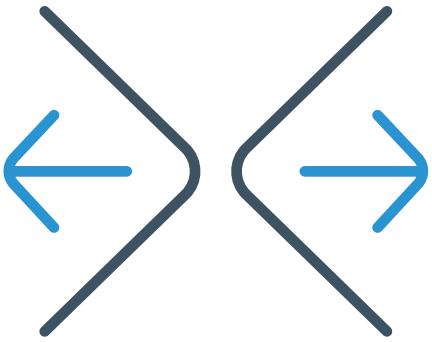
FORESCOUT



eyeExtend Ecosystem

他ベンダーソリューションとの連携におけるサイバーセキュリティのプロセスと対応を自動化

優れた拡張性

70以上のテクノロジーベンダーが参加するForescoutの広範なエコシステムから、必要な連携先をお選びいただけます。

事前構築

多くの領域に対しForescoutの連携機能により素早い構築が実現可能にはやくデプロイできます。

ROIの早期実現

実証済ですぐに使えるアプリや連携機能で、時間とコストを節減できます。

Forescout eyeExtend Ecosystem を介してForescout Platformと他社製IT及びセキュリティソリューションを連携し、一連のセキュリティプロセスを自動化することで運用効率の改善やセキュリティポスチャー全般の強化を図れます。Forescoutの資産インテリジェンスやエンフォースメント機能を、すでに導入済みの現行IT/セキュリティ製品と連携することで、以下を実現できます。

- 死角を排除し、資産をくまなく可視化
- 複数製品にまたがるワークフローの自動化
- リスク、インシデント、コンプライアンスギャップへの対応のスピードアップ

デバイスコンテキストの共有

- 管理対象/対象外のデバイスに関する現行セキュリティツールの可視性を向上
- CMDBの更新とデバイスプロパティの同期
- インシデントの相関付けや優先順位の判定材料となるデバイスコンテキストをリアルタイムでSOCに提供

ワークフローの自動化

- 複数ツールにまたがるセキュリティプロセスとネットワーク接続ワークフローのデジタル化
- トリガー条件をもとに脆弱性のリアルタイムスキャンを開始し、パッチ適用とセキュリティ更新を実行
- エンドポイントエージェントが正常に機能し、更新済であることを確認し、脅威情報を統合して予防的なリスク探索を実施

対応のスピードアップ

- インシデント発生時にシステム全体の緩和・修復策を迅速に展開
- ユーザー、デバイス、セキュリティポスチャーにもとづくネットワークアクセス制御をポリシー主導型で実施
- 侵害された脆弱で高リスクなデバイスの封じ込め/隔離/ブロック

eyeExtend Ecosystemが解決する問題

- **セキュリティ/規制要件、ソフトウェアライセンス条件の準拠違反**

  現行ITソリューションで可視化しきれず、死角が生まれることが原因

- **運用コストの高さ、生産性の低さ**

  複数のセキュリティツールがサイロ化し、問題解決にあたり手動での調整が必要

- **脅威拡散のリスク**

  現行ベンダー製ソリューションの機能不足により、セキュリティ脅威やインシデントへの迅速かつ効果的な対応ができない

デバイスコンテキストの共有

Forescoutと他社製ソリューションの間でデバイス情報やコンテキストを双方向に共有することで、ポリシーのワークフローを効率化できます。

- デジタル環境にまたがる各種資産(IT、IoT、OTデバイスなど)の種類、設定、ユーザー情報、所在地、認証パターンに関してForescoutプラットフォームが提供するコンテキストベースの洞察を活用し、エージェントレスでセキュリティポスチャーを評価
- 資産インベントリデータベースを自動更新して常に最新の状態を維持できるため、社内の貴重なリソースの時間を節減可能
- Forescoutプラットフォームのデータと外部データソースと組み合わせて異常を検知し、インシデントの優先順位を判断

ワークフローの自動化

セキュリティポリシー評価や修復に関する全社的なワークフローを自動化し、社内のセキュリティポリシーや外部基準、業界規制などへの準拠状態を維持できます。

- 新規または一時利用のデバイスがネットワーク接続した時点でリアルタイムの脆弱性スキャンを実行
- セキュリティのパッチ適用や更新を実行し、攻撃対象領域を縮小
- エンドポイントセキュリティーソフトウェアが適切に機能していることを確認し、違反している場合は修復措置を自動実行
- 管理対象外のアカウントをリアルタイムで自動検出し、コンプライアンス条件を適用
- 外部ツールから得た脅威情報、危急化の指標、ポリシー違反情報を活用し、管理対象外デバイスについても脅威検出を実施

対応のスピードアップ

他社製ソリューションが検出したアラートへの対応を迅速化し、インシデントや脅威発生時の解決するまでの時間を短縮します。

- セキュリティポリシーに従ってネットワークアクセス制御に関するアクションを自動実行、または手動で開始
- 侵害された、または悪質なデバイスによるネットワークアクセスを制限/ブロック
- 準拠違反のデバイスは、修復措置が完了するまで隔離/分離

「我々は、現行システムと親和性の高い製品を探していた。
Forescoutのソリューションはベンダーの制限なく使えるというだけでなく、迅速・簡単に導入でき、リアルタイムの可視性やコンプライアンス、分類にも大変優れている。
組織内の他システムとも容易に連携できるため、
現行システムの効率性・有効性が高まった」

フィル・ベイツ氏
ユタ州政府　情報セキュリティ最高責任者

事例を読む

多岐にわたる製品と連携し、拡張性に優れたプラットフォーム

eyeExtend Ecosystem モジュール

Foresoutでは、以下9種類のセキュリティテクノロジー領域を対象にeyeExtend Ecosystem モジュールを提供し、定期的に更新・改良しています。

ATD
Check Point SOFTWARE TECHNOLOGIES LTD.
FIREEYE
paloalto NETWORKS

EMM
vmware
IBM
MobileIron
Microsoft

SIEM
IBM
MICRO FOCUS
splunk>

PAM
CYBERARK

VA
RAPID7
tenable network security
Qualys.

ITSM IRM
servicenow

COMPLIANCE
SCAP

EPP/EDR
CROWDSTRIKE
Symantec
Carbon Black.
McAfee
FIREEYE

NGFW
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
paloalto NETWORKS

Forescout eyeExtend Ecosystem でご利用いただけるサービス

	ご利用可能
Advanced Compliance Module	✔
eyeExtend for Carbon Black	✔
eyeExtend for Check Point Next Generation Firewall	✔
eyeExtend for Check Point Threat Prevention	✔
eyeExtend for CrowdStrike	✔
eyeExtend for CyberArk	✔
eyeExtend for FireEye EX	✔
eyeExtend for FireEye HX	✔
eyeExtend for FireEye NX	✔
eyeExtend for Fortinet Next-Generation Firewall	✔
eyeExtend for HPE ArcSight	✔
eyeExtend for IBM BigFix	✔
eyeExtend for IBM Qradar	✔
eyeExtend for McAfee ePolicy Orchestrator	✔
eyeExtend for Palo Alto Networks Next-Generation Firewall	✔
eyeExtend for Palo Alto Networks WildFire	✔
eyeExtend for Qualys Vulnerability Management	✔
eyeExtend for Rapid7 Nexpose	✔
eyeExtend for ServiceNow	✔
eyeExtend for Splunk	✔
eyeExtend for Symantec Endpoint Protection Manager	✔
eyeExtend for Tenable Vulnerability Management	✔

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
詳細はこちら：Forescout.com