クイック スタート ガイド:レポートの基本

Umbrella のレポート

このドキュメントで説明する内容は、次のとおりです。

Umbrella のレポートの基本

Umbrella のレポート機能を使用することで、Cisco Umbrella の使用状況を詳細に把握できます。ここでは、要求アクティビティやブロック アクティビティに関する詳細な情報を把握でき、どのアイデンティティがブロックされる要求を生成しているかを判断できます。レポートにより、セキュリティ脅威に対応するための実用的なインテリジェンスを構築でき、時間経過によるトレンドの変化などの情報も考慮することができます。

Umbrella ダッシュボードのレポートでは、さまざまな領域の事象が扱われており、一部のレポートではより詳細な情報を確認できます。本ドキュメントは、上記のことが反映されるように、複数のセクションに分けられています。

レポートの概要

Umbrella の主要なレポートは、次のとおりです。

- **アクティビティ検索**：指定期間内の環境内のアイデンティティによるアクティビティ。アイデンティティ名、接続先、接続元 IP、応答、コンテンツ カテゴリ、セキュリティ カテゴリによるフィルタが可能です。
- **セキュリティ アクティビティ**：指定期間内のセキュリティ関連のアクティビティ。マルウェア、フィッシング、その他のすべてのセキュリティ カテゴリが含まれます。アイデンティティ、接続先、接続元 IP、セキュリティ カテゴリによるフィルタが可能です。
- **クラウド サービス**：指定期間内に組織がアクセスしたクラウド サービスの概要。クラウド サービス名、アイデンティティ、分類によるフィルタが可能です。
- **接続先レポート**：すべてのアイデンティティを対象に、ダッシュボード内で最もアクティブな接続先を表示するレポート。自身のアイデンティティから特定の接続先に送信されるトラフィックを確認したり、Umbrella の全グローバル ネットワークのトラフィックと比較したりできます。
- **アイデンティティ レポート**：最もアクティブな順にアイデンティティを表示するレポート。特定のアイデンティティに関する詳細、接続先、その接続先が悪意のあるものかどうか、トラフィック全体の傾向などを詳細に確認できます。
- **総要求数**：指定期間内に組織から接続先へ送られた要求の総数。アイデンティティによるフィルタが可能です。
- **アクティビティ ボリューム**：指定期間内の組織内のクエリの合計。セキュリティ カテゴリや結果で項目分けされています。アイデンティティによるフィルタが可能です。このレポートには 2 つのビューがあります：スナップショット（表）、時系列での傾向（グラフ）。
- **上位ドメイン**：指定期間内に組織内で最も要求の多かったドメインのリスト。アイデンティティ、応答、接続先、コンテンツ カテゴリ、セキュリティ カテゴリによるフィルタが可能です。
- **上位カテゴリ**：指定期間内の、組織における上位のコンテンツ カテゴリのリスト。アイデンティティ、応答によるフィルタが可能です。
- **上位アイデンティティ**：指定期間内の、トラフィックを生成した上位のアイデンティティのリスト。アイデンティティ、接続先によるフィルタが可能です。
- **管理監査ログ**：ダッシュボードのすべての管理者による、すべての設定変更に関する記録。

アイデンティティ レポートと接続先レポートの 2 つについては、限定提供のベータ リリース プログラムの一部として、現在テスト中です。これらのレポートの詳細については、数週間のうちに公開されます。

レポートのエクスポート、共有、ブックマーク、スケジューリング

レポートの共有機能は、[レポートの共有（Share Reports）] アイコンをクリックすると [レポート（Reports）] の下に表示されます。

レポートの保持期間

情報のレポートは、Cisco Umbrella へのトラフィック送信が開始されるとすぐに始められます。

Umbrella では、次のレポートが 2 年間保持されます。

- アクティビティ ボリューム
- 総要求数
- 上位ドメイン
- 上位カテゴリ
- 上位アイデンティティ

フィルタの [日付検索（Date Search）] フィールドの [カスタム日付範囲（Custom Date Range）]、 オプションで、直近 2 年間のレポートを、最大 90 日間の区切りで検索できます。

次のレポートは、30 日間の検索ウィンドウに限定されています。

- 上位ドメイン
- 総要求数
- セキュリティ アクティビティ*
- アクティビティ検索*
    - アクティビティ検索、またはセキュリティ アクティビティのデータについては、現在、30 日以上は保持されていません。

クイックスタートガイド：レポートの基本 > セキュリティ カテゴリについて

セキュリティ カテゴリについて

セキュリティ カテゴリとは、Cisco Umbrella が提供するセキュリティ防御に関するカテゴリです。このセキュリティ脅威の分類によって、有効にしたい内容やレポートしたい内容をより正確に制御できます。このドキュメントを確認することで、各カテゴリでブロックされる脅威タイプについて把握することができます。

セキュリティ設定へアクセスするには、[ポリシー（Policies）] > [セキュリティ設定（Security Settings）] に移動してください。

セキュリティ カテゴリで予定されている変更

Cisco Umbrella サービスのセキュリティ カテゴリに関して、いくつかの変更が予定されています。有効にしたい内容やレポートしたい内容をより正確に制御できるように、セキュリティ脅威のカテゴリを改善する方法が常に模索されています。
カスタマー フィードバックに基づいて、4 月の中旬から後半に、次の変更が行われる予定です。**なお、ユーザによる変更は不要です。**

疑わしい応答のカテゴリが削除されます。疑わしい応答のカテゴリは数年前に作成され、実際には広く使われることのなかった理論的な攻撃を扱っていました。多くのお客様からご意見を受け、このカテゴリについては削除することが最善であると決定されました。セキュリティ レポートにおいては、お客様が最も重要なイベントに集中できるようになることが目標とされています。このカテゴリには価値が見出せず、レポートに不要な情報を表示させ、混乱を生じさせるものでした。

モバイル脅威、ドライブ バイ ダウンロード、高リスク サイトは、マルウェア カテゴリに統合されます。カテゴリ管理をシンプルにする観点から、これらのカテゴリが統合されることになりました。これにより、管理がより容易になり、機能も損なわれないことがご確認いただけると考えています。
予期しない変更により、質問や疑問点も生じるかと思います。そのような場合には、アカウント マネージャや umbrella-support@cisco.com まで、ご遠慮なくお問い合わせください。

結果として、「高度な脅威」に属するすべての脅威カテゴリが既存のカテゴリに統合されます。同様に、保護や機能が損なわれることはありません。この変更はレポートを改善し、ご利用の環境で脅威を分類する際の実用性を向上させることを目的としています。

セキュリティ カテゴリの概要

セキュリティ カテゴリは、防止、封じ込め、高度な脅威の個別のグループに分けられています。

- 防止：ユーザが、マルウェアやエクスプロイトの仕込まれたコンテンツやサイトにアクセスすることを阻止します。要求が送信される際のアプリケーション、ポート、プロトコルに関わりなく、ユーザがそのようなコンテンツに確実にアクセスしないようにします。
- 封じ込め：マルウェアからのコマンド アンド コントロール サーバへの要求を遮断します。ユーザが欺かれてフィッシング サイトにアクセスするのを止め、それによって、ネットワーク上の脅威を封じ込め、ハッカーがリモートからアクセスするのを防ぎます。
- 高度な脅威：悪意のあるドメインを予測的に保護します。Cisco Umbrella Security Graph のセキュリティ アルゴリズムの活用により、予防的なセキュリティ保護を提供し、将来の高度な脅威を現時点で阻止します。

また、統合と呼称される特定のパッケージが、サブカテゴリとして利用可能です。統合セキュリティ カテゴリは、それぞれの統合を通じて Umbrella に追加されたドメインから構成されます。統合に関する詳細については、こちらを参照ください。

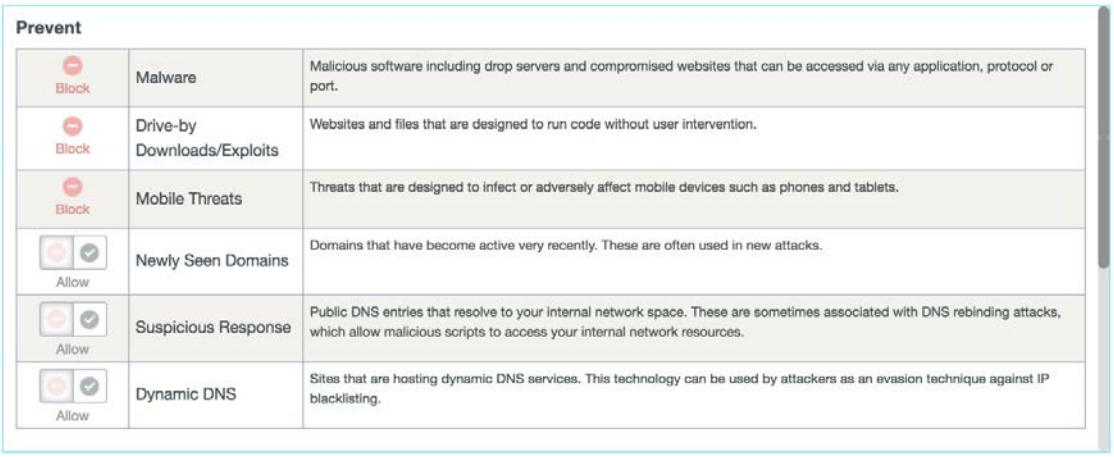
サブカテゴリ

これらの大項目のセキュリティ カテゴリの中には、それぞれに小項目のカテゴリがあります。デフォルトのセキュリティ設定が、設定の簡単な説明と共に記載されています。

注

ここでいうところの「デフォルト」とは、新規のお客様や、新規/既存ポリシーに対して事前設定されたデフォルトの Umbrella 設定を選択したお客様にとってのものです。セキュリティ カテゴリには、個別に無効化したり、設定したりすることのできないものもあり、「デフォルトで有効」とみなされます。

防止



- マルウェア：マルウェアをホストするサーバ、侵害された Web サイトへの、アプリケーション、プロトコル、ポートからのアクセスをブロックします。*デフォルトで有効となっています。*
- ドライブ バイ ダウンロード/エクスプロイト：ユーザの操作なしにマルウェアを配布するエクスプロイトをホストしている Web サイトへの要求をブロックします。*デフォルトで有効となっています。*
- モバイル脅威：特定の電話、タブレット、その他のローミング デバイスに特化した脅威への要求をブロックします。*デフォルトで有効となっています。*
- 疑わしい応答：パブリック DNS エントリの内部ネットワーク空間への解決を防止します。これにより、悪意のあるスクリプトが内部ネットワーク リソースへアクセスすることを可能にする、DNS 再バインディング攻撃を阻止します。疑わしい応答に関する詳細については、こちらを参照ください。*デフォルトで無効となっています。*
- ダイナミック DNS：ダイナミック DNS コンテンツをホストしているサイトをブロックします。*デフォルトで無効となっています。*
- 新しく確認されたドメイン：直近で初めてクエリされたことが確認されたドメインを検出します。このカテゴリに関する重要な詳細については、こちらを参照ください。*デフォルトで無効となっています。*

封じ込め

- 侵害されたデバイスから、任意のアプリケーション、プロトコル、ポートを通じてハッカーのコマンド アンド コントロール サーバに通信が行われることを防ぎ、ネットワーク上の潜在的な感染端末を特定できるようにします。*デフォルトで有効となっています。*
- フィッシング：個人情報の窃盗を企図して、ユーザを欺くための偽の Web サイトからユーザを保護します。*デフォルトで有効となっています。*

高度な脅威

- 高リスクサイトおよびロケーション：Umbrella の予測的なセキュリティ アルゴリズムに一致するドメイン

これらのセキュリティ カテゴリはすべて、セキュリティ概要レポートなどのその他のレポートについて理解する上で重要です。

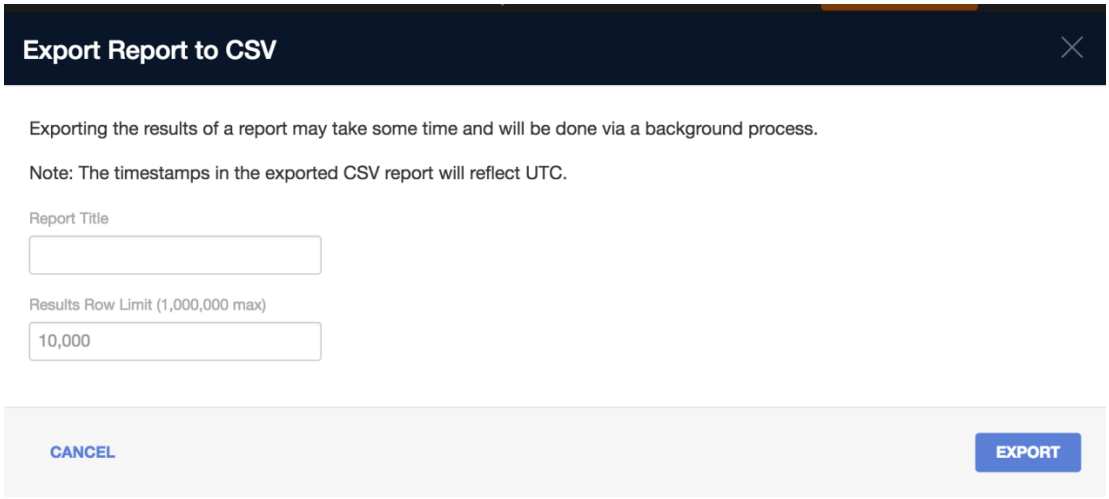
クイック スタート ガイド：レポートの概要 > **セキュリティ カテゴリについて** > レポートのエクスポート、共有、ブックマーク

レポートのエクスポート、共有、ブックマーク

CSV へのエクスポート

レポートを取り扱う場合、特定のクエリの結果を CSV フォーマットでエクスポートすることができます。CSV フォーマットにすることで、他のツールに流し込み、別のレポートやグラフを作成することができます。エクスポートするデータは、ユーザのタイムゾーンに関わりなく、常に UTC に設定されます。
また、CSV へのデータのエクスポートには、1,000,000 行までという制限があります。
ほとんどのレポートの上部に、[エクスポート(Export)] ボタンがあります。次のようなアイコンです。

エクスポートするレポートには、1,000,000 行の制限があります。レポートが 1,000,000 行を超える場合は、より短い期間を指定するか、より詳細にフィルタを設定して、レポートを再実行するようにしてください。最初に実行したレポートの最後の行を確認し、その行に記載されている時間から次のデータ群のレポートを再実行することでも対応できます。

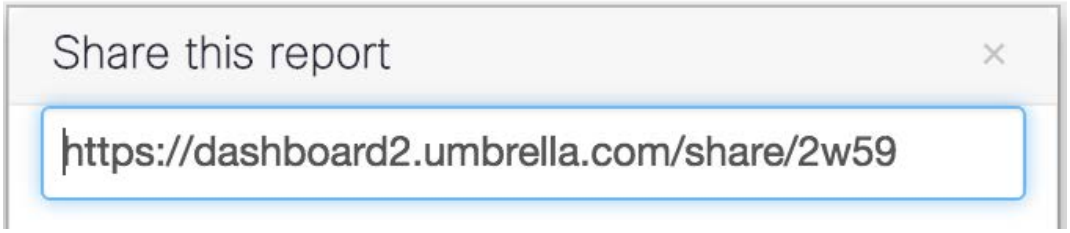


共有

リンクを作成して、自身が実行したレポートを組織内にいる他の Umbrella ダッシュボード管理者にも確認できるようにするには、共有レポート機能を利用します。

レポートの共有機能は、[レポートの共有（Share Reports）] アイコンをクリックすると [レポート（Reports）] の下に表示されます。

レポートを共有するには、定義したフィルタを使ってレポートを実行するか、事前定義済みのフィルタを使用する新しいブックマーク レポート機能を活用してください。レポートの実行後、[レポートの共有（Share Reports）] アイコンをクリックすると、ハイパーリンクが表示されます。そのハイパーリンクを、電子メール、インスタント メッセージ、ツイートなどで、他の Umbrella 管理者に送信することができます。



注:このレポートの共有リンクは、Umbrella ダッシュボードにログインできるユーザに対してのみ有効です。レポートのすべての情報を管理者以外のユーザに向けてエクスポートしたい場合は、CSV へのエクスポート機能を使用します。

次に、レポートの URL をクリップボードにコピーし、必要なところにペーストします。別の管理者がその送信されたリンクをクリックすると、ダッシュボードへの認証が行われます(まだ認証していない場合)。認証が完了すれば、共有されたレポートに直接アクセスできるようになります。

ブックマーク

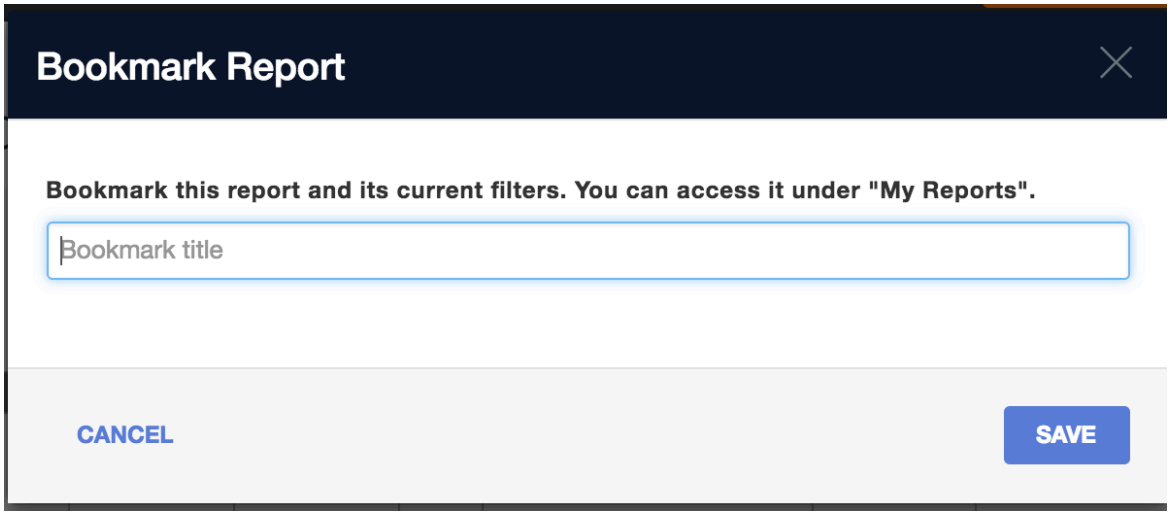
レポートをブックマークすることで、レポートを素早く保存し、後で再実行できます。再実行する際は、レポートを設定し直す必要はありません。そのためにはまず、事前定義されたレポートから独自のセットを作成します。
それを行うには、[レポート(Reports)] の [ブックマーク レポート(Bookmark Report)] 機能を利用します。

ブックマーク機能により、特定のレポートを再実行し、迅速かつ容易に結果を得ることができます。
まず、アクティビティ検索や事前定義済みレポートのいずれかから、実行したいレポートのパラメータを選択します。この例では、過去 7 日間にブロックされた要求に関するアクティビティ検索を表示させます。

[フィルタ(Filter)] オプションを選択し、[レポートの実行(Run Report)] をクリックします。

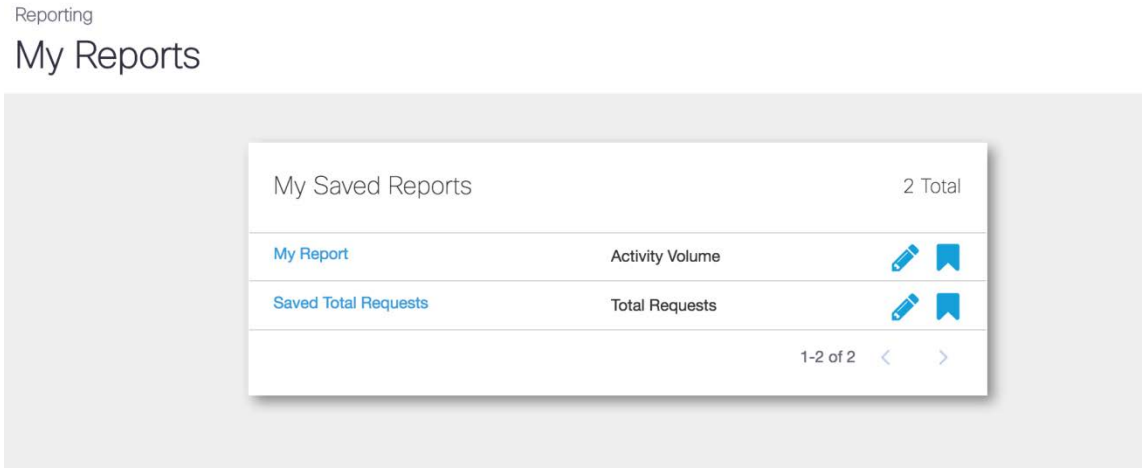
次に、[ブックマーク(bookmark)] アイコンをクリックします。

ポップアップ画面が表示されるので、レポートに名前をつけます。



注:ブックマーク レポートは後で名前を変更することができ、再度ブックマークする必要もありません。

ブックマークを作成すると、左側のサイドバーに [マイ レポート(My Reports)] という新しいメニューができ、そこからブックマークされたレポートにアクセスできるようになります。



レポートをクリックすると、直接レポートにアクセスでき、ブックマークの名前とレポートのタイプが表示されます。

注:ブックマーク レポートの日付の範囲は、固定日時を選ぶか、相対的なデータ スタンプを選ぶかによって異なります。たとえば、[直近 24 時間(Last 24 Hours)] の場合は、ブックマーク レポートを実行した時点から 24 時間後までの範囲になります。一方、[カスタム日付範囲(Custom Date Range)] の場合は、再実行しても、日付がシフトされることはなく、同じ日付の範囲のデータが表示されます。

アクティビティ検索の場合は、レポートのデータ量が大きいことから、過去 28 日分のみがレポートされます。[カスタム日付範囲(Custom Date Range)] を選択し、ブックマークしてから再実行した場合、28 日を超える範囲のデータについては、一切レポートされません。

セキュリティ カテゴリについて > **レポートのエクスポート、共有、ブックマーク** > スケジューリングされたレポート:概要および設定

スケジューリングされたレポート：概要および設定

このドキュメントでは、Umbrella ダッシュボードで電子メール レポートをスケジューリングする方法を説明します。また、スケジューリングされた電子メール レポートを変更または削除する方法についても説明します。送信されるレポートの電子メールには、レポートの HTML バージョンの表が含まれ、データ セット全体が含まれた CSV ファイルが添付されます。また、同じレポートの実際のバージョンへのリンクも含まれます。

重要事項：Cisco Umbrella では、電子メール配信サービスに MailGun を使用します。ローカル レベル、またはトランスポート層（ISP など）のメール フィルタによっては、MailGun からの通信がマーケティング関係のスパムとしてブロックされる場合があります。レポートのスケジューリングを設定した後に、レポートを受け取れない場合は、メール サーバ ゲートウェイのスパム フィルタを確認してください。メール サーバ ゲートウェイがローカルまたはクラウドでホストされている場合、いずれかで電子メールが隔離されている場合があります。

レポートは、次のアドレスから送信されます。
scheduled-reports-feedback@opendns.com

スケジューリングされたレポートの情報には 10,000 行までという制限があります。なお、DNS 要求 1 つにつき 1 行です。

スケジューリングされた電子メール レポートの追加

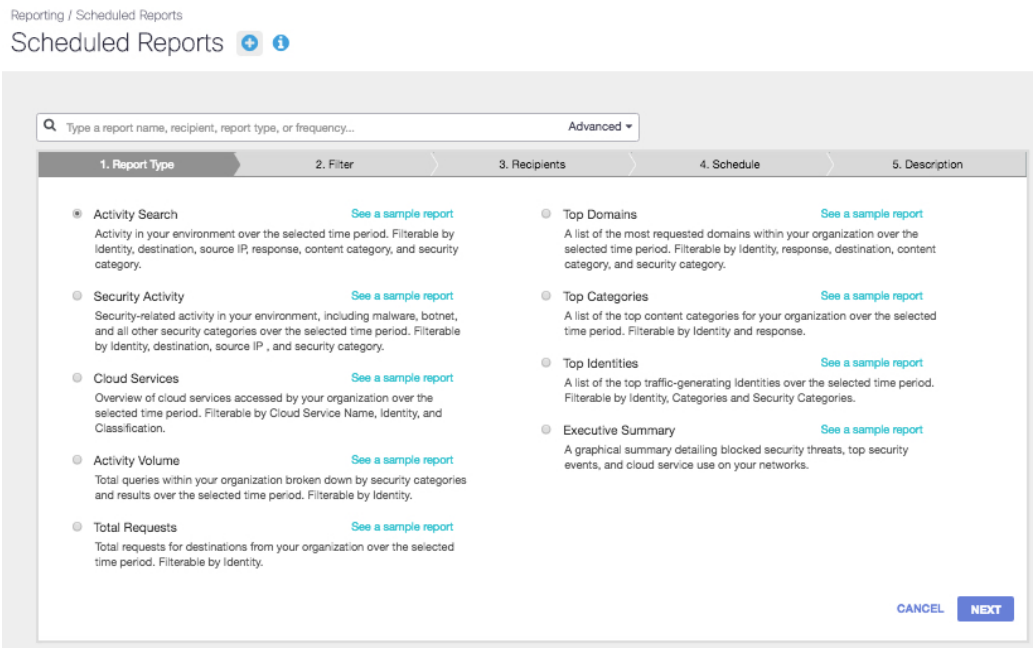
1. [レポート（Reporting）] > [スケジューリングされたレポート（Scheduled Reports）] に移動します。

2. [+] アイコン（[追加（Add）] アイコン）をクリックして、レポートのスケジューリングを行います（上のスクリーンショットを参照）。

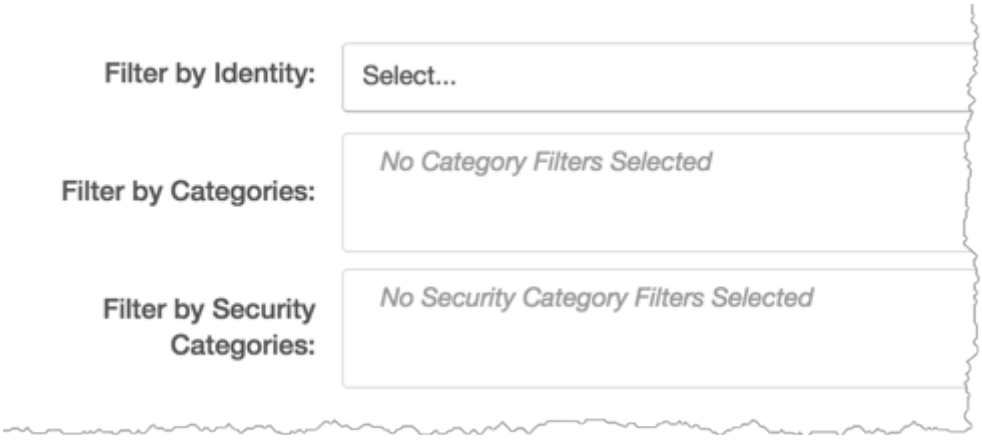
3. 5 つの手順によるウィザードが表示されます。スケジューリングできるレポートが 8 つ表示され、それぞれに簡単な説明が示されています。
   また、すべてのレポートに、[カレンダー（Calendar）] アイコンがついており、それをクリックして同じウィザードを開始することもできます。

3. 希望するレポートのタイプを選択し、スケジューリングされたレポートに名前を付け、[次へ（Next）] をクリックします。
   次のレポートをスケジューリングすることができます：
   アクティビティ検索、セキュリティ アクティビティ、クラウド サービス、アクティビティ ボリューム、総要求数、上位ドメイン、上位カテゴリ、上位アイデンティティ

4. リストからレポートを選択します。選択したレポートの表示例を念のために確認したい場合は、[サンプル レポートの表示（See a sample report）] をクリックします。

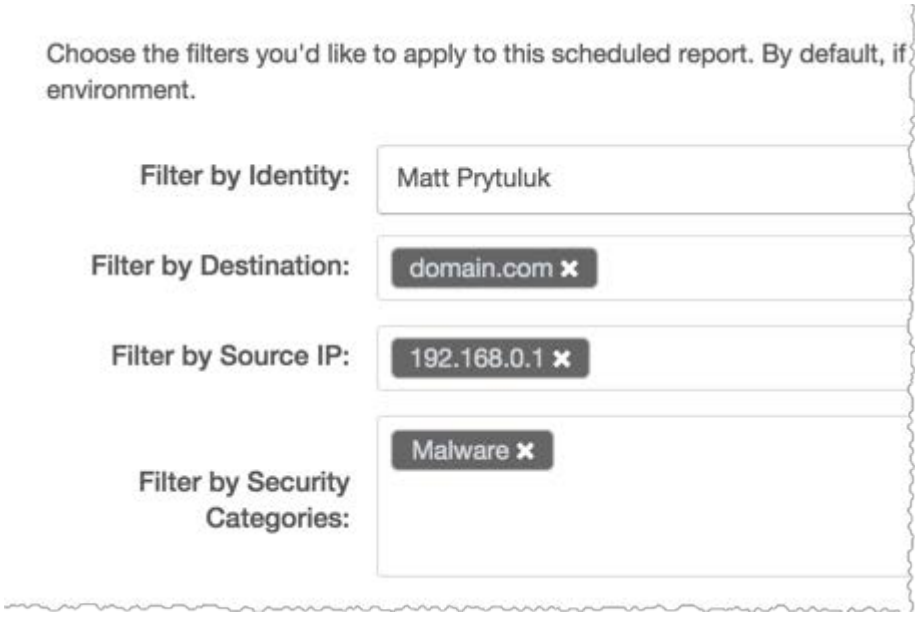


5. 適切なフィルタを選択します。スケジューリングされたレポートが 10,000 行を超えないように適切なフィルタを設定することが重要です。そうすることで、レポートが受信者にとってわかりやすく実用的なものとなります。フィルタを一切追加しない場合、環境全体のすべてのタイプのトラフィックについてレポートされます。ウィザードの手順 2 で、アイデンティティ用のフィルタ、またはセキュリティ カテゴリ、コンテンツ設定、接続先など他の主要フィルタを適用することができます。フィルタはレポートのタイプごとに異なりますが、レポート自体にすでに関連付けられているフィルタを利用できます。たとえば、セキュリティ アクティビティ レポートを選択した場合、アイデンティティ、接続先、接続元 IP、セキュリティ カテゴリでのフィルタが可能となります。



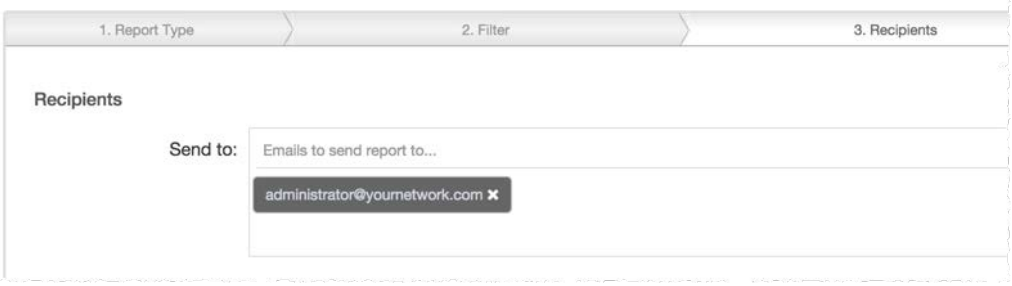
注: 接続先（ドメイン）や接続元 IP アドレスを追加する場合は、フィルタを入力してから Enter を押します。そうしないと保存されません。

フィルタを追加すると、レポートの設定は次のようになります。



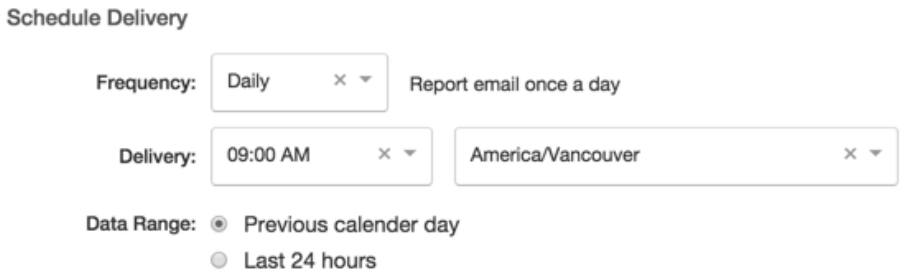
ほとんどのレポートでは、[セキュリティ カテゴリによるフィルタ(Filter by Security Categories)] が表示されますが、クラウド サービス レポートでは、[分類によるフィルタ(Filter by Classifications)] が表示されます。

6. ウィザードの手順 3 で、電子メールの受信者を設定します。追加したい受信者をの数だけ入力してください。エンター キー、スペース キー、タブ キーを押すか、各電子メールの間に、コンマやセミコロンを入力します。



メール アドレスは、既存のシステム管理者に関連付ける必要はありません。メーリング リストや組織外の電子メールアドレスなど、どのようなアドレスでも追加できます。そのため、選択したレポートのデータを受け取るべきでない相手を追加してしまわないように注意してください。

7. ウィザードの手順 4 では、レポートの送信頻度をスケジューリングします。頻度には、[日次（日に 1 回）（Daily (once a day)）] 、[週次（週に 1 回）（Weekly (once a week)）] 、[月次（月に 1 回）（Monthly (once a month)）] を設定できます。
   頻度に日次を指定した場合は、予定日の前日のデータか、スケジューリングされたレポートの送信時間から 24 時間前のデータのいずれかになります。



頻度に週次を指定した場合は、スケジューリングされたレポートを送信する予定日の前の週のデータか、直近 7 日前のデータのいずれかになります。送信時刻は、ログインしたユーザの Umbrella のタイム ゾーンがデフォルトになります。ただし、受信者が異なるタイム ゾーンにいる場合は、受信者の勤務時間帯にレポートが送信されるように設定することができます。受信者が管理者やヘルプデスク スタッフで、レポート内の情報に応じて行動することが期待されている場合は、それぞれの地域に合わせて、2 回目のレポート送信時刻を設定することが推奨されます。

注：スケジューリングされたレポートを当日の時刻に設定しようとした場合、当日の現在時刻よりもあとに設定しているかどうかに関わらず、スケジュール レポートは翌日以降の最も近いタイミングに、週次や月次でスケジュールされます。

8. ウィザードの手順 5 では、レポートの分かりやすい説明を設定するか、自動生成の名前を選択するかが求められます。レポートの目的や適用範囲、適用されるアイデンティティ フィルタの簡単な説明などを追加することが推奨されます。

9. [保存（Save）] をクリックしてウィザードを終了し、スケジューリングされたレポートを確定します。

スケジューリングされたレポートのレビューおよび削除

レポートを保存すると、レポートの概要が表示されます。

レポートの任意の場所をクリックすると、ウィザードに戻ります。[詳細（Details）] には、レポートの作成者、作成日時、最終変更日時と変更したユーザに関する情報が含まれます。設定されている次回の送信スケジュールについても、ここに表示されます。送信スケジュールを過ぎてもレポートが送信されない場合には、ローカルでホストされている、またはクラウドでホストされているメール サーバ ゲートウェイのスパム フィルタを確認してください。電子メールが隔離されている可能性があります。

変更する場合は、ウィザードに戻り、各項目を変更してください。

レポートを削除するには、右下隅にある [削除（Delete）] をクリックします。

レポートのエクスポート、共有、ブックマーク > **スケジューリングされたレポート：概要および設定** > セキュリティの概要レポート

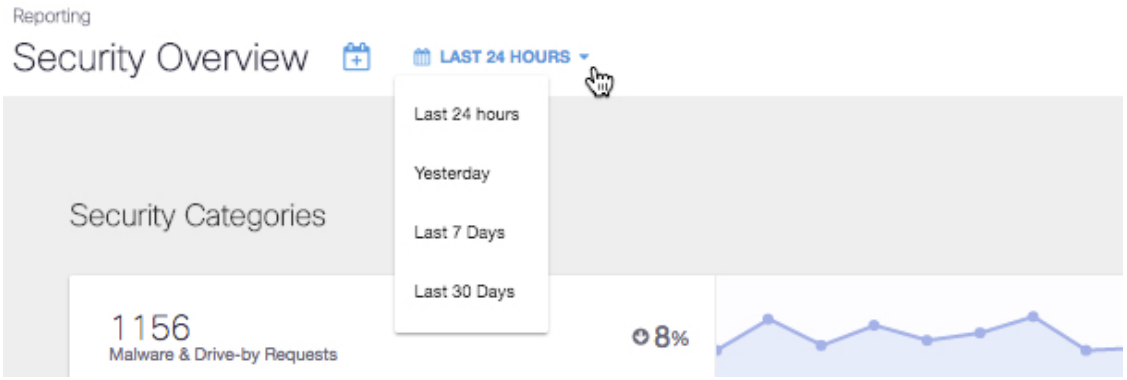
セキュリティの概要レポート

セキュリティの概要レポートにより、詳細なレポートを精査する前に、環境に関する総合的なスナップショットを確認できます。一括管理によるレポートを通じて、全体像がより適切に把握できるようにします。レポート自体が、特に説明の不要なデザインになっていますが、このドキュメントでは、レポートの各機能について説明します。
セキュリティの概要レポートにアクセスするには、[レポート（Reports）] > [セキュリティの概要（Security Overview）] に移動します。

セキュリティの概要レポートは、4 つの主要領域から構成されています。

- **セキュリティ カテゴリ**：環境の傾向について、時系列の簡単な概要を示します。
- **上位セキュリティ イベント**：**ドメインごとのイベント**：潜在的なアウトブレイクについての一覧を表示します。
- **上位のセキュリティ イベント**：**アイデンティティごとのイベント**：潜在的な感染ホストについての簡単な一覧を表示します。
- **導入の概要**：Umbrella のセキュリティ ソフトウェアの導入状況についての概要を示します。

いずれのレポートも、一定の期間内の情報を表示します。カレンダー アイコンの横にある時間をクリックすることで、過去 24 時間、カレンダーの前日（昨日）、過去 7 日間、先月の時間枠でレポートを実行することができます。

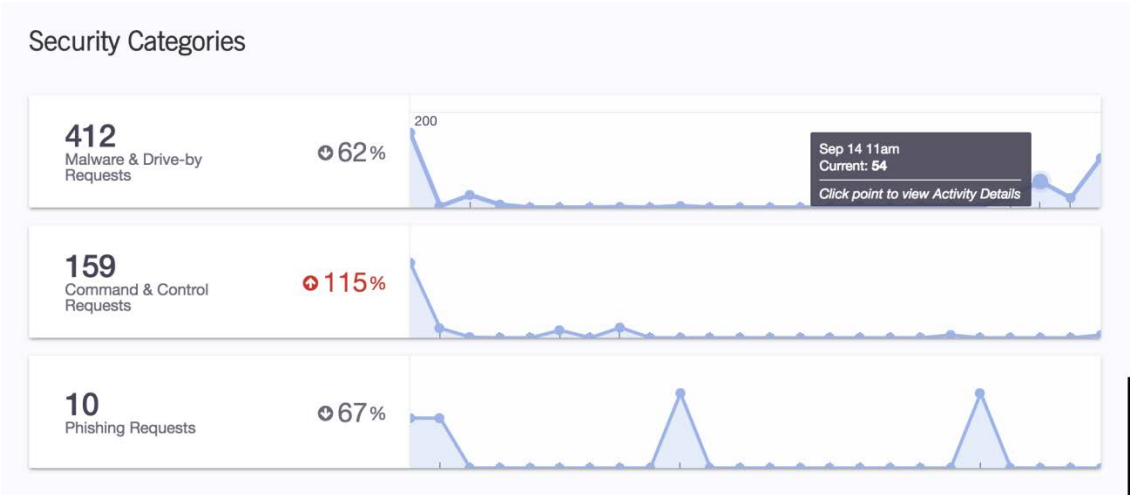


ヒント

すべてではありませんが、ほとんどの Umbrella のレポートは、時刻に大きく関係しています。デフォルトの時刻は UTC ですが、ユーザ単位で別のタイムゾーンに変更ができます。[設定（Settings）] > [アカウント（Accounts）] に移動し、アカウントの時刻設定を更新します。

セキュリティの概要：セキュリティ カテゴリ

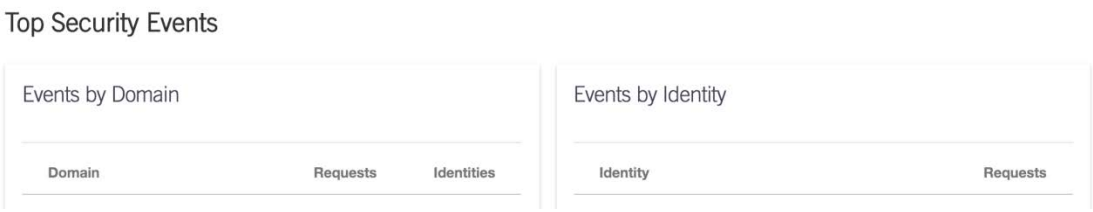
レポートのセキュリティ カテゴリの項目では、防止（マルウェアおよびドライブ バイ ダウンロード）、封じ込め（ボットネット コマンド アンド コントロール要求）、フィッシングのグループごとにまとめられた主要なセキュリティ カテゴリの結果が表示されます。グラフの上にカーソルを合わせると、特定の期間の詳細が強調表示されます。



上位のセキュリティ イベント

上位のセキュリティ イベントは、ドメインごとの上位イベントとアイデンティティごとの上位イベントの 2 つの領域に分割されています。

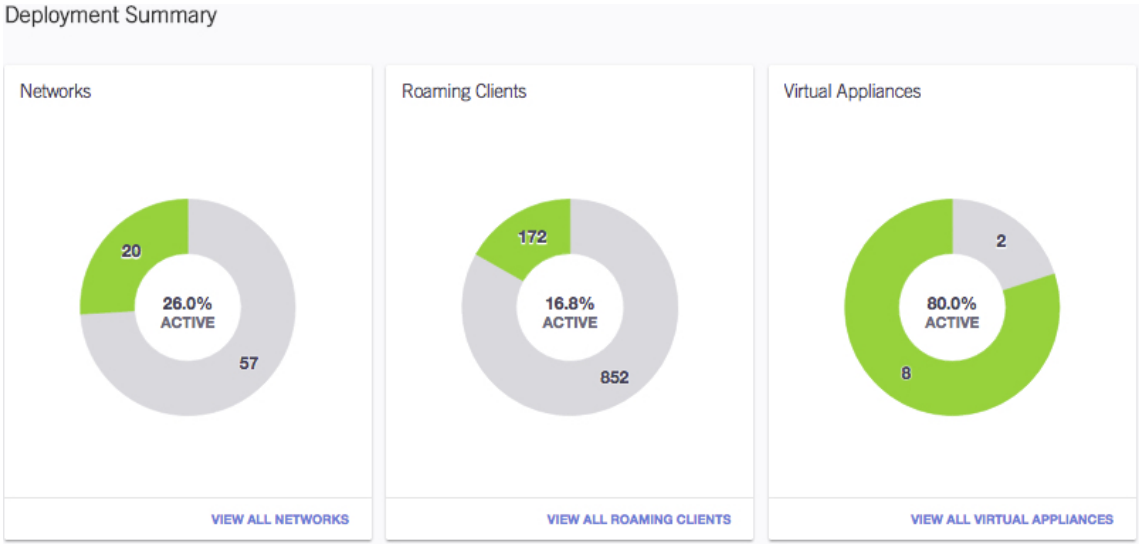
また、上位のイベントのドメインを要求するアイデンティティの数についても記録されています。このレポートから直接実行できるアクションはありませんが、このレポートをベースラインの確立に使用することが推奨されます。時系列で見る場合、たとえば、ネットワークなどの頻繁に動作するアイデンティティが常にほぼ上位に位置しており、これは通常の傾向ですが、ローミング クライアントが単一のドメインに多数のコールアウトを行っていることが示される場合などは異常な傾向と判断することができ、これは実用的なものとなります。



イベント リストの最後では、上位ドメインや上位アイデンティティについてのレポートをより詳細に確認することができます。

導入の概要

レポートの導入の概要に関する項目では、ネットワーク、ローミング クライアント、仮想アプライアンスのチャートにより、それぞれのタイプのアイデンティティが現在、どの程度オンラインおよびアクティブになっているかすぐに確認できます。それぞれのレポートの中でグリーンのステータスになっている部分は「アクティブ」であることを示しています。詳細を確認するには、[すべての [アイデンティティ タイプ] を表示（View All [Identity Type] ）] をクリックします。



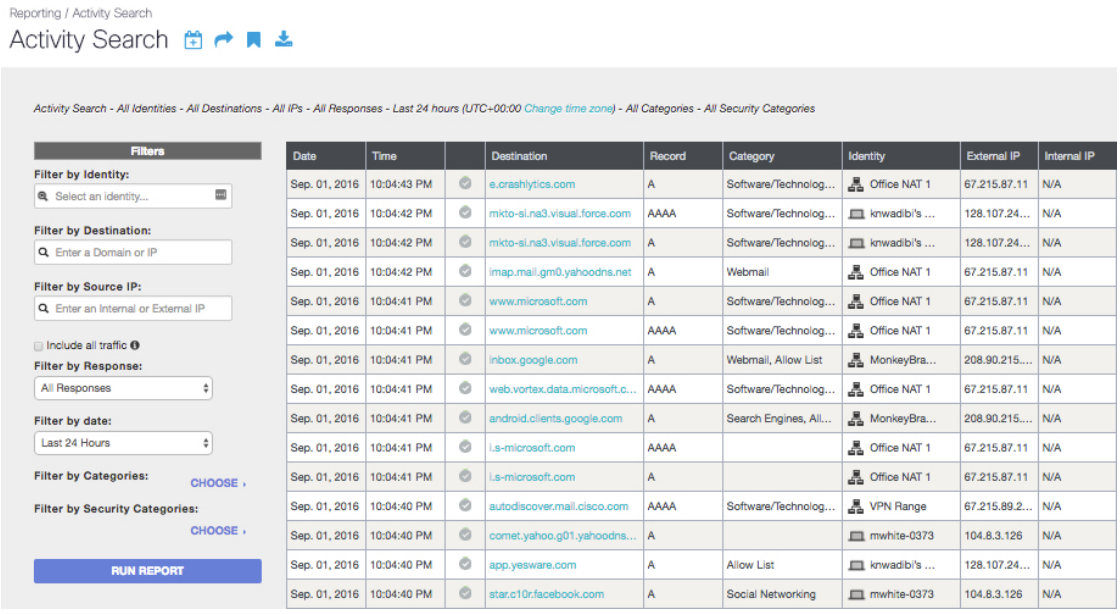
[スケジューリングされたレポート：概要および設定](#) > **セキュリティの概要レポート** > [アクティビティ検索レポート](#)

アクティビティ検索レポート

アクティビティ検索レポートでは、プロビジョニング済みのさまざまなアイデンティティから送信されたすべての DNS 要求の結果を、日時順に確認することができます。このレポートは、複数の中核的な機能の中でも基本となるレポートです。たとえば、他のレポートのデータが正しく表示されているかを確認したりできます。アイデンティティの列からは、どのアイデンティティからのレポートかを確認できます。それに基づいて、他のレポートでどのアイデンティティが表示され、どのようなことが表示されるかを予測できます。

[レポート（Reporting）] > [アクティビティ検索（Activity Search）] に移動します。

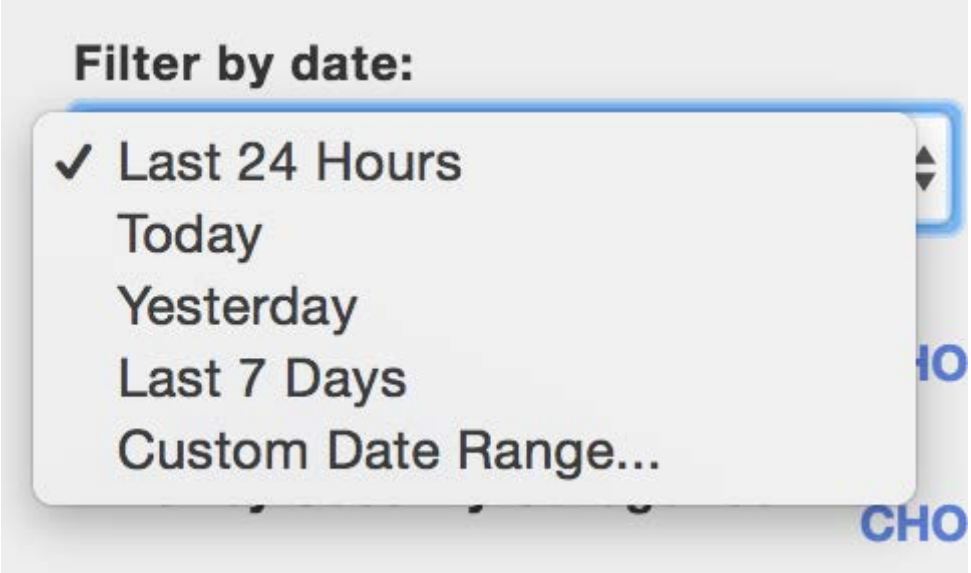
精度を向上させるために Umbrella VA を使用している場合、アクティビティ検索バーには、応答も表示されます。応答には、許可/ブロック、プロキシ、接続先リストによる許可/ブロック、DNS クエリを実行したアイデンティティ、要求を行った外部 IP、その要求の接続先となる内部 IP が含まれます。



アクティビティ検索の場合は、レポートのデータ量が大きいことから、*過去 28 日分のみがレポートされます*。

28 日より長い期間のデータを保存するには、ログのエクスポート機能と、Amazon S3 にデータを保存する機能について参照してください。

検索には、選択した期間内の Umbrella 内のすべてのアクティビティが反映されます。



これらの結果は、Umbrella のアイデンティティでフィルタできます。レポートしたいアイデンティティ名を入力し、[レポートの実行（Run Report）] をクリックします。

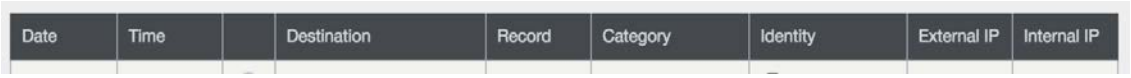
ドメインのフィルタには、「domain.com」を設定します。つまり、Google からの結果を検索するには、「google.com」と指定します。さらに精度をあげたい場合は、たとえば、mail.google.com などのようにサブドメインを追加します。

ワイルドカードは、このフィルタには適用されません。

許可とブロックの両方、または許可とブロックのどちらかなど、正しい種類の DNS 応答が選択されていることを確認し、[レポートの実行（Run Report）] をクリックします。

不明な要求がなにか、いつレポートが実行されたか、いつ Active Directory 用の詳細情報が設定されたかが不明な場合は、こちらをクリックしてください。

アクティビティ検索には、次の情報が含まれます。



- **レコード**は、DNS のレコード タイプです（例：A、AAAA、MX など）。
- **カテゴリ**は、セキュリティ、コンテンツに関わりなく、接続先が分類されたカテゴリです。

セキュリティの概要レポート > **アクティビティ検索レポート** > セキュリティ アクティビティ レポート

セキュリティ アクティビティ レポート

セキュリティ アクティビティ レポート([レポート(Reporting)] > [セキュリティ アクティビティ(Security Activity)])は、ポリシー用に設定されたセキュリティ カテゴリに対してトリガーされたイベントがある Umbrella のアイデンティティをハイライトするために設計されています。

セキュリティ アクティビティは、マルウェアをホストするサイトやフィッシング サイトへのアクセス試行や、ローカル ネットワーク上の感染マシンにおけるボットネット アクティビティなどを指します。

セキュリティ アクティビティ レポートを選択すると、セキュリティ カテゴリに基づいてフィルタできます。フィルタを行うには、左側のサイドバーの下から、[フィルタ(Filters)] > [セキュリティ カテゴリによるフィルタ(Filter by Security Categories)] > [セキュリティカテゴリの選択(Choose Security Categories)] を選択します。

完了すると、ポップアップが展開され、選択可能なオプションが表示されます。

カテゴリを選択すると、カテゴリがフィルタの下に表示されます。

ヒント:リストのカテゴリをクリックするだけで、リストからカテゴリを削除することができます。

レポートの対象とするカテゴリ、期間、希望するアイデンティティ フィルタやネットワーク フィルタを選択したあと、[レポートの実行（Run Report）] をクリックします。

1. [日付によるフィルタ（Filter by date）] では、レポートでアクティビティをフィルタする期間を選択します。
2. [フィルタ（Filters）] > [セキュリティ カテゴリによるフィルタ（Filter by Security Categories）] で、[選択（Choose）] をクリックします。
3. フィルタしたいセキュリティ カテゴリを確認します。
4. カテゴリを選択すると、Umbrella の [セキュリティ カテゴリによるフィルタ（Filter by Security Categories）] にカテゴリがリストされます。
5. [レポートの実行（Run Report）] をクリックします。

アクティビティ検索レポート > **セキュリティ アクティビティ レポート** > 接続先レポート

接続先レポート

接続先レポートにより、アイデンティティがアクセスした接続先に関する情報を確認できます。それにより、最もアクティブな要求や、特定のアクティビティがいつ発生したかを判断できます。このレポートでは、指定期間中にアクセスされたすべての接続先がリストされます。[接続先（Destination）] ページでは、特定の接続先に関する情報を表示して、アクティビティをドメイン レベルで調べることができます。選択したドメインに誰がいつアクセスしていたを確認できます。この情報により、コンピュータやネットワークが侵害されていたり、既知の悪意のあるサイトに接続したりしていないかを判断できます。その結果、自身や他のユーザをより適切に保護することができます。

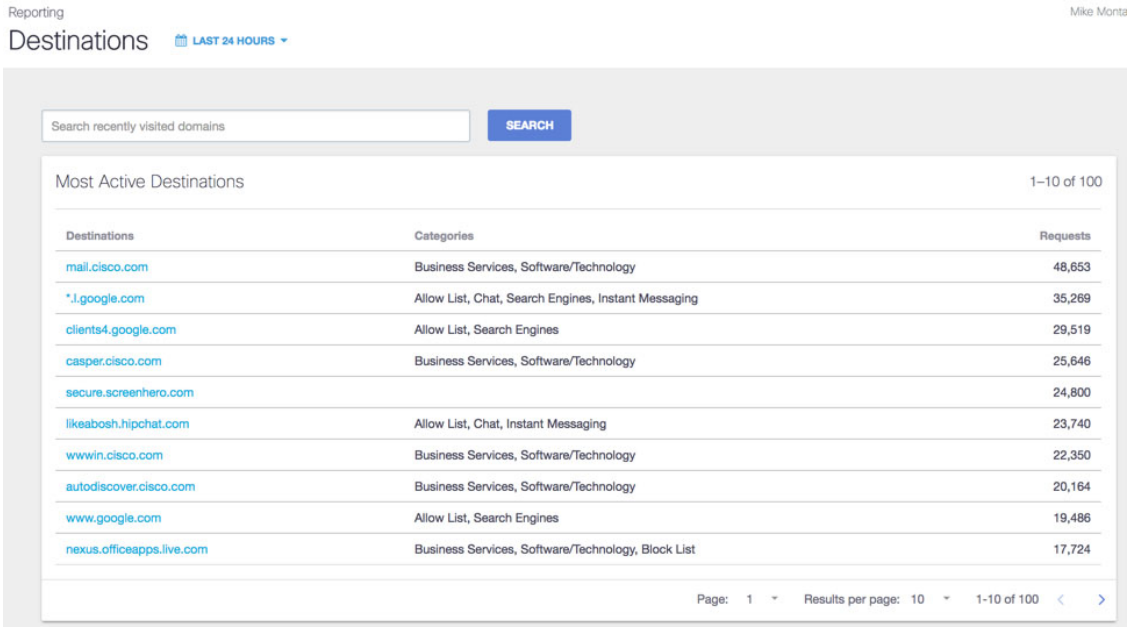
注：接続先レポートは、セキュリティ インサイト レポートの代わりとなるレポートです。セキュリティ インサイト レポートに含まれていた情報は、現在、接続先レポートに含まれています。接続先レポートには、ドメインをレビュー用に送信する機能が含まれており、ダッシュボードから [調査（Investigate）] に移動できます。

このレポートが利用できるのは、Umbrella Insights もしくは Platform のパッケージを使用するお客様か、MSP や MSP のお客様のみです。パッケージのアップグレードの詳細については、Cisco Umbrella の担当者までお問い合わせください。

接続先レポートへのアクセス

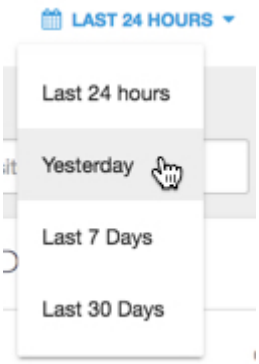
[レポーティング（Reporting）] > [接続先（Destinations）] の順に選択します。

上位レベルの接続先レポート ページが表示され、指定期間内でのシステムのすべての接続先アクティビティが表示されます。デフォルトは 24 時間です。

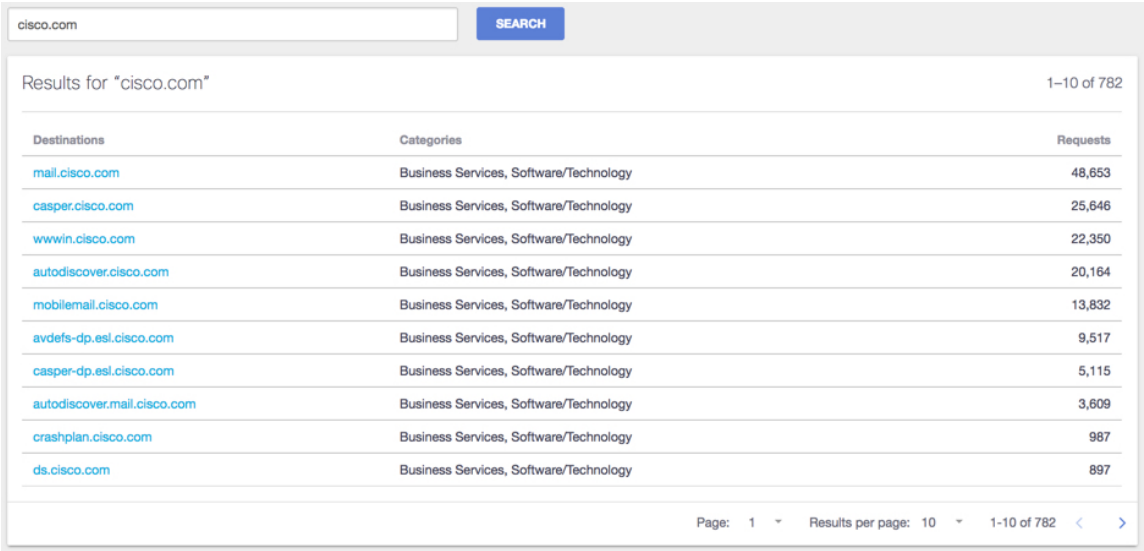


この上位レベルの接続先レポートでは、指定期間内で要求された上位 100 の接続先がリストされます。特定の接続先についてリストを検索して、要求された接続先のドメイン レベルでの詳細なアクティビティ情報を調べることができます。これにより、インシデント対応のワークフローがシンプルになり、問題が検出された場合の修復の時間が短縮できます。接続先の要求元とその時刻を特定することができるため、セキュリティ リスクに対して、適切に対応することができます。

他の Umbrella のレポートと同様に、この接続先レポートも時刻に関連しています。アクティビティをドキュメント化するためのレポートは、過去 24 時間、カレンダーの前日（昨日）、過去 7 日間、先月の期間で生成できます。



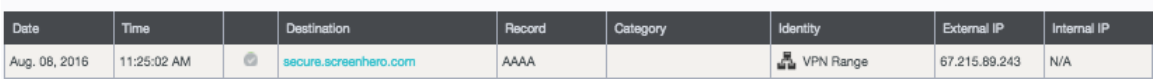
接続先を検索すると、Umbrella は関連するすべてのドメインとサブドメインを返します。下の例では、過去 24 時間以内の cisco.com へのすべての要求を検索しました。検索を実行すると、Umbrella は、各接続先への要求数を返します。これには一致するすべてのサブドメインも含まれます。cisco.com については、この検索で 782 のサブドメインが返され、過去 24 時間内に最も頻繁に要求されたドメインは、mail.cisco.com でした。



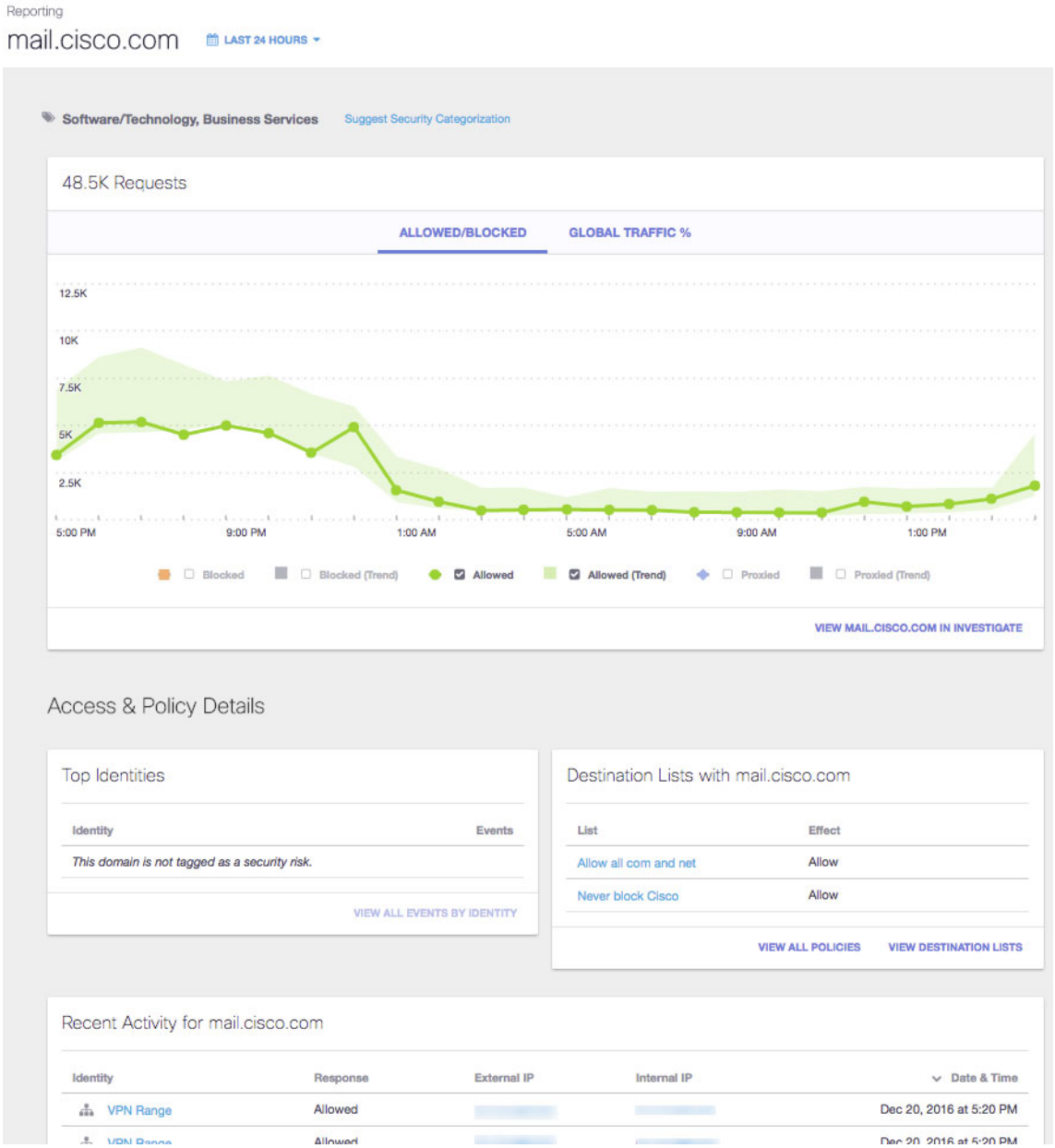
特定の接続先の詳細にアクセスするには、接続先をクリックします。Umbrella により、その接続先の [接続先（Destinations）] レポート ページに移動されます。

また、アクティビティ検索、セキュリティ アクティビティ レポート、上位接続先レポートを通じて、特定の接続先レポートにアクセスすることもできます。

[レポート（Reporting）] > [アクティビティ検索（Activity Search）] または [レポート（Reporting）] > [セキュリティ アクティビティ（Security Activity）] をクリックして、フィルタによって接続先を検索し、接続先（青色で強調表示）をクリックします。



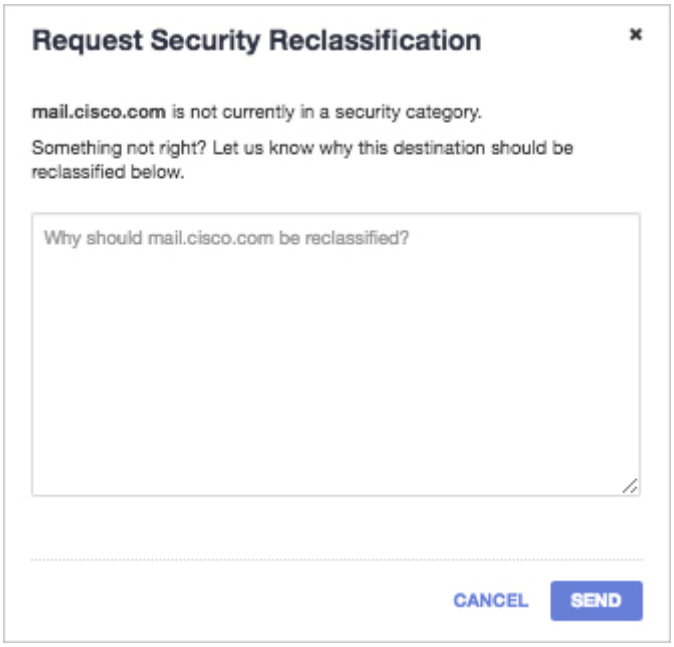
特定の接続先の [接続先（Destinations）] ページでは、その接続先のアクティビティがチャートで表示されます。このレポートは 3 つの領域に分割され、接続先やその要求を行ったネットワーク上のアイデンティティに関する重要な情報を確認するのに役立ちます。



注：接続先レポートのスケジューリングや、レポートのダウンロードができない点についてお気づきかも知れません。これは、このレポートの情報が、テキストではなくグラフにより表示されるためです。これらの機能をレポートに追加したい場合は、電子メールにて要望をお伝えください：umbrella-support@cisco.com。

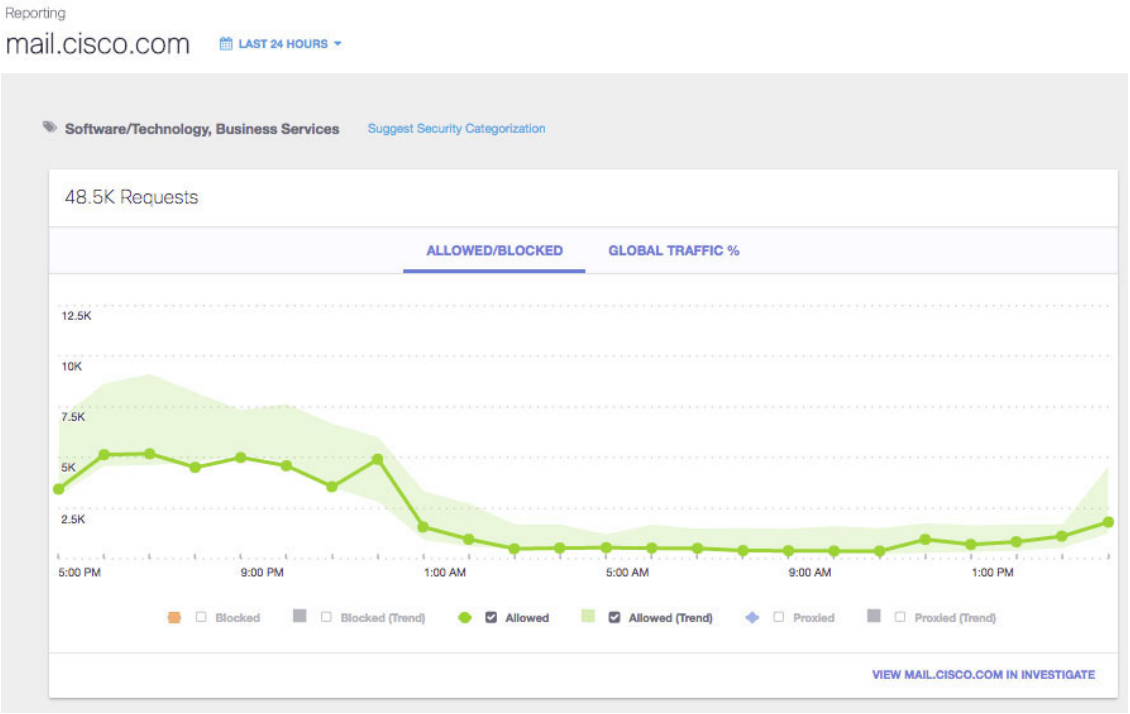
許可/ブロックおよびグローバル トラフィックの割合に関するチャート

許可/ブロックおよびグローバル トラフィックの割合に関するチャートにより、選択した接続先の指定期間内における DNS アクティビティを表示することができます。DNS のアクティビティを可視化することで、その接続先に対する要求のピークやアクティブだった時間帯について、すぐに確認することができます。これは、疑いのあるアクティビティの調査に役立ちます。レポートのページの上部には、セキュリティ カテゴリのリストが表示されます。カテゴリの分け方に異論がある場合は、[セキュリティのカテゴリ分けを提案する（Suggest Security Categorization）] をクリックし、カテゴリの変更要求を送ります。[送信（Send）] をクリックすることで、Umbrella の内部チケットが作成され、セキュリティ研究者にドメインのカテゴリのレビューを依頼することができます。すぐに回答を受け取ることができます。

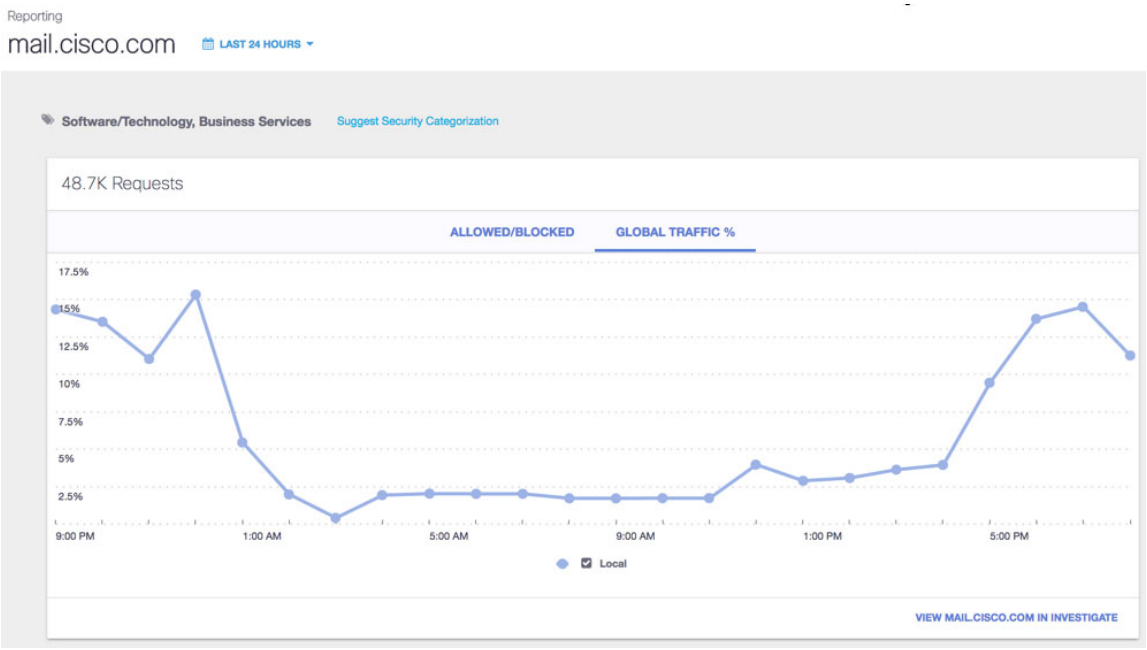


許可/ブロックのチャートでは、指定期間内を対象にして、調査対象の接続先への許可/ブロックされたアクセスの数を表示します。さまざまなアクティビティが比較できるように、複数の線グラフのオン/オフを切り替えて、グラフを重ね合わせて素早く比較できます。

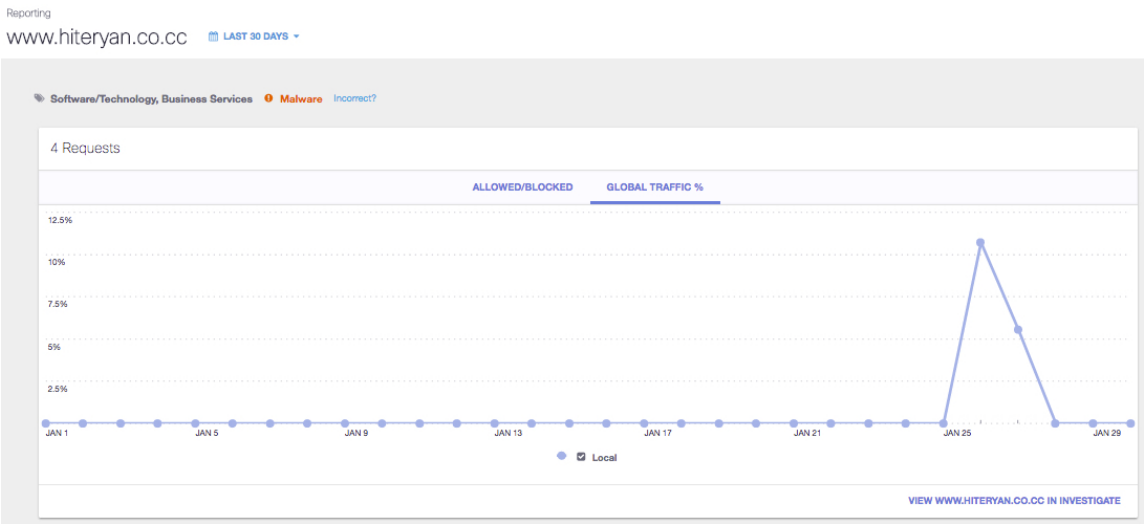
[調査対象の <接続先> を表示（View <destination> in Investigate）] をクリックして、調査対象の接続先を開き、その接続先の詳細について確認します。



グローバル トラフィックの割合のチャートには、接続先へのグローバル トラフィックの割合が表示されます。チャートは、組織の各アイデンティティからのトラフィックで構成されます。

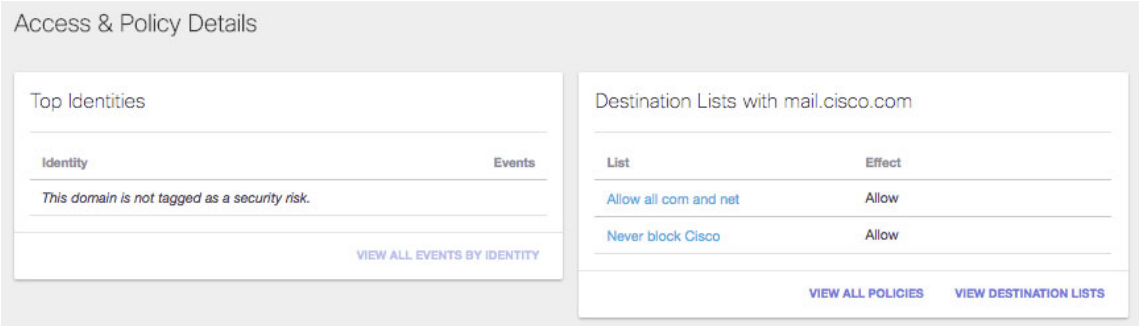


このアクティビティを確認することで、接続先へのローカル トラフィックが不自然に急増していないかモニタすることができるようになります。そのようなトラフィックの急増が意味するのは、スピア フィッシングやその他の標的型攻撃などのセキュリティ リスクであり、さらに調査が必要です。次の例では、1 月 25 日のトラフィックに不自然な急増があり、調査すべきであることがみてとれます。組織内のユーザがフィッシング メールのリンクをクリックした可能性があります。



アクセスとポリシーの詳細

[アクセスとポリシーの詳細（Access & Policy Details）] の領域は、[上位アイデンティティ（Top Identities）] と [<接続先> を含む接続先リスト（Destination lists with <destination>）] に分割されています。ここに表示される情報により、接続先がカスタム接続先リストに含まれているかを把握でき、その接続先の許可またはブロックにその他のポリシーが影響を与えているかを判断できます。



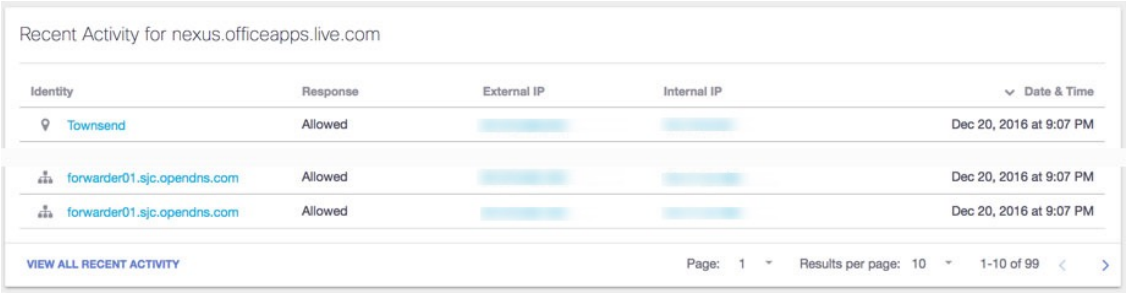
「上位アンデンティティ」には、特定のドメインを参照したアイデンティティがすべてリストされます。「<接続先> を含む接続先リスト」には、調査対象の接続先を含むすべての接続先リストがリスト表示されます。リストをクリックすると、[接続先リスト（Destination Lists）] ページ（[ポリシー（Policies）] > [接続先リスト（Destination Lists）] ）が表示され、選択した接続先リストに含まれる接続先が表示されます。このページから、必要に応じて接続先の状態を許可/ブロックに変更して、接続先リストを更新することができます。

すべてのポリシーを表示させて、[接続先（Destinations）] ページに表示される情報を元に、更新が必要かどうかを判断できます。
[すべてのポリシーを表示（View All Policies）] をクリックします。Umbrella の [ポリシー リスト（Policy List）] ページ（[ポリシー（Policies）] > [ポリシー リスト（Policy List）] ）が表示されます。

また、接続先リストもすべて確認できます。
[接続先リストを表示（View Destination Lists）] をクリックします。Umbrella の [接続先リスト（Destination Lists）] ページ（[ポリシー（Policies）] > [接続先リスト（Destination Lists）] ）が表示されます。

最近のアクティビティ

最近のアクティビティの領域では、接続先の DNS アクティビティについて調査することができます。接続先を要求したアイデンティティ、要求への応答（許可/ブロック）、要求の発生元の IP アドレスについて、すぐに確認することができます。これらの情報を確認することで、接続先リストを管理する方法を決定できます。たとえば、悪意のあるサイトへのアクセスがブロックされておらず、アイデンティティがリスクにさらされていないかどうか、アクセスできなければならないドメインがブロックされていないかどうか、などを確認します。また、これらの情報は、アイデンティティの DNS アクティビティのモニタに使用することもできます。たとえば、あるアイデンティティがどこにアクセスしようとしているか確認したり、そのアイデンティティのアクセスを許可またはブロックするために、接続先リストを更新すべきかを判断できます。



[すべての最近のアクティビティを表示（View All Recent Activity）] をクリックし、[アクティビティ検索（Activity Search）] ページ（[レポート（Reporting）] > [アクティビティ検索（Activity Search）] ）に移動します。選択した接続先のアクティビティがすぐに表示されます。

セキュリティ アクティビティ レポート > **接続先レポート** > アイデンティティ レポート

アイデンティティ レポート

アイデンティティ レポートにより、アイデンティティのアクティビティの情報にアクセスできるようになります。最もアクティブなアイデンティティや、各アイデンティティのアクセス先などを判別できます。このレポートでは、指定期間中でアクティブになっていたすべてのアイデンティティがリストされます。[アイデンティティ（Identities）] ページでは、特定のアイデンティティの情報にアクセスして、そのアクティビティの詳細についてドメイン レベルで調査できます。セキュリティ脅威を示すアクティビティがあった場合に、どのサイトにアクセスしていたかを確認できます。この情報により、アイデンティティがブロックすべきサイトにアクセスしていたかどうかが分かります。

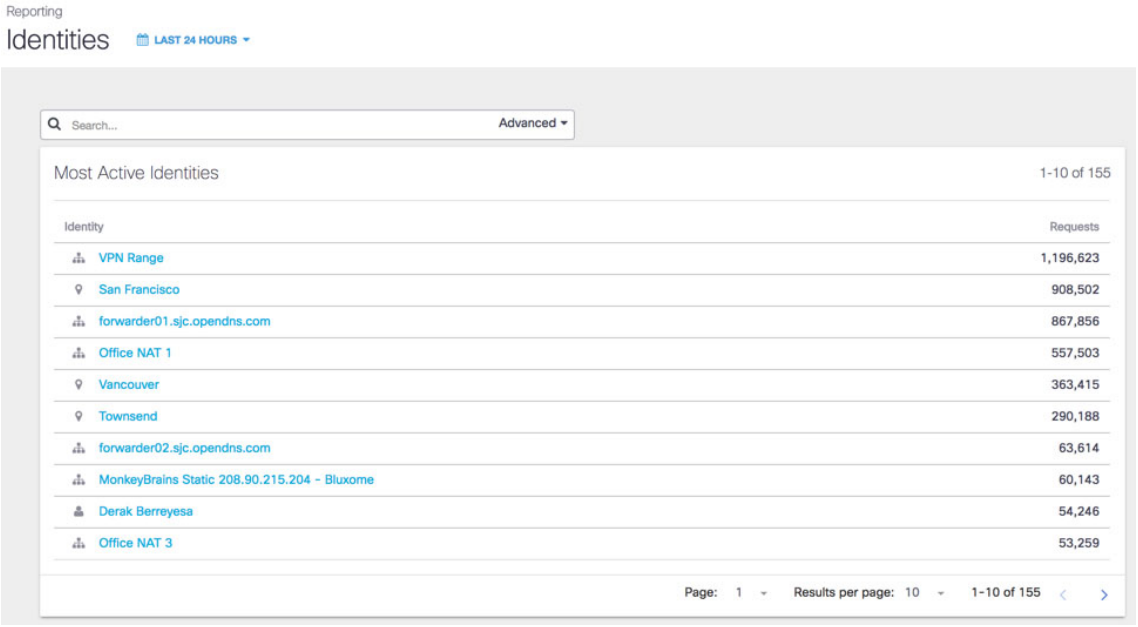
注: アイデンティティ レポートは、セキュリティ インサイト レポートの代わりとなるレポートです。セキュリティ インサイト レポートに含まれていた情報は、現在、アイデンティティ レポートに含まれています。

このレポートが利用できるのは、Umbrella Insights もしくは Platform のパッケージを使用するお客様か、MSP や MSP のお客様のみです。パッケージのアップグレードの詳細については、Cisco Umbrella の担当者までお問い合わせください。

アイデンティティ レポートへのアクセス

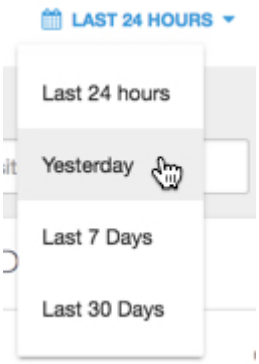
[レポーティング（Reporting）] > [アイデンティティ（Identities）] の順に選択します。

上位レベルのアイデンティティ レポート ページが表示され、指定期間内でのシステムのすべてのアイデンティティのアクティビティが表示されます。デフォルトは 24 時間です。



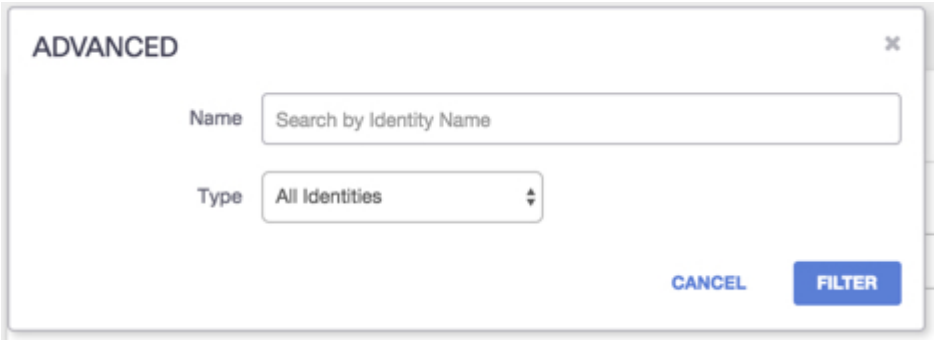
この上位レベルのアイデンティティ レポートには、指定期間内でアクティブだったアイデンティティがリストされます。特定のアイデンティティについてリストを検索して、要求されたアイデンティティのドメイン レベルでの詳細なアクティビティ情報を調べることができます。これにより、インシデント対応のワークフローがシンプルになり、問題が検出された場合の修復の時間が短縮できます。接続先の要求元とその時刻を特定することができるため、セキュリティ リスクに対して、適切に対応することができます。

他の Umbrella のレポートと同様に、このアイデンティティ レポートも時刻に関連しています。アクティビティをドキュメント化するためのレポートは、過去 24 時間、カレンダーの前日（昨日）、過去 7 日間、先月の期間で生成できます。

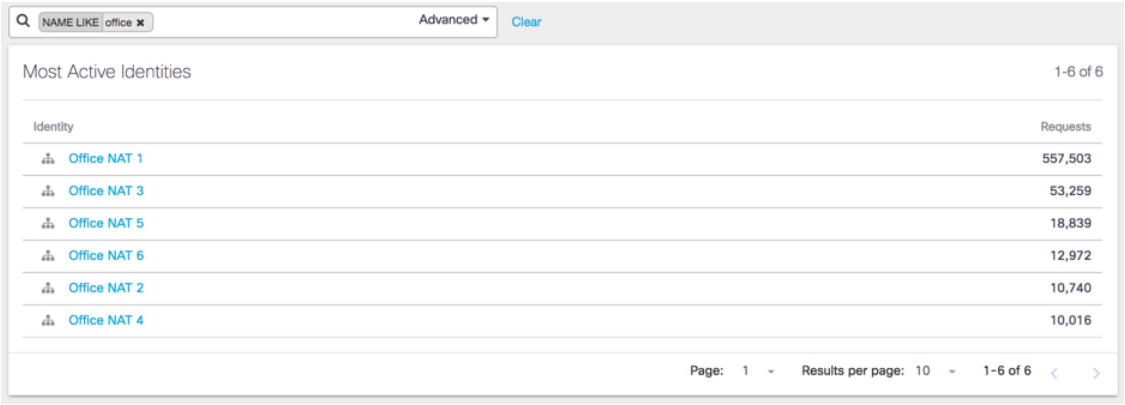


アイデンティティを検索すると、検索バーの入力内容に応じて、関連するすべてのアイデンティティが動的にリストされます。結果のリストからアイデンティティを選択するか、[<名前> に関連するすべての結果（All results with a name like: <name>）] を選択できます。

また、詳細な検索も実行できます。検索バーの [詳細（Advanced）] をクリックすると、[詳細（Advanced）] のポップアップ ウィンドウが開きます。

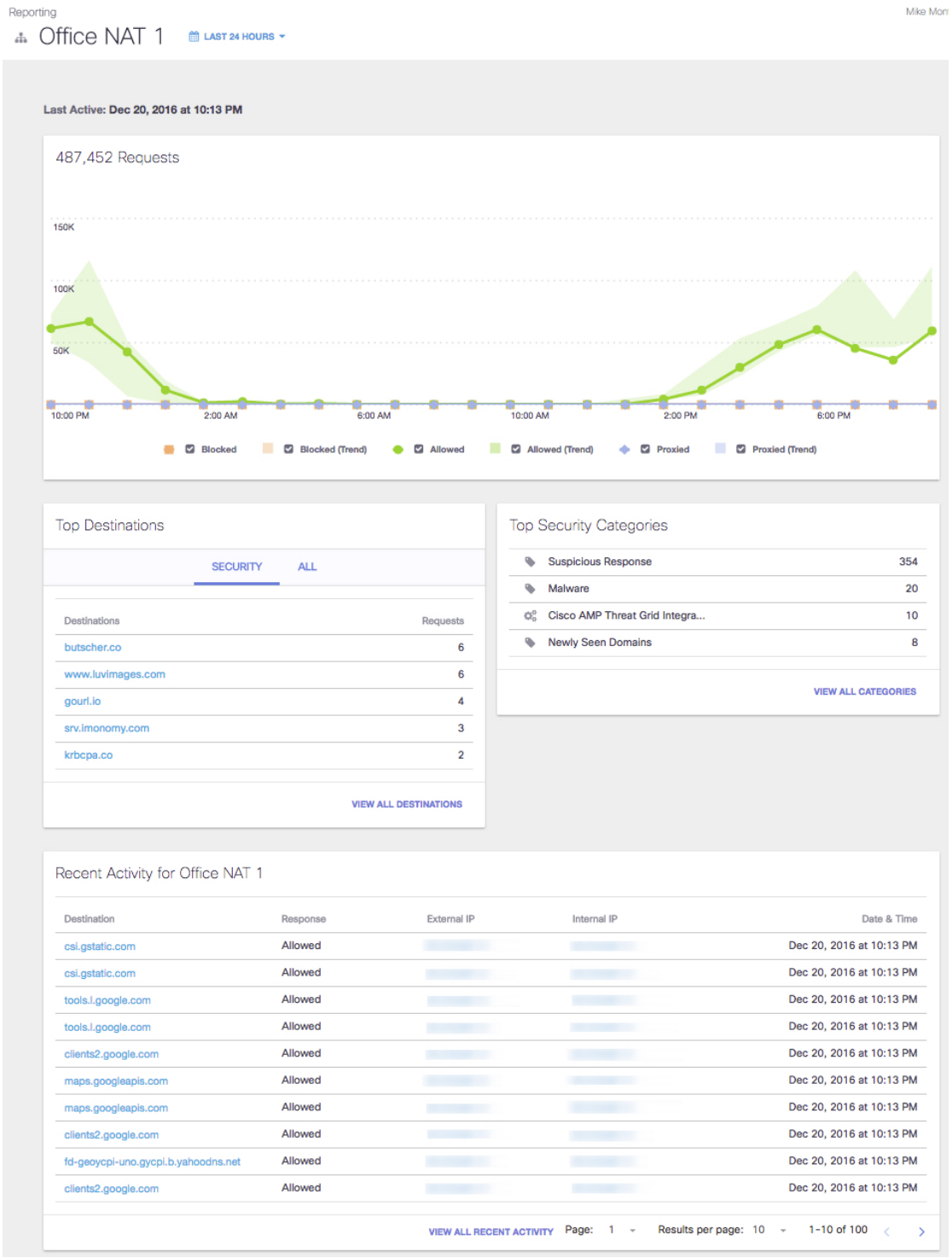


アイデンティティ名、アイデンティティのタイプ、もしくはその両方で検索できます。これにより、検索結果を絞り込むことができます。たとえば、同じタイプのアイデンティティをすべて表示させたい場合や、同じ名前のアイデンティティが複数ある場合に便利です。アイデンティティの検索の際、その結果は選択した検索パラメータの種類により異なります。Umbrella は、選択したアイデンティティのみを返すか、関連するアイデンティティのすべてを返します。次の例では、過去 24 時間でアクティブだったアイデンティティのうち、office という名前を持つアイデンティティをすべて検索しています。Umbrella は関連するアイデンティティを返す際に、実行された要求数もアイデンティティごとに返します。office で検索した場合、7 つのアイデンティティが返され、過去 24 時間では、Office Nat 1 が最もアクティブでした。



特定のアイデンティティの詳細にアクセスするには、アイデンティティをクリックします。Umbrella により、そのアイデンティティの [アイデンティティ（Identities）] レポートページに移動されます。

[アイデンティティ（Identities）] ページでは、指定した期間内のアイデンティティのアクティビティがグラフ化されます。このレポートは 3 つの領域に分割され、ネットワーク上のアイデンティティのアクティビティに関する重要な情報を確認するのに役立ちます。

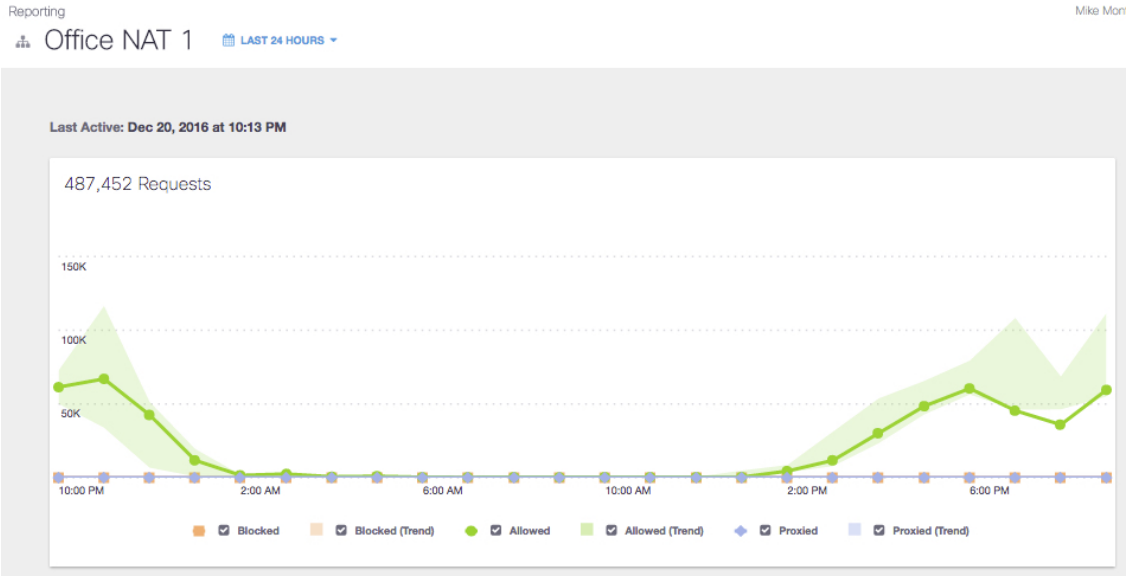


注：アイデンティティのレポートのスケジューリングや、レポートのダウンロードができない点についてお気づきかも知れません。これは、このレポートの情報が、テキストではなくグラフにより表示されるためです。これらの機能をレポートに追加したい場合は、電子メールにて要望をお伝えください：umbrella-support@cisco.com。

アクティビティ チャート

アクティビティ チャートでは、選択したアイデンティティの指定期間の DNS アクティビティが、グラフ化されて表示されます。DNS アクティビティの可視化により、そのアイデンティティによって行われた要求アクティビティのピークの時間帯と減少している時間帯をすぐに確認できます。これは、疑いのあるアクティビティの調査に役立ちます。レポートのページの上部には、そのアイデンティティが指定期間内に行った要求数のリストが表示されます。

さまざまなアクティビティが比較できるように、複数の線グラフのオン/オフを切り替えて、グラフを重ね合わせて素早く比較できます。



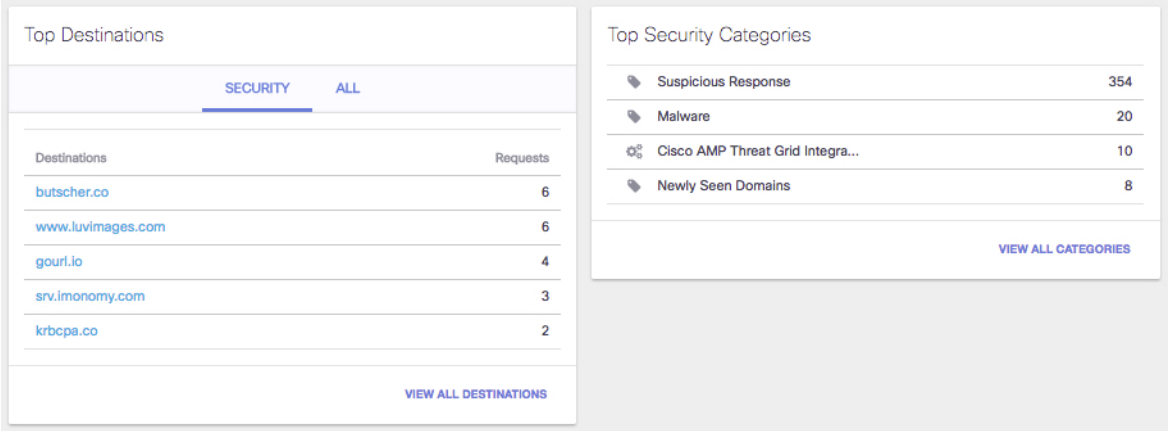
セキュリティの詳細

セキュリティの詳細の領域は、「上位の接続先」と「上位セキュリティ カテゴリ」に分割されています。ここに表示される情報により、調査対象のアイデンティティのアクティビティにリスクがあるかを把握でき、接続先リストで許可すべきかブロックすべきかを判断できます。

[上位の接続先（Top Destinations）] では、マルウェアやフィッシング サイトなどのセキュリティ リスクとなる接続先にアイデンティティが行った要求がリストされます。また、[すべて（All）] タブを選択することで、そのアイデンティティの上位の接続先をすべて確認することができます。

[上位のセキュリティ カテゴリ（Top Security Categories）] では、悪意のある接続先へのアクセス要求が原因で発生したセキュリティ脅威の種類がリストされます。

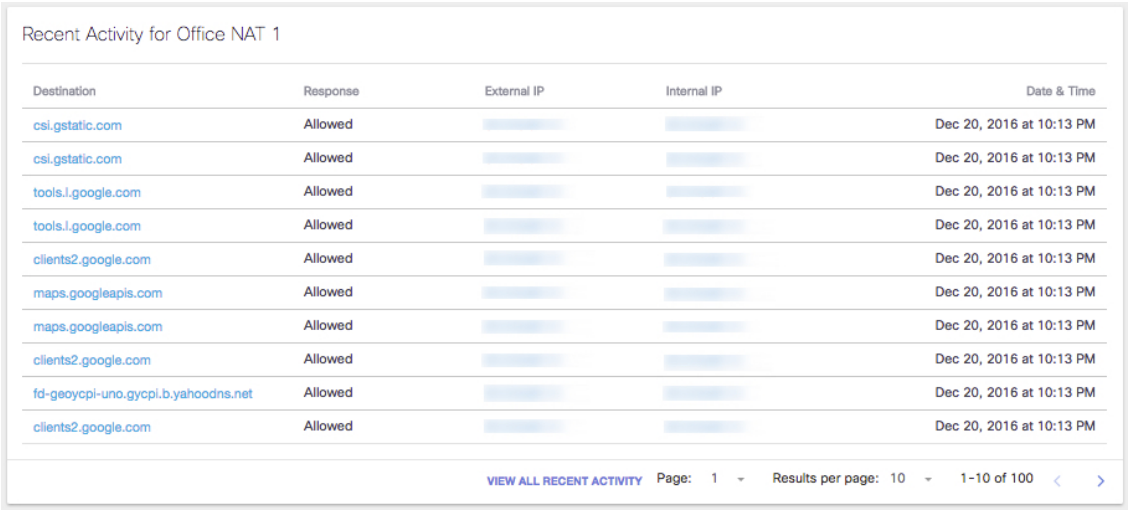
組織のすべての接続先とカテゴリを確認することができ、必要に応じて、更新することもできます。
[すべての接続先を表示（View All Destinations）] をクリックします。[レポート（Reporting）] > [上位ドメイン（Top Domains）] ページが表示されます。
[すべてのカテゴリを表示（View All Categories）] をクリックします。[レポート（Reporting）] > [上位カテゴリ（Top Categories）] ページが表示されます。



最近のアクティビティ

最近のアクティビティの領域では、アイデンティティの DNS アクティビティについて調査することができます。アイデンティティによって要求された接続先、要求への応答（許可/ブロック）、要求の発生元の IP について、すぐに確認することができます。これらの情報を確認することで、接続先リストを管理する方法を決定できます。たとえば、悪意のあるサイトへのアクセスがブロックされておらず、アイデンティティがリスクにさらされていないかどうか、アクセスできなければならないドメインがブロックされていないかどうか、などを確認します。また、これらの情報は、アイデンティティの DNS アクティビティのモニタに使用することもできます。たとえば、あるアイデンティティがどこに

アクセスしようとしているか確認したり、そのアイデンティティのアクセスを許可またはブロックするために、接続先リストを更新すべきかを判断できます。



[すべての最近のアクティビティを表示（View All Recent Activity）] をクリックし、[アクティビティ検索（Activity Search）] ページ（[レポート（Reporting）] > [アクティビティ検索（Activity Search）] ）に移動します。選択した接続先のアイデンティティがすぐに表示されます。

接続先レポート > **アイデンティティ レポート** > クラウド サービス レポート

クラウド サービス レポート

Umbrella のクラウド サービス レポートにより、組織全体で使用されているクラウド サービスを把握したり、使用パターンを特定したり、シャドー IT を発見することができます。組織内のユーザがクラウド サービスを使用している場合、シャドー IT となっているクラウド サービスを特定することが、管理者にとって日常的な懸念事項となっています。特に、データの損失や情報の抑制、エンド ユーザにとっての必要性が懸念されます。

シスコのグローバル ネットワークを活用することで、組織がアクセスしているすべてのドメインを確認できます。通常、これらのイベントはアクティビティ検索レポートに記録されます。また、セキュリティ イベントもセキュリティ アクティビティ レポートに記録されます。クラウド サービス レポートでは、蓄積されたクラウド サービスのリストと一致する DNS 要求が示されます。このような独特の観点を用いることで、組織内のユーザがどの程度クラウド サービスを使用しているかをより把握できるようになります。

Umbrella Insights もしくは Umbrella Platform をご利用のお客様には、すでにこのレポートが含まれています。レポートに興味をお持ちで、これらのパッケージを使用していない場合は、担当のアカウント マネージャにご連絡いただくか、umbrella-renewals@cisco.com まで電子メールでお問い合わせください。

本ドキュメントは、レポートを最大限に活用できるように、3 つの主要な項目に分かれています。レポートをすぐに確認したい場合は、[レポート（Reports）] > [クラウド サービス（Cloud Services）] でレポートがすでに利用可能です。あらかじめ有効にする必要はありません。

クラウド サービス レポートの概要

組織内のユーザがクラウド サービスを使用している場合、シャドー IT となっているクラウド サービスを特定することが、管理者にとって日常的な懸念事項となっています。特に、データの損失や情報の抑制、エンド ユーザにとっての必要性が懸念されます。

クラウド サービス レポートにアクセスするには、[レポート（Reporting）] > [クラウド サービス（Cloud Services）] に移動します。クラウド サービスのリストは、下の例のように表示されます。

Name	Classification	Identities	Trend	Requests	Blocked	First S...	Last S...
Facebook	Social Media, Communication	65	↓ 10	134,508	0%	Jun. 25, 2014	Sep. 19, 2016
HipChat	Collaboration	73	↓ 15	132,753	0%	Jun. 18, 2014	Sep. 19, 2016
Gmail	Communication, Cloud Dat...	67	↓ 8	74,875	0%	Jun. 18, 2014	Sep. 19, 2016
Salesforce	CRM & SFA	42	– 0	57,281	0%	Jun. 18, 2014	Sep. 19, 2016
Informatica Cloud	PaaS	2	– 0	48,701	0%	Jun. 24, 2014	Sep. 19, 2016
Cisco Webex	Web Conferencing, Collabo...	50	↓ 17	48,102	0%	Jun. 18, 2014	Sep. 19, 2016
Twitter	Social Media, Messaging	61	↓ 7	43,543	0%	Jun. 25, 2014	Sep. 19, 2016
Apple iCloud	Cloud Data Services	52	↓ 14	39,392	0%	Jul. 22, 2014	Sep. 19, 2016
PubNub	Development, Cloud Data S...	35	↓ 7	36,975	0%	Jun. 25, 2014	Sep. 19, 2016
Yesware	CRM & SFA, Tracking	38	– 0	36,848	0%	Jun. 18, 2014	Sep. 19, 2016

クラウド サービス レポートは、ユーザのクラウド サービスへのアクセス時のふるまいに関する情報を取得します。そのようなレポートの情報を利用して、対応を行うことができます。また、Umbrella の「いつでも、どこでも、どんなデバイスでも」というアプローチにより、ユーザがネットワーク上に存在しない時でさえ、ユーザのクラウド サービスへのアクセスを把握できます。Umbrella では、電子メール、ファイル共有、SaaS/IaaS/PaaS サービスなどの使用中のクラウド サービスが検出され、その使用状況がレポートされます。

クラウド サービス レポートは、プロビジョニング済みのアイデンティティの既存のポリシー設定など、Umbrella ダッシュボードの既存のデータを活用して、組織から特定のクラウド サービスへの DNS トラフィックと照合し、ユーザのクラウド サービスの使用状況を示します。レポートには、新しいサービスの導入傾向も含まれます。最初の使用日や最終確認日などが含まれます。

クラウド サービスの内容と重要性

近年では、ほぼすべてのユーザが、業務上もしくは個人的な理由から、オンライン ストレージ、Web ベースの電子メール、コラボレーション ツール、教育用のサイト、ソーシャル メディアなどを利用しています。このレポートにおける「クラウド サービス」とは、数ある SaaS、IaaS、PaaS のすべて、つまり、現在利用可能な「クラウド」コンピューティング サービスを意味します。実際に、Umbrella 自体もクラウド サービスであり、レポートにリストされます。リストには、30 を超えるクラウド サービスの分類がまとめられており、個別のクラウド サービスが数百の単位で把握されています。

クラウド サービス レポートは、かつなく拡大を続けているクラウド サービスのユーザの使用状況を把握するための入口であり、その使用の緩和、制限、補足を可能とするものです。この情報は、いくつかの方法で使用できます。クラウド サービスが使用される理由や、ニーズがありながら、組織の正式手順が定められていない状況なのかどうかなどを把握する上で有用です。たとえば、ユーザがファイル サーバの代わりに、オンラインのストレージ システムを使用している場合、それはセキュリティを回避するためではなく、生産性を向上させるためである可能性があります。また、クラウド サービスが、データの損失防止目的で設置された従来の安全措置の回避に使われる場合もあります。そうした状況を把握することで、業務環境でのデータ損失のリスク軽減を図ることができます。

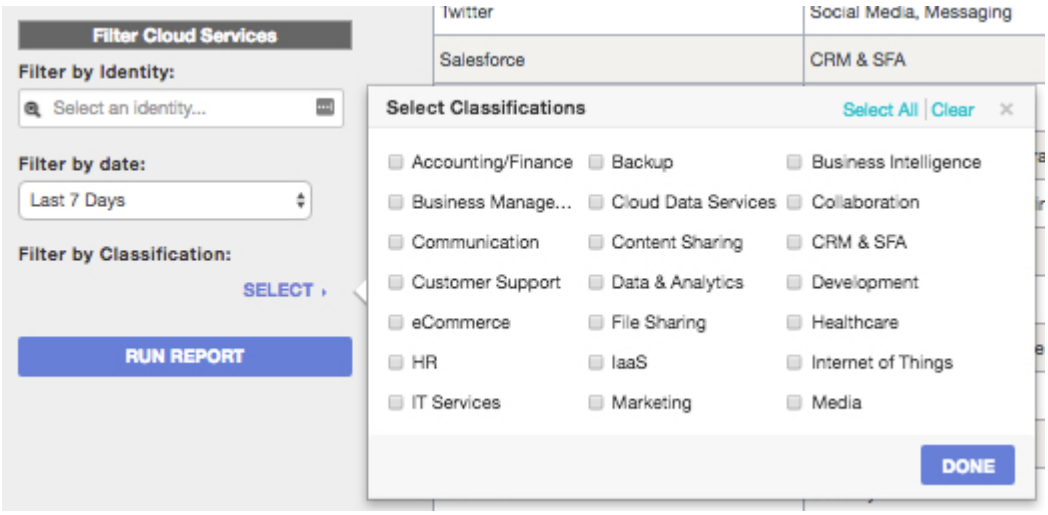
クラウド サービスの認識方法

Umbrella は、小規模な企業から有名ソフトウェア企業までの数千のクラウド サービスのリストにアクセスしています。組織のユーザがアクセスしたドメインが、クラウド サービスであると Umbrella が特定したドメインに一致する場合は、クラウド サービスのレポートでそれが示されます。クラウド サービス レポートでは、それぞれのクラウド サービスを構成する URL に関する詳細が示されます。
また、クラウド サービスは分類ごと、またはサービス タイプごとに分けられています。そうすることで、クラウド サービスの分類へのクエリを、セキュリティ ニーズ上より重要なものに絞ることができます。

注: サービス分類はカテゴリ設定（[ポリシー（Policies）] > [コンテンツ（Content）] > [カテゴリ（Categories）] ）と同じものではありません。重複する部分もありますが、クラウド サービスの分類には、[コンテンツ（Content）] > [カテゴリ（Categories）] にはないものが含まれており、またその逆の場合もあります。たとえば、アダルト サイトは [クラウド サービス（Cloud Service）] > [分類（Classification）] では考慮されませんが、コンテンツ カテゴリでは対象となります。Salesforce などのサービスは、[クラウド サービス（Cloud Service）] > [分類（Classification）] では、CRM/SFA にあたりますが、カテゴリの設定では、ソフトウェア/テクノロジーになります。したがって、レポートを目的とするのか、適用を目的とするのかによって、両者は使い分けられる必要があります。

クラウド サービス分類のリストの場所

1. [レポート(Reporting)] > [クラウド サービス(Cloud Services)] へ移動します。
2. [分類によるフィルタ(Filter by Classification)] で、[選択(Select)] をクリックします。



現在、利用可能なクラウド サービスの分類は次になります。

会計/財務	バックアップ	ビジネス インテリジェンス
ビジネス管理	クラウド データ サービス	コラボレーション
コミュニケーション	コンテンツ共有	CRM および SFA
カスタマー サポート	データおよび分析	開発
e-コマース	ファイル共有	医療
HR	IaaS(Infrastructure as a Service)	Internet of Things(IoT)
IT サービス	マーケティング	メディア
メッセージ	生産性	プロジェクト管理
セキュリティ	ソーシャル メディア管理	ソーシャル メディア
SSO および ID 管理	ストレージ	トラッキング
Web 会議	Web メール	その他

クラウド サービス レポートの使用と理解

クラウド サービス レポートは、アイデンティティが訪問する URL を参照することで、組織から収集されたデータを蓄積しています。現在、この情報はアクティビティ検索レポートで確認することができます。Umbrella は、このデータを特定のクラウド サービスに属する URL と組み合わせます。

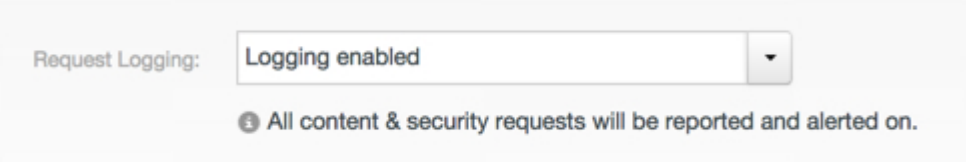
注

データを収集するには、ロギングを有効にする必要があります。ロギングが有効になっていない場合は、レポートは空白になります。

要求のロギングが有効になっていることの確認

レポートがデータを生成するには、ポリシーでコンテンツ要求のロギングを有効にする必要があります。ロギングが無効になっている場合、クラウド サービス レポートでデータを表示させるには、ロギングを再度有効にする必要があります。クラウド サービスへの要求に対してロギングが必要となるのは、それがセキュリティ イベント（例：マルウェア）ではなく、DNS クエリに関連したコンテンツだからです。

1. [ポリシー（Policies）] > [ポリシー リスト（Policy List）] の順に移動します。
2. ポリシーを展開します。
3. [ポリシーの詳細を設定（Set Policy Details）] タブをクリックします。
4. [要求のロギング（Request Logging）] > [ロギングを有効にする（Logging enabled）] を選択します。



5. [保存（Save）] をクリックします。

また、関連するすべてのアイデンティティからイベントを収集するには、ロギングを有効にしたポリシーをポリシーの階層の中で、適切な場所に位置づけることが重要です。

レポートのフィルタおよび検索

このレポートにおいて重要な点は、レポートの概要などの表示されるデータのすべてが、レポートの時間枠に結び付いている点です。デフォルトでは、時間枠は 7 日ですが、日付を指定してフィルタをかけることで変更できます。レポートの範囲を「過去 24 時間」にせばめることで、ネットワークで使用された新しいクラウド サービスを特定できるようになります。

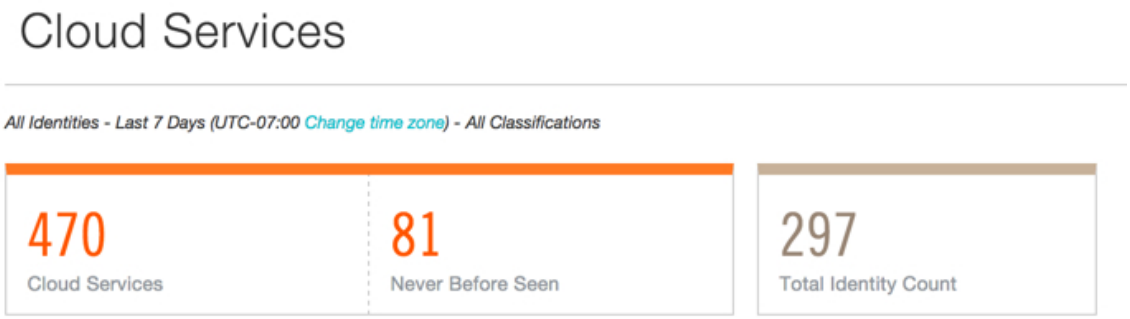
また、検索バーに名前か名前の一部を入力することで、クラウド サービスを検索することもできます。

関心があるサービスを選択して、[サービス詳細(Service Details)] をクリックします。レポートの [サービス詳細(Service Details)] セクションが表示され、クラウド サービスを使用していたアイデンティティのみが表示されます。

クラウド サービス レポート:概要

概要には、指定期間中のクラウド サービスの数、指定期間中の新しいクラウド サービスの数、クラウド サービスにアクセスした組織内のアイデンティティの数などが含まれます。

注:また、レポート概要の一番上には、フィルタが表示されます。次の例では、すべての分類を対象として、過去 7 日間のすべてのアイデンティティが表示されるようにレポートが設定されています。

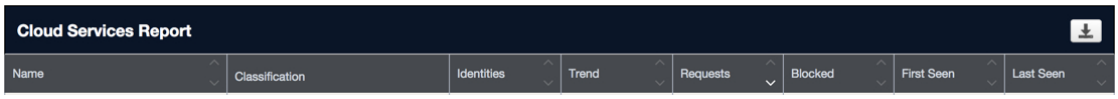


- クラウド サービス：フィルタで指定した期間内に組織内のアイデンティティによってアクセスされたことが確認された個々のクラウド サービスの数。
- 過去に確認されていないサービス：フィルタで指定した期間内に確認されたが、組織での使用がそれまでに確認されていなかったクラウド サービスの数。
- アイデンティティ総数：フィルタで指定した期間内における、クラウド サービスにアクセスしたアイデンティティの総数。

クラウド サービス レポート：サービス リスト

クラウド サービス レポートの概要には、すべてのクラウド サービスがリストされています。分類を除く各列がソート可能です。分類でソートしたい場合は、[分類によるフィルタ（Filter by Classification）] を使用します。

デフォルトのレポートでは、要求数の最も多いクラウド サービスが、一番上にソートされています。上向きの矢印や下向きの矢印をクリックすることで、列をソートできます。

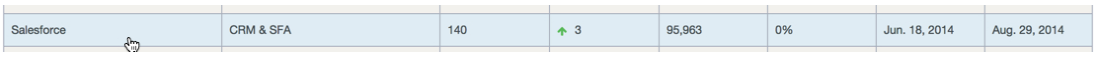


- 名前：クラウド サービス自体の名称。サービス内容の詳細については、サービスを選択してクリックします。
- 分類：分類では、サービスが一般的に何に使用されているかが説明されます。各サービスに 1 つ以上の分類があります。クラウド サービスの分類の完全なリストに関しては、[分類によるフィルタ（Filter by Classification）] をクリックします。
- アイデンティティ：対象のクラウド サービスにアクセスしている組織内のアイデンティティの数。

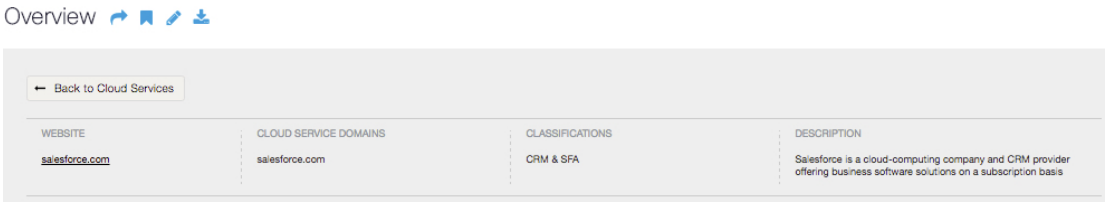
- トレンド：指定期間内における、対象のクラウド サービスを要求するアイデンティティの数の増減。
- 要求：指定期間内の、組織から対象のクラウド サービスに送信された要求数の合計。
- ブロック：指定期間内の、ブロックされたサービスへの要求の割合。
- 最初の確認：対象のサービスが組織内のアイデンティティによって使用されたことが最初に確認された日付。
- 最新の確認：対象のサービスへの要求が行われた最新の日付。

クラウド サービス レポート：サービスの詳細

それぞれのクラウド サービスをドリルダウンすることで、組織内のアイデンティティによる個々のサービスの使用状況に関するレポートを表示できます。レポートのクラウドサービスの名前をクリックするか、[クラウド サービスの検索（Search for a cloud service）] オプションを使用します。ここでは、著名な CRM/SFA ツールである Salesforce を選択します。



クリックすると、このサービスの [サービス詳細（Service Details）] が表示されます。

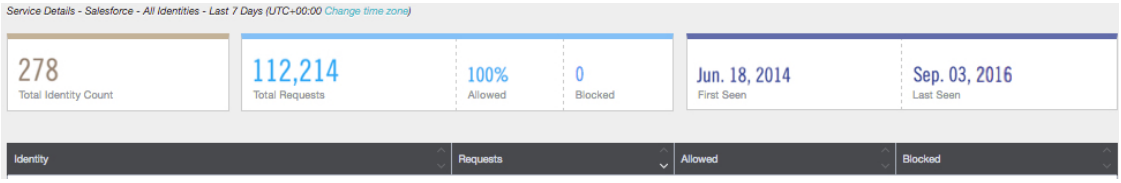


- Web サイト：クラウド サービスを提供する企業の Web サイト。例では、クラウド サービスの名前と企業名が同じですが、異なる場合もあります。
- クラウド サービス ドメイン：クラウド サービスが使用されているかを判断する際に、Umbrella が一致を発見した URL のリスト。通常、クラウド サービスが持つクラウド サービス ドメインは 1 つです。ただし、クラウド サービス ドメインにリストされたサービスが複数あり、どれかにユーザがアクセスした場合は、一致したものとみなされます。Salesforce の例の場合は、インターフェイスで一致した URL 以外にも複数の URL があります。[+] をクリックして展開すると、それらがすべて表示されます。

- 分類：サービスのタイプおよび分類が表示されます。次の例では、分類は 1 つだけですが、クラウド サービスは複数の分類に含まれる可能性があります。
- 説明：クラウド サービスに関する簡単な説明。クラウド サービスの内容や、サービスの使用によりユーザに提供される IT サービスの効果について説明されます。

クラウド サービス レポート：サービスの詳細（アイデンティティによる使用状況）

下記のクラウド サービスの概要では、クラウド サービスを使用するアイデンティティのリストで示されます。

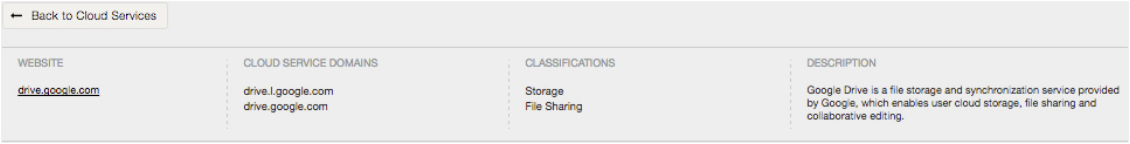


注：また、レポート概要の一番上には、時刻およびアイデンティティ用のフィルタが表示されます。この例では、過去 7 日間のすべてのアイデンティティが表示されるよう、レポートが設定されています。

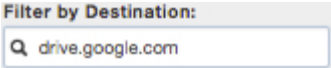
- アイデンティティの総数：対象のクラウド サービスにアクセスする特定の総数。個別のアイデンティティは、[アイデンティティ（Identities）] の列の下に示されます。
- 総要求数：対象のクラウド サービスへの要求の総数。アイデンティティごとの要求数は、[要求数（Requests）] の列に示されます。
- 許可：このサイトへの許可された要求の割合。アイデンティティごとの許可された要求の数は、[許可（Allowed）] の列に示されます。
- ブロック：このサイトへのブロックされた要求の割合。アイデンティティごとのブロックされた要求の数は、[ブロック（Blocked）] の列に示されます。

FAQ

Q：アイデンティティが実行したクラウド サービスへの要求はどれか、またいつ実行されたかを正確に確認するには、どうすればいいですか。
クラウド サービスの詳細レポートでリストされているドメインで、調査対象のクラウド サービスのドメインを確認します。たとえば、Google Drive を使用しているアイデンティティを検出したい場合は、まず、そのクラウド サービスのドメインを確認します。

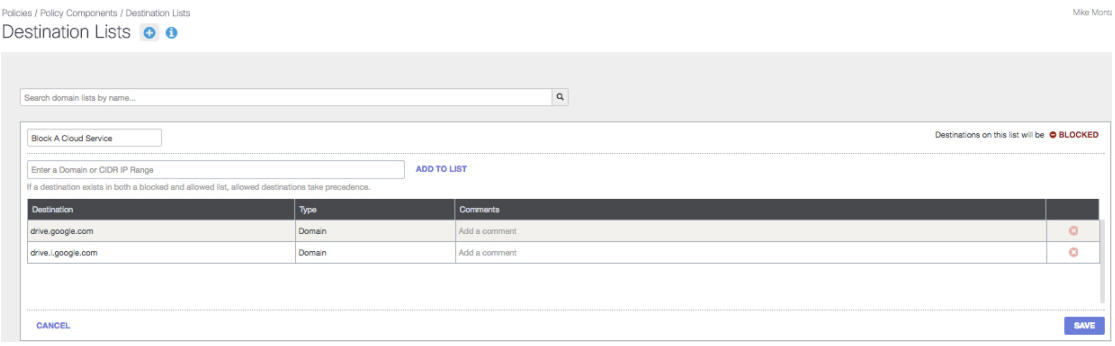


次に、アクティビティ検索レポートに移動し、そのサービスのクラウド サービスのドメインを対象に [ドメインでのフィルタ(Filter by Domain)] を適用します。その結果、組織内のどのアイデンティティがサービスを使用していたか、また使用した時刻が表示されます。

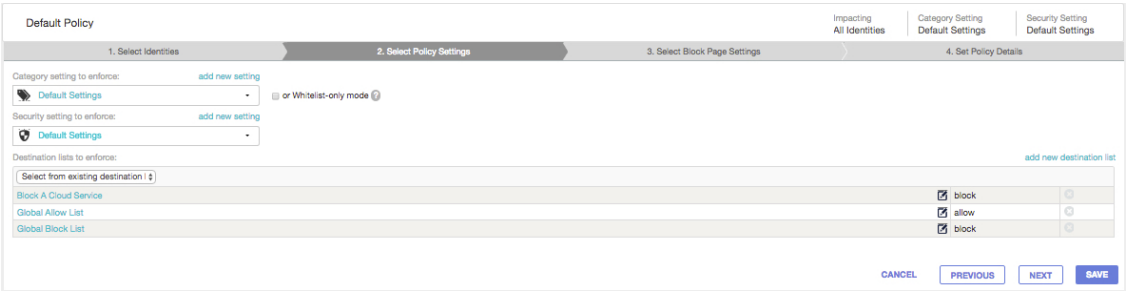


Q:Umbrella で、クラウド サービスの使用を推奨する、もしくは使用をブロックするにはどうすればいいですか。

次のステップに進み、ユーザのクラウド サービスの使用をブロックする場合を想定します。クラウド サービスの使用を推奨することに関しては、お客様が判断すべきことであり、組織にとって何が最適化を判断する必要があります。しかし、それは単一のドメインをブロックするのに比べ、シンプルなものではありません。上述の Google Drive の例の場合、少なくとも 2 つのクラウド サービスのドメインがブロックされる必要があります。
リストを収集し、ダッシュボードで、[設定(Configuration)] > [ポリシー設定(Policy Settings)] > [ダッシュボード(Destination)] に移動します。新しい接続先リストを追加することも、既存の接続先リストを編集することもできます。次の例では、Google Drive のクラウド サービスにリストされている 2 つのドメインをブロックするように新しいリストを作成しています。



接続先リストが保存されると、複数の既存のポリシーに適用できるようになります。例では、デフォルト ポリシーに適用していますが、組織内のすべてのアイデンティティに適用されるため、注意が必要です。



Q:新しいクラウド サービスの追加や既存のクラウド サービスの編集は可能ですか。
はい。サービスを追加するには、ページの上部にある「提案」アイコンをクリックし、フォームに入力します。

可能であれば、コメントの項目に、サービスのクラウド サービス ドメインや、簡単な説明を追加してください。要望はサポート チーム送付されてレビューされます。クラウド サービスのリストへの追加を確認するために、フォローアップの質問が送信される場合があります。

サービスの変更または編集を行うには、編集したいクラウド サービスの詳細をクリックするか、左側の検索バーでサービスを検索します。

サービス、詳細が表示されたら、ページの上部にある「編集の提案」アイコンをクリックし、フォームに入力します。

そのサービスのクラウド サービス ドメインの編集または更新を希望している場合は特に、変更したい URL やドメインについて明確にするようにしてください。要望はサポート チーム送付されてレビューされます。クラウド サービスの変更を確認するために、フォローアップの質問が送信される場合があります。

Q:レポートからクラウド サービスを削除するにはどうすればいいですか。
レポートに表示させるクラウド サービスを少なくしたり、もしくは、クラウド サービス（通常の IT サービスの一部として有償で使用しているものなど）を安全なサービスとしてマークして、レポートから削除したりしたい場合があるかも知れません。現在、こうした機能は利用できませんが、ご要望があればお聞かせください。

Q:利用可能なクラウド サービスのリストはどこで確認できますか。
できる限り早期での公開が検討されていますが、現時点では、包括的なリストは公開されていません。検索ウィンドウでの「入力予測」機能を使用すれば、関心のあるサービスを見つけることができます。特定のクラウド サービスが含まれているか質問したい場合は、サポート部門までお問い合わせください。

Q:対象のカテゴリに設定した独自のカテゴリ(コンテンツ)が、クラウド サービスの分類に適用されないのはなぜですか。
カテゴリ設定(ダッシュボードの [ポリシー設定(Policy Settings)] > [カテゴリ設定(Category Settings)] に表示される内容)は、クラウド サービスの分類とは別のものです。場合によっては、サイトがカテゴリ設定に当てはまるが、カテゴリ設定に類似したクラウドサービスの分類には当てはまらないことがあります。各クラウド サービスに個別に適用を行うには、ブロックしたい各クラウド サービスのサービス詳細を確認した上で、手順に従うのが最適です。

Q:シャドー IT とは何ですか。
シャドー IT は、一般に認識されつつある概念で、好むと好まざるとに関わらず、使用しているネットワークに存在する可能性があります。実質的には、BYOC(Bring Your Own Cloud:個人のクラウドの持ち込み)になります。従来のツールを使用するよりも素早く効率的に業務を行うために、ユーザ、また場合によっては IT チームのメンバー自身が、自分の使用するクラウド サービスを職場に持ち込むことを意味します。

シャドー IT が使用されると、機密データが損なわれる、もしくは組織内で正式ではないプロセスや手順が発生するなど、複数の望ましくない影響が生じる可能性があります。ただし、シャドー IT について理解することで、組織の従業員のニーズが把握できる可能性もあります。多くの場合、クラウド SaaS のシャドー IT を使用するユーザは、単に業務を完了させるための方法を探しているだけである場合がほとんどです。そして、IT 部門の役割は、業務の安全で滞りない遂行を支援することです。クラウド サービス レポートにより、将来のクラウド サービス ソリューションにおける生産性とセキュリティのギャップを埋めることができるようになります。

アイデンティティ レポート > クラウド サービス レポート > 管理監査ログ レポート

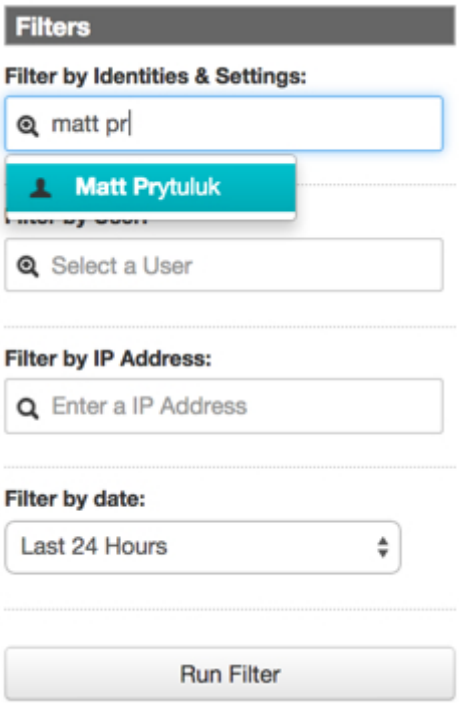
管理監査ログ レポート

管理監査ログには、管理チームが組織の Umbrella 設定に対して行った変更が記録されます。管理監査ログには、ダッシュボードで行われた変更に関する情報が、1年分保存されます。情報には追加、変更、削除などの変更が含まれます。

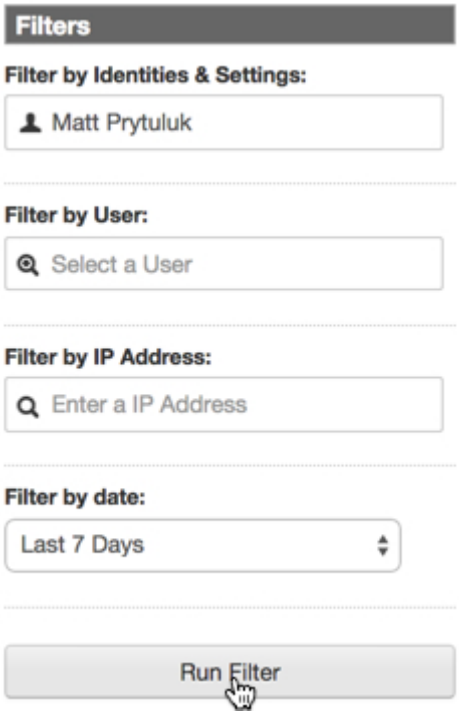
レポートには、次のような内容が含まれます。

- 変更の日時
- 変更を行った IP アドレス
- ログインした管理者ユーザ
- 変更されたダッシュボードの項目または領域
- 行われたアクション

フィルタにより、さらに細かい内容を表示できます。アイデンティティや設定でフィルタすることができます。最初の数文字を入力すると、変更の対象となったアイデンティティや設定の候補が表示されます。



日付の範囲を選択すると、その期間内での変更について確認できます。また、変更を行ったユーザや、変更を行ったネットワークの IP を選択することもできます。

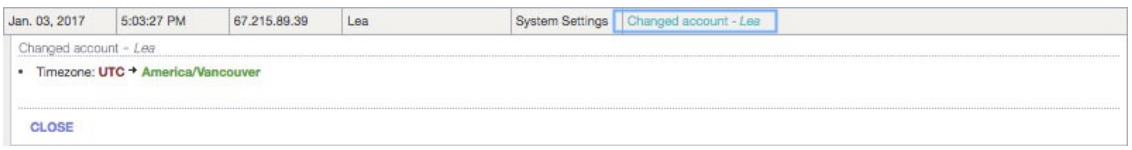


管理監査ログには次のものが含まれます。

- 作成されたポリシー、アイデンティティ、ブロック ページ
- 変更されたポリシー、アイデンティティ、ブロック ページ
- 削除されたポリシー、アイデンティティ、ブロック ページ

注: 管理者の変更により削除または名前変更されたアイデンティティや設定は、データベースから失われるため、フィルタでは検索できなくなります。しかしながら、変更の記録はされているため、ユーザ、IP アドレス、時間範囲でのフィルタは可能です。

関心がある変更に関して詳細情報を確認する場合は、その変更の [アクション (Action)] の列にあるハイパーリンクをクリックしてください。



クラウド サービス レポート > **管理監査ログ レポート**