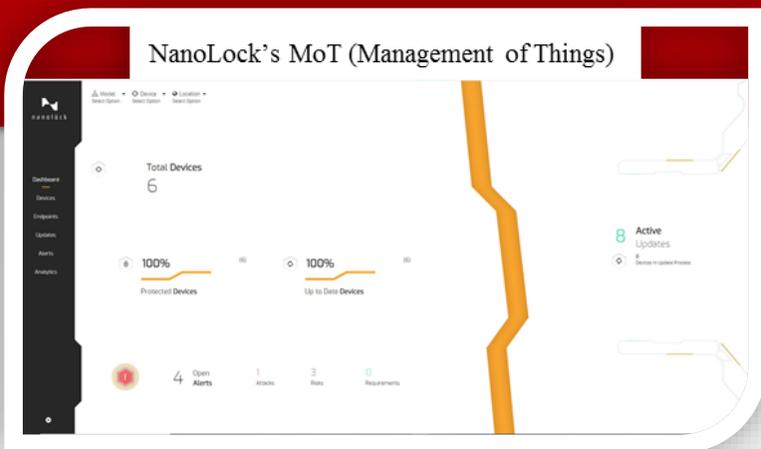


NanoLock Security

nanolock

分野: サイバーセキュリティ、デバイスレベル、ゼロトラスト



NanoLockのゼロトラスト(すべての通信を信用しないことを前提にさまざまなセキュリティ対策を講じる)でデバイスレベルのセキュリティ保護によって、コネクテッドデバイスや産業機器の運用性を維持し、収益を守ることで、事業の継続性を保持することができます。

- サイバーイベントであろうと、ヒューマンエラーであろうと、デバイスや機器レベルで重要なコードやデータを不正に改ざんされることを未然に防ぐことができます。
- スマートメーター、産業機器、センサー、EV充電器、RTU(リモート端末装置)などのコネクテッドデバイスを、アウトサイダー・インサイダー・サプライチェーン上でのサイバーイベント・技術者のミス等から守ります。

NanoLockは、日本、イタリア、スペイン、スイス、オランダ、インド、シンガポール、アメリカ、イスラエルの主要な公益事業者、生産企業、大規模エコシステムパートナーと協業しています。

社会が抱える問題とその解決策

公益事業や工業生産におけるサイバー攻撃の脅威は、高度性、複雑さ、影響力の点で高まり続けており、コネクテッドデバイス・機器は最終的に侵害されてしまいます。

- 侵害されたデバイスや機器は、サービス運用性や収益を損ない、お客様・従業員・一般の人々の安全を脅かすこととなります。
- そのため、公益事業者や生産企業は、デバイスが設計・設定・校正通りに動作していることを常に確認する必要があります。

NanoLockは、必ずデバイスを意図したとおりに動作させます。 NanoLockのゼロトラストでデバイスレベルの保護機能は、産業機器の動作運用性を担保し、収益源とビジネスの継続性を確保します。NanoLockソリューションは、アウトサイダー・インサイダー・サプライチェーン上でのサイバーイベント・技術者のミス等複数の攻撃ベクトルに対して防御するよう設計されています。

自社・製品の強み

- デバイス・機器レベルで重要なコードやデータが不正に改ざんされることを防止します。
- インサイダー、サプライチェーン上の改ざん、さらにはヒューマンエラーも防止します。
- パフォーマンスや機能への影響はありません。必要な電力はほぼゼロです。
- 旧型、新型、電動、バッテリー式など、あらゆる機器に適用可能です。

ビジネスモデル

保護するデバイスごとの年間サブスクリプションモデルで、次の2つのライセンスタイプに基づきます。

- ライフタイム保護と認証管理されたローカル及びリモートアップデートを提供するSTANDARDライセンス
- 詳細なアラートや独自のフォレンジックデータ、アナリティクスなど、運用コストを大幅に節約する機能を備えたADVANCEDライセンス

Hack Osakaの参加目的

- 日本企業との協業のため。
- 投資家を見つけるため。

創立年	2017
ウェブサイト	https://www.nanolocksecurity.com/
所在地	ホド・ハシャロン(イスラエル)
資金調達	1,820万米ドル(約20億6,700万円)
世界市場での実績	日本、イタリア、スペイン、スイス、オランダ、インド、シンガポール、アメリカ、イスラエルの主要な公益企業、事業法人、大規模エコシステムパートナー
日本語対応	○