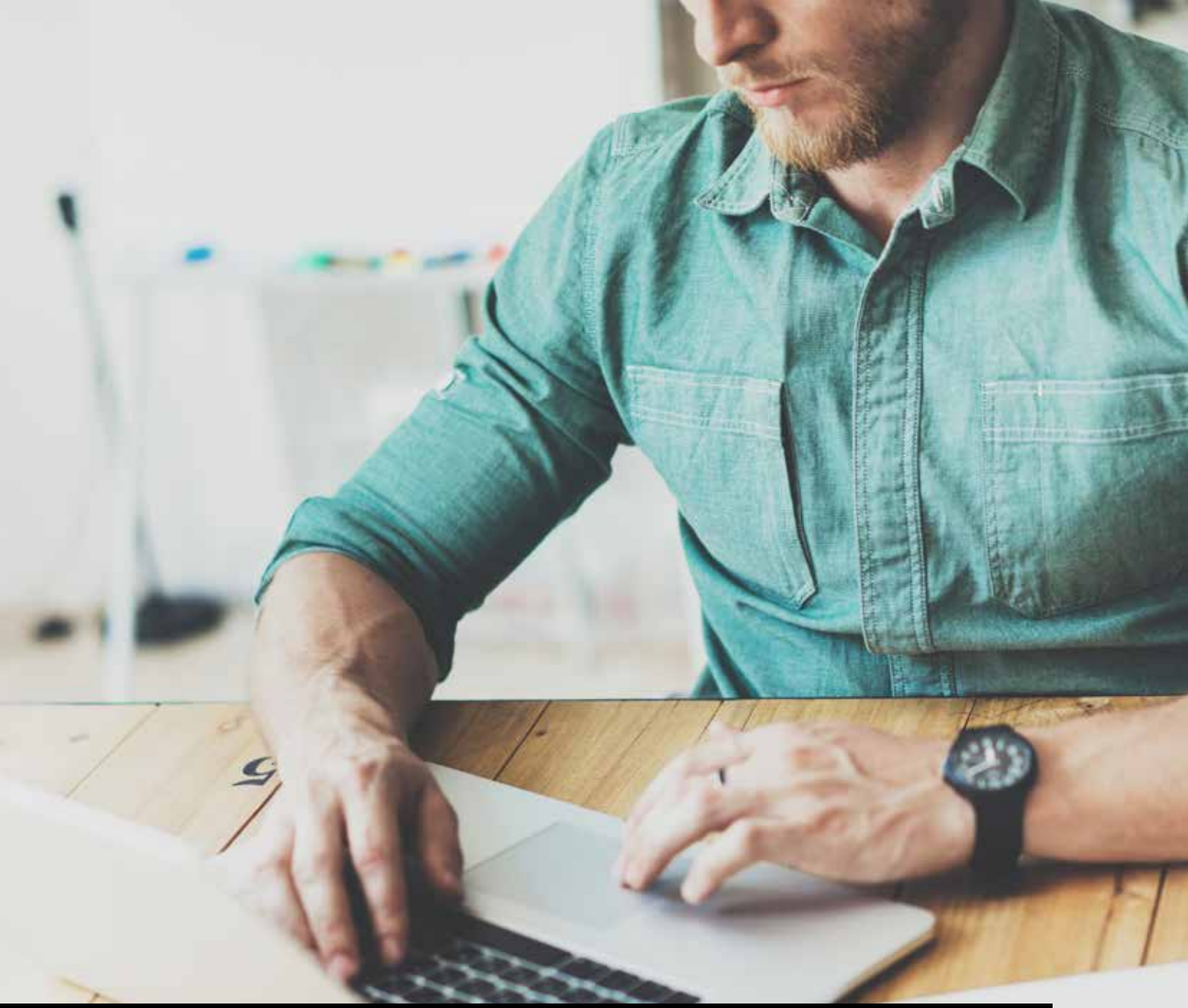


機能紹介：Cylance®
管理コンソールレポート機能

CylancePROTECT® 管理における対話型ダッシュボード
およびレポート

CYLANCE

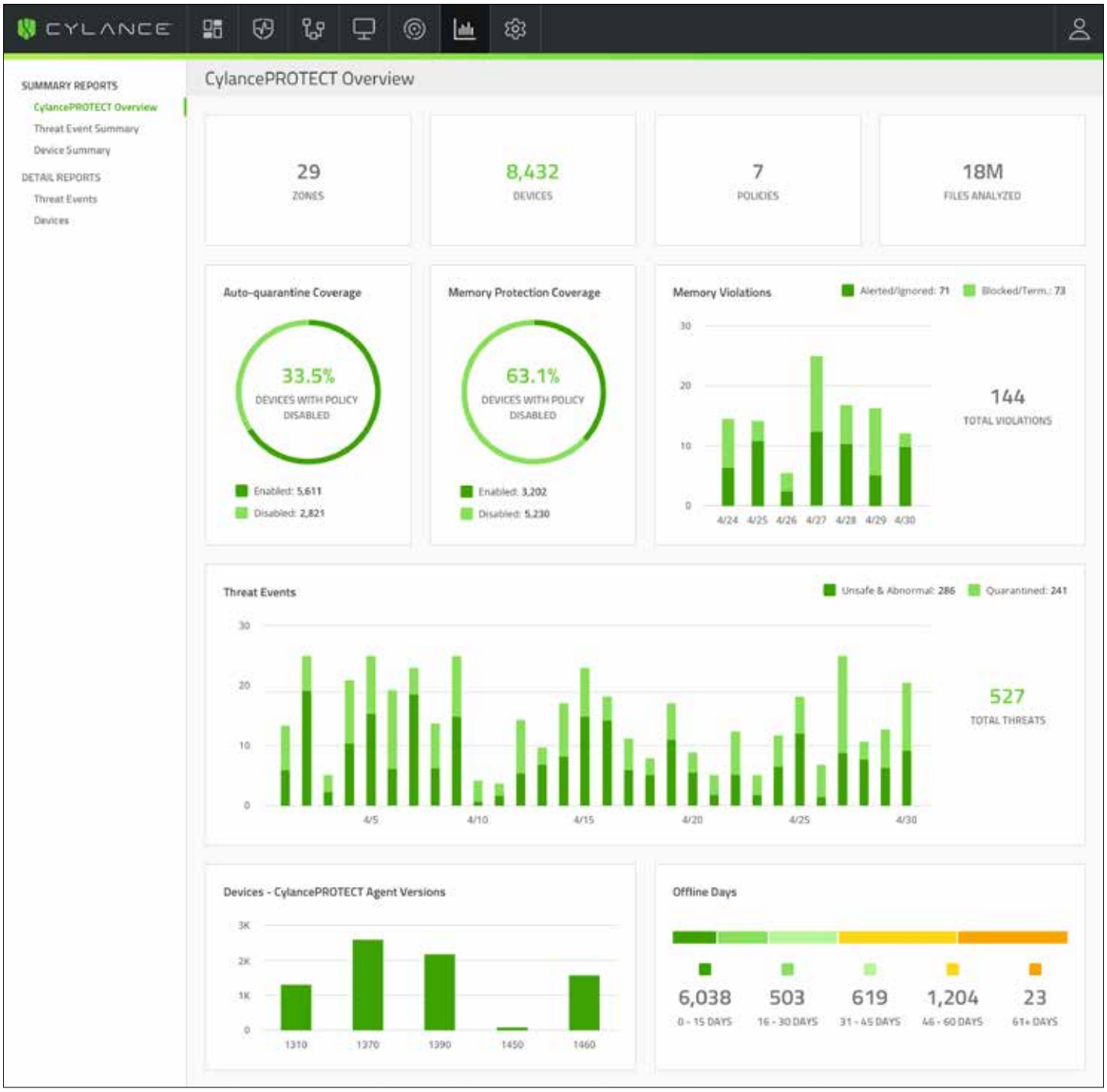
はじめに

組織のエンドポイントやサーバーをセキュリティ侵害から防御することは、Cylance のセキュリティソリューションの最優先事項です。CylancePROTECT と CylanceOPTICS™では、特許を取得した人工知能（AI）や専用のセキュリティ機能を使用し、継続的な防御を提供することで、企業の機密データを確実に防御します。

このたび、Cylance の管理コンソールに追加されたレポート機能により、ユーザーはリアルタイムの対話型の統計を容易に入手し、状況をより的確に把握して、潜在的な攻撃対象領域に対する洞察を得られるようになりました。本書では、Cylance 管理コンソールで提供される新たなダッシュボードやレポートについて詳しく説明します。

CylancePROTECT の概要

ゾーンやデバイスの数から、自動隔離やメモリ防御がカバーするデバイスの割合、脅威イベント、メモリの侵害、Agent バージョン、デバイスのオフライン日数までの、CylancePROTECT の使用状況の概要を提供します。

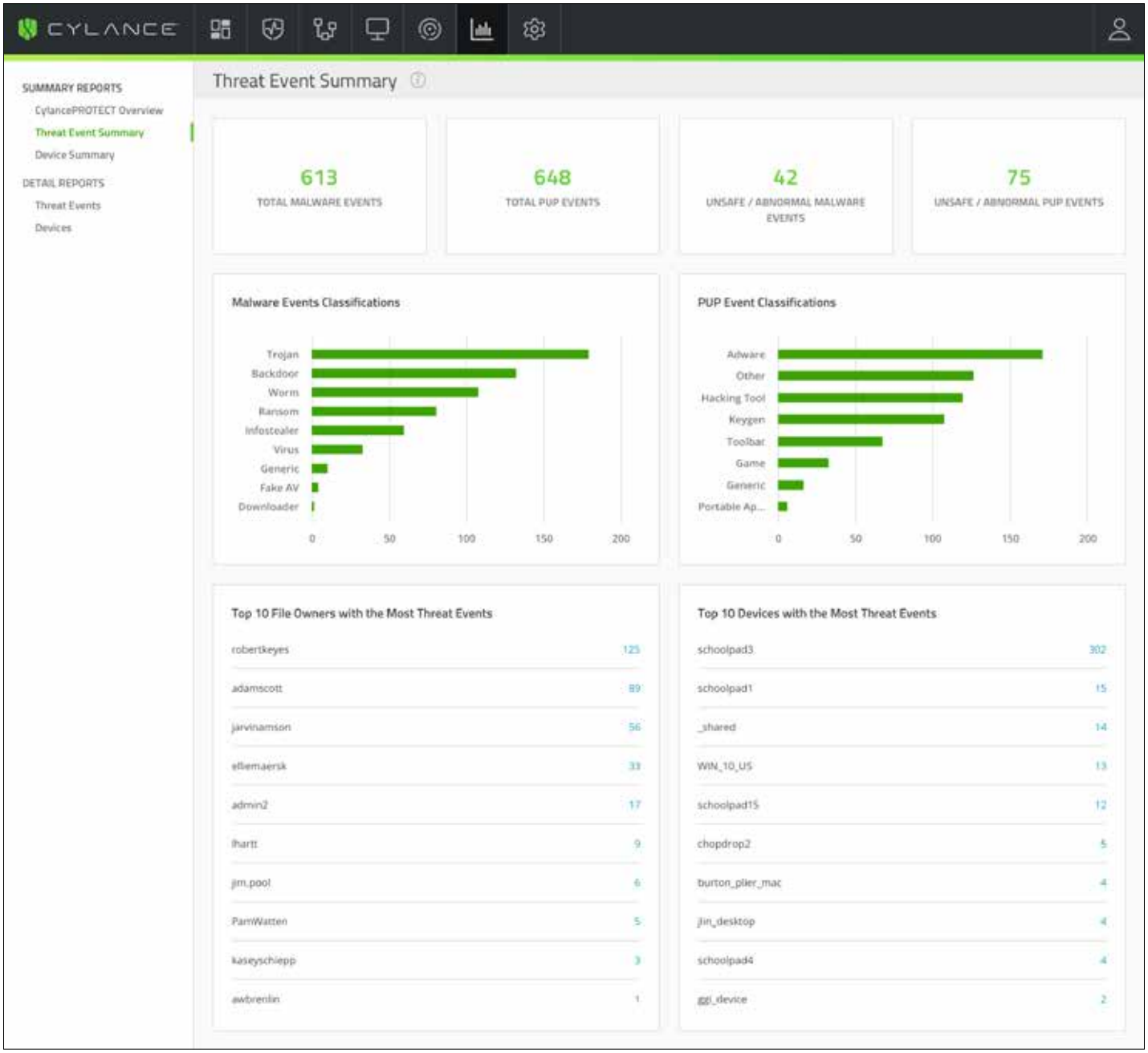


CylancePROTECT の概要レポートの詳細

レポートのセクション	説明
自動隔離のカバー率	ポリシーで Unsafe と Abnormal の両方について自動隔離が選択されているデバイスの数を表示します。これらのデバイスは、有効（Enabled）とみなされます。オプションの一方または両方が無効となっているポリシーに割り当てられているデバイスは無効（Disabled）なデバイスです。円グラフには、Unsafe、Abnormal、またはその両方について自動隔離が無効となっているポリシーに割り当てられたデバイスの割合が表示されます。このウィジェットをクリックすると、自動隔離のステータス（有効／無効）ごとのデバイスの詳細なリストが表示されます。
デバイス数	組織内のデバイスの数を表示します。デバイスとは、登録された CylancePROTECT Agent を持つエンドポイントのことです。このウィジェットをクリックすると、デバイスの詳細なリストが表示されます。
デバイス - CylancePROTECT バージョンに関する統計	Agent バージョンを実行中のデバイスの数を表す棒グラフを表示します。表の棒上にカーソルを合わせると、その Agent バージョンを実行中のデバイスの数が表示されます。このウィジェットをクリックすると、Agent バージョンでフィルタリングされたデバイスの詳細なリストが表示されます。
分析したファイル総数	組織内のすべてのデバイスにわたって分析されたファイルの数を表示します。
メモリ防御のカバー率	ポリシーに記載された 16 のメモリ違反タイプ中 11 以上についてメモリ防御が Block または Terminate に設定されたポリシーを持つデバイスの数を表示します。これらのデバイスは有効（Enabled）とみなされます。10 以下のメモリ違反タイプについてメモリ防御が Block または Terminate に設定されたポリシーに割り当てられているデバイスは無効（Disabled）なデバイスです。円グラフには、10 以下のメモリ違反タイプが Block または Terminate に設定されているポリシーに割り当てられたデバイスの割合が表示されます。このウィジェットをクリックすると、メモリ防御のステータス（有効／無効）ごとのデバイスの詳細なリストが表示されます。
メモリ違反	この 7 日間に、アラート／無視（Alert/Ignore）または遮断済み／停止済み（Block/Term）のいずれかであったメモリ違反を棒グラフで示します。表の棒上にカーソルを合わせると、各データタイプの内訳が表示されます。
オフラインの日数	ある期間（「0 ～ 15 日」から「61 日以上」まで）オフラインだったデバイスの数を表示します。また、それぞれの期間ごとに色分けされた棒グラフも表示されます。
ポリシー数	組織内で作成されたポリシーの数を表示します。
脅威イベント	過去 30 日間の日付ごとにグループ化された脅威イベントの数を示す棒グラフを表示します。グラフの棒上にカーソルを合わせると、その日のイベントの内訳が表示されます。このウィジェットをクリックすると、脅威の詳細なリストが表示されます。
ゾーン数	組織内のゾーンの数を表示します。

脅威イベントサマリー

脅威イベントサマリーレポートには、マルウェアと Potentially Unwanted Programs（PUP、怪しいプログラム）という 2 つの分類で CylancePROTECT に検知されたファイルの数と、各ファミリーの特定のサブカテゴリ分類の詳細が表示されます。

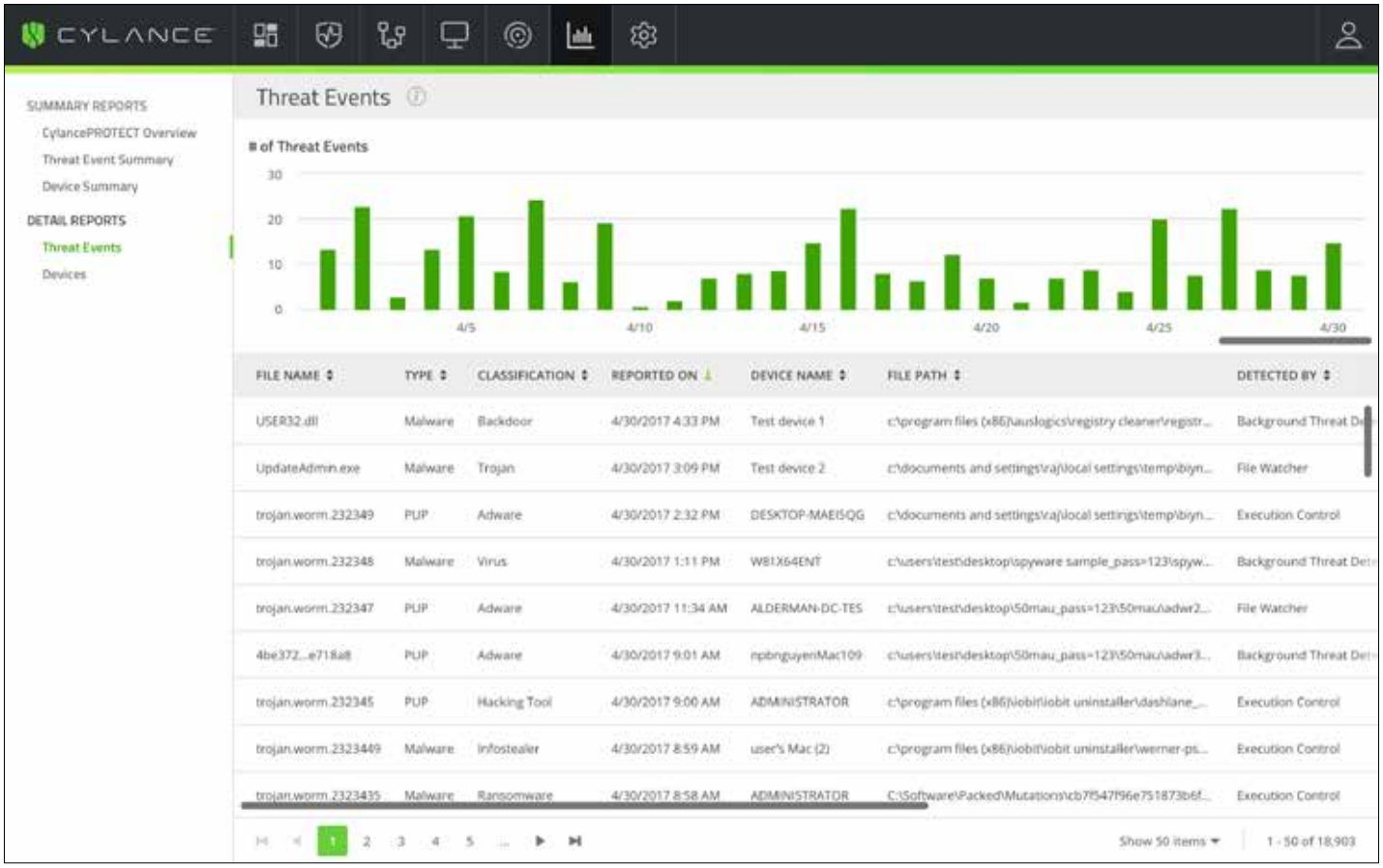


脅威イベントサマリーレポートの詳細

レポートのセクション	説明
マルウェアイベントの分類	組織内のデバイスで見つかった脅威イベントのマルウェアの分類タイプごとの棒グラフを表示します。グラフの棒上にカーソルを合わせると、その分類で見つかったマルウェアイベントの合計数が表示されます。このウィジェットをクリックすると、マルウェアの詳細なリストが表示されます。
Potentially Unwanted Program（PUP）イベントの分類	組織内のデバイスで見つかった脅威イベントの PUP 分類タイプごとの棒グラフを表示します。グラフの棒上にカーソルを合わせると、その分類で見つかった PUP イベントの合計数が表示されます。このウィジェットをクリックすると、PUP の詳細なリストが表示されます。
脅威イベントが最も多いトップ 10 デバイス	脅威イベントが最も多いトップ 10 デバイスのリストを表示します。このウィジェットをクリックすると、デバイス名でフィルタリングされた脅威の詳細なリストが表示されます。
脅威イベントが最も多いトップ 10 ファイルの所有者	脅威イベントが最も多いトップ 10 ファイルの所有者のリストを表示します。このウィジェットをクリックすると、ファイル所有者でフィルタリングされた脅威の詳細なリストが表示されます。
マルウェアイベントの合計	組織内で特定されたマルウェアイベントの合計数を表示します。このウィジェットをクリックすると、マルウェアイベントの詳細なリストが表示されます。
PUP イベントの合計	組織内で特定された PUP イベントの合計数を表示します。このウィジェットをクリックすると、PUP イベントの詳細なリストが表示されます。
Unsafe/Abnormal 判定のマルウェアイベント数	組織内で検出された Unsafe/Abnormal マルウェアイベントの合計数を表示します。このウィジェットをクリックすると、Unsafe/Abnormal 状態のマルウェアイベントの詳細なリストが表示されます。
Unsafe/Abnormal 判定の PUP イベント数	組織内で検出された Unsafe/AbnormalPUP イベントの合計数を表示します。このウィジェットをクリックすると、Unsafe/Abnormal 状態の PUP イベントの詳細なリストが表示されます。

脅威イベント

脅威イベントレポートでは、過去 30 日に環境内で検出された脅威のデータを毎日提供します。

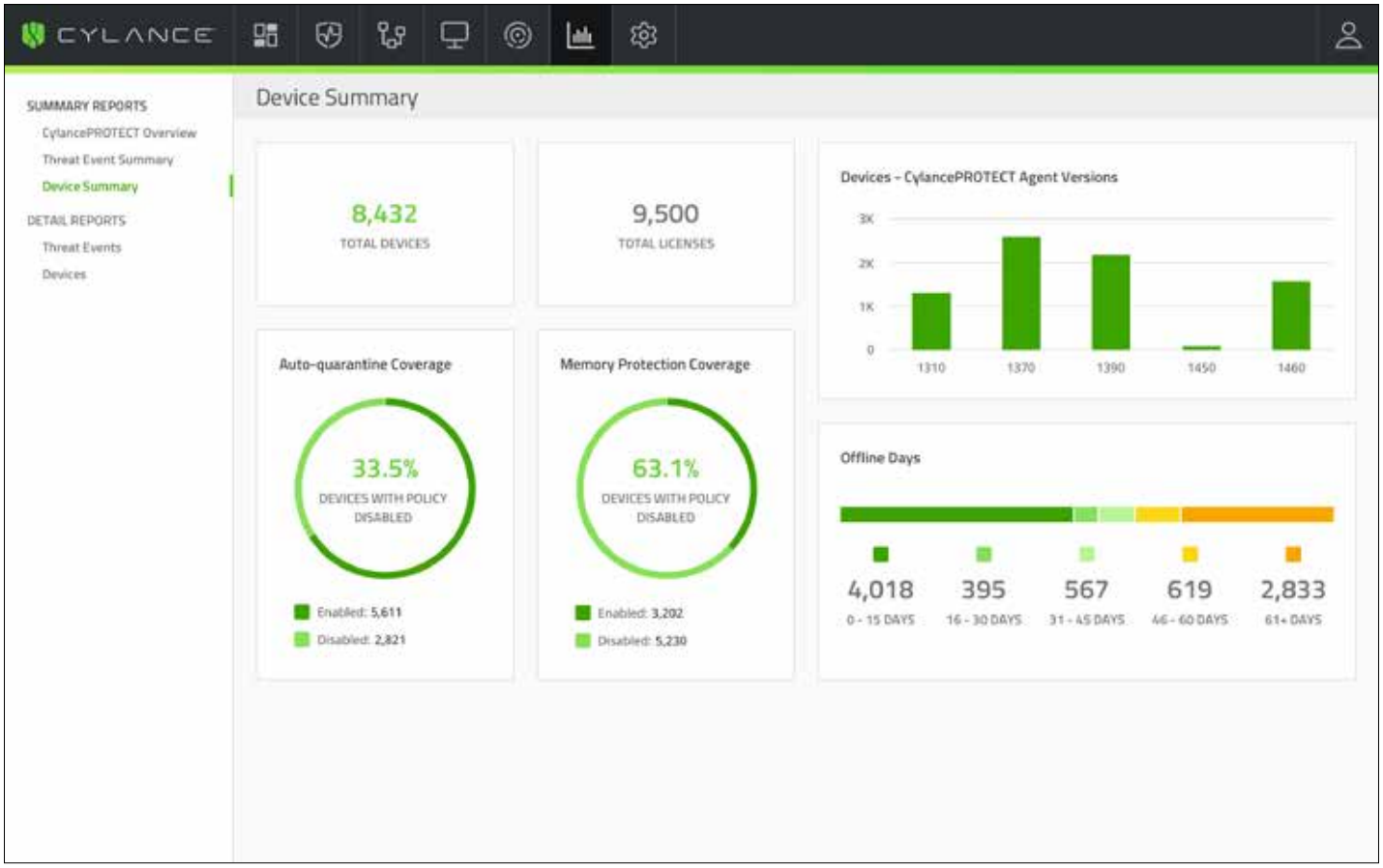


脅威イベントレポートの詳細

レポートのセクション	説明
脅威イベントの数	組織で報告された脅威イベントを示す棒グラフを表示します。グラフ上の棒にカーソルを合わせると、その日に報告された脅威イベントの合計数が表示されます。棒グラフは過去 30 日分が表示されます。任意の棒をクリックすると、その下の表が報告日によってフィルタリングされます。棒を再度クリックするとフィルタが解除されます。
脅威イベントテーブル	脅威イベント情報を表示します。テーブルの項目をクリックすると、リストが列ごとに（昇順または降順で）ソートされます。

デバイスサマリー

デバイスサマリーレポートには、デバイスに関する複数の測定結果が表示されます。

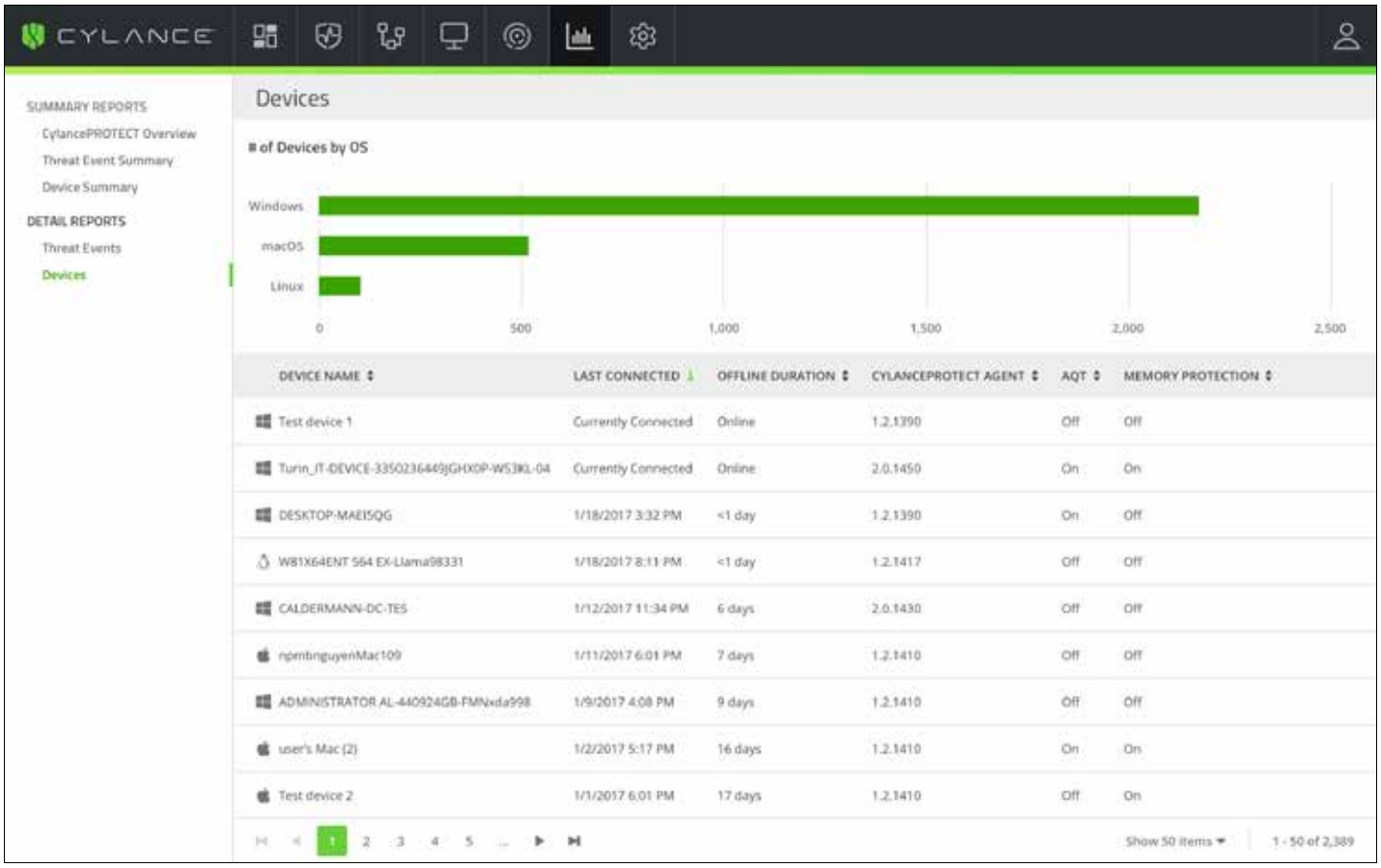


デバイスサマリーレポートの詳細

レポートのセクション	説明
自動隔離のカバー率	ポリシーで Unsafe と Abnormal の両方について自動隔離が選択されているデバイスの数を表示します。これらのデバイスは、有効（Enabled）とみなされます。オプションの一方または両方が無効となっているポリシーに割り当てられているデバイスは無効（Disabled）なデバイスです。円グラフには、Unsafe、Abnormal、またはその両方について自動隔離が無効となっているポリシーに割り当てられたデバイスの割合が表示されます。このウィジェットをクリックすると、自動隔離のステータス（有効／無効）ごとのデバイスの詳細なリストが表示されます。
デバイス - CylancePROTECT バージョンに関する統計	Agent バージョンを実行中のデバイスの数を表す棒グラフを表示します。表の棒上にカーソルを合わせると、その Agent バージョンを実行中のデバイスの数が表示されます。このウィジェットをクリックすると、Agent バージョンでフィルタリングされたデバイスの詳細なリストが表示されます。
メモリ防御のカバー率	ポリシーに記載された 16 のメモリ違反タイプ中 11 以上についてメモリ防御が Block または Terminate に設定されたポリシーを持つデバイスの数を表示します。これらのデバイスは有効（Enabled）とみなされます。10 以下のメモリ違反タイプについてメモリ防御が Block または Terminate に設定されたポリシーに割り当てられているデバイスは無効（Disabled）なデバイスです。円グラフには、10 以下のメモリ違反タイプが Block または Terminate に設定されているポリシーに割り当てられたデバイスの割合が表示されます。このウィジェットをクリックすると、メモリ防御のステータス（有効／無効）ごとのデバイスの詳細なリストが表示されます。
オフラインの日数	ある期間（「0 ～ 15 日」から「61 日以上」まで）オフラインだったデバイスの数を表示します。また、それぞれの期間ごとに色分けされた棒グラフも表示されます。
デバイス数の合計	組織内のデバイスの合計数を表示します。デバイスとは、登録された CylancePROTECT Agent を持つシステムのことです。このウィジェットをクリックすると、デバイスの詳細なリストが表示されます。
ライセンスの合計数	組織が購入した CylancePROTECT ライセンスの合計数を表示します。

デバイス数

デバイスレポートには、オペレーティングシステムファミリー（Microsoft Windows、Apple macOS、および Linux）ごとのデバイス数が示されます。



デバイスレポートの詳細

レポートのセクション	説明
OS ごとのデバイスの数	主要な OS グループ（Microsoft Windows、Apple macOS、Linux）ごとにデバイスが分類された棒グラフを表示します。グラフ上の棒にカーソルを合わせると、その OS グループのデバイスの合計数が表示されます。任意の棒をクリックすると、その下の表が OS グループによってフィルタリングされます。棒を再度クリックするとフィルタが解除されます。
デバイステーブル	組織内のデバイスのデバイス名とデバイス情報のリストを表示します。

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)