AMP for Endpoints
リリース ノート

バージョン 5.4

2018 年 4 月 24 日

AMP for Endpoints コンソール 5.4.20180424

バグ修正/機能拡張

- コンテキスト メニューの [AMP の可視性（AMP Visibility）] を [可視性（Visibility）] に名称変更しました。
- カスタム レポート作成時のユーザ エクスペリエンスを向上しました。
- スケジュール スキャンの設定中に発生する可能性があるエラーを修正しました（CSCvj04576）。
- 期限切れの CSV エクスポート ファイルに関するエラー メッセージを改善しました。
- レガシー レポートへのアクセスを削除しました。
- デモ データの入力にかかる時間を削減するための改善を行いました。
- AMP for Endpoints Mac コネクタポリシーに自動クラッシュ ダンプをアップロードするための制御を追加しました。

2018 年 4 月 17 日

Cisco Security Connector 1.08

新規

- 新しいコネクタは、Apple iOS 11.3 以降をサポートしています。
- iOS デバイスのアプリケーションが AMP for Endpoints の Clarity モジュールを介して行ったネットワーク接続の監査が含まれています。
- Umbrella モジュールを介して、悪意のある Web サイトの DNS フィルタリングを提供できます。

AMP for Endpoints コンソール 5.4.20180416

新規

- ダッシュボードの [iOS Clarity] タブから、Cisco Security Connector の新機能（[アプリトラジェクトリ（App Trajectory）]、[最近監視されたアプリ（Recently Observed Apps）] を介したアプリの使用状況の追跡など）にアクセスできます。
- [MDM の統合（MDM Integration）] 設定が、[アカウント（Accounts）] > [ビジネス（Business）] ページに追加されています。

2018 年 4 月 3 日

AMP for Endpoints コンソール 5.4.20180403

新規

- 選択したコンピュータ グループのカスタム レポートを作成できるようになりました。

バグ修正/機能拡張

- CSV のエクスポートはバックグラウンドで行われるようになり、CSV ファイルのダウンロード リンクを含む電子メールが送信されます。

2018 年 3 月 28 日

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.7.0.593

新規

- ClamAV ウイルス定義ファイルのバージョンが表示されます。

バグ修正/機能拡張

- ディスク書き込み操作を削減しました(CSCvd15950)。
- 送信される重複ネットワーク検出イベントの数を削減しました。
- 実行時の大容量ファイルのスキャンを強化しました。
- UI 内の情報のフォーマットを改善しました。
- 出力アーカイブの最大サイズを指定するための SupportTool オプションを追加しました。
- 通常動作時に頻繁に記録されるエラー メッセージを再分類しました。
- サードパーティ製ライブラリを更新しました。
- パッチを適用した ClamAV の脆弱性:
  - CVE-2018-1000085
  - CVE-2012-6706
  - CVE-2017-6419
  - CVE-2017-6418
  - CVE-2017-6420
  - CVE-2018-0202

AMP for Endpoints Linux AMP for Endpoints コネクタ 1.7.0.545

新規

- ClamAV ウイルス定義ファイルのバージョンが表示されます。

バグ修正/機能拡張

- 実行権限がない状態でシステムの一時ディレクトリがマウントされているときのインストール エラーを修正しました。
- カーネル モジュールの競合が原因でシステムが起動時にハングアップする問題を修正しました。
- ディスク書き込み操作を削減しました。
- 送信される重複ネットワーク検出イベントの数を削減しました。
- 実行時の大容量ファイルのスキャンを強化しました。
- 完全アンインストール時にユーザのホーム ディレクトリから CLI 履歴ファイルを削除しました。

- 出力アーカイブの最大サイズを指定するための SupportTool オプションを追加しました。
- SupportTool によるネットワーク マウント ドライブの処理を改善しました。
- CLI の表示フォーマットを改善しました。
- 通常動作時に頻繁に記録されるエラー メッセージを再分類しました。
- サードパーティ製ライブラリを更新しました。
- パッチを適用した ClamAV の脆弱性:
  - CVE-2018-1000085
  - CVE-2012-6706
  - CVE-2017-6419
  - CVE-2017-6418
  - CVE-2017-6420
  - CVE-2018-0202

重要! Linux と MacOS の ClamAV 定義は、利用可能な最新の定義をコネクタにダウンロードしている場合でも、AMP for Endpoints コンソールには古い定義として表示されることがあります。この問題は、今後のリリースで修正される予定です。

2018 年 3 月 27 日

AMP for Endpoints コンソール 5.4.20180227

新規

- 脆弱性の新しい概要のレポートが毎週更新されるようになりました。

バグ修正/機能拡張

- API パフォーマンスが向上しました。

2018 年 3 月 12 日

AMP for Endpoints Windows AMP for Endpoints コネクタ 6.0.9

バグ修正/機能拡張

- 複数の Clam AV の脆弱性を修正しました(CVE-2017-6420、CVE-2017-12378、CVE-2018-0202、CVE-2017-6418)。
- トレンドマイクロとの互換性が向上しました(CSCvi07080)。
- PDF ファイルに対して誤検出をトリガーした Clam AV の問題に対処しました(CSCvi01400)。

2018 年 2 月 22 日

AMP for Endpoints コンソール 5.4.20180222

新規

- 展開ステータス、アプリケーション ブロック、低拡散度の実行可能ファイルの検出結果、脅威の根本原因についてのレポートが毎週更新されるようになりました。

2018 年 2 月 8 日

AMP for Endpoints Windows AMP for Endpoints コネクタ 6.0.7（後継 6.0.9）

新規

- Windows セキュリティ更新プログラム KB 4072699 の受信に必要なレジストリ キーを自動設定する /kb4072699 インストーラ スイッチが追加されました。

重要: このインストーラ スイッチを使用する前に、インストールされているすべての AV 製品の互換性を確認してください。インストーラ スイッチを使用してレジストリ キーを設定する際に適用される注意と考慮事項のセクションの重要な詳細については、『Cisco AMP for Endpoints の Windows セキュリティ更新プログラム KB4056892 との互換性』[英語] を参照してください。

バグ修正/機能拡張

- TETRA ファイル検出解析が改善されました（CSCvh54783、CSCvh77705）。
- まれな条件下で AMP for Endpoints コネクタが原因でブルー スクリーンが発生する問題に対処しました（CSCvh56811）。

2018 年 1 月 16 日

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.6.0

新規

- 自動クラッシュ レポート機能を追加しました。

重要! AMP for Endpoints Mac AMP for Endpoints コネクタでは、OS X 10.10 のバージョン 1.6.0 以降がサポートされなくなりました。

バグ修正/機能拡張

- レトロスペクティブ検疫が成功した場合でも、障害イベントが表示されるバグを修正しました。
- MacOS 10.13 との互換性を改善しました。
- サードパーティ製ライブラリを更新しました。
- 通常の状況下で頻繁に記録されていた一部のエラー メッセージを再分類し、AMP for Endpoints コネクタの実行中、ポリシーでデバッグ ロギングが有効になっている場合にのみ、それらのメッセージが表示されるようにしました。
- レトロスペクティブ データベースのサイズを 50 MB から 500 MB に増量し、ディスクの読み取りと書き込みに対するプルーニング効果を高めました。

AMP for Endpoints Linux AMP for Endpoints コネクタ 1.6.0

バグ修正/機能拡張

- 障害から保護するアップグレード プロセスを改善しました。
- レトロスペクティブ検疫が成功した場合でも、障害イベントが表示されるバグを修正しました。
- サードパーティ製ライブラリを更新しました。
- 通常の状況下で頻繁に記録されていた一部のエラー メッセージを再分類し、AMP for Endpoints コネクタの実行中、ポリシーでデバッグ ロギングが有効になっている場合にのみ、それらのメッセージが表示されるようにしました。
- レトロスペクティブ データベースのサイズを 50 MB から 500 MB に増量し、ディスクの読み取りと書き込みに対するプルーニング効果を高めました。

2018 年 1 月 30 日

AMP for Endpoints コンソール 5.4.20180130

新規

- 電子メールの送信元が no-reply@amp.cisco.com になりました。
- 週次レポートが再設計され、新たにデータ概要が表示されるようになりました。
- AMP アップテート サーバがリリースされ、TETRA 定義をローカルで定義できるようになり、コネクタからのインターネット経由の帯域幅使用を削減することが可能になりました。Windows ポリシーの [詳細設定(Advanced Settings)] > [TETRA] で表示される AMP アップデート サーバ定義のリンク先での指示に従ってください。

2017 年 12 月 5 日

AMP for Endpoints Windows コネクタ 6.0.5

新規

- エクスプロイト防止の検出エンジンが、特定のプロセスをターゲットとするエクスプロイトやメモリ攻撃をブロックします。
- システム プロセスの保護により、特定の Windows システム プロセスへのメモリ攻撃に対する保護を増強しました。
- このバージョンの AMP for Endpoints コネクタは、Windows 7、Windows 8 および 8.1、Windows 10、Windows Server 2008 R2、ならびに Windows Server 2012 で動作します。それ以前のバージョンの Windows はサポートされません。

重要: Windows 7 および Windows Server 2008 R2 では、コネクタをインストールする前に Microsoft Security Advisory 3033929 のパッチを適用する必要があります。

エクスプロイト防止コネクタのベータ リリース以降のバグ修正:

- 現在、AMP for Endpoints コネクタ サービスは、Windows 10 Fall Creators Update にインストールされている場合は正しく機能します。
- AMP for Endpoints コネクタが [コンピュータの管理(Computer Management)] ウィンドウを開いたときに警告を発生させることがなくなりました。

2017 年 12 月 5 日

バグ修正/機能拡張:

- 複数の ClamAV の脆弱性を修正しました。
- AMP for Endpoints コネクタ の保護パスワードのセキュリティを改善しました。
- Windows のプロキシ検出を改善しました。
- AMP for Endpoints コネクタ のアップグレードの堅牢性をさらに促進するための改善を行いました。
- AMP for Endpoints コネクタが多くの一時ファイルを残して、ディスクをいっぱいにする問題に対処しました。
- AMP for Endpoints コネクタ のユーザ インターフェイスの [履歴(History)] ページに、すでにローカル キャッシュにある検疫済みファイルの正しい検出名を表示するようにしました。
- エンドポイント IOC スキャン起動時の信頼性を改善しました。
- CPU の高使用率を防ぐために SQLite バージョンを更新しました。
- AMP for Endpoints コネクタ ユーザ インターフェイスの応答性を改善しました。

重要! 6.x.x より前の AMP for Endpoints Windows AMP for Endpoints コネクタ バージョンから 6.x.x へアップグレードする場合は、エンドポイントをリブートする必要があります。

AMP for Endpoints コンソール 5.4.20171205

新規

- AMP for Endpoints Windows コネクタ バージョン 6.0.5 以降でシステム プロセス保護をサポートするためにプロセス除外タイプを追加しました。
- AMP for Endpoints Windows AMP for Endpoints コネクタ バージョン 6.0.5 以降でエクスプロイト防止とシステム プロセス保護を可能にするためにポリシー設定を追加しました。

重要! AMP for Endpoints Windows AMP for Endpoints コネクタ バージョン 6.0.5 以降を導入する際には、事前にクラウド マイグレーション ツールを実行して、すべてのポリシーを新しい AMP クラウド インフラストラクチャ上に配置させる必要があります。2016 年 2 月以降に作成された新しいポリシーはすべて、デフォルトで新しい AMP クラウド インフラストラクチャを使用します。

バグ修正/機能拡張

- AMP for Endpoints コネクタ のバージョン番号を [コネクタのダウンロード(Download Connector)] ページに追加しました。グループを選択した後に、ダウンロードする AMP for Endpoints コネクタ のバージョンが AMP for Endpoints コネクタ タイプごとに表示されるようになりました。

2017 年 11 月 30 日

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.5.1

バグ修正/機能拡張

- 複数の ClamAV の脆弱性を修正しました。
- plist ファイルのスキャン時のメモリ リークに対処しました。
- レトロスペクティブでの検疫が失敗した際にクラッシュする可能性があった点を修正しました。

AMP for Endpoints Linux AMP for Endpoints コネクタ 1.5.1

新規

- RHEL/CentOS 7.4 を公式にサポートしました。
- RHEL/CentOS 6.9 を公式にサポートしました。

バグ修正/機能拡張

- 複数の ClamAV の脆弱性を修正しました。
- 特定のプロセスの HTTP 解析を修正しました。

2017 年 11 月 28 日

AMP for Endpoints コンソール 5.4.20171128

新規

- 2 段階認証を設定するための通知をユーザに送信できるようになりました。
- [ユーザ(Users)] ページに新しいフィルタ([最終ログイン(Last Login)]、[2 段階認証(Two-Step Verification)]、[リモートファイルの取得(Remote File Fetch)]、[コマンド ライン(Command Line)])を追加しました。
- ユーザが何度もログインに失敗した場合に、CAPTCHA が表示されるようになりました。
- 新しい UI でポリシー設定を改善しました。
- コマンド ライン データが API で使用できるようになりました。
- EU の企業は AMP for Endpoints アカウントを切り替えて、新しい EU Threat Grid Cloud を使用できるようになりました。
- 権限を使用して個人ユーザを設定し、コマンド ライン データを表示できるようになりました。

- IP アドレス、URL、SHA-256 をクリックすると新しいポップオーバーが表示されるようになりました。
- Word、PowerPoint、Excel のファイル タイプのスキャンが AMP for Endpoints Mac と AMP for Endpoints Linux の コネクタ のポリシーで可能になりました。

2017 年 10 月 31 日

AMP for Endpoints コンソール 5.4.20171031

新規

- 他の高度な脅威対策製品との整合性を高めるため、メニューの色を更新しました。
- ユーザは OS として Windows 10 を指定して、Threat Grid にファイルを送信するときに分析を実行できるようになりました。
- ユーザは新しいポリシー UI をプレビューできるようになりました。既存のポリシーの UI は、間もなく廃止されます。
- パスワード要件がより厳格になりました。
- 新しい Splunk アプリケーションを Splunk App Store に追加しました。
  https://splunkbase.splunk.com/app/3670/#/details
  https://splunkbase.splunk.com/app/3686/#/details

2017 年 10 月 18 日

AMP for Endpoints Linux AMP for Endpoints コネクタ 1.5.0.518

新規

- Linux 署名付きファイル検疫ガードレールを更新しました。
- デーモンが再起動した場合に、ファイルシステムのスキャンが再開するようになりました。
- ポリシー設定に基づき UI で除外リストが非表示になりました。
- 古い検疫済みファイルが自動的に削除されるようになりました。

バグ修正/機能拡張

- サードパーティ製のライブラリを更新しました。
- AMP 登録サーバに接続できない場合は、プロキシをバイパスするようになりました。
- 必要な場合に実行がスキャンから除外されないように修正しました。
- カスタム スキャンの誤動作を修正しました。
- CentOS 6 でのリブート後の意図しない ampmon の自動起動が無効になりました。
- マルウェアを含むアーカイブのコンテンツ全体をスキャンするようになりました。

- ゼロファイルを失敗として処理していた指定スキャンまたは定期スキャンを処理しなくなりました。
- 検疫失敗からの復元を修正しました。
- 非常に長い除外リストを表示すると発生する CLI クラッシュを修正しました。
- CLI が初期化フェーズで停止する間欠的障害を修正しました。

2017 年 10 月 17 日

AMP for Endpoints Mac コネクタ 1.5.0.548

新規

- macOS High Sierra（10.13）をサポートするようになりました。
- AMP サービス デーモンが再起動した後に、ファイルシステムのスキャンを再開するようになりました。
- ポリシー設定に基づき UI で除外リストが非表示になりました。

バグ修正/機能拡張

- サードパーティ製のライブラリを更新しました。
- メモリ リークを修正しました。
- 除外の適用方法を最適化しました。
- Cloud Recall Restore エラーの処理を改善しました。
- マルウェアを含むアーカイブのコンテンツ全体をスキャンするようになりました。
- 古い検疫済みファイルが自動的に削除されるようになりました。
- 一部の内部ファイルのアクセス権限を制限しました。

2017 年 10 月 5 日

AMP for Endpoints Windows コネクタ 5.1.13

重要! Windows コネクタ 6.0.1 以降は、Windows XP、Windows Vista、Windows Server 2003、および Windows Server 2008（R2 以外）の各オペレーティング システムに追加された新機能をサポートしません。重要なバグ修正やセキュリティ パッチは、期間限定で引き続きコネクタの 5.x.x ブランチに行われます。詳細については、サポート終了のお知らせを参照してください。

2017 年 9 月 28 日

バグ修正/機能拡張

- コネクタ インストーラにあった DLL ハイジャックの脆弱性にパッチを適用しました（CVE-2017-12312）。
- 非常に長いプロセスのコマンド ライン引数を正しく取得するようになりました。
- コネクタ UI にクラウド接続ステータスが正確に表示されるようになりました。
- 通常の使用時およびコネクタ アップグレード時に設定の問題を検出して修復するコネクタの機能を改善しました。
- Windows Vista より前のオペレーティング システムでのプロセス除外のパフォーマンスを改善しました。
- コネクタ保護が有効になっている場合にコネクタをバージョン 5.0.9 以前から 5.1.11 に直接アップグレードできない問題に対処しました。
- サポート パッケージ生成の信頼性を改善しました。
- BIOS シリアル番号にスペースが含まれているマシンではコネクタが新しい ID を生成しなくなりました。
- リブートせずに複数回のアップグレードを実行した後はコネクタ サービスが自動的に起動しない問題に対処しました。
- Windows Server 2003 でのアップグレード後のシステム リブートの信頼性を改善しました。

2017 年 9 月 28 日

AMP for Endpoints コンソール 5.4.20170928

新規

- 上部バーのナビゲーションを再編成しました。
  - [サポート（Support）] リンクを [ヘルプ（Help）] メニューに含めました。
  - [マイ アカウント（My Account）] と [ログアウト（Log Out）] リンクは新しい [ユーザ（User）] メニューに配置されています。
- ダッシュボードの自動更新：お客様が大画面でダッシュボードをより適切に表示できるように（たとえば、ネットワーク オペレーション センター内）、[ダッシュボード（Dashboard）] ページの自動更新が設定できるようになりました。

2017 年 8 月 24 日

AMP for Endpoints Mac コネクタ 1.4.5

新規

- デジタル署名されたマルウェアは、Mac コネクタで検疫されるようになりました。

バグ修正/機能拡張

- DMG コンテナの処理が改善されました。
- 結果的に検疫の復元に失敗していた競合状態に対処しました。
- 結果的にゼロ ファイルをスキャンしていたカスタム スキャンまたは定期スキャンが失敗したスキャンとして報告されなくなりました。
- 複数のユーザを持つシステムへのコネクタのインストールは、誤って失敗として報告されなくなりました。

2017 年 8 月 9 日

AMP for Endpoints コンソール 5.4.2017080915

新規

- ユーザ名検索機能。
- 分析用のファイルの送信時に使用する AMP Threat Grid VM をユーザが選択できるようになりました。

バグ修正/機能拡張

- [ポリシーの編集/作成(Edit/Create Policy)] ページの [製品の更新(Product Updates)] セクションで、コネクタのバージョン番号が正しく並べ替えられなかったバグを修正しました。
- shas だった検索結果によって誤ったコンテキスト メニューが表示されていたバグを修正しました。
- 受信トレイのイベントが正しくグループ化されない問題に対処しました。

2017 年 8 月 3 日

AMP for Endpoints Mac コネクタ 1.4.3

バグ修正/機能拡張

- 「/Users」ディレクトリ内のサブディレクトリに空白文字が含まれているサブディレクトリがある場合、アンインストール プロセス時に、別のフォルダが不注意で削除されることがある問題に対処しました。

  MacOS のシステム設定では、アカウント名に空白文字のあるユーザの作成は阻止されるため、ほとんどのシステムに影響がない点に注意してください。

  この問題が発生するのは、2 つの類似の名前のディレクトリが存在する場合です（例：「/Users/JohnDoe」と「/Users/JohnDoe Copy」）。「/Users/JohnDoe Copy」に AMP コネクタ ログ ファイルへのパスが含まれる場合（例：「/Users/JohnDoe Copy/Library/Logs/Sourcefire/」）、アンインストールまたはアップグレードするとユーザ ディレクトリ「/Users/JohnDoe」が削除されます。

重要! Mac コネクタ 1.4.2 は、ポータルでは入手できなくなりました。

1.4.2 をインストール済みの場合は、1.4.2 をアンインストールせずに直接 1.4.3 にアップグレードする必要があります。

1.4.2 インストーラをダウンロードした場合は、すぐに 1.4.3 インストーラに置き換えることを推奨します。

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.1.11

重要! Windows コネクタ 6.0.1 以降は、Windows XP、Windows Vista、Windows Server 2003、および Windows Server 2008（R2 以外）の各オペレーティング システムに追加された新機能をサポートしません。重要なバグ修正やセキュリティ パッチは、期間限定で引き続きコネクタの 5.x.x ブランチに行われます。詳細については、サポート終了のお知らせを参照してください。

バグ修正/機能拡張

- TETRA ライセンス キーを更新しました。

重要! バージョン 5.1.11 より前のすべての Windows コネクタの TETRA ライセンスは、2017 年 11 月 1 日に失効します。Windows コネクタのクラウドベースの保護を補完するために引き続き TETRA エンジンの使用を希望する場合は、この日付より前にアップグレードする必要があります。

- DFC ドライバが、より確実に初期化されるようになりました。
- ネットワーク接続を監視するためのコネクタのウィンドウの数が 1 つ増えました。
- ローカル DFC キャッシュが正しく更新されるようになりました。
- 特定の IP 範囲がコネクタによって間違ってホワイトリストに追加されることはなくなりました。
- CIDR ブロックとポート番号の組み合わせで構成されていたカスタム IP ブラック/ホワイトリストのエントリは、コネクタによって正しく処理されるようになりました。
- コネクタ保護パスワードは、アンインストール プロセス時に記録されなくなりました。
- ローカル定義が最新の場合、不要な TETRA 定義はダウンロードされなくなりました。
- アップグレード時にコネクタが新しい ID を生成する可能性を低減しました。
- コンテナ ファイル（pdf、zip、tar など）のスキャンがより堅牢になりました。
- 親プロセスのレポートの精度が向上しました。
- プロセス除外のパフォーマンスが改善されました。

2017 年 7 月 18 日

AMP for Endpoints Linux AMP for Endpoints コネクタ 1.3.1

バグ修正/機能拡張

- unrar の脆弱性にパッチを適用しました（CVE-2012-6706）。
- curl の脆弱性にパッチを適用しました（CVE-2017-7468）。

2017 年 7 月 11 日

AMP for Endpoints コンソール 5.4.20170711

新規

- シスコのポートフォリオ全体の一貫性を確保するため、Cisco AMP for Endpoints の条件（前 EULA）を更新しました。最新バージョンのクラウドの条件は http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html を参照してください。

バグ修正/機能拡張

- AMP for Endpoints コネクタ ダウンロード ページのグループのリストがアルファベット順に表示されるよう変更しました。
- （API のみ）実行されたマルウェア侵害の兆候のイベントには、提供可能な場合、ファイル名やパスなどの追加フィールドが含まれるようになりました。
- ポリシーのシリアル番号が特定の状況下で正しく増分しないバグを修正しました。
- 削除されたコンピュータが [自動分析（Automatic Analysis）] ページのコンピュータの台数に含まれないようになりました。
- ライセンス供与されたコンピュータの台数と [コンピュータ（Computers）] ページに表示されるコンピュータの台数の間に相違が生じる問題に対処しました。

2017 年 7 月 6 日

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.1.9

バグ修正/機能拡張

- unrar の脆弱性にパッチを適用しました（CVE-2012-6706）。

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.4.2（後継 1.4.3）

重要! AMP for Endpoints Mac AMP for Endpoints コネクタ 1.3.0 のユーザは、1.4.2 へアップグレードする前に、システムを 1.3.1 へアップグレードした後、リブートすることを強く推奨します。1.3.0 から 1.42 へ直接アップグレードすると、カーネル パニックが発生する可能性があります。詳細については、特別なアドバイザリ [英語] を参照してください。

重要! MacOS 10.12（Sierra）を実行中のユーザは、10.12.4 以降にアップグレードする必要があります。これは、システムの安定性に影響を及ぼす互換性の問題があるためです。この問題は、MacOS 10.12.4 では解決されています。

2017 年 7 月 6 日

新規

- Sourcefire FireAMP から AMP for Endpoints へブランドを変更しました。

  ブランド変更の一環として、コネクタのインストール パスを次のように変更しました。

  - `/Applications/Cisco AMP`
  - `/Library/Application Support/Cisco/AMP for Endpoints Connector`
  - `/opt/cisco/amp`

  このバージョンにエンドポイントをアップグレードする前に、AMP for Endpoints とともにインストールされているサードパーティ製のソフトウェアに設定した除外を必ず確認してください。
- 簡体字中国語、日本語、および韓国語に対する AMP for Endpoints コネクタの UI にローカリゼーション サポートを追加しました。

バグ修正/機能拡張

- カーネル パニックを引き起こす可能性がある AMP ネットワークのカーネル拡張のバグを修正しました。
- unrar の脆弱性にパッチを適用しました（CVE-2012-6706）。
- SSL インスペクションがネットワーク ゲートウェイで有効になっている場合に AMP クラウドへの接続が失敗する可能性のあるバグを修正しました。
- OpenSSL、cURL、xmlsec など、AMP for Endpoints コネクタで使用されるサードパーティ製のライブラリからセキュリティ修正を適用しました。
- ユーザが開始したスキャンがリアルタイムのファイル操作での検出に悪影響を与える可能性のあるバグを修正しました。
- 正常に動作しない UI クライアントに対するガードを強化しました。
- 検出イベントが生成される前にオフライン エンジンによって悪意があると見なされるファイルを AMP クラウドを使用してスキャンされるようにバグを修正しました。
- ポリシーで機能が無効になっている場合でも、ファイル パスがクラウド クエリに含まれるバグを修正しました。
- MSXML ファイルの解析後に「開いているファイルが多すぎます（too many open files）」というエラーが発生するバグを修正しました。
- 長時間 AMP クラウドから切断すると AMP デーモンがクラッシュする可能性のあるバグを修正しました。
- いくつかのイベントに関するユーザ情報が欠落するバグを修正しました。
- フラッシュ スキャンを実行中に UI ロックアップが引き起こされるバグを修正しました。
- 検疫失敗メッセージの読みやすさを改善しました。
- 破損した ClamAV 定義ファイルの復元力を改善しました。
- インストーラの Perl 依存関係を削除しました。
- コネクタが悪意のあるリソース フォークを検疫できない問題を解決しました。

2017 年 6 月 20 日

AMP for Endpoints コンソール 5.4.20170620

新規

- [ダッシュボード（Dashboard）] タブおよび [受信トレイ（Inbox）] タブにカスタム フィルタとアラート機能を追加しました。これにより、ユーザは新しい感染に関するアラートを電子メールで受け取ることができます。
- WannaCry デモ データと関連付られたドキュメントを追加しました。

バグ修正/機能拡張

- [ファイル分析（File Analysis）] のオプションとして、Windows 7 の日本語および韓国語のオペレーティング システムを追加しました。Windows XP および Windows 7 の 32 ビット オペレーティング システムは [ファイル分析（File Analysis）] でサポートされなくなりました。これらのいずれかが現在の [ビジネス（Business）] ページにデフォルトのイメージとして設定されている場合は、デフォルトでは自動的に Windows 7 x64 に変更されます。

2017 年 6 月 8 日リリース ノート

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.1.7

バグ修正/機能拡張

- Windows SMB サーバにインストールされた AMP for Endpoints コネクタによりマップされた共有ドライバにアクセスできなくなる問題に対処しました。

2017 年 6 月 6 日リリース ノート

AMP for Endpoints コンソール 5.4.20170606

新規

- Active Directory、Okta、および Ping フェデレートを介したシングル サインオンのサポートが追加されました。
- バージョン 5.1.3 以降には、AMP for Endpoints Windows AMP for Endpoints コネクタ UI から除外のリストを非表示にするポリシー オプションが追加されました。

バグ修正/機能拡張

- [拡散度(Prevalence)] には、自身の導入のみでなく、拡散度のグローバル リストに基づくデータが表示されるようになりました。
- 新しいポリシーの作成に伴い、次のポリシー項目のデフォルト値が変更されました。
  - [ハートビート間隔(Heartbeat Interval)] が 15 分に設定されています。
  - [イベントのユーザ名を送信(Send User Name in Events)] が有効になっています。
  - [ファイルの通知を表示しない(Hide File Notifications)] が有効になっています。
  - [最大スキャンファイルサイズ(Maximum Scan File Size)] が 50 MB に設定されています。
  - [最大アーカイブスキャンファイルサイズ(Maximum Archive Scan File Size)] が 50 MB に設定されています。
- コマンド ライン ログ ポリシー項目は、AMP for Endpoints コネクタ ログ レベルが [デバッグ(Debug)] に設定され、[コマンドラインキャプチャ(Command Line Capture)] が有効の場合にのみ使用できます。
- 新しい除外設定を作成する場合のデフォルト ウィンドウの除外を更新しました。

2017 年 6 月 1 日リリース ノート

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.3.1

バグ修正/機能拡張

- この特別なリリースでは、予期しないシステムの再起動を引き起こす AMP for Endpoints Mac AMP for Endpoints コネクタ バージョン 1.3.0 の不具合を修正しました。1.3.0 のユーザは、新しい AMP for Endpoints コネクタ バージョンにアップグレードする前に、このバージョンにアップグレードしてシステムを再起動することを強くお勧めします。現在 1.2.6 以前を実行中のユーザは、このバージョンをスキップして新しいバージョンに直接アップグレードすることをお勧めします。

  詳細については、アドバイザリ『AMP for Endpoints Mac Connector 1.3.0 Defect Can Cause Unexpected System Restart(AMP for Endpoints Mac コネクタ 1.3.0 の不具合により予期しないシステムの再起動が発生する可能性がある)』を参照してください。

2017 年 5 月 9 日リリース ノート

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.1.5

バグ修正/機能拡張

- [ID の同期(Identity Sync)] が有効になっている場合に、AMP for Endpoints コネクタがクラウドへの接続が失われる可能性のある問題に対処しました。
- [AMP for Endpoints コネクタ保護(Connector Protection)] が有効である場合に、AMP for Endpoints コネクタが admin 権限を持つユーザによって無効にされる可能性のある問題に対処しました。
- デバッグ ロギングを有効にしようとすると発生するクラッシュに対処しました。
- AMP for Endpoints コネクタ サービスのシャットダウン時に発生する可能性のあるクラッシュを修正しました。
- [AMP for Endpoints コネクタ保護(Connector Protection)] が有効である場合に、コマンド ラインで AMP for Endpoints コネクタをアンインストールしようとする際に特定の特殊文字を含むパスワードが正しく解析されない問題に対処しました。
- 韓国語のオペレーティング システムのエンドポイントで複数の検疫通知が表示される場合の軽微な問題に対処しました。

2017 年 5 月 2 日リリース ノート

AMP for Endpoints コンソール 5.4.20170502

新規

- [デバイストラジェクトリ(Device Trajectory)] にコンピュータの説明ドロップダウンを追加しました。
- Mac コネクタ(バージョン 1.3.0 以降)のポリシーに [イベントのユーザ名を送信(Send User Name in Events)] を追加しました。
- Linux コネクタ(バージョン 1.1.1 以降)のポリシーに [イベントのユーザ名を送信(Send User Name in Events)] を追加しました。

2017 年 4 月 4 日リリース ノート

AMP for Endpoints コンソール 5.4.20170404

新規

- AMP for Endpoints Windows AMP for Endpoints コネクタ 5.1.3 以降のプロセス除外を追加しました。

バグ修正/機能拡張

- [ダッシュボード（Dashboard）] タブおよび [受信箱（Inbox）] タブに、侵害イベントに関するアーティファクトのページネーションを追加しました。
- [ダッシュボード（Dashboard）] タブおよび [受信箱（Inbox）] タブに、侵害イベントに関するアーティファクトをミュートする機能を追加しました。
- [ダッシュボード（Dashboard）] タブおよび [受信箱（Inbox）] タブに、侵害イベントに関するアーティファクトの詳細を表示する機能を追加しました。
- [ダッシュボード（Dashboard）] タブおよび [受信箱（Inbox）] タブに、SHA-256 のアーティファクトのファイル名を追加しました。
- ユーザが AMP for Endpoints コネクタのインストール日付を確認できるように、コンピュータ API に install_date タイムスタンプを追加しました。

AMP for Endpoints Linux コネクタ 1.3.0

新機能

- Red Hat Enterprise Linux および CentOS 7.2 と 7.3 のサポートを追加しました。

バグ修正/機能拡張

- SSL インスペクションがネットワーク ゲートウェイで有効になっている場合に AMP クラウドへの接続が失敗する可能性のあるバグを修正しました。
- OpenSSL、cURL、xmlsec など、AMP for Endpoints コネクタで使用されるサードパーティ製のライブラリからセキュリティ修正を適用しました。
- ユーザが開始したスキャンがリアルタイムのファイル操作での検出に悪影響を与える可能性のあるバグを修正しました。
- 正常に動作しない UI クライアントに対するガードを強化しました。
- 検出イベントが生成される前にオフライン エンジンによって悪意があると見なされるファイルを AMP クラウドを使用してスキャンされるようにバグを修正しました。
- ポリシーで機能が無効になっている場合でも、ファイル パスがクラウド クエリに含まれるバグを修正しました。
- MSXML ファイルの解析後に「開いているファイルが多すぎます（too many open files）」というエラーが発生するバグを修正しました。

- 長時間 AMP クラウドから切断すると AMP デーモンがクラッシュする可能性のあるバグを修正しました。
- DFC 検出イベントのユーザ情報が欠落するバグを修正しました。
- 検疫失敗メッセージの読みやすさを改善しました。
- 破損した ClamAV 定義ファイルの復元力を改善しました。
- サポート ツールの診断アーカイブに abrt クラッシュ レポートを追加しました。

2017 年 4 月 3 日リリース ノート

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.1.3

新機能

- TETRA がポリシーを介して有効にされ、すべての定義のダウンロードが完了すると、Windows セキュリティ センターに AMP for Endpoints コネクタが登録されるようになりました。

バグ修正/機能拡張

- VMware Persona Management を含むシステムに AMP for Endpoints コネクタがインストールされている場合のシステム パフォーマンスが向上しました。
- まれな条件下で AMP for Endpoints コネクタにより BSOD が発生する可能性のある問題に対処しました。
- AMP for Endpoints コネクタによりシステムのフリーズが発生する可能性のある問題を修正しました。
- 大量の CPU を消費するエンドポイント IOC スキャンの問題に対処しました。
- 5.1.1 以降にアップグレードされた古い AMP for Endpoints コネクタの高度が Microsoft ソフトウェアの推奨に沿うように変更されない問題を修正しました。
- AMP for Endpoints コネクタにより、SSL を介して TETRA 定義をダウンロードできるようになりました。
- 5.1.1 より前のバージョンからアップグレードすると「Sourcefire」から「Cisco」へのインストール ディレクトリの移行が正常に機能しない Windows XP の問題を修正しました。
- ポリシーを挿入せずに AMP for Endpoints コネクタをインストールした場合に、クラウド通知がデフォルトで表示される問題に対処しました。
- bzip2 の脆弱性に対処する修正を追加しました（CVE-2016-3189）。
- 接続テスト ツールを使用すると表示される誤ったログ行を削除しました。

2017 年 3 月 7 日リリース ノート

AMP for Endpoints コンソール 5.4.20170307

バグ修正/機能拡張

- [ダッシュボード（Dashboard）] タブおよび [受信箱（Inbox）] タブに [侵害イベントのタイプ（Compromise Event）] を追加しました。
- AMP for Endpoints コンソールと Firepower Management コンソール間のコンピュータの IP を適切に配置するようにアプリケーション統合のバグを修正しました。
- 認証サーバを変更すると、ユーザがログインした際に新しいホストにリダイレクトされるようになりました。保留中のパスワード リセットを再送信する必要がある場合があります。

2017 年 2 月 16 日リリース ノート

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.1.1

新規

- Sourcefire FireAMP から AMP for Endpoints へのブランド変更を制限しました。

  重要: ブランド変更の一環として、コネクタのデフォルトのインストール パスを `C:\Program Files\Cisco\AMP` に変更しました。このバージョンにエンドポイントをアップグレードする前に、AMP for Endpoints とともにインストールされているサードパーティ製のソフトウェアに設定した除外を必ず確認してください。

- 簡体字中国語、日本語、および韓国語に対する AMP for Endpoints コネクタの UI にローカリゼーション サポートを追加しました。
- 署名デルタをダウンロードするサポートを追加するために、TETRA エンジンを更新しました。
- AMP for Endpoints AMP for Endpoints コネクタのスタート メニュー グループで、新しい [時間指定診断ツール（Timed Diagnostic Tool）] オプションを使用できるようになりました。
- エンドポイントから シスコ クラウドへの接続をテストするユーティリティをインストール ディレクトリ内に組み込みました。
- AMP for Endpoints コネクタのバイナリは、シスコ EV コード署名証明書を使用して署名されるようになりました。
- AMP for Endpoints Windows AMP for Endpoints コネクタは、セキュア ブートを有効にしたシステムにインストールできるようになりました。

バグ修正/機能拡張

- 報告された多くのクラッシュに対処することにより、AMP for Endpoints コネクタの安定性を改善しました。
- 設定エラーによる不安定性を低減するローカル コンフィギュレーション ファイルの処理を改善しました。
- AMP for Endpoints コネクタのネットワーク ドライバに Windows Driver Verifier を使用した場合に、BSOD が発生する可能性のある問題に対処しました。
- AMP for Endpoints Windows ドライバの高度をより適切に Microsoft ソフトウェアの推奨に沿うように変更しました。
- AMP for Endpoints コネクタがデッドロック状態になる可能性のある問題に対処しました。
- VMWare View Persona Management と LabLogic Debra の互換性の問題に対処しました。
- 仮想化システムが一意として正しく識別されない問題に対処しました。
- インストーラが特定の状況下で正常に完了しない問題に対処しました。
- 以前にダウンロードした TETRA 定義を、一部をアンインストールしてから再インストールすると使用できなくなる問題に対処しました。
- TETRA 定義をダウンロードしているときに、AMP for Endpoints コネクタがタイムリーにシャットダウンしない問題に対処しました。
- アプリケーション ブロッキング イベントが親プロセス情報を適切に報告しない問題を修正しました。
- ログ ファイルが最大サイズを超えて大きくなる可能性のある問題に対処しました。
- ポリシーから高度なカスタム検出定義が削除された後に AMP for Endpoints コネクタが再起動されるまで、AMP for Endpoints コネクタによりこの定義が引き続き適用される問題を修正しました。
- ファイル サイズにワイルドカードを使用するように設定すると HDB の高度なカスタム検出の署名が正しく適用されない問題を修正しました。
- インストール後の最初のスキャンが、ネットワーク アクティビティなしで、またはTETRA 定義が完全にダウンロードされる前に実行される問題に対処しました。
- ソリッド ステート ドライブ（SSD）が搭載されたマシンに AMP for Endpoints コネクタをインストールすると書き込みパフォーマンスに悪影響を与える問題に対処しました。
- 静的 IP アドレスで設定され、かつ [この接続のアドレスを DNS に登録する（Register this connection's addresses in DNS）] オプションが無効な場合に、AMP for Endpoints コネクタがマシンの IP アドレスを取得できない Windows XP の問題に対処しました。

2016 年 12 月 7 日リリース ノート

AMP for Endpoints コンソール 5.4.20161207

新規

- AMP for Endpoints Linux AMP for Endpoints コネクタ ポリシーは、SOCKS プロキシをサポートするようになりました。
- AMP for Endpoints Linux AMP for Endpoints コネクタ ポリシーは、HTTP プロキシを介して NTLM 認証をサポートするようになりました。
- 組織で AMP for Endpoints コネクタがないコンピュータからインシデントを表示するために、エージェントレス認識型インシデントが追加されました。この機能を使用するには、Cognitive Threat Analytics 統合を有効にする必要があります。

バグ修正/機能拡張

- [ダッシュボード（Dashboard）] タブおよび [受信箱（Inbox）] タブにフィルタのリセット ボタンを追加しました。
- [ダッシュボード（Dashboard）] および [受信箱（Inbox）] の [侵害イベントに関するアーティファクト（Significant Compromise Artifacts）] に IP アドレスおよび URL のアーティファクトを追加しました。
- カスタマー フィードバックに基づいて [ダッシュボード（Dashboard）] および [受信箱（Inbox）] の動作をいくつか改善しました。

2016 年 12 月 5 日リリース ノート

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.3.0

新規

- 高度なカスタム検出のサポートを追加しました。
- AMP for Endpoints Mac AMP for Endpoints コネクタは、実行中に使用されるコマンド ライン引数をキャプチャして、この情報を AMP クラウドに送信できるようになりました。この情報は、二要素認証が有効になっている管理者の [デバイストラジェクトリ（Device Trajectory）] で表示できます。
- AMP for Endpoints コネクタは、LZMA によって圧縮された Adobe Flash ファイル、MS Office 2003 XML ファイル内の MSO 添付ファイル、および Hancom Office ファイルに対するクラウド クエリを送信できるようになりました。
- スタートアップおよび起動関連の plist によって参照されるファイルのスキャンを追加しました。
- ClamAV エンジンを 0.99.2 にアップグレードしました。

重要! AMP for Endpoints Mac AMP for Endpoints コネクタは、OS X 10.7 のバージョン 1.3.0 以降をサポートしなくなりました。

バグ修正/機能拡張

- OpenSSL、Jansson、Libxml2 など、サードパーティ製のライブラリからセキュリティ修正を適用しました。
- クラウドから切断されると ClamAV によるファイルのスキャンが停止するバグを修正しました。
- 特定のファイル アクティビティによりスキャンが途中で停止する可能性のある問題に対処しました。
- PDF ファイル内のファイルがスキャンされないバグを修正しました。
- 一部の UDP 接続がモニタされないバグを修正しました。
- ユーザ情報が一部のイベントから欠落しているバグを修正しました。
- 遅延スキャン ファイルが正常に書き込まれなかったため、一部の遅延スキャンがドロップされるバグを修正しました。
- 一部のネットワーク イベントに対して報告された URL の形式が正しくないバグを修正しました。
- 定義更新イベントがイベント テーブルから欠落しているバグを修正しました。
- 定義更新イベントの既知のウイルス件数が正しくないバグを修正しました。
- ClamAV の自動定義更新の堅牢性を増強しました。
- AMP for Endpoints コネクタが監査モードで実行されているときに、実行がブロックされたイベントおよび通知でアクションが実行されなかったことが明確になるようにしました。
- デーモンの起動時に ClamAV の作業ディレクトリから古いファイルを削除しました。
- ワイルドカード除外のパフォーマンスのオーバーヘッドを削減しました。
- デーモンが失敗した初期化手順を停止または再試行しているときに、アクティブなネットワーク接続が存在すると、カーネル拡張がパニックになる可能性のあるバグを修正しました。
- さまざまなロギングの問題を修正しました。

2016 年 11 月 29 日リリース ノート

AMP for Endpoints Linux コネクタ 1.2.1

新規

- Red Hat Enterprise Linux および CentOS 6.7 と 6.8 のサポートを追加しました。

バグ修正/機能拡張

- OpenSSL、cURL、Jansson など、AMP for Endpoints コネクタで使用されるサードパーティ製のライブラリからセキュリティ修正を適用しました。
- コネクタが AMP クラウドに接続していないときの検出機能を改善しました。
- ワイルドカードを含むカスタムの ClamAV ハッシュ ベースの署名（.hdb）がトリガーに失敗するバグを修正しました。

- 遅延スキャン ファイルが正常に書き込まれなかったため、一部の遅延スキャンがドロップされるバグを修正しました。
- PDF ファイル内のファイルがスキャンされないバグを修正しました。
- 除外ルールの大文字と小文字が区別されないバグを修正しました。
- デーモンの起動時に ClamAV の作業ディレクトリから古いファイルを削除しました。
- ClamAV 定義の更新のスケジューリングを最適化しました。
- ローカル データベースが特定のサイズに到達するとコネクタが CPU を大量に消費する問題に対処しました。
- コネクタによる正常なアクションの一部が ampcli で正しく報告されない問題に対処しました。

2016 年 11 月 22 日リリース ノート

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0.9

バグ修正/機能拡張

- curl をバージョン 7.51.0 に更新しました。
- パスワード フィールドに特定の文字を入力するとアンインストール中に AMP for Endpoints コネクタ保護がバイパスされる可能性のある脆弱性に対処しました。

2016 年 11 月 15 日リリース ノート

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.2.6

バグ修正/機能拡張

- curl をバージョン 7.51.0 に更新しました。
- ローカル データベースが特定のサイズに到達すると AMP for Endpoints コネクタが CPU を大量に消費する問題に対処しました。
- 一部のローカルのサードパーティ製ソフトウェアが定期的にファイルにアクセスしても変更しない場合に、AMP for Endpoints コネクタが CPU を大量に消費するバグを修正しました。
- AMP for Endpoints コネクタは、ミュート不可フラグが設定されたファイルを正常に検疫できるようになりました。
- スキャン エラー レポートのさまざまな問題に対処しました。

2016 年 11 月 8 日リリース ノート

AMP for Endpoints コンソール 5.4.20161108

新規

- AMP for Endpoints 導入に対する侵害および脅威のより包括的なビューを表示するために [ダッシュボード（Dashboard）] タブを追加しました。
- [受信箱（Inbox）] タブに、AMP for Endpoints 導入で侵害を処理して解決する単一のビューが表示されるようになりました。

バグ修正/機能拡張

- 導入度の低いオペレーティング システムのファイルにより他の拡散度の低いファイルがわかりにくくならないようにするため、オペレーティング システムのフィルタを [低格拡散度の実行可能ファイル（Low Prevalence Executable）] ページに追加しました。
- 脆弱性データの API にアラート URL を追加しました。

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0.7

バグ修正/機能拡張

- バージョンが 4.2.0 以前のコネクタを、local.xml が破損した状態でアップグレードすると AMP for Endpoints Windows AMP for Endpoints コネクタがボリュームのルート ディレクトリにあるファイル（ただし、サブフォルダ内のファイルではない）を削除する可能性のある問題に対処しました。

  重要： この問題は、以前の AMP for Endpoints Windows AMP for Endpoints コネクタ バージョン 4.2.0 ～ 4.4.2 および 5.0.1 ～ 5.0.5 のすべてに影響していました。以前にこれらをダウンロードした場合は、コネクタの更新にこれらのバージョンのインストーラを使用しないことが重要です。最新バージョン 4.4.4 および 5.0.7 をダウンロードして使用してください。

- クラッシュ状態のコネクタをアップグレードまたはアンインストールするコネクタの機能を改善しました。

重要! 特定のコネクタのバージョンからアップグレードすると、リブートが必要になります。ポリシーを介して新しいインストーラをダウンロードしたり、更新を実行したりすると、選択したグループのコンピュータまたはリブートに必要なポリシーが一覧表示されます。

AMP for Endpoints Windows AMP for Endpoints コネクタ 4.4.4

バグ修正/機能拡張

- バージョンが 4.2.0 以前のコネクタを、local.xml が破損した状態でアップグレードすると AMP for Endpoints Windows AMP for Endpoints コネクタがボリュームのルート ディレクトリにあるファイル（ただし、サブフォルダ内のファイルではない）を削除する可能性のある問題に対処しました。

  重要： この問題は、以前の AMP for Endpoints Windows AMP for Endpoints コネクタ バージョン 4.2.0 ～ 4.4.2 および 5.0.1 ～ 5.0.5 のすべてに影響していました。以前にこれらをダウンロードした場合は、コネクタの更新にこれらのバージョンのインストーラを使用しないことが重要です。最新バージョン 4.4.4 および 5.0.7 をダウンロードして使用してください。

- クラッシュ状態のコネクタをアップグレードまたはアンインストールするコネクタの機能を改善しました。

重要! 特定のコネクタのバージョンからアップグレードすると、リブートが必要になります。ポリシーを介して新しいインストーラをダウンロードしたり、更新を実行したりすると、選択したグループのコンピュータまたはリブートに必要なポリシーが一覧表示されます。

2016 年 10 月 25 日リリース ノート

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0.5（後継 5.0.7）

バグ修正/機能拡張

- バージョン 4.4.2 以前からバージョン 5.0.X にアップグレードすると AMP for Endpoints コネクタが AMP for Endpoints コンソールに新しいコンピュータとして表示される可能性のある問題に対処しました。
- NTLM 認証でプロキシを使用するように設定すると 5.0.X コネクタがクラウドとの通信に失敗する問題を修正しました。
- インストールおよびアップグレードに関連する AMP for Endpoints コネクタ イベントがクラウドに送信されないことがある問題を修正しました。

重要! 5.0.x から 5.0.5 へのアップグレードには、リブートは必要ありません。以前の他のすべてのバージョンからのアップグレードには、**リブートが必要です**。

2016 年 10 月 17 日リリース ノート

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0.3（後継 5.0.7）

バグ修正/機能拡張

- アンインストーラがコマンド ライン引数を受け取らない AMP for Endpoints Windows AMP for Endpoints コネクタ v5.0.1 の問題に対処しました。

重要! 5.0.1 から 5.0.3 へのアップグレードには、リブートは必要ありません。以前の他のすべてのバージョンからのアップグレードには、**リブートが必要です**。

2016 年 10 月 6 日リリース ノート

AMP for Endpoints コンソール 5.4.20161006

新規

- AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0 のコマンド ライン キャプチャにポリシー オプションが追加されました。

バグ修正/機能拡張

- 1 台のコンピュータの監査ログのページネーションが破損するバグを修正しました。
- IOC スキャンから一致するエンドポイント IOC を表示しようとするとエラーが発生する問題を修正しました。

AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0.1（後継 5.0.7）

新規

- AMP for Endpoints Windows コネクタは、CiscoSSL を使用して AMP クラウドと通信するようになりました。コネクタは、2 台の新しいサーバを使用して、この変更の一部としてクラウド ルックアップを実行します。新しいファイアウォールの除外については、『AMP for Endpoints User Guide（AMP for Endpoints ユーザガイド）』を参照してください。

重要: AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0.1 のみ、TCP ポート 443 でのクラウド ルックアップをサポートします。

- AMP for Endpoints Windows AMP for Endpoints コネクタは、実行中に使用されるコマンド ライン引数をキャプチャして、この情報を AMP クラウドに送信できるようになりました。この情報は、二要素認証が有効になっている管理者ユーザの [デバイストラジェクトリ(Device Trajectory)] で表示できます。
- ClamAV を 0.99.2 にアップグレードしました。

バグ修正/機能拡張

- TETRA が悪意のあるファイルとして誤ってフラグを付ける可能性のある問題を修正しました。
- TETRA が特定の状況下で悪意のあるアーカイブ ファイルの検出を適切に処理していない問題を修正しました。
- MTU およびポリシー サイズが原因で、コネクタにより CPU 使用率が高くなる問題を修正しました。
- デバッガ アクセスによりコネクタ プロセスを停止できる問題に対処しました。
- AMP クラウドと継続して接続できるようにするために新しいポリシーの検証を改善しました。
- コマンド ライン スイッチによるインストール プロセス中に、ユーザが一時ファイルを保存するパスを設定できるようになりました。
- コネクタがアンインストールする前の無効な状態であるシナリオを最適に処理するために、アンインストール プロセスを改善しました。
- コネクタ全体の安定性を改善しました。
- コネクタが無効なパスに対するカスタム スキャンの完了を報告する軽微な問題に対処しました。
- AMP クラウドへの部分的な接続によりインストールが無制限にハングする問題を修正しました。
- エラー レポートを改善しました。

重要! AMP for Endpoints コネクタの以前のすべてのバージョンから AMP for Endpoints Windows AMP for Endpoints コネクタ 5.0.1 にアップグレードした場合は、リブートが必要です。

2016 年 9 月 29 日リリース ノート

AMP for Endpoints Mac AMP for Endpoints コネクタ 1.2.5

バグ修正/機能拡張

- AMP for Endpoints Mac AMP for Endpoints コネクタ 1.2.4 および OS X 10.12 の互換性の問題に対処しました。AMP for Endpoints コネクタのバージョン 1.2.4 を実行しているすべてのユーザは、1.2.5 にアップグレードする必要があります。

2016 年 9 月 27 日リリース ノート

AMP for Endpoints Linux AMP for Endpoints コネクタ v1.2.0

新規

- 高度なカスタム検出のサポートを追加しました。
- AMP for Endpoints Linux AMP for Endpoints コネクタは、実行中に使用されるコマンド ライン引数をキャプチャして、この情報を シスコ クラウドに送信できるようになりました。この情報は、二要素認証が有効になっている管理者ユーザの [デバイス トラジェクトリ（Device Trajectory）] で表示できます。
- ClamAV を 0.99.2 にアップグレードしました。
- AMP for Endpoints コネクタは、LZMA によって圧縮された Adobe Flash ファイル、MS Office 2003 XML ファイル内の MSO 添付ファイル、および Hancom Office ファイルに対するクラウド クエリを送信できるようになりました。

バグ修正/機能拡張

- 一部のネットワーク検出イベントがクラウドに正しく報告されないバグを修正しました。
- ClamAV がクラウドから切断されるとファイルがスキャンされないバグを修正しました。
- ClamAV 定義が無効な状態になる可能性のある問題に対処しました。
- ClamAV の自動定義更新の堅牢性を増強しました。
- 特定の状況下で、要求されたファイルをファイル リポジトリにアップロードできない問題に対処しました。
- データが欠落しているため、一部のレトロスペクティブ操作が失敗する可能性のあるバグを修正しました。
- 信頼できる署名済み RPM パッケージからインストールされたファイルは検疫されなくなりました。
- ワイルドカード除外のパフォーマンスのオーバーヘッドを削減しました。
- 一時停止した仮想マシンの再開後に、DNS 解決エラーが発生する可能性のあるバグを修正しました。
- AMP for Endpoints コネクタのロギングの問題を修正しました。

特別なアドバイザリ

RHEL および CentOS 6.0 ～ 6.5 のユーザのための重要なメモ

この更新をインストールする前に、インストールされている procps のバージョンが 3.2.8-30 以降であることを確認してください。古いバージョンの procps は互換性がないため、最新バージョンに更新することをお勧めします。詳細については、次の Red Hat のアドバイザリを参照してください。

https://rhn.redhat.com/errata/RHBA-2014-1595.html
https://rhn.redhat.com/errata/RHBA-2015-1407.html
https://rhn.redhat.com/errata/RHBA-2015-1812.html
https://rhn.redhat.com/errata/RHBA-2015-2643.html
https://rhn.redhat.com/errata/RHBA-2016-0904.html

2016 年 9 月 20 日リリース ノート

AMP for Endpoints コンソール v5.4.20160920

バグ修正/機能拡張

- [イベント（Events）] ページのフィルタに日付フィルタを追加しました。過去 1 日のイベント、過去 1 週間のイベント、またはすべてのイベントを表示できます。
- デモ データ コンピュータに、API ユーザが使用できる MAC アドレスを組み込みました。

2016 年 9 月 8 日リリース ノート

AMP for Endpoints Mac AMP for Endpoints コネクタ v1.2.4.431（後継 1.2.5）

新規

- Mac OS X 10.12 のサポートを追加しました。

バグ修正/機能拡張

- ファイルが削除されると、同じファイルの他のコピーがコンピュータに存在していても、そのファイルをコンピュータから取得できなくなる問題を修正しました。
- AMP for Endpoints コネクタがコンピュータ上のファイルの最初のインスタンスにレトロスペクティブ検疫しか実行しない問題に対処しました。
- コンピュータのリブート時に進行中のスキャンが、コンソールに完了と表示されないバグを修正しました。

2016 年 9 月 7 日リリース ノート

AMP for Endpoints コンソール v5.4.20160907

新規

- デモ データに Cognitive Threat Analytics の例を追加しました。

2016 年 8 月 23 日リリース ノート

AMP for Endpoints コンソール v5.4.20160823

バグ修正/機能拡張

- 監査ログ フィルタが正しく適用されていないバグを修正しました。

2016 年 8 月 9 日リリース ノート

AMP for Endpoints コンソール v5.4

バグ修正/機能拡張

- FireAMP コンソールを AMP for Endpoints にブランド変更しました。

2016 年 7 月 12 日リリース ノート

AMP for Endpoints Mac コネクタ v1.2.2.407

バグ修正/機能拡張

- コネクタによって古い ClamAV 定義がロードされる場合がある問題を修正しました。これにより、誤検出が増加する可能性がありました。

2016 年 7 月 5 日リリース ノート

AMP for Endpoints コンソール v5.3.20160706

新規

- 指定されたグループから AMP for Endpoints コネクタのすべての GUID を取得する API コールを追加しました。
- ユーザは、電子メールでコンソール通知を受信できるようになりました。
- 管理者は、権限のないユーザがアクセス権限を持つグループからのファイル取得を許可できるようになりました。

2016 年 6 月 8 日リリース ノート

AMP for Endpoints コンソール v5.3.20160607

新規

- AMP for Endpoints を、シスコ Cognitive Threat Analytics と統合しました。サポートされる Web プロキシを使用するユーザは、この統合の使用により可視性と効率が向上します。

バグ修正/機能拡張

- Microsoft Windows Defender に対する AMP for Endpoints Windows コネクタのデフォルト ポリシーに、新しい除外を追加しました。

2016 年 5 月 26 日リリース ノート

AMP for Endpoints コンソール v5.3.20160526

新規

- AMP for Endpoints API を使用すると、ビジネスに変更を加えることができるようになりました。API ユーザは、コンピュータを移動し、グループにポリシーを割り当て、アプリケーション ブロッキング リストおよびシンプル カスタム検出リストに変更を加えることができます。
- サードパーティ製のアプリケーション管理を簡素化するために [API クレデンシャル(API Credentials)] ページを追加しました。

バグ修正/機能拡張

- [週次レポート(Weekly Reports)] セクションにリンクを追加しました。これらのリンクにより、レポート メトリックと同じビューにフィルタされた AMP for Endpoints コンソールの該当するセクションに移動します。
- アーカイブ内のファイルによって検出がトリガーされると、アーカイブ ファイルの SHA-256 が表示されるようになりました。
- コネクタが監査モードを使用するポリシー グループに属する場合に、検出イベントが明確になるようにしました。

2016 年 5 月 19 日リリース ノート

AMP for Endpoints Windows コネクタ 4.4.2(後継 4.4.4)

バグ修正/機能拡張

- 特定のアーカイブ ファイル タイプ(CVE-2016-1371、CVE-2016-1372)を処理するときに、潜在的な脆弱性に対処するために ClamAV エンジンにパッチを適用しました。
- コネクタが特定のイベントに対して現在のユーザに関する情報を送信しない問題を修正しました。
- TETRA 定義のダウンロードが完了しても、正常に完了したことが表示されないバグに対処しました。
- コネクタで親ファイル タイプが正しく報告されない場合がある問題を修正しました。

AMP for Endpoints Mac コネクタ v1.2.2.382

バグ修正/機能拡張

- 特定のアーカイブ ファイル タイプ(CVE-2016-1371、CVE-2016-1372)を処理するときに、潜在的な脆弱性に対処するために ClamAV エンジンにパッチを適用しました。
- コネクタ インストーラをローカルで実行するときにダウングレードしないようにこのインストーラを変更しました。
- サポート ツールで収集される診断情報をさらに追加しました。
- Mac OS X 10.8 と 10.9 でアプリケーション ブロッキング リストを使用する際のパフォーマンスを改善しました。
- ネストされたアーカイブ ファイルの処理を改善しました。
- コネクタが特定のイベントに対して現在のユーザに関する情報を送信しない問題を修正しました。
- コネクタがその子プロセスをクリーンアップしない問題を修正しました。
- コネクタがポリシーで設定されているプロキシ サーバに接続できない場合は、Cisco クラウドに直接接続するようになりました。

AMP for Endpoints Linux コネクタ v1.1.0.277

バグ修正/機能拡張

- 特定のアーカイブ ファイル タイプ(CVE-2016-1371、CVE-2016-1372)を処理するときに、潜在的な脆弱性に対処するために ClamAV エンジンにパッチを適用しました。
- コネクタが特定のイベントに対して現在のユーザに関する情報を送信しない問題を修正しました。

- レトロスペクティブな復元操作が失敗する場合がある問題を修正しました。
- ネストされたアーカイブ ファイルの処理を改善しました。
- コネクタがポリシーで設定されているプロキシ サーバに接続できない場合は、Cisco クラウドに直接接続するようになりました。
- [CLI 履歴(CLI history)] ページに非常に長いファイル パスを正しく表示できない問題に対処しました。
- コネクタの問題のデバッグを補助するようにロギングを改善しました。

2016 年 4 月 26 日リリース ノート

AMP for Endpoints コンソール v5.3.20160426

新規

- 右クリックのコンテキスト メニューに VirusTotal を統合しました。
- ポリシーの [製品の更新(Product Update)] セクションおよび [コネクタのダウンロード(Download Connector)] ページにリブートの要件に関する情報が追加されました。

2016 年 4 月 14 日リリース ノート

AMP for Endpoints Windows コネクタ 4.4.1(後継 4.4.4)

バグ修正/機能拡張

- TETRA エンジンが誤検出を生成する問題に対処しました。この問題が発生した顧客にはシスコ サポートから通知しました。
- AMP for Endpoints Windows コネクタの以前のバージョンからアップグレードした際のエラー処理を改善しました。

重要! AMP for Endpoints Windows コネクタのバージョン 4.3.1 または 4.4.0 からアップグレードした場合、このアップグレードにリブートは必要ありません。

2016 年 4 月 7 日リリース ノート

AMP for Endpoints Linux コネクタ v1.0.2.261

新規

- AMP for Endpoints Linux コネクタは、リモートファイルの取得をサポートするようになりました。
- RAR アーカイブのスキャンを追加しました。

バグ修正/機能拡張

- ローカル キャッシュの最適化によるクラウド コミュニケーションのオーバーヘッドを削減しました。
- 全体の安定性とメモリ使用率を改善しました。
- コネクタの問題のデバッグに役立つようにロギングを改善しました。
- SELinux が有効であるとコネクタ アップデータが失敗する問題を解決しました。
- OpenVPN の互換性の問題を修正しました。
- ユーザが作成した除外の処理に関するさまざまな問題を修正しました。
- コネクタが無関係のファイル作成および実行イベントを報告するバグを修正しました。
- ClamAV 定義が、誤ったパスに配置されることがある問題に対処しました。
- 実行可能ファイルの悪意のあるフォークを処理する機能が向上しました。
- 一時停止の後に再開される仮想マシンにインストールされたコネクタの問題に対処しました。
- 権限のないユーザによってローカルの復元操作が開始される可能性のあるバグを修正しました。

重要! バージョン 1.0.0 の AMP for Endpoints Linux コネクタのアップデータの問題により、ポリシー設定を介してアップグレードを実行するユーザに、更新に失敗したイベントが 1 つ以上表示される場合があります。これは正常な状態です。それぞれが失敗した後に、コネクタは自動的に別の試行をスケジュールします。アップグレード プロセスは、24 時間以内に正常に完了する必要があります。rpm または yum を使用した手動アップグレードは影響を受けません。

2016 年 3 月 31 日リリース ノート

AMP for Endpoints Windows コネクタ 4.4.0（後継 4.4.4）

新規

- エンドポイント IOC スキャナは、ファイル システムの変更のみをカタログにする機能をサポートするようになりました。これにより、最初のカタログ全体が完了した後に IOC スキャンをより高速に完了できます。
- AMP for Endpoints Windows では、スケジュール スキャンに Windows 管理者クレデンシャルが不要になりました。

バグ修正/機能拡張

- コネクタの安定性（特に AMP for Endpoints サービスの正常なシャットダウンに関する）を改善しました。
- インストール中およびアップグレード中の コネクタ の信頼性を改善しました。
- ポリシーで変更されると、コネクタはファイルのスキャン サイズの制限を動的に適用するようになりました。以前はコネクタ サービスを停止して再起動する必要がありました。
- 除外処理のさまざまな問題を修正しました。
- AMP for Endpoints コンソールのポリシー更新イベントは、取得したポリシーのシリアル番号を正確に反映するようになりました。
- トラブルシューティングに役立つようにコネクタのエラー レポートを改善しました。
- アーカイブ ファイルの処理を改善しました。
- 以前のバージョンに新しいコネクタ バージョンをインストールすることにより実行されたアップグレードが、ドライバ以外の関連するコマンド ライン スイッチ オプションを適用しない問題を修正しました。

重要! AMP for Endpoints Windows コネクタのバージョン 4.3.1.10163 からアップグレードした場合、このアップグレードにリブートは必要ありません。

2016 年 3 月 24 日リリース ノート

AMP for Endpoints Mac コネクタ v1.2.0.368

新規

- AMP for Endpoints Mac コネクタは、CiscoSSL を使用して AMP クラウドと通信するようになりました。コネクタは、2 台の新しいサーバを使用して、この変更の一部としてクラウド ルックアップを実行します。新しいファイアウォールの除外については、『AMP for Endpoints User Guide（AMP for Endpoints ユーザガイド）』を参照してください。

  重要： AMP for Endpoints Mac AMP for Endpoints コネクタ 1.2.0 のみ、TCP ポート 443 でのクラウド ルックアップをサポートします。

- AMP for Endpoints Mac コネクタにコマンド ライン インターフェイスを追加しました。これを使用して、スキャンの開始、ポリシーの同期、コネクタの履歴の表示などを行うことができます。

バグ修正/機能拡張

- ClamAV をバージョン 0.98.7 に更新しました。
- コネクタ全体の安定性および効率を改善しました。
- ClamAV が必要以上に定義をダウンロードする問題に対処しました。
- イベントを実行する無関係のファイルをコネクタが送信する問題を解決しました。
- さまざまなメモリ使用率の問題に対処しました。
- ネットワーク イベントを確実に処理するために DFC エンジンを改善しました。
- [デバイストラジェクトリ（Device Trajectory）] での表示を向上させるために、ファイル移動イベント検出データを改善しました。
- コネクタがファイル スキャン キューをクリアしない場合がある問題を修正しました。
- さまざまな UI メッセージおよびエラー通知を改善しました。
- 管理コンソールに表示されるイベントのメッセージを改善しました。
- 無効なパスに対してカスタム スキャンを試行する際のエラー メッセージを改善しました。
- コネクタのアップグレード機能およびコンソール通知を改善しました。
- ポリシーの変更に伴ってファイルのスキャン サイズの制限を動的に適用するようにコネクタを更新しました。
- 除外処理のさまざまな問題を修正しました。
- アーカイブ ファイルの処理を改善しました。
- 実行可能ファイルの悪意のあるフォークを処理するコネクタの機能を改善しました。
- OS X 10.10 以降のコネクタの互換性を改善しました。
- コネクタがインストールされた OS X をアップグレードするとシステムがフリーズすることがある問題に対処しました。

- 読み取り専用メディア（DVD など）からインストールする際のコネクタのパフォーマンスを改善しました。
- キャッシュ TTL が想定どおりに期限切れにならない問題に対処しました。
- 効率と柔軟性を向上させるサポート パッケージ作成プロセスを変更しました。
- サポート パッケージのカスタム出力パスを「-o」オプションを使用して指定する機能を追加しました。

2016 年 3 月 22 日リリース ノート

AMP for Endpoints コンソール v5.3.20160322

バグ修正/機能拡張

- ハングルの文書作成ソフトウェア ファイルのサポートを追加しました。これらのファイルは、[ファイル（File）] および [デバイストラジェクトリ（Device Trajectory）] に表示され、ファイル分析に送信できるようになりました。
- ファイル分析の送信に失敗し続けることはほとんどありませんが、その場合、AMP for Endpoints はファイルの送信を無制限に続けようとします。7 日後にファイルを送信しようとするのを停止するために、制限を追加しました。

2016 年 2 月 25 日リリース ノート

AMP for Endpoints コンソール v5.3.20160226

新規

- 週次レポートを、[分析（Analysis）] > [レポート（Reports）] の下に新しいインターフェイスとともに追加しました。以前のレポートには古いレポート リンクを使用してアクセスできますが、そこから新しいレポートを作成することはできません。以前に作成した定期レポートは引き続き実行されます。

2016 年 2 月 22 日リリース ノート

AMP for Endpoints Mac コネクタ v1.0.8.352

バグ修正/機能拡張

- コネクタのネットワーク使用率を削減するために、ローカル クラウドのキャッシュ サイズを増やしました。
- ローカル スキャン エンジンのパフォーマンスを改善しました。
- Mac OS X 10.11 に付属の mail.app のバージョンの除外を更新しました。

2016 年 2 月 10 日リリース ノート

AMP for Endpoints コンソール v5.3.20160210

バグ修正/機能拡張

- ファイル分析と自動分析で使用される Cisco AMP Threat Grid の毎日の送信数を制限する機能を追加しました。その日の残りの送信数も表示されます。
- Cisco AMP Threat Grid のファイル分析に使用する VM のオペレーティング システム イメージを選択できるようになりました。
- [脆弱性(Vulnerabilities)] ページのアプリケーションごとに表示される CVE ID の数を、最新かつ重大な 10 個に制限しました。
- コネクタによって使用される Cisco クラウド サーバのホスト名を変更しました。クラウド サーバは、エンドポイント コネクタの通信にファイアウォールの除外を許可する顧客の機能を向上させるために、静的 IP アドレスも使用するようになりました。この展開は、AMP for Endpoints ユーザに段階的に導入されます。ツールが使用可能になると、AMP for Endpoints コンソールに表示され、既存のポリシーを移行して、新しい静的 IP アドレスを使用する際に役立ちます。

2016 年 2 月 5 日リリース ノート

AMP for Endpoints Windows コネクタ 4.3.1(後継 4.4.4)

バグ修正/機能拡張

- AMP for Endpoints Windows コネクタ v4.3.0.10148 には、悪意のあるファイルが検出されても、デジタル署名された特定の悪意のあるファイルの検疫に問題があるという問題に対処しました。Windows コネクタ v4.3.0.10148 がコンソールから削除されたため、可能な限り早くアップグレードする必要があります。v4.3.0.10148 から v4.3.1.10163 へのアップグレードには、リブートは必要ありません。
- IOC フラッシュ スキャンが、以前のスキャンからファイルを正しくクリーンアップしない問題に対処しました。

重要! AMP for Endpoints Windows コネクタのバージョン 4.3.0.10148 からアップグレードした場合、このアップグレードにリブートは必要ありません。

2015 年 12 月 15 日リリース ノート

AMP for Endpoints コンソール v5.3.20151215

新規

- ユーザは、コンソール全体に選択したタイムゾーンで日時が表示されるようにタイムゾーンを指定できるようになりました。
- 日付エントリの任意の場所をクリックすると、ポップアップ メニューが表示され、追加のオプションが表示されます。
- コンソール全体のメニュー バーにグローバル検索を追加しました。これは、[分析（Analysis）] > [検索（Search）] からアクセスできる検索と同じです。
- 監査ログのフィルタ ビューに移動するビュー変更リンクを追加しました。
- [監査ログ（Audit Log）] ページにフィルタを追加しました。

バグ修正/機能拡張

- 使いやすさを向上させるために [監査ログ（Audit Log）] ページを再設計しました。
- ファイル分析に対する Cisco AMP Threat Grid API のクエリ制限が、[ビジネス（Business）] ページ表示されるようになりました。
- バージョン番号を [ヘルプ（Help）] ダイアログに移動しました。

AMP for Endpoints Windows コネクタ 4.3.0（後継 4.4.4）

新規

- バージョン 4.3.0 からは、これ以降のバージョンにアップグレードした場合、各更新後に AMP for Endpoints Windows コネクタをリブートする必要がなくなりました。

  重要： 主要な機能変更またはバグ修正を含む更新には、リブートが必要になることがあります。

- Windows 10 に対するサポートが追加されました.

バグ修正/更新

- XML、PPT、および DOC ファイルのクラウド ルックアップ サポートを追加しました。
- コネクタの強制リブート タイマーは、ポリシーを介して 2 分、10 分、または 30 分に設定できるようになりました。
- コネクタがプロキシ サーバを使用するように設定されている場合は、TETRA 定義をダウンロードできるようになりました。
- [コネクタ保護（Connector Protection）] が有効な場合は、コマンド ラインでコネクタ サービスを停止できるようになりました。
- 以前のコマンド ライン オプションを保持するためにインストーラを改善しました。
- さまざまな安定性の改善やバグの修正を行いました。

2015 年 11 月 24 日リリース ノート

AMP for Endpoints コンソール v5.2.20151124

バグ修正/機能拡張

- 特定の状況でポリシーの更新が失敗するバグを修正しました。
- 製品を更新するためのイベント タイプ フィルタを追加しました。
- API に、トラジェクトリ データの照会時のファイル パスと名前が含まれるようになりました。
- CSV エクスポートおよび API クエリの結果に、コンピュータの MAC アドレスが含まれるようになりました。
- トラジェクトリ データに誤ったファイル タイプが表示されるバグを修正しました。

2015 年 10 月 15 日リリース ノート

AMP for Endpoints コンソール v5.2.20151015

新規

- アプリケーション プログラミング インターフェイス（API）を使用できるようになりました。これにより、ユーザはコンソールにログインしなくても自分のアカウントのデータおよびイベントにアクセスできます。

バグ修正/機能拡張

- ClamAV コンテンツの更新頻度を選択するオプションを AMP for Endpoints Mac コネクタポリシーに追加しました。

AMP for Endpoints Mac コネクタ v1.0.7.330

バグ修正/機能拡張

- OS X 10.11 のサポートを追加しました。
- AFP を介したタイム マシンのバックアップに時間がかかる問題に対処しました。
- 監査モード中にコネクタがアプリケーションをブロックする問題を修正しました。
- フラッシュ スキャンをより高速に実行するために最適化しました。
- さまざまなバグを修正しました。

2015 年 9 月 30 日リリース ノート

AMP for Endpoints Linux コネクタ v1.0.0.184

新規

- 新しいコネクタは、CentOS 6.4/6.5/6.6 および Red Hat Enterprise Linux 6.5/6.6 をサポートするようになりました。
- SHA-256 照合、ClamAV オフライン エンジン、およびデバイス フロー コリレーション機能を搭載しました。
- シンプル カスタム検出、アプリケーション制御、ネットワーク、除外など、現在のリストをサポートするようになりました。
- 新しい AMP for Endpoints Linux ポリシーは、既存の AMP for Endpoints グループに追加できるようになりました。

2015 年 9 月 21 日リリース ノート

AMP for Endpoints Windows コネクタ 4.1.4

AMP for Endpoints Windows コネクタ 4.2.1（後継 4.4.4）

バグ修正/機能拡張

- コネクタがクラウドから切断される可能性のある問題に対処しました。この問題が発生すると、コンピュータが新しくインストールされたコネクタとしてデフォルトグループに表示されることがあります。AMP for Endpoints Windows のバージョン 4.1.0.10054、4.1.1.10073、および 4.2.0.10084 が影響を受けます。

2015 年 9 月 14 日リリース ノート

AMP for Endpoints コンソール v5.2.20150914

バグ修正/機能拡張

- 使いやすさと一貫性を向上させるために複数の UI を改善しました。
- さまざまなバグ修正および改善を行いました。

2015 年 8 月 13 日リリース ノート

AMP for Endpoints コンソール v5.2.20150813

バグ修正/機能拡張

- ファイル分析に送信されたファイルの AMP Threat Grid スコアが表示されるようになりました。
- 新しいマルウェア サンプルをデモ データに追加しました。
- さまざまなバグ修正および改善を行いました。

2015 年 7 月 21 日リリース ノート

AMP for Endpoints コンソール v5.2.20150721

新規

- 個々のイベント アラートの電子メールをサブスクライブするオプションを追加しました。
- 脆弱プログラム データを CSV ファイルにエクスポートできるようになりました。
- コネクタ GUID でコンピュータを検索する機能を追加しました。
- Internet Explorer で Microsoft Script Host(cscript.exe)を起動するコマンド シェルが起動されたときにフラグを付けるため、疑わしい Cscript の起動と呼ばれる新しい侵入の兆候イベントを追加しました。

バグ修正/機能拡張

- [グループ(Groups)] ページのインターフェイス(グループの作成や編集など)を改善しました。

2015 年 7 月 16 日リリース ノート

AMP for Endpoints Windows コネクタ 4.2.0(後継 4.4.4)

バグ修正/機能拡張

- 対象範囲を増やすためにエンドポイント IOC フラッシュ スキャンのインデックス作成範囲を拡張しました。詳細については、『Cisco Endpoint IOC Attributes(Cisco エンドポイント IOC 属性)』のドキュメントを参照してください。
- 収集時間を短縮するためにエンドポイント IOC コレクション フェーズ中のパフォーマンスを改善しました。
- コネクタのインストールがときどき失敗する問題に対処しました。
- コネクタ全体の安定性を改善しました。
- さまざまなバグを修正しました。

2015 年 6 月 16 日リリース ノート

AMP for Endpoints コンソール v5.2.20150616

バグ修正/機能拡張

- [ユーザ権限（User Permissions）] ページのインターフェイスを改善しました。
- アウトブレイク コントロール リストのインターフェイスを改善しました。
- 簡単にデフォルトの AMP Threat Grid API キーに戻す機能を追加しました。

2015 年 5 月 28 日リリース ノート

AMP for Endpoints Windows コネクタ v4.1.1.10073

バグ修正/機能拡張

- ワイルドカード除外を処理するときの除外エンジンの効率性を改善しました。
- コネクタ クラッシュ レポート ツールが失敗するバグを修正しました。
- 長時間デバッグ モードにするとコネクタがクラッシュする問題を修正しました。
- コネクタが特定のシステムでローカル コンピュータの完全修飾ドメイン名（FQDN）を正しく取得できないバグを修正しました。

2015 年 5 月 12 日リリース ノート

AMP for Endpoints コンソール v5.2.20150512

新規

- 管理者が権限のないユーザに対してグループの表示、ポリシーの編集、およびアウトブレイク コントロール リストの作成と編集を行うためのアクセス権を割り当てる機能を追加しました。

バグ修正/機能拡張

- 高度なカスタム検出リストのすべてのユーザ アクションが監査ログに記録されるように問題を修正しました。

2015 年 4 月 16 日リリース ノート

AMP for Endpoints Mac コネクタ v1.0.6.292

新規

- コマンド ライン パラメータでサポート パッケージの出力パスを指定する機能を追加しました。

バグ修正/機能拡張

- ファイルのハッシュの計算および ClamAV のスキャンをより効率的に行うために、ファイル スキャン エンジンのパフォーマンスを改善しました。
- IOC 検出機能を向上させるために起動 plist ファイルの追加モニタリングを追加しました。
- エンドポイント UI を使用してポリシーを手動で同期しようとした際の誤った通知を削除しました。
- システムの起動時に誤ったログ メッセージが表示される問題を解決しました。
- システムがネットワークに接続されていないか、インターフェイスが無効な場合は「オフライン（Off-line）」と表示し、クラウドへの接続に問題がある場合は「サービスを利用できません（Service Unavailable）」と表示することにより、エンドポイント通知をわかりやすくしました。

2015 年 4 月 7 日リリース ノート

AMP for Endpoints コンソール v5.1.2015040718

新規

- [脆弱性（Vulnerabilities）] ページに、AMP for Endpoints Windows コネクタによって確認された既知の脆弱性を含む実行可能ファイルが表示されるようになりました。
- AMP for Endpoints クラウドへのクラッシュ ダンプ ログ ファイルの自動アップロードを有効または無効にする設定項目をポリシーに追加しました。
- AMP for Endpoints Android コネクタがインストールされたデバイスのすべてのアプリケーションを表示できるようになりました。
- 非標準ポートを介してパブリック IP アドレスからダウンロードされた実行可能ファイルにフラグを付けるために、疑わしいダウンロードと呼ばれる侵入の兆候イベントを追加しました。

バグ修正/機能拡張

- [ファイル分析(File Analysis)] ページに、過去 30 日より前のファイルが表示されない問題を修正しました。
- 検索結果から [デバイストラジェクトリ(Device Trajectory)] ページにアクセスするとこのページに一部のデータが表示されない問題を修正しました。
- [コンピュータ(Computers)] ページからの CSV のエクスポートに IP アドレスを追加しました。

2015 年 3 月 26 日リリース ノート

AMP for Endpoints コンソール v5.1.2015032618

バグ修正/機能拡張

- クラウド クエリの効率を向上させるために AMP for Endpoints Mac コネクタ ポリシーを更新しました。

2015 年 3 月 12 日リリース ノート

AMP for Endpoints Windows コネクタ v4.1.0.10054

新規

- ClamAV エンジンをバージョン 0.98.5 に更新しました。
- TETRA エンジンをバージョン 3.0.0.71 に更新しました。
- Windows Vista、Windows 7、Windows Server 2003、および Windows Server 2008 にコネクタ プロセスの保護を追加しました。

バグ修正/機能拡張

- 最大 10 個のファイルに対するコネクタ ログ ファイルのサイズ制限の適用を追加しました(それぞれのサイズは常に最大 50 MB)。
- 高度なカスタム署名が、コネクタを再起動しなくても動的に適用できるようになりました。
- ポリシーの更新失敗時のエラー レポートを改善しました。
- コネクタのアンインストール イベントが、プロキシの背後から正常に報告されるようになりました。
- コネクタは、プロキシの背後から ID の同期を実行できるようになりました。
- 特定のファイル タイプをスキャンするとコネクタがクラッシュする可能性のあるバグを修正しました。
- 権限のないユーザが UI を使用するとコネクタがクラッシュする脆弱性を修正しました。
- Microsoft Application Verifier ツールを使用するとコネクタがクラッシュするバグを修正しました。

2015 年 3 月 4 日リリース ノート

AMP for Endpoints コンソール v5.1.20150304

新規

- 低拡散度の実行可能ファイルが自動的にファイル分析に送信されるように設定できるようになりました。
- コンピュータの詳細が [コンピュータ(Computers)] ページから CSV ファイルにエクスポートされるようになりました。
- アナウンスにより、新しいリリースまたは次回のシステム メンテナンスがユーザに通知されるようになりました。
- カスタムの Cisco AMP Threat Grid API キーを入力するサポートを追加しました。

バグ修正/機能拡張

- [コンピュータ(Computers)] ページからコンピュータを一括削除する機能を追加しました。
- [コンピュータ(Computers)] ページの一括移動操作を改善しました。
- ユーザがファイル分析から PCAP ファイルをダウンロードしようとすると間違ったファイルがダウンロードされるバグを修正しました。
- ファイル分析検索は、[ユーザのファイル(Your Files)] または [グローバルファイル(Global Files)] コンテキストで実行できるようになりました。
- AMP for Endpoints Windows コネクタ 3.0 が廃止されてサポートされていないため、コネクタ 3.0 ClamAV 互換性モード ポリシー設定を削除しました(このオプションは旧式になります)。

AMP for Endpoints Mac コネクタ v1.0.5.279

新規

- OS X 10.10 で、AMP for Endpoints Mac コネクタが正式に認定されました。

バグ修正/機能拡張

- 悪意のある電子メールが AMP for Endpoints Mac コネクタによって継続的にダウンロードおよび検疫される OS X mail.app の互換性の問題に対処しました。コネクタは悪意のある電子メールが存在することを検出して通知しますが、mail.app で作成された悪意のある .emlx ファイルを検疫しないようになりました。サーバから悪意のある電子メールを手動で削除するのは管理者が行います。自動的に添付ファイルをダウンロードするように mail.app が設定されている場合に、これらが悪意があると判断されると、コネクタはこれらの添付ファイルを検疫し続けます。

重要: この修正は、OS X mail.app にのみ影響します。他の電子メール アプリケーションの動作は異なる可能性があります。

- まれにコネクタが一定期間ポリシーを同期できない問題を解決しました。
- コンピュータがスリープから復帰したり、リブートを実行したりした後に、CPU 使用率が高くなるパフォーマンスの問題に対処しました。
- Spotlight の変更により、OS X 10.10 で CPU 使用率が高くなる問題を修正しました。
- シャットダウンまたはリブートでカーネル拡張が正常にアンロードできない競合状態を解消しました。
- ユーザが作成した除外のコネクタ検証を改善しました。

2015 年 2 月 18 日リリース ノート

AMP for Endpoints コンソール v5.1.20150218

バグ修正/機能拡張

- 互換性と信頼性を向上させるために、AMP for Endpoints Mac コネクタのプロトコル バージョンをアップグレードしました。この更新は、シスコ クラウドと AMP for Endpoints Mac コネクタの間の今後の接続を保証するために必要です。この変更を有効にするために、すべての AMP for Endpoints Mac コネクタ ポリシーが更新されます。
- OpenIOC 形式と AMP for Endpoints エンドポイント IOC エンジンとの互換性に対処するためにバグを修正しました。エンドポイント IOC で誤検出が発生したユーザは、これらを再アップロードする必要があります。

2015 年 2 月 5 日リリース ノート

AMP for Endpoints コンソール v5.1.20150204

バグ修正/機能拡張

- ユーザが SHA-256 またはファイル名でファイル分析の結果を検索できるように修正しました。

2015 年 1 月 29 日リリース ノート

AMP for Endpoints コンソール v5.1.20150129

新規

- ファイル分析を Cisco AMP Threat Grid と完全に統合しました。
- [コンピュータ(Computers)] ページは、エンドポイントがクラウドに接続した最終時刻でフィルタリングできるようになりました。
- 日付を右クリックしてコンテキスト メニューを開くと、すべての日付とタイムスタンプがさまざまな形式で表示される新しい UI 機能を追加しました。

バグ修正/機能拡張

- デバイス トラジェクトリのロード時間のパフォーマンスを改善しました。

2014 年 12 月 11 日リリース ノート

AMP for Endpoints コンソール v5.1.20141211

新規

- AMP for Endpoints コンソールに、管理者および権限のないユーザ アカウントを作成する機能を追加しました。

バグ修正/機能拡張

- 複数のページでのクロスサイト スクリプティングの問題を修正しました。
- ページの外観のさまざまな軽微のバグ修正および機能強化を行いました。

2014 年 12 月 2 日リリース ノート

AMP for Endpoints Mac コネクタ v1.0.4.259

バグ修正/機能拡張

- WebDAV のカーネル パニックの問題を修正しました。
- ポリシーの更新が失敗する競合状態を修正しました。
- ファイル イベント キューを最適化してパフォーマンスを大幅に改善しました。
- メタデータのインデクサに関連する OS X 10.10 Yosemite の互換性を更新しました。
- コネクタ の誤った syslog メッセージをクリーンアップしました。

2014 年 11 月 8 日リリース ノート

AMP for Endpoints コンソール v5.0.2014

バグ修正/機能拡張

- リストまたはレポートを作成したユーザが削除された場合のさまざまなリスト ページおよびレポートに関する修正を行いました。これらのリストの作成者は不明として表示されるようになりました。
- グループ移動に影響を与えることがあるクエリを修正しました。
- プロビジョニングに複数の電子メール アドレスを指定できるようになりました。
- [ダッシュボードの概要(Dashboard Overview)] タブの自動更新を修正しました。

2014 年 11 月 1 日リリース ノート

AMP for Endpoints コンソール v5.0.20141031

バグ修正/機能拡張

- サポート ケースのさまざまなバグを修正しました。

2014 年 10 月 28 日リリース ノート

AMP for Endpoints コンソール v5.0.20141028

新規

- 選択したグループに基づいてビューをフィルタリングできるグループ フィルタを、[ダッシュボード(Dashboard)]、[脅威の根本原因(Threat Root Cause)]、および [導入の概要(Deployment Summary)] ページに追加しました。

バグ修正/機能拡張

- [コンピュータ(Computers)] ページを再設計して、新しいコンピュータ ビューを導入しました。ビューをフィルタリングして、新しいグループに複数のコンピュータを移動できるようになりました。
- [ユーザ(Users)] ページを再設計し、新しいレイアウトになりました。ユーザ アカウントを名前および電子メール アドレスで検索して、自分のアカウントにすぐにアクセスできるようになりました。
- [インストールされているエンドポイント IOC(Installed Endpoint IOCs)] ページでは、エンドポイント IOC 状態に基づいてビューをフィルタリングしたり、エンドポイント IOC を一括で有効化、非アクティブ化、および削除したりすることもできるようになりました。

2014 年 10 月 23 日リリース ノート

AMP for Endpoints Windows コネクタ v4.0.2.10018

新規

- AMP for Endpoints Windows コネクタでサポートされているすべての Windows プラットフォームを含めるために、エンドポイント IOC スキャンの公式サポートを拡張しました。

バグ修正/機能拡張

- IOC スキャナ エンジンを改善するためにさまざまなバグを修正しました。

2014 年 10 月 16 日リリース ノート

AMP for Endpoints Mac コネクタ v1.0.3.228

新規

- ユーザ インターフェイスに、[イベント履歴(Event History)]、[ポリシーの表示(Policy View)]、[ローカルスキャン(Local Scanning)]、および [ヘッドレスモード(Headless Mode)] を追加しました。

重要: 更新後にコネクタにユーザ インターフェイスが表示されない場合は、ポリシーの [クライアントユーザインターフェイスの起動(Start Client User Interface)] 設定を確認します。

重要: 1.0.2 からアップグレードするコネクタには、[履歴(History)] ペインに以前のイベントがすべて表示されるとはかぎりません。

バグ修正/機能拡張

- デバイス フロー コリレーション、定義の更新、Cloud Recall、および製品の更新の通知を追加しました。
- raw DMG ファイルのスキャンをサポートする ClamAV ライブラリを更新しました。
- パフォーマンスの向上。
- サポート ケースのさまざまな修正を行いました。

2014 年 10 月 8 日リリース ノート

AMP for Endpoints コンソール v5.0.20141008

バグ修正/機能拡張

- 属性の再カタログ化の想定時間に関するエンドポイント IOC ドキュメントを強化しました。
- 個々のコンピュータでスキャンを実行する際の [コンピュータ(Computers)] ページをわかりやすくしました。
- [分析のファイルを送信する(Send Files for Analysis)] ポリシー項目が削除され、すべての AMP for Endpoints コネクタでこの設定がオフになりました。
- [オンコピーモード(On Copy Mode)] および [オンムーブモード(On Move Mode)] ポリシー項目が削除され、すべての AMP for Endpoints コネクタでこれらの設定がパッシブになりました。
- [不可視のキャッシュ TTL(Unseen Cache TTL)] ポリシー項目は AMP for Endpoints コネクタで使用されないため、削除しました。
- サポート ケースのさまざまな修正を行いました。

2014 年 10 月 7 日リリース ノート

AMP for Endpoints Windows コネクタ v4.0.1.10011

バグ修正/機能拡張

- コンピュータのディスク容量を使い果たす可能性のある ClamAV のアーカイブ ログの蓄積によって引き起こされるバグを修正しました。ClamAV のアーカイブ ログは、1 時間ごとに削除されるようになりました。

AMP for Endpoints Windows コネクタ v3.1.15.9681

バグ修正/機能拡張

- コンピュータのディスク容量を使い果たす可能性のある ClamAV のアーカイブ ログの蓄積によって引き起こされるバグを修正しました。ClamAV のアーカイブ ログは、1 時間ごとに削除されるようになりました。

2014 年 9 月 25 日リリース ノート

AMP for Endpoints コンソール v5.0.20140925

新規

- エンドポイント IOC（侵入の兆候）機能を追加しました。

バグ修正/機能拡張

- [初回使用（First Use）] ウィザードを若干変更しました。
- サポート ケースのさまざまな修正を行いました。

AMP for Endpoints Windows コネクタ v4.0.0

新規

- エンドポイント IOC（侵入の兆候）スキャナを追加しました。

重要： この機能は、現在 Windows XP SP3 および Windows 7 でのみサポートされています。

バグ修正/機能拡張

- 特定のシナリオで CPU 使用率が高くなる問題を修正しました。

2014 年 8 月 18 日リリース ノート

AMP for Endpoints Mac コネクタ v1.0.2

- さまざまなバグを修正しました。
- [リモート ファイルの取得（Remote File Fetch）] 機能を追加しました。

重要： AMP for Endpoints Mac コネクタのバージョン 1.0.1 のバグにより、ポリシーを介した自動的なアップグレードが行われません。バージョン 1.0.2 にアップグレードするには、インストーラをダウンロードしてこれを手動で実行する必要があります。

2014 年 7 月 24 日リリース ノート

AMP for Endpoints コンソール v4.5.20140724

新規

- わかりやすさと AMP for Endpoints コンソール内での一貫性を向上させるために、[ファイル分析(File Analysis)] ページを完全に再設計しました。
- AMP for Endpoints コネクタのダウンロード ページを再設計して統合しました。
- AMP for Endpoints Windows コネクタ ポリシーに、[最大スキャンファイルサイズ(Maximum Scan File Size)] および [最大アーカイブスキャンファイルサイズ(Maximum Archive Scan File Size)] 項目を追加しました。

バグ修正/機能拡張

- オンライン ヘルプを若干修正しました。
- Google 認証システム アプリケーションで 2 段階認証が正しく同期されていない問題に対処しました。
- イベント フィルタに特殊文字を含めると javascript 除外が発生する可能性のある問題を修正しました。

2014 年 6 月 26 日リリース ノート

AMP for Endpoints コンソール v4.5.20140623

新規

- AMP for Endpoints Windows コネクタのインストーラは、Authenticode 署名検証の変更に準拠しています(https://technet.microsoft.com/en-us/library/security/2915720.aspx)。

バグ修正/機能拡張

- [ファイルリポジトリ(File Repository)] ページの SHA-256 値は、性質に応じて色分けされるようになりました。
- AMP for Endpoints Mac コネクタ ポリシーから [詳細な通知(Verbose Notifications)] ポリシー項目を削除しました。
- 20 MB より大きいファイルをファイル分析にアップロードする際の警告を追加しました。

2014 年 5 月 15 日リリース ノート

AMP for Endpoints コネクタ 3.1.10

バグ修正/機能拡張

- TETRA ライセンス情報を更新しました。TETRA が有効になっているすべての AMP for Endpoints コネクタは、このバージョンにアップグレードする必要があります。
- Microsoft Excel スプレッドシートをネットワーク共有に保存する際の問題を修正しました。

2014 年 5 月 8 日リリース ノート

AMP for Endpoints コンソール 4.5.20140508

新規

- Google 認証システム アプリケーションで、AMP for Endpoints コンソールがアカウント情報の一部として表示されるようになりました。
- 検索結果にリモートで取得されたファイルが含まれるようになりました。
- アウトブレイク コントロールの検索結果が、正しいリストにリダイレクトされるようになりました。
- ファイルの取得時に、ユーザに電子メールで通知が送信されるようになりました。
- [イベント（Events）] ページに、リモート ファイル取得イベントが表示されるようになりました。
- ファイルのステータスを示すようにファイル取得コンテンツ メニューを更新しました。

バグ修正/機能拡張

- ユーザが自分のメール アカウントから URL を送信できるように、コネクタの電子メール導入ページに導入 URL を追加しました。
- Android デバイスで、オペレーティング システムが Windows XP として報告されなくなりました。
- 複数の拡張子がある電子メールアドレス（yahoo.co.uk など）が正しく機能するようになりました。
- ユーザは、別の電子メール アドレスを指定して通知を受信できるようになりました。

AMP for Endpoints Mac コネクタ v1.0.1

バグ修正/機能拡張

- ファイルのスキャンやキャッシュ、コンソール イベント、およびクラウド機能に関連する 40 を超える不具合に対処しました。
- アプリケーション ブロッキング リストが正しく適用されるようになりました。
- ネットワークを介したタイム マシンのバックアップに影響する問題を修正しました。
- アイドル状態のときに CPU 使用率が 100 % に到達する問題に対処しました。

2014 年 4 月 10 日リリース ノート

AMP for Endpoints コンソール v4.5.20140410

新規

- AMP for Endpoints Windows コネクタのバージョン 3.1.9 を実行するコンピュータから個々のファイルを要求する機能。

バグ修正/機能拡張

- [初回使用(First Use)] ウィザードには、[管理(Management)] > [クイックスタート(Quick Start)] メニュー項目からの初期設定後にアクセスできるようになりました。
- 結果の品質とわかりやすさを向上させるために [検索(Search)] ページを強化しました。
- 検索機能から [ベータ(Beta)] タグが削除されました。
- EU 固有の AMP for Endpoints サーバを導入するためのドキュメントを更新しました。
- 2 段階認証を若干修正しました。
- [ビジネス(Business)] ページを再設計しました。

AMP for Endpoints コネクタ 3.1.9

新規

- AMP for Endpoints 管理者は、[リモートファイルの取得(Remote File Fetch)] を使用してコンピュータから個々のファイルを要求できるようになりました。
- Windows Server 2012 へのインストールのサポートが追加されました。

バグ修正/機能拡張

- Microsoft Excel スプレッドシートをネットワーク共有に保存する際に時間がかかる問題を修正しました。
- AMP for Endpoints サーバの初回ルックアップに対する CNAME のサポートを追加しました。
- バージョン 3.1.5 ～ 3.1.8 のインストール中にまれに発生する問題に対処しました。

2014 年 3 月 6 日リリース ノート

AMP for Endpoints コンソール v4.5.20140306

新規

- 2 段階認証はすべてのユーザが使用できるオプションになりました。

バグ修正/機能拡張

- 詳細なファイル情報には、ファイル名または SHA-256 値を検索するか右クリックすることにより、[ファイルトラジェクトリ(File Trajectory)] ページからアクセスできるようになりました。
- 単一のデフォルトの除外設定は、監査、保護、およびトリアージのポリシーごとに 1 つではなく初回使用時に作成されるようになりました。
- 1 月に作成されたポリシーのスケジュール スキャンの実行に失敗する問題に対処しました。
- AMP for Endpoints コンソールのファビコンが新しくなりました。
- 疑わしい動作にフラグを付ける汎用 IOC と呼ばれる新しい侵入の兆候イベントを追加しました。

2014 年 1 月 23 日リリース ノート

AMP for Endpoints コンソール v4.5.20140123

新規

- [AMP for Endpoints の初回使用(AMP for Endpoints First Use)] ウィザードが、最初のログイン時の新しいビジネスで使用できるようになりました。

バグ修正/機能拡張

- 検索時にファイル名を識別しやすくしたり、デバイス トラジェクトリに直接リンクしたりするなど、検索を改善しました。
- ファイル名または SHA-256 値を検索するか右クリックすることにより、[ファイルトラジェクトリ(File Trajectory)] ページから詳細なファイル情報にアクセスできるようになりました。
- コネクタの更新および TETRA コンテンツのダウンロードからネットワーク トラフィックを低減させるポリシー設定。
- タイムスタンプが深夜であるデモ データが作成されたときに、IOC イベントがその時間内に出現しない問題に対処しました。
- さまざまなページにわたるすべてのブラウザのタイプのユーザに対して多数の外観および検証の修正を行いました。
- セキュリティの脆弱性に対処するために、Ruby on Rails の最新バージョンにアップグレードしました。

AMP for Endpoints クラウド IOC エンジン

新規

- バック オフィスで新しい IOC を作成して表現するための VRT および AMP for Endpoints エンジニアの機能。

2013 年 12 月 17 日リリース ノート

AMP for Endpoints コンソール v4.4.20131212

新規

- [ベータ - 再設計済み(Beta - Redesigned)] 検索ページでは、両方のサンドボックス分析レポート全体に豊富なコンテンツや、トラジェクトリ、グループ、ポリシー、ユーザが表示されるようになりました。

バグ修正/機能拡張

- コンソールの他の部分との設計の整合性を高めるため、右クリック メニューを再設計しました。

2013 年 11 月 21 日リリース ノート

AMP for Endpoints コンソール v4.4.20131121

新規

- [拡散度(Prevalence)] という [分析(Analysis)] メニュー項目の下の新しいセクション。[拡散度(Prevalence)] は、顧客の環境で不明な実行ファイルのイベント ビューであり、別の方法で顕在化するのが難しい可能性のある未知の脅威ベクターをよりフォーカスできます。
- 顧客にリリースする前にフィードバックを提供する機会をセールス エンジニア チームに提供する、[AMP for Endpoints の初回使用(AMP for Endpoints First Use)] ウィザードの非表示のビュー。

バグ修正/機能拡張

- 10 月 24 日リリースのヘルプ ドキュメントのコンテキスト依存。これにより、顧客が関連情報をすぐに簡単に見つけることができるようになります。
- コネクタのダウンロード中にエラーが発生すると、ユーザにエラー メッセージが表示されるようになりました。
- [失敗したポリシーの更新(Policy Update Failed)] イベントの誤字を修正しました。
- 除外のパスで、円とウォンの文字が処理されるようになりました。

- 侵入の兆候がない場合の情報メッセージを IOC ウィジェットに追加しました。
- 電子メールでコネクタを展開する場合の javascript の問題を修正しました。
- ダッシュボードのイベント ページのホスト名を使用して可能性のある XSS 攻撃に対処しました。

2013 年 10 月 30 日リリース ノート

Windows コネクタ 3.1.6.9505

バグ修正/機能拡張

- 失敗したスキャン中にユーザに表示されるエラー メッセージの誤字を修正しました。
- ヘルプのショートカットが不要になったため、Windows のスタート メニューおよびコネクタ UI から削除されました。
- SHA-256 および ETHOS を介したファイルの検出に関連する一貫性のない検出動作を修正しました。
- 64 ビットのコンピュータで発生する可能性のある DFC のメモリ リークに対処しました。
- ドライブのルート ディレクトリのカスタム スキャンの実行時に除外が無視されている問題を修正しました。
- DFC により NetMotion VPN クライアントが正常に接続できない NetMotion VPN クライアントのまれな問題に対処しました。
- Windows コネクタのインストール後に、LMS.exe がクラッシュする場合があるまれなケースを修正しました。
- 欠落データによりデバイス トラジェクトリに空のファイル パスが表示されるケースに対処しました。

2013 年 10 月 24 日リリース ノート

AMP for Endpoints コンソール v4.4.20131024

バグ修正/機能拡張

- 既存のヘルプ ドキュメントに完全に索引を付けて検索できるようにしました。これは以前と同じ場所からアクセス可能で、同じ形式であることに注意してください。
- アイテムが悪意があるまたはクリーンとして識別されても、右クリック メニューで常に不明な性質が表示されるデバイス トラジェクトリの問題を修正しました。
- イベント フィルタ リストからの DFC 検出イベント タイプの誤った削除を修正しました。
- デバイス トラジェクトリのロードが遅いまたは正しくロードされないという 2 つのまれな javascript の問題に対処しました。
- シンプルカスタム検出リストのページネーションが 500 エラーになる可能性のある問題を修正しました。

2013 年 10 月 4 日リリース ノート

AMP for Endpoints コンソール v4.4.2013092717

新規

- [導入の概要(Deployment summary)] ページを、Windows コネクタのインストール ステータスのソートとエクスポートができるように再設計しました。
- バックエンド ソフトウェアのインフラストラクチャのアップグレードにより、全体的なエクスペリエンスを高速化しました。

バグ修正/機能拡張

- Defense Center と一貫性のある名称にするために、ニュートラルな性質の名前を [デバイス(Device)] ページおよび [ファイルトラジェクトリ(File Trajectory)] ページで [不明(Unknown)] に変更しました。
- ポリシーに関連付けられている除外設定を削除するとポリシーの除外がなくなるというシナリオを修正しました。
- 移動イベントの検出情報が表示されない javascript エラーに対処しました。
- Windows コネクタ製品をよりタイムリーに更新できるように、ポリシーの製品の更新間隔を 24 時間から 60 分に変更しました。
- [分析(Analysis)] > [イベント(Events)] の下にすべてゼロの SHA-256 が表示されるまれな問題を修正しました。
- MAC アドレスによって ID の同期を実行するとコンソールにコネクタが重複して表示される問題を修正しました。

2013 年 8 月 27 日リリース ノート

AMP for Endpoints コンソール v 4.4.2013082215

バグ修正/機能拡張

- 有効な SHA-256 を検索するとファイル分析レポートが戻されない問題に対処しました。
- 侵害の兆候の親 SHA に分類がないとイベントがレンダリングされないケースを修正しました。
- DC が有効な FQDN なしで登録されるとまれに Defense Center の認証が競合する問題を修正しました。
- 特定のファイル名を送信するコンピュータのデバイス トラジェクトリがまれにレンダリングされない問題を修正しました。

- ユーザが過去に発生した製品更新ウィンドウがあるポリシーをコピーすると通知されるようになりました。
- イベント フィルタの作成時に、ユーザはサブスクリプション タイプを指定できるようになりました。
- 変更する Windows コネクタのファイル名とパス情報をポリシーを介して送信できるようになりました。

2013 年 7 月 29 日リリース ノート

AMP for Endpoints コンソール v4.4.2013072618

新規

- 使用可能になると、Windows コネクタのファイル名とパスが [デバイス（Device）] および [ファイルトラジェクトリ（File Trajectory）] に表示されるようになりました。
- 現在、脅威、パス、およびファイル拡張子の除外に加えてワイルドカード除外が使用できるようになりました。
- フィルタの使用時に時間を短縮するために、論理グループでイベント フィルタを選択できるようになりました。

バグ修正/機能拡張

- フィルタリング可能なイベント タイプとして定期スキャン イベントを追加しました。
- [コンピュータ（Computers）] ページのイベント リストを、[ダッシュボード（Dashboard）] ページで選択したコンピュータに対するイベントをフィルタリングするボタンに置き換えました。
- コンピュータを含むサブグループが表示されないことがあるヒートマップの問題に対処しました。
- イベント アイコンのいずれかで常にゼロが表示されるコメントを修正しました。
- 既存のユーザに変更を加えたときに更新されない [最終更新日（Last Modified）] フィールドを修正しました。
- 有効な DFC のブラックリストのアップロードが失敗する問題に対処しました。

2013 年 7 月 19 日リリース ノート

Windows コネクタ 3.1.5.9394

バグ修正/機能拡張

- トレイ アイコン UI に、[接続済み（Connected）]、[切断済み（Disconnected）]、および [サービス停止済み（Service Stopped）] の 3 つの状態が表示されるようになりました。以前は [接続済み（Connected）] および [切断済み（Disconnected）] のみが表示されていました。
- 特定の条件下で、Windows XP では 3.0.6 からのアップグレードが成功しないドライバの問題を修正しました。
- フラッシュ スキャンがコネクタの登録後すぐに開始されない競合状態に対処しました。
- コネクタがユーザ特権のみのアカウントで実行されているときに、UI に [切断済み（Disconnected）] が表示される問題を修正しました。
- コネクタのインストールの開始時にネットワーク情報が送信されない Windows XP の問題に対処しました。
- Windows 8 でコネクタが [切断済み（Disconnected）] と表示されるまれな状態を修正しました。

2013 年 6 月 27 日リリース ノート

AMP for Endpoints コンソール v4.4.2013062716

新規

- AMP for Endpoints のすべてのイベント タイプに対してイベント フィルタリングが有効になりました。
- より多くの関連情報を提供するために、サブスクリプションの電子メールを含むイベント サブスクリプションを完全に再設計しました。

バグ修正/機能拡張

- ヒートマップで、問題になっているグループをドリルダウンして、過去 7 日間の検出を表示できるようになりました。
- AMP for Endpoints インストーラは、インストーラ名にグループ名を組み込むようになりました。
- 以前に保存されたイベント フィルタの名前を変更できるようになりました。
- ヒートマップが非アクティブなコネクタの検出を表示する問題に対処しました。
- ファイル分析、各イベントから使用可能なすべてのコンピュータに対する検疫の復元。
- [ファイル（File）] および [デバイストラジェクトリ（Device Trajectory）] にトップ レベル イベントのボタンを追加しました。

2013 年 5 月 30 日リリース ノート

Windows コネクタ 3.1.4

新規

- Windows 8 の完全サポート。
- サポートされているすべての OS の Tetra エンジンを更新しました。

バグ修正/機能拡張

- 右クリック メニューのスキャンを無効にする新しいコマンド ライン スイッチおよびコンテキスト メニュー。
- 別のインストールがすでに進行している場合にインストールが失敗する可能性のある問題を修正しました。
- サポートされていない OS に対してインストールが有効になっている不具合に対処しました。
- ルートキットの削除が完了しない、および削除のプロンプトが表示されない問題を修正しました。
- コネクタを再起動しないと適用されない CSIDL 除外を修正しました。
- agent.exe の名前を sfc.exe に変更しました。
- プロキシ環境でのインストールに関連する修正をいくつか行いました。

AMP for Endpoints コンソール v4.4.20130530

新規

- ダッシュボードのイベントの永続フィルタを保存および作成する機能。

バグ修正/機能拡張

- ポリシーを XML としてダウンロードする機能を追加しました。
- シンプル カスタム検出、アプリケーション ブロッキング リスト、およびホワイトリストの名前を変更できるようになりました。
- [ポリシーの作成(Create Policy)] をすばやく続けてクリックするとサイレント障害が発生する問題に対処しました。

2013 年 5 月 6 日リリース ノート

AMP for Endpoints コンソール v4.4.2013050623

新規

- 既存のポリシーをコピーする機能を追加しました。
- DFC イベントに関連するプロセスの処理が使用可能な場合は表示されるようになりました。

バグ修正/機能拡張

- 既存のカスタム除外を更新するときにサイレント障害が発生する可能性のある問題を修正しました。
- Chrome および Internet Explorer のトラジェクトリ検索ページでページ分けするときに発生する可能性のある問題に対処しました。

総合イベント

新規

- 使用されるポートや DGA（ドメイン生成アルゴリズム）などのさまざまな特性に基づいて感染を特定する IOC「疑わしいボットネット」を最近追加しました。

2013 年 3 月 8 日リリース ノート

AMP for Endpoints コンソール v4.4.2013030807

新規

- ダッシュボードのイベントで使用できる代替リスト ビュー。
- 新しいダッシュボード リスト ビューの個々のイベントにコメントを追加する機能。
- ダッシュボード、イベント、およびトラジェクトリ ビューに追加された追加の IOC。

バグ修正/機能拡張

- 一部のイベントの順序設定を向上させるために、デバイス トラジェクトリでナノ秒のタイムスタンプがサポートされるようになりました。
- 3 つ以上の IP アドレスに対して表示されない DFC IP リストのまれな問題を修正しました。
- デバイス トラジェクトリの軽微なさまざまな外観および javascript の問題に対処しました。

Windows コネクタ 3.1.1.9252

バグ修正/機能拡張

- 一部のアップグレードの状態が以前に発生したまれなケースでコネクタのアップグレードが完了するように修正しました。
- コネクタの起動とアンインストールの間の競合状態を修正しました。
- バージョン チェック フラグが付いたアップグレード時に以前のコネクタ バージョンを検出する不具合に対処しました。

総合イベント

新規

- コマンド シェルを起動する不明なアプリケーションを実行する次のプログラムに IOC を追加しました。
  - Java
  - Acrobat
  - Word
  - Excel
  - PowerPoint

バグ修正/機能拡張

- 既存の IOC の効果を向上させるために SHA を追加しました。

2013 年 4 月 8 日リリース ノート

AMP for Endpoints コンソール v4.4.2013040823

新規

- [脅威の根本原因（Threat Root Cause）] を全面的に再設計し、パフォーマンスを大幅に改善しました。
- 電子メール通知が再設計され、豊富で詳細な実用的なデータが含まれるようになりました。
- ダッシュボードのイベント ページからイベントを CSV としてエクスポートできるようになりました。

バグ修正/機能拡張

- ダッシュボード ウィジェットの [侵入の兆候（IOC）（Indication of Compromise (IOC)）] をクリックすると、デバイス トラジェクトリで強調表示されている総合イベントに直接移動するようになりました。
- デバイス トラジェクトリでスライド可能なタイム スケールを使用できるようになりました。これにより、ユーザは表示する時間幅を指定できます。
- カスタマー フィードバックに基づいて、ポリシー、ID の同期、および一般的な使用方法のさまざまなバグに対処しました。

総合イベント

新規

- マルウェアが実行されたコンピュータを特定する新しい IOC。

バグ修正/機能拡張

- 既存の IOC の効果を向上させるためにフィールドに新しい SHA を追加しました。