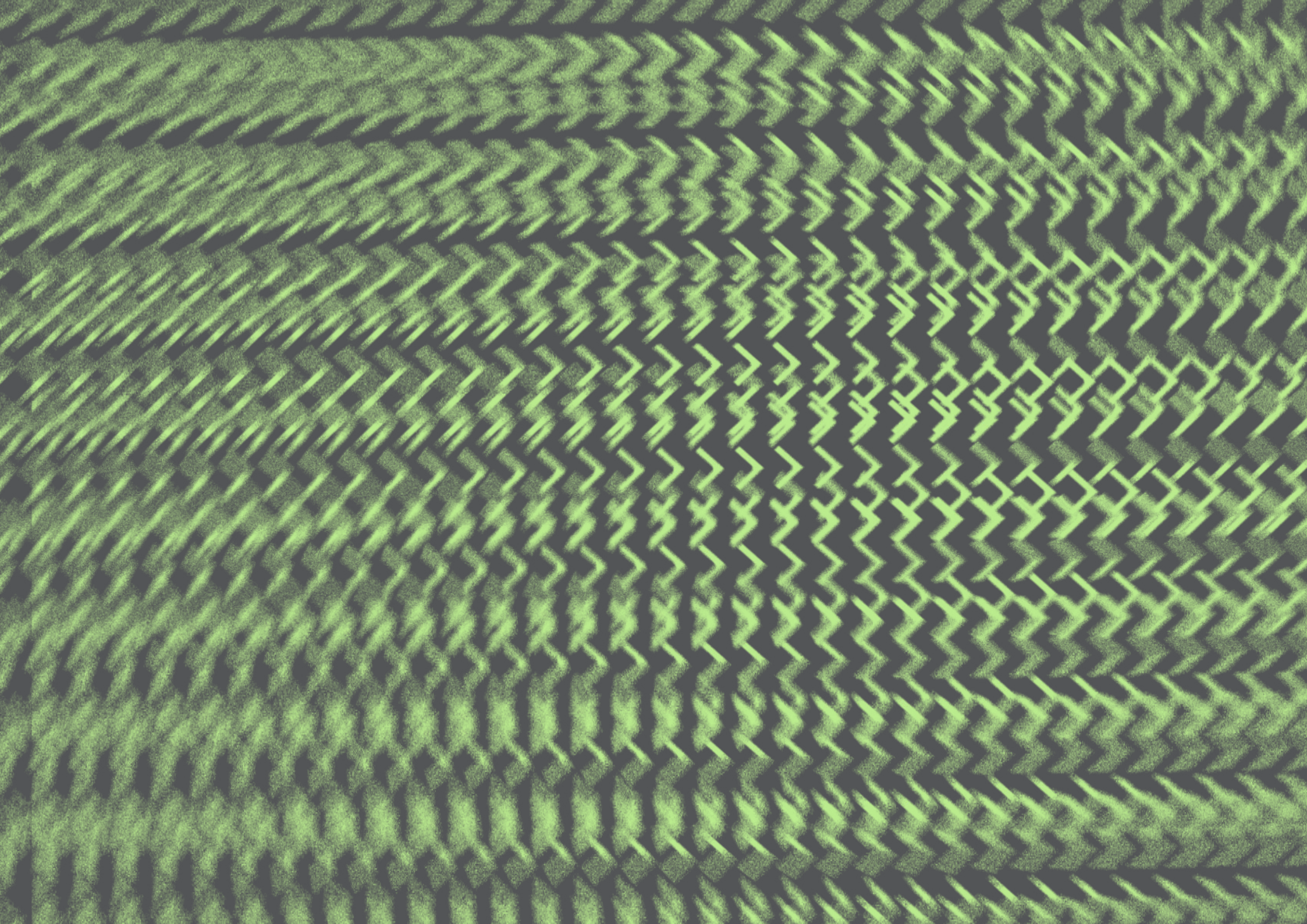
EBOOK

Sysdig CNAPPの特徴について

お客様事例と共に紹介



Sysdigのクラウドネイティブアプリケーション
保護プラットフォーム(CNAPP)

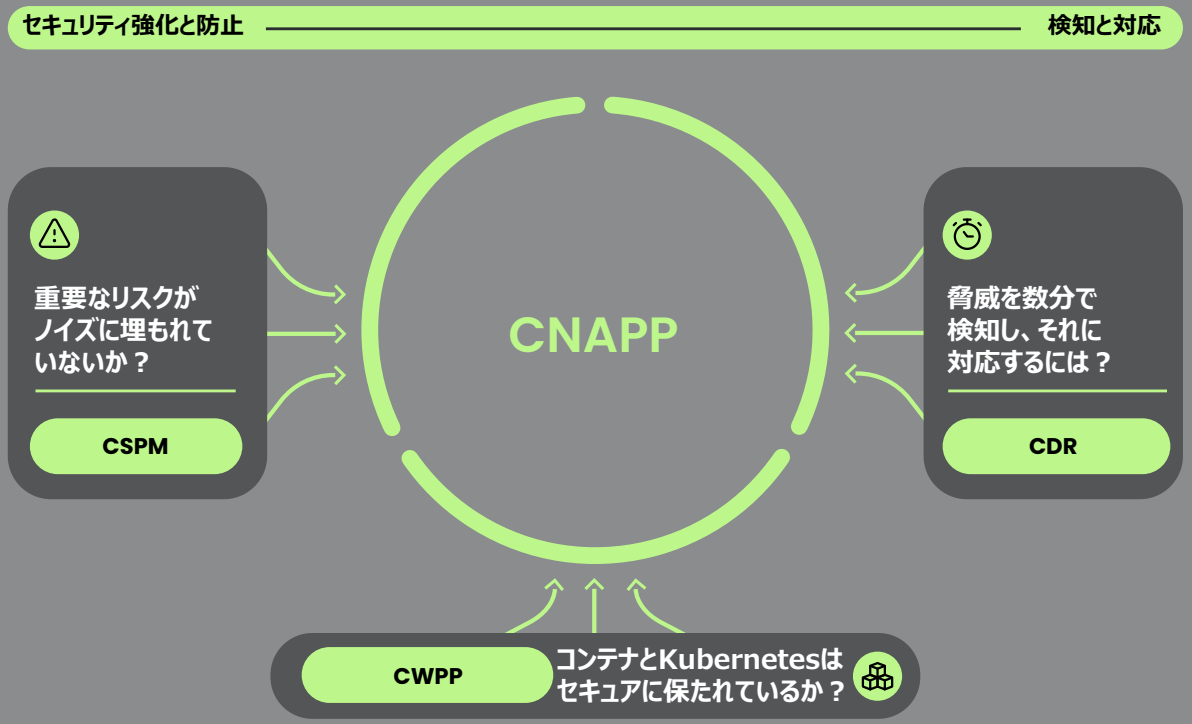
クラウドセキュリティの発祥とその行く末

2000年代初頭、クラウドの人気が高まり始めていたにもかかわらず、ほとんどの企業は、まだオンプレミスのインフラを使っていました。同様に、セキュリティもクラウド向けではなくオンプレミス向けに設計されていました。その結果、企業や組織は従来のセキュリティ対策（ファイアウォール、侵入検知システム、アクセス制御など）をクラウド環境に再利用していました。

このため、クラウド環境の可視化は企業や組織にとって課題となっていました。セキュリティチームは、クラウドインフラ内のインシデントや脆弱性の監視に課題を抱えており、クラウドプロバイダーが実装したセキュリティ対策に頼るしかありませんでした。

当然ながら、クラウドの規模が拡大し、複雑化するにつれて、この　不十分なアプローチは通用しなくなりました。レガシーアプローチでは、クラウドにおけるアタックサーフェスの拡大や、クラウドにおける攻撃のスピードと規模についていけなかったのです。

企業は今、より強固なクラウドセキュリティ上のプラクティスを採用した上で、より優れた管理対策を導入し、さらにその対応についても準備しておく必要があります。予防を超えて、クラウドをエンドツーエンドで保護するようなツールが必要です。サイロ化、死角、ツールの乱立を解消する必要もあります。結論として、最新のクラウドには統合されたクラウドセキュリティ機能が必要です。



1つのツールで完全なクラウドセキュリティを実現

セキュリティ業界は長年にわたって多くの頭字語を同時に利用してきましたが、どうやらそれらは「CNAPP（クラウドネイティブアプリケーション保護プラットフォーム）」という1つの頭字語へと収束しつつあります。CNAPPとは、クラウドセキュリティポスチャー管理（CSPM）、クラウド検知と対応（CDR）、クラウドワークロード保護プラットフォーム（CWPP）の機能を統合したものです。

クラウドセキュリティの主なユースケースを1つのプラットフォームに集約することで、クラウド環境をエンドツーエンドで保護することが容易になります。しかし、それは同時に、完全なCNAPPを実現するには、クラウドセキュリティスタックのあらゆる部分を処理できるツールが必要であることも意味します。

以降のページでは、**Sysdig**が提供する**CNAPP**を利用することでいかなるメリットが得られたかについて、当社のお客様の声を紹介します。

クラウドセキュリティポスチャー管理（CSPM）

CSPMが担う機能

CSPMは、セキュリティポスチャーを強化することにより、クラウドインフラのリスクを最小限に抑えることを重視しています。CSPMツールは、設定ミスやポスチャードリフトを検知して修正し、侵害を防止すると共に、コンプライアンスの確保を支援します。

CSPM

“当社では、Sysdigが、より適切な情報に基づいてポスチャーに関する意思決定を行うために、本番環境で使用されているあらゆるものに関する知識を利用している点を気に入っています。Sysdigは80%以上のノイズを除去できます。要するに、CSPMはSysdigの主力製品であり、インフラリスクへの不安を軽減します。

— BigCommerce社のシニア
インフラストラクチャセキュリティエンジニア

CSPの導入事例

BigCommerce社、リアルタイムのクラウドセキュリティを実現

課題

BigCommerce社はクラウドベースのeコマースプラットフォームであるため、セキュリティとコンプライアンスを維持することが欠かせません。大量のアラートノイズと不十分なサポートに悩まされた結果、BigCommerce社はSysdigを採用することにしました。

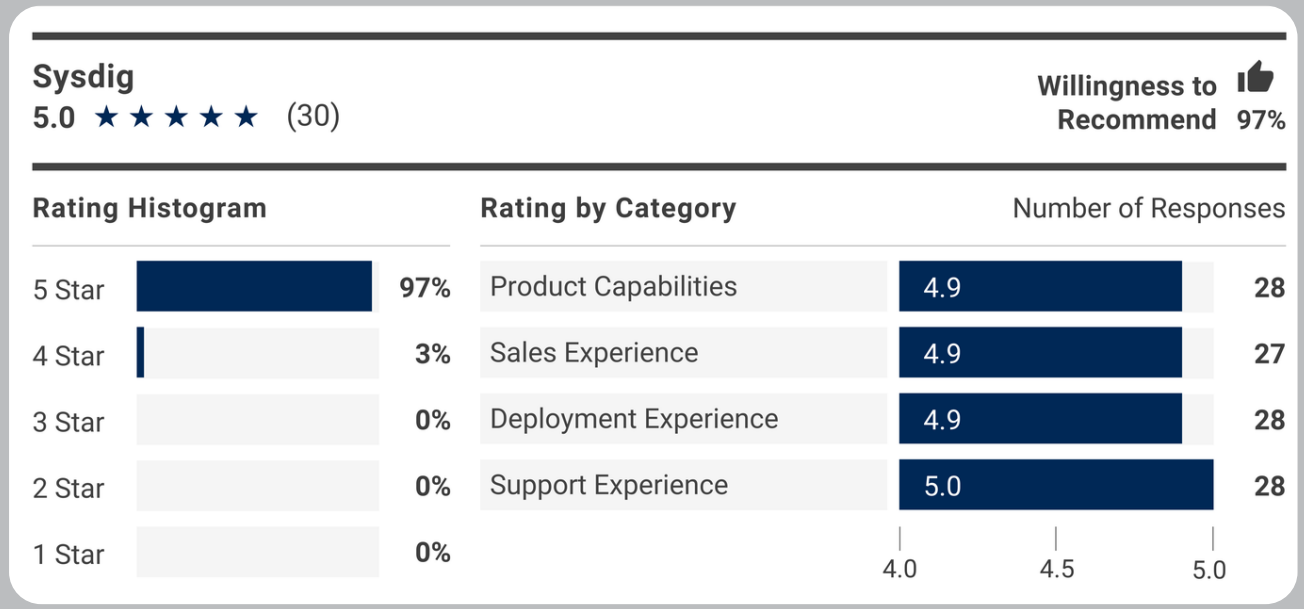
導入結果

Sysdigの導入により、BigCommerce社は脆弱性、脅威、設定ミスをリアルタイムで特定し排除できるようになり、同時にコンプライアンス要件もすべて満たすことが可能となりました。また、ランタイムインサイトを活用することで、脅威データの可視化と分析を直感的に行えるようになりました。

20% 設定ミスや脆弱性の特定と優先順位付けにおける効率性が向上

80% 脆弱性に関するノイズを低減

BigCommerce社における導入事例のビデオを見る >>>



Gartner®『Voice of the Customer』レポートのCSPM分野におけるSysdigの評価結果

CSPM

Sysdigが第1位にランクされる

Gartner®『Voice of the Customer』レポートのCSPM分野において

Gartner®『Voice of the Customer』レポートは、実際の顧客からのレビューと評価を統合したものです。Sysdigは、同レポートのCSPMツール分野において、2社しかないストロングパフォーマーの1社として評価され、顧客から5つ星中5つの総合評価を得た唯一のベンダーとなりました。

クラウド検知と応答（CDR）

CDRが担う機能

クラウド検知と対応（CDR）を利用することで、セキュリティチームは、クラウドのワークロードとインフラを保護できるようになります。CDRは、既知および未知の脅威のリアルタイム検知、イベントに対するクラウドネイティブなディープコンテキスト、そして脅威を根絶するための手動および自動の対応策を提供します。

CDR

SOC 2コンプライアンスを実現するために、当社では、脆弱性スキャン、監査ロギング、そしてランタイムセキュリティを必要としていました。Sysdigは、これらの機能をすぐに提供してくれます。

— Data Notebook Company社の
シニアDevOpsエンジニア

CDRの導入事例

Data Notebook Company社、高度な攻撃の阻止に成功

課題

この企業の提供するクラウドベースのデータノートブックは、ビジネスインテリジェンス、プロジェクト管理、A.I.による分析を融合したものです。ユーザー数が急増した後、同社はクリプトマイニング攻撃の急増を防ぐためにSysdigを採用しました。

導入結果

予想された大量の攻撃は発生せず、同社はポリシーを調整する必要すらありませんでした。また、Sysdigは、監査ロギング、ポリシー管理、脆弱性スキャンを通じて、同社のSOC 2コンプライアンスを支援しています。さらに、同社のDevOpsチームは、作業負荷への影響を最小限に抑えつつ、クラウドセキュリティとコンプライアンスを実現できるようになりました。

99% 悪質な行為への対処にかかる時間を削減

60件以上 1日あたり発生するクリプトマイニング攻撃をブロック

CDR

Falcoをベースとして構築されたリアルタイムの脅威検知
SysdigのCDRはFalcoをベースとして構築されていること、そしてFalcoを開発したのはSysdigであり、現在もSysdigがFalcoのメンテナンスを支援していることをご存知ですか？

Falcoは、ダウンロード件数が1億1,500万を超えており、IBM、Apple、Booz Allen Hamiltonのような企業から貢献を得ています。Falcoは、あらゆるクラウドプロバイダーを含む業界全体で選ばれている脅威検知エンジンです。

CLOUD NATIVE COMPUTING FOUNDATION

FALCO GRADUATION 2024

クラウドワークロード保護プラットフォーム（CWPP）

CWPPが担う機能

CWPPは、コンテナ、サーバー、サーバーレスワークロードなどのクラウドワークロードを保護します。CWPPは、ハイブリッド環境やマルチクラウド環境を可視化し、開発パイプラインにおけるリスクをスキャンし、ランタイムの攻撃からワークロードを保護します。

CWPP

Sysdigを導入してすぐに、当社では、脆弱性を特定し、稼働中のクラスタに対するポスチャーとコンプライアンスを確認できるようになりました。この可視性のレベルは驚異的であり、このような可視性が理由で、当社はSysdigをKubernetes向けに使用する唯一のセキュリティツールとして導入しています。

— Apree Health社の
情報セキュリティ部門シニアマネージャー

CWPPの導入事例

Apree Health社、コンテナに関する可視性を実現し、コンプライアンスを満たす

課題

Apree　Health社では、患者がより手頃な価格で、より適切な治療結果を得られるように設計された一連のソリューションを通じて、医療業界が抱えるデータサイロを打破しようとしています。同社は、コンプライアンスを合理化し、全体的なセキュリティとインシデント対応を強化するためにSysdigを導入しました。

導入結果

Sysdigを導入することで、Apree Health社は、単一の統合ビューを通じて同社のKubernetesデプロイメントに関して深くまで可視性を確保できるようになりました。これは、脆弱性と設定ミスのスキャンと共に、同社のコンプライアンスへの取り組みにとって非常に貴重なものです。また、Sysdigの導入により、Apree　Health社のセキュリティオペレーションチームは、リスク、脅威、脆弱性の管理が大幅に容易になりました。

10時間以上　セキュリティとコンプライアンスの実現にかかる月あたりの時間を削減

80%　修正にかかる時間を短縮

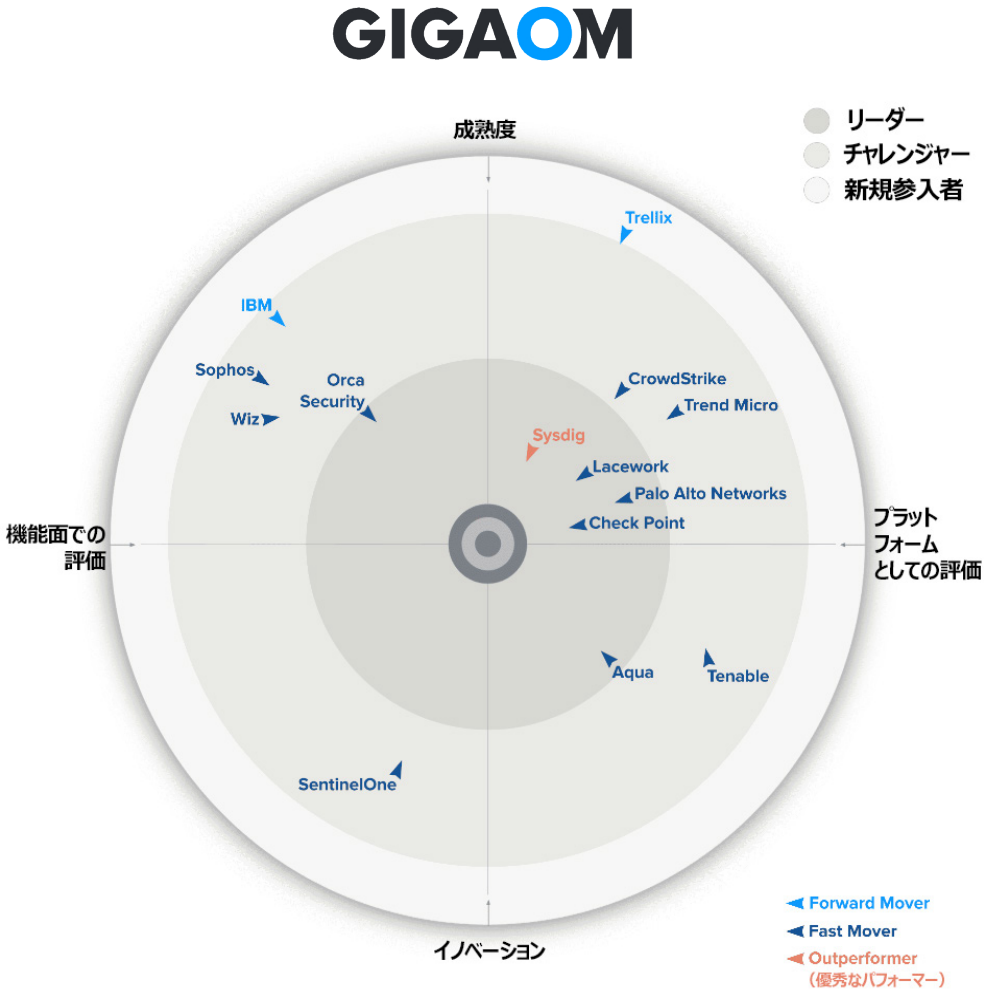
CWPP

GigaOmレポート、クラウドワークロードセキュリティ分野でSysdigを最も高く評価

『GigaOm Radar for Cloud Workload Security』において、Sysdigはリーダーに認定されたほか、「アウトパフォーマー」に選ばれた唯一のソリューションとなりました。

Sysdigは、その卓越したハイブリッド環境サポートと優れたワークロード検知および応答機能が理由で、「成熟度/プラットフォームプレイ」クオドラントにおいて、「リーダー」および「アウトパフォーマー」として位置付けられています。

— GigaOm Radar for Cloud Workload Security 2024



クラウドネイティブアプリケーション保護プラットフォーム（CNAPP）

統合により強力なソリューションを実現

これまで説明してきたユースケースはすべて、クラウドを保護するために不可欠なものです。しかし、それらをひとつのプラットフォームにまとめることで、個々の要素を単に組み合わせた以上のソリューションが実現します。

セキュリティ強化と防止 ——— 検知と対応

SysdigのCNAPPを活用することで、環境のあらゆる側面を、エージェントベースおよびエージェントレスで、多層かつ詳細にカバーすることができます。ワークロードの事前検証から、実行中のパブリッククラウドプラットフォームの監査ポリシーまで、すべてに対応します。

Sysdigの強みは、市場最高のエンジンを搭載していることであり、これによりリアルタイムのランタイムインサイトが得られるのです。ランタイムインサイトは、使用中の知識を活用して重要なリスクを優先付けし、そのリスクを修正するためのコンテクストを提供します。

脅威の監視、検知、そして修復に対するこの包括的なアプローチの主な利点をいくつかご紹介しましょう。

- エンドツーエンドの可視化
- 運用効率の向上
- 経費の削減
- 全体的なセキュリティポスチャーの強化

CNAPP

“当社が持つ手動ソリューションのコストとSysdigのコストを1年間比較した結果、当社はSysdigを選びました。今では、以前は6つのツールを必要としていた作業が1つのツールで実現でき、Sysdigのコストを上回る削減効果を達成しています。

— 医療IT組織のシニアクラウドセキュリティおよびDevOpsエンジニア

CNAPPの導入事例

医療IT企業、コスト削減を通じてコンプライアンスを実現

課題

この会社のクラウドベースのプラットフォームは、プランの比較、コスト見積もり、医師検索ツールなどを通じて医療保険を簡素化するものです。しかし、同社が州政府と協力するようになると、ますます厳しくなるコンプライアンス基準を満たす必要が出てきました。このような理由から、同社はSysdigを採用することとなったのです。

導入結果

Sysdigを使うことで、同社はコンプライアンスを容易に実現できるようになりました。これには、コンプライアンスポスチャーのスナップショットを即座に提供し、合格したコントロールと不合格のコントロールをそれぞれ強調表示するような、すぐに使えるコンプライアンスチェックが含まれています。また、Sysdigを導入することで、同社は、医療保険の顧客とそのデータに対する脅威をリアルタイムで特定し、関連する脆弱性に優先順位を付け、コンテキスト情報を使って迅速に脅威に対処できるようになりました。

98% 脆弱性ノイズを低減

30% コンピューティングコストを削減

10時間以上 週あたりのインフラ監査にかかる時間を短縮

CNAPP

Sysdigを導入する前、当社は可視性のギャップを抱えていました。Sysdigを導入したことで、当社はリスクがどこに存在しているかをリアルタイムで把握できるようになりました。

— データ生産性企業の
クラウドセキュリティ部門責任者

CNAPPの導入事例

データ生産性企業、SaaSの配信を保護

課題

この企業は、データパイプラインの構築、デプロイ、スケーリングを行うためのシームレスで統一された環境を提供しています。オンプレミスからSaaS環境へと拡張する時点で、同社は、Sysdigと協力することで、コンテナ化された環境にセキュリティとコンプライアンスを拡張しました。

導入結果

Sysdigを導入することで、同社はセキュリティとコンプライアンスの機能をコンテナ化された環境に持ち込むことが可能となりました。高い透明性を維持しつつ、リアルタイムで脆弱性、脅威、設定ミスを特定し排除できるようになりました、Sysdigが提供する包括的な可視性により、脅威の発見と特定が容易になりました。

80%	脆弱性ノイズを低減
20%	CNAPPへの統合により時間を節約
6分間	このタイムフレームで、統合されたチェックを通じてコードをセキュアにデプロイ可能

ランタイムインサイト

“Sysdigを使用して、すべてのことをランタイムインサイトに基づいて行うことで、より迅速な脅威検知、より適切な脆弱性管理、より優れたコスト最適化、そして最終的にはより優れたセキュリティポスチャーを実現できます。

— 詐欺検知ソフトウェア会社の
ITセキュリティマネージャー

1つのソリューションで完全なセキュリティを実現

互いに通信できないポイントセキュリティソリューションに頼る時代は過去のものとなりました。今日の脅威からクラウドを保護するには、クラウド環境を、あらゆるユースケースにわたってエンドツーエンドで保護するような統合ソリューションを導入する必要があります。つまり、CSPM、CDR、CWPP機能を効果的に処理するCNAPPソリューションが必要なのです。

本書で紹介したお客様事例からも分かるように、Sysdigはまさに CNAPPソリューションの提供者です。Sysdigは、クラウドセキュリティのあらゆるユースケースにおいて1秒単位で保護を行うことで、最も重要な脆弱性、設定ミス、権限、脅威に優先順位を付けるような、完全なCNAPPを実現しています。Sysdigは、かつてないほどに脅威の防御を容易にします。防御できない脅威が発生した場合、Sysdigは、そのような脅威を数秒でシャットダウンします。

より詳しい情報を知りたい方は、Gartner社のマーケットガイドで取り上げられている当社のCNAPPに関する評価をご覧ください。

sysdig

E-BOOK : Sysdig CNAPPの特徴について

EBK-012-JA Rev. A 8/24