

Winkermann Group

Winkermann Group、 リスク低減と監査対応に Forescoutを採用

2時間

ネットワーク環境を
2時間で完全に可視化

170%～

想定を170%上回る数の
デバイスを検出

数日単位

毎月、数日単位の
SecOps工数を削減

業種

製造業

事業環境

- ▶ 3大陸で6,800台の
有線/無線デバイスが稼働中
- ▶ 従業員数:4,300名

課題

- ▶ ネットワーク接続デバイス
(IT、IoT、OT デバイスなど)
すべてを完全に可視化
できていない
- ▶ 自動車業界のセキュリティ基準
TISAX への準拠が必要
- ▶ サイバー攻撃による
事業中断リスクを極小化したい

概要

Winkermann Group は、主に自動車、給水・暖房機器業界向けの高度な金型成型加工を専門とする多国籍メーカーです。ドイツのアーレンを本拠地とする同社は Forescout Continuum プラットフォームを導入し、欧州、アジア、北米の製造拠点ネットワークに接続する IT、IoT、OT およびその他のデバイスをグループ全体で完全に可視化しました。さらに、正確なリアルタイム資産インベントリ、デバイスの常時コンプライアンス、ネットワークアクセスコントロール (NAC) 機能も確保できたため、侵害リスクや事業中断リスクを最小限に抑制することができました。

「ネットワークアクセスコントロールと
セグメンテーション実施の大前提として、
社内ネットワークに接続中のデバイスを正確に
可視化する必要がありました」

—Winkermann Group システム・ネットワーク管理者 Niklas Kaiteer 氏

業務における課題

ドイツの自動車メーカーに義務付けられるセキュリティ基準 TISAX の認証を取得するには、NAC と ネットワークセグメンテーションを実施する必要があります。また、同社では過去にウィルス感染インシデントが数件発生し、エンドポイントやサーバーの運用が中断した経緯があります。幸い、すべて社内 IT スタッフの手で感染端末を完全復旧できましたが、こうしたサイバー攻撃や監査での指摘を受け、経営陣によってサイバーセキュリティ方針が見直され、ユーザーや資産の保護を強化する適切なソリューションに投資するという経営判断がなされました。その第一歩がネットワーク接続デバイスすべてを可視化することでした。

今回導入した セキュリティ ソリューション

- ▶ Forescout Continuum
プラットフォーム
- ▶ Forescout eyeExtend

ユースケース

- ▶ 資産インベントリ
- ▶ デバイスコンプライアンス
- ▶ ネットワーク
アクセスコントロール

導入成果

- ▶ 価値の早期実現:
ネットワーク接続する IT、IoT、
OT デバイスを 2 時間で完全に
可視化
- ▶ 正確なリアルタイム資産インベ
ントリの初回版が、わずか半日で完成
- ▶ セキュリティオペレーション
部門のネットワーク/デバイス
管理工数を 1 日あたり数時間削減
- ▶ 接続デバイスすべての
セキュリティポスチャーを常時、
自動評価して侵害リスクを極小化
- ▶ 脆弱性の検知および
修復所要時間の短縮
- ▶ ポリシー作成および適用の効率化
- ▶ エコシステム全体の連携と
ネットワークセグメンテー
ションに必要な基盤の確立

Forescout を採用した理由

Winkelmann Group は、NAC およびセグメンテーションソリューション選定における初回検討を経て、候補となるベンダーを 4 社に絞り込みました。同社のシステム・ネットワーク管理者 Niklas Kaiter 氏は、次のように述べています。「Forescout は他社製品に比べて機能群が幅広く、より包括的な可視性を得られるだけでなく、導入も簡単です。他社製品は機能性に乏しい、複雑すぎて実装に時間がかかる、などの欠点がありましたが、Forescout Continuum プラットフォームは柔軟性が非常に優れていました。直感的なダッシュボードで簡単にデータを深掘りでき、現行ツールやシステムの大半ともシームレスに連携できます」

業務における効果

わずか数時間で IoT や OT を含むデバイスを完全に可視化

Kaiter 氏は、さらに説明します。「当初、デバイスの数は 2,500 台程度だろうと想定していましたが、Forescout プラットフォームの初期トライアル段階ですでに、これまで認識していなかった IoT、OT デバイスを含むデバイスが 5,000 台も検出されました。わずか 2 時間で、広範囲にわたる環境全体を可視化し、ほぼすべてのデバイスを自動分類できました。Forescout プラットフォームのトライアル展開から本番運用への移行も、わずか数時間で完了しました。プラットフォーム実装完了後わずか半日で、正確なリアルタイム資産インベントリを作成できました。ダッシュボードを数回クリックするだけで簡単に作成できます。最終的に、合計 6,800 台の資産が特定されました。これは当初の想定より 170% も多い数です」

デバイスコンプライアンスの簡便化により、 セキュリティポスチャーを強化

Continuum プラットフォームでネットワーク接続デバイスすべて (IT、OT、IoT デバイス) のセキュリティポスチャーを常時、自動評価することで、同社のセキュリティが強化されました。個々のデバイスがグループ内ネットワークへの接続を試みると、Continuum プラットフォームが各種項目 (ウイルス対策ソフトのインストールおよび実行の有無、Windows ファイアウォールの有効化有無、Windows 更新の最新版適用有無、および適切な VLAN にデバイスが配置されていること) をチェックします。たとえばウイルス対策ソフトが実行されていない場合は、Continuum プラットフォーム側で再度アクティブ化します。準拠違反デバイスを自動修復できない場合は管理者に通知し、別の VLAN に移動するなどの手動修復を要請します。

同社のシステム・ネットワーク管理者 Jan- Erik Strauss 氏は、次のように述べています。「Forescout は、デバイスハイジーンに関する問題解決だけでなく、ブラックリスト上のアプリが使用されている、または社用ノートパソコン以外の端末が VPN 経由でグループ内ネットワークにアクセスしている、などの深刻な脆弱性や脅威も特定してくれます。現在も、これまで見過ごしていたような新たな気づきがほぼ毎週発生しています」



「深刻な脆弱性や脅威を
Forescoutが特定してくれました。
(中略)現在も、これまで見
過ごしていたような新たな気づ
きがほぼ毎週発生しています」

— Winkelmann Group
システム・ネットワーク管理者
Jan-Erik Strauss氏

ネットワーク管理の負担を軽減

同グループのセキュリティ・ネットワーク管理部門は少人数体制ですが、Continuumプラットフォームを導入した結果、毎月数日単位の工数を節減でき、業務負担が軽減されました。たとえば、数年前にグループ全体のウィルス対策ソリューションをオンプレミス版からクラウド版に移行した際、エージェントがインストールされていない状態から再インストールしたため、一部のエンドポイントにウィルス対策が適用されないままになっていました。Strauss氏は、次のように述べています。「Forescoutのおかげで要注意デバイスが何台あるか把握できるようになっただけでなく、個々のデバイス名や所有者の名前まで正確に特定できるようになりました。Forescoutが提供するデバイスの詳細情報は非常に有用で、様々な面で工数削減に役立っています」

「Forescout Continuumプラットフォームはきわめて強力でありながら、設定・利用が簡単です。外部のサポートをほとんど借りずにプラットフォームの構成設定を完了できました。ダッシュボードは直感的で、新たなグループやポリシーをあっという間に作成できます」と同氏。

「NACだけにとどまらない価値を実現」

Winkelmann Groupは、Forescout導入初日からその価値を実感しましたが、Continuumプラットフォームにはまだまだ多くの包括的機能があり、これから徐々に活用範囲を広げていく予定です。今後、同社ではより多くのセキュリティプロセスを自動化してネットワークセグメンテーションを拡充し、IT資産だけでなく生産現場の機械も、単なる監視でなくポリシー適用の対象に含める予定です。すでにContinuumプラットフォームをVMWareのインフラやファイアウォール、Active Directoryと連携し、今後は同社のネットワーク環境で稼働する別のシステムともシームレスに連携し、相乗効果を得たいと考えています。

同様の課題に悩む業界の仲間に「Continuumプラットフォームについて感想を聞かれた場合、どう説明するか質問したところ、Kaiter氏は次のように答えています。「コストを抑えることを重視して、Forescoutプラットフォームより安い、例えば1/4の価格で導入できる製品を使うことは可能ですが、得られるセキュリティ効果もその1/4、もしくはそれ以下になってしまうでしょう。当然ながら、Forescoutが提供する幅広い機能も享受できません。当社はForescoutをNAC目的で購入しましたが、日々のデバイス管理にも活用しています。今後はもっと広い用途に活用できると思っています。Forescoutは確かにNACソリューションですが、はるかに多くの付加価値が期待できます」



Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
詳細は [Forescout.com](https://www.forescout.com)
をご覧ください。

©2023 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. はデラウェア法人です。当社の商標および特許の一覧は <https://www.forescout.com/company/legal/intellectual-property-patents-trade-marks> でご確認ください。他のブランド、製品、サービス名は、それぞれの所有者の商標またはサービスマークである可能性があります。Version: 01_02