Insert Partner Logo
Size to be visually equal to F5 Logo.
Align to left edge and center vertically.

クラウドネイティブアプリケーションのための包括的なセキュリティ

すべてのクラウドワークロードで脆弱性と脅威を検出し阻止する

最新のアプリケーションを実行することで、価値実現までの時間の短縮、ビジネスの俊敏性の向上、業務効率の改善など、大きなメリットを得ることができます。ただし、このメリットの可能性を実現するには、クラウドで動作するように構築されたアプリと API に特定のセキュリティ要件に対処する必要があります。

クラウドネイティブアプリケーションへの移行は、セキュリティチームが考慮しなければならない脅威の対象領域が拡大することを意味します。これは、アプリそのものと、アプリが実行されるクラウドネイティブインフラストラクチャの両方が脆弱になる可能性があるからです。実際には、クラウドネイティブアプリと API の安全性は、それらが実行されるインフラストラクチャと同程度でしかありません。

以前は Threat Stack と呼ばれていた F5 ® Distributed Cloud App Infrastructure Protection（AIP）は、高度な Web アプリケーションおよび API Protection（WAAP）をアプリケーションインフラストラクチャ保護と組み合わせることで、増え続ける脅威の対象領域を制し、最新のアプリケーションを保護します。F5 の Distributed Cloud AIP は、最新の環境全体を包括的に保護します。

「デジタルトランスフォーメーションの加速に照準を当てている組織の77%が、アプリケーションの最新化に投資しており、これは前年比で133%の増加となっています」

F5アプリケーション戦略状況のレポート

アプリケーションはあらゆる面で脆弱

クラウドネイティブアプリは、コンテナ内のマイクロサービスとして提供され、継続的開発 / 継続的統合（CD/CI）パイプラインを通じて新機能を迅速に提供したり、仮想化されたコンピューティングおよびストレージの環境で実行したりできます。このようなアプリは運用効率を向上させますが、攻撃の脅威対象領域が拡大するため、脅威の調査や修復に多くの労力が必要となります。

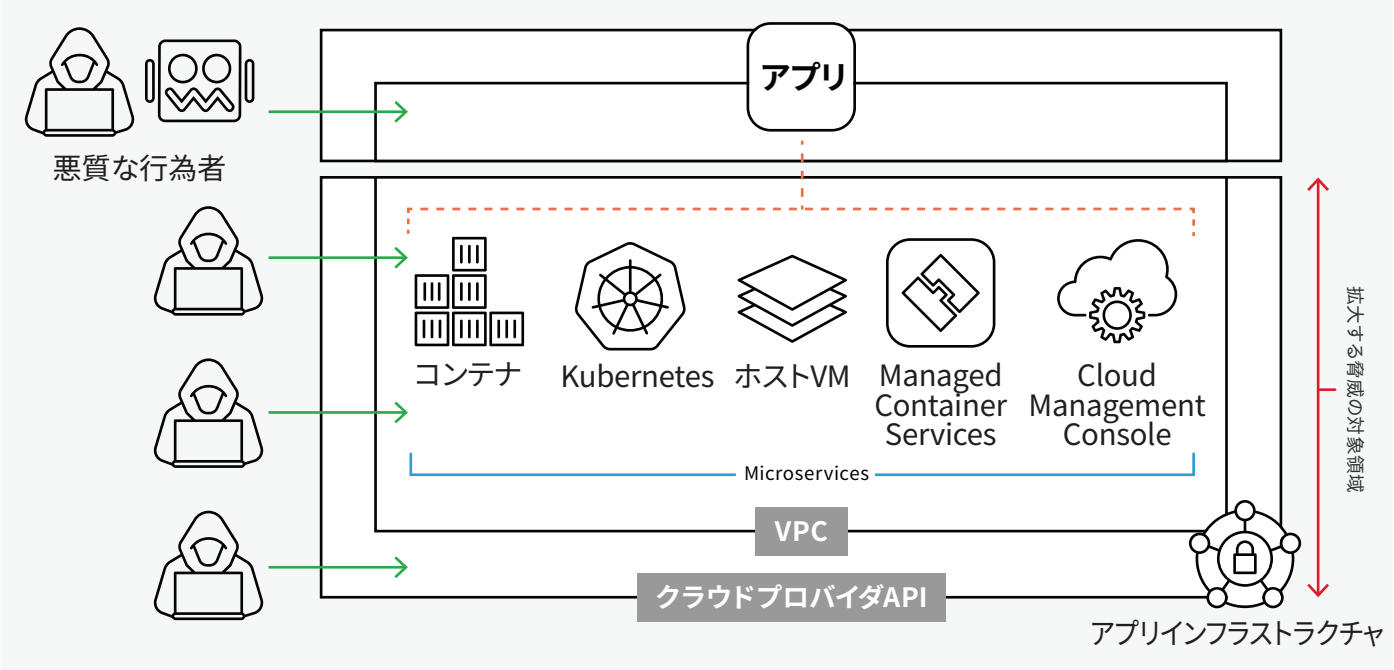
アプリ /API + インフラストラクチャ保護

アプリ /API

アプリケーションと API は、コード、ソフトウェア、またはビジネスロジックの脆弱性を悪用するレイヤー 7 攻撃、ゼロデイ攻撃、および OWASP Top 10 の影響を受けやすいとされています。

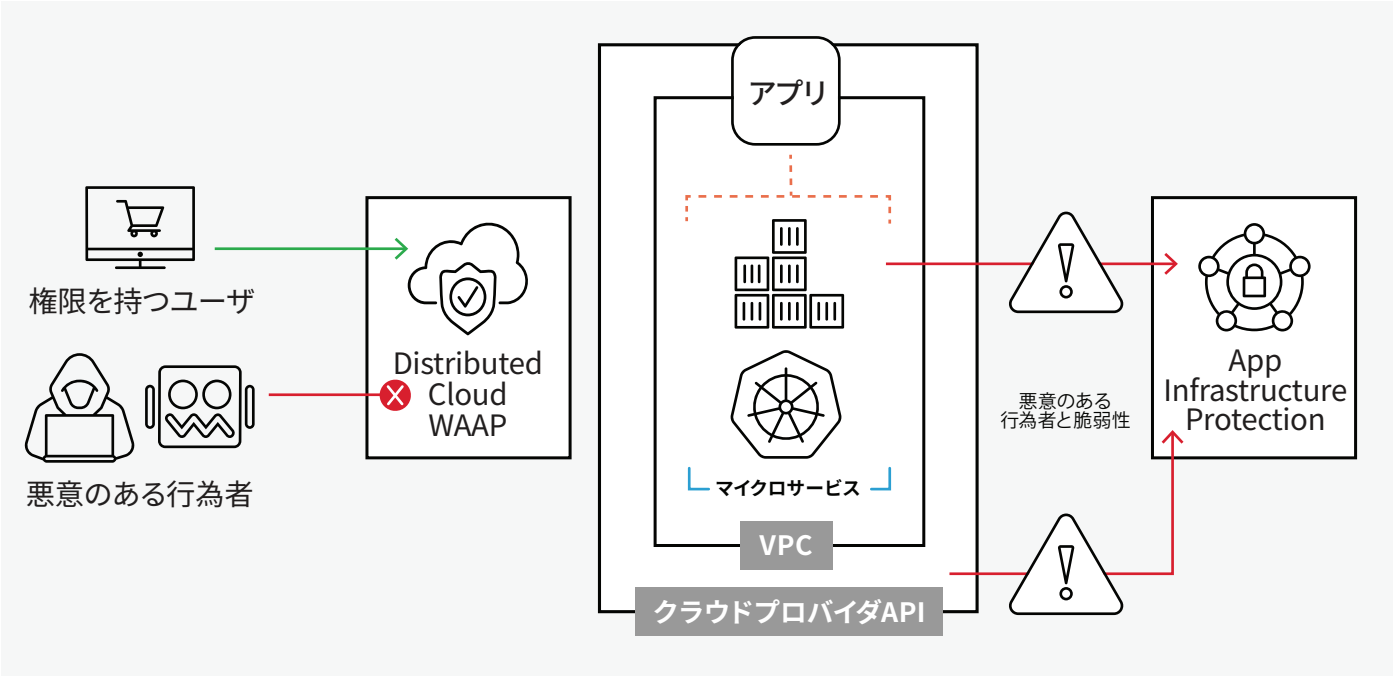
クラウドネイティブインフラストラクチャ

Kubernetes を含むコンテナ、オーケストレーションツール、仮想マシン、クラウドプロバイダの API などのクラウドインフラストラクチャは、設定が誤っていると、不正行為者によるデータの流出、コンテナログイン、暗号化、クレデンシャルの盗難に対して脆弱になる可能性があります。



Distributed Cloud App Infrastructure Protection によるアプリとインフラストラクチャの両方のセキュリティ

最新のアプリケーションを保護するには、実行時のアプリケーションからサポートするクラウドインフラストラクチャまで、クラウド環境のすべての対象領域を保護する包括的なセキュリティの状態を把握する必要があります。Distributed Cloud AIP は、環境に対する脅威の共通認識をご提供いたします。



F5 Distributed Cloud Web App および API Protection（WAAP）

- 堅牢かつ効果的なアプリケーションと API の保護を広範囲に実現します
- Web Application Firewall（WAF）、API Protection、Bot Defense、DDoS Protection から構成されます

Distributed Cloud AIP

- すべてのクラウドワークロード全体で、ルールと ML ベースの異常検出を組み合わせた高効率の脅威検出を実現します
- 内部の脅威、外部の脅威、データ損失のリスクを特定して警告します

顧客からコードに至るまでの包括的なセキュリティ

F5 Distributed Cloud WAAP と AIP をセキュリティ戦略の一部として一緒に活用することで、さらに次のような利点があります。

- 効率の高い検出：F5 Distributed Cloud WAAP と組み合わせ、コンテキストとワークフローを使用して、毎日収集される数十億のデータポイントから脅威をリアルタイムで検出し、迅速な修復を実現します。
- 迅速な導入：一時的環境向けに設計されており、アプリケーションの配信やイノベーションのペースを妨げることなく、テレメトリ収集を自動化します。
- 可視性の向上：オンプレミス、ハイブリッド、パブリッククラウドプロバイダーなど、導入場所にかかわらず、クラウドワークロードからテレメトリ収集と分析を行う。脅威検出のための統一見解を提供いたします。
- 改善の統合：Distributed Cloud AIP は、お客様の SIEM または SOAR プラットフォームとの堅牢な統合を提供し、修復作業をサポートいたします。

F5 Distributed Cloud WAAP と AIP の組み合わせが優れている理由

F5 は、お客様がクラウド導入のどの段階にある場合でも、クラウドワークロードを安全に保つための経験と実績のある専門知識を有しています。

Threat Stack は F5 ソリューションの一つになりました

現在、Threat Stack は F5 Distributed Cloud App Infrastructure Protection（AIP）と名称変更いたしました。このソリューション、F5 のセキュリティオペレーションセンター（Distributed Cloud AIP Managed Security Services と Distributed Cloud AIP Insights を含む）などの詳細については、クラウドセキュリティやコンプライアンスの専門家にお問い合わせください。

F5 のセキュリティ専門家がお客様のクラウドセキュリティに関する懸念を解消いたします。そのため、お客様は安心して業務に専念いただけます。詳細またはデモのご予約については、F5 の Web サイトでご確認ください。

DC 12.2022 | JOB-CODE-DS-950864156-AIP-Insights