エクリプシアム・サプライチェーン・セキュリティ・プラットフォーム_

テクノロジーへの信頼をコアからクラウドまで

ほとんどの組織は、ITインフラの基盤レイヤーを暗黙のうちに信頼しています - この事実が、攻撃者にとって低レベルのエクスプロイトを特に望ましいターゲットにしているのです。Eclypsiumのサプライチェーン・セキュリティ・プラットフォームは、調達、導入、運用において、ITインフラストラクチャの重要な低レベルのコンポーネントを継続的に監視し、修復することができます。

このデータシートでは、クライアント、サーバ、ネットワークデバイスに対するEclypsiumの機能の詳細を提供します。サポートに関するその他の詳細については、文中のハイパーリンクから弊社Webサイトをご覧ください。

デバイス、およびコンポーネントのインベントリー_

Eclypsiumは、システムUEFIとBIOSファームウェア、プロセッサーとチップセット、PCIデバイス、ネットワークコンポーネント、周辺機器、Trusted Platform Module、Intel Management Engineなどを含む、デバイスとその低レベルコンポーネントのインベントリーを作成します。詳細レベルは、ベンダーやモデルによって異なります。

	クライアント	サーバー	ネットワーク
識別情報 IPアドレス（オプション）、MACアドレス、ホスト名、オペレーティング・システム（ベンダー、バージョンなど）などのデバイスの特徴。	✅	✅	✅
ファームウェアとハードウェアの詳細情報 プロセッサ、チップセット、デバイス、ファームウェアベンダー、リリース日、システムおよびデバイスメーカー、モデル番号など。	✅	✅	✅
ハードウェアの状態と設定			
CPU、チップセット、I/Oレジスタ、その他の関連設定	✅	✅	
PCI/PCIe情報 - PCI/PCIeデバイス設定とオプション（拡張）ROMファームウェア	✅	✅	
デバイス、コンポーネント、その他ファームウェアの詳細			
ブートローダ情報	✅	✅	
ベンダー固有のファームウェアとその他の種類のファームウェア	✅	✅	✅
コンポーネントのハードウェアとファームウェアのコンフィギュレーション	✅	✅	
トラステッド・プラットフォーム・モジュールの状態	✅	✅	

ハーディング（要塞化）_

Eclypsium は、デバイスのセキュリティ・ポスチャーに影響を与える脆弱性や設定ミスがないか、低レベルのコンポーネントを分析します。これにより、改善すべき問題の優先順位付けが容易になります。Eclypsiumは、メーカーにより異なりますが、ほとんどの場合アップデートの適用を支援します。

	クライアント	サーバー	ネットワーク
影響を受けるコンポーネントを持つデバイスの検索 新しい問題が最初に発見されたとき、組織は、問題の影響を受ける特定のコンポーネントを含むデバイスを追跡することによって、その影響を評価する必要がある。そのためには、コンポーネントレベルの可視化が必要である。	✅	✅	
古いファームウェアの検索 脆弱性やその他の問題の影響を受ける可能性のある、古いファームウェアを持つデバイスを見つける。	✅	✅	✅
脆弱性の発見 従来のソフトウェア脆弱性スキャンでは見逃されがちな、ハードウェアやファームウェア・コンポーネントに影響する脆弱性やCVEを持つデバイスを特定する。	✅	✅	✅
リスク別にデバイスをソート 累積リスクに基づいてデバイスを素早くソート。 OS、グループ、ベンダー、製品、コンポーネント、セキュリティ機能、脆弱性でフィルタリングし、表示をさらに絞り込むことができる。	✅	✅	✅
脆弱性による検索 特定の脆弱性を検索・調査し、影響を受け、特定の脆弱性についてスキャンされたすべてのデバイスを検索できる。	✅	✅	✅
デバイスの誤設定の検索 無効化されたBIOS書き込み保護や、SMIやFlash記述子などのアンロックされたコンポーネントなど、デバイスを危険にさらす可能性のある構成の問題を特定する。	✅	✅	✅
パッチマネジメントとアップデート* Eclypsiumコンソールを介して、またはAPIを介して、ファームウェア・アップデートをダウンロードしてインストールすることで、問題を直接修正する。	✅	✅	✅

* 機能はメーカーやモデルによって異なります。

jp-info@eclypsium.com
eclypsium.com

検知と対応_

Eclypsiumは、EDRやその他のセキュリティ制御を回避するように設計された攻撃の侵害指標を検出するために、さまざまなメカニズムを使用します。新たなサプライチェーンの脅威が発見された場合、Eclypsium はサプライチェーンの脆弱なコンポーネントを特定して修復し、お客様の環境で悪用の兆候を探すことで、お客様の組織が迅速に対応できるよう支援します。

	クライアント	サーバー	ネットワーク
ベースラインの変更 ベースラインから逸脱したデバイスを素早く特定し、価値の高いシステムに予期せぬ、または計画外の変更があった場合に、それを簡単に認識することができます。ベースラインは、デバイスのグループに適用することもできる。	✅	✅	✅
未知のバイナリーの検出 Eclypsiumは、業界で最も広範な既知のベンダー・ファームウェアのライブラリを維持しており、この継続的に維持されている許可リストにないファームウェアを特定することができる。	✅	✅	✅
既知の脅威の検知 ルートキット、ハードウェアインプラント、バックドアなど、既知のさまざまな脅威の存在を検出。ユーザーは、独自のファームウェア固有のYARAルールをインポートし、定義することができる。	✅	✅	✅
行動異常の検知 Eclypsiumは、潜在的な脅威を示す可能性のある異常を明らかにするために、システムの動作データのヒューリスティックモデルを作成し、分析する。これにより、検出を回避するハードウェア・メカニズムを利用したファームウェア・インプラントの検出を可能とする。	✅	✅	
ダイナミック・アラート 設定可能なアラートにより、特定の脆弱性や侵害の兆候についてデバイスのグループを監視し、セキュリティ運用チームやインシデント対応チームに通知することができる。	✅	✅	✅
サプライチェーンの脅威への対応 Eclypsiumは、新たな脆弱性や疑わしいコンポーネントが判明したときに、セキュリティチームが影響を受けるシステムを迅速に特定できる。	✅	✅	✅
自動化された対応 強力なREST APIは、SIEMやSOARソリューションなどの他のエンタープライズセキュリティツールと統合し、自動応答やプレイブックをトリガーする。	✅	✅	✅

jp-info@eclypsium.com
eclypsium.com

対応アセット・タイプ_

クライアント

Eclypsiumは、ラップトップ、ワークステーション、タブレットを含む幅広いエンドポイントデバイスや、現金自動預け払い機（ATM）やPOSシステムなどの最新のコンピューティングプラットフォームを使用する特殊な機器をサポートします。
EclypsiumはWindows、macOS、および多くのLinuxディストリビューションをサポートし、Apple、Asus、Dell、富士通、HP、Lenovo、Quanta、および東芝のシステムを含む、事実上すべてのx86ベースのプラットフォーム上で動作します。

サポートされるオペレーティングシステム、ハードウェア、チップセットの詳細については、eclypsium.com/platform/specs/をご覧ください。

サーバー

Eclypsiumは広範なサーバーとマイクロサーバー、そしてそれらの基盤となるコンポーネントをサポートしています。EclypsiumはWindowsとLinuxの多くのディストリビューションをサポートし、Dell、HPE、Lenovo、Quanta、Supermicroなどのサーバーを含む、事実上すべてのx86ベースのプラットフォーム上で動作します。Eclypsiumは、VMware ESXi環境におけるファームウェアの整合性監視、リスク管理、パッチ管理もサポートしています。

サポートされるサーバーとマイクロサーバーの詳細については、eclypsium.com/platform/specs/をご覧ください。

ネットワークデバイス

Eclypsiumは、Arista、Cisco、Citrix、Extreme Networks、F5、Fortinet、HPE Aruba、Juniper、Palo Alto Networks、Pulse Secureなどのベンダーのルーター、スイッチ、ゲートウェイ、VPNアプライアンス、セキュリティアプライアンス、その他の製品を幅広くサポートしています。

対応アセット・タイプ_

- Intel CoreおよびCore Mベースのシステム、第2世代以降
- Intel Xeonベースのサーバー
- Intel Atomベースのシステム
- AMD Zenベースのシステム
- Apple M1、M2

サポートされるハードウェアの詳細については、eclypsium.com/platform/specs/をご覧ください。

サード・パーティー製品との統合_

アドホックな統合を可能にする強力なREST APIに加えて、以下の製品との統合がテスト済みです：

展開、インストール	さらなる可視化と分析
• *Airwatch (VMWare)* • *Microsoft SCCM* • *JAMF* • *Tanium* • *Microsoft Intune*	• *インテル・インテリジェンス・フィード*

システムへのアクセスと認証	セキュリティ分析
• *Cloudflare Access* • *Ping Identity* • *Okta* • *Google SSO*	• *Kenna Security* • *Splunk*

デプロイメント_

Eclypsium Analytics Service は SaaS であり、クラウドインスタンス上で動作します。必要に応じてオンプレミスでの導入も可能です。

データの収集_

Eclypsiumサプライチェーンセキュリティプラットフォームは、デバイスを監視し、修復するためのいくつかの方法を提供します。

Eclypsiumエンドポイントセンサー

Eclypsiumエンドポイントセンサーは、クライアントとサーバーに対して堅牢なモニタリングと修復オプションを提供します。このセンサーは、カーネルドライバーを使用してシステムデータを収集し、暗号化された認証チャネルを介してクラウド分析サービスにメタデータを送信します。このセンサーはまた、実行中のシステム構成と動作のリアルタイム分析を行い、インプラントや疑わしい動作を検出します。

センサーは、継続的に実行されるサービス（永続的デプロイメント）または一時的に実行されるアプリケーション（エフェメラルデプロイメント）の2つのモードでデプロイできます。センサーには複数の設定オプションがあり、展開の柔軟性とスキャンの深さと速度のトレードオフを可能にします。エフェメラルデプロイメントは、ランタイムの相互作用を避けるために、ブート中に実行することもできます。

リモートスキャン

Eclypsiumは、ネットワーク機器やサーバーなどのインフラデバイスをリモートスキャンする方法も開発しました。Eclypsiumは、認証済みまたは未認証のリモートインターフェース（SSH、Redfish、vSphere APIなど）を使用して、サポートされているインフラデバイスのデータを収集し、修復を実行します。