ジュニパーネットワークスが提供する
次世代セキュリティソリューション（JATP）
よくあるご質問 (FAQ)

Table of Contents

General

1. JATP とはどのような製品ですか？

サンドボックスと SIEM 機能を有した次世代セキュリティソリューションです。

2. どんなメリットがありますか？

マルウェアの高い検知率を誇り、他のセキュリティ製品との連携、自動化によるコスト削減が可能です。

3. 具体的な機能を教えて下さい。

ウェブ、E メール、端末間の通信上の未知なる脅威を静的/動的(ふるまい)検知、機械学習、レピュテーションにて継続的にモニタし検知します。検知した脅威に対しては手動/自動により同じ脅威通信を通過させないように、また、感染端末から C&C サーバーへの通信を通過させないように迅速に対応することが可能です。

4. ライセンスは必要ですか？

はい、ご利用になられる機能/帯域/年数を元にライセンスをご選択頂き、適用して頂く必要がございます。

5. 必要な構成要素は何ですか？

脅威分析エンジンであるスマートコア及びデータ収集の為のコレクターが必要となります。

6. スマートコアは専用のアプライアンスが必要ですか？

専用の HW アプライアンス（JATP700）もございますが、仮想アプライアンス(VMware)でもご利用が可能です。仮想アプライアンス版についてはクラウド環境でご利用頂く事も可能です。

7. コレクターは専用のアプライアンスが必要ですか？

専用の HW アプライアンス（JATP700）もございますが、仮想アプライアンス(VMware)でもご利用が可能です。将来的に、SRX シリーズをコレクターとしてご利用頂く事も可能です（2018 年 3 月末予定）。

8. スマートコアはインターネット接続が必要ですか？

はい、最新の脅威を分析する為のアップデートがあるので接続をお願いします。

9. コレクターは通信に影響を与えませんか？

専用アプライアンス(JATP700) や VMware にてご利用の場合は SPAN/TAP での構成となりますので、基本的にインラインの通信への影響は発生致しませんが、SPAN/TAP から受信するトラフィック量に合わせたコレクターの設置をお願い致します。また、SRX をコレクターとご利用の場合は、インラインでご利用される形が多いかと考えられますので、ご環境に合わせた機器のご選択をお願い致します。

10. 既存の管理システムを運用しておりますが、連携は可能ですか？

はい、登録されたエコパートナーの製品であれば Web 画面から簡単に連携する事が可能です。

11. どんなサードパーティ製品やソリューションとでも連携可能ですか？

現時点では登録されたエコパートナーのみが相関分析の対象となっております。

しかしながら、セキュリティに関連するテキストベースのログであれば、どのような

フォーマットであっても収集/相関分析可能となるよう拡張予定です。(2018 年末予定）。

12. テストしたいのですが、テストライセンスはありますか？

はい、テストライセンスは 30 日で、最長 90 日が可能です。

Technical

13. Syslog はどの値を見てタイムラインの相関分析を作成していますか？

タイムスタンプ、 IP アドレス, ホストネーム, ユーザネーム, Email アドレスを見ています。

14. HTTPS トラフィックの解析は可能ですか？

SRX をコレクターとしてご使用頂く事で解析可能です。

15. ストレージにアーカイブされているファイルのスキャンは可能ですか？

不可です。

16. コレクターは IPv6 トラフィックをサポートしていますか？

現時点ではサポートしておりませんが検討中です（2018 年 6 月予定）。

17. JATP は Mac OS をサポートしていますか？

はい、Mac Mini をセカンダリコアとしてご導入頂く事により、追加で Mac OS のファイルが検出可能となります。

18. チケット管理の機能はありますか？

はい、チケット管理機能が御座います。また、API も公開されておりますので、外部チケット管理システムと連携することも可能です。