サンドボックスとSIEM機能を搭載した次世代ソリューション

“未知の脅威検知と自動隔離“

2018年2月

ジュニパーネットワークス株式会社

セキュリティの共通課題

共通課題

- **ネットワーク全体を監視対象**にすることが難しい。
- 優先的に対応しなければならない**脅威の特定と判断に時間が掛かる**。
- 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。**
- セキュリティ機器、サンドボックス、SIEMを揃えると**費用が莫大になる。**

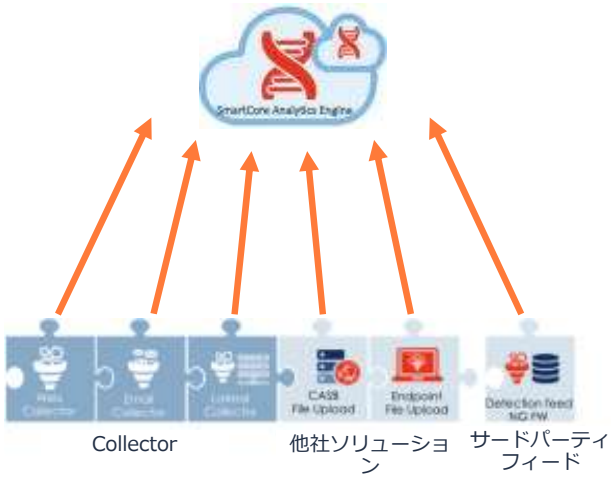
Juniper Advanced Threat Prevention (JATP)

- JATPの独自センサーとサードパーティ製品のログ分析によりネットワーク全体の監視が可能です。
- JATPのサンドボックス、機械学習、レピュテーションにより脅威のレベルの判断が可能です。
- サードパーティ製品へ自動的にポリシ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です。
- JATPとSRXを組み合せることにより大幅な費用削減が可能です。

JATP は“サンドボックス、機械学習、SIEM の機能”を搭載した次世代セキュリティ ソリューションです。

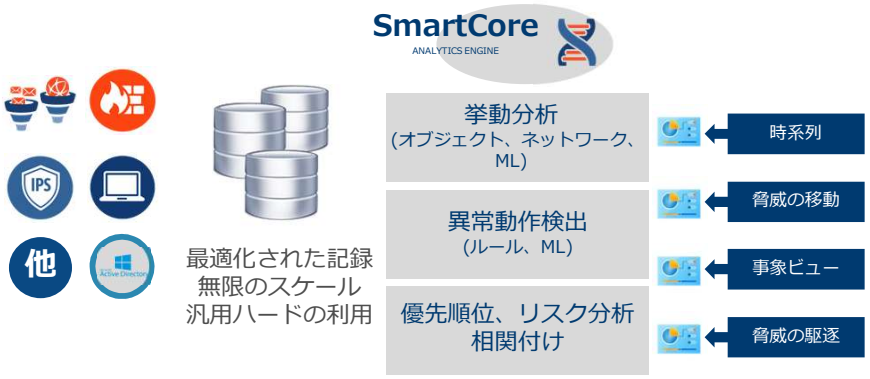
未知の脅威検知

他社を含む複数のデータソースをサポート



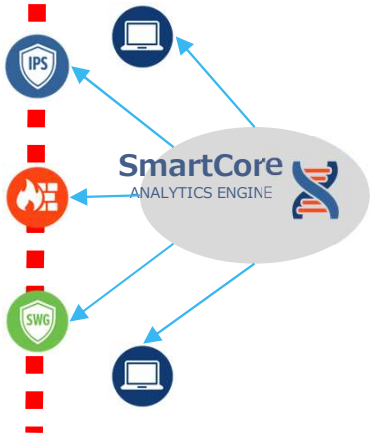
先進的な分析

データ取込 → 蓄積 → 分析 → 可視化



迅速な対応

ポリシ適用・感染確認



JATP の**ハニーポット(Agent)とサードパーティ製品の両方から**ネットワーク全体の情報を収集

ふるまい検知サンドボックス、機械学習機能、レピュテーションによる高度分析により、リスクレベルと優先順位を判断

分析結果を元に**自動的に**感染範囲の特定、**感染端末の隔離**

JATP の自動分析により優先的に対応しなければならない脅威の特定と対応を自動的に実施可能です。

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

連携実績のあるベンダー

Endpoint

Carbon Black.
CROWDSTRIKE
McAfee
Symantec.
CYLANCE
TANIUM

Firewall/SWG

Check Point SOFTWARE TECHNOLOGIES LTD.
BLUE COAT
Infoblox
cisco
FORTINET
JUNIPER NETWORKS
SONICWALL
paloalto NETWORKS

SIEM

splunk>
JUNIPER
IBM QRadar
ArcSight An HP Company

CASB

netskope

NAC/Identity

BRADFORD NETWORKS the smart edge
Pulse Secure
aruba a Hewlett Packard Enterprise company
PFU a Fujitsu company

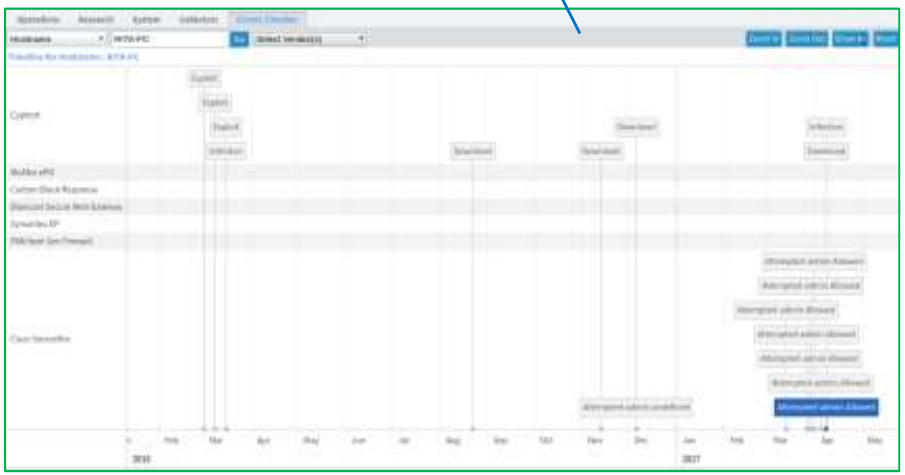
Other

Gigamon
riverbed
DB NETWORKS
exabeam
Phantom
CYBERSPONSE ADAPTIVE SECURITY

GUI 画面（一部）

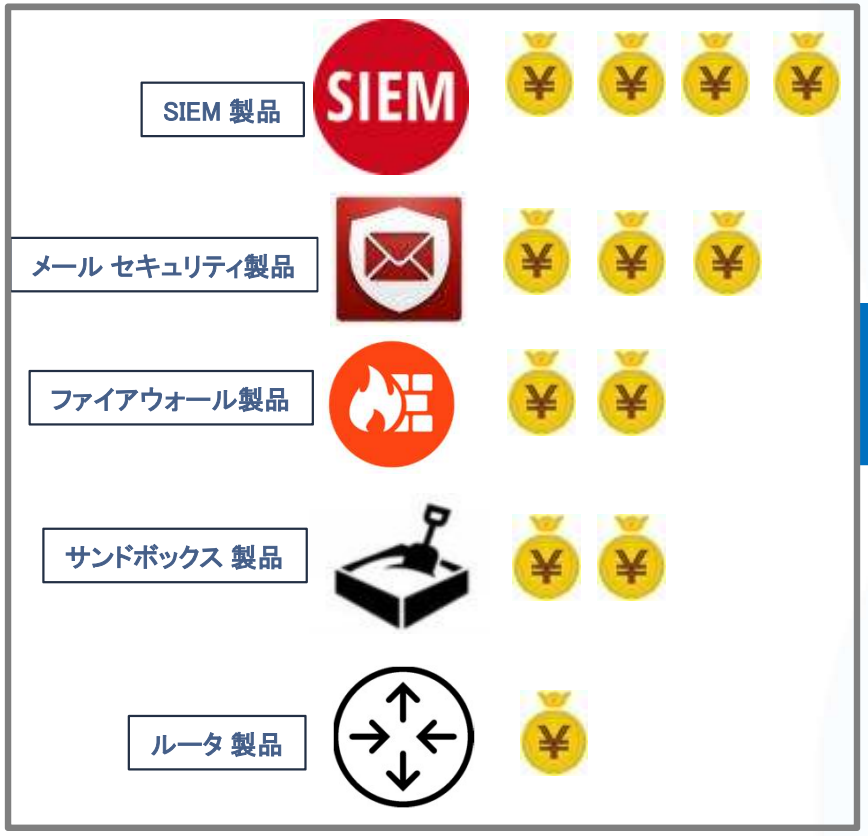
ダッシュボード上でネットワーク全体のリスク状態を把握できます。

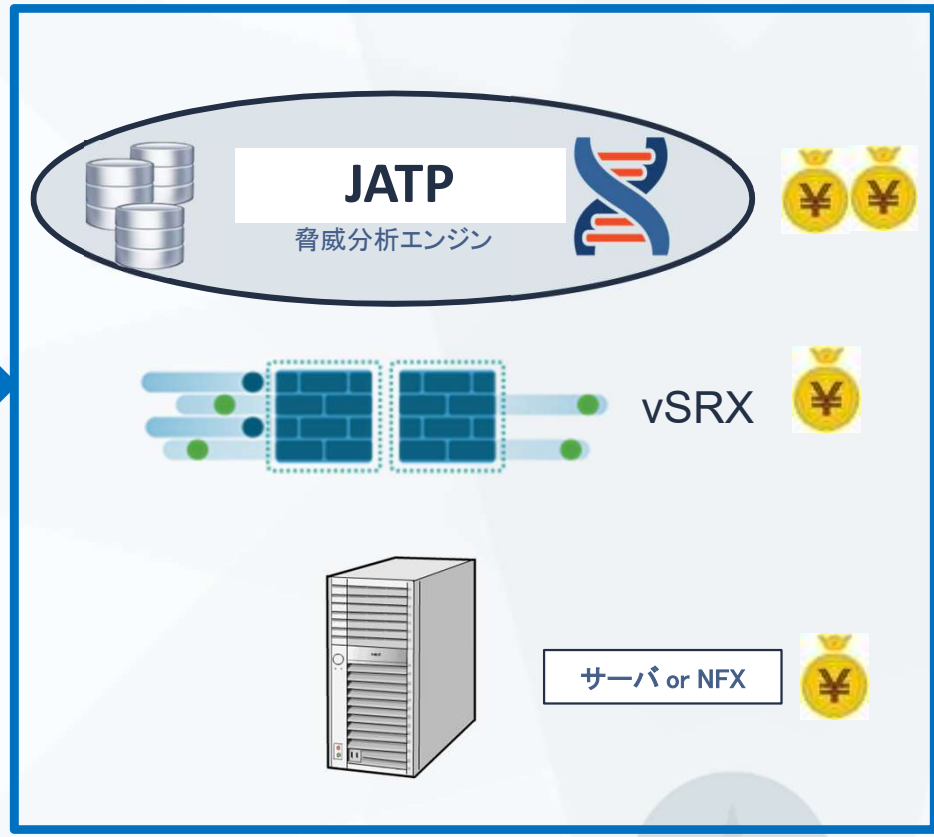
ネットワーク内のどのセキュリティ機器がいつ許可、検知しているのか分かります。



脅威に対するキルチェーンのステータスが確認できます。

JATP とvSRXの組み合わせで約70%のコストダウンが可能です。





Juniper Advanced Threat Prevention (JATP)

ご評価につきましては、弊社担当営業まで
ご連絡をお願い致します。

www.cyphort.com

Advanced Threat Detection
Advanced Threat Analytics
One-touch Threat Mitigation