# MSSPやMDRに最適！

# 最新のAIと機械学習を用いたリアルタイムICSサイバーセキュリティ可視化ソリューション！

Gartner Cool Vendor 2017

テクノロジーアライアンス（一部）

IBM / Hewlett Packard Enterprise / Check Point SOFTWARE TECHNOLOGIES LTD. / FORTINET / FireEye / paloalto NETWORKS / splunk>

- 最高クラスのソリューションを使用してサイバー脅威をすぐに検出&追跡
- リアルタイムの見識を用いてICSのネットワーク及びプロセスを迅速に監視
- ICSサイバーセキュリティの脅威及びリスクに効率的に対応
- 優れたトラブルシューティング及びフォレンジックサービスを提供
- 柔軟なアーキテクチャを用いてカスタムのソリューションを容易に実装
- OT向けに設計されたソリューションを自信を持って使用

重要インフラおよび製造の組織に対するサイバーセキュリティリスクが高まるにつれて、企業がOTネットワークを積極的に監視・保護することがこれまで以上に重要になっています。

このニーズに応えるのを支援するために、MSSP(Managed Security Service Provider:マネージド・セキュリティ・サービス・プロバイダ)及びMDR(Managed Detection and Response:マネージド・ディテクション・レスポンス)ベンダは、産業ネットワークを網羅するマネージドITサービスを拡張しています。但し、そうすることは、既存のツールやプラクティスを産業制御システム(ICS)に拡張することだけではありません。

この市場に効率的にサービスを提供するには、可用性が機密性または完全性よりも重要な懸念事項であることが多い、24時間365日運用するシステムを管理するという独自の課題を理解する製品が必要です。

更に、多くの場合、**ICSはレガシーシステムを含み、安全ではない産業プロトコルを使用**しており、これらは何れも、ITソリューションを使用して監視・管理することができません。

Nozomi Networksは、産業ネットワークやプロセスを徹底的に理解しているので、マルチテナントICSサイバーセキュリティ及び可視性ソリューションの理想的なプロバイダです。Nozomi Networksのテクノロジーは完全にパッシブであり、影響を受けやすい制御ネットワーク向けの最も安全で最も効果的なソリューションを実現します。

＊世界の産業MSSP/MDRがNozomi Networksのソリューションを選択する理由についてはnozominetworks.com/contactにご連絡ください。

## ● 柔軟でスケーラブルなアーキテクチャ

- 共有インフラを用いたサービス提供を強化するように設計されたマルチテナントアプリケーション
- 柔軟な導入オプション
- 使い易いオープンAPI
- 多種多様なアプライアンス

## ● 高度なICS脅威検出

- 最高クラスのICS脅威検出
- ルール及びシグネチャベースの脅威検出
- 挙動ベースの異常検出
- 脅威追跡のための複数のツール
- AIによる迅速で正確な解析

## ● すぐに利用できる脅威&プロセス・インテリジェンス

- 直観的なネットワーク可視化
- 脅威、資産及び通信のリアルタイム監視
- カスタマイズ可能なダッシュボードやアラート
- 自動パケットキャプチャ
- アラートをインシデントにスマートグループ化
- リアルタイムのアドホッククエリツール

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

## マネージドOTセキュリティサービスを強化するためにNozomi Networksを選択する理由

### ● 柔軟でスケーラブルなアーキテクチャ

Nozomi Networksのソリューションを使用して、クライアントのサイバーセキュリティリスクを低減します

- 数千の産業拠点にわたってサイバーセキュリティ可視性を一元管理します
- 複数のアプライアンス・フォーマット及びICSデータの柔軟なアグリゲーションを用いて各クライアントの事業に適合するように導入します
- フルスタック技術を所有することにより、最適な性能を提供します

### ● IT/OT環境との容易な統合

- SIEM、ファイアウォール及びユーザ認証システムとのビルトイン統合を利用します
- オープンAPIを介して他のアプリケーションとデータを統合・交換します
- 数十のIT/ICSプロトコルをサポートし、プロトコルSDKによって他のプロトコルまで拡張します
- 他のアプリケーションで解析・提示するためにデータをエクスポートします
- 多くのカスタマイズ可能なコンポーネントを用いてクライアント毎に適応します

### ● 高度なICS脅威検出

Nozomi Networksの高度な脅威検出は、下記を組み合わせます。

- 最高クラスの挙動ベースの異常検出
- ルール及びシグネチャベースの脅威検出
- AI解析

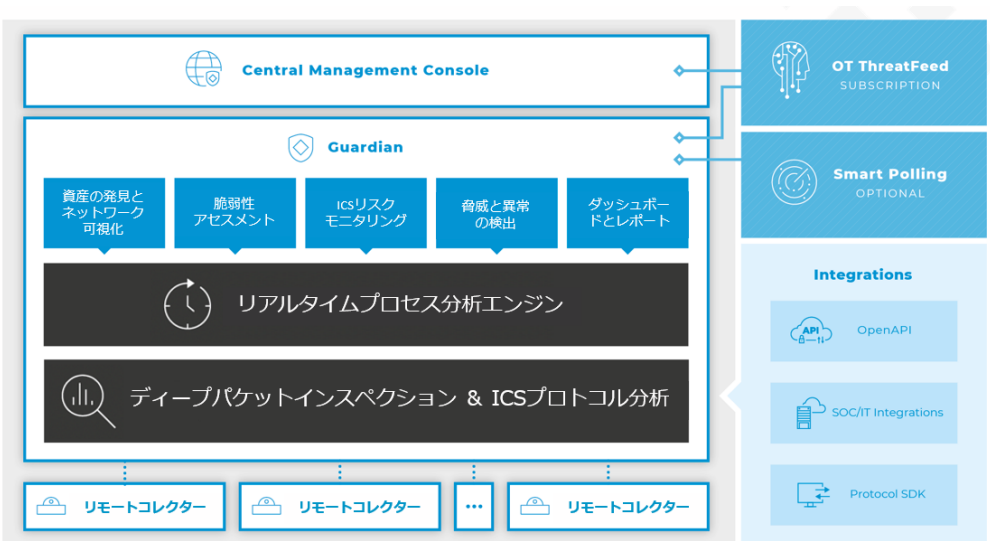
### ● 特定される脅威およびリスクの例としては下記が挙げられます。

- 侵入: スキャン及びMITM攻撃・複雑な攻撃、又はゼロデイ攻撃・持続的標的型攻撃・既知のマルウェアファイル/パケットなど
- 不正な挙動: リモートアクセス・設定変更・ダウンロードなど
- 懸念すべき状態: 複数の変数を伴うクリティカルな状態・弱いパスワード・更新の未実行・開いているポート・デバイスの脆弱性など

### ● 高度なICS脅威検出

- カスタムアサーション(ルール)がネットワークステータスまたはプロセスステータスの任意の側面をチェックします
- 関連するアラートが根本原因インシデントにグループ化されます
- 自動パケットキャプチャが解析を迅速化します
- TimeMachine™が2つの異なる時点のスナップショットを比較しICSネットワーク全体の変更を可視化します

## Nozomi Networksのソリューションアーキテクチャ




- ディープパケットインスペクション&プロトコル解析 - 安全ではないICS通信をOSIモデルの7つの全レイヤにおいて評価します
- リアルタイムプロセス解析エンジン - 信頼性に影響を及ぼす可能性がある高度なマルウェアアクティビティ及びクリティカルな状態の指標であるプロセス制御変数を解析します
- Guardian - セキュアなアプライアンスとしてクライアントの産業ネットワークに導入し、トラフィックをパッシブに解析します
- 中央管理コンソール(CMC) - ICSの可視化、及びすぐに利用できる脅威インテリジェンスをMSSP/MDR SOCに提供します
- 統合 – セキュリティインフラとの容易な統合を可能にします

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

## クライアントがNozomi Networksのソリューションを望む理由

### ● パッシブで導入が容易なソリューション

- SPANポート、又はミラーポートを介してネットワークデバイスに接続することによって、パッシブにインストールします
- ネットワークを変更することなしに容易に導入します
- 様々なGuardianアプライアンスにより、クライアント設備に適合します

### ● 脅威およびリスクの迅速なリアルタイム監視

- 機械学習、及び人工知能を使用して、クライアントの大規模な異種ICSを自動的に学習・モデル化します
- 脅威、ICSプロトコル通信、資産、及びプロセスをリアルタイムで監視します
- 学習モードから保護モードに自動的に切り替える(動的学習)ことで、MSSPおよびMDRが保護サービスの提供を迅速に開始することを可能にします

### ● 実績のある大規模な導入

- 現在、大手の重要インフラ、プロセス制御、製造の組織においてサイバーレジリエンスを強化しています
- 数百のクライアント拠点まで拡張します

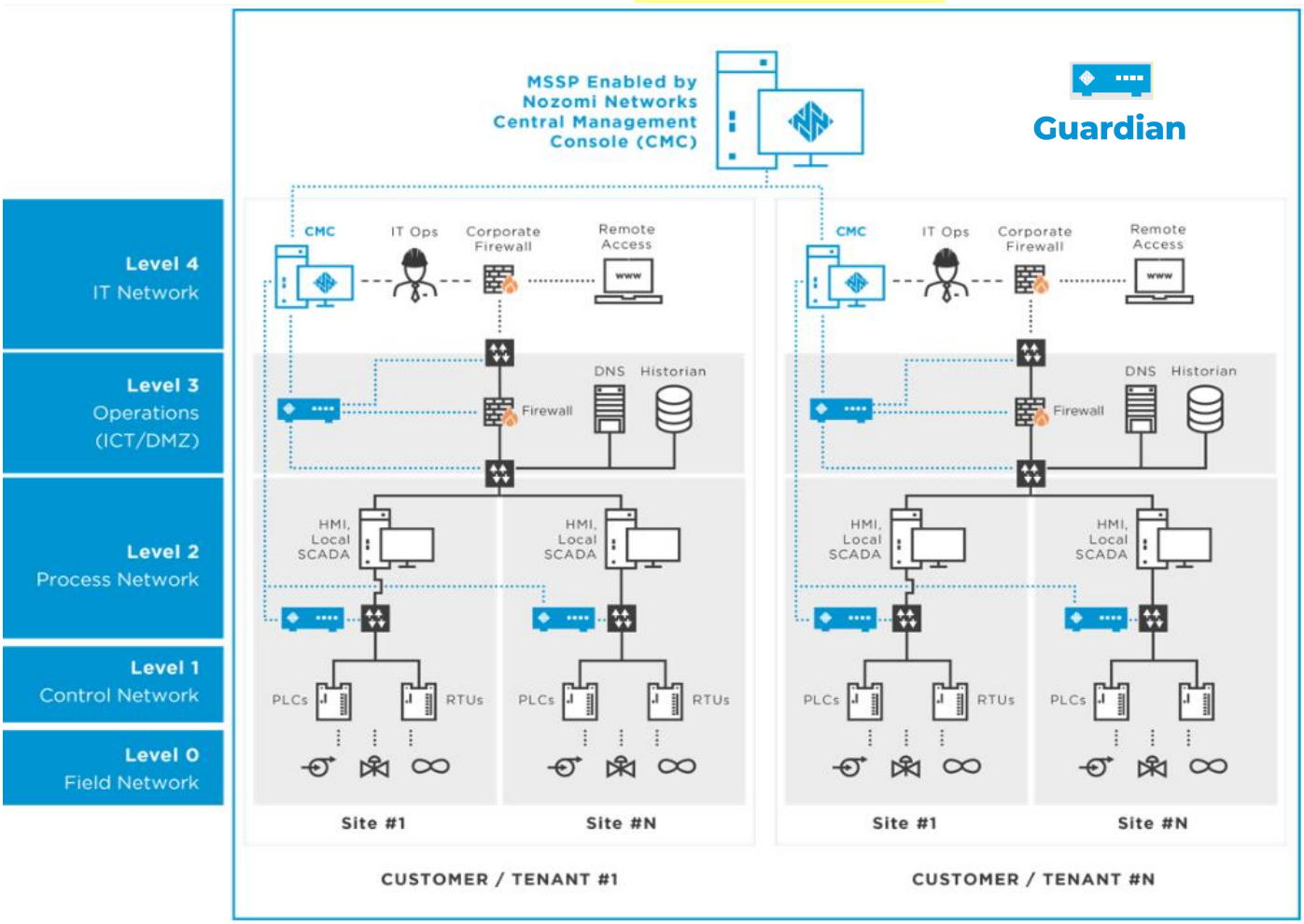
### ● 改善された信頼性および可用性

- ICSオペレータの主要な懸念事項(サイバーインシデントに起因する信頼性の低減)に対処します
- サイバーリスクだけではなく、可用性を下げる可能性があるプロセス異常(正常に動作していない機器など)も特定します

### ● 今後は信頼できるパートナーがICSリスクに対応

- 信頼できるMSSPまたはMDRプロバイダがITセキュリティサービスとICSセキュリティサービスの両方を提供するのを可能にすることによって、ICSサイバーセキュリティの課題を解決します

### ● 導入アーキテクチャの例




コーネットソリューションズ株式会社
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

# Guardian

NOZOMI NETWORKS

## ● Nozomi Networksの製品

・Guardian は、産業制御ネットワークのリアルタイムのサイバーセキュリティと運用の可視性を提供します。Guardianはクライアントの産業ネットワークにパッシブに導入され、ローカル、又はCMCを介してリモートでアクセスすることができます。

・中央管理コンソール（CMC）は、集中型の遠隔ICSサイバーセキュリティ及び監視をMSSP/MDR SOCに提供します。CMCは、最大で数千台のGuardianアプライアンスのデータをアグリゲートするセキュアなマルチテナントアプリケーションです。

## ● あらゆるタイプの導入に対応する複数のGuardian™アプライアンス




| Guardian | NSG-M 1000 | NSG-M 750 | NSG-L 250 | NSG-L 100 |
|---|---|---|---|---|
| 説明 | ハードウェアアプライアンス<br>リアルタイムでの産業用ネットワークの可視化、サイバーセキュリティ、監視用のラックマウント型アプライアンス | | | |
| フォームファクター | 1 Rack Unit | 1 Rack Unit | 1 Rack Unit | 1 Rack Unit |
| モニタリングポート数 | 7 RJ45 + 4 SFP | 7 RJ45 + 4 SFP | 5 RJ45 | 5 RJ45 |
| 拡張スロット* | 1 | 1 | 1 | 1 |
| 最大プロテクトノード数 | 40,000 | 10,000 | 5000 | 1000 |
| 最大スループット | 1 Gbps | 1 Gbps | 500 Mbps | 250 Mbps |
| 最大リモートコレクター数** | 50 | 50 | 20 | 20 |
| ストレージ | 256 Gb | 256 Gb | 64 Gb | 64 Gb |
| H x W x L<br>mm/in | 44 x 429 x 438<br>1.73 x 16.89 x 17.24 | 44 x 429 x 438<br>1.73 x 16.89 x 17.24 | 44 x 438 x 300<br>1.7 x 17.2 x 11.8 | 44 x 438 x 300<br>1.7 x 17.2 x 11.8 |
| 重量 | 14 Kg | 14 Kg | 8 Kg | 8 Kg |
| 最大消費電力 | 360W | 360W | 250W | 250W |
| 電源タイプ | 100-240V AC 50/60Hz | 100-240V AC 50/60Hz | 100-240V AC50/60Hz | 100-240V AC 50/60Hz |
| 対応温度範囲 | 0 / +45 º C | 0 / +45 º C | 0 / +45 º C | 0 / +45 º C |

* 拡張スロットで、RJ45 4ポートあるいはSFP 4ポートを追加可能。
** 詳細はリモートコレクタ技術仕様をご覧ください。

## ●仮想のマルチテナントCMCは導入が容易でスケーラブルです

| 概要 | MSSP及びMDR向けマルチテナントICS可視性、及びすぐに利用できる脅威インテリジェンス | | |
|---|---|---|---|
| インストール仕様 | AWS EC2、Hyper-V 2012以上、KVM 1.2以上、VMware ESX 5.x以上、XEN 4.4以上 | | |
| 管理対象アプライアンスの最大数 | 無制限(*) | ストレージ | 100Gb以上 |
| 更新 | 脆弱性、ルール、**Guardian**の更新を行う場合は、Nozomi Networksのカスタマーポータルに任意選択で接続します。現場のすべてのアプライアンスに変更を容易に適用します。 | | |

(*) インフラに基づきます：最新の技術仕様についてはnozominetworks.comをご覧ください。

## ● Nozomi Networksについて

本社をカリフォルニア州サンフランシスコに置くNozomi Networks は、リアルタイムのサイバーセキュリティと運用の可視性を提供する最も包括的なプラットフォームによって、産業制御システム(ICS)サイバーセキュリティに大変革をもたらしています。

2013年以来、Nozomi Networksは、重要インフラの運用を保護するために機械学習および人工知能の使用を取り入れています。
ICSを標的とする脅威が増大する中で、Nozomi Networksは、リアルタイムのICS監視、ハイブリッドの脅威検出、プロセス異常検出、産業ネットワーク可視化、資産インベントリ、脆弱性評価を備えた統合ソリューションを提供しています。

Nozomi Networksの製品は既に世界最大級の産業施設に導入されており、顧客は高度なサイバーセキュリティ、改善された運用の信頼性、強化されたIT/OT統合の恩恵を受けています。 詳細はwww.nozominetworks.comをご覧ください。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp