

F R O S T & S U L L I V A N

2024 COMPANY OF THE YEAR

グローバルなコンテナ/
Kubernetesセキュリティ
業界部門

F R O S T & S U L L I V A N

BEST
2024 PRACTICES
AWARD

sysdig

ワールドクラスのパフォーマンスを実現するためのベストプラクティス基準

Frost & Sullivan は、最終的に受賞企業を決定する前に、厳格な分析プロセスを適用して、各カテゴリで選ばれた複数のノミネート企業を評価します。このプロセスには、ノミネートされた各企業が、2 つの次元においてベストプラクティスの基準を満たしているかどうかを詳細に評価することが含まれます。Sysdig は、コンテナ/Kubernetes セキュリティ分野における多くの基準で優れています。

賞の選考基準	
先見性のあるイノベーションとパフォーマンス	顧客への影響
潜在ニーズの掘り起こし	価格性能比
メガトレンドによる先見的なシナリオ	顧客の購入体験
ベストプラクティスの実施	顧客の保有体験
リーダーシップフォーカス	顧客のサービス体験
財務実績	ブランド価値

業界が抱える課題

Frost & Sullivan の Cloud User Survey 2023 によると、調査対象となった企業の 31.7%が、クラウドはデジタルトランスフォーメーションの移行プロセスにおいて最も重要な部分であると考えているとのこと。この認識により、今後 12 か月間、これらの企業にとってクラウドが最優先のテクノロジー投資となることが確実視されています。クラウド導入に対する高い信頼性は、業務効率と顧客体験の向上につながり、現代のビジネス環境において持続可能な成長を達成できるという信念に根ざしています。

世界中の企業によるクラウド技術の広範な採用により、バックエンドのインフラストラクチャと顧客向けのフロントエンドアプリケーションの両方の構築、運用、管理方法に大きな変化が生じています。その結果、多くがクラウドネイティブなアプリケーション開発ツールに目を向けています。これには、Infrastructure-as-Code (IaC)、サーバーレスコンピューティング、継続的インテグレーション (CI) / 継続的デプロイメント (CD) プラットフォーム、コンテナなどが含まれます。その一方で、しかし、コンテナや Kubernetes(K8s)を含むクラウドおよびクラウドネイティブなアプリケーション開発ツールの採用が増加するにつれて、特にコンテナや K8s のセキュリティの観点において、組織が対処しなければならない複数のセキュリティ上の課題が生じています。コンテナ化された環境は、コンテナの動的な性質と、分散クラスター間で実行されるマイクロサービスアーキテクチャーが理由で複雑になっています。この結果、セキュリティチームが管理すべき複雑さのレベルが高まっているほか、アタックサーフェスが拡大しています。

脅威の対象領域が広がるにつれ、従来のセキュリティソリューションはもはや効果的ではなくなっています。なぜなら、コンテナ化されたアプリケーションや K8s クラスターを標的とした攻撃を検出および緩和するように設計されていないからです。現在、組織はコンテナおよびコンテナ化された環境独自の特性に合わせた包括的な保護を提供するソリューションを必要としています。これにより、これらの課題に対処するために特別に設計されたコンテナおよび K8s のセキュリティソリューションへの需要が世界的に高まっています。標準コンテナ/K8s セキュリティソリューションは、イメージとレジストリの検査、相互依存関係のチェック、コンプライアンスの検証、異常な動作のリアルタイム監視、不正アクセス防止、実行時の不審な振る舞いの検知と緩和など、さまざまな機能を提供します。

潜在ニーズの掘り起こし

2013 年に設立された Sysdig は、サンフランシスコを拠点とするサイバーセキュリティ企業です。Sysdig は、コンテナ、K8s、クラウド環境のセキュリティと信頼性の確保に貢献できるソリューションを企業や組織に提供しています。同社のソリューションは、Sysdig Secure という名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) です。CNAPP は、ソフトウェアのライフサイクル全体にわたってエンドツーエンドの保護を提供するものです。Sysdig Secure に統合されているコンテナ/K8s セキュリティソリューションには、イメージ、CI/CD パイプライン、レジストリ、そしてホストにおける脆弱性、シークレット、設定ミスなどをスキャンする機能が含まれています。また、Sysdig Secure は、新しい「一般的な脆弱性と暴露を意味する Common Vulnerabilities and Exposures (CVE)」にフラグを立てた上で、実行時のコンテキストを使用してそれらに自動的に優先順位を付けます。さらに、このプラットフォームは、すぐに使えるマネージド型ポリシーを利用して、コンテナや K8 内における悪意あるアクティビティを迅速に検知し対応するほか、Open Policy Agent (OPA) を使用してコンプライアンス制御を実施します。また、個々のオブジェクトに関して、すべての Sysdig セキュリティ関連機能を統合することにより、インシデント対応を容易にします。

コンテナおよび K8s セキュリティソリューションのプロバイダーは、多くの場合、コンテナイメージのスキャン、ネットワークセキュリティ、ランタイム保護のような、特定分野に特化しており、1 つか 2 つの部分的分野に秀でています。一方、Sysdig は、クラウド、コンテナ、K8s 環境のセキュリティと監視を単一のプラットフォームに統合したアプ

メガトレンドによる先見的なシナリオ

「Frost & Sullivan は、Sysdig がビルドからランタイムに至るまで、アプリケーションの開発提供プロセス全体の保護を支援するような、包括的なプラットフォームを提供していることを高く評価しています。Sysdig が提供するコンテナおよび K8s セキュリティソリューションは、顧客に自信を与えるような機能を提供します。これは Sysdig が、顧客のニーズへの対応、そしてコンテナおよびコンテナ化環境の継続的な保護に関して、卓越した熟練度を備えていることを示しています。」

- 研究員、Daphne Dwiputriane 氏

日々の運用に関して顧客に自信を与える機能を提供します。これは、顧客のニーズに対応し、コンテナおよびコンテナ化環境の継続的な保護を確保する上で、Sysdig が卓越した熟練度を備えていることを示しています。

ローチを通じて、競合他社との差別化に成功しています。他のベンダーもプラットフォーム上で同様の機能を提供していますが、Sysdig は、K8s とオープンソースの監視アラートツールとして有名な Prometheus との深い統合により際立っています。この統合を通じて、顧客はインフラ、サービス、アプリケーションをエンタープライズ規模で深い可視性を確保できるようになります。この重要な機能は、コンテナ化された環境全体に包括的な可視性を提供するコンテナと K8s のセキュリティソリューションを求める顧客のニーズを満たすものです。

Frost & Sullivan は、Sysdig がビルドからランタイムに至るまで、アプリケーションの開発からデリバリープロセス全体の保護を支援するような、包括的なプラットフォームを提供していることを高く評価しています。Sysdig が提供するコンテナおよび K8s セキュリティソリューションは、

メガトレンドによる先見的なシナリオ

Frost & Sullivan は、サイバーセキュリティを今後 5 年間で飛躍的に成長するメガトレンドとして位置付けています。企業が情報技術(IT)インフラ、クラウドネイティブアプリケーション、セキュリティ運用に投資する方法を変えると予測しています。コンテナの利用が拡大し続ける中、コンテナ/K8s セキュリティソリューションへの投資も拡大しており、特に包括的なランタイム保護を提供するようなソリューションへの投資が増加すると予想されています。

包括的なランタイム保護機能を備えたコンテナ/K8s セキュリティソリューションに対する需要の高まりは、コンテナおよび K8s の利用により企業や組織が遭遇するアタックサーフェスが広がっていることに起因しています。ランタイム保護機能は、本番環境内でリアルタイムに脅威を検知して軽減することで、セキュリティの追加レイヤーを提供します。ほとんどのベンダーは、ランタイム保護機能を自社のコンテナ/K8s セキュリティソリューションに組み込んでいますが、市場での成功のレベルはさまざまです。一方、Sysdig は、Falco を使用することで他社とは一線を画しています。Sysdig が開発したこのオープンソースのランタイムセキュリティツールは、コンテナやコンテナ化された環境における不審な振る舞いを特定した上で、それに対応します。他のベンダーも堅牢なランタイム保護機能を提供してはいますが、Falco は業界標準のランタイムセキュリティツールであると広くみなされています。これは特に、Falco が 2018 年にインキュベーションプロジェクトとして Cloud Native Computing Foundation (CNCF) に採用された後に顕著となりました。Falco は、CNCF のサンドボックスに受け入れられた最初のランタイムセキュリティプロジェクトとして、オープンソースコミュニティの間でさらなる信頼性と可視性を獲得し、この分野で Sysdig を際立たせることになりました。Falco は、オープンソースツールとして、開発者コミュニティからの継続的な貢献と改善の恩恵を受けているため、最新のセキュリティ課題に対して迅速に適応できます。

Sysdig が開発した革新的な製品は Falco だけではありません。オープンソースプロジェクトとして設立された Sysdig は、Sysdig OSS も作成しています。Sysdig OSS は、デジタルフォレンジックとインシデントレスポンス (DFIR) およびトラブルシューティングのためのクラウドネイティブな標準ツールです。オープンソースプロジェクト開発の経験を活かして、Sysdig は Falco と Sysdig OSS を含むオープンソーススタック上に、CNAPP プラットフォーム内に統合されたコンテナと K8s セキュリティソリューションを構築しました。このアプローチにより、同社のプラットフォームはランタイム脅威の検知と対応のオープンスタンダードとして確立されました。Sysdig は、業界標準のオープンソースプロジェクトを作成し維持することに専念することで、イノベーションへのコミットメントを強調し、顧客基盤の拡大に成功しています。これは、世界的な組織、特に自社環境でオープンソースツールを利用する組織にとって、Sysdig が最善の選択肢となることを可能にしています。

リーダーシップフォーカス

Sysdig は、コンテナおよび K8s セキュリティ業界におけるリーダーシップを確固たるものにするために、さまざまな戦略を採用しています。同社は、コンテナ/K8s セキュリティソリューションに Falco と Sysdig OSS を活用することで、オープンソースのルーツへのコミットメントを表明しています。また、同社は、その他の注目すべきオープンソースツールも積極的に保守しています。例としては、主要なオープンソース監視ソリューションである Prometheus や、エンタープライズレベルの Prometheus 監視のためのオープンソースカタログである Promcast などが挙げられます。さらに、同社は、高く評価されているネットワークプロトコルアナライザーである Wireshark の最も注目すべきサポーターでもあります。オープンソースへのコミットメントを通じて、Sysdig は、そのソリューションの有効性の改善と検証に継続的に貢献する活発で魅力的なコミュニティの育成に成功しています。オープンソースコミュニティに積極的に参加してフィードバックを得ることで、Sysdig は、自らのコンテナ/K8s セキュリティソリューションを強化し、最新のセキュリティ課題に効果的に対処しています。

コンテナセキュリティ分野でのリーダー的地位を維持するために、Sysdig は自らの脅威リサーチチームに多大な投資を行ってきました。こうした継続的な取り組みにより、同社は新たな脅威を特定し、特にクラウドとコンテナ環境を標的とする未知の脆弱性を発見することができました。その結果、Sysdig は検知ルールを確立し、自らの機械学習モデルをアップデートすることに成功しました。これにより、Sysdig の顧客は、新たな脅威から身を守ることが可能となりました。

財務実績

Frost & Sullivan の推計によると、Sysdig は 2023 年に世界のコンテナ/K8s セキュリティ分野で、前年比 50.9%の力強い成長を記録したとのことです。同社は長年にわたり安定した成長を維持しており、世界的なコン

メガトレンドによる先見的なシナリオ

「Sysdig が開発した革新的な製品は Falco だけではなく。オープンソースプロジェクトとして設立された Sysdig は、Sysdig OSS も作成しています。Sysdig OSS は、デジタルフォレンジックとインシデントレスポンス (DFIR) およびトラブルシューティングのためのクラウドネイティブな標準ツールです。オープンソースプロジェクト開発の経験を活かして、Sysdig は Falco と Sysdig OSS を含むオープンソーススタック上に、CNAPP プラットフォーム内に統合されたコンテナと K8s セキュリティソリューションを構築しました。このアプローチにより、同社のプラットフォームはランタイム脅威の検知と対応のオープンスタンダードとして確立されました。」

- 研究員、Daphne Dwiputriane 氏

テナセキュリティ業界におけるリーダー企業の地位を確固たるものにしていきます。さらに、Sysdig のコンテナ/K8s セキュリティソリューションは、さまざまな業界や規模の組織で広く採用されています。これは、Sysdig が、コンテナやコンテナ化された環境で遭遇するセキュリティ上の課題に、多様な分野や企業規模で効果的に対処する汎用性の高いソリューションを提供していることを裏付けています。最近寄せられた顧客からの評価では、技術スタック全体を K8s 上でマイクロサービスとして実行するように移行した結果、Sysdig のソリューションによって運用が大幅に簡素化されたことが強調されていました。さらに、Sysdig のコンテナ/K8s セキュリティソリューションを導入することで、この顧客は現在、一元化されたダッシュボードを利用できるようになっています。このダッシュボードを使うことで、同顧客は、自社環境内のアクティビティに対する理解を高め、本番稼働前にセキュリティ問題に対処するための迅速なインサイトを確保できます。

購入とサービスに関する顧客エクスペリエンス

Sysdig はシンプルで透明性の高い価格モデルを提供しています。コンテナと K8s のワークロードについては、同社はエージェントに基づいて価格を計算しています。このようなシンプルな価格設定モデルにより、顧客は価格設定の詳細を迅速に理解できるようになるほか、潜在的なコストをより迅速かつ効果的に見積もることが可能となります。これとは対照的に、他の多くのコンテナセキュリティベンダーは、コンテナ/K8s セキュリティソリューションに関して、比較的複雑な価格設定モデルを採用しています。これでは、価格構造を理解することが難しくなるため、潜在的な顧客の意欲を削いでしまう可能性があります。さらに Sysdig は、アマゾン ウェブ サービス (AWS) 、Google Cloud Platform (GCP) 、Azure などのクラウドマーケットプレイスや、ライセンスモデルを持つチャネルパートナーを通じてソリューションを提供しており、顧客の購入プロセスを合理化しています。

さらに、Sysdig は、顧客の要件や購入基準に照らして製品を評価し、投資価値の最大化を支援するような、体系的かつ統合的な価値実証（PoV）プロセスを提供しています。Sysdig は、カスタマーサクセスマネージャーとテクニカルアカウントマネージャーを通じて、顧客向けのトレーニングやイネーブルメントを提供することで、購入後のサポートを拡大し、Sysdig のソリューションの効果的な活用を保証しています。このアプローチにより、Sysdig は顧客満足度の高いレベルを維持しています。その好例として、同社のトップ 60 社は、平均して年間 100 万ドル以上の継続的な収益を同社に投資しています。

結論

クラウドネイティブアプリケーション開発ツールの導入が進む中、コンテナセキュリティソリューションの需要は飛躍的に拡大すると予想されています。企業や組織は、コンテナとコンテナ化された環境を継続的に保護する必要性を認識しています。Sysdig は、世界のコンテナ/K8s セキュリティ業界のパイオニアであり、かつリーダーでもあります。包括的なクラウドセキュリティプラットフォームである Sysdig Secure に統合されている同社のコンテナ/K8s セキュリティソリューションは、ビルドからランタイムに至るまで広範な保護と可視性を提供し、企業や組織がセキュリティ上の課題に対処できるよう支援します。Sysdig のソリューションは、業界をリードするランタイムセキュリティツールである Falco を搭載しています。コンテナ/K8s セキュリティ市場でランタイム保護機能の強化がますます重視される中、Sysdig のソリューションは独自のバリュープロポジションを提供するものとなっています。

その優れた総合的なパフォーマンスにより、Frost & Sullivan が主催する『2024 Company of the Year Award : グローバルなコンテナ/K8s セキュリティ業界部門』を受賞しました。

Company of the Year Award について

Frost & Sullivan が主催する『Company of the Year Award』は、当社が提供する最高の栄誉であり、ビジョナリーイノベーション、市場をリードするパフォーマンス、そして比類のない顧客ケアの模範となる市場参加者を表彰するものです。

ベストプラクティス基準の分析

『Company of the Year Award』において、Frost & Sullivan の複数のアナリストたちは、下記に挙げる基準を独立して評価しました。

ビジョナリーイノベーションとパフォーマンス

潜在ニーズの掘り起こし：顧客が気づいていない潜在ニーズや十分に提供されていないニーズを発掘し、強固なソリューション開発プロセスを通じてそれに対応していること。

メガトレンドを通じたビジョナリーシナリオ：長期的なマクロレベルのシナリオを、メガトレンドの利用を通じてイノベーション戦略に組み込むことで、市場初のソリューションと新たな成長機会を可能にしていること。

リーダーシップフォーカス：コア市場において主導的地位を築くこと、そして新規競合他社に厳しい参入障壁を設けることに注力していること。

ベストプラクティスの実施：クラス最高の実装は、一貫した再現可能なレベルの成功を生み出すプロセス、ツール、または活動によって特徴付けられます。

財務業績：収益、収益成長率、営業利益率、その他の主要な財務指標において、力強い全体的な業績を達成していること。

顧客への影響

価格/パフォーマンスバリュー：製品またはサービスが、市場で提供される同様の製品と比較して、価格に対して最高の価値を提供していること。

購買に関する顧客エクスペリエンス：購入エクスペリエンスの質が、顧客が独自のニーズや制約に対応する最適なソリューションを購入していることを保証するものであること。

所有に関する顧客エクスペリエンス：顧客が、その企業の製品やサービスを自分のものとして誇りに思い、製品やサービスの寿命を通じてポジティブな経験をしていること。

サービスに関する顧客エクスペリエンス：カスタマーサービスが、アクセスしやすく、迅速でストレスがなく、かつ高品質であること。

ブランドエクイティ：顧客が当該ブランドを肯定的に受け止め、高いブランドロイヤルティを示していること。

