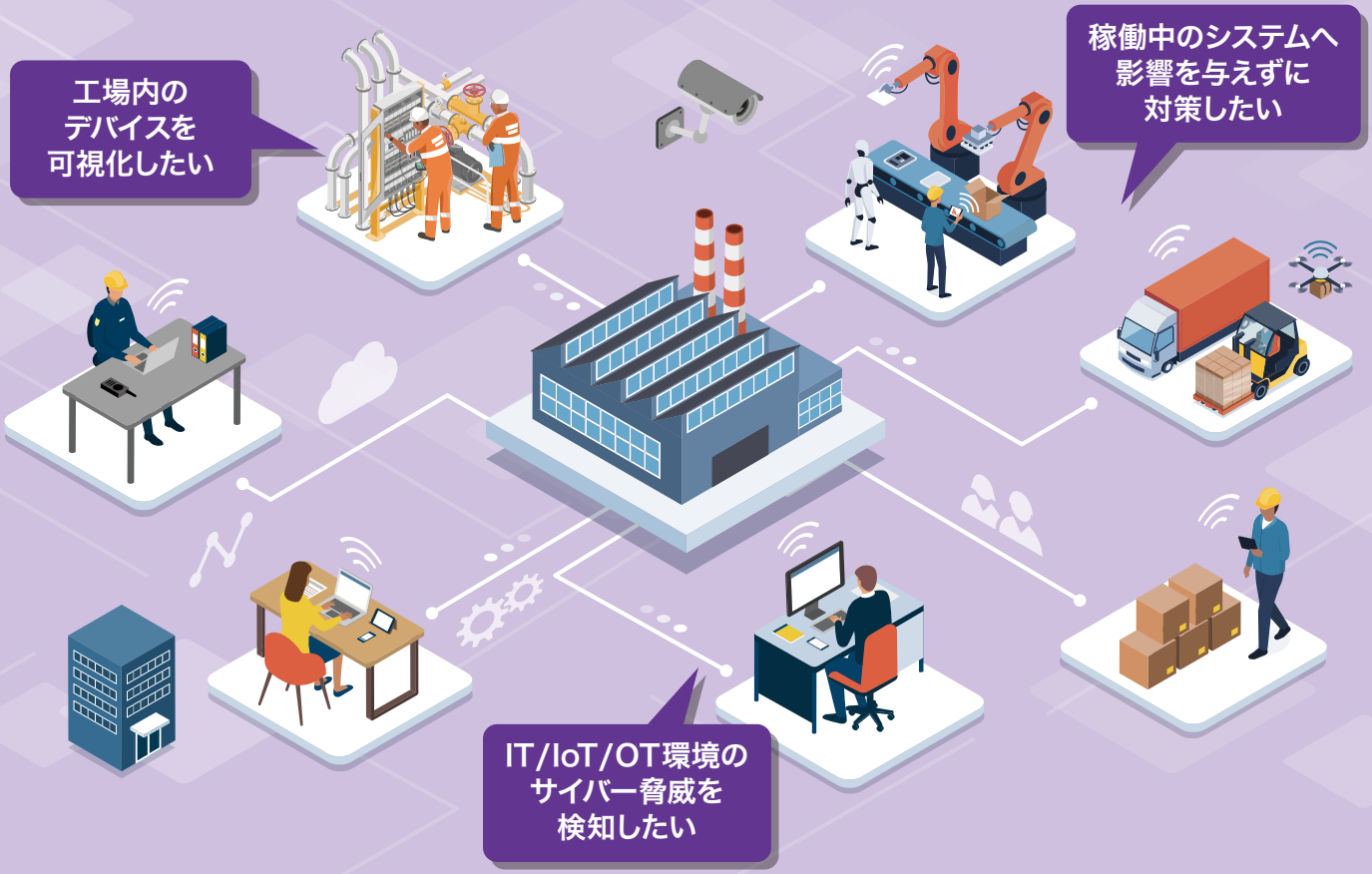
HITACHI
Inspire the Next

IT / IoT / OT 向け
Armis社のセキュリティプラットフォーム



IT / IoT / OT のさまざまデバイスを可視化し、サイバーリスクを包括的に管理

POINT 1 2,500万以上のデバイスを識別可能*

デバイスのメーカーやOSのバージョン、プロトコルなどの詳細情報を含む独自のデータベース（デバイスプロファイル）との照合により、デバイスを識別。独自のプロトコルにも幅広く対応し、把握できていないデバイスも含めネットワーク内のさまざまなデバイスを可視化します。

*2023年11月時点

POINT 2 エージェントレスでOTシステムの安定稼働を妨げないシンプルな導入

対象のデバイスにエージェントソフトウェアのインストールは不要。Windows以外のOSが使用されているOT/IoT機器がある環境へも導入いただけます。ネットワークにつなぐだけのシンプルな導入で、可用性が重視されるOTシステムの安定稼働への影響を最小限に抑えます。

POINT 3 組織全体で包括的・効率的にサイバーリスクを管理

クラウド上にある解析エンジンが随時新しい脆弱性情報を取り込むことで、最新のサイバー脅威を検知可能です。IT/OT/IoTを区別せず、組織内のネットワークに存在するデバイスに関連するサイバー脅威を包括的に可視化します。脅威情報はクラウド上で共有されるため、複数の部門や拠点間で連携し効率的に対応可能です。

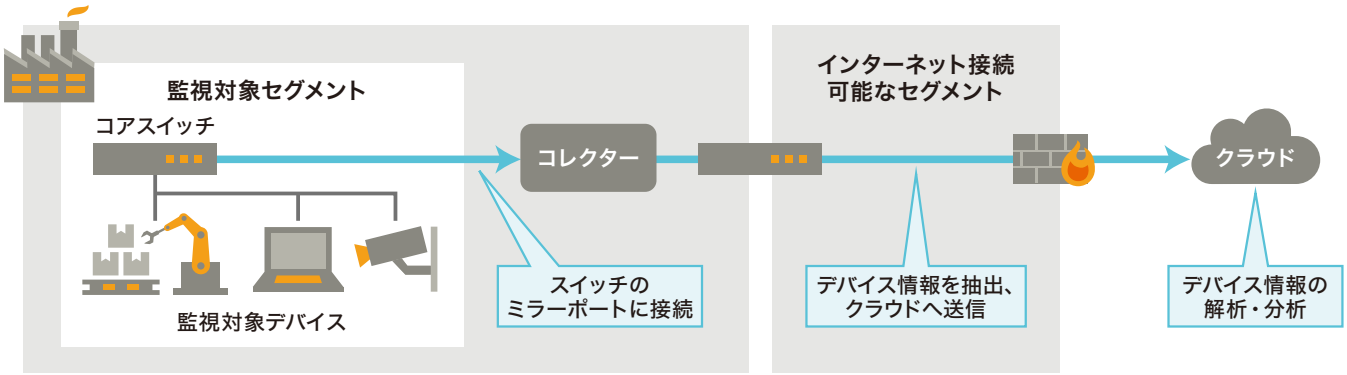
株式会社 日立ソリューションズ

主な機能

デバイス識別		世界中の35億を超えるデバイスをトラッキング。デバイスの識別情報や通常時の挙動を機械学習・蓄積したデバイスプロファイルを備えており、2,500万以上のデバイスを識別可能です。
	OT/IoTデバイス	SCADA、PLC、DCSなどのOTデバイスや監視カメラ、ハンディスキャナ、プリンターなどのIoTデバイスに幅広く対応しています。
	メディカルデバイス	ナースコールシステム、輸液ポンプ、MRI、CT、X線など、さまざまな種類の医療機器、臨床資産に対応しています。
デバイス(資産)可視化		パケット情報などを解析し、ネットワーク内にあるデバイスのメーカー名、型番、OS、ファームウェアバージョンなどを自動識別し、デバイスを可視化します。
通信可視化・脅威検知		脆弱性を悪用した通信やマルウェア感染の可能性がある通信、類似デバイスと比較した異常な挙動など不審な通信を検知し、管理者に通知します。

導入イメージ

監視対象デバイスが接続されているスイッチのミラーポートにコレクターを接続すると、各デバイスの情報を自動抽出し、クラウドへ送信。クラウド上にある独自のデータベースと照合し、デバイス情報を解析・分析します。



日立ソリューションズの強み

セキュリティに精通した技術者による導入前・導入後の支援はもちろん、お客さまの課題に合わせた
セキュリティ関連商品との連携ソリューションをトータルに提供しています。

◆ 導入前・導入後支援 ＊別途費用が発生します。詳しくはお問い合わせください。

導入前	導入前の運用検討支援	導入後に重要となる効果的な運用について、導入前から検討を支援
	現地導入作業	ネットワークおよびセキュリティに詳しい技術者が導入作業を実施
導入後	アラートレポート作成	検知したアラートの詳しい情報や対処方法のわかりやすいレポートを提供
	導入後のアラートチューニング支援および資産管理支援	アラートの優先順位や対象となるデバイス、アクティビティのチューニングを支援

◆ 連携ソリューションのご提供 ＊連携可能な製品・サービスについてはお問い合わせください。

各種ネットワークセキュリティ製品と連携し、不正なデバイス接続の遮断や不審な通信を行うデバイスをネットワークから切り離すといったインシデント対応を行うソリューションを提供しています。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/device_security/

S23S-02-00 | 2024.01