
クラウド時代のゼロトラストセキュリティ
Juniper Networks .K.K
JUNIPER NETWORKS
Engineering Simplicity

Legal Disclaimer

This statement of direction sets forth Juniper Networks' current intention and is subject to change at any time without notice.

No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

Agenda

1．ゼロトラスト セキュリティとは？

2．Juniper の考えるゼロトラスト

　セキュリティとは？

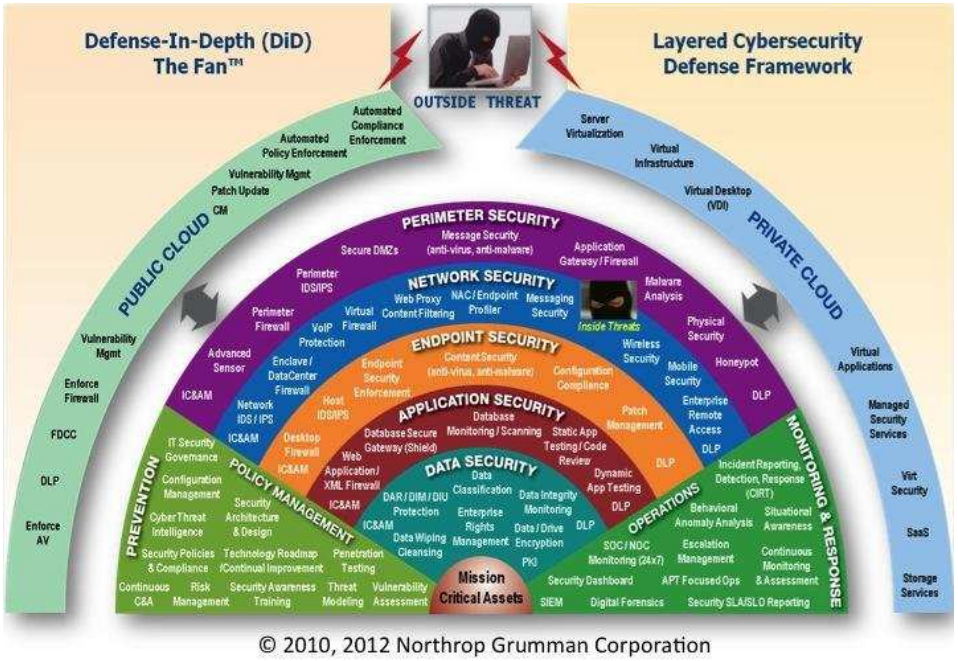
3．Juniper のConnected Securityとは？

4．よくある課題

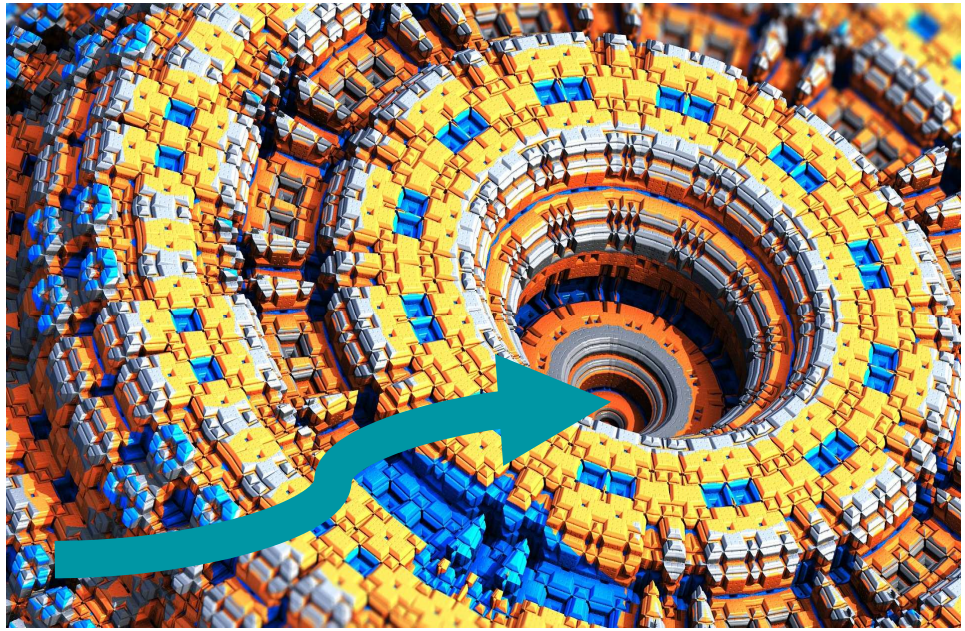
5．まとめ

現在のセキュリティの課題

多層防御によるセキュリティ



複雑になるセキュリティ



ゼロトラスト セキュリティは製品ではありません。

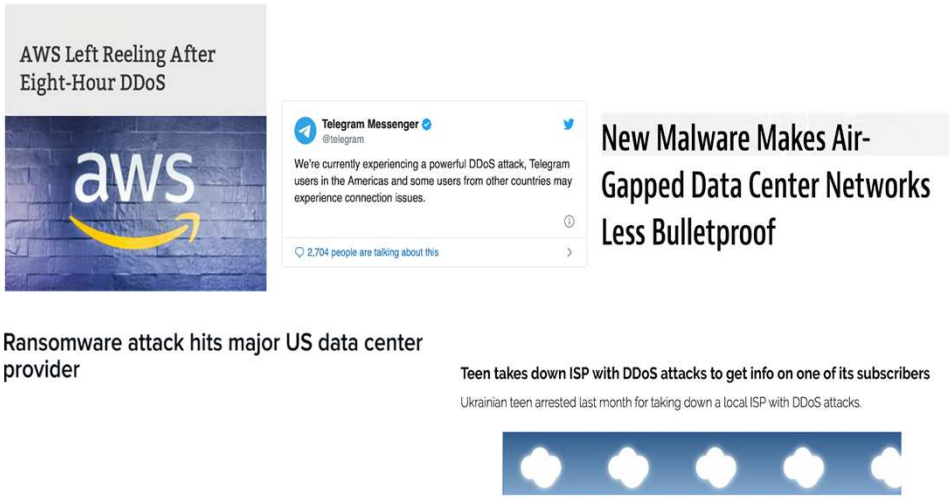
トラストモデル

ゼロトラストモデル

なぜ、ゼロトラスト セキュリティが必要？

デジタルトランスフォーメーション

未知の脅威の増加



データを守るということは？

管理されている？

管理されていない？

ゼロトラスト セキュリティはゼロから作る必要がある？

ゼロトラスト セキュリティのゴール

- 全ての環境における正確な可視化
- ネットワーク内の許可されていないアクセスを防ぐ。
- 未知の脅威のリアルタイム検知と自動化を含むリアルタイム対応

2．Juniper の考えるゼロトラストセキュリティとは？

ポイント① ネットワークとセキュリティの融合

ポイント② 機械学習エンジンを活用した未知の脅威検知

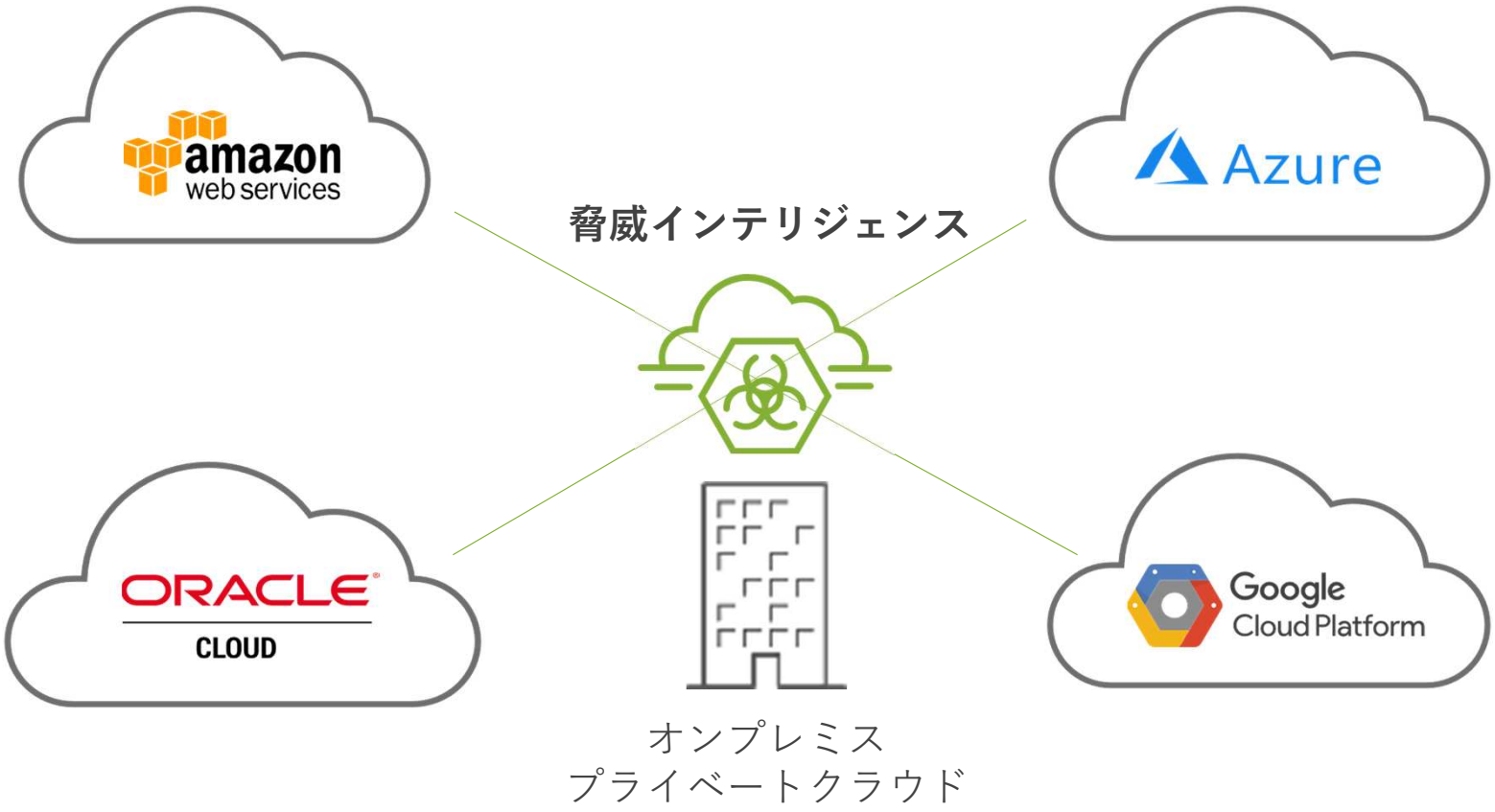
悪意のあるサイトとの
通信時の振る舞い情報

クリーンなサイトとの
通信時の振る舞い情報

サイトのReputation 情報

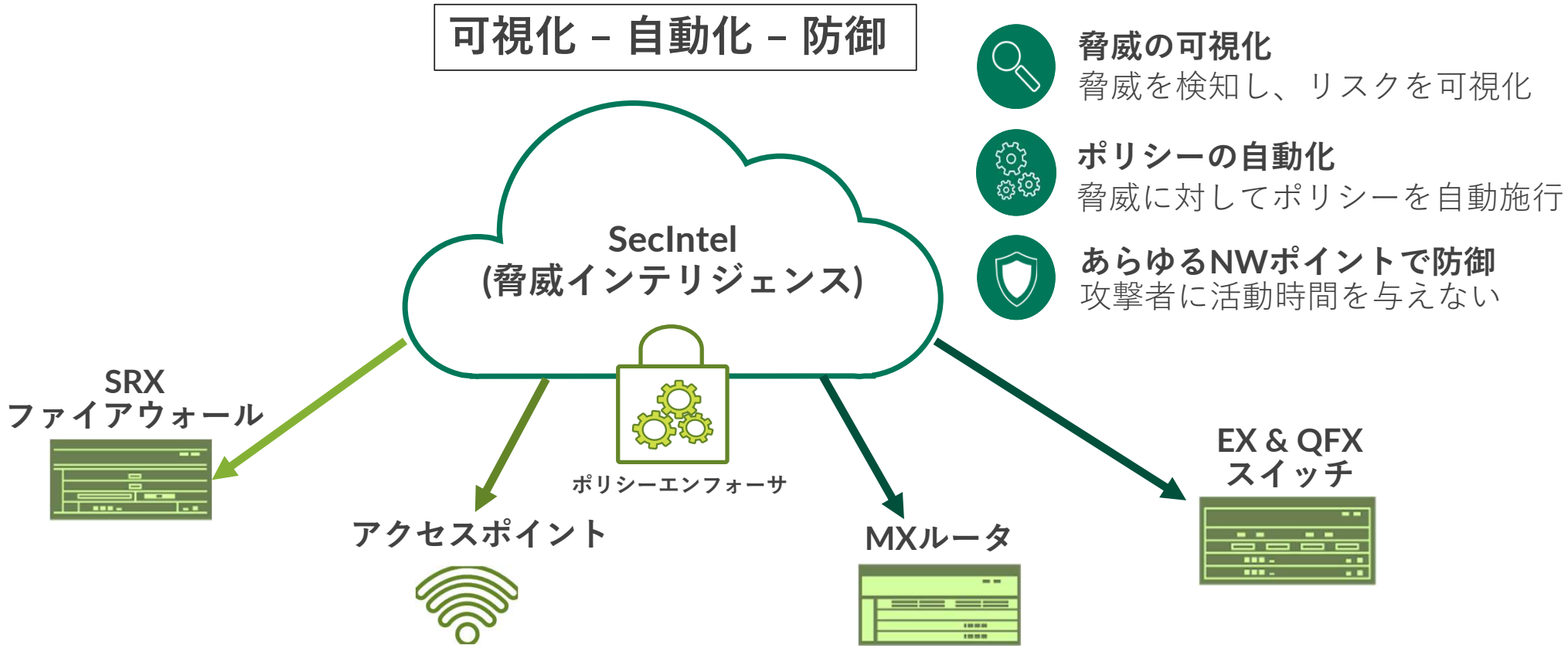
機械学習エンジン

ポイント③ オンプレミス、クラウドの統合セキュリティ



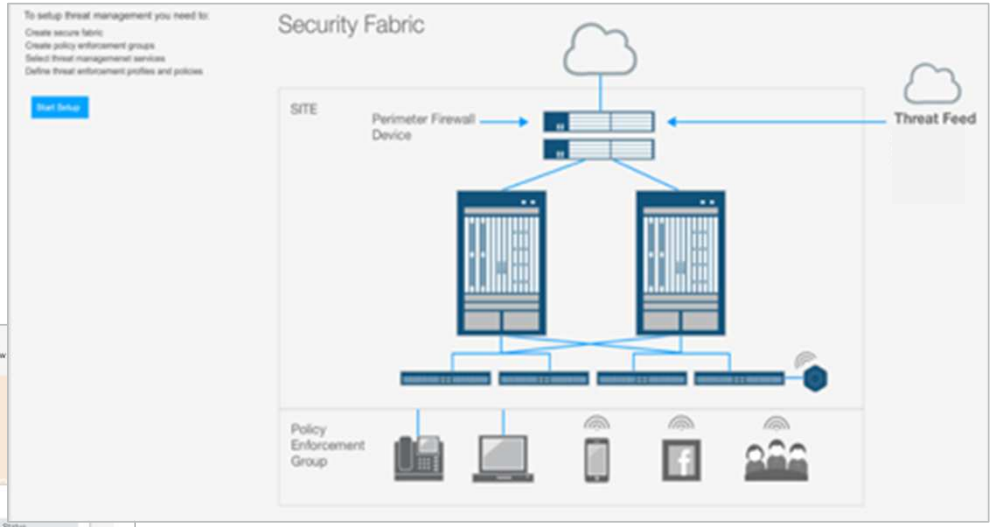
3．Juniper のConnected Security とは？

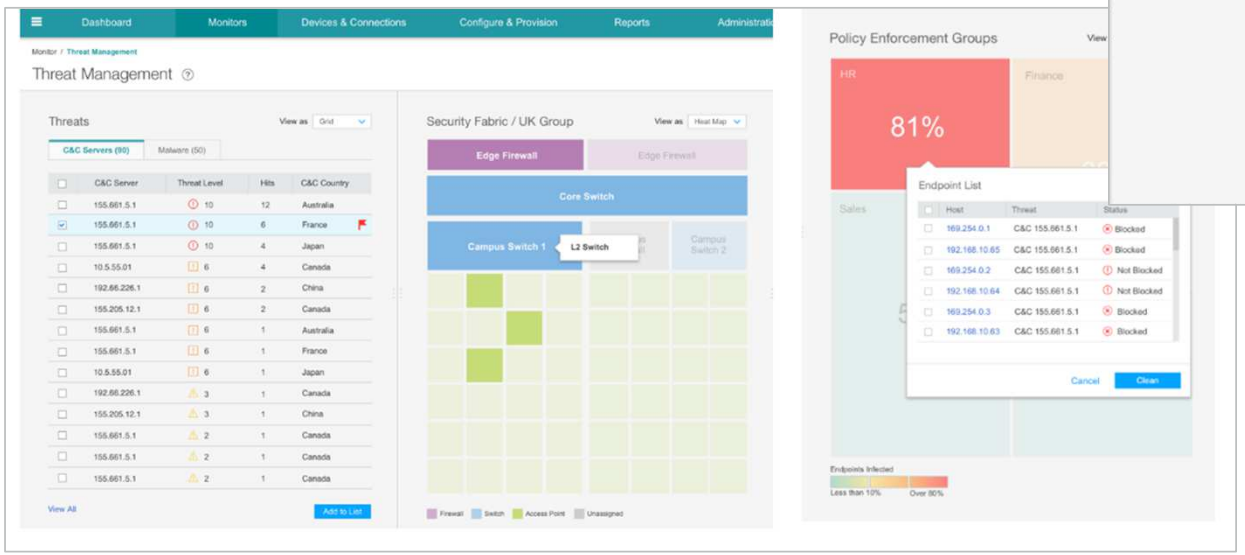
SecIntel（脅威インテリジェンス）とネットワーク機器との連携



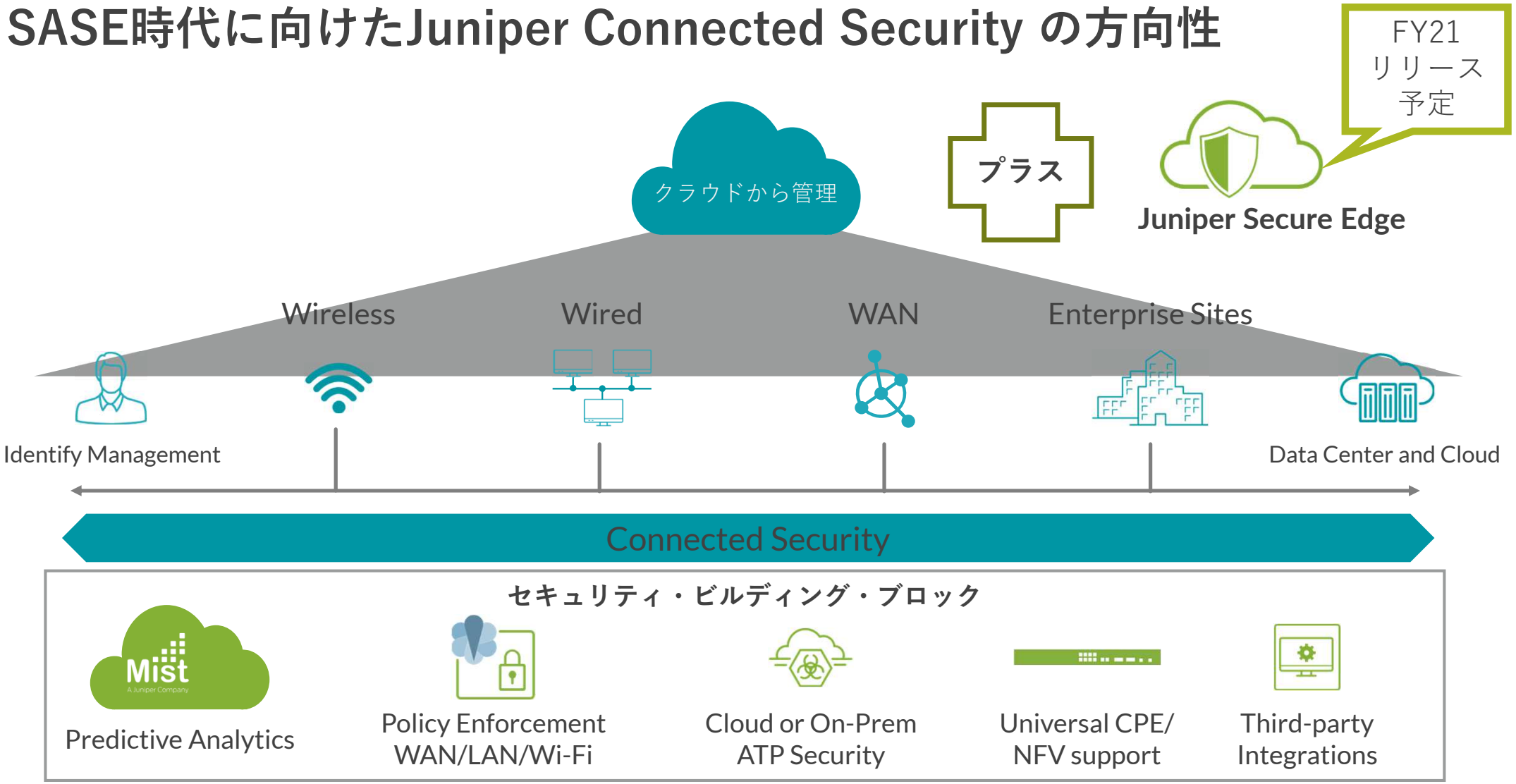
感染端末/コンプライアンス違反端末への自動対応

- 脅威への対応を自動化
- 隔離、追跡、ブロック、リリースなど柔軟な運用
- ポリシーの統合管理





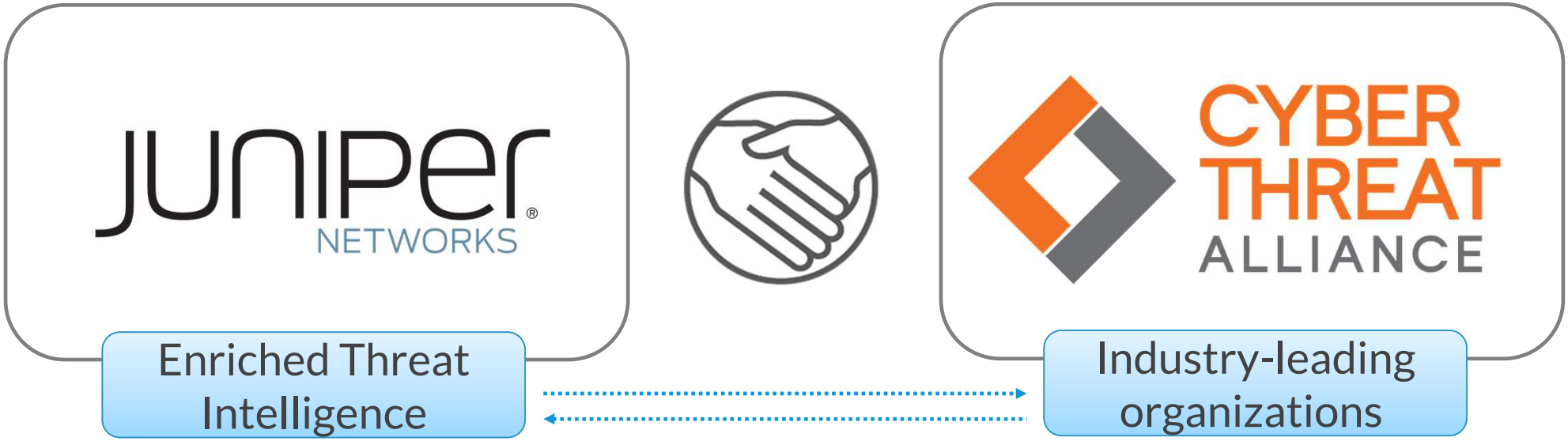
SASE時代に向けたJuniper Connected Security の方向性



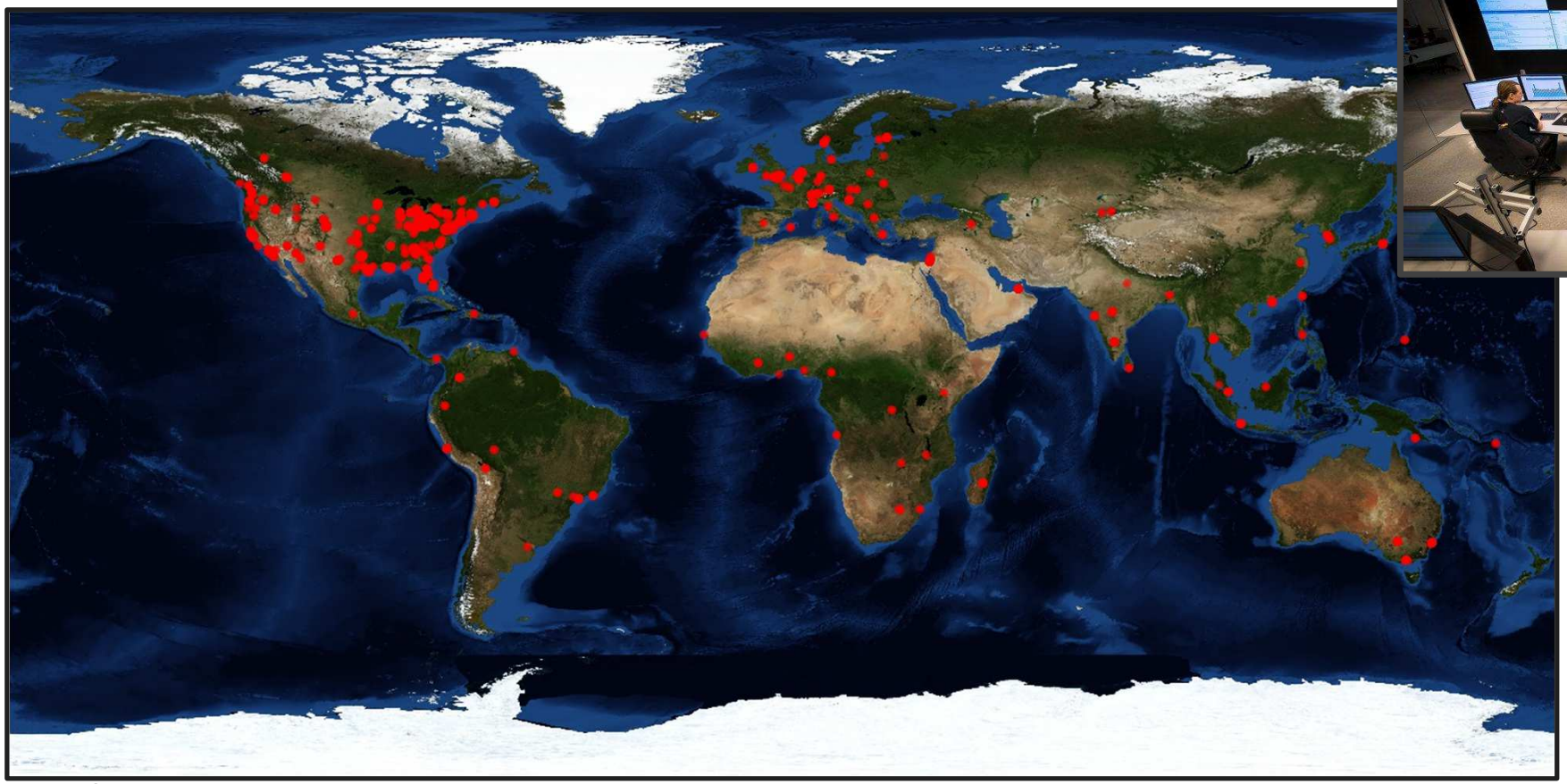
CTA (Cyber Threat Alliance) のメンバーとして活動

競合他社からもトップセキュリティベンダーとしての認知

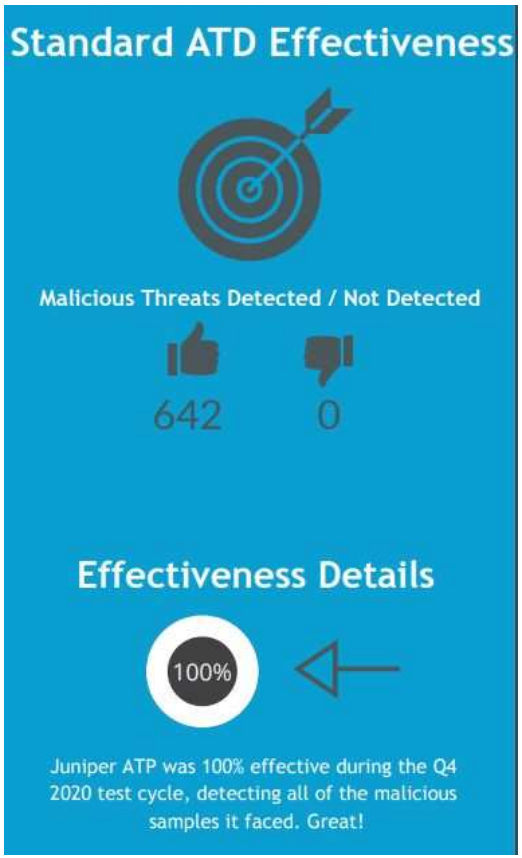
直ちに実行可能な脅威情報をアライアンスメンバーと共有することで、
サイバーセキュリティ対策を強化



HoneyPots に加えてCloud ATPの検知もリアルタイムに分析



最新のICSA の検知テストで100％検知, 0％誤検知を達成。（2020年Q4）



4. よくある課題

① 暗号化通信へのセキュリティ対策について

② コンプライアンス違反の通信対策について

③ サードパーティ製の機器との連携

④ セキュリティログの管理問題

① 暗号化通信へのセキュリティ対策について

暗号化通信へのセキュリティについてよくある会話

(疑問)
最近ファイアーウォールが検知している数が減っている気がするな。これって悪意のある通信が減っているからなのかな？

具体的にどの位増えているの？

暗号化通信かどうか、ってどこで分かるの？

確認したら普段使っているGoogleなどのサイトも暗号化通信なんだね。

それって暗号化通信が増えているからじゃない？

インターネット通信の約80%が暗号化されているって言われているよ。

例えばWeb通信だったら、HTTPS:// の文字列から始まっていたら暗号化通信だよ。

気づかないうちに自動的に暗号化通信になっているよ。

暗号化通信へのセキュリティについてよくある会話

暗号化通信だから悪意のある通信を検知できず、ファイアウォールの検知ログが減っていたんだね。

暗号化通信に対してセキュリティ対策ってどうすればいいのかな？

導入するのに課題ってある？

その可能性はあるね。

暗号化通信に対するセキュリティ対策はいくつかあるよ。

1．PCなどの端末側にセキュリティソフトを入れる。
2．暗号化通信を復号化する。

実は、導入するために検討しなければならないことがいつくかあるよ。個人端末など管理対象外の端末にセキュリティソフトや暗号通信復号化用の証明書を入れることが難しい可能性が高いよ。

暗号通信の復号化の構成例

端末側に証明書を入れる必要がある。

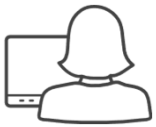
暗号化通信へセキュリティ対策の課題

問題：
インターネット通信の約80％以上が暗号化通信(HTTPs) になっている。

課題：
1．管理対象外の端末(私物端末、海外からのゲスト）が多く、エンドポイントセキュリティのソフトや、復号化するための証明書配布が難しい。
2．仮に配布できたとしてもソフトウェアのコスト、運用コストが高い。
3．IoT機器(プリンターなど) にはソフトや証明書をそもそも入れることができない。
4．アプリケーションによっては復号化すると動作しなくなるものもある。

求められるソリューション：
1．ソフトウェアの適用、証明書配布などが難しい端末へも暗号化通信のセキュリティ対策ができる。
2．管理対象の端末には証明書を配布して復号化によるセキュリティを同時にかけたい。
3．悪意のあるサイトへの通信を検知した際には、スイッチやWifi APなどで該当端末を隔離したい。
4．現在のネットワークの変更がいらない。
5．安価に実行できる。

ジュニパーで実現する暗号化通信へセキュリティ対策 (Encrypted Traffic Insights)



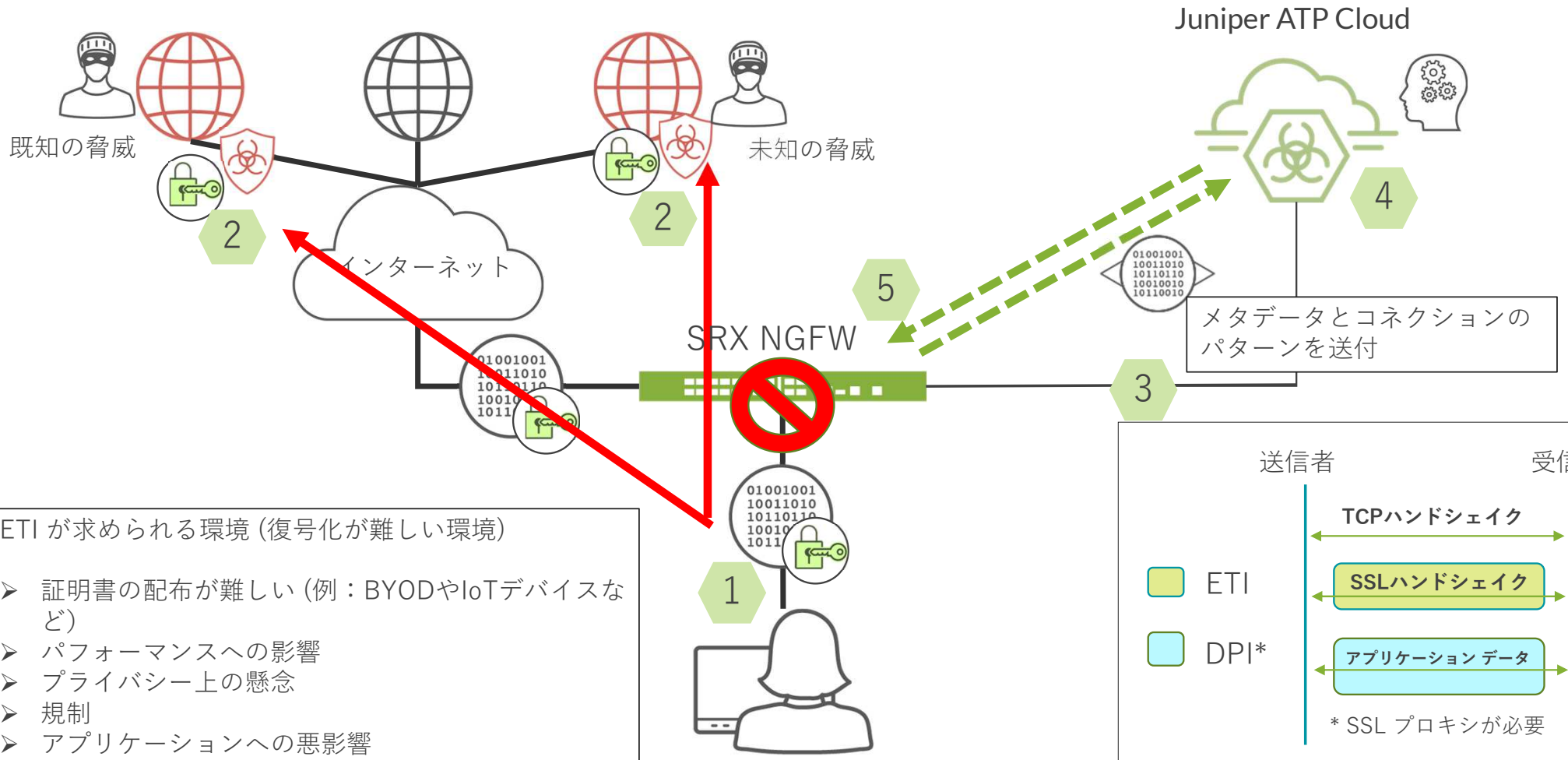
ジュニパーが何かソリューション持っているみたいだよ。

そうなんだ。必要な機器って何？

「必要な機器」

1. SRX (物理アプライアンス)、 もしくは、vSRX（仮想アプライアンス） ＊スイッチなどからミラー通信を受信
2. SaaS型のATP Cloud ＊センサーが検知した情報を収集しブロックリストを配信する脅威インテリジェンス
3. Security Director/Policy Enforcer ＊ジュニパー製やサードパーティ製のスイッチ/Wifiで自動隔離するためのオーケストレーター

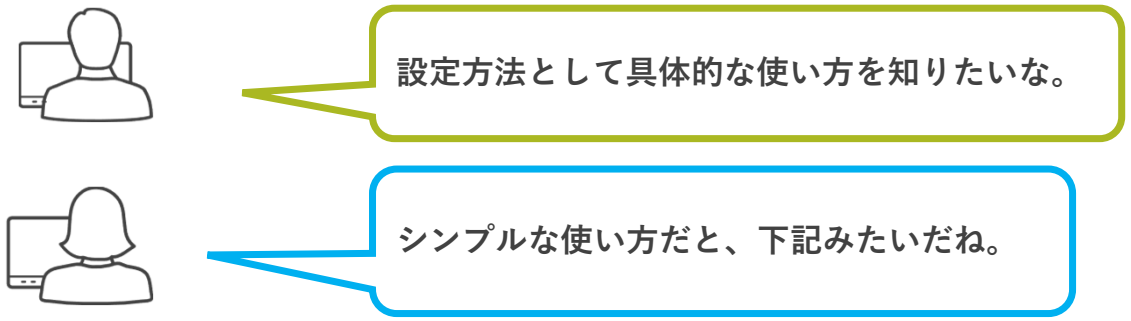
ジュニパーで実現する暗号化通信へセキュリティ対策 (Encrypted Traffic Insights)



ETI が求められる環境 (復号化が難しい環境)

- 証明書の配布が難しい (例：BYODやIoTデバイスなど)
- パフォーマンスへの影響
- プライバシー上の懸念
- 規制
- アプリケーションへの悪影響

ジュニパーで実現する暗号化通信へセキュリティ対策 (Encrypted Traffic Insights)



「シンプルなユースケース例」

1. 管理対象の端末には証明書を配布して、インラインで入っているファイアウォール (ジュニパー製SRXでも可能) で復号化によるセキュリティをかける。

2. 管理対象外の端末(私物端末、海外からのゲスト）、IoT機器(プリンターなど) は SRXの Encrypted Traffic Insightsでセキュリティをかける。

3. インラインに入っているSRX、ジュニパー製EX スイッチ、サードパーティ製のスイッチ/Wifi などで、悪意のあるサイトとの通信を行っている端末を自動的に隔離する。

② コンプライアンス違反の通信対策について

社内のコンプライアンス違反の通信についてよくある会話

(疑問)
最近社内からの不正アクセスが増えている気がするんだよね。

アクセスログを整理している中で気付く感じだからリアルタイムに対応できないんだよね。

セキュリティ機器はあくまで悪意のある通信を検知する製品だからうちのコンプライス違反の通信は検知しないんだよね。

アクセスリストだと設定した機器だけで止める形で、他の経路でアクセスされると止められないし、その端末も引き続きネットワーク上に存在しているから怖いんだよね。

本来アクセスするはずのない端末が社内サーバーにアクセスみたいな動作のこと？

確かに社内のルールやコンプライアンスって学校によって異なるから、世の中で言われる悪意のある通信とは種類が異なるよね。

でも、セキュリティ機器、ネットワーク機器でもアクセスリストの設定があるから、それを使えばいいんじゃない？

コンプライアンス違反した端末がネットワーク全体にアクセスできなくなる自動化ソリューションが理想ということだね。

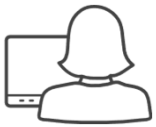
社内のコンプライアンス違反の通信の課題

問題：
社内からの不正アクセスが増えている

課題：
１．管理対象外の端末が多い。(私物端末、海外からのゲスト、倉庫に眠っていた古い端末）
２．故意の犯行の場合は、通常のセキュリティ機器の検知ロジックと異なる通信なのでリアルタイムで検知できない。

求められるソリューション：
１．故意の犯行の場合もリアルタイムに検知できる。
２．現在のネットワークの変更がいらない。
３．安価に実行できる。

ジュニパーで実現するコンプライアンス違反の通信への対策



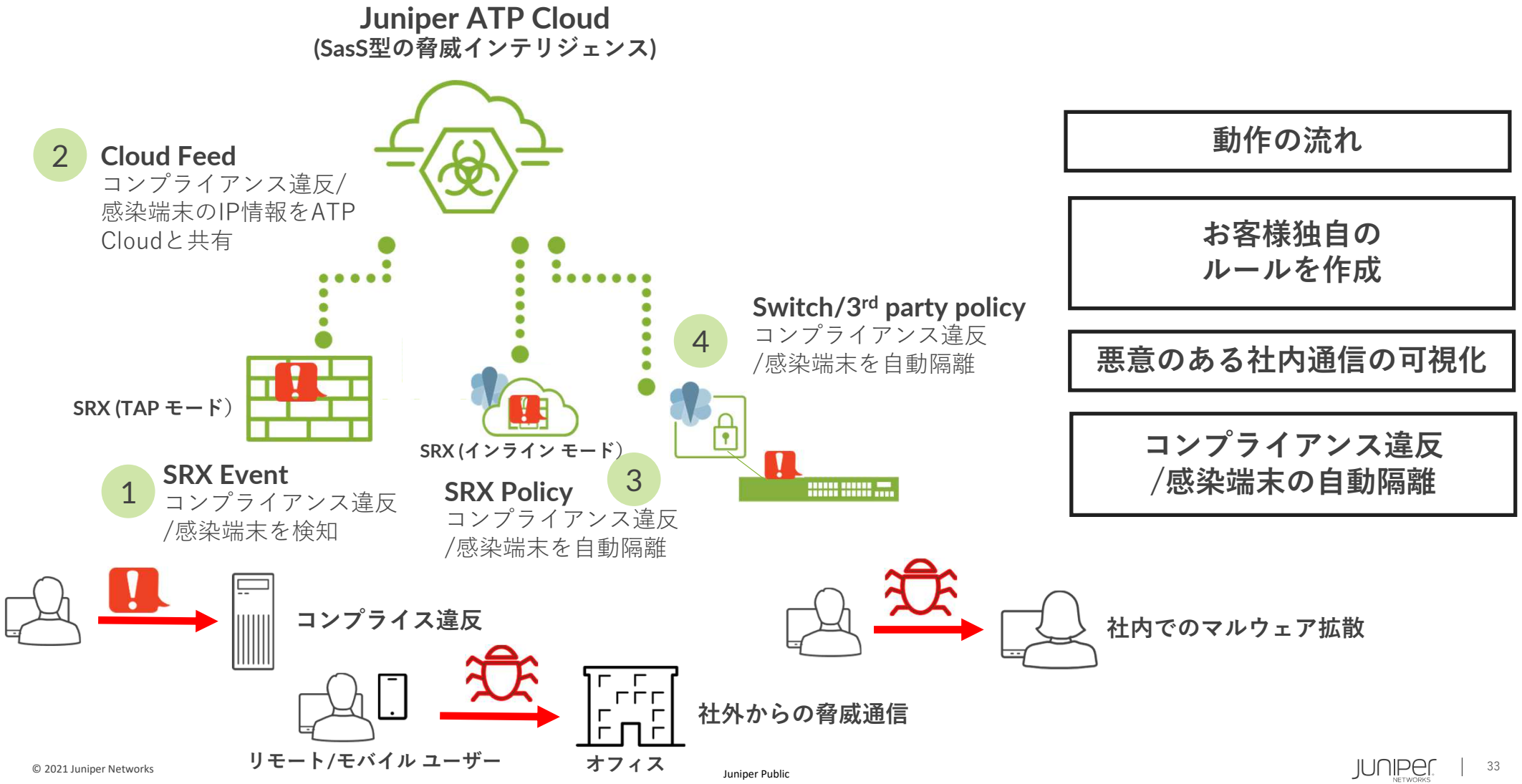
ジュニパーが何かソリューション持っているみたいだよ。

そうなんだ。必要な機器って何？

「必要な機器」

1. SRX (物理アプライアンス)、 もしくは、vSRX（仮想アプライアンス） ＊スイッチなどからミラー通信を受信
2. SaaS型のATP Cloud ＊センサーが検知した情報を収集しブロックリストを配信する脅威インテリジェンス
3. Security Director/Policy Enforcer ＊ジュニパー製やサードパーティ製のスイッチ/Wifi で自動隔離するためのオーケストレーター

ジュニパーで実現する社内のコンプライアンス違反の通信への対策



動作の流れ

お客様独自の
ルールを作成

悪意のある社内通信の可視化

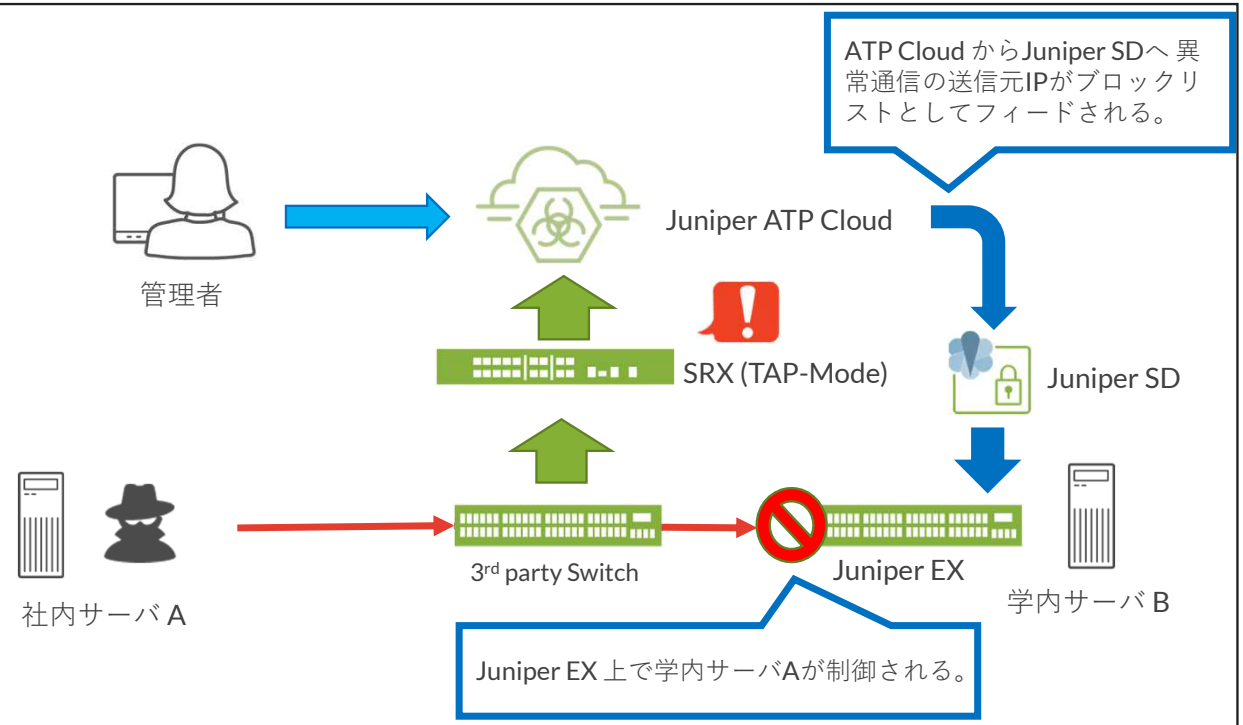
コンプライアンス違反
/感染端末の自動隔離

社内犯行やコンプライアンス違反の通信も検知し、自動制御できます。ユースケース①

[要件例]

1. 内部サーバ A とBとの間の通信において事前定義してある通信以外が流れた場合は異常通信として検知する。
2. 検知した場合は異常通信を発生している送信元IPアドレスをブロックリストとして自動配信。

[構成例]



[SRX上の設定例]

1. サーバ A とB 間の通信のみ正常
2. 通信は ポート番号 50000 のみ正常

[異常通信として検知するパターン例]

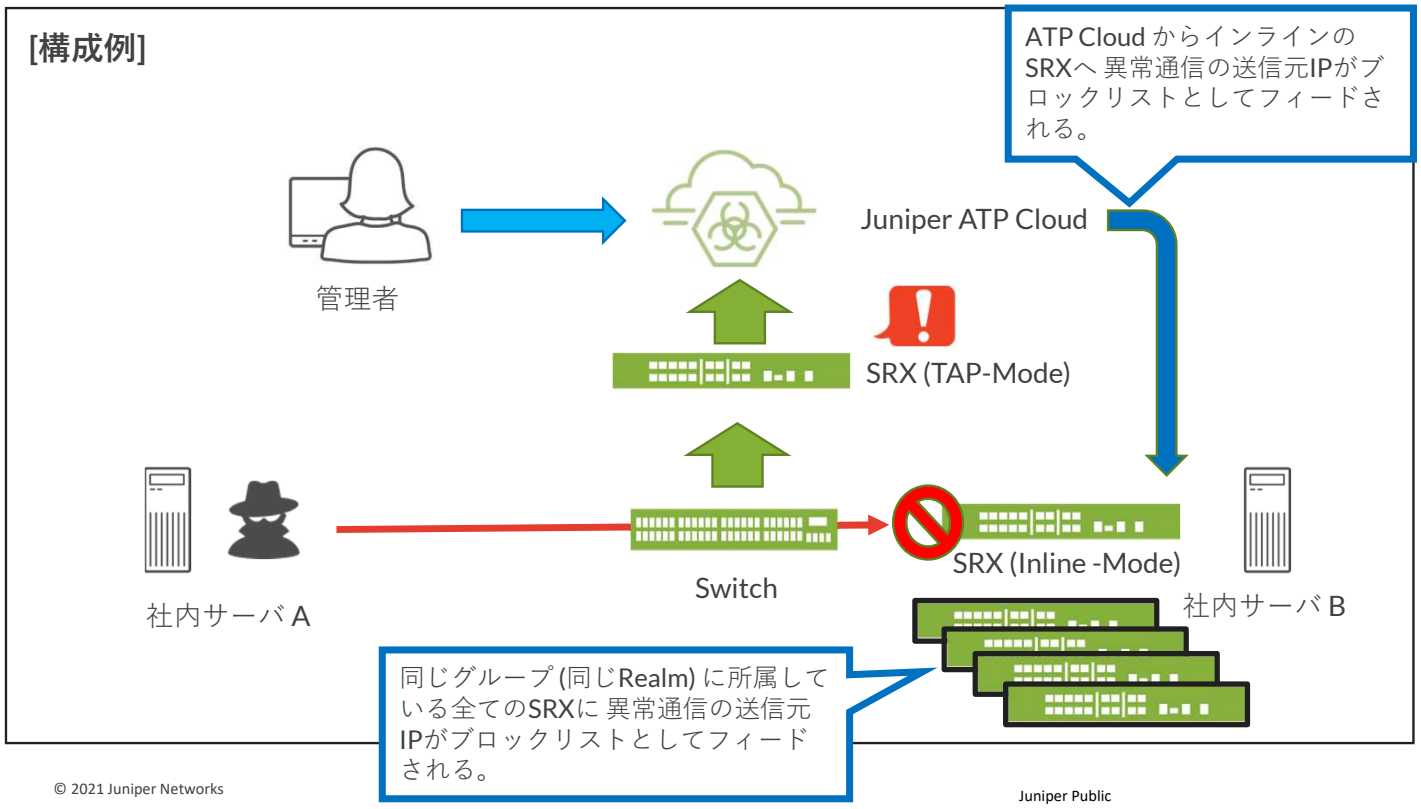
1. サーバA 以外のデバイスからサーバB への通信が発生
2. ポート番号 50000 以外の通信がサーバBへ送信 (サーバAが壊れて間違った通信を発生。または、マルウェア感染等によりPort Scanなどの悪意のある通信が発生)

社内犯行やコンプライアンス違反の通信も検知し、自動制御できます。ユースケース②

[要件例]

1. 内部サーバ A とBとの間の通信において事前定義してある通信以外が流れた場合は異常通信として検知する。
2. 検知した場合は異常通信を発生している送信元IPアドレスをブロックリストとして自動配信。

[構成例]



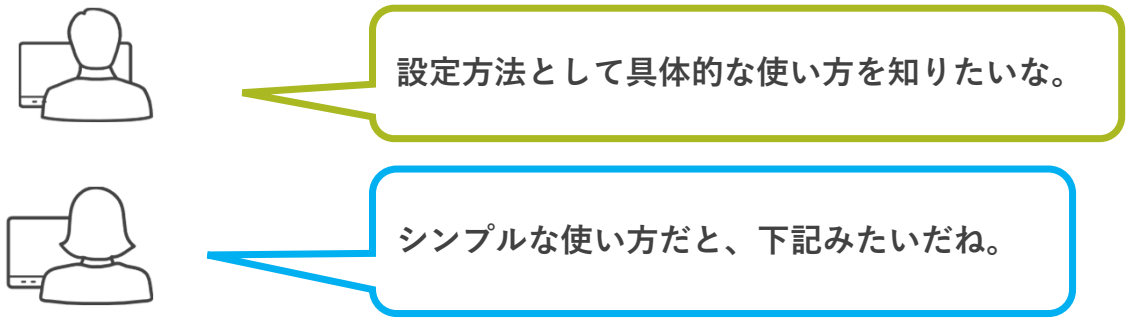
[SRX上の設定例]

1. サーバ A とB 間の通信のみ正常
2. 通信は ポート番号 50000 のみ正常

[異常通信として検知するパターン例]

1. サーバA 以外のデバイスからサーバB への通信が発生
2. ポート番号 50000 以外の通信がサーバBへ送信 (サーバAが壊れて間違った通信を発生。または、マルウェア感染等によりPort Scan などの悪意のある通信が発生)

ジュニパーで実現する社内のコンプライアンス違反の通信への対策



「シンプルなユースケース例」

1. Aというサーバーへのアクセスの時はPort 443の通信でアクセスすることになっているので、Port443 以外の通信コンプライアンス違反 (正常では無い通信) というルールをTAP モードのSRXに入れる。

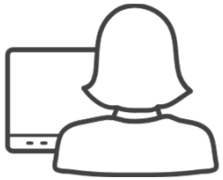
2. TAP モードのSRXがPort443以外の通信を検知した場合、ソースIP アドレスをATP Cloudへ共有する。

3. ATP Cloudを経由して、インラインに入っている他のSRX、ジュニパー製EX スイッチ、サードパーティ製のスイッチ/Wifiなどに情報を共有し、自動的に該当端末を隔離する。

③サードパーティ製の機器との連携

サードパーティ製の機器との連携についてよくある会話

(疑問)
いろいろなベンダーの機器が入っているんだけど、未知の脅威が検知された時に、各機器ごとに手動でブロックポリシーを入れるの大変なんだよね。



ベンダーが異なると機器ごとに設定方法がことなるもんね。

リアルタイムにブロックポリシー入れないと社内内に脅威広がってしまう可能性があるのに。。

全ての設定を管理するのは無理だとしても、ブロックポリシーだけは一括で適用してくれるソリューションがあるといいよね。

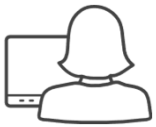
サードパーティ製の機器との連携についての課題

問題：
異なるベンダーの機器が社内に存在しているが、未知の脅威が検知された時も手動で各機器にブロックポリシーを追加しなければならない。

課題：
１．ベンダー毎にブロックポリシーの設定方法が異なる。
２．手動だと時間がかかり、その間に脅威が社内に広がってしまう。

求められるソリューション：
１．未知の脅威を検知できる。
２．脅威を検知したら、一括でブロックポリシーを各ベンダー機器に適用できる。

ジュニパーで実現するサードパーティ製の機器との連携対策



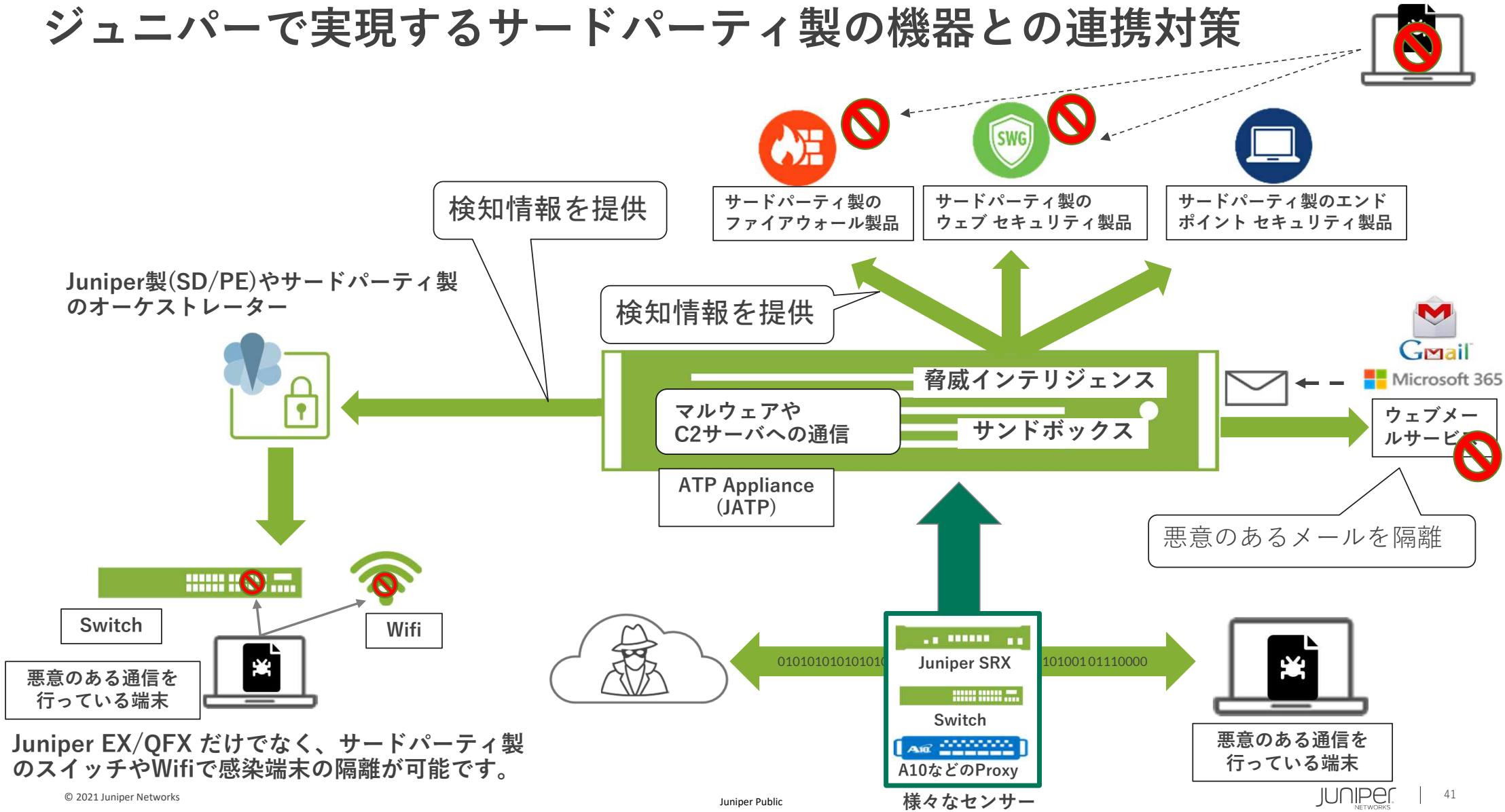
ジュニパーが何かソリューション持っているみたいだよ。

そうなんだ。必要な機器って何？

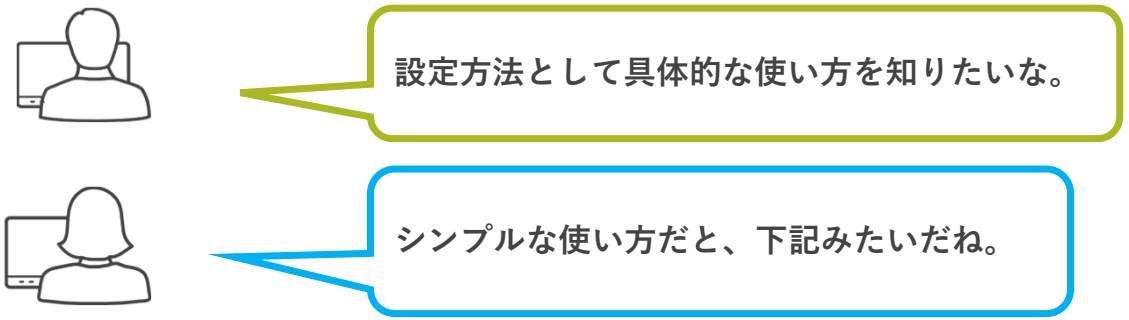
「必要な機器」

1. オンプレミス型の ATP Appliance ＊スイッチなどからミラー通信を受信し未知の脅威を分析/検知/対応する脅威インテリジェンス
2. Security Director/Policy Enforcer ＊ジュニパー製やサードパーティ製のスイッチ/Wifiで自動隔離するためのオーケストレーター

ジュニパーで実現するサードパーティ製の機器との連携対策



ジュニパーで実現するサードパーティ製の機器との連携対策



「シンプルなユースケース例」

1. SRX、A10、スイッチのミラーポートなどで、ウェブ/メール/SMB通信コピーをATP Appliance へ転送する。
2. ATP Appliance 上で未知の脅威を検知した際のブロックポリシーの適用先を決める。
3. サードパーティ製のスイッチやWifi へもブロックポリシーを適用される場合は、Security Director/Policy Enforcer とサードパーティ製の認証サーバーとの連携を設定する

④セキュリティログの管理問題

セキュリティログの管理についてよくある会話

(疑問)
いろいろなセキュリティベンダーの機器が入っているんだけど、検知ログをリアルタイムに分析できていないんだよね。

Syslogサーバーはログをためる用途ではいいんだけど、どの検知ログに注意すべきなのか分からないんだよね。

SIEMは機能が沢山あるんだけど、価格が高いんだよね。少ない管理者メンバーで使いこなせるか微妙だし。

Syslogサーバーではダメなの？

じゃあ、SIEMと言われるの製品を検討したらどう？

機能が多くても全ての機能を使いこなせるか分からないもんね。SyslogサーバーとSIEMのあいだぐらいのソリューションあるといいよね。

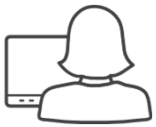
セキュリティログの管理の課題

問題：
社内のセキュリティベンダー機器が検知したログをリアルタイムに分析/管理できていない。

課題：
１．シスログサーバーではどの検知ログに注意すべきか分かりづらい。
２．SIEMを検討したが、少ない管理者で運用できるか分からないし、価格も高いので手が出しにくい。

求められるソリューション：
１．各セキュリティベンダーからの検知ログを受信できる。
２．注意すべき検知ログが分かる。
３．安価に実行できる。

ジュニパーで実現するセキュリティログの管理対策（Security Director Insights）



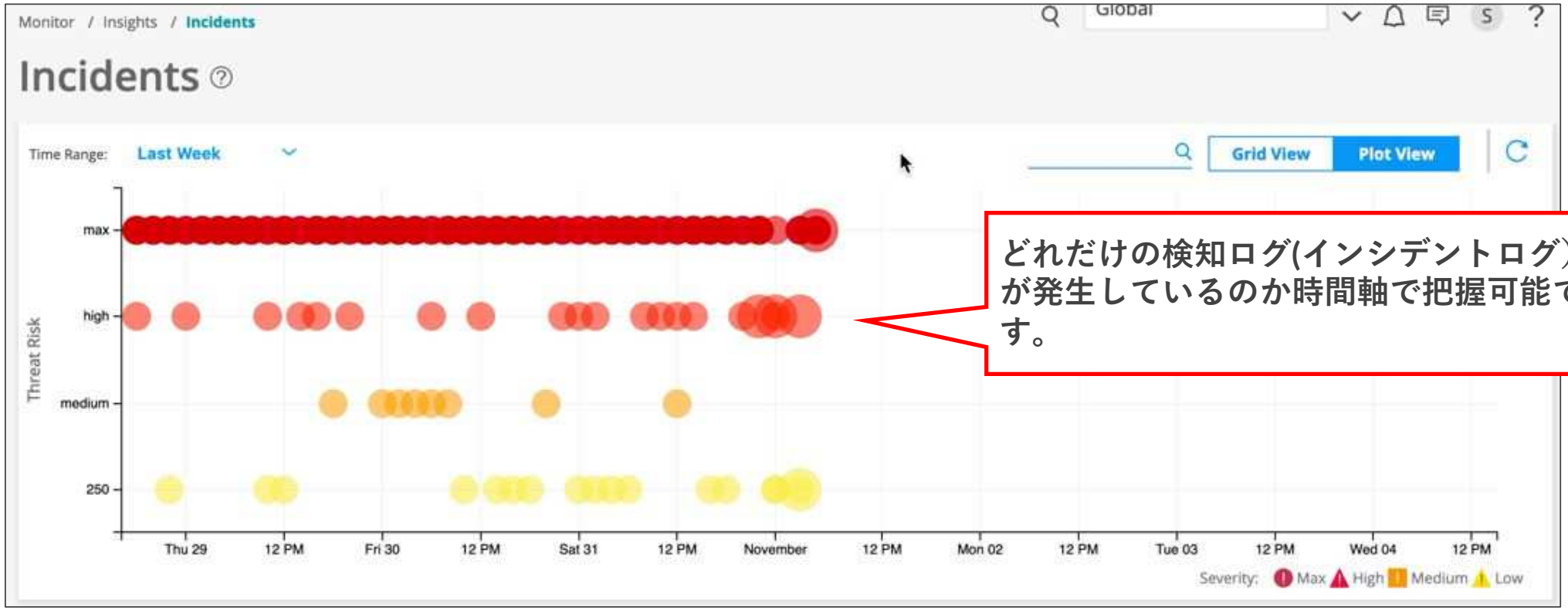
ジュニパーが何かソリューション持っているみたいだよ。

そうなんだ。必要な機器って何？

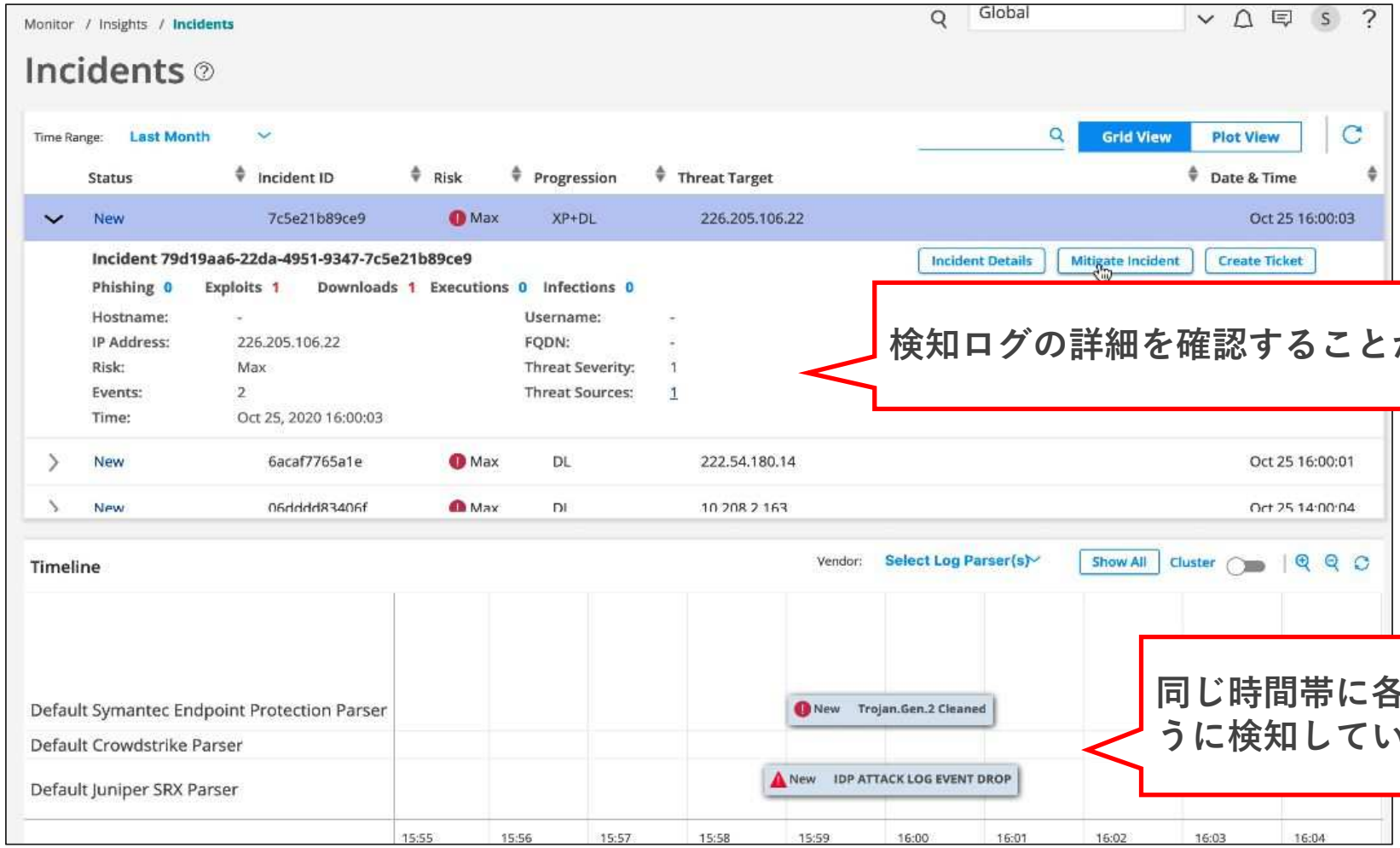
「必要な機器」

Security Director Insights ＊ジュニパー製やサードパーティ製のセキュリティ機器からのシスログ(検知ログ)を受信する機器

ジュニパーで実現するセキュリティログの管理対策 (Security Director Insights)



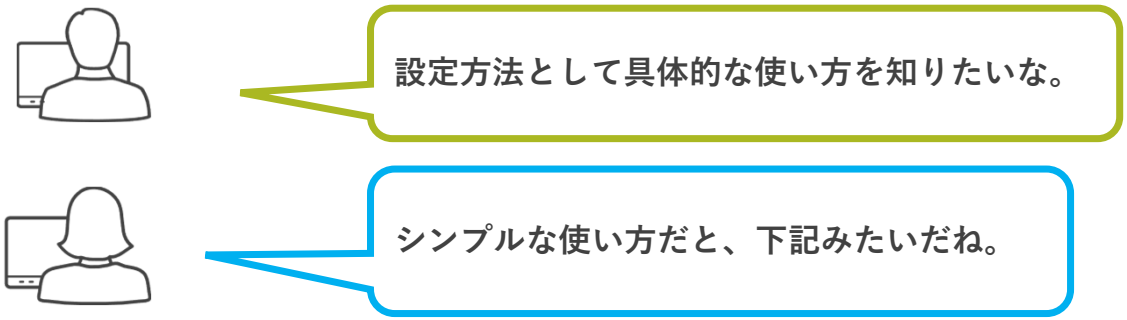
ジュニパーで実現するセキュリティログの管理対策 (Security Director Insights)



検知ログの詳細を確認することができます。

同じ時間帯に各ベンダーがどのように検知しているのか分かります。

ジュニパーで実現するセキュリティログの管理対策（Security Director Insights）



「シンプルなユースケース例」

1. 取り込む予定のシスログのサンプルログを使ってSecurity Director Insights にログフォーマットを認識させる。
2. 閾値を超えた検知ログを受信した場合は管理者にアラートメールを送付する設定を入れる。

5．まとめ

Juniper Connected Security のまとめ

ネットワークとセキュリティは日々複雑になります。

ゼロトラスト セキュリティに向けたリアルタイムで自動化できるセキュリティが必要です。

Juniper Connected Securityはオンプレミス、クラウドに関わらず、全てを繋ぐセキュリティを提供します。


Thank you
JUNIPER NETWORKS
Engineering
Simplicity