



# 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



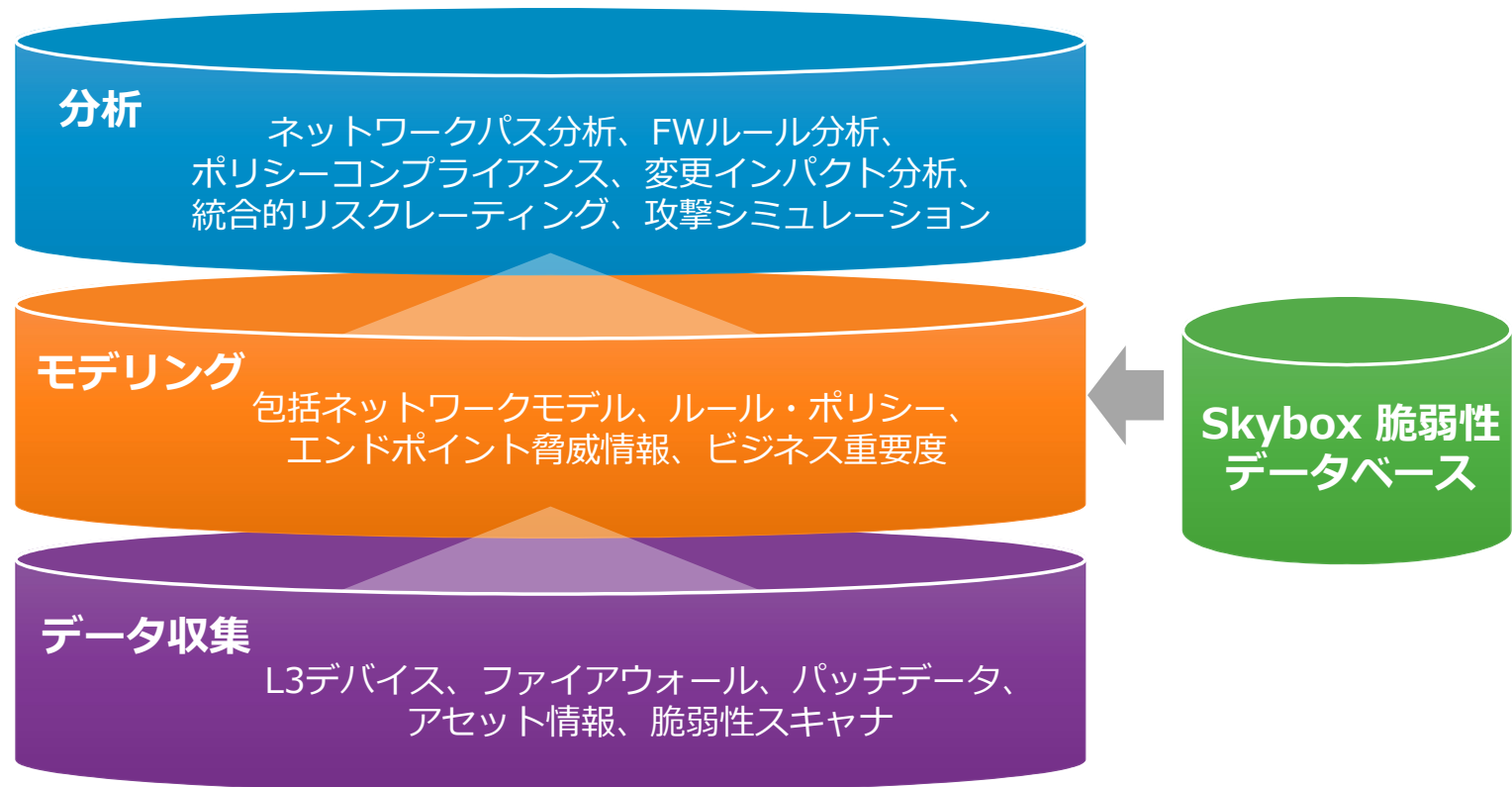
- ネットワーク機器の設定情報を収集してネットワークを可視化し、設定・運用を容易にします。
- ネットワーク機器の設定ミスやポリシー違反を監視し、サイバー攻撃の可能性を未然に防ぎます。

## 脆弱性リスク管理



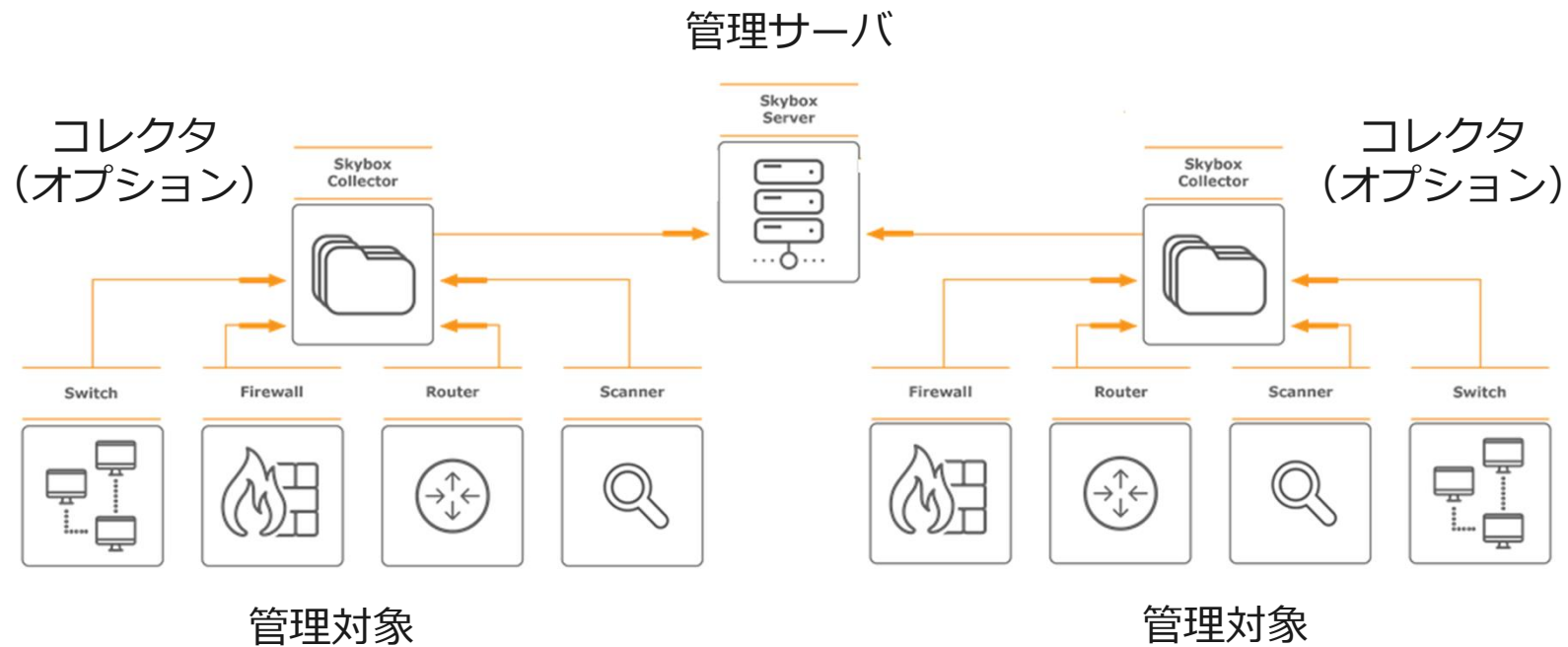
- ネットワーク設定とアセットの脆弱性を統合的に評価し、リスクに優先度付けして対策を提示します。

# アーキテクチャ



# データ収集

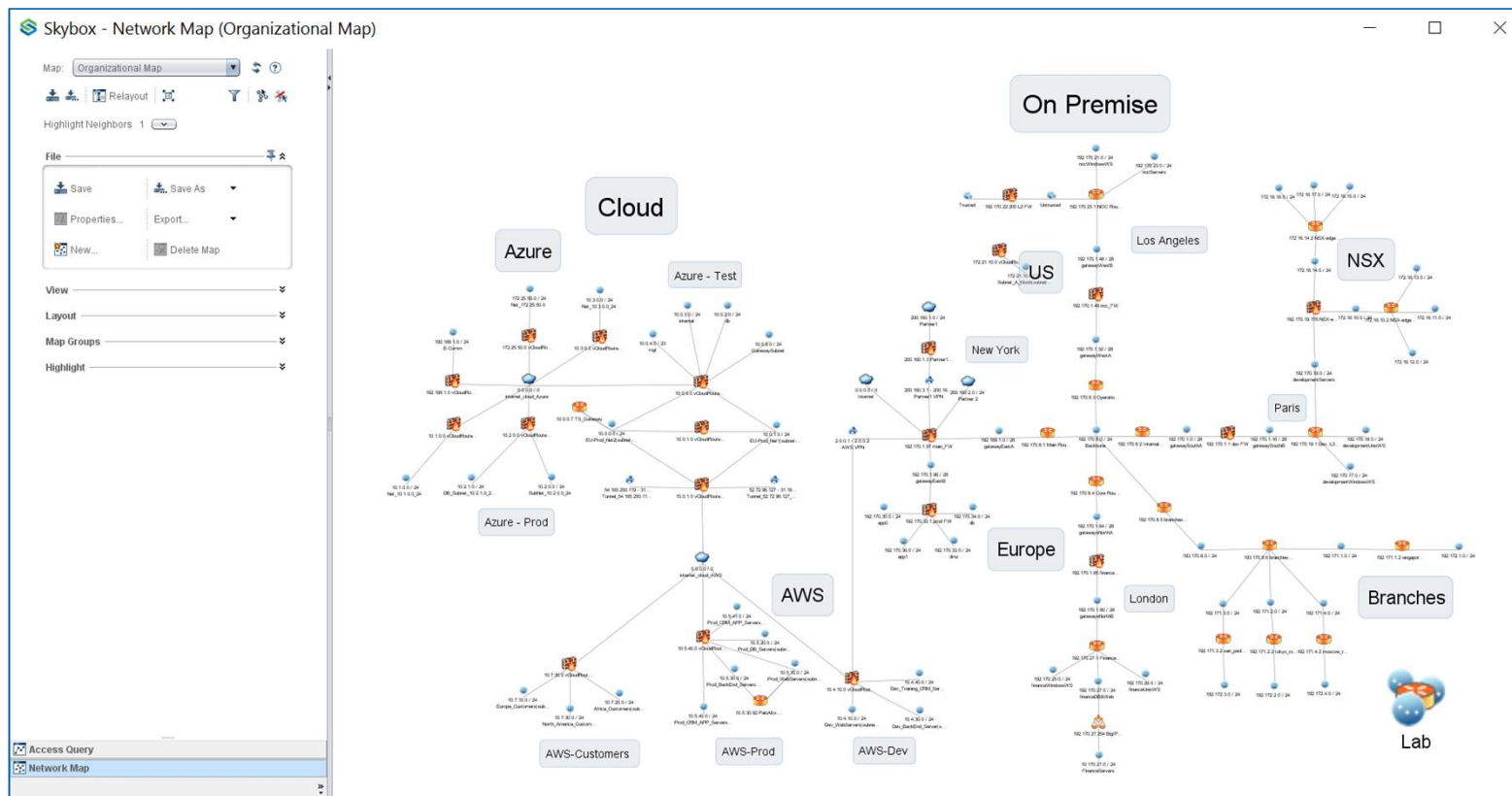
管理サーバ（コレクタ）から管理対象にアクセスし設定情報を収集する  
収集方法は管理対象により予め設定されたSSH、API、CSV等



# ネットワークモデリング



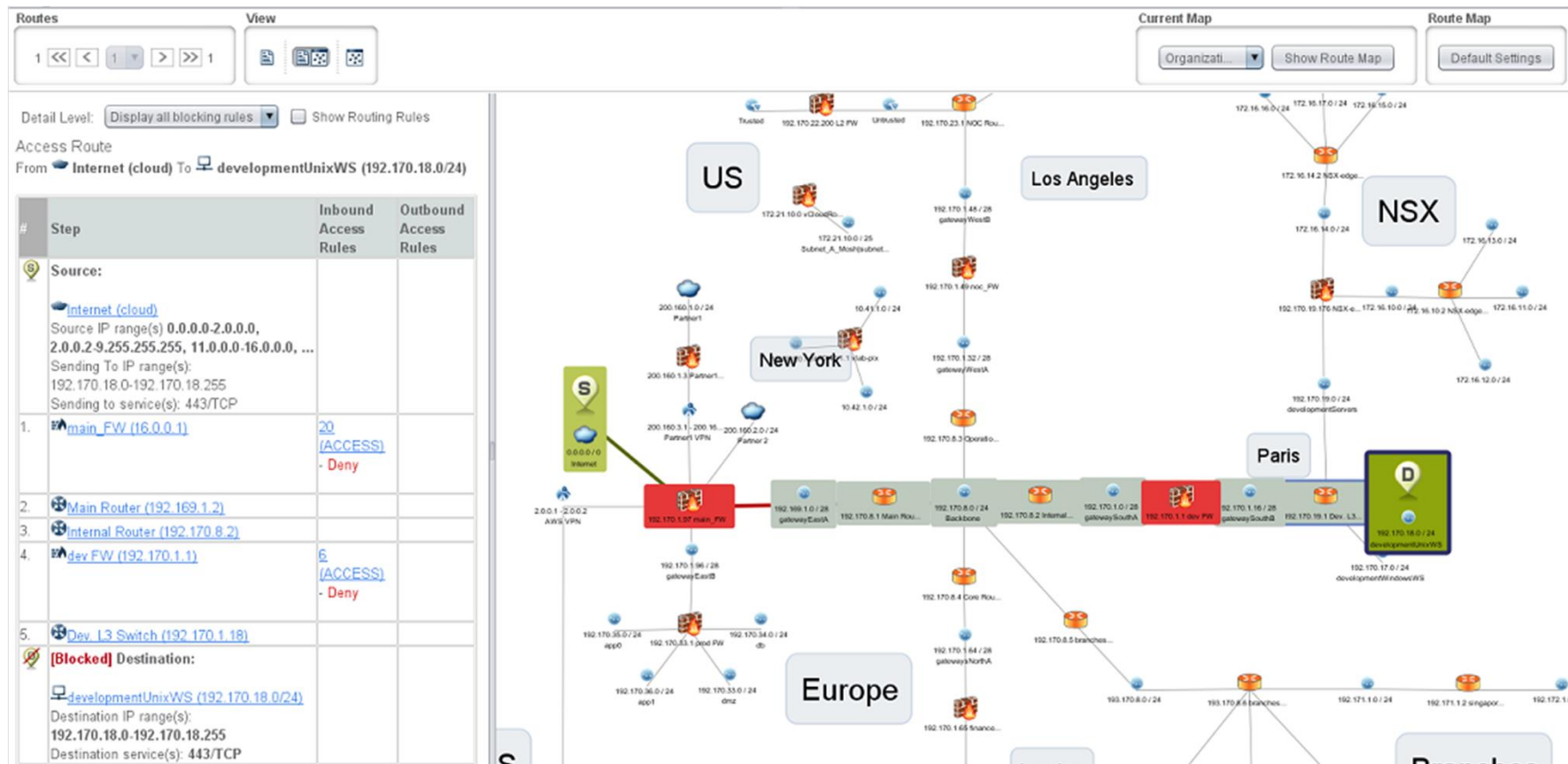
150+ のサポート対象製品データを標準化  
物理、仮想、クラウド、OT環境に対応



# ネットワークパス分析

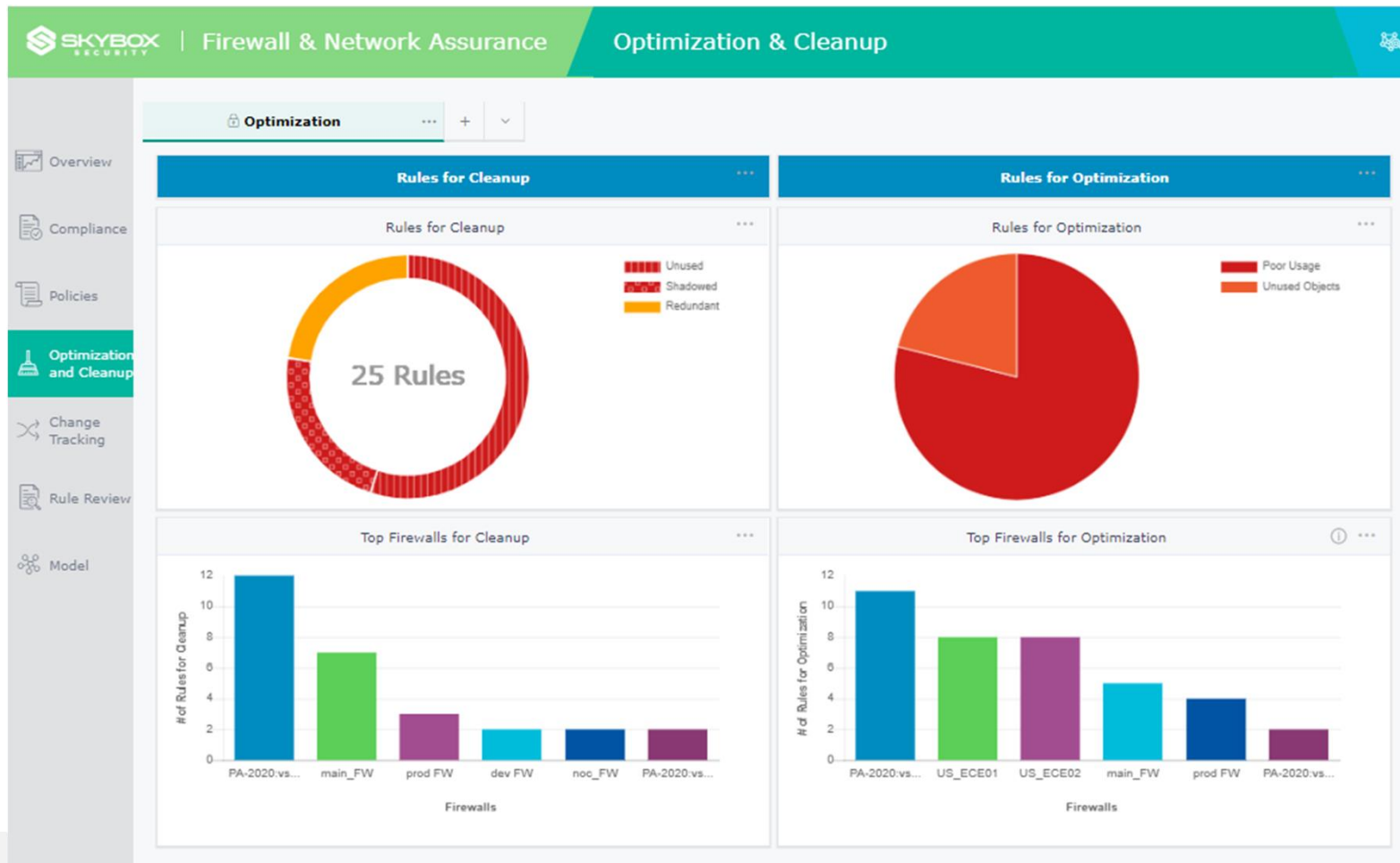


セグメント・ゾーン間のパス分析 (アクセス可・アクセス不可)



# 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

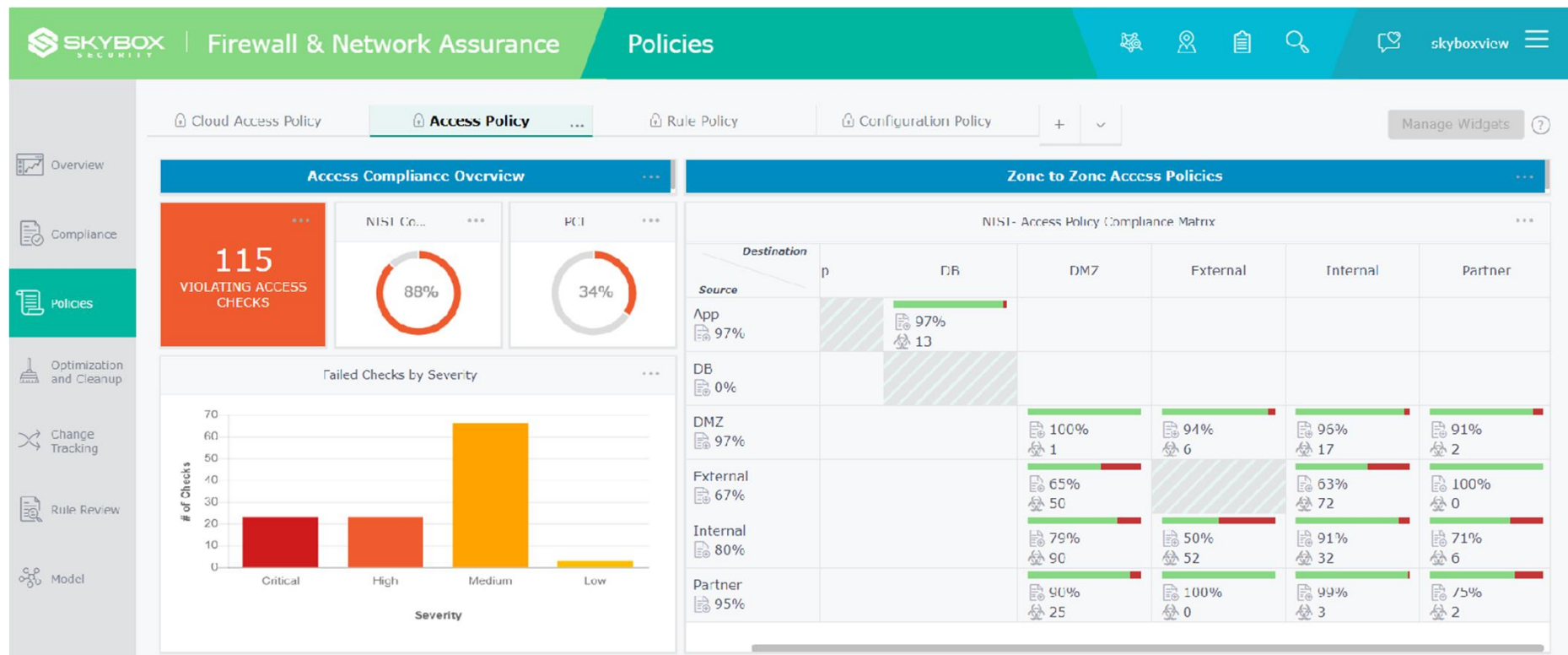




# FWポリシー管理



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

Change...	Change Time	Changed Entity	Change Type	Changed By	Change Description	Status	Origin	Original Ru...
624	23/11/16 08:35	Rule #18 (ACCESS)	Changed	Mike Brown	1 object added to Service, 1 object removed from Service	Unauthorized	Change Tra...	16
623	23/11/16 08:35	Rule #8 (ACCESS)	Changed	Mike Brown	1 object removed from Service	Authorized	Change Tra...	7

22 Firewall Changes

### Firewall Change: Rule #18 (ACCESS)

Change Summary | **Change Details** | Affected Access Rules | Change Reconciliation | Comments | Log Messages

**ACL Properties**

- Source
- Source Users
- Destination
- Service**
  - By Objects**
  - By FW Service
- Applications

**Before Change**

TCP-8500  
0-65535/8500-8500/TCP

**After Change**

http  
0-65535/80-80/TCP

Deleted New Changed

# 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

The screenshot displays the SKYBOX Change Manager interface. On the left sidebar, the 'Create New Ticket' button is highlighted with an orange circle. The main area shows a 'Select Workflow' dialog box with a table of workflows. The 'General' workflow is selected and also circled in orange. Below the table, a process flow is shown: Request > Technical Details > Risk Assessment > Implementation Details > Verification. The 'General' workflow is the standard workflow for all change requests.

Name	Description	Default
APAC - Multi Approval	Workflow for users in the APAC region who are submitting any type of change req...	
EMEA - Access Update Requests	Workflow for users in the EMEA region who are submitting Access Update change...	
General	Standard workflow	
NA - Modify Object	Workflow for users in the NA region who are submitting Modify Object requests. T...	
Recertification	Workflow used for recertifying access rules	

5 Items (1 selected)

Request > Technical Details > Risk Assessment > Implementation Details > Verification

OK Cancel



# 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イクダウン  
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	<a href="#">Add Rule</a>	main_FW	-	Source: Host_200.200.200.200 ★ Destination: Host_192.170.19.20 ★ Services: ftp			No - Already Allo...		
2	361	<a href="#">Add Rule</a>	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

Save | Clone | Reassign | Comment... | Attachments... | History | Reject... | More... |

Demote | Promote...

Title: \* Open access from partner to FTP server Priority: \* High Status: In Progress Ticket Due Date: 2/19/20

## Additional Information

Workflow: General Owner: skyboxview Requestor: skyboxview

Description: \* Partner2 access to the FTP server

Request > Technical Details > Risk Assessment > Implementation Details > Verification

Implementation Preview | Implement... | Mark as Implemented... | Mark as Not Implemented... | Comment... | Revert

ID	Chan...	Firewall/Manag...	Objec...	Change Details	Additional Details	Comment	Change Required	Assignee	Status	Imple...
704	Add R... ⚠	prod FW	-	Source: 200.160.2.0, 200.160.2.2-200.16... Destination: 192.170.33.36/31 Services: 21/TCP Rule Applications: ftp	Source: netInterfac... Destination: netIter... Rule Logging		No - Already Allowed	skyboxvi...		
705	Add R... ⚠	main_FW	-	Source: Host_200.160.2.0 ★, Range_200... Destination: Host_192.170.19.20 ★, Host... Services: ftp Rule Applications: ftp	Source: int18 [200.... Destination: int15 [... Suggested Position: La... Rule Logging	Demo	Yes	skyboxvi...	✓	2/17/20
706	Add R... ⚠	dev FW	-	Source: 200.160.2.0, 200.160.2.2-200.16... Destination: 192.170.19.20-192.170.19.25	Source: int2789 [1... Destination: int279...		No - Already Allowed	skyboxvi...		



# 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

SKYBOX SECURITY

Vulnerability Control

Prioritization

Overview

Discovery

Prioritization

Remediation

Threat Intelligence

Attack Map

Model

Vulnerabilities

Filter Set: All Vulnerabilities 68 +

Sort By: Risk Score

Group By: Business Unit & 'Exposed & Ex...

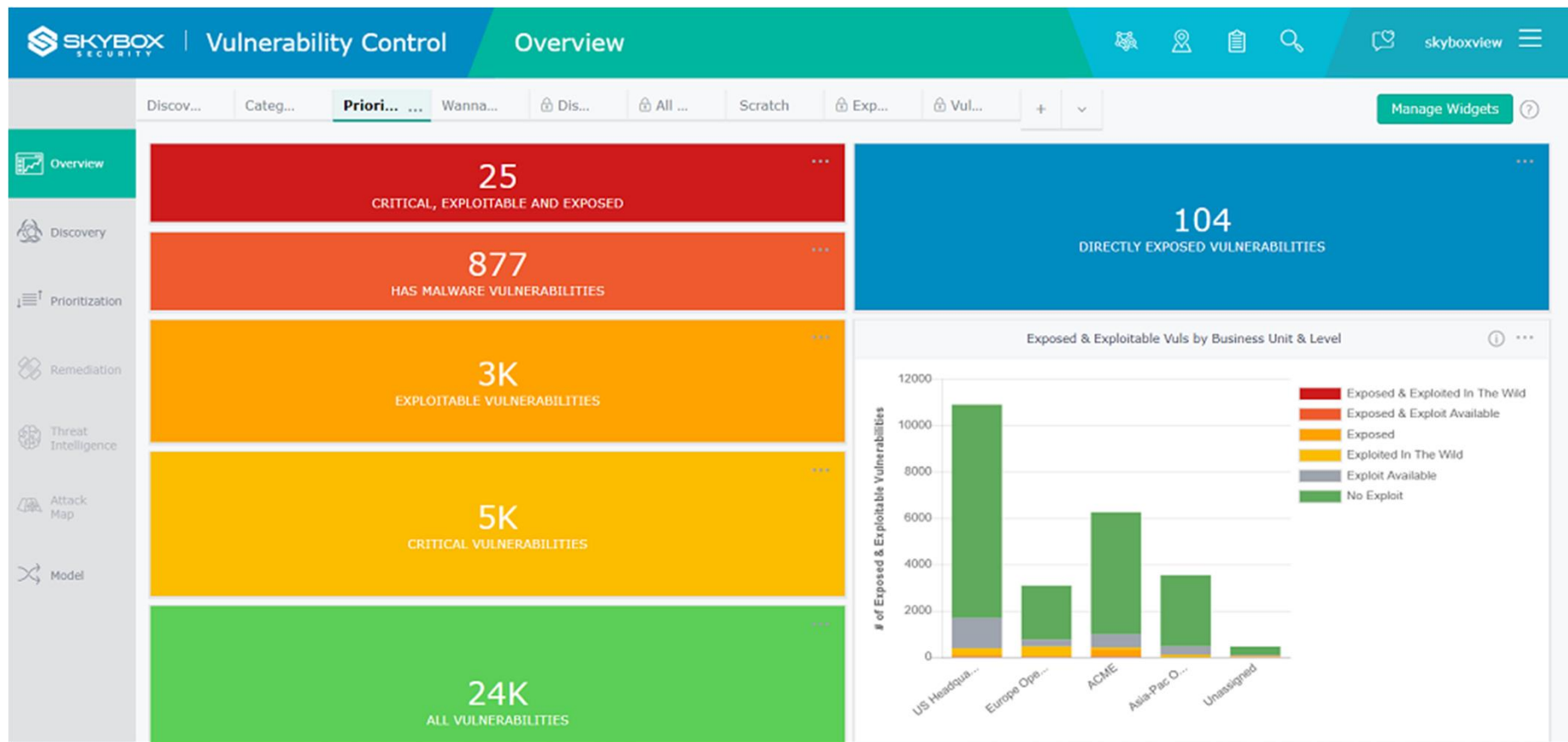
Found 24,216 vulnerabilities

ID	Title	CVSS	Exploitability	Asset	Exposure	Discovery Method	Risk Score
> US Headquarters (10886) Risk Score: 270184							
> Europe Operations (3083) Risk Score: 140687							
v ACME (6250) Risk Score: 85958							
v Exposed & Exploited In The Wild (8) Risk Score: 678							
SBV CVE	SBV-83230 CVE-2018-7600	Drupal Remote Code Execution Vulnerability - CVE-2018-7600	9.8	Exploited In The Wild 7 Exploits	Name OS Import...	dev_ftp0 [192... CentOS CentOS ... 3 (Medium)	Direct Qualys 90
SBV CVE	SBV-95184 CVE-2017-3623	IBM AIX 5.3, 6.1, 7.1, 7.2 and VIOS 2.2.x Remote Code Execution Vulnerability - CVE-2017-3623	10.0	Exploited In The Wild 1 Exploit	Name OS Import...	dev_web5 [192... CentOS CentOS ... 3 (Medium)	Direct Qualys 90
SBV CVE	SBV-83230 CVE-2018-7600	Drupal Remote Code Execution Vulnerability - CVE-2018-7600	9.8	Exploited In The Wild 7 Exploits	Name OS Import...	dev_ftp0 [192... CentOS CentOS ... 3 (Medium)	Direct Qualys 90
SBV CVE	SBV-89682 CVE-2018-11776	Apache Struts Remote Code Execution Vulnerability - CVE-2018-11776	8.1	Exploited In The Wild 5 Exploits	Name OS Import...	dev_web5 [192... CentOS CentOS ... 3 (Medium)	Direct Qualys 89
SBV CVE	SBV-89682 CVE-2018-11776	Apache Struts Remote Code Execution Vulnerability - CVE-2018-11776	8.1	Exploited In The Wild 5 Exploits	Name OS Import...	dev_web0 [192... CentOS CentOS ... 3 (Medium)	Direct Qualys 89



# 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

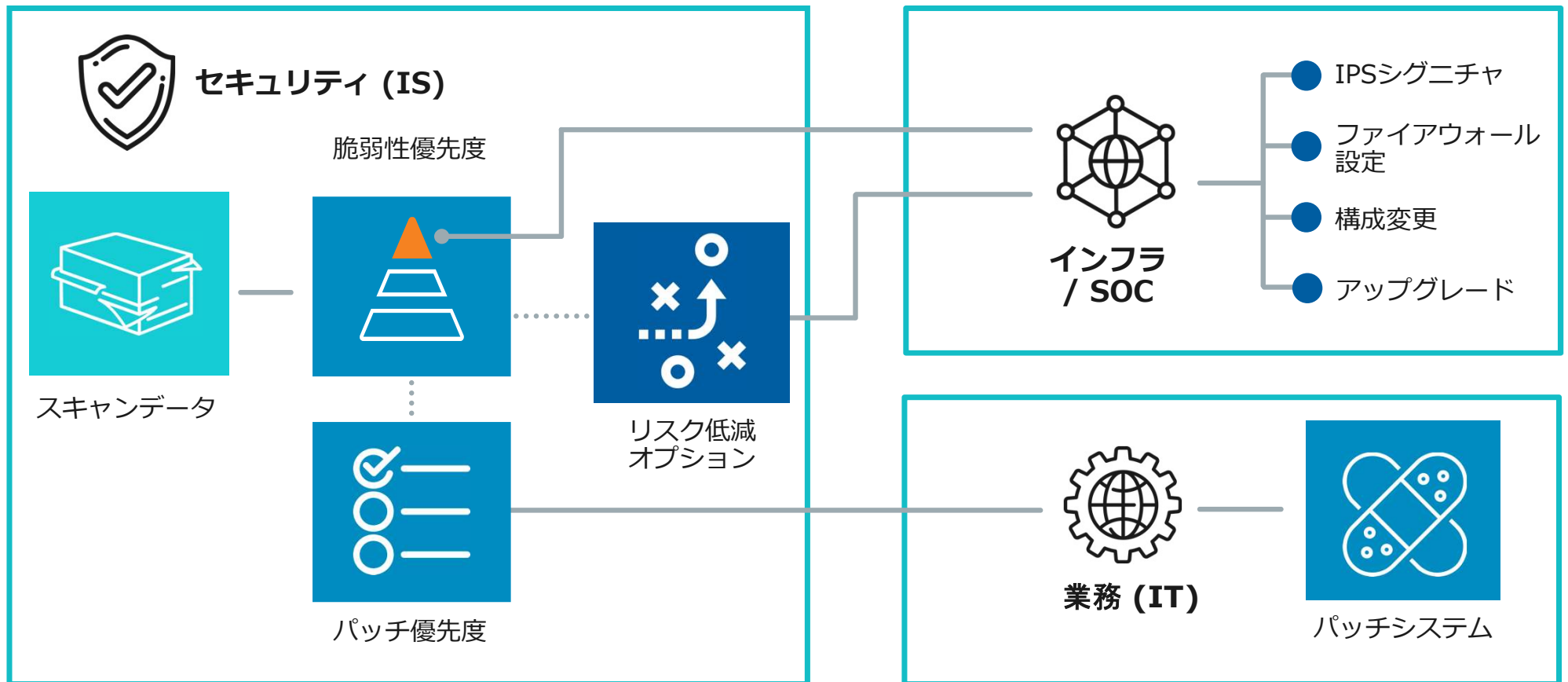




# 複数のリスク対応策



リスク対応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](mailto:skybox_pr@jscom.co.jp)

