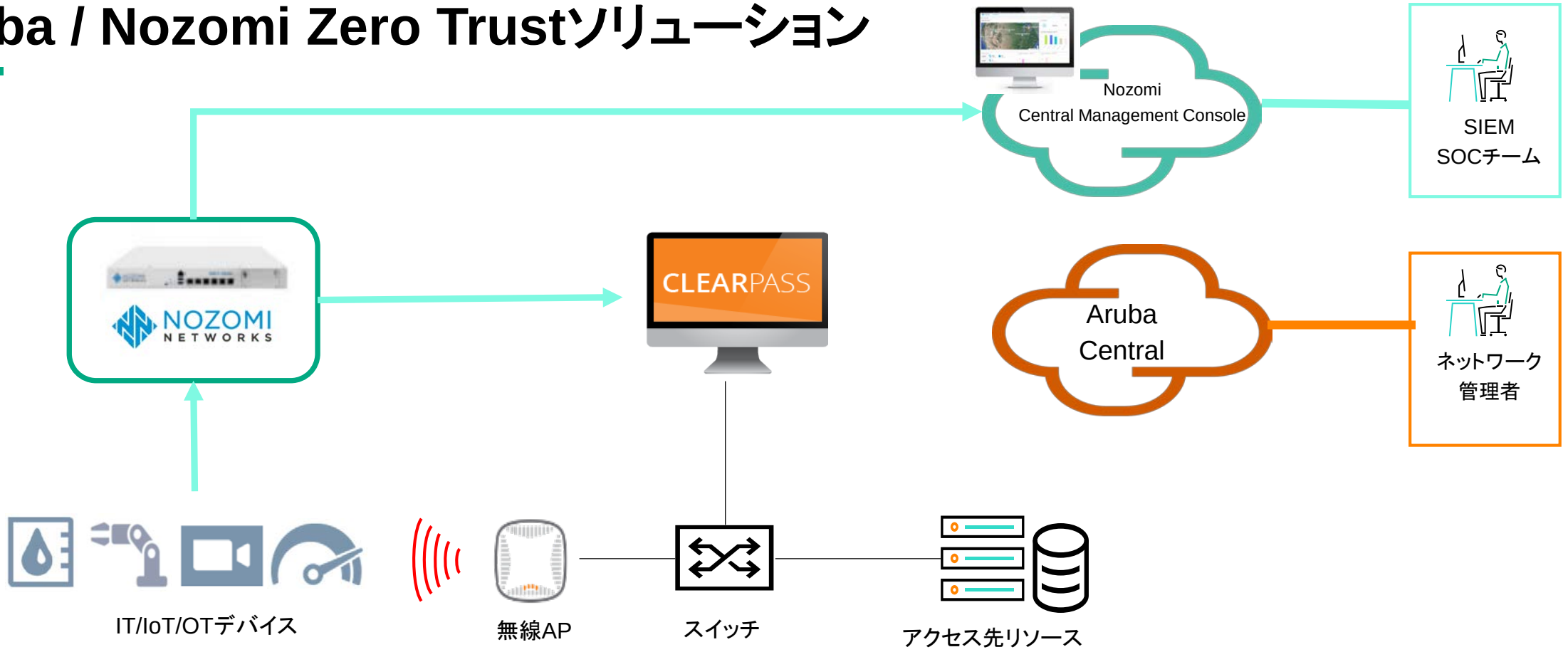
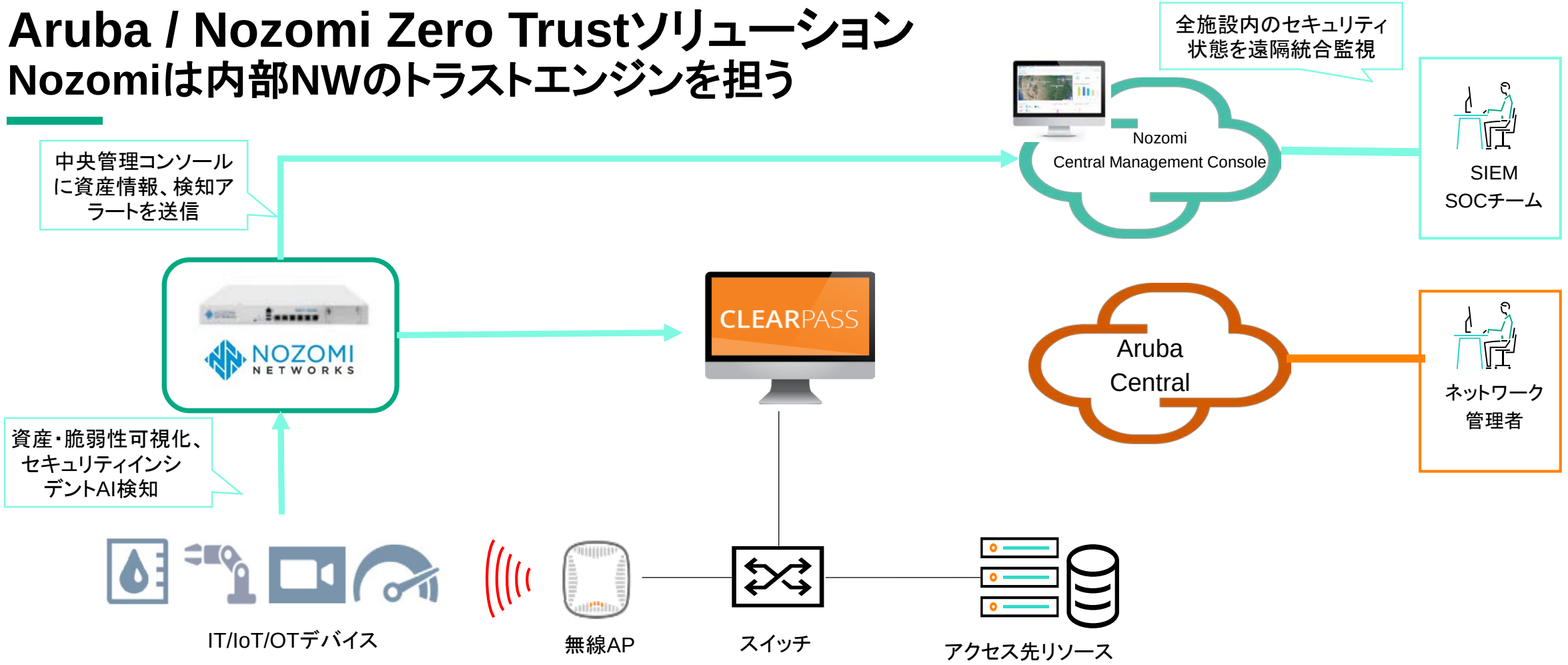
Nozomi GuardianとHPE Aruba連携ソリューション

IoT/OTのゼロトラストセキュリティーアーキテクチャの実装

Aruba / Nozomi Zero Trustソリューション



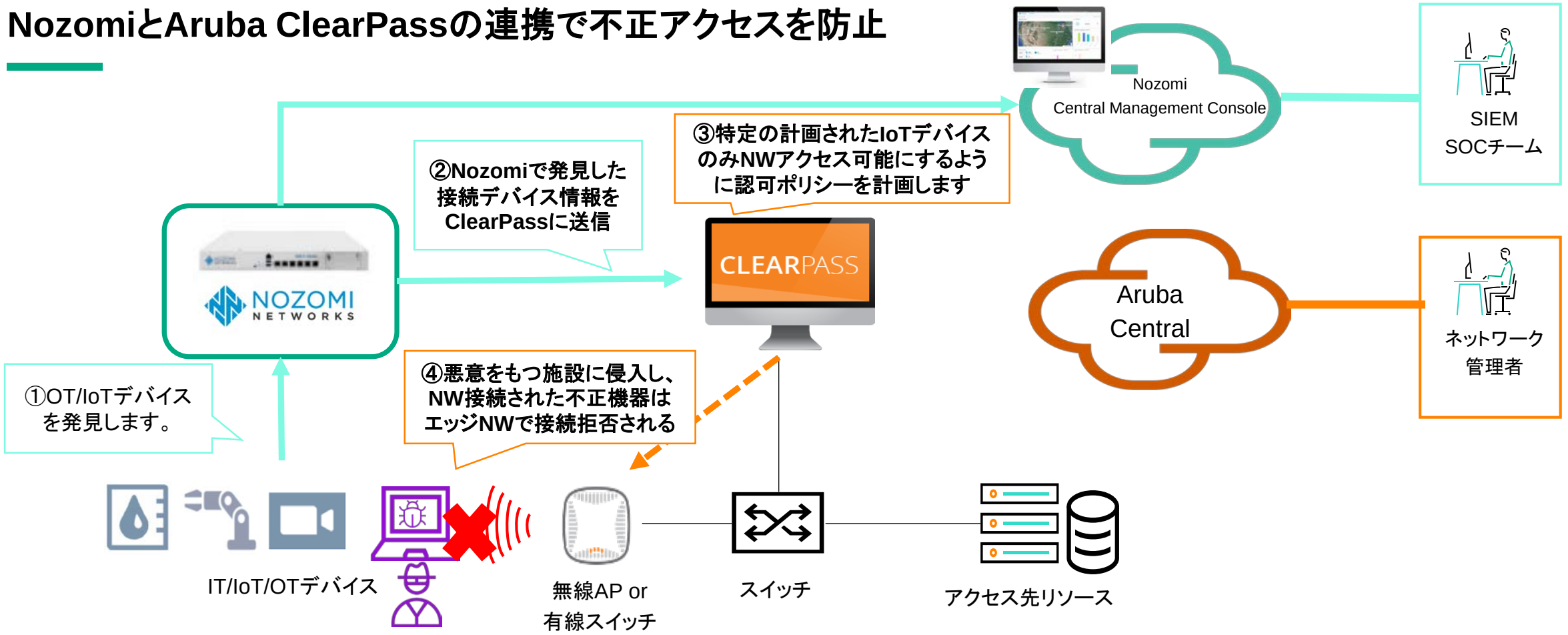
Aruba / Nozomi Zero Trustソリューション
Nozomiは内部NWのトラストエンジンを担う



- **Nozomi Guardian**はビル・工場内の資産・脆弱性をリアルタイムに可視化し、AIによりセキュリティインシデントを検知
- Central Management Consoleより全施設を統合管理できます。
- CMCからSOCチーム（SIEM）がインシデント対応策を検討に活用できます。

Aruba / Nozomi Zero Trustソリューション

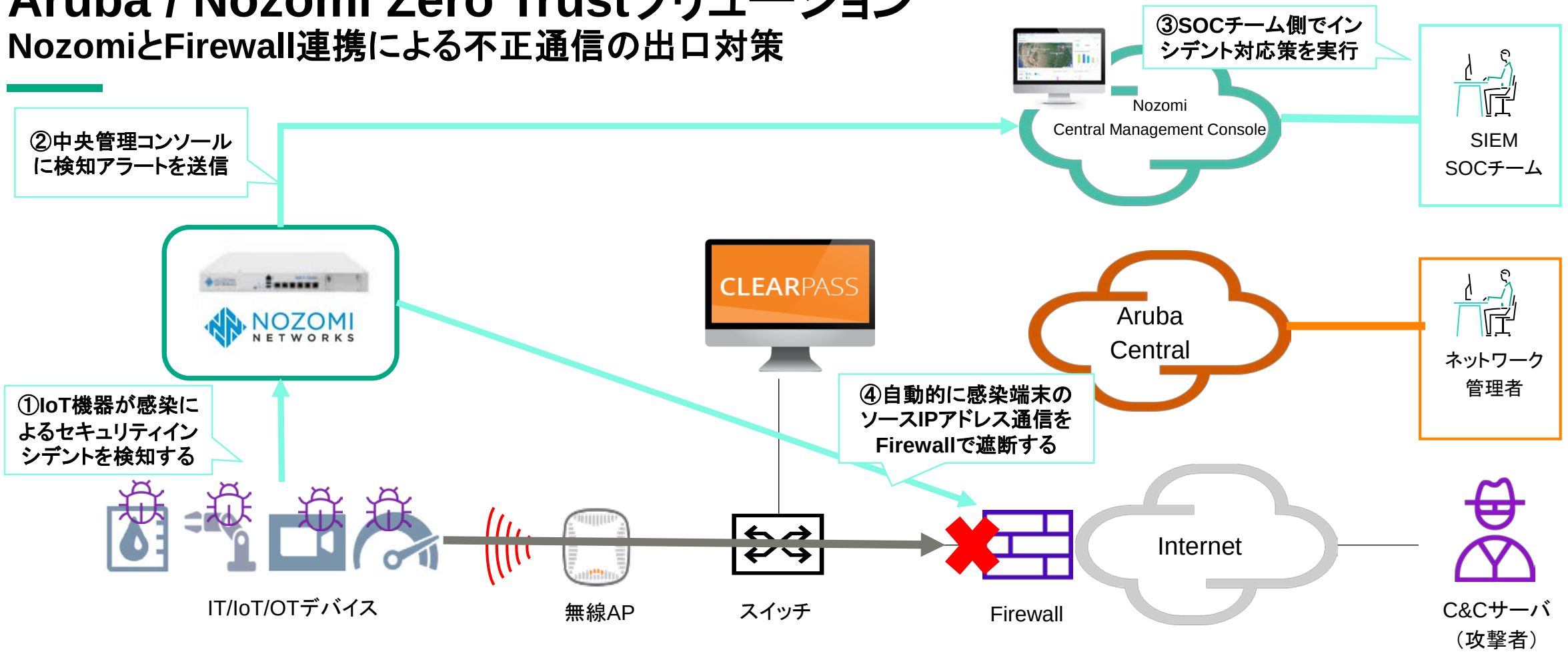
NozomiとAruba ClearPassの連携で不正アクセスを防止



- **Aruba ClearPass**はNW認証認可ポリシーを決定するポリシーエンジンです
- NW認証認可ポリシー計画に**Nozomi Guardian**から取得したOT/IoTデバイス情報を利用することができます
- ネットワーク管理者またはセキュリティ管理者がIoT/OTネットワークアクセスポリシーを定義します。（特定のSiemens製品は許可、それ以外は拒否等）
- 計画にない不正な端末のNW接続をエッジネットワークで遮断することができます

Aruba / Nozomi Zero Trustソリューション

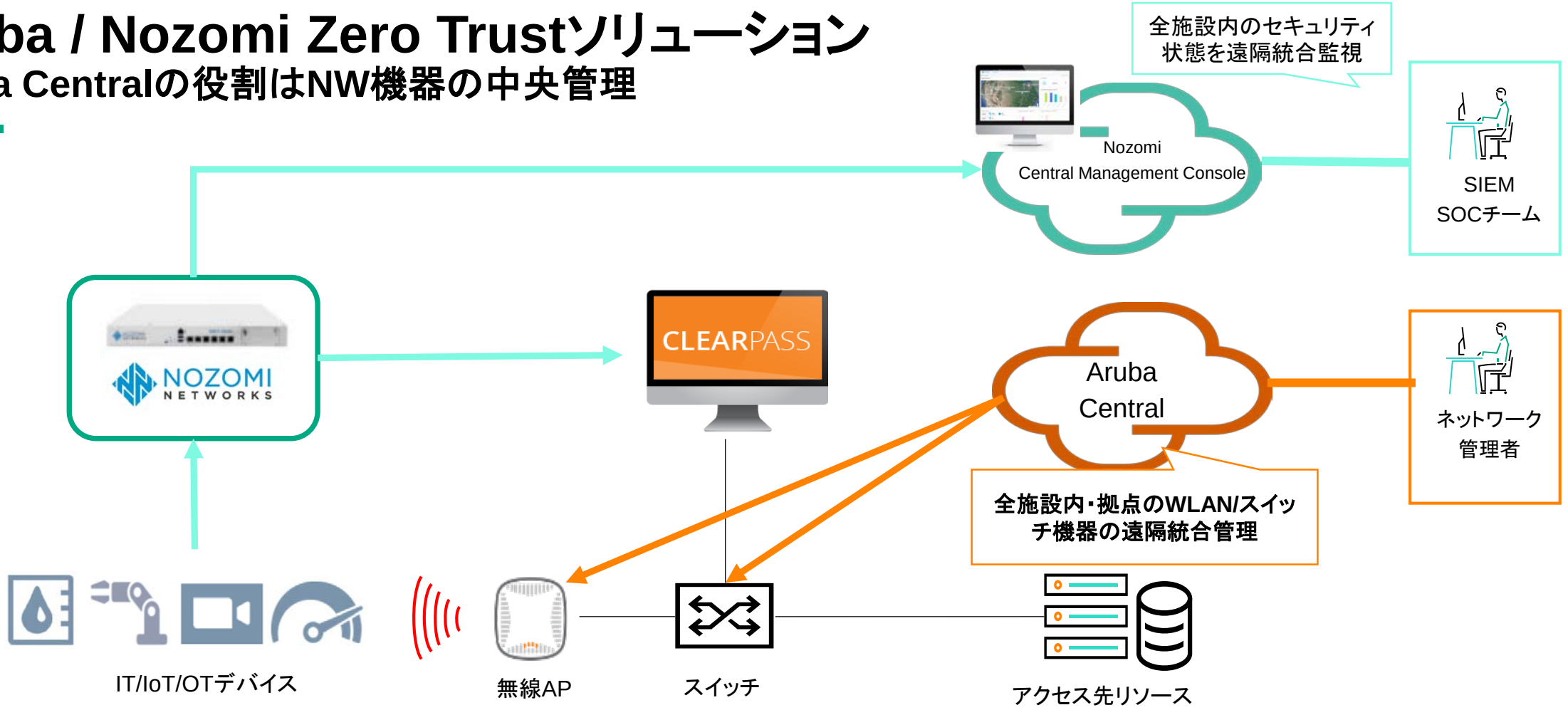
NozomiとFirewall連携による不正通信の出口対策



1. **Nozomi Guardian**のAIによりセキュリティインシデントを検知しSOCチームがインシデント対応策を検討します。
2. 動的にNozomiよりFirewall（Paloalto/Fortigate等）に感染端末情報を連携、通信を遮断する

Aruba / Nozomi Zero Trustソリューション

Aruba Centralの役割はNW機器の中央管理



- **Aruba Central**はNW機器の管理監視、WLAN機器の管理監視、無線センサーからのロケーション情報、SD-WAN（将来）を一元管理するクラウドサービスです。
- ネットワーク管理者が利用します
- SOCチームからの要請に必要に応じ、特定ノードのNW通信の遮断設定を遠隔から行うことがあります

NIST-SP 800-207 “Zero Trust Security Architecture”における定義

ポリシーエンジンで決定したポリシーを実行する
対象からリソース間通信を確立したり遮断したりする指示コマンドをPEPに命令する
企業リソースにアクセスするために利用される認証トークンやクリデンシャルを生成する

外部のデータソースからトラストアルゴリズムにインプットして、リソースへのアクセスを許可・拒否、変更する。
ポリシーエンジンはログを生成し、ポリシーを決定する。

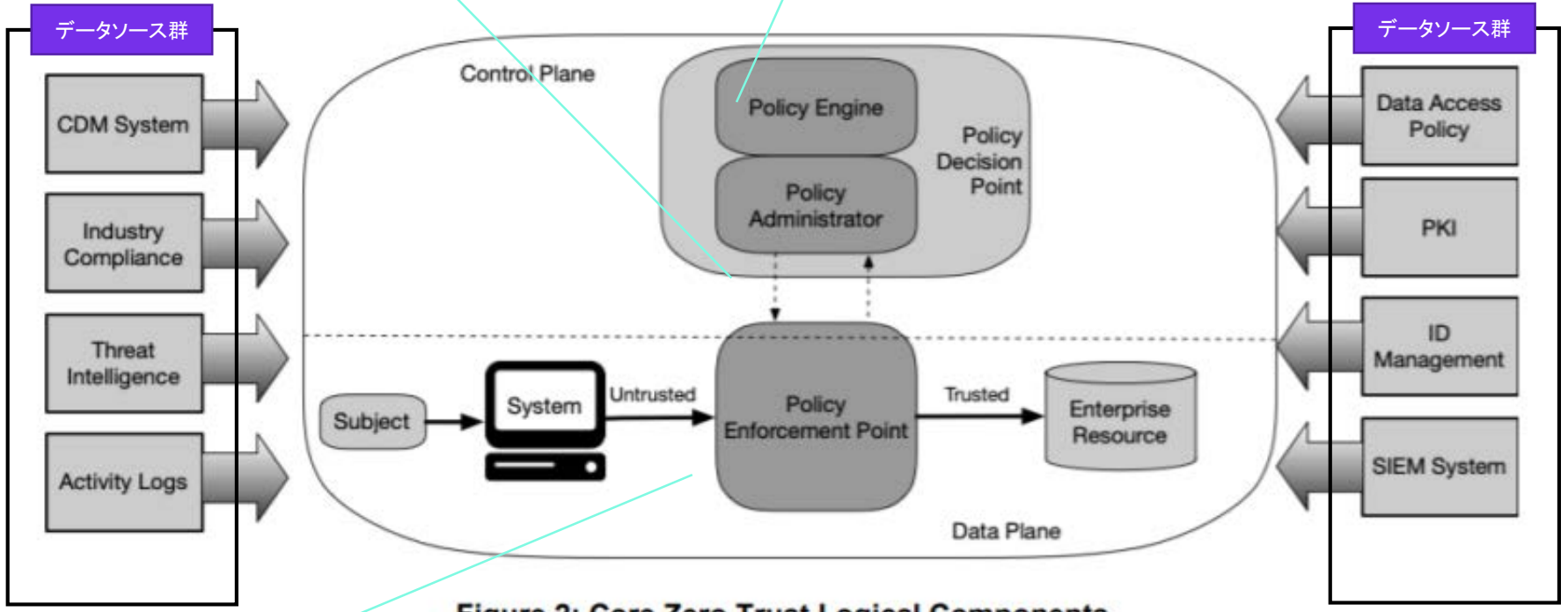


Figure 2: Core Zero Trust Logical Components

企業リソース間の接続を有効化したり監視したり、遮断したりする
PAにリクエストを送信する、PAからポリシー更新を受け取る
2つに分解して考えらる
クライアントサイド（エージェントソフト）
リソースサイド（ゲートウェイ）またはシングルポータル（ゲートキーパー的な）

<参考> https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

ゼロトラストセキュリティアーキテクチャ視点における製品の位置づけ

NIST-SP 800-207のゼロトラストセキュリティアーキテクチャにおいて、ご提案製品をマッピングします。

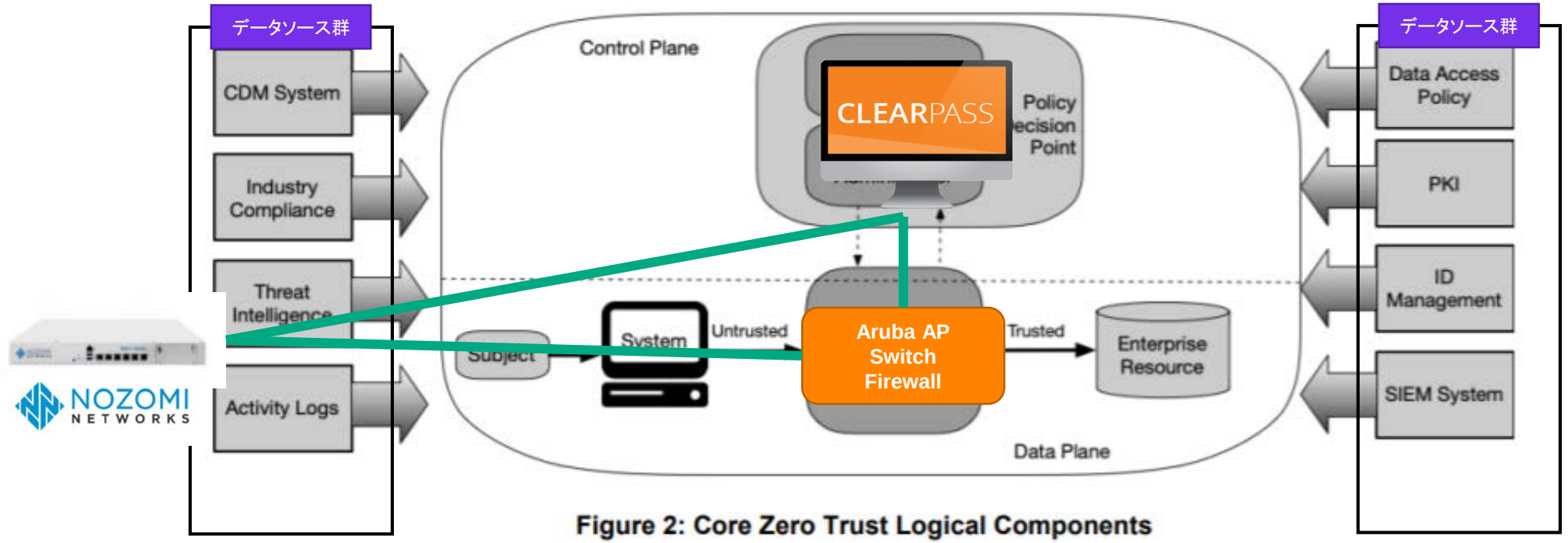


Figure 2: Core Zero Trust Logical Components

THANK YOU