

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、
およびインフラのセキュリティを確保する

2019年9月24日

ジュニパーネットワークス株式会社
技術統括本部

JUNIPER
NETWORKS

Engineering
Simplicity

内容

JUNIPER
NETWORKS®

セキュリティを
もっと簡単に

サイバーセキュリティ脅威の傾向と企業IT担当者の課題

ジュニパーネットワークスセキュリティに対する取り組み

運用負荷を大幅に削減するConnected Security

多層防御の課題を解決するConnected Security

まとめ



サイバーセキュリティ脅威の 傾向と企業IT担当者の課題

IPA 情報処理推進機構の「情報セキュリティ10大脅威 - 2019」

「情報セキュリティ10大脅威 2019」

順位		順位	
1位	標的型攻撃による被害	6位	サービス妨害攻撃によるサービスの停止
2位	ビジネスメール詐欺による被害	7位	インターネットサービスからの個人情報の窃取
3位	ランサムウェアによる被害	8位	IoT機器の脆弱性の顕在化
4位	サプライチェーンの弱点を悪用した攻撃の高まり New	9位	脆弱性対策情報の公開に伴う悪用増加
5位	内部不正による情報漏えい	10位	不注意による情報漏えい

引用: IPA 「情報セキュリティの企業向け10大脅威」より <https://www.ipa.go.jp/security/vuln/10threats2019.html>

IPA 情報処理推進機構の「情報セキュリティ10大脅威 - 2019」

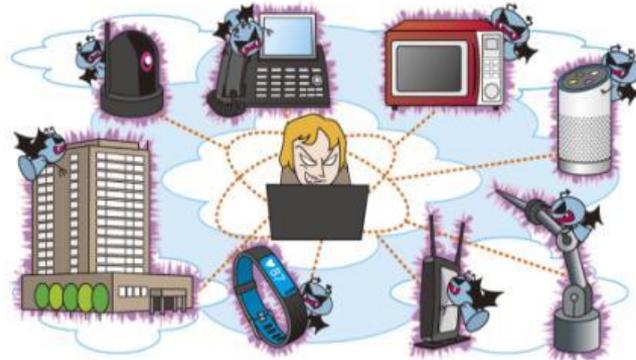
第1位 標的型攻撃による被害



第4位 サプライチェーンの弱点を悪用した攻撃の



第8位 IoT機器の脆弱性の顕在化



IoT機器をウイルスに感染させ、そのIoT機器を踏み台として大規模なDDoS（分散型サービス妨害）攻撃を行い、サービスやネットワーク、サーバーに悪影響を与える被害が確認されている。IoT機器は稼働台数が多く、脆弱性対策も浸透していないことからサイバー攻撃の対象になりやすい。IoT機器を狙ったサイバー攻撃は年々増加傾向で深刻な被害も発生しており、早急なセキュリティ対策が必要となっている。

原材料や部品の調達、製造、在庫管理、物流、販売までの一連の商流、およびこの商流に関わる複数の組
ンと呼ぶ。また、組織が特定の業務を外部組織に委託している場合、この外部組織もサプライチェーンの一
組織がセキュリティ対策を適切に実施していないと、業務委託元組織への攻撃の足がかりとして狙われる。
が攻撃され、預けていた個人情報漏えいする等の被害が発生している。

組織の従業員や元従業員等、組織関係者による機密情報の漏えい、費用等の不正行為が発生している。組織関係者による不正行
為は、組織の社会的信用の失墜、損害賠償による経済的損失等により、組織に多大な損害を与える。

引用: IPA「情報セキュリティの企業向け10大脅威」より <https://www.ipa.go.jp/security/vuln/10threats2019.html>

企業IT担当者の抱える課題

IT担当やセキュリティ
エキスパートの不足



「働き方改革」の実現に向けて、
情報システム部門においても
業務改善が求められている

多様化するサイバー脅威に対して
正確で迅速な対応



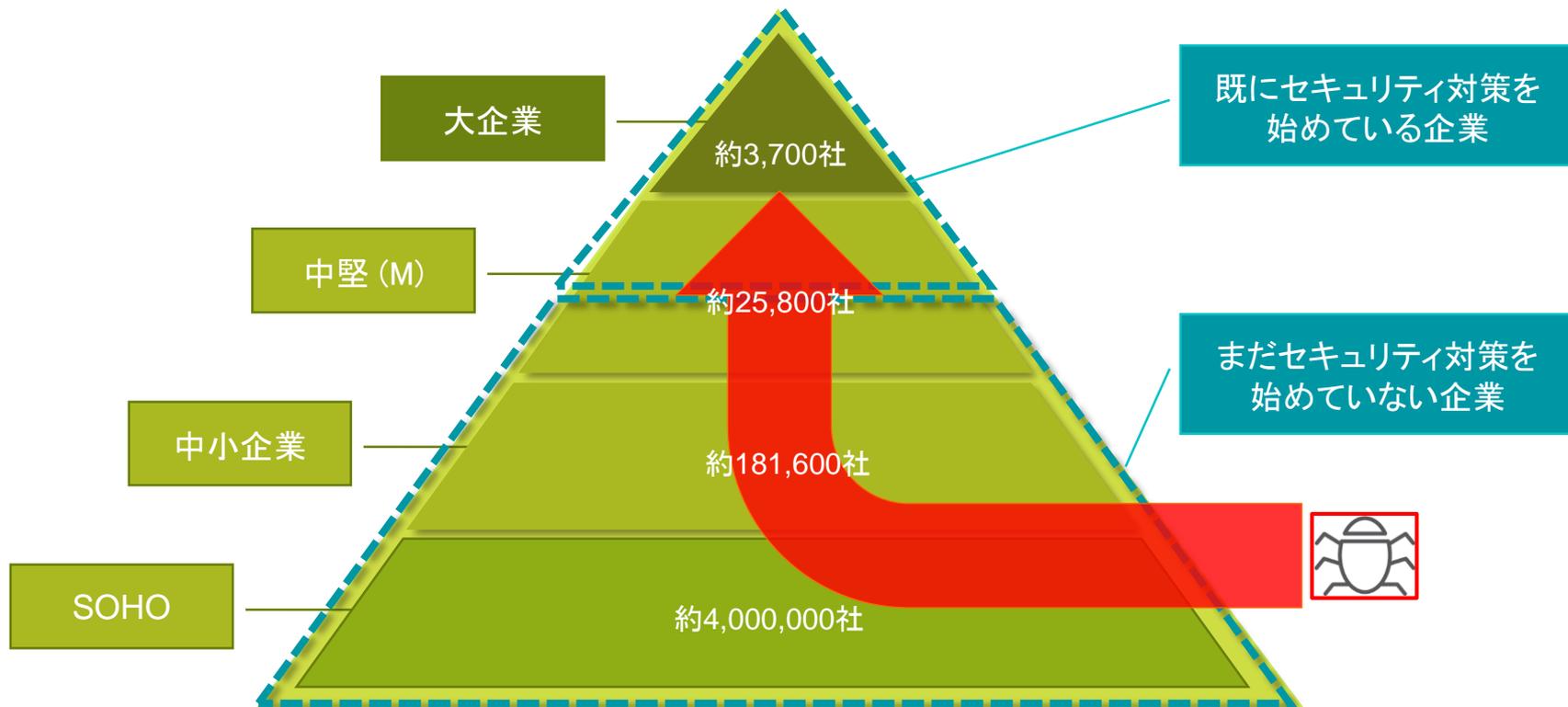
「多層防御」の運用負荷が増大し、
コストを掛けずに正確で迅速な
運用を行うことが難しい。

IoTやBYOD等、増え続ける
デバイスのセキュリティ管理



エージェントソフトウェアの更新、
IoTやBYODデバイスの管理が
困難になってきている

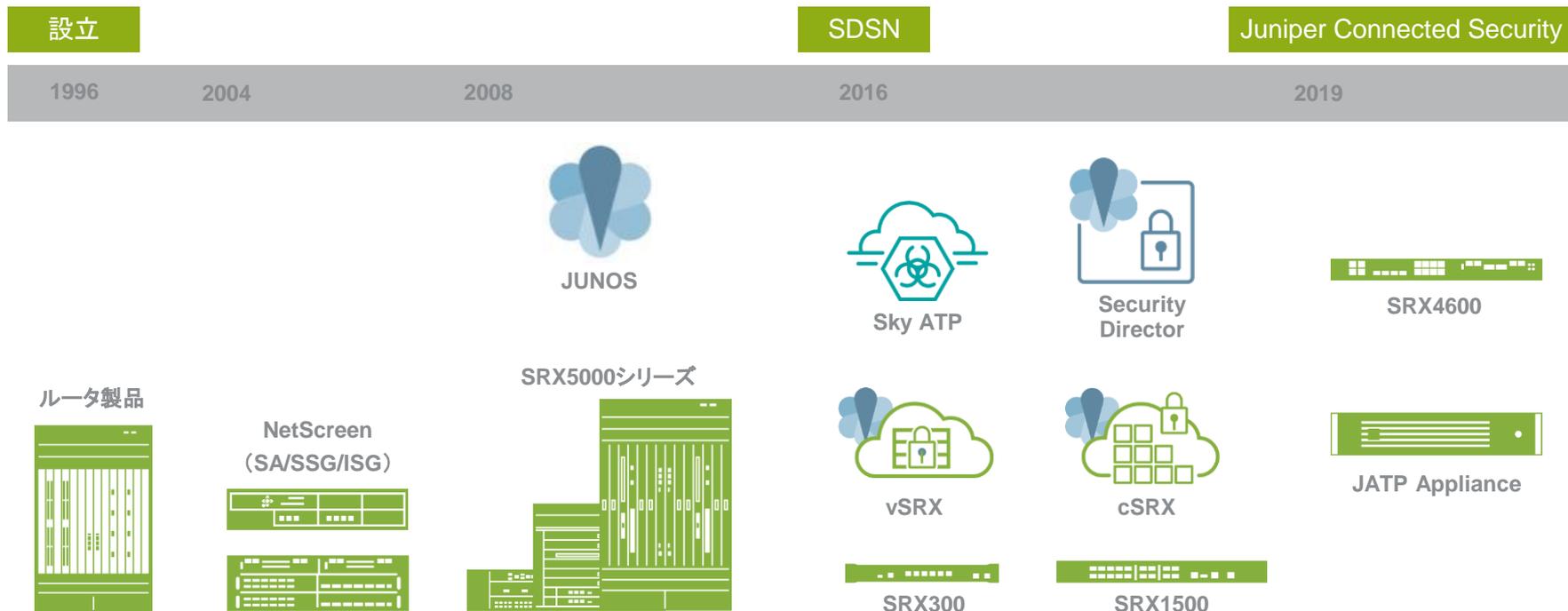
サプライチェーン攻撃





ジュニパーネットワークス セキュリティに対する取り組み

ジュニパーのセキュリティに対する取り組み





運用負荷を大幅に削減する Connected Security

ジュニパーのConnected Security



監視



- マルチベンダ環境における
- セキュリティのイベント
 - 脅威インテリジェンス



可視化

自動化



- すべてもセキュリティシステムで
関係して脅威を検知
- ノイズの多いログから脅威を発見



検知



- 感染ホストの自動隔離
- ワンタッチのリスク軽減
- サードパーティ連携

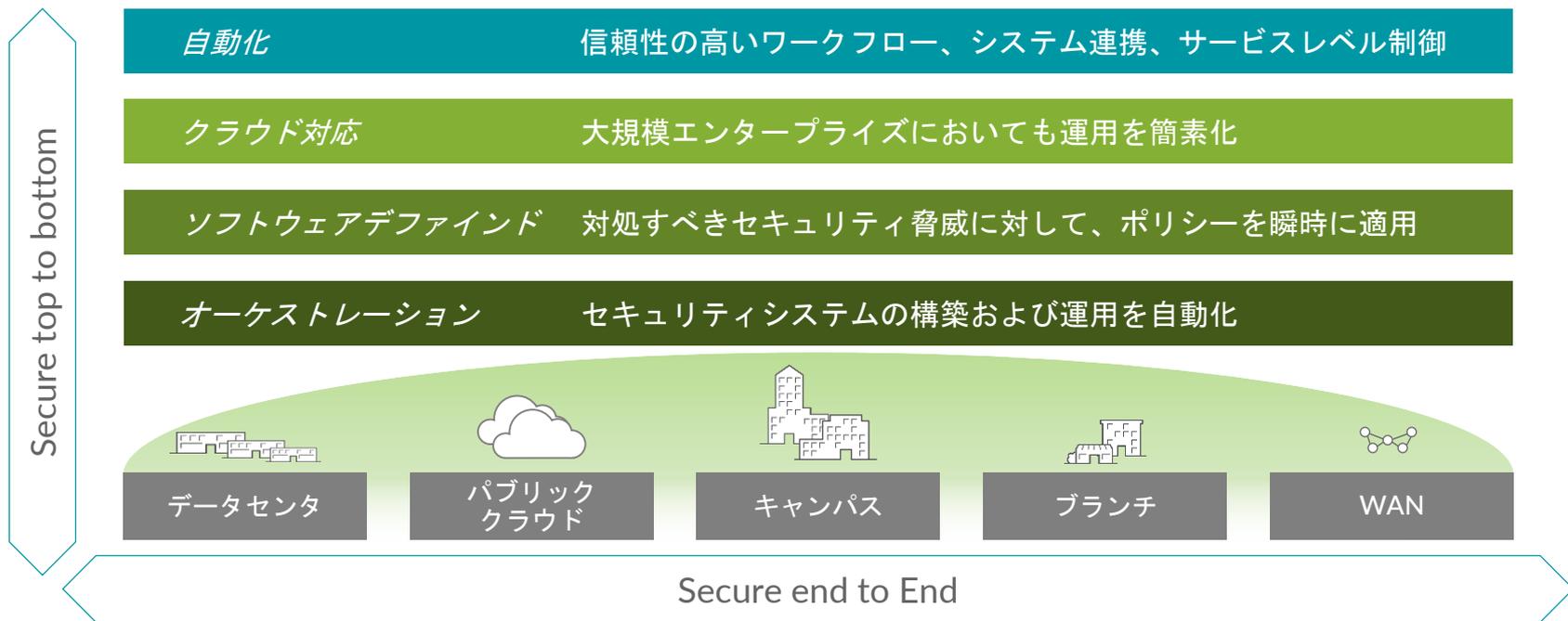


対処

防御

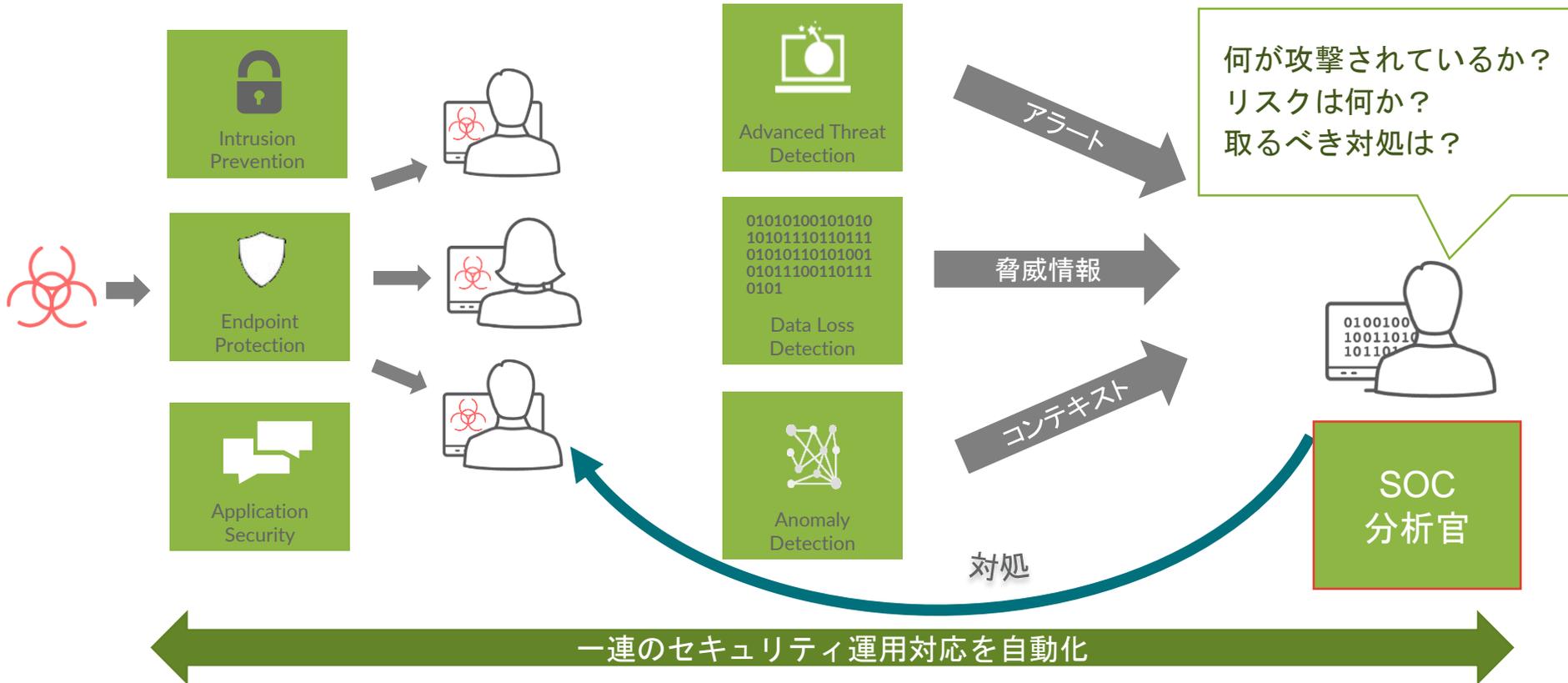


可視化：エンドポイントから、エッジおよびクラウドまで



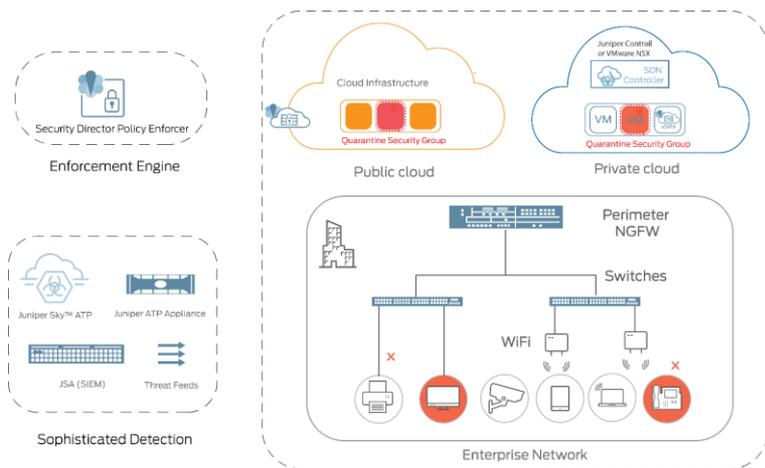


機械学習による検知：データ収集および解析



自動化された対処：既定ルールまたはカスタムアクション

自動脅威制御



- 段階的な隔離レベル
- パブリッククラウド、プライベートクラウドおよびオンプレ環境において、ネットワークレベルで脅威を封じ込める
- サードパーティ製品との連携（スイッチ、WiFi AP, EDR）

DevOpsとの連携

標準ベース



サードパーティ連携



ネットワーク運用の簡素化

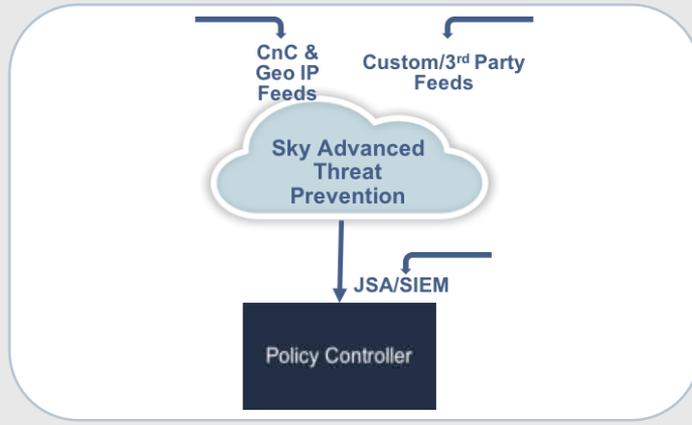


Connected Security: セキュリティ脅威を自動的に検知し排除する仕組み

手動による脅威への対応

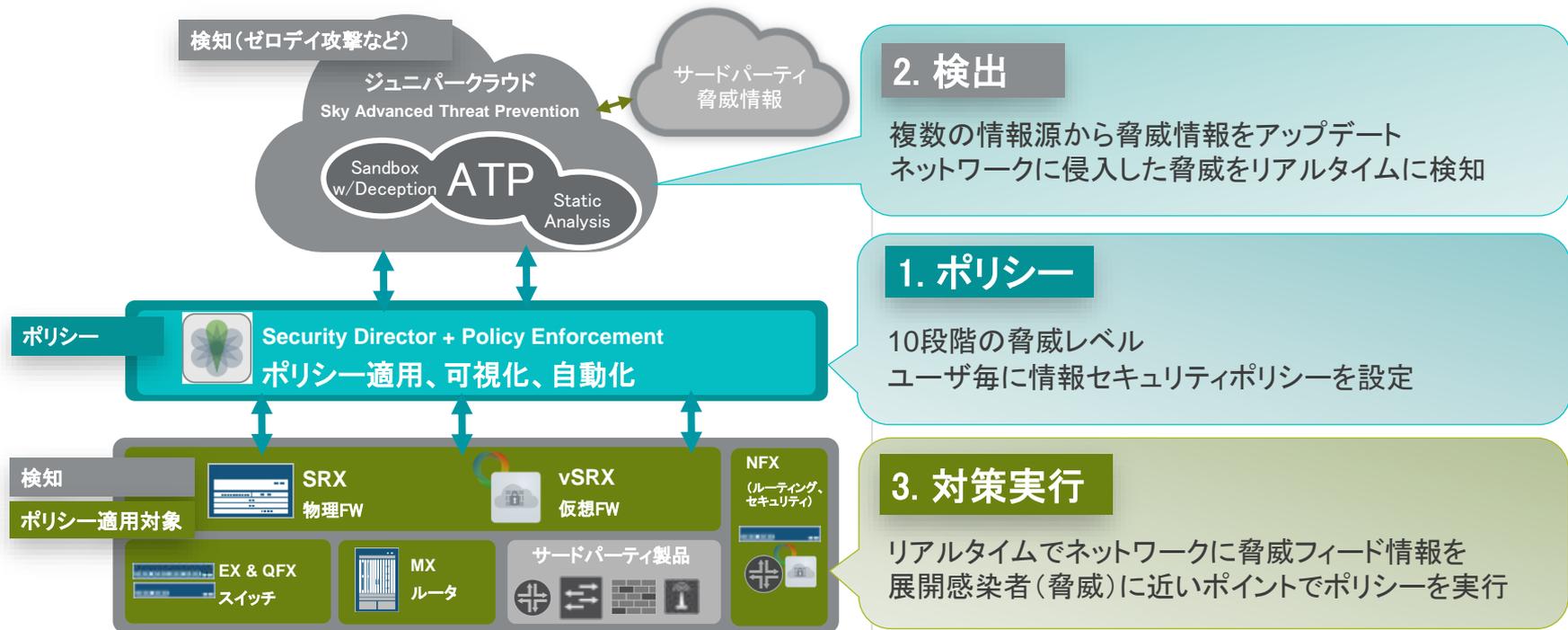


自動的に脅威を検知・排除



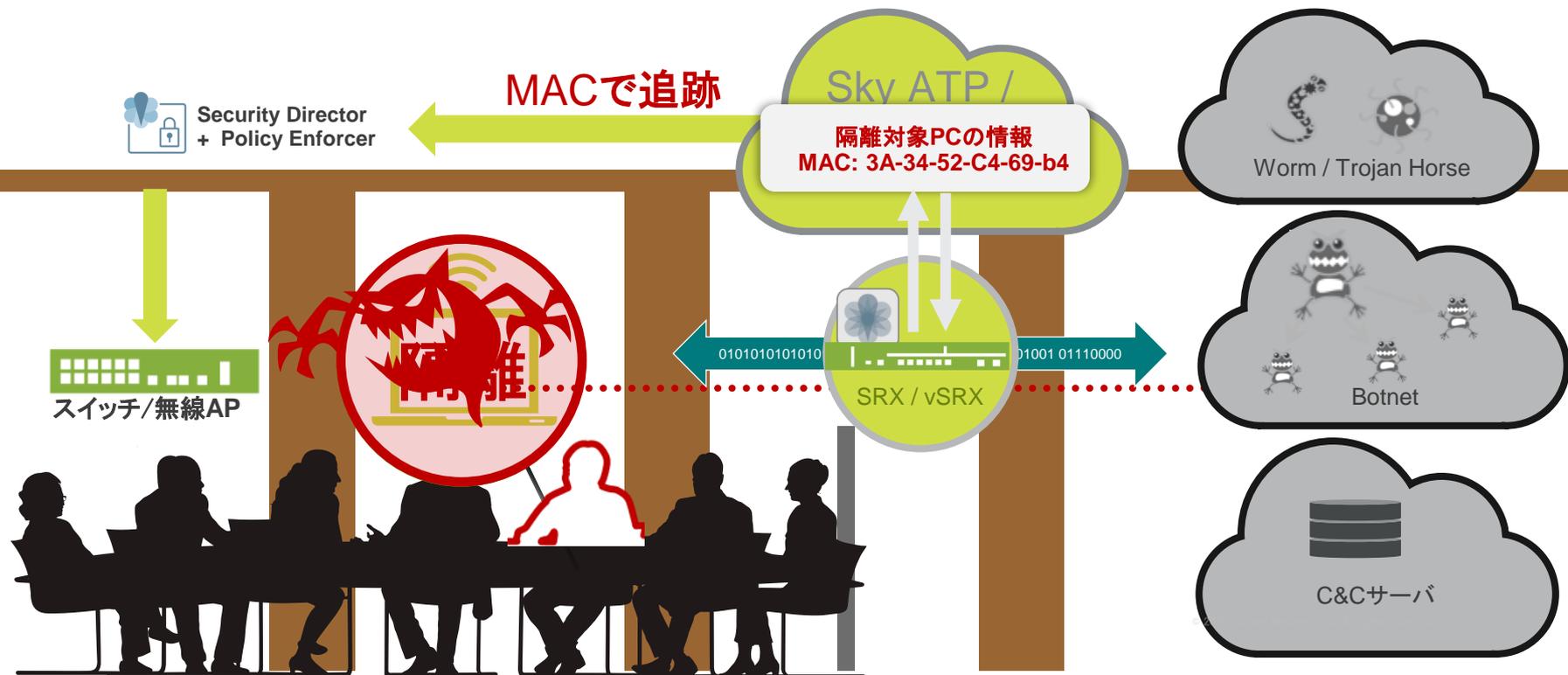
脅威の検知から、対応・防止策までを自動化

Connected Security: 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

Connected Security: MACアドレスで追跡・隔離



標的型攻撃対策 (ATP) のポートフォリオ

SaaS



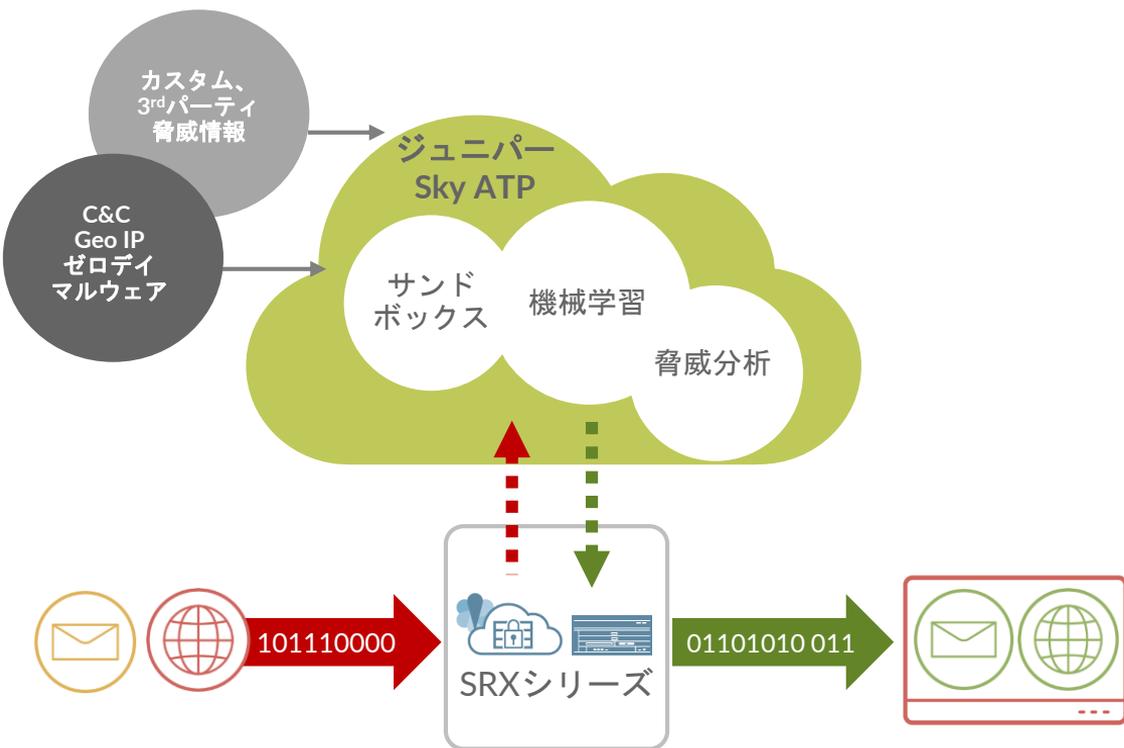
Sky ATP

オンプレ



JATPアプライアンス

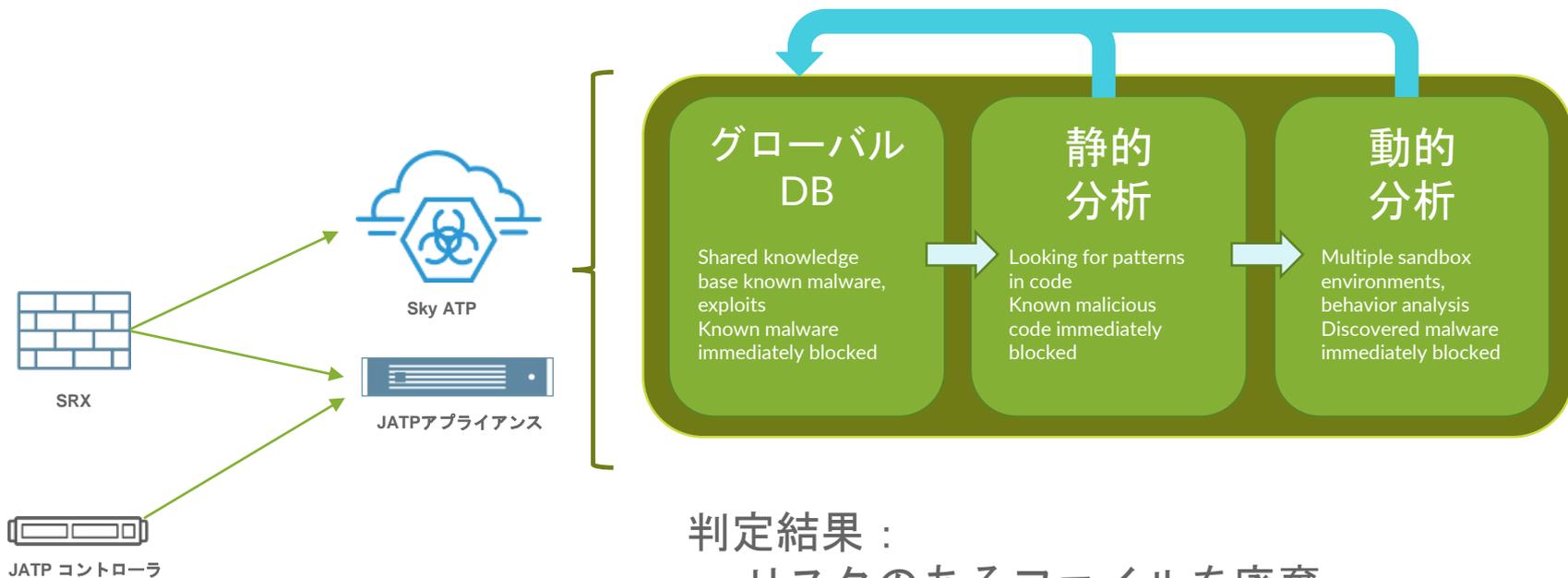
Sky ATP - クラウドベースの脅威防御サービス



- ランサムウェアなどの高度なマルウェアからの保護
- 脅威インテリジェンス
 - レピュテーション
 - フィード情報 (C&C, GeoIP, カスタム)
- ウェブとメールのファイルを分析
- 日本、欧州、米国、カナダにデータセンターを設置
- STIX / TAXII
- FedRAMP認定



ATPマルウェア検知フロー



判定結果：

- リスクのあるファイルを廃棄
- グローバルDBにはHash値を追加

Sky ATP管理画面のイメージ

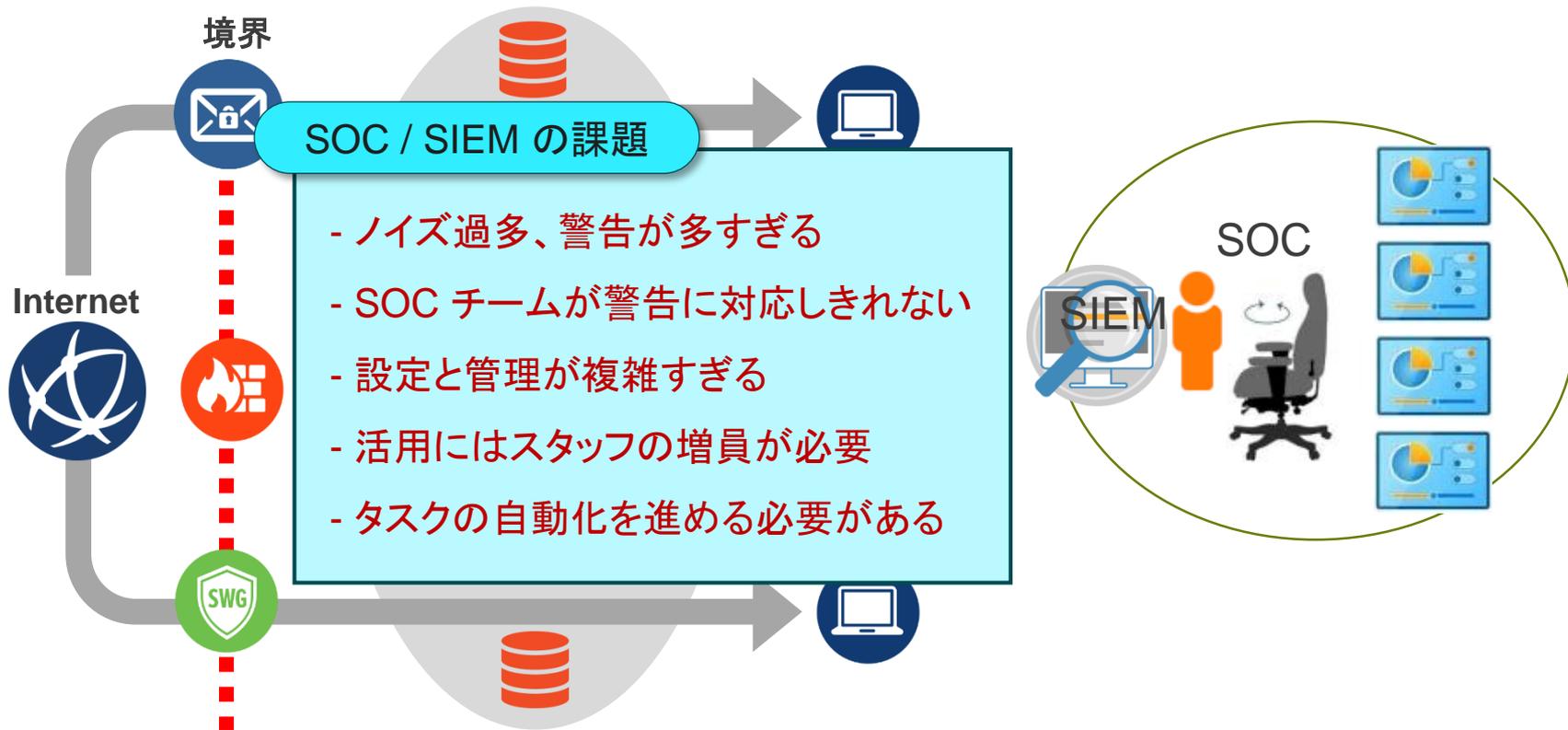
The screenshot displays the Sky ATP management interface, which is divided into several sections:

- Header:** Shows the product name "SKY ADVANCED THREAT PREVENTION" and the user "security-tme@juniper.net".
- Left Navigation:** Includes "Hosts", "C&C Servers", "File Scanning" (with sub-items for HTTP File Download, Email Attachments, and Manual Upload), and "Email Quarantine".
- Main Content Area:**
 - Email Attachments:** A summary view showing a threat level of "High" (indicated by a red circle) and a status of "Clean, no action is required".
 - Event Log:** A table listing events with columns for "Time", "Filename", and "Recipient".
- Host Details (Host 192.168.222.111):**
 - General:** Host IP, Host Status (Clean), and Threat Settings.
 - Threat Settings:** Investigation Status (Resolved - Fixed) and Policy override options.
 - Time Range:** A bar chart showing the host's threat level over time from April 11 to May 10. The threat level starts at Low (yellow), moves to Medium (orange), and then to High (red) around May 17.
- Behavior Analysis (Behaviors by Severity):** A donut chart showing the distribution of behaviors by severity. Key behaviors include File-grained behavior (26%), Persistence (25%), and Evasion (15%).

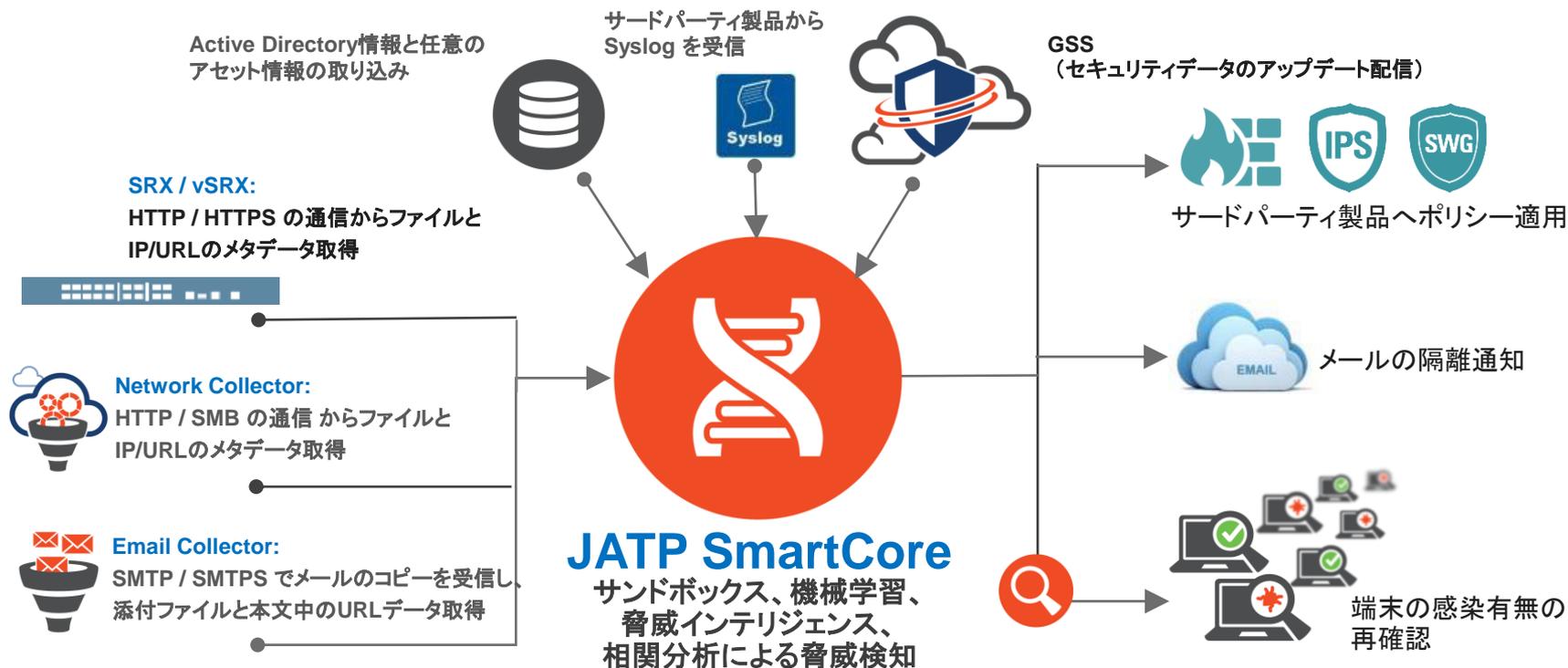


多層防御の課題を解決する Connected Security

多層防御環境における課題



JATP (機械学習を駆使し、脅威を自動分析/可視化・自動対応)

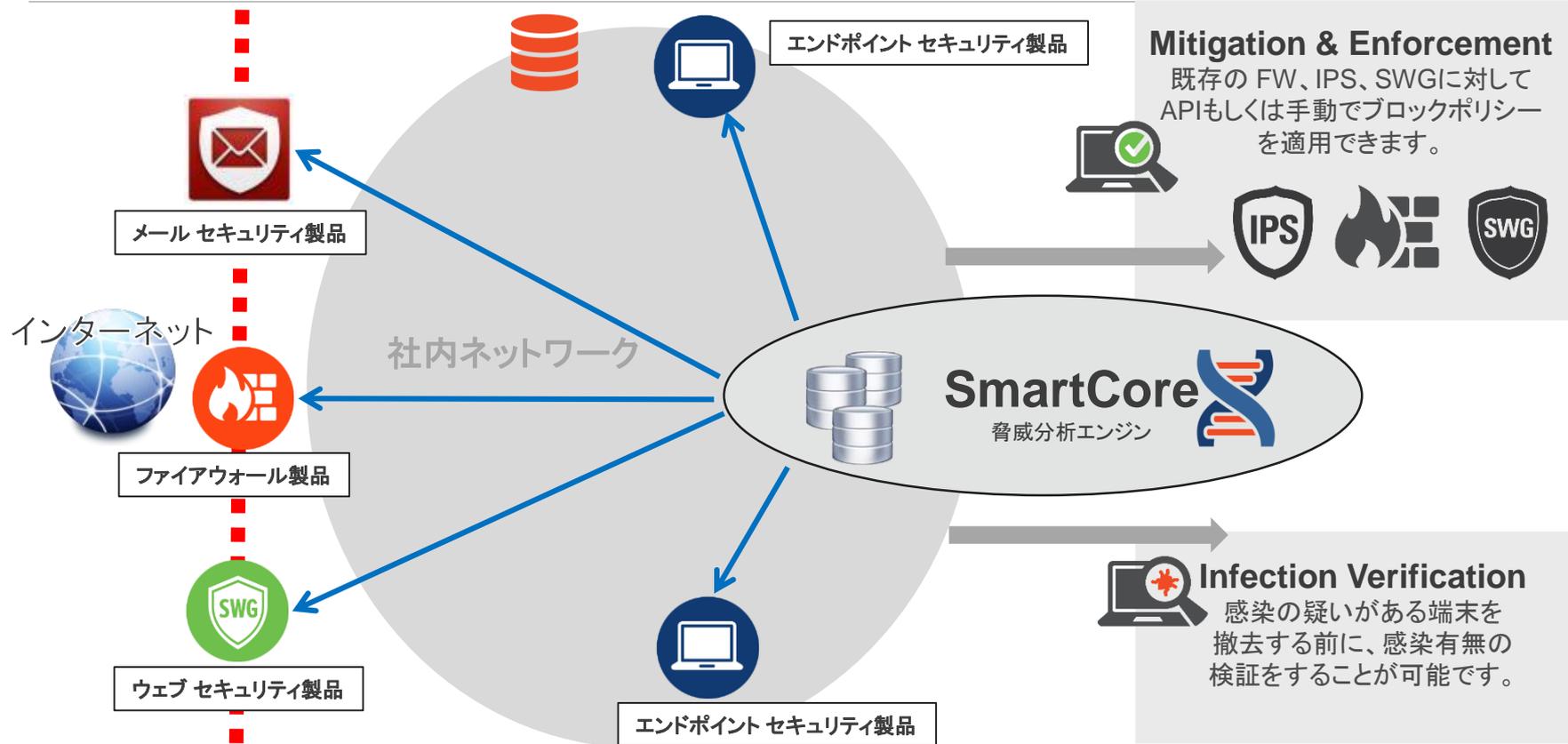


未知の脅威検知

先進的な分析

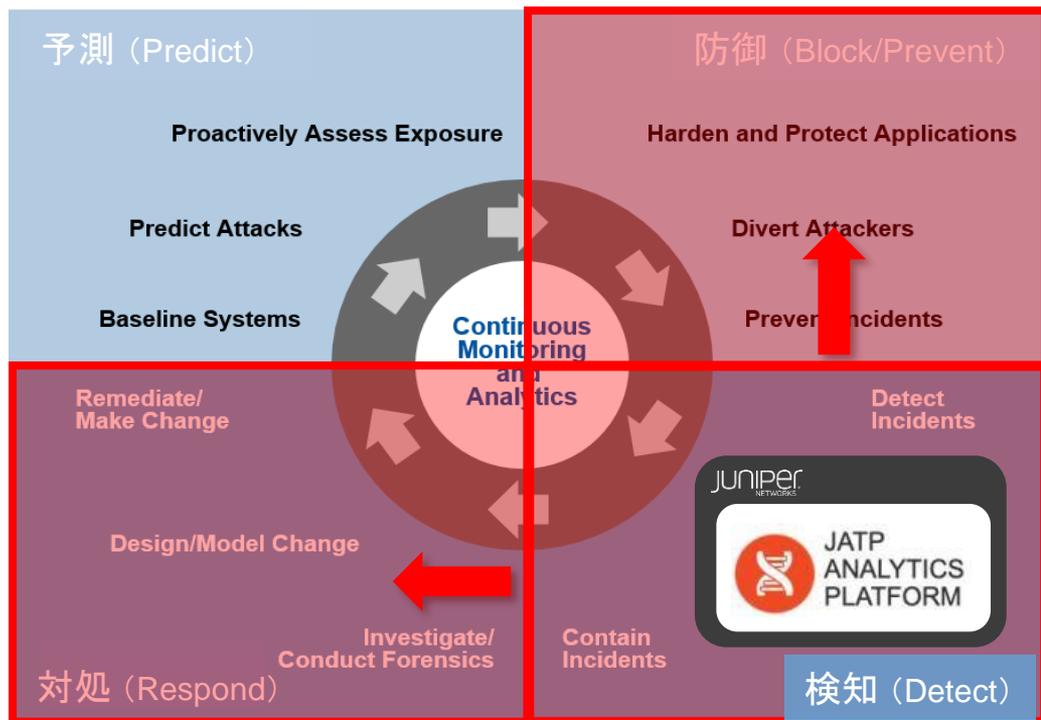
迅速な対応

インシデントレスポンスの自動化



強固な検知能力、対処及び防御との連携

“サンドボックスの検知能力は極めて重要である。何故なら・・・
既に脅威が侵入していることを前提に、素早く対処しなければならないから。”



Gartner 評価の連携モデル

- ✓ セキュリティの防衛ラインを突破した脅威を素早く発見
- ✓ 脅威が内在する時間を短くすることで潜在被害を最小限にする
- ✓ サードパーティ機器と連携
 - インシデント検知
→ 「防御」へ指示して、攻撃を回避
 - インシデント抑制
→ 「対処」へ指示して、調査またはフォレンジックを促す

Gartner

単一画面から、キルチェーンのステージを可視化



ユースケース①（脅威の検知・キルチェーンの確認）

The screenshot displays the Juniper ATP interface. At the top, the navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The main area shows a table of incidents with columns for Status, Incident ID, Risk, Threat, Progression, Collector Type, Threat Source, Threat Target, Zone, Target OS, Collector, and Date & Time. A red box highlights the 'Risk' column for the incident 'TROJAN_Pincav.CY', which is marked as 'HIGH'. Another red box highlights the 'Progression' column, which is marked as 'DL-IN'. A callout box on the left explains that the network environment has a high risk of malware threats. A callout box on the right explains that the kill chain indicators show a flag for malware infection status, indicating a high possibility of endpoint infection. Below the table, the 'Details for TROJAN_Pincav.CY' panel is visible, showing a 'Progression' diagram with stages: DELIVERY (Phishing: 0, Exploits: 0), EXPLOITATION & INSTALLATION (Downloads: 1, Executions: 0), COMMAND & CONTROL (Infections: 1, Custom Rules: 0), and ACTION ON TARGETS (Lateral Spread: 0). The 'Network' tab is selected in the bottom panel.

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	5251	HIGH	TROJAN_Pincav.CY	DL-IN	Web LOG	newsofts29.microka.com	RITA-PC	Default Zone	Windows 7	2 Collectors	May 3 20:09:50 GMT-0900

Details for TROJAN_Pincav.CY

Progression:

- DELIVERY: Phishing (0), Exploits (0)
- EXPLOITATION & INSTALLATION: Downloads (1), Executions (0)
- COMMAND & CONTROL: Infections (1), Custom Rules (0)
- ACTION ON TARGETS: Lateral Spread (0)

ネットワーク環境においてこのマルウェア脅威はリスクがHigh（高い）とJATPが判断していることが分かります。

下記のキルチェーンの指標ではマルウェア感染ステータスにフラグが立っているため、端末が感染している可能性が分かります。

ユースケース②（タイムライン－時系列の確認）

The screenshot displays the 'Events Timeline' for host 'RITA-PC'. The timeline shows three key events:

- Download:** Occurs on May 6, 2020, at approximately 10:06 AM.
- Infection:** Occurs on May 6, 2020, at approximately 10:08 AM.
- Attempted admin Allowed:** Occurs on May 6, 2020, at approximately 10:10 AM.

Below the timeline, the details for the event 'TROJAN_Pincav.CY' are shown:

Field	Value	Field	Value
Zone:	Default Zone	Risk:	High
Incident ID:	5251	Threat Category:	Trojan_Generic
Hostname:	RITA-PC	Asset Value:	Low
Username:	rita	Target OS:	Windows 7
IP Address:	10.1.3.103	Relevance:	Max
FQDN:	rita.eng.cyphort.com	Progression:	Download - Infection
Source Email ID:	-	Protocol:	HTTP,LOG
Destination Email ID:	-	OS Matched:	No

マルウェアをダウンロードしていることが分かります。

端末が感染していることが分かります。

Cisco FWのログにより、端末が**管理者権限でアクセス**を試みていることが分かります。

ユースケース③（タイムライン（時系列）全体の確認）

“Zoom Out” “Show All” をクリックすることにより、過去のログを含めて確認することが可能です。

過去にも**何度もマルウェア**をダウンロードしていることが分かります。

端末が**管理者権限でアクセス**を試みる行動が、過去においても**複数回**行われていることが分かりますので、明らかに異常な行動であることが分かります。

ユースケース④ (Infection - C2サーバとの通信状況の確認)

InfectionのタブをクリックするとC2サーバへの通信状況が確認できます。



Infection Summary:
Name: TROJAN_Pincav.CY
Severity: High
Category: Trojan_Generic
Derived MD5: 1e5499640ca31e4b1f113b97a0cae08b Find on VirusTotal
Collector: demo next x collector

C2 Serverのドメインが確認できます。

実際に発生している通信の確認できます。

Network Information:

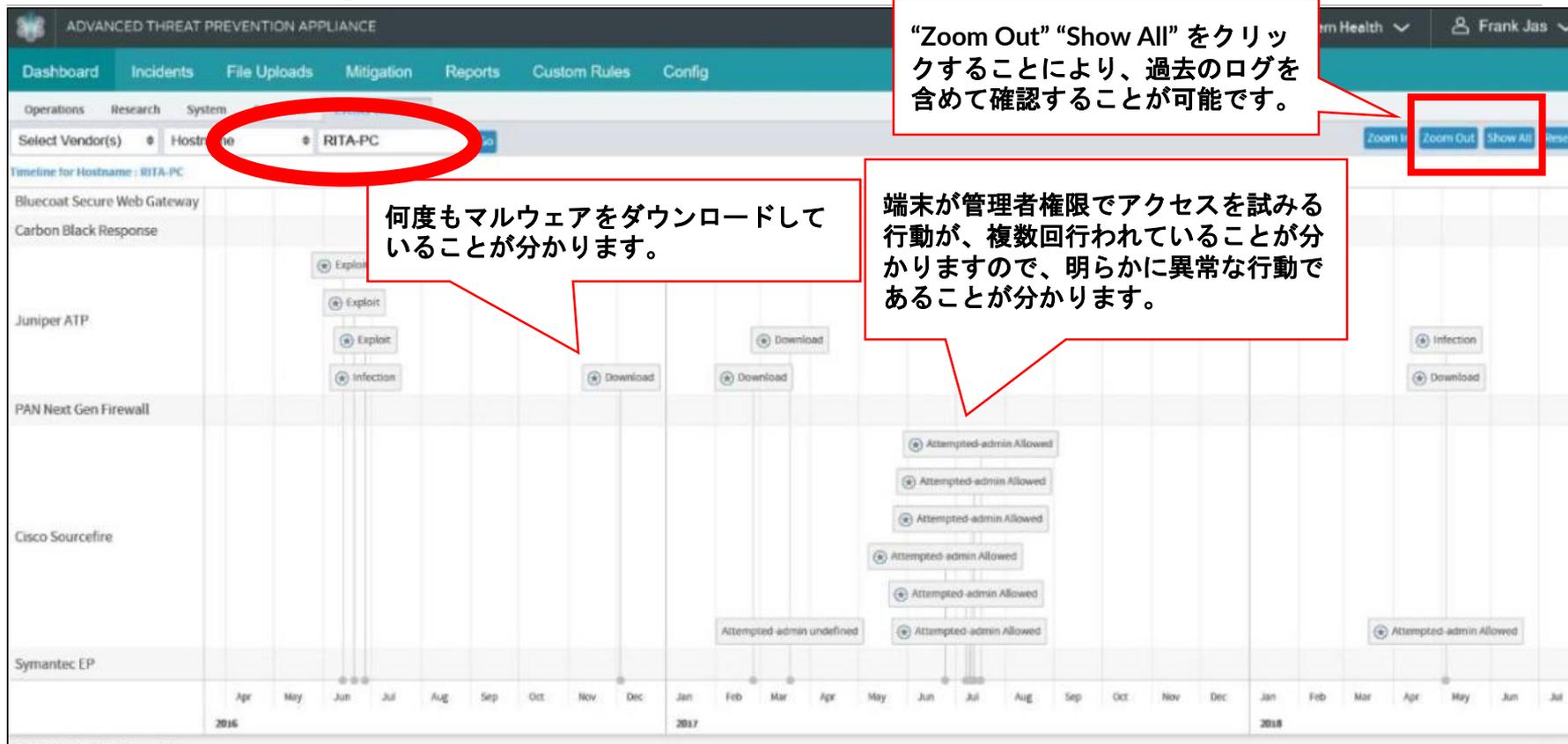
Date	Rule Id	Summary	C2 Server	Details	Actions
Mar 11 21:08:33 GMT+0900	8926319	CY AUTO TROJAN Generic ccaed7c3c6e58a2844c9896246997f62 HTTP Callback 8926319	newwolfs21.mezoka.com	POST /mits/login.php HTTP/1.1. User-Agent: Asynchronous WinHTTP/1.0. Host: newwolfs21.mezoka.com. Content-Length: 44. Connection: Keep- Alive...CyoKCy0149093D15B2C0A1855DD98685- F51362DCyoK	<input checked="" type="checkbox"/> Add to Whitelist <input checked="" type="checkbox"/> Report False Positive <input checked="" type="checkbox"/> Download Signature
Mar 11 21:08:33 GMT+0900	2015753	CY1 TROJAN Pincav.cjvb Checkin	newwolfs21.mezoka.com	POST /mits/login.php HTTP/1.1. User-Agent: Asynchronous WinHTTP/1.0. Host: newwolfs21.mezoka.com. Content-Length: 44. Connection: Keep- Alive...CyoKCy0149093D15B2C0A1855DD98685- F51362DCyoK	<input checked="" type="checkbox"/> Add to Whitelist <input checked="" type="checkbox"/> Report False Positive <input checked="" type="checkbox"/> Download Signature
Mar 11 21:08:33 GMT+0900	8926319	CY AUTO TROJAN Generic ccaed7c3c6e58a2844c9896246997f62 HTTP Callback 8926319	newwolfs29.mezoka.com	POST /docs/login.php HTTP/1.1. User-Agent: Asynchronous WinHTTP/1.0. Host: newwolfs29.mezoka.com. Content-Length: 44. Connection: Keep- Alive...CyoKCy0149093D15B2C0A1855DD98685- F51362DCyoK	<input checked="" type="checkbox"/> Add to Whitelist <input checked="" type="checkbox"/> Report False Positive <input checked="" type="checkbox"/> Download Signature

脅威の特定と対応時間を大幅に短縮

インシデント対応に掛かるプロセス	手動による対応	JATPの自動対応
ホスト、ユーザの特定	0.5 時間	自動
アンチウィルス、EDRのデータを収集	1 時間	自動
NGFW等からのネットワークデータ収集	1 時間	自動
相関分析	1 時間	自動
感染の進行と範囲を特定	0.5 時間	自動
一次対応を開始	0.5 時間	自動
合計時間	4.5 時間	10分以内

対応時間の軽減

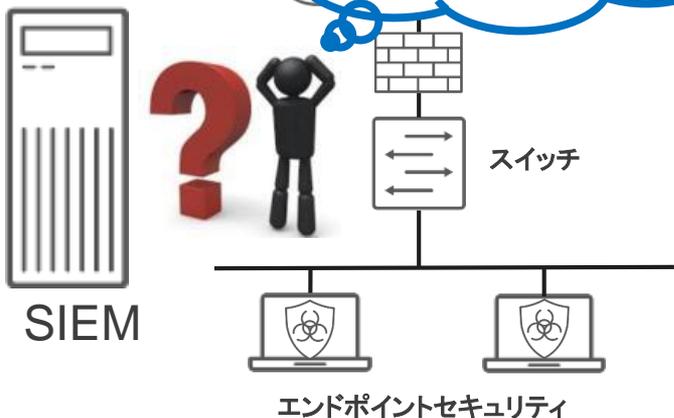
ユースケース⑤（個人の感染状況を確認）



ユースケース⑥ (SIEMの代わりにキルチェーンを可視化)

現在の
お客様環境例

SIEMを購入したけど、
脅威が残っているのか
追跡が難しい。。



お客様のご環境とニーズ

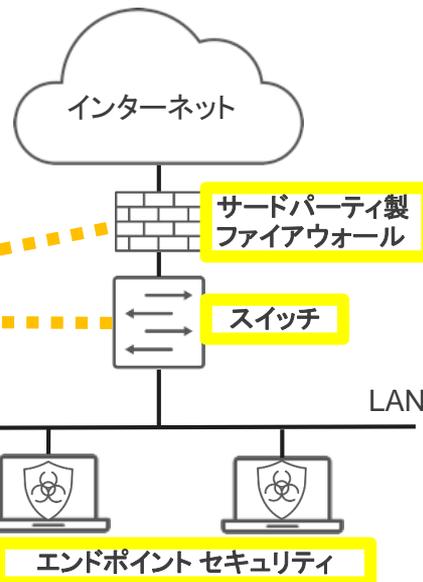
SIEMを購入したが使いこなすことが難しく、最終的に脅威が残っているのかキルチェーンのステータスが可視化できていないので、簡単に可視化できるソリューションが欲しい。

ご提案構成例

ネットワークとエンドポイントからシスログを受信し端末毎のインシデントとして自動的に紐づけ

SmartCore

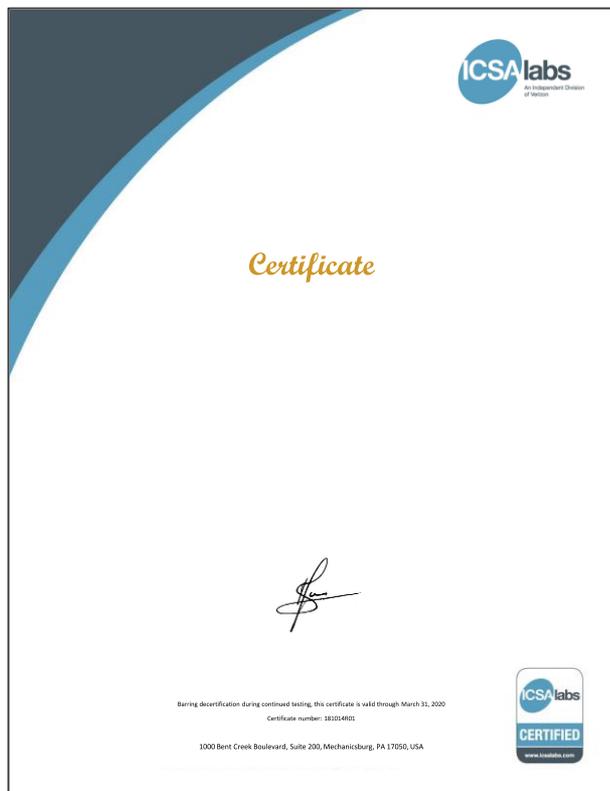
SIEM



ご提案構成によるメリット

SIEMでシスログを集めてフィルターをかけた後に、SIEMからJATPへシスログを飛ばして頂くことで、簡単にキルチェーンのステータスが可視化できます。

ICSA の最も厳しいテストにて高い検知率が証明済み



Test Length	28 days	Malicious Samples	504	Innocuous Apps	555
Test Runs	1059	% Detected	99.2%	% False Positives	1.1%

Fig. 1 – High Detection Effectiveness & Few False Positives

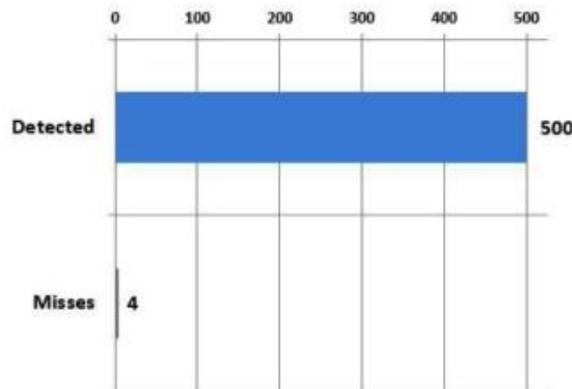
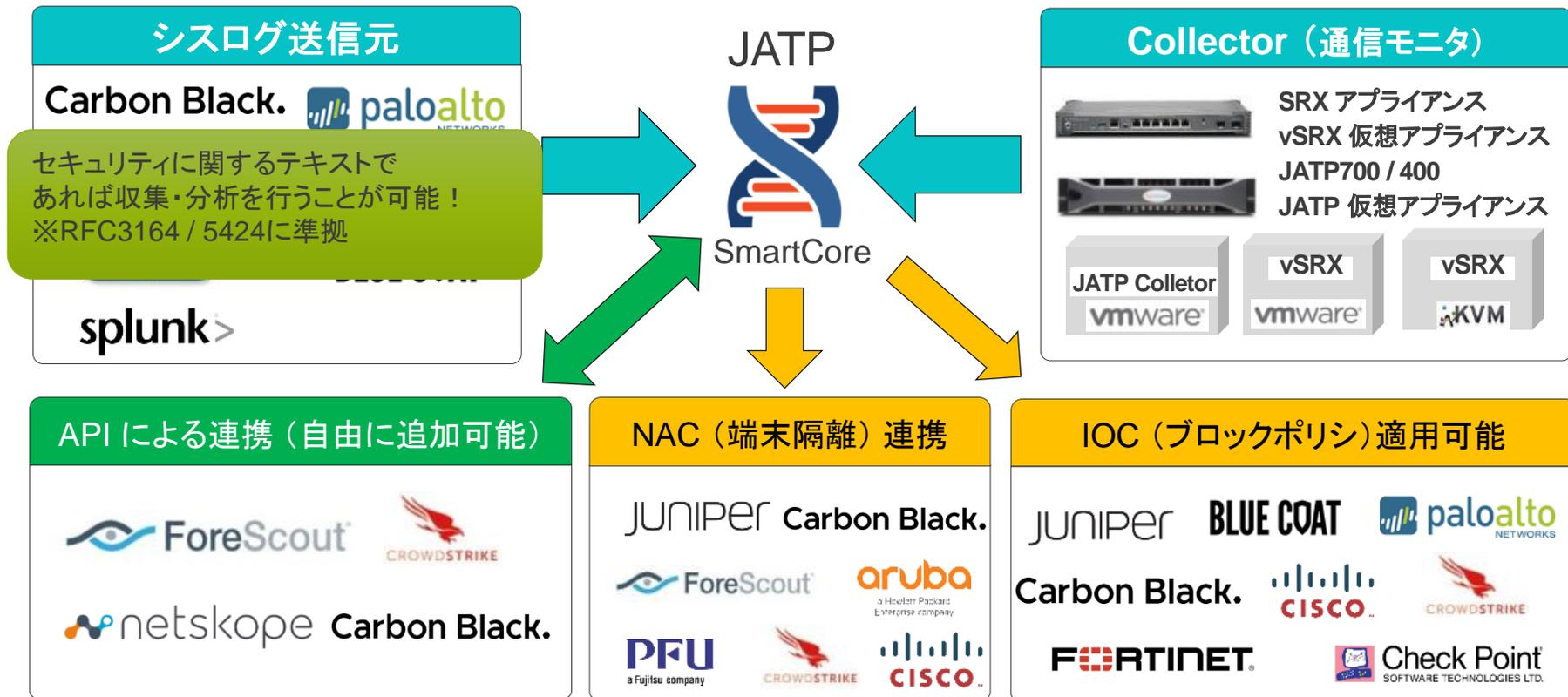


Fig. 2 – Detected 500 of 504 New & Little-Known Malicious Samples



Fig. 3 – 6 Alerts on Innocuous Applications

JATPによる統合セキュリティ連携例





まとめ

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



多層防御、マルチベンダ環境における
セキュリティ管理負荷と対応時間の長さ



ジュニパーの提案

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のログ分析、および
脅威を可視化することにより、
短時間で脅威の特定と対応が可能

Juniperのセキュリティで、最先端の安全 & コストの抑制！！

ジュニパー コネクテッドセキュリティ

セキュリティ脅威から、ユーザ、アプリケーション、およびインフラストラクチャを守る

脅威の可視化



タスクの自動化



検知および防御



ネットワーク全体にセキュリティを拡張！！