Skybox Securityご紹介

ジェイズ・コミュニケーション
マーケティング推進部

ソリューション概要

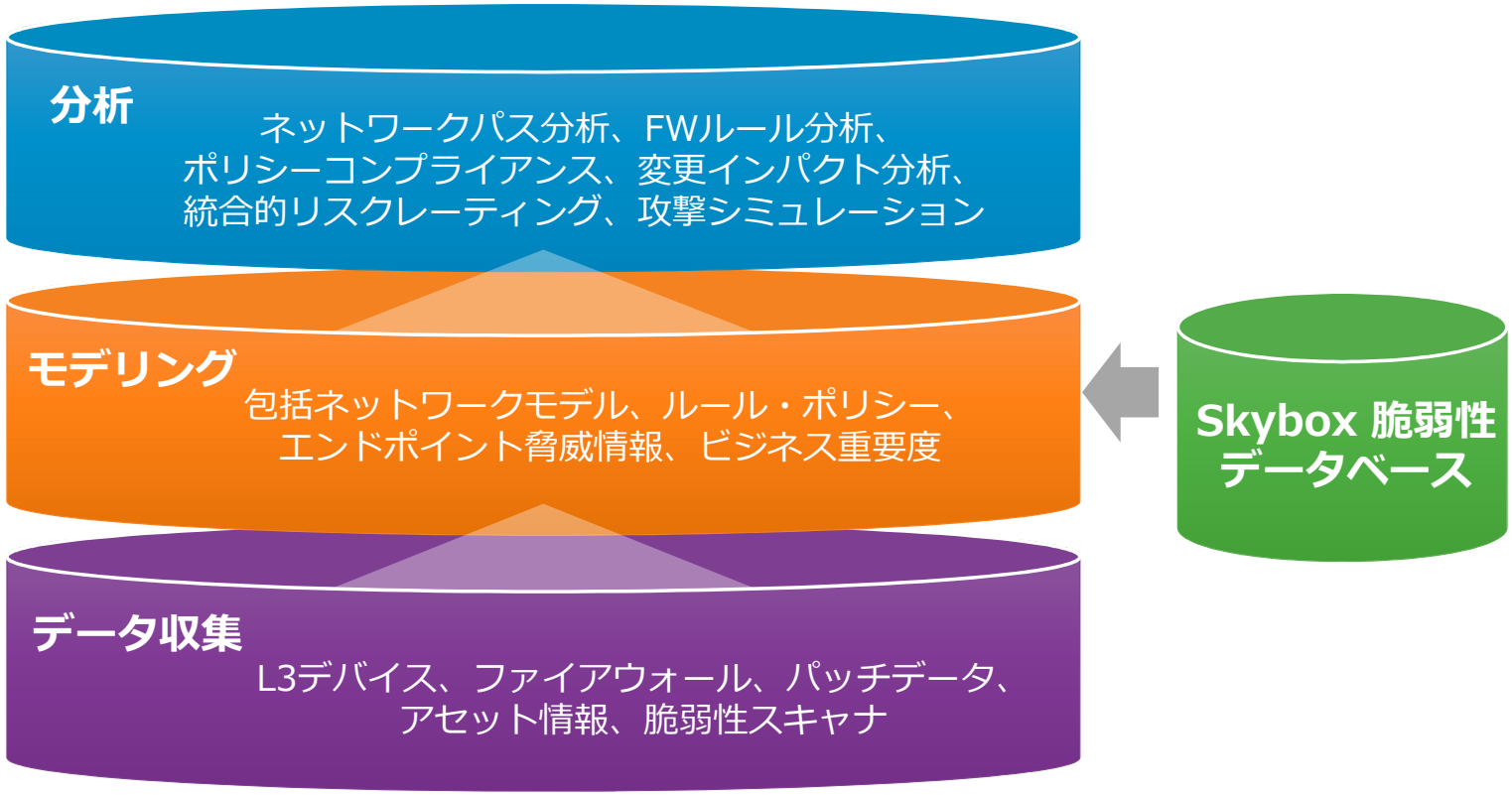
ネットワークリスク管理 

- ネットワーク機器の設定情報を収集してネットワークを可視化し、設定・運用を容易にします。
- ネットワーク機器の設定ミスやポリシー違反を監視し、サイバー攻撃の可能性を未然に防ぎます。

脆弱性リスク管理 

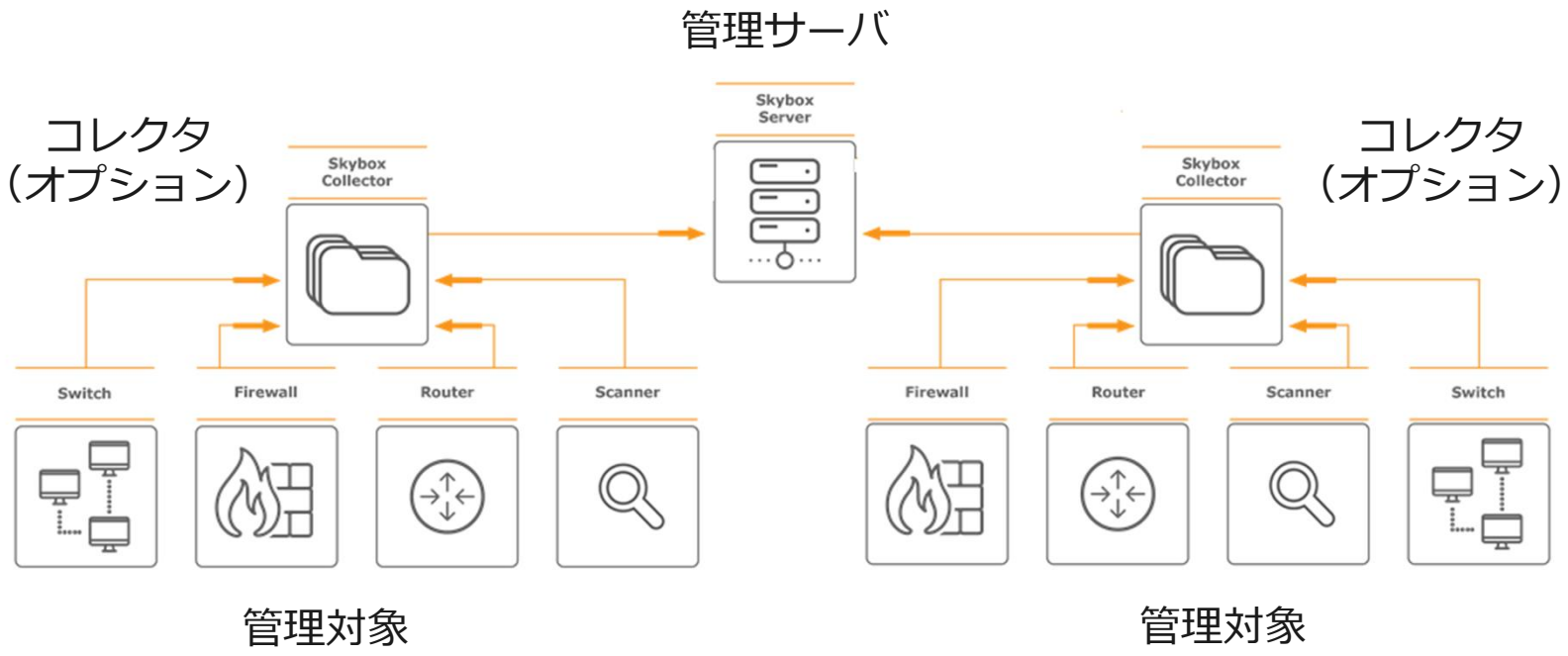
- ネットワーク設定とアセットの脆弱性を統合的に評価し、リスクに優先度付けして対策を提示します。

アーキテクチャ


分析
ネットワークパス分析、FWルール分析、
ポリシーコンプライアンス、変更インパクト分析、
統合的リスクレーティング、攻撃シミュレーション
モデリング
包括ネットワークモデル、ルール・ポリシー、
エンドポイント脅威情報、ビジネス重要度
データ収集
L3デバイス、ファイアウォール、パッチデータ、
アセット情報、脆弱性スキャナ
Skybox 脆弱性
データベース

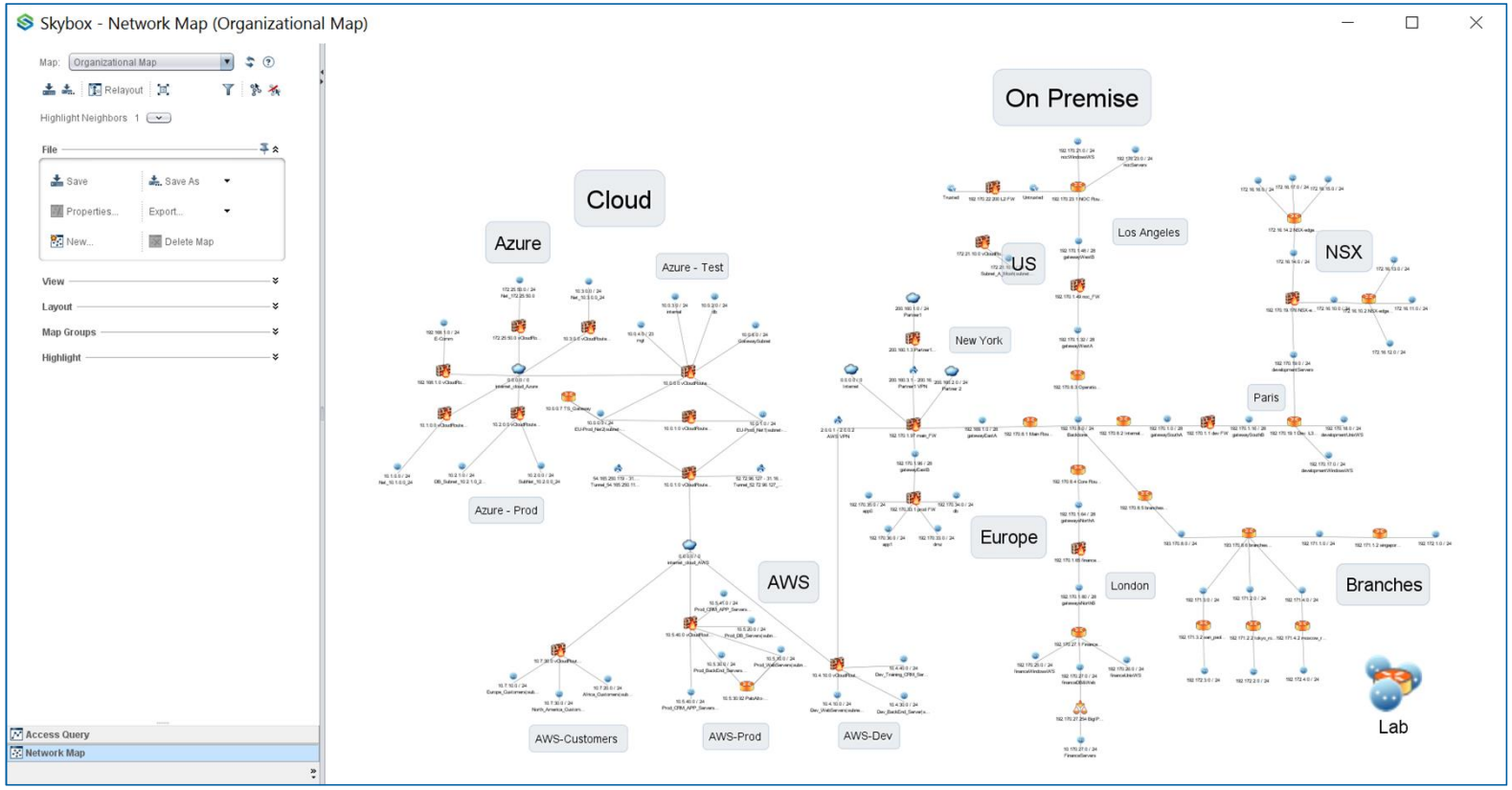
データ収集

管理サーバ（コレクタ）から管理対象にアクセスし設定情報を収集する
収集方法は管理対象により予め設定されたSSH、API、CSV等



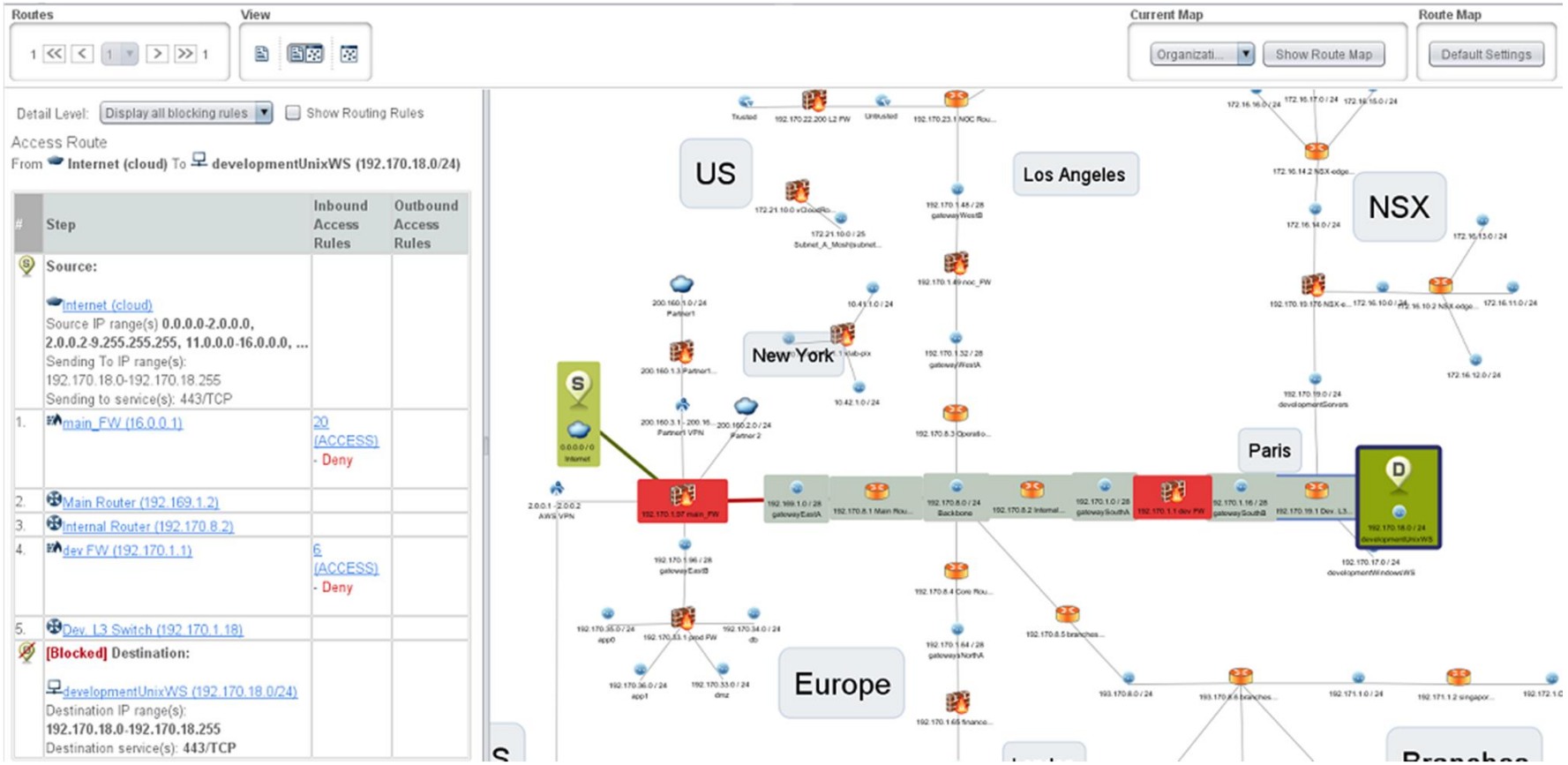
ネットワークモデリング

150+ のサポート対象製品データを標準化
物理、仮想、クラウド、OT環境に対応



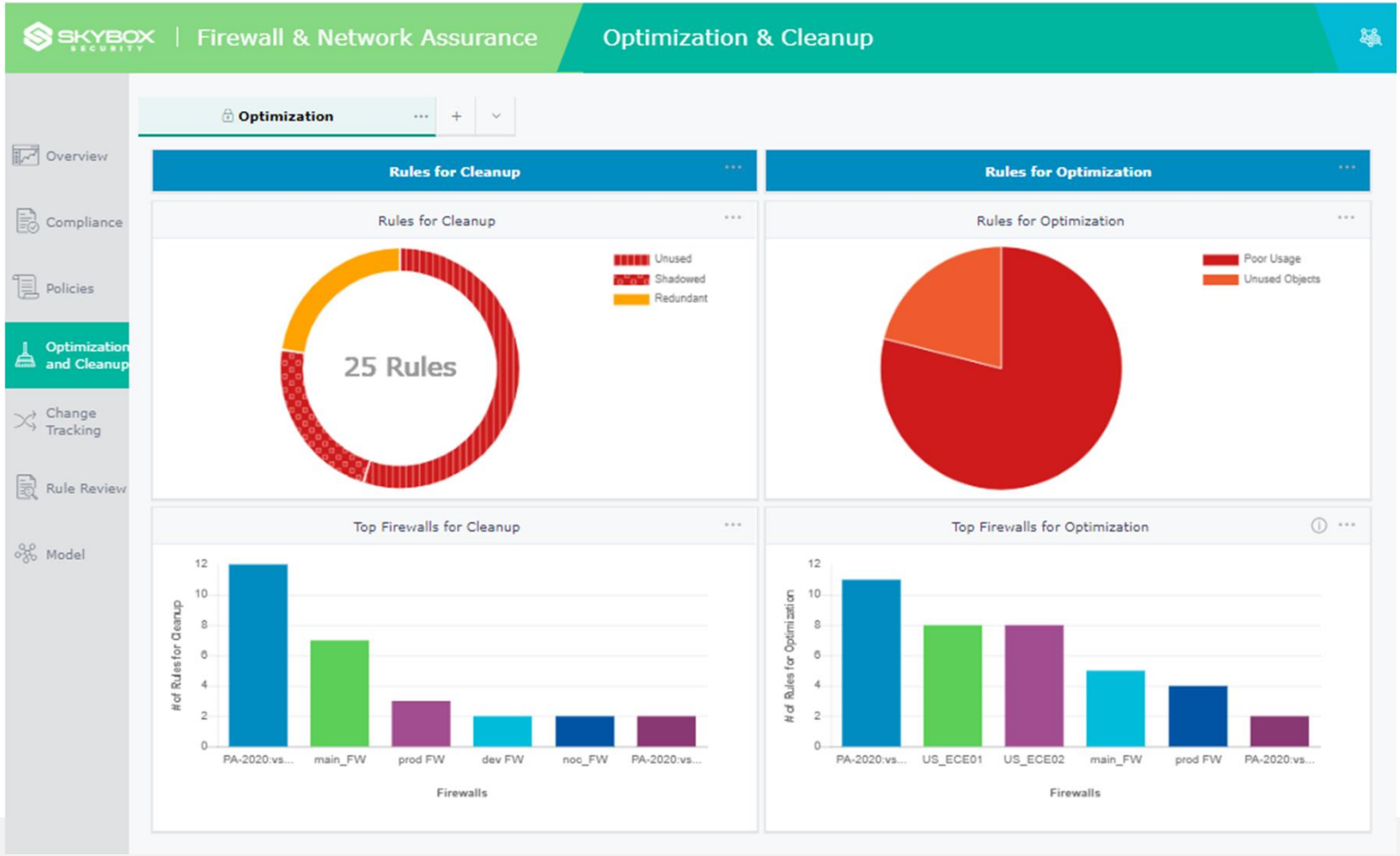
ネットワークパス分析

セグメント・ゾーン間のパス分析（アクセス可・アクセス不可）



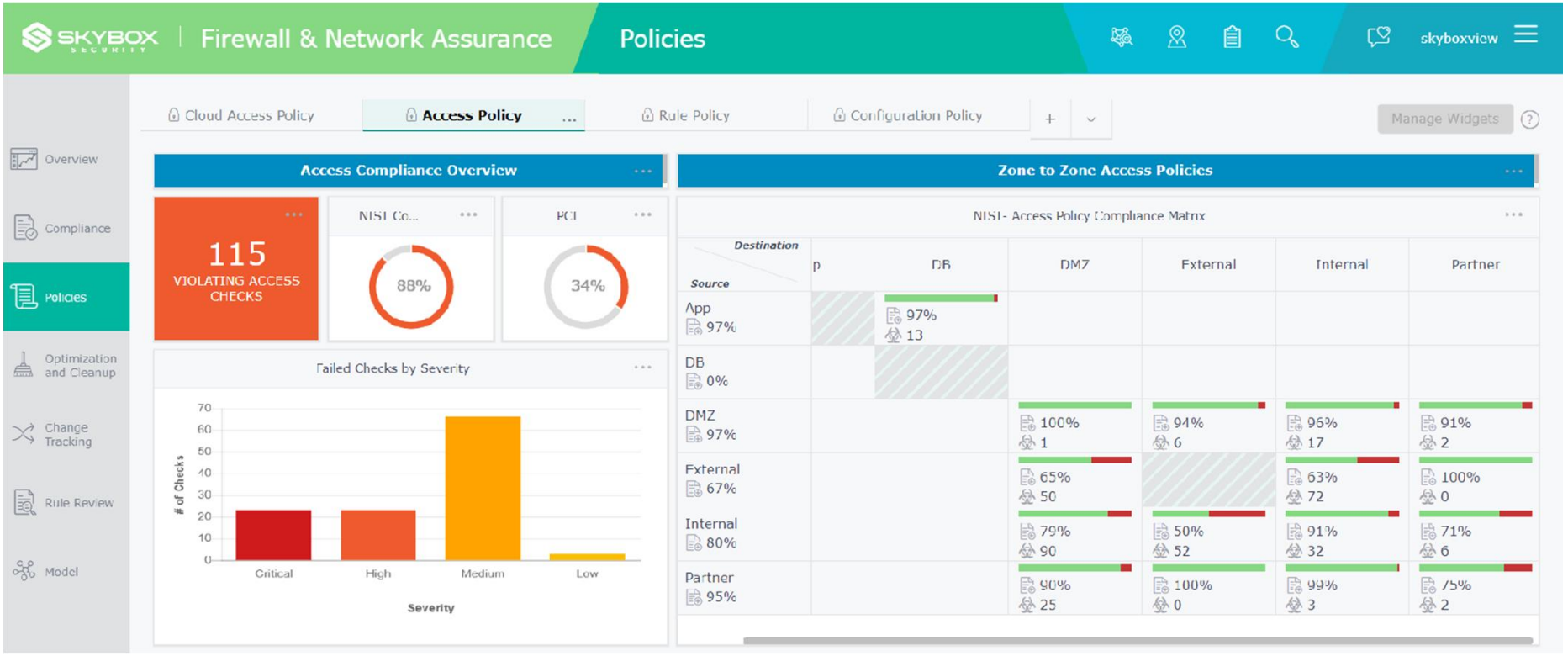
FWルールクリーンアップと最適化

重複ルール、低利用ルールを洗い出します



FWポリシー管理

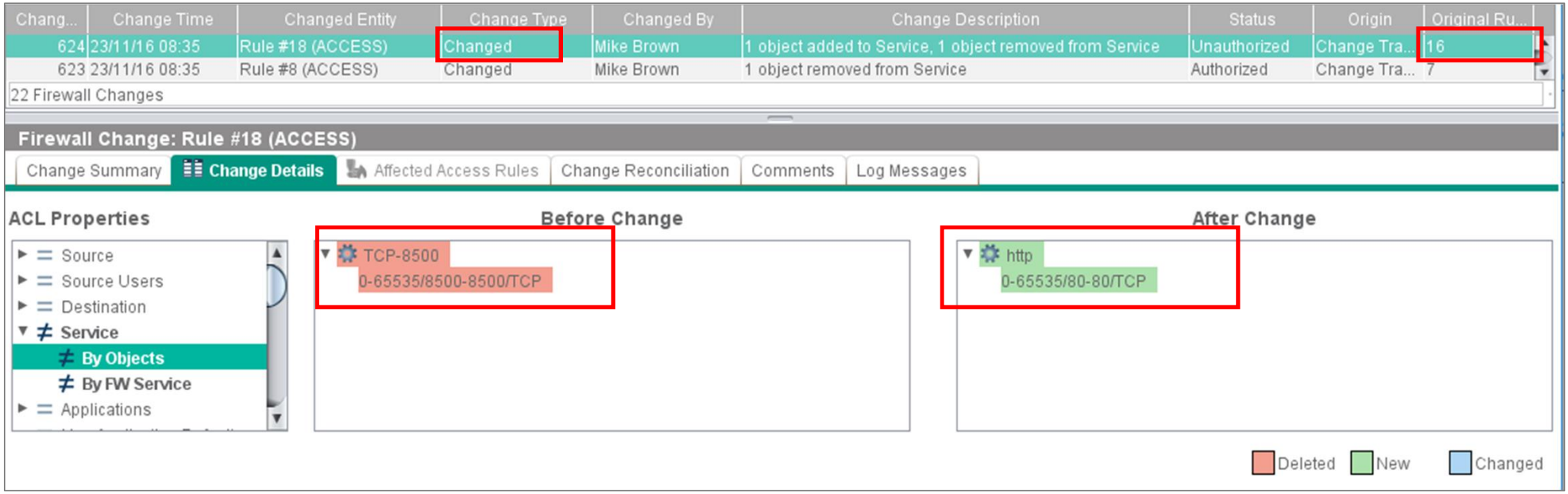
NIST、PCI、CIS、独自ポリシーへの準拠状況を管理します



※ NIST 800-41 / PCI DSS

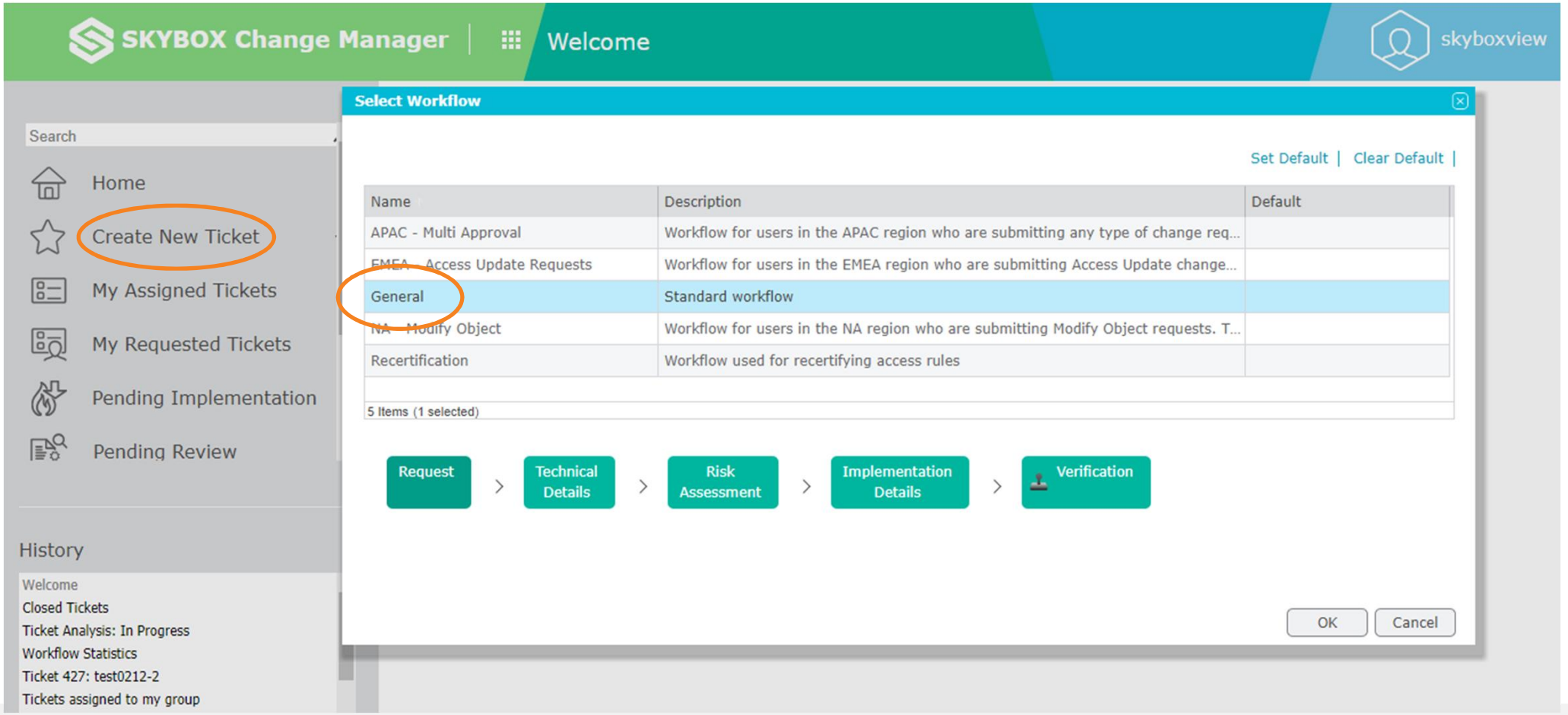
FW変更記録

FWログによる変更記録、および差分ベースの変更記録を管理します



FW変更ワークフロー

FW設定変更のチケット生成、リスク管理、確認、監査証跡を提供します



変更インパクト分析

ソース/デスティネーションのサービス変更要求をブレークダウン
変更によるリスクのアセスメント

Original Change Requests

Access Update... | Add Rule... | Modify Object... | More... | Firewalls... | Set Attributes | Edit | Delete |

#	ID	Chan...	Firewall/Manag...	Objec...	Change Details	Additional Details	Comment	Change Req...
1	103	Requi...		-	Source: 200.200.200.200 Destination: 192.170.19.20 Services & Applications: 21/TCP			Yes

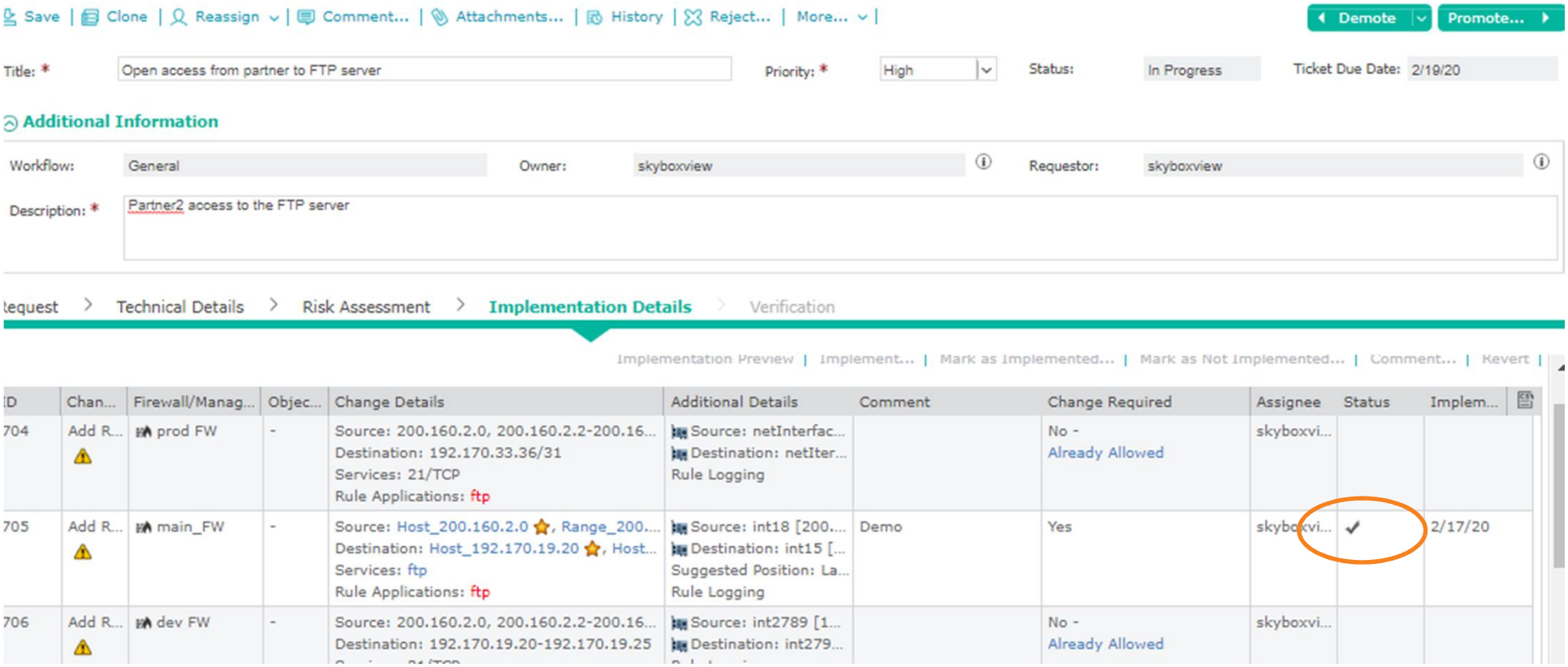
Derived Change Requests

Convert Type | Set Attributes | Edit | Delete |

#	ID	Change...	Firewall/Ma...	Objec...	Change Details	Additional Details	Comment	Change Req...	Assignee
1	358	Add Rule	main_FW	-	Source: Host_200.200.200.200 Destination: Host_192.170.19.20 Services: ftp			No - Already Allo...	
2	361	Add Rule	dev FW	-	Source: Host_200.200.200.200 Destination: Host_192.170.19.20 Services: Service_21_TCP	Suggested Position: Before ...		Yes	

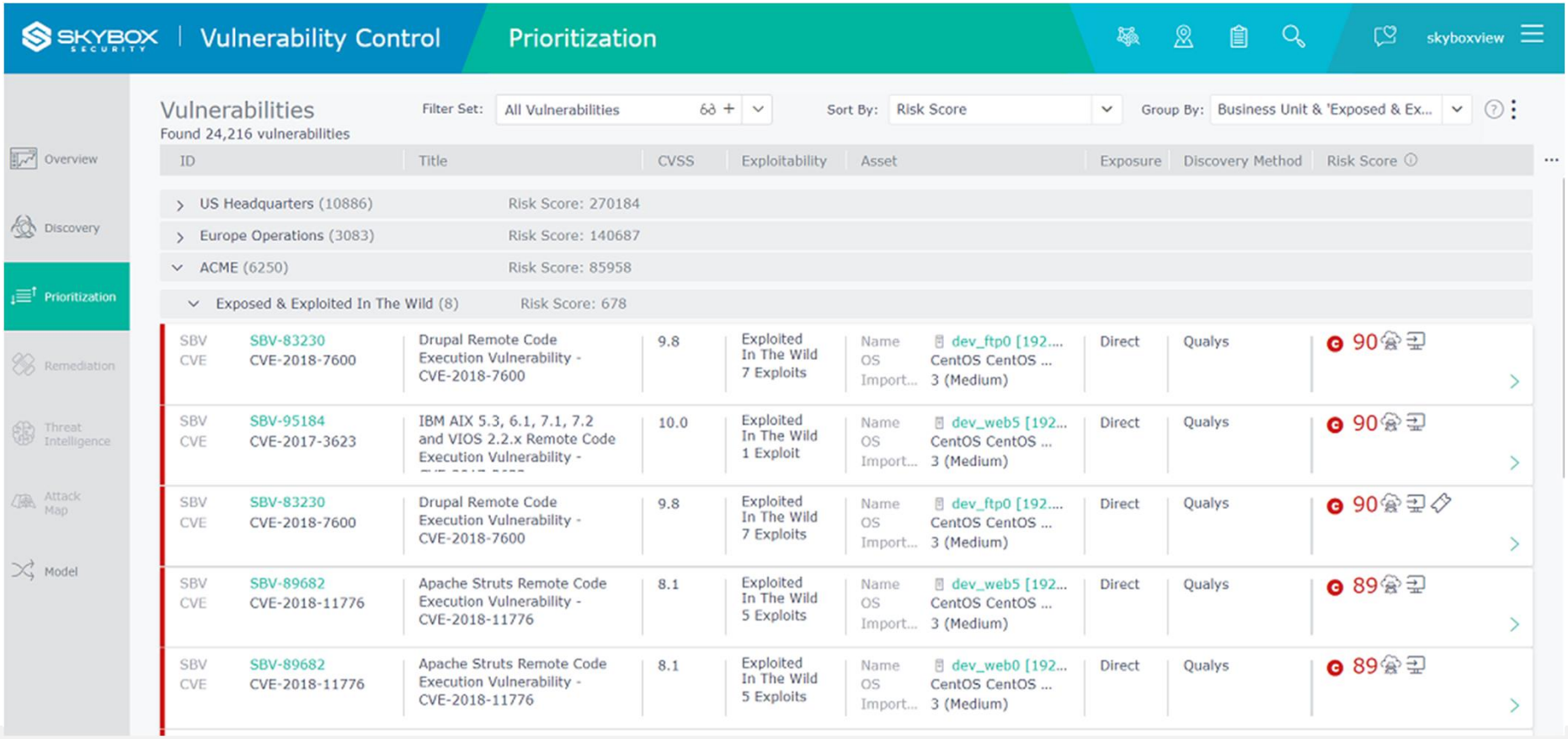
変更を実装

主要５ベンダー（Cisco、Juniper、PaloAlto、Fortinet、Checkpoint）についてはプッシュによる設定変更が可能です



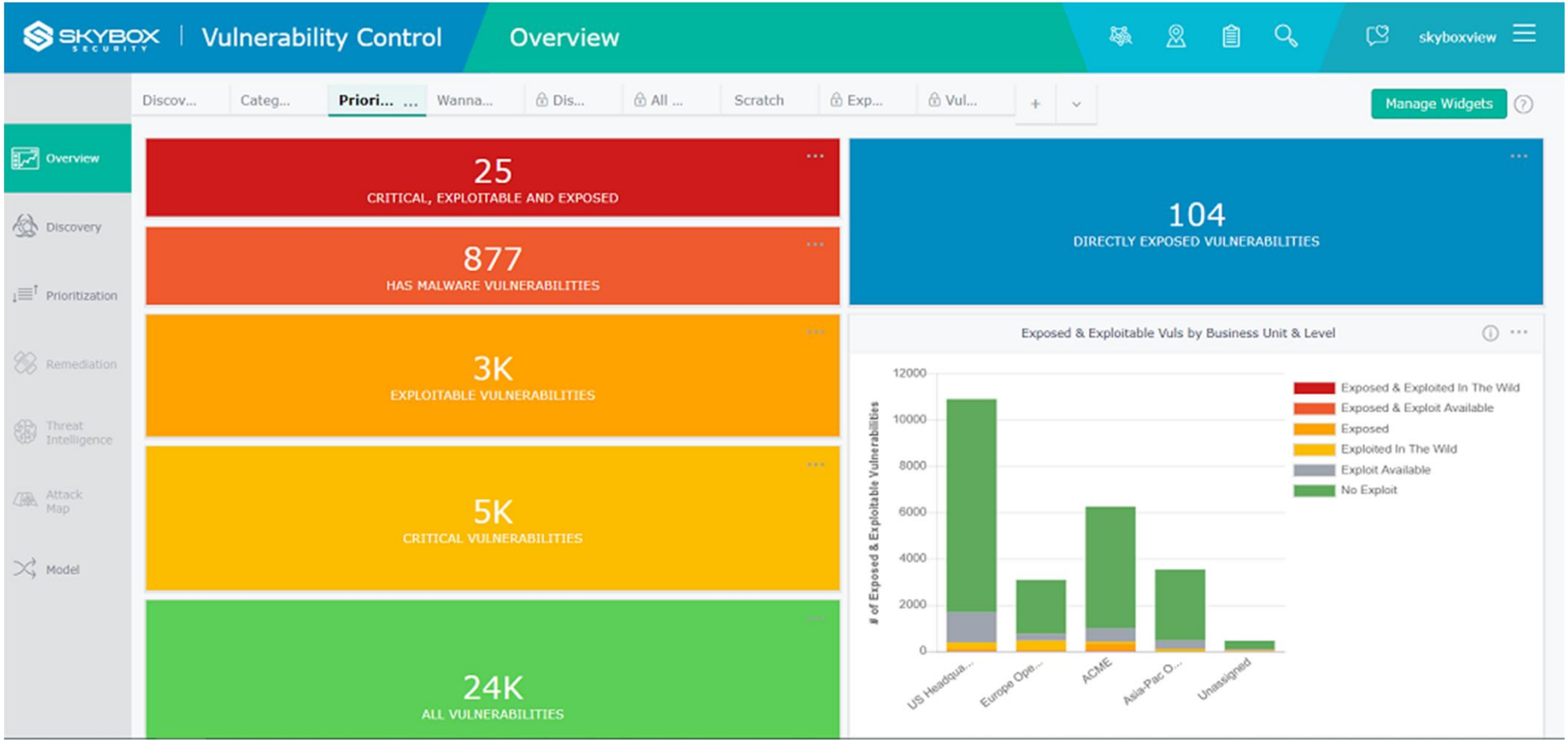
統合的リスクレーティング

ネットワーク設定とアセット脆弱性によりリスクレーティングします
攻撃元（インターネット、パートナー、社内等）の設定が可能です



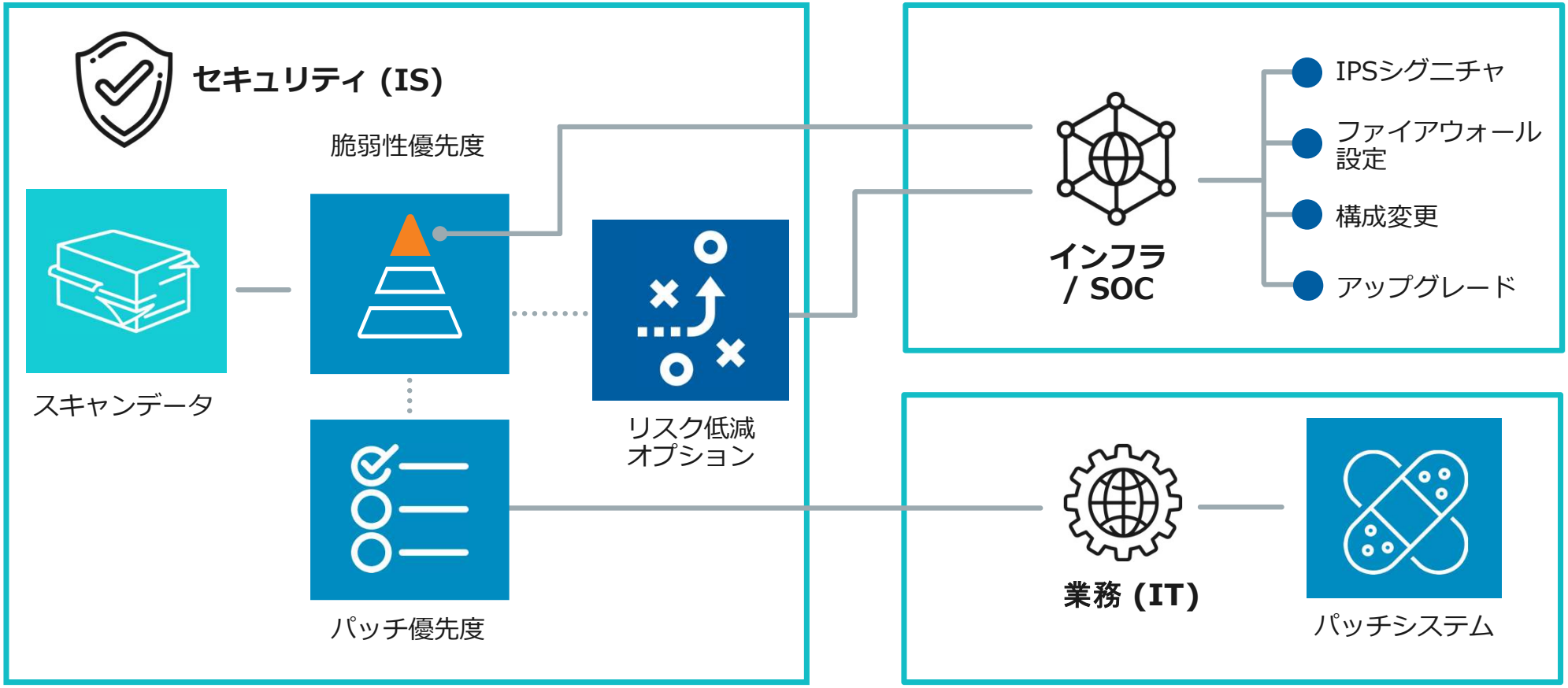
リスクレベル分析

全脆弱性<危機的脆弱性<EXPLOIT可能<マルウェア有<アクセス可能
ビジネスにおいて重要なアセット



複数のリスク対応策

リスク対策はアセットへのパッチ、経路上のIPSシグニチャ適用が含まれます
ネットワーク構成変更、FW設定変更による回避も可能



お問合せは下記までお願いします
skybox_pr@jscom.co.jp

J's Communication