

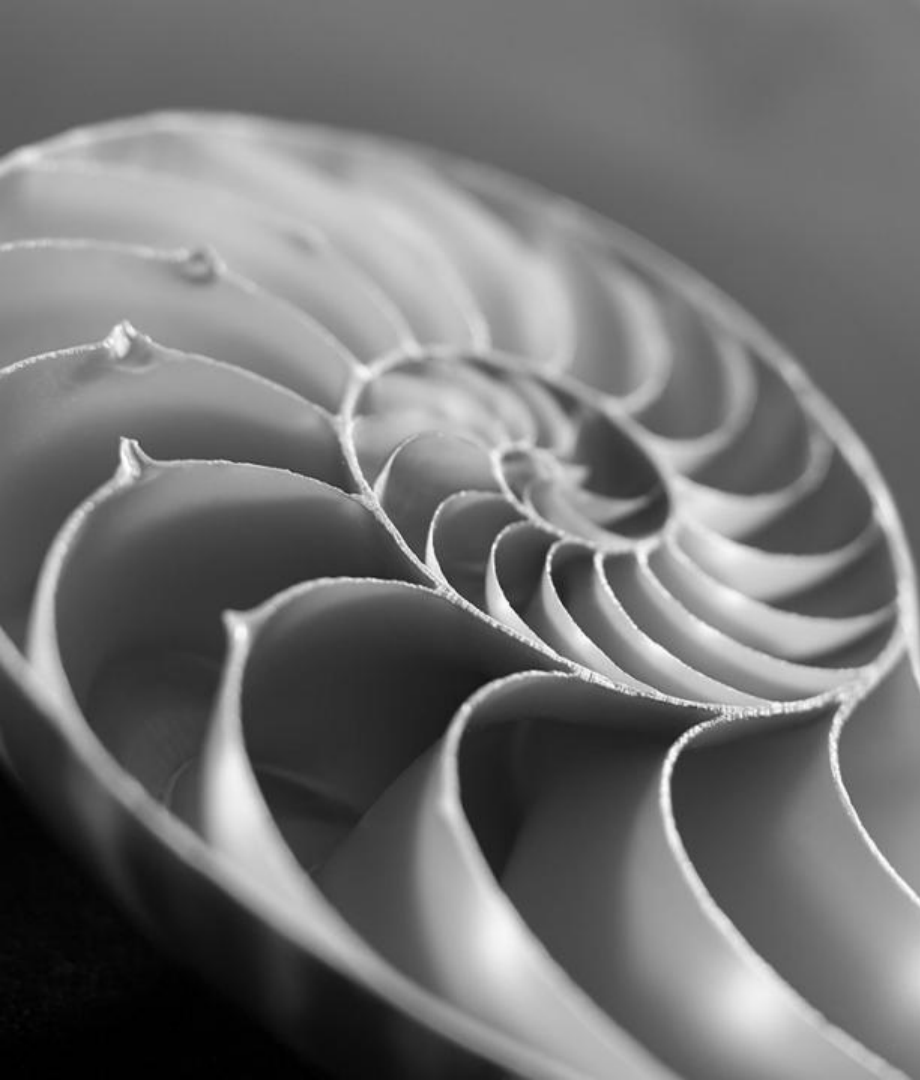
ジュニパーネットワークス コネクテッドセキュリティ

ネットワーク全体で
「ユーザ」「アプリケーション」「インフラ」の
セキュリティを保証する

2019年6月12-14日

JUNIPER
NETWORKS

Engineering
Simplicity



ネットワークセキュリティの課題

あるべきネットワークセキュリティの姿

脅威対応の自動化



IoT・Wi-Fi・BYOD対応

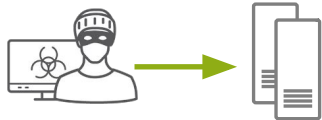


コストの抑制



セキュリティを取り巻く現状

高度化する攻撃



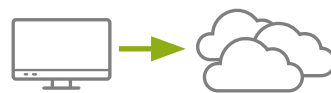
多様化する
就業形態・
増えるデバイス

IoT・BYOD



攻撃後、
脅威が潜伏
発見が長期化

人材不足

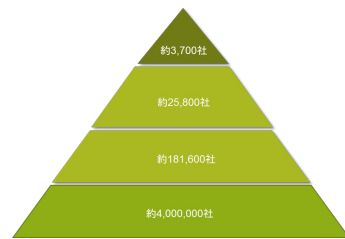


高まるニーズ
教育の限界

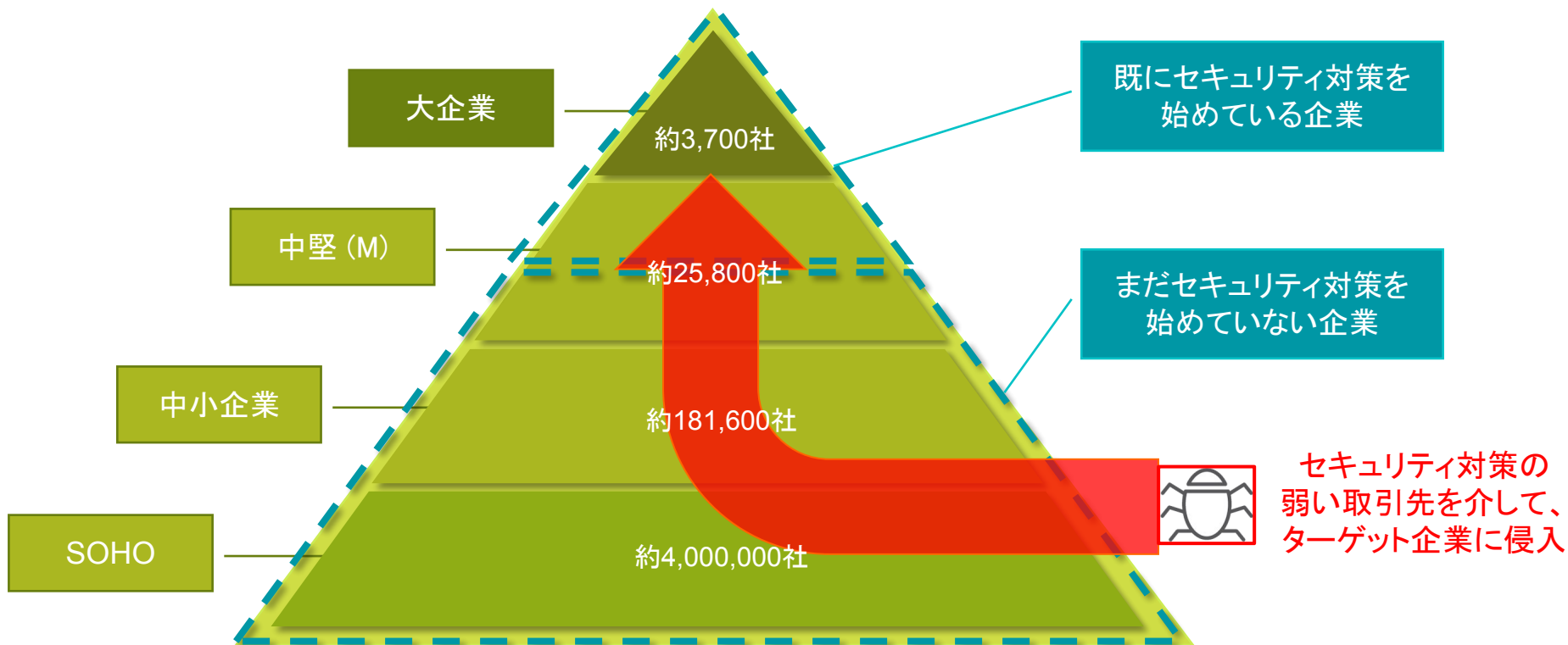
新たな脅威



**サプライチェーン
攻撃**



サプライチェーン攻撃



現実とのギャップ(課題)

脅威対応の自動化



人による手順書ベースの対応
セキュリティ人材不足

IoT・Wi-Fi・BYOD対応



膨大なデバイス数への
エージェント導入
対応OSの増加

コストの抑制



減らないコスト

Are you ready?

(セキュリティ対策は万全ですか?)



ネットワークセキュリティの実現

ジュニパー コネクテッドセキュリティ

「ユーザ」「アプリケーション」「インフラストラクチャ」のセキュリティ対策



脅威の可視化



タスクの自動化

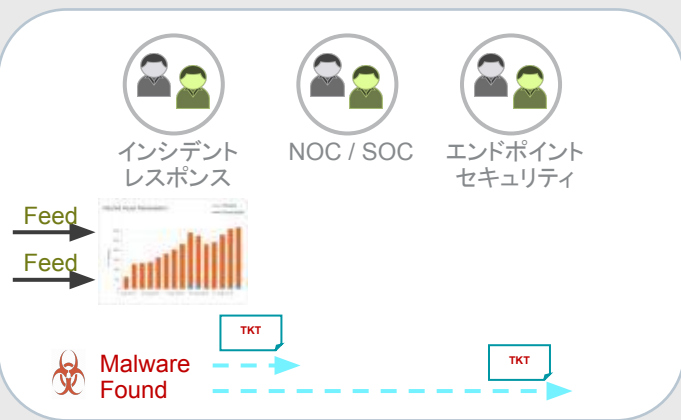


検知から防御まで

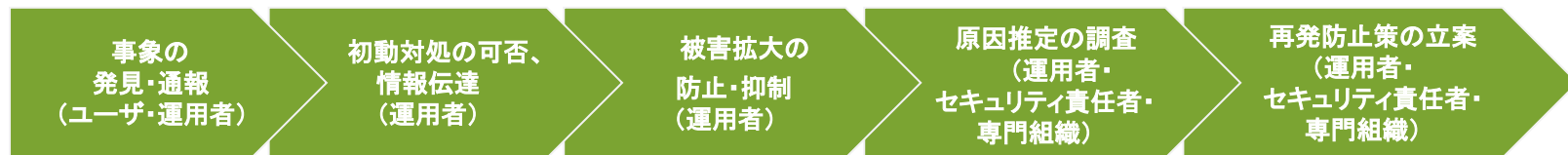
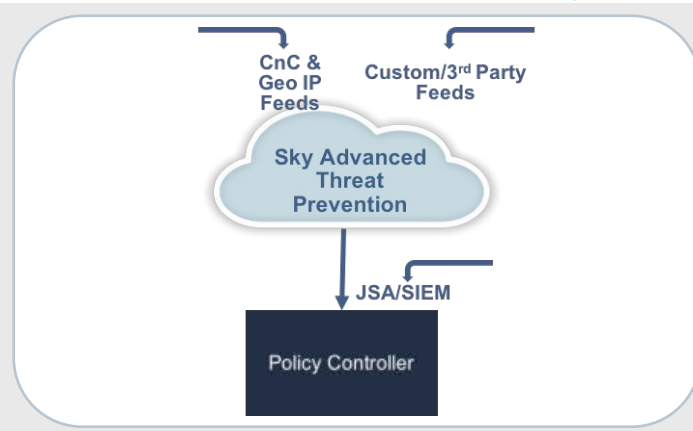
ネットワーク全体にセキュリティを拡張！！

サイバー脅威を自動的に検知し排除する仕組みが必要

手動による脅威への対応

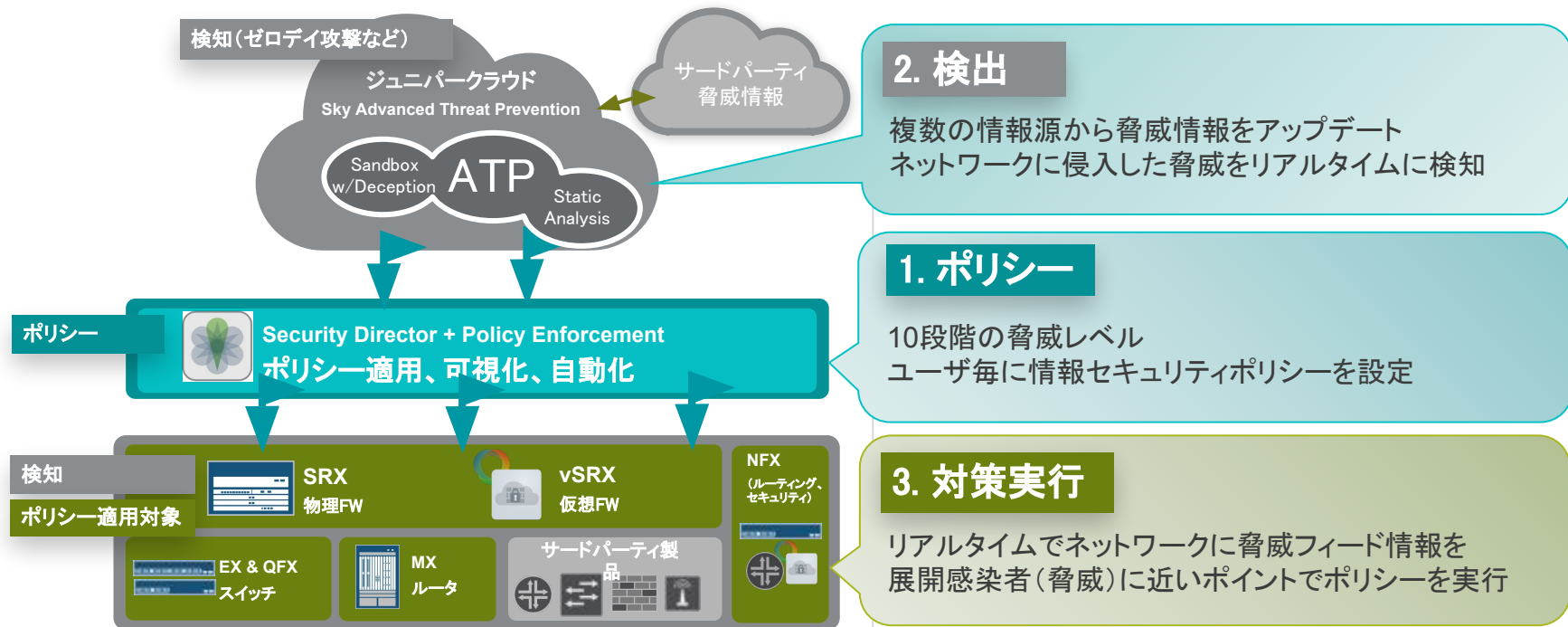


自動的に脅威を検知・排除



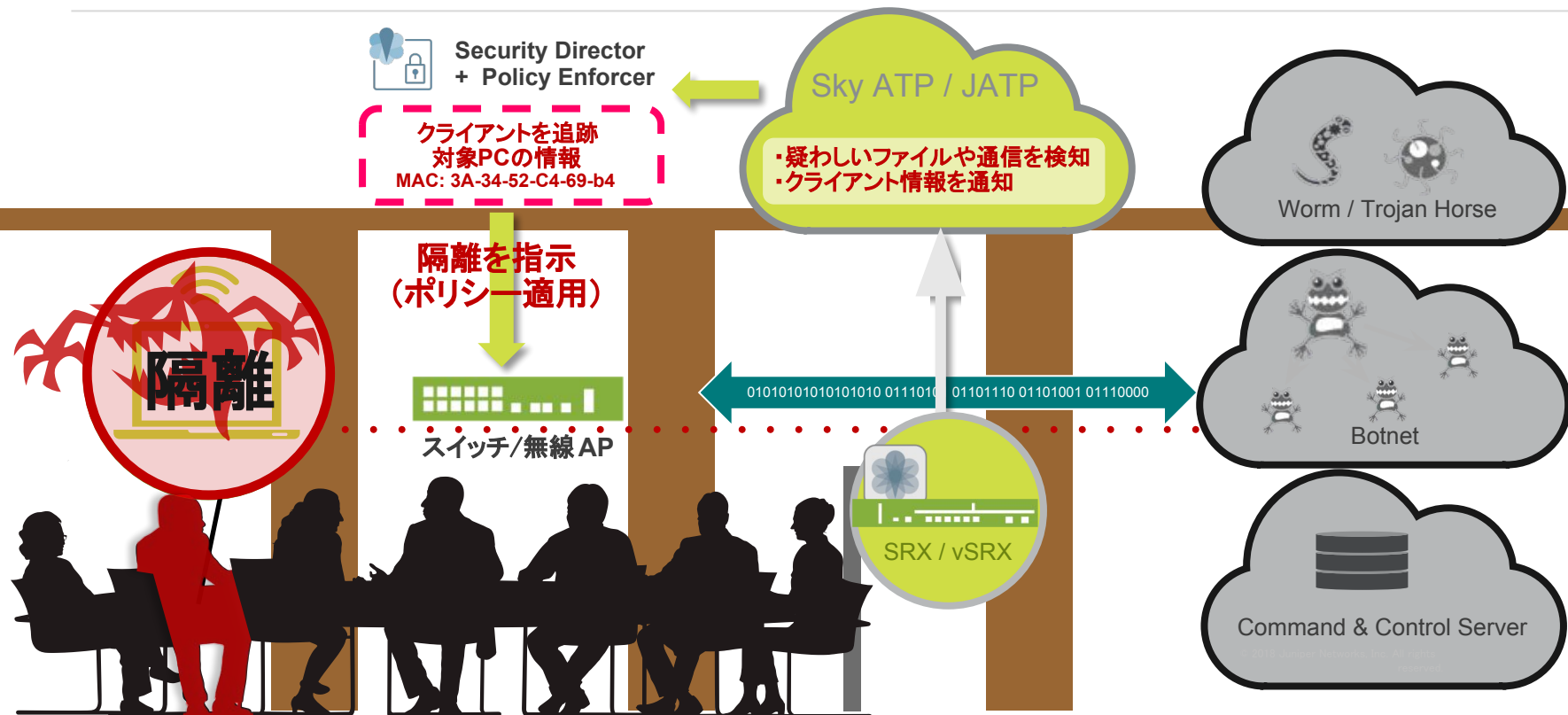
脅威の検知から、対応・防止策までを自動化

ネットワークをセキュリティドメインとして、自動検知と対処

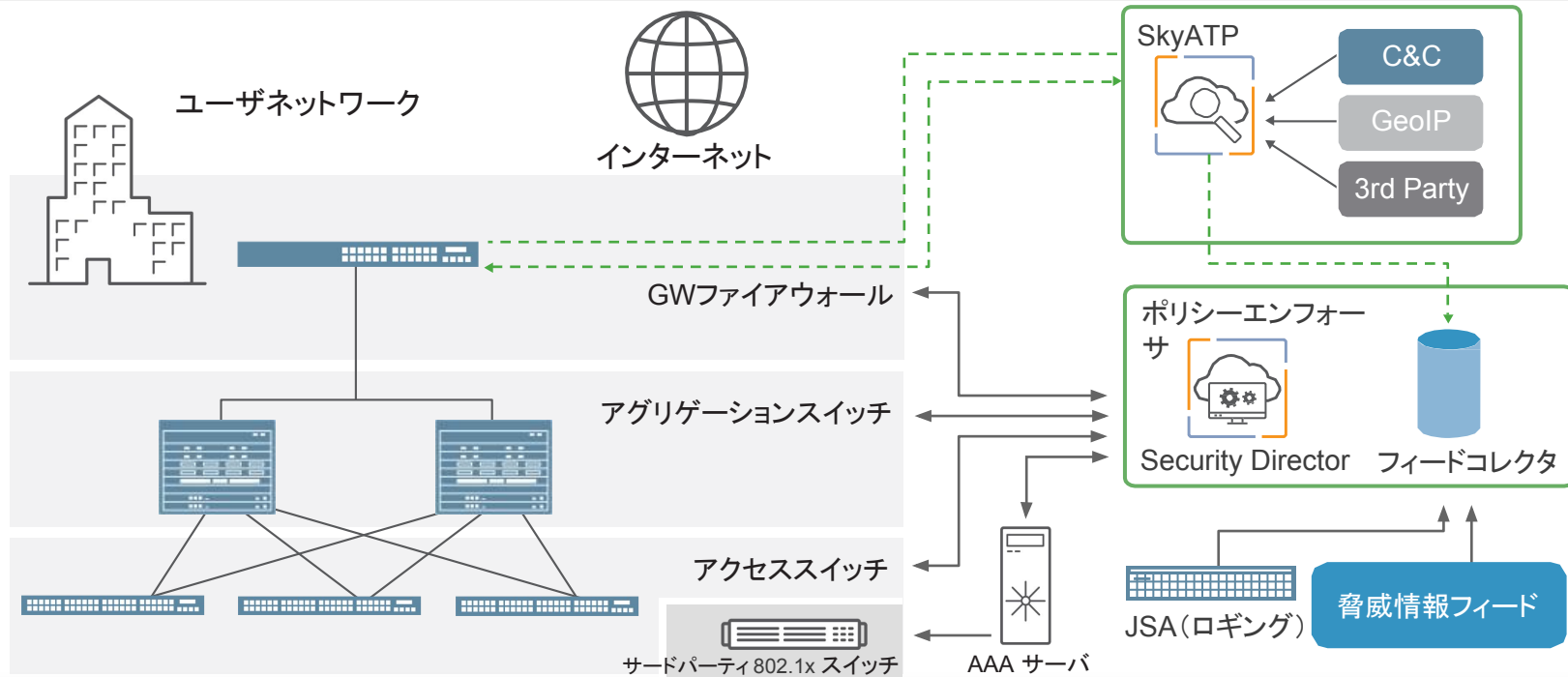


ネットワーク全体を単一の対策実行ドメインに！それぞれの機器がポリシーの適用ポイント

MACアドレスで隔離



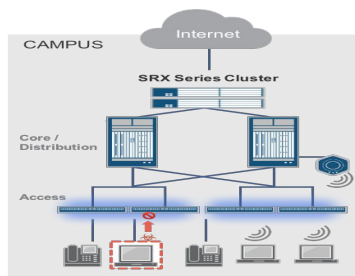
企業ネットワークの構成例



ネットワークをSDN制御可能なセキュリティドメインとして構成することで、侵入したサイバー脅威を自動的に検知して、その対処・防止策を実行する。

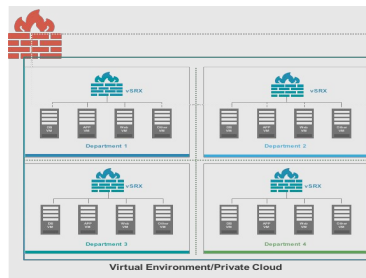
コネクテッドセキュリティのユースケース

企業のキャンパスネットワーク



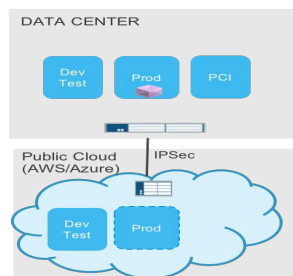
感染ホストの自動
検知と脅威の隔離

プライベートクラウド



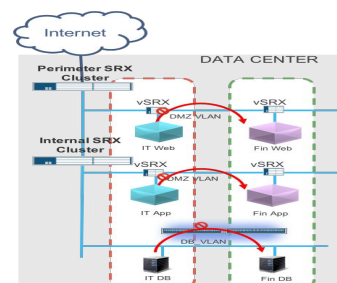
ダイナミック
セグメンテーション、
および
サービス
チェイニング

マルチクラウド



クラウドアプリと
オンプレの一貫した
ポリシー制御

データセンタ マイクロセグメンテーション



物理および仮想環
境における
East-West
トラフィックの制御

セキュリティポートフォリオ



Management, Automation



SIEM



Advanced Threat Protection



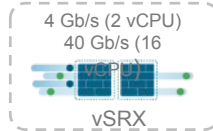
IPS/IDS
Anti Malware
Application Security
URL Filtering
IoT Security
Security Services



Router
Integrated Security



NFX



Advanced Security Acceleration (SPC3)



SD-WAN
Capable

SRX300



2U
5.5Gb/s

SRX500



1U
5Gb/s

SRX1500



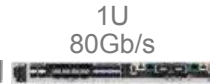
1U
20Gb/s

SRX4100



1U
40Gb/s

SRX4200



1U
80Gb/s

SRX4600



5U
280 Gb/s

SRX5400



8U
560 Gb/s

SRX5600



16U
1.2 Tb/s

SRX5800

Routing/SD-WAN

IPsec/VPN

High Availability

SSL/TLS Proxy

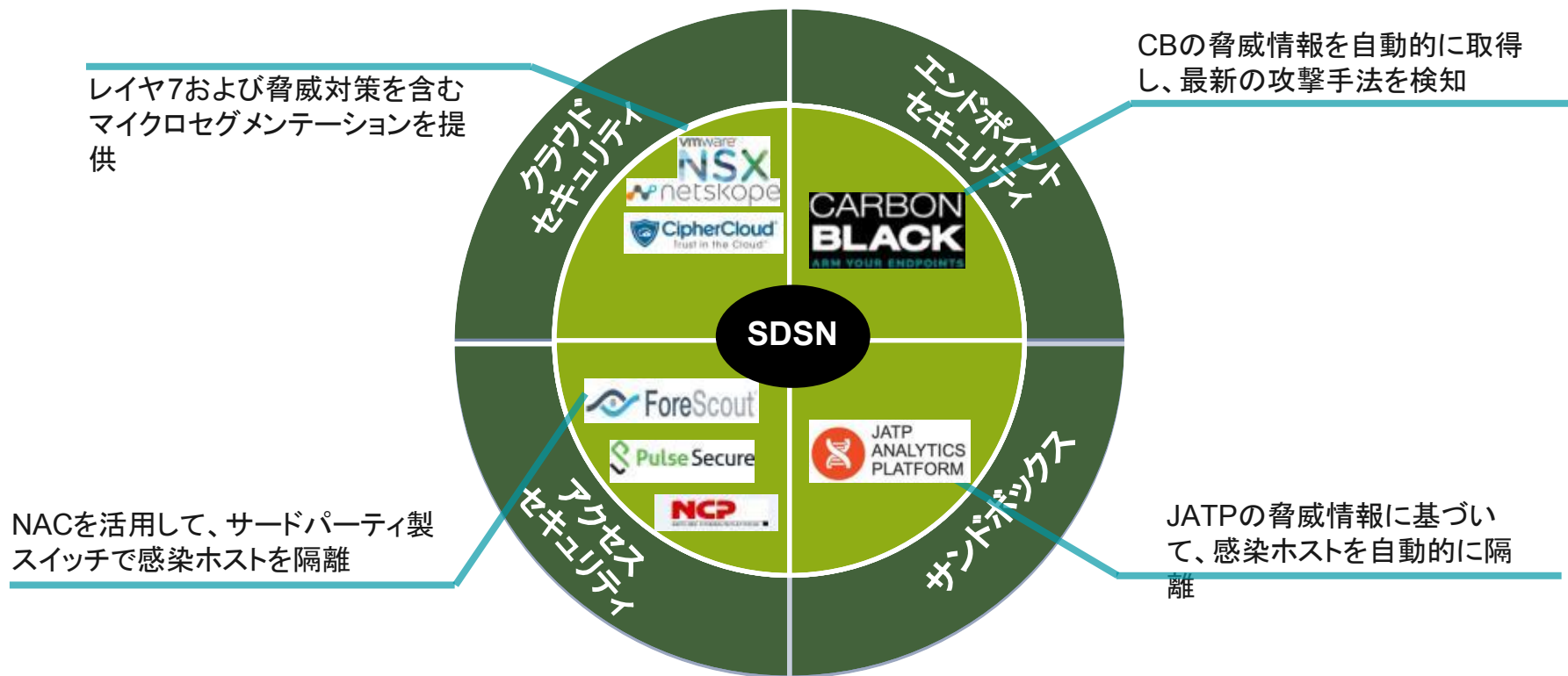
Branch

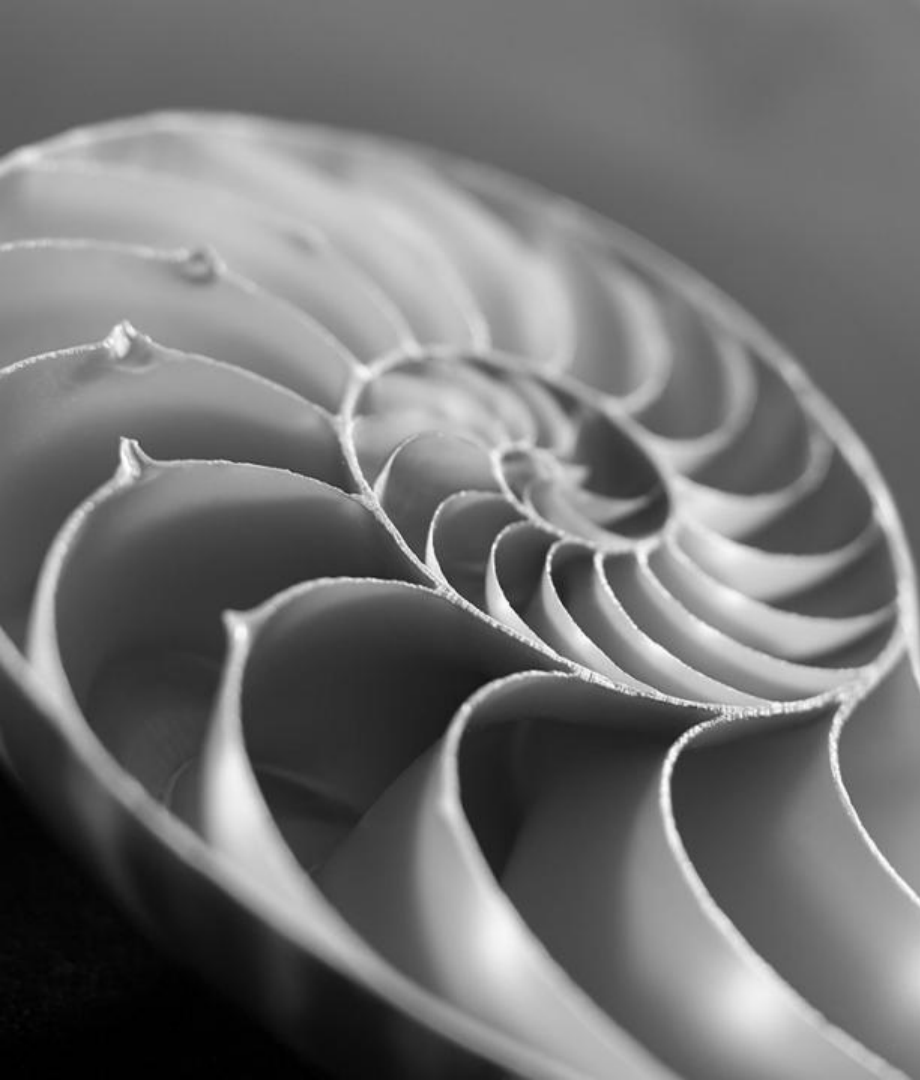
Campus

Private Cloud/Multicloud

Large Data Center/Service Provider

Connected Securityサードパーティ連携





ネットワークセキュリティ導入の ポイント

なぜ、ジュニパーのセキュリティなのか？



ユーザの課題

セキュリティ担当者・
専任のセキュリティ技術者の不足



IoTやBYOD等の持ち込まれる脅威による
セキュリティリスク



ネットワーク内に侵入した脅威が拡散する前に
迅速に対応したい



Juniperの提案

脅威検知および施行を自動化することで、
セキュリティ担当者のワークロードを軽減し、迅速かつ正確に脅威への対処

ネットワーク全体で脅威を検知し、
エージェントレスで MACアドレス
により感染デバイスを隔離

サードパーティ製品へ自動的にポリシーを
適用することにより、被害の拡散を抑制
することが可能

Juniperのセキュリティで、最先端の安全 & コストの抑制！！



THANK YOU

JUNIPER
NETWORKS

Engineering
Simplicity