になった場合のメッセージを修正します。
- ゲートウェイ名の詳細検索でゲートウェイの完全なリストが入力されない問題を修正します。
- サインアウト操作の機能が一貫していない問題を修正します。
- [ポリシー規則セット（Policy Rule Set）] テーブルの表示に想定以上に時間がかかる問題を修正します。

Multicloud Defense Gatewayの機能拡張

- バージョン 23.10 （10 ページ）

バージョン 23.10

バージョン 23.10-02（2023 年 11 月 16 日）

修正

このアップグレードには、次の修正が含まれています。

- DNS キャッシングを有効にすると、ポリシーの変更と DNS 解決の間隔の間で競合状態が発生し、ドメインのキャッシュが値 0（キャッシュなし）にリセットされる、DNS ベースの FQDN アドレス オブジェクト リソースに関連する問題を修正します。この状況が発生すると、ドメイン解決はキャッシュされず、既存のキャッシュ値は TTL の期限が切れるとフラッシュされます。最終的に、ゲートウェイはそのドメインのトラフィックと一致しなくなります。この修正により、キャッシュが期待どおりに動作するように競合状態が解決されます。

バージョン 23.10-01（2023 年 11 月 3 日）

拡張機能

このアップグレードには、次の機能拡張が含まれています。

- ポリシータイプ（転送および転送プロキシ）が一致しない 2 つのルールによって処理される各セッションに対して生成されるポリシータイプの不一致メッセージを、各セッションに関連するイベントに移動します。これにより、このシナリオが発生した場合に多くのシステムログメッセージが排除され、各セッションに関連付けられたイベントとしてエラーが生成されます。このシナリオが発生すると、セッションは拒否され、イベントによって理由が報告されます。拒否は、トラフィックサマリーログにも表示されます。
- バックエンド TLS セッションをネゴシエートするときにサーバー証明書を検証するように転送プロキシポリシーを拡張します。証明書の検証はデフォルトでは無効になっていますが、すべての TLS セッションの復号プロファイルで、およびドメイン（またはドメインのセット）ごとに FQDN 一致オブジェクトで設定できます。
- リバース SSH に対応するためのテレポートとの統合により、特にゲートウェイがパブリック IP なしでオーケストレーションされている場合に、ゲートウェイインスタンス管理インターフェイスへの SSH を容易にします。SSH に対する要件はまれであり、高度なトラブルシューティングを目的とする場合のみ必要です。インバウンド通信は、クラウドサービスプロバイダーの制限（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、ファイアウォールルール）を使用してデフォルトで禁止されます。

修正

このアップグレードには、次の修正が含まれています。

- 復号例外にFQDN一致オブジェクトを使用してトラフィック処理の問題を引き起こす可能性のある、転送プロキシルールに関連する問題を修正します。
- 証明書検証の遅延が原因で、FQDN一致プロファイルで設定された転送プロキシルールによって、トラフィックが誤って拒否される問題を修正します。FQDNフィルタリングプロファイルが適用されていなくても、拒否はFQDNFILTERセキュリティイベントと見なされます。
- FQDN一致オブジェクトを使用するルールが、未分類のドメインのトラフィックを誤って処理する問題を修正します。
- IPが多数存在し、それらのIPに対する変更が多数あるためにデータパスが変更を受け入れないことが原因で一致の問題が発生し、トラフィックが正しく処理されない可能性がある、ダイナミック アドレス オブジェクトに関連した問題を修正します。
- DNS解決の間隔を設定してもDNS解決の頻度が変更されないDNSベースのFQDNキャッシングの問題を修正します。
- ゲートウェイが異常になる可能性があるパケット収集の問題を修正します。
- ゲートウェイからの特定のログに秘密キー情報が含まれる可能性がある問題を修正します。
- さまざまなゲートウェイの安定性の問題を修正します。
- トラフィック処理の問題の原因となるCPUの問題も引き起こす可能性があるゲートウェイのメモリリークを修正します。
- URI情報がトラフィックサマリーログに表示されない問題を修正します。
- L7DOSイベントがURIを正しく表示しない問題を修正します。

バージョン 23.08

バージョン 23.08-10（2023 年 12 月 18 日）

修正

このリリースには、次の修正が含まれています。

- SYNの受信後にSYN ACKを待機するタイムアウトを変更します。元のタイムアウトは120秒でした。SYN ACKが返されることのない特定のシナリオ（ポートスキャンなど）では、長いタイムアウトにより、セッションプルのエントリが必要以上に消費されます。多くのセッションがSYN ACKで応答しないシナリオでは、セッションプールが使い果たされる可能性があります。これは多くの場合、SYNフラッドと呼ばれます。タイムアウトを短縮することで、有効なセッションの処理に使えるようにセッションプールを解放する

ために、セッションがより早くリリースされます。タイムアウトは30秒に短縮され、ゲートウェイ設定を介して設定できます。

- アクティブまたは非アクティブのルールに DNS ベースの FQDN キャッシングが設定されている場合に、ゲートウェイが IP キャッシュを正常に構築しない可能性がある問題を修正します。キャッシュが適切に構築されていない場合、ポリシーはトラフィックの照合に失敗する可能性があります。この修正により、ポリシーが一致し、トラフィックが適切に処理されるように、IP キャッシュが適切に構築されます。
- 生成されたゲートウェイ診断バンドルが、コントローラへの送信が許可されないほどに大きくなり、ゲートウェイログを分析できなくなる問題を修正します。この修正により、生成された診断バンドルがコントローラに正常に送信されるように制限が追加されます。
- ゲートウェイの安定性を向上させます。

バージョン 23.08-09（2023 年 11 月 16 日）

修正

このアップグレードには、次の修正が含まれています。

- DNS キャッシングを有効にすると、ポリシーの変更と DNS 解決の間隔の間で競合状態が発生し、ドメインのキャッシュが値0（キャッシュなし）にリセットされる、DNS ベースの FQDN アドレス オブジェクト リソースに関連する問題を修正します。この状況が発生すると、ドメイン解決はキャッシュされず、既存のキャッシュ値は TTL の期限が切れるとフラッシュされます。最終的に、ゲートウェイはそのドメインのトラフィックと一致しなくなります。この修正により、キャッシュが期待どおりに動作するように競合状態が解決されます。

バージョン 23.08-08（2023 年 11 月 8 日）

修正

このアップグレードには、次の修正が含まれています。

- すべてのユースケースでゲートウェイの安定性が向上します。

バージョン 23.08-07（2023 年 10 月 18 日）

修正

このアップグレードには、次の修正が含まれています。

- GCP ロギングへのログ転送が JSON エンコード文字列ではなく JSON 構造としてログを送信するように問題を修正します。

バージョン 23.08-06（2023 年 10 月 7 日）

修正

この更新には、次の修正が含まれています。

- 復号例外にFQDN一致オブジェクトを使用してトラフィック処理の問題を引き起こす可能性のある、転送プロキシルールに関連する問題を修正します。

バージョン 23.08-05（2023 年 10 月 3 日）

修正

この更新には、次の修正が含まれています。

- 証明書検証の遅延が原因で、FQDN一致プロファイルで設定された転送プロキシルールによって、トラフィックが誤って拒否される問題を修正します。FQDNフィルタリングプロファイルが適用されていなくても、拒否はFQDNFILTERセキュリティイベントと見なされます。

バージョン 23.08-04（2023 年 9 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- FQDN一致オブジェクトを使用するルールが、未分類のドメインのトラフィックを誤って処理する問題を修正します。

バージョン 23.08-03（2023 年 9 月 10 日）

修正

このアップグレードには、次の修正が含まれています。

- IP が多数存在し、それらの IP に対する変更が多数あるためにデータパスが変更を受け入れないことが原因で一致の問題が発生し、トラフィックが正しく処理されない可能性がある、ダイナミック アドレス オブジェクトに関連した問題を修正します。
- DP がリークを検出してデータパスを再起動する、UDP トラフィックに関連した低速セッションプールリークを修正します。

バージョン 23.08-02（2023 年 9 月 3 日）

修正

このアップグレードには、次の修正が含まれています。

- 200KB を超えるペイロードで HTTP POST を送信するとトラフィックがドロップされるリバースプロキシの問題を修正します。
- 静的 IP を含む DNS ベースのアドレスオブジェクトが適正に一致しない問題を修正します。
- TCP 転送プロキシの SNI またはホストヘッダーへの依存関係を削除します。

バージョン 23.08-01（2023 年 8 月 25 日）

拡張機能

このアップグレードには、次の機能拡張が含まれています。

- ゲートウェイ接続とプロキシのタイマーが超過した場合に、セッションサマリーイベントを生成するようにデータパスを拡張します。この拡張機能は、タイマー設定が原因でセッションがゲートウェイによって閉じられた場合のトラブルシューティングに役立ちます。
- L4（TCP）および L5（TLS）プロキシに対応するように転送プロキシ サービス オブジェクトを拡張します。この拡張は、`transport_mode` 引数の有効な値として TCP または TLS を指定することにより達成されます。
- セッションのパフォーマンスを追跡するようにゲートウェイのデータパスを拡張します。
- TCP リセットを生成するゲートウェイ データパス プロセスを拡張し、データパスの再起動中に接続を意図的に閉じるようにします。

修正

このアップグレードには、次の修正が含まれています。

- HTTP オブジェクト名の URL エンコード文字 [および] がゲートウェイによって復号化された後、サーバーに要求を送信する前に再エンコードされない問題を修正します。この問題より、サーバーはオブジェクトを正しく捕捉することができず、400 応答コードを返します。この修正により、サーバーに要求を送信する前に、文字が適切に再エンコードされるようになります。
- SNI に下線が存在すると、プロキシによってトラフィックが渡されない問題を修正します。この変更により、プロキシ設定でドメイン名での下線の使用に対応できるようになります。
- トラフィックが正しいポリシーと一致するのに、間違った証明書が発行される問題を修正します。
- トラフィックが正しいポリシーと一致するのに、間違った証明書が発行される問題を修正します。
- プロキシタイムアウトによって 408 ステータスコードが発生する HTTP コマンド（GitHub リポジトリの複製など）に関連した大規模ファイル転送の問題を修正します。

- URLフィルタリングカテゴリのクエリタイムアウトが期限切れになり、トラフィックが拒否される問題を修正します。
- アップストリームプロキシの問題が原因でデータパスが自己修復される可能性がある、イングレスゲートウェイの安定性の問題を修正します。
- ゲートウェイが特定のタイプのトラフィックを処理するときに、遅延が長引く可能性がある問題を修正します。
- メモリプロファイリングを有効にするときにトリガーされる、データパスの不要な再起動を修正します。
- ポリシーの変更によってトリガーされたデータパスの再起動が原因で、ゲートウェイが断続的に 502 を生成する可能性がある問題を修正します。
- CPUベースの自動スケーリングで不要なスケールアウトが発生する可能性がある問題を修正します。
- プロキシ接続リークを修正します。
- ゲートウェイの安定性を向上させます。

バージョン 23.06

バージョン 23.06-14（2023 年 11 月 12 日）

修正

このアップグレードには、次の修正が含まれています。

- DNS キャッシングを有効にすると、ポリシーの変更と DNS 解決の間隔の間で競合状態が発生し、ドメインのキャッシュが値0（キャッシュなし）にリセットされる、DNSベースの FQDN アドレス オブジェクト リソースに関連する問題を修正します。この状況が発生すると、ドメイン解決はキャッシュされず、既存のキャッシュ値は TTL の期限が切れるとフラッシュされます。最終的に、ゲートウェイはそのドメインのトラフィックと一致しなくなります。この修正により、キャッシュが期待どおりに動作するように競合状態が解決されます。

バージョン 23.06-13（2023 年 10 月 18 日）

修正

このアップグレードには、次の修正が含まれています。

- GCP ロギングへのログ転送が JSON エンコード文字列ではなく JSON 構造としてログを送信するように問題を修正します。

バージョン 23.06-12（2023 年 10 月 6 日）

修正

この更新には、次の修正が含まれています。

- 復号例外にFQDN一致オブジェクトを使用してトラフィック処理の問題を引き起こす可能性のある、転送プロキシルールに関連する問題を修正します。

バージョン 23.06-11（2023 年 9 月 27 日）

修正

この更新には、次の修正が含まれています。

- 証明書検証の遅延が原因で、FQDN一致プロファイルで設定された転送プロキシルールによって、トラフィックが誤って拒否される問題を修正します。FQDNフィルタリングプロファイルが適用されていなくても、拒否はFQDNFILTERセキュリティイベントと見なされます。

バージョン 23.06-10（2023 年 9 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- FQDN一致オブジェクトを使用するルールが、未分類のドメインのトラフィックを誤って処理する問題を修正します。

バージョン 23.06-09（2023 年 9 月 10 日）

修正

このアップグレードには、次の修正が含まれています。

- IP が多数存在し、それらの IP に対する変更が多数あるためにデータパスが変更を受け入れないことが原因で一致の問題が発生し、トラフィックが正しく処理されない可能性がある、ダイナミック アドレス オブジェクトに関連した問題を修正します。
- DP がリークを検出してデータパスを再起動する、UDP トラフィックに関連した低速セッションプールリークを修正します。

バージョン 23.06-08（2023 年 9 月 3 日）

修正

このアップグレードには、次の修正が含まれています。

- 静的 IP を含む DNS ベースのアドレスオブジェクトが適正に一致しない問題を修正します。

バージョン 23.06-07（2023 年 8 月 29 日）

修正

このアップグレードには、次の修正が含まれています。

- 200KB を超えるペイロードで HTTP POST を送信するとトラフィックがドロップされる転送プロキシの問題を修正します。

バージョン 23.06-06（2023 年 8 月 23 日）

修正

このアップグレードには、次の修正が含まれています。

- SNI に下線が存在すると、プロキシによってトラフィックが渡されない問題を修正します。この変更により、プロキシ設定でドメイン名での下線の使用に対応できるようになります。
- ゲートウェイの安定性を向上させます。
- プロキシタイムアウトによって 408 ステータスコードが発生する HTTP コマンド（GitHub リポジトリの複製など）に関連した大規模ファイル転送の付加的な問題を修正します。
- トラフィックが正しいポリシーと一致するのに、間違った証明書が発行される問題を修正します。
- URL フィルタリングカテゴリのクエリタイムアウトが期限切れになり、トラフィックが拒否される問題を修正します。
- プロキシ接続リークを修正しました。修正：HTTP オブジェクト名の URL エンコード文字 [および] がゲートウェイによって復号化された後、サーバーに要求を送信する前に再エンコードされない問題を修正します。この問題より、サーバーはオブジェクトを正しく捕捉することができず、400 応答コードを返します。この修正により、サーバーに要求を送信する前に、文字が適切に再エンコードされるようになります。

バージョン 23.06-05（2023 年 8 月 4 日）

修正

このアップグレードには、次の修正が含まれています。

- 下線を使用している HTTP ヘッダーがプロキシルールによって渡されない問題を修正します。この変更により、プロキシ設定で下線付きのヘッダーに対応できるようになります。

- プロキシタイムアウトによって 408 ステータスコードが発生する HTTP コマンド（GitHub リポジトリの複製など）に関連した大規模ファイル転送の問題を修正します。
- HTTP トラフィックがまず転送プロキシルールによって処理され、次いでさらに詳細な照合のために転送ルールによって処理された後、拒否する必要があるときに許可される問題を修正します。

バージョン 23.06-04（2023 年 7 月 27 日）

修正

このアップグレードには、次の修正が含まれています。

- マルウェア対策エンジンによって特定のタイプのトラフィックが処理されると、CPU の使用率が高くなり、トラフィック処理の遅延が発生する可能性がある問題を修正します。

バージョン 23.06-03（2023 年 7 月 21 日）

修正

このアップグレードには、次の修正が含まれています。

- ポリシー規則セットに、IP/CIDR の包含と除外の組み合わせを使用するアドレスオブジェクトが含まれている場合、新しいゲートウェイの展開により起動エラーが発生する可能性がある問題を修正します。

バージョン 23.06-02（2023 年 7 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- CIDR ベースのアドレスオブジェクトへの更新がデータパスワーカーに適切に適用されず、誤ったルール照合が発生する問題を修正します。
- DNS キャッシュが適切に確立されているものの、データパスワーカーに適切に適用されないために誤ったルール照合が発生する、DNS ベース FQDN アドレスオブジェクトの問題を修正します。
- 同じ L3/L4（IP/ポート/プロトコル）照合基準の転送ルールが転送プロキシルールに先行するものの、別個の L5（SNI）照合により、適切なルール照合が発生してもトラフィックが転送として処理されるデータパス処理動作を修正します。転送ルールと転送プロキシルールの順序を逆にした場合も、同様の動作が発生する場合があります。この動作が発生する理由は、L5（SNI）照合に対応するために、TCP ハンドシェイクを完全に確立して、TLS hello メッセージを受信し、SNI を取得する必要があるためです。TCP ハンドシェイクが完了すると、トラフィックは最初のルールのルールタイプによってすでに処理されています。セッションが一旦確立されると、トラフィック処理を転送から転送プロキシに（またはその逆に）変更することはできません。ポリシー規則セットにこの競合が設定されてい

る場合、データパスは競合を検出し、システムログメッセージを生成します。競合するルールではトラフィックを正常に処理できないため、トラフィックは拒否されます。

- アップストリームプロキシの問題が原因でデータパスが自己修復される可能性がある、イングレスゲートウェイの安定性の問題を修正します。
- データパスの再起動によって CPU のスパイクが発生し、不要な自動スケーリングが発生する可能性がある問題を修正します。

バージョン 23.06-01（2023 年 7 月 6 日）

修正

このアップグレードには、次の修正が含まれています。

- GCP ゲートウェイがサポート関連の診断バンドルを生成できない問題を修正します。
- プロファイルの変更が導入されていないにもかかわらず、NTP プロファイルがゲートウェイに繰り返し適用される問題を修正します。
- 空のアドレスオブジェクトがゲートウェイに適用されると、トラフィック処理の問題が発生する問題を修正します。
- NTP プロファイルとログ転送プロファイルの両方をゲートウェイに同時に適用すると、データパスの不要な自己修復が発生する問題を修正します。この問題は、それぞれの操作が独立しているため、オーケストレーションを使用してプロファイルが適用された場合にのみ発生します。順次、非常に短い期間内に発生します。
- 3 つを超えるレベルを含むドメインでルールが設定されている場合に、イングレスゲートウェイが誤った証明書を発行する可能性がある問題を修正します。
- アドレスオブジェクトを頻繁に変更すると、データパスがそれ以上の変更を受け入れなくなる可能性がある問題を修正します。
- FQDN 一致を使用するルールセットによってトラフィックが処理されるときに、拒否時のリセット（TCP リセット）が実行されない問題を修正します。
- ゲートウェイによって処理されるトラフィックに対して L4_FW イベントが一貫して生成されない問題を修正します。
- WAF アクションを [ログの許可（Allow Log）] から [ルールデフォルト（Rule Default）] に変更すると、データパスが複数回再起動する可能性がある問題を修正します。
- チャンクされた転送エンコーディングを含む HTTP トラフィックにより、WAF で大量のメモリが消費され、データパスの自己修復がトリガーされる可能性がある問題を修正します。修正：低速メモリリークによってデータパスのサイレント再起動が生じ、トラフィックが中断する可能性がある問題を修正します。
- データパスの自己修復を引き起こす可能性のあるメモリの問題を修正します。

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。