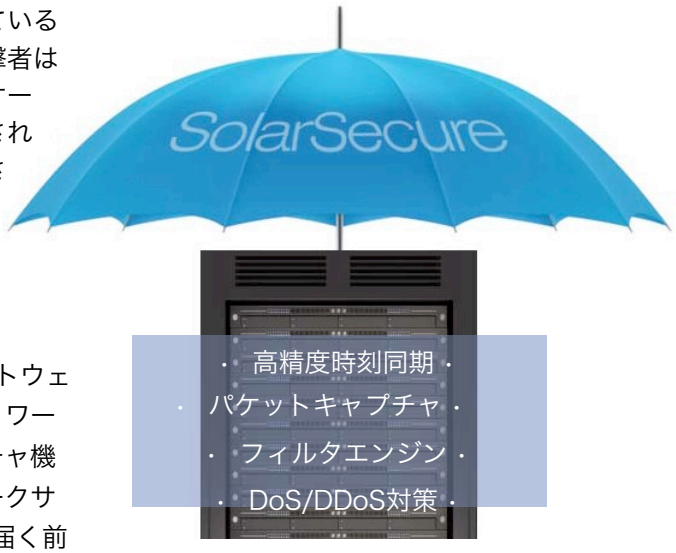
SOLARFLARE®

SolarSecure

SolarSecure 分散アクティブセキュリティ

SolarSecure™ は、ネットワークサーバー内に実装されるサイバー攻撃対策を主眼とした初の分散アクティブセキュリティソリューションです。 SolarSecure は、正確な記録・キャプチャ・フィルタ・悪意あるトラヒックがサーバーに届く前でのフィルタとブロック、等の機能をサーバーに構築します。

最近において、より大きく公表されているセキュリティ上の弱点を見ると、攻撃者はビジネス上のクリティカルなアプリケーションや影響の大きなデータが格納されていながら、外部ネットワークに晒されて保護されていないようなネットワークサーバを標的としています。



そこで今。

SolarSecure はアプリケーションソフトウェア群として提供される初めてのネットワーク強化技術であり、効果的なキャプチャ機能・悪意あるトラヒックがネットワークサーバーのOSやアプリケーションへと届く前に検出しブロックする機能・セキュリティーポリシーの施行などに必要な精巧さを備えており、追加的ハードウェアを必要としません。

SolarSecure アクティブセキュリティ層は Solarflare の先進的な Flareon™ 10/40ギガビットイーサネットアダプタに装備されており、最新水準の保護をネットワーク全体に展開し、目的の資産に対する統合的・リアルタイム・アクティブな保護をもたらします。現在はこれらの機能に加え、高精度時刻機能・パケットキャプチャ機能・分散サービス妨害攻撃(DDoS)対策を提供しています。

高精度時刻機能

現在、企業の最高情報責任者(CIO)や最高情報セキュリティ責任者(CISO)などがeコマースやサービスプロバイダーネットワークを運営する際、高い性能・データや電子的記録の精密な監視・記録・解析による適切な調整・法令遵守上の警告・包括的リアルタイムネットワークセキュリティへの要求の増大に直面しています。

ネットワークとすべてのサーバーに高精度時刻を供給した上で、タイムスタンプが付与されたネットワークデータにて通信を行うことにより、ネットワーク遅延やパケット損失などの測定値がよりずっと正確となり、的確な対処を行いやすくなります。

Solarflare は IEEE-1588 v2 高精度時刻同期プロトコル(PTP)によるクロック同期とイーサネットパケットへのハードウェアタイムスタンプ機能を提供します。

これにより、サーバーへの二枚目のネットワークアダプタの実装や専用装置の装備の必要、さらには時刻同期を目的とした追加の物理ネットワークの必要はありません。

Solarflare SolutionsGuide

hpc@elsa-jp.co.jp
Tel: (03) 5442-4161
Fax: (03) 5765-7235
www.elsa-jp.co.jp

SolarCapture™ Pro

データセンター管理者はシステムの性能向上を図る際に、正確な計測手段がないために非常に苦労することがよくあります。
正確な計測を行うために、ラインレート処理可能なパケットキャプチャ装置とそれを接続するためのネットワークタップ装置とをより多く設置することによって、ネットワークの状況をより正確に観測出来るようにしながら、その追加ハードウェア基盤のために莫大な費用がかかること及び、性能低下をもたらすことを避けなければなりません。アプリケーションとネットワーク性能の最適化、企業の法令遵守の維持、セキュリティー上の脅威およびデータ損失の回避のためには、より大規模なネットワーク可視化が必要となります。
SolarCapture Proにより、ネットワーク監視専用の追加的ネットワーク装備・特殊で高価なスイッチ装置やネットワークアダプタの必要性とそれに掛かる費用を削減します。それらの代わりに SolarCapture Pro はすべてのサーバーを高精度時刻を持ったネットワークタップとして利用可能とし、ネットワークの可視化・ネットワーク装置とその性能の解析性能を向上します。
SolarCapture Pro は、ネットワークスタックおよびカーネルをバイパスしてユーザー空間に直接パケットを転送する機構により、高水準なパケットキャプチャ性能を実現しています。

SolarSecure™ フィルタエンジン

Solarflare DDoSアタック防御機能の中核部に、Solarflare フィルタエンジンがあります。このフィルタエンジンはネットワークアダプタに統合されており、ネットワークからの攻撃がOSを通過してサーバー上のアプリケーションに影響を与える前にブロックします。フィルタエンジンは、パケットをフィルタし、ブロックし、転送レートを制限し、悪意あるトラヒックに対し警告を発するとともに、お客様のポリシーやルールセットおよびサードパーティによる脅威情報データサービスと連携させることを可能とするAPIを含みます。フィルタエンジンはきわめて早期に悪意あるトラヒックを検出し、攻撃を長期にわたり吸収しながら、正常なトラヒックの処理能力の低下がなく、サーバーの追加による処理能力のスケールアップを保ちます。

また、DDoSアタックに対する際も、フィルタエンジンを用いることによりサーバーのヘッドルームと応答性の向上をもたらします。事実、フィルタエンジン利用のテストによりサーバーのヘッドルーム、すなわち悪意あるトラヒックに見舞われている中で正常なトラヒックを供給し続ける能力が、8倍に向上することを示しました。ベンチマークテストにおいて、SolarSecureが機能しているウェブサーバーは一秒間12万接続の攻撃を受けながらも性能低下なくサービスを維持しました。一方で、SolarSecure が機能していないウェブサーバーは一秒間に1万5千接続までの攻撃に耐えるに留まりました。さらに、SYNフラッド攻撃テストにおいて、SolarSecureフィルタエンジンは他社製品と比較して180%高い性能を発揮しました。Solarflare 製ハードウェアとソフトウェアにより一秒間に1600万パケット(1パケット60バイトの場合)を送出できます。一方、他社の最も高性能なモデルでは一秒間に900万パケットの能力に留まりました。

SolarSecure による DoS/DDoS 防御

サービス妨害攻撃(DoS)や分散サービス妨害攻撃(DDoS)はネットワークセキュリティにより対策する問題の中でも拡大を見せている攻撃で、ネットワークリソースを枯渇させることにより意図するユーザーがマシン・サービス・ネットワークリソースを利用することを妨げます。ある一般的な攻撃方法では、標的マシンの外部通信応答部を枯渇させることにより、正常なトラヒックへの応答を不能にしたり、応答時間をサービス不能状態とみなされるまでに遅くさせることで攻撃を達成します。SolarSecure DDoSはホストサーバーにおけるセキュリティーを目的とした拡張レイヤーで、DoSおよびDDoS攻撃に対する防御を行って、ホストOSがこれら攻撃に晒されることを防ぎ、さらにルーター装置・ファイアウォール・ホストOSと連動させることができます。SolarSecure DDoS Linux カーネルドライバは SYNクッキー、ブロック、フィルタリング、転送レート制限とともに、独自のルールセットの適用およびサードパーティによる脅威情報データサービスと連携させることを可能とするAPIを含みます。

SolarSecure

SolarflareSolutionsGuide

SOLARFLARE®

ELSA

hpc@elsa-jp.co.jp
Tel: (03) 5442-4161
Fax: (03) 5765-7235
www.elsa-jp.co.jp