# ARXAN がクライアント Web アプリ向けの
# 高度なセキュリティソリューションを発表

*アプリケーションセキュリティのリーダーである Arxan が、*
*コード保護、リアルタイム監視、アラート、脅威分析を Web アプリケーションへ拡張*

**2018 年 9 月 14 日米国カリフォルニア州サンフランシスコ市発信** – アプリケーション保護ソリューションで信頼を得ている Arxan Technologies Inc. (日本法人：アークサン・テクノロジー合同会社：東京都港区)は本日、業界最高レベルのクライアント Web アプリ向け保護ソリューションの最新機能強化版 Arxan for Web を発表しました。 Arxan for Web は、多層防御アプローチで企業がサーバー側（API）攻撃や認証情報の盗難から組織を容易に守れるようにします。

- パッシブ保護 - コードを難読化し、攻撃者がリバースエンジニアリングを理解し分析することを困難にします
- アクティブ保護 - コード分析、改ざんまたはマルウェア攻撃を検知した場合、ブラウザをシャットダウンするか攻撃されたコードを修復できます
- リアルタイムアラート - Arxan Threat Analytics を使用して、不正行為や分析を試みたと疑わしいアカウントを通知し、隔離した上で保護されたコードを更新します。

グローバルなデータ侵害の継続的な増加は、たった一度の被害で平均 386 万ドルのコストがかかるため、ビジネスパフォーマンスに大きな影響を与えます。 また、API ベースの攻撃が特に急増すると想定されています。 ガートナーによると、2022 年までに、API 乱用が最も頻繁に発生する攻撃進路になり、その結果、エンタープライズ Web アプリケーションのデータ侵害が起こるとしています。クライアント側の脅威が増えれば、積極的でタイムリーな脅威対応の重要性が増します。

Arxan の CEO である Joe Sander は次のように述べています。「Arxan for Web により、組織がリアルタイムに脅威レポートを受け取ることができるので、企業は、攻撃が API を介してバックエンドシステムに到達する前に脅威に対応できるようになります。 コード展開、クライアント側の早期攻検出と修復の一連のセキュリティプロセスを実現することで、重要なバックオフィスシステムや資産の侵害を防ぐことが可能です。」

OWASP によると、JavaScript は主要な Web 言語になっています。 同時に、OWASP は、資格情報を盗んだり、Web トラフィックを悪意のあるサイトにリダイレクトしたり、Web サイトを改ざんするためにブラウザセッションを乗っ取るクライアント側の攻撃である Cross Site Scripting（XSS）が、アプリケーションの最高のセキュリティリスクの 1 つであると報

告しています。 ブラウザは、何年も Cross Site Scripting 攻撃に対抗しようとしていますが、Arxan for Web はこれを防御し、攻撃をリスク管理システムに報告することができます。

Arxan の製品管理担当 VP である Rusty Carter は次のように述べています。「JavaScript は信じられないほど強力な言語ですが、それがセキュリティに関しての 1 つの欠点になっています。JavaScript コードは実行時に解釈されます。これは、JavaScript ベースのソフトウェアをダウンロードするほとんどの人が、それを動かすコードに完全にアクセスできることを意味します。企業や組織のセキュリティチームは、これまで、セキュリティ資産をファイアウォールの背後で実行されるいわば境界セキュリティに集中させてきました。 特に金融サービス、電子商取引、ゲーム、デジタルメディアなどの Web アプリケーションを展開している場合、その境界を通過する攻撃は、クライアント側で、数週間、数日または数時間、つまり不審なやりとりの発生を疑う前に開始されてしまいます。

OWASP の調査では、ほとんどの組織が侵害を検出するまでには時間がかかりすぎて、手遅れになるまで脅威に適切に対処することができないとしています。「ほとんどの違反調査では、侵害を検出する時間が 200 日を超えていることが示されています。そしてそれは通常、内部プロセスや監視ではなく外部の当事者によって検出されます。不十分なログの搾取と監視は、ほぼすべての主要な事件の根幹の課題です。攻撃者は、タイムリーなモニタリングとその対応の欠如を拠り所として、検知されることなく目標を達成することができるのです。

Arxan Threat Analytics は、組織にタイムリーなレポートとインテリジェンスでアプリケーションセキュリティに必要とする可視性を提供します。それにより、ワイルドな環境に配信されている Web アプリケーションに対する進化する脅威の先を行くことができます。 たとえば、デバッガが Web アプリケーションに接続されている場合、Arxan はすぐにその行為をレポートし警告します。

Arxan のエンジニアリング担当上級副社長に最近就任した Krixh Kalkiraj は次にように付け加えます。「クライアント側を保護し、悪意を持ったハッカーが調査に入っている段階で差し迫った脅威の早期警告を組織に提供することは、画期的です。 このような先進的なイノベーションは、グローバルビジネスに真の影響をもたらします。私が Arxan チームに加わった理由がここにあります。」

Kalkiraj は、Arxan for Web や Threat Analytics だけでなく既存のアプリケーション、コード、キー保護技術の継続的な開発をリードしていきます。 Kalkiraj はこれまで、Intuit、PTC、ThreatMetrix などの企業でリーダーシップを発揮してきたテクノロジーリーダーです。 彼は、技術的な専門知識の深さ、製品開発の全体像、共通の目標に向かって共同作業するクロスファンクショナルチームへのサポート力で定評があります。

## Arxan Technologies について

業界で最も包括的なアプリケーション保護ソリューションを提供し世界的に信頼される業界リーダーである Arxan は、ビジネスにおいて重要なアプリケーションを保護し、安全に配信および管理したいというお客様にソリューションを提供しております。 Arxan は、現在、金融サービス、モバイルペイメント、ヘルスケア、自動車、ゲーム、エンターテイメントなど、多くの業界で 10 億以上のアプリケーションインスタンスを保護しています。 Arxan は、悪意のあるハッカーをパラメータ設定による障壁で排除したり、デバイス管理の制御を必要とするこれまでのセキュリティプロバイダのアプローチとは異なり、アプリケーションレベルで内部から保護するソリューションを提供しています。この Arxan のアプローチでは、アプリケーションのソースコードとバイナリコードを保護することで企業の信頼領域を拡大します。 Arxan は、ダイナミックなアプリケーションポリシーエンジン、コード堅牢化、難読化、暗号化、ホワイトボックス暗号、脅威解析などの幅広いセキュリティ機能を提供しています。 2001 年に設立され、北米に本社を置き、EMEA および APAC にグローバルオフィスを構えています。詳細については、www.arxan.co.jp をご覧ください。