

Cloud Workload Security

クラウドVMとコンテナ向けEPP+EDR

パブリッククラウド、プライベートクラウド、サーバー、コンテナを問わず、どのような稼働環境でも、俊敏性を維持しながらクラウドのワークロードを保護する手段を、あらゆる規模の企業が模索しています。

数百とはいわないまでも、数十ものアカウントが複数のクラウドに分散しており、開発者はコンテナ化されたマイクロサービスを毎日、あるいは毎時更新しています。また、多数のVMが稼働しており、マルチクラウドのフットプリントは常に変化しています。そのため、クラウドインフラストラクチャを利用する場合、セキュリティが最大の関心事になりやすいのは当然のことです。迅速かつ広範にわたりもたらされる変化にはメリットだけでなくデメリットも伴いますが、SentinelOneならお客様をサポートできます。

SentinelOne Cloud Workload Securityは、分散型の自律的なエンドポイント保護、脅威検知、インシデント対応を、パブリッククラウド、プライベートクラウド、オンプレミスのデータセンターで稼働するコンピューティングワークロードまで拡張します。SentinelOneを使えば、セキュリティチームは、LinuxやWindowsサーバー、Dockerコンテナ、Kubernetesクラスタをすべて、Singularity™プラットフォームから管理できます。4,000社以上のお客様が、このマルチクラウド、マルチテナント対応のプラットフォームをユーザーエンドポイントの管理に役立てています。

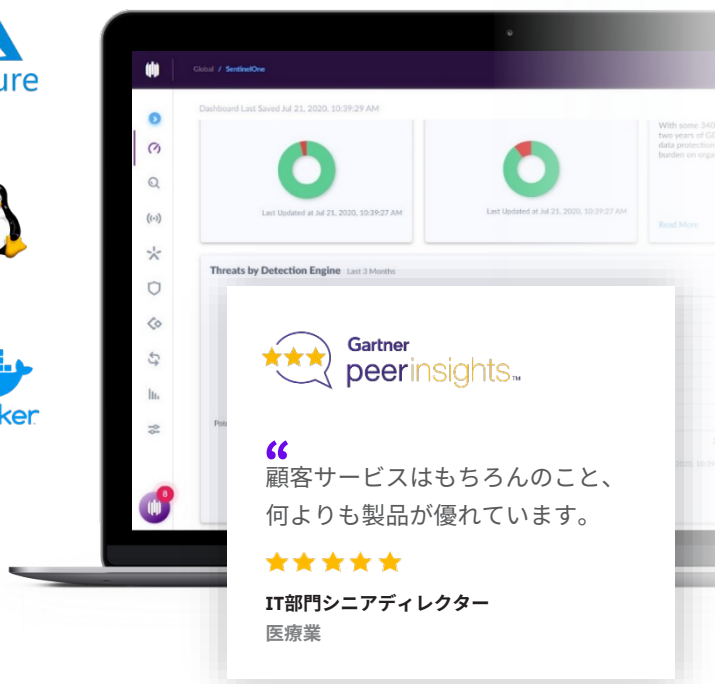
ハイブリッドクラウド環境は複雑です。だからといって、クラウドワークロードの保護まで複雑であってはいけません。

自律型のCWS

クラウドVMとコンテナ向け
EPP+EDR

主な特長

- + Cloud VMセキュリティ (Linux、Windows)
- + EKS、AKS、GKE、自己管理型 Kubernetes向けのランタイム コンテナセキュリティ
- + コンテナ用アプリケーション コントロール (Kubernetes、Linux)
- + VM用アプリケーション コントロール (近日提供予定)
- + 1台のコンソールでマルチクラウド/マルチテナントに対応



利点

- + マルチクラウドの可視化
- + クラウドVMでの自律型リアルタイムEPP+EDR
- + ランタイム保護 (DockerとKubernetes向け)
- + MTTRの削減
- + 迅速なインシデント対応
- + アラートの削減

主な機能

- ✓ 複雑な脅威をVMやKubernetesのPodレベルで**自律的かつリアルタイム**に検知および修復します。人による介入は必要ありません。
- ✓ コンテナ化されたワークロードの**ランタイム保護**により、マルウェアやクリプトジャッキングなどの不正なプロセスを識別して強制終了します。また、コンテキストに即したEDRテレメトリには、クラスタ、ノード、Pod、イメージ名、コンテナIDなど、主要なコンテナの詳細情報が含まれます。
- ✓ **エンタープライズクラスのEPP+EDR**を導入すれば、マルウェアを阻止し、インシデント対応を迅速化し、脅威ハンティングを変革できることが、世界中の何千ものお客様によって実証されています。
- ✓ リモートシェルを全面的に使用して、VMやKubernetesのPodに関する**詳細なフォレンジック**を実施できます。
- ✓ **リソース効率の高いKubernetesエージェント**をワーカーノードごとに1つずつ配置し、インストールメンテションを追加せずにノード内にあるすべてのPodのランタイムを保護します。
- ✓ MITRE ATT&CKのテクニックに対応するストーリーにイベントを自動的に相関付けて、**インシデント対応 (IR) を迅速化**します。
- ✓ **マルチクラウド、マルチテナント**対応のSentinelOneコンソールを使用すると、ハイブリッドクラウドとマルチクラウドの管理を効率化できます。
- ✓ **修復とロールバックをワンクリックで実行できるため**、インシデント対応が簡素化され、平均修復時間 (MTTR) を大幅に短縮できます。



“今すぐSentinelOneを導入しなければ、遅れを取り戻すのに1年かかるでしょう。”



クラウドDevOps I&O部門
その他の業界、10億~30億米ドル



“使いやすく効果的なEPPとEDRが1つになったソリューションです。”



セキュリティアナリスト
製造業、30億~100億米ドル

信頼性と評価の高い革新的なソリューション



2021年のエンドポイント保護プラットフォーム分野のマジックアドラントのリーダーに選出

クリティカルケイバビリティレポートのユースケースすべてにおいて最高ランクを獲得



過去最高のATT&CK評価

- 検知漏れがゼロであり、100%の可視性を提供
- 2年連続で最も完全なアナリティック検知を実現
- 遅延がなく、構成の変更が不要



Gartner Peer Insights™の

98%が高評価

「お客様の声」の多くがSentinelOneを推奨



SentinelOneについて

より多くの機能を、よりシンプルに。SentinelOneは、エンタープライズレベルの機能を損なうことなくセキュリティスタックを簡素化するために、自律的な分散型エンドポイントインテリジェンスを活用してサイバーセキュリティの未来を開拓しています。SentinelOneの技術は、脅威への対応を自動化してスムーズに行えるようにすることで、セキュリティ担当者の生産性が向上するよう設計されています。ぜひ、SentinelOneのソリューションをお試しください。

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733