

OpenText Secure Cloud のガイド

成長に対応できるように構築されたプラットフォームを MSP ビジネスに統合する



MSP をよりスマートに管理する方法を見つける

アプリのスプロール化、レガシーシステム、広がる人材不足により、多くのクライアントがマネージドサービスプロバイダー (MSP) を利用しています。これは一見良いことのように思えるかもしれませんが、軽視できない問題が1つだけあります。MSP は、新規の事業すべてを処理できるだけの規模にすぐには拡張できないのです。

収益力の高い取引を断らなければならなかったことがある人は、それがどのようなものか分かるでしょう。有望なクライアントを失うことは、会社の将来に対する投資の損失を意味します。ビジネスの拡大は依然として最重要課題ではあるものの、現実には、多くのMSPがアプリやサービスを効果的な戦略に導く能力を十分に備えていません。

91%

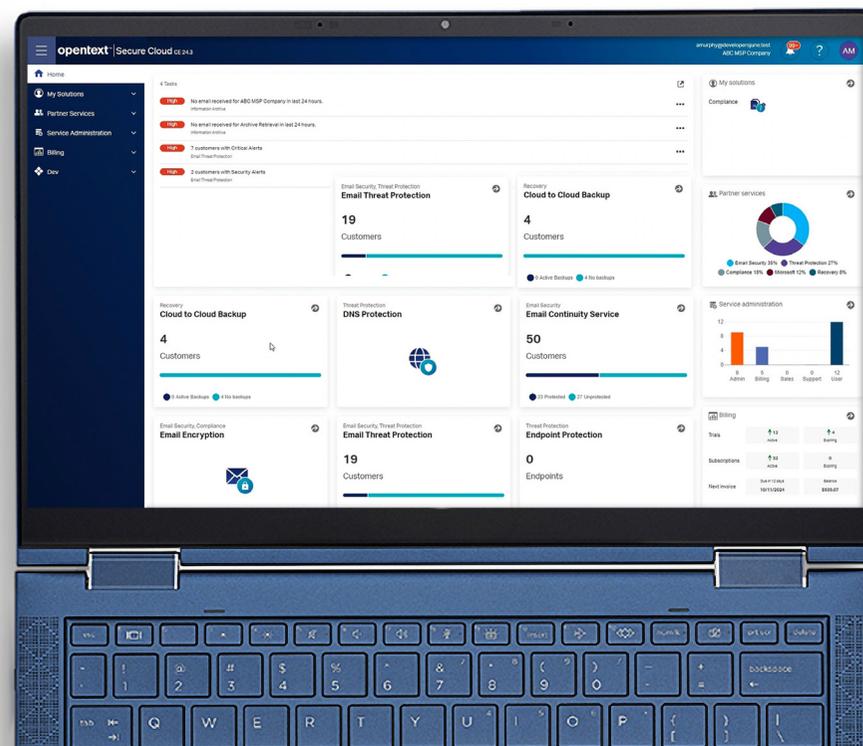
自社のソフトウェアを十分に活用できないことを最大の課題に挙げたMSPの割合。¹

Kaseya が調査した MSP の幹部と技術者のうち 91% が、自社のソフトウェアを十分に活用できないことを最大の課題に挙げ、その後に、アプリ間の切り替え時間と不十分な統合が続きました¹。ビジネスの成長に合わせて拡張できるクライアント管理は、成功に不可欠です。

¹ Kaseya, 『2024 MSP Benchmark Survey Report』, <https://www.kaseya.com/resource/2024-msp-benchmark-survey-report/>

受け入れ可能なクライアントの数は、リソースに応じて、かつ、管理が複雑になりすぎて最終損益に影響を及ぼさない範囲に限られます。クライアントは、そもそも貴社を選んだ理由であり、関係を継続している理由でもある、スムーズな運用と高いサービス水準を常に期待しています。

スタートアップから合併、買収に至るまで、マネージドサービス市場はますます競争が激しくなっています。新しいサービスプロバイダーが次々と登場し、その提供範囲が拡大するにつれて、かつてビジネスパートナーだったベンダーの製品チームと競合する可能性も高くなります。



クライアントを増やし、管理を減らす

スタックが負担になっていると感じるなら、それは一刻を争う事態です。サイバーセキュリティ管理を拡張し、効率を上げ、重要なワークフローを簡素化する次世代のクラウドプラットフォームで、より多くのクライアントを獲得し、その成長を維持しましょう。OpenText™ Secure Cloud なら、スマートかつ簡単に複雑さを制御しながらビジネスを構築できます。

当社の統合型の成長基盤は、MSP とそのクライアントに合わせてカスタマイズされているため、プロビジョニング、管理、レポート、サブスクリプション、ライセンス付与などのあらゆる場面で、Secure Cloud はサポートが可能です。これは、クライアントが必要とするすべてのサイバーセキュリティツールを提供するミッションコントロールセンターのように機能し、完全なデータ可視性とレポート機能、統合型タスク管理、ライセンス管理、コンプライアンス管理の 4 つの機能を備えたポータルとなっています。

千社でも十万社でも、SMB クライアントに対応できるソリューションからなる包括的なポートフォリオにより、実証可能な価値を備えた総合的なセキュリティ機能と管理機能の利点を得ることができます。



負担を減らす

新しいワークフローを備え、スピードと効率のために最適化された使いやすいインターフェイスで、顧客管理に費やす時間を短縮。

運用を向上

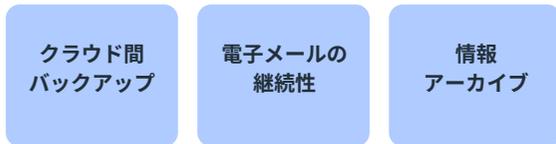
より強力な分析と実用的なインサイトを提供するだけでなく、サブスクリプション、請求書作成、請求が統合された新しいワークフローも備えた単一のコンソールからよりスマートに作業し、スピードと効率を最適化。

品質を高める

カスタマイズに対するクライアントの要求が増加した場合、品質を損なうことなくビジネスを拡大し、スケーラビリティと柔軟性を実現。

opentext™ Secure Cloud

リカバリとコンプライアンス



脅威からの保護と電子メールセキュリティ



脅威ハンティングと修正



統合コンソール

効率化されたプロビジョニング

一元化されたサポート

脅威インテリジェンス

- ✓ **リカバリとコンプライアンス**
クラウド間のバックアップ、メールの継続性、情報アーカイブにより、データのリカバリとコンプライアンスを実現。

- ✓ **ベンダーと請求管理**
請求書作成、製品バンドル、サブスクリプション管理、および一元化された月次請求の統合により、複雑さを軽減。

- ✓ **サポートとオンボーディングの強化**
24時間 365日対応の専門家によるサポートと、トレーニング、市場投入 (GTM) 戦略、共同販売に関して豊富な知識を持つチャネルマネージャーを活用可能。

- ✓ **統合型ダッシュボード**
データの全体像を把握できる一元管理されたインターフェイスから、顧客、製品、セキュリティツールを管理。

- ✓ **API と PSA の統合**
Kaseya、Autotask、ConnectWise、HaloSPA などのプラットフォームに接続。

- ✓ **AI アシスト型の脅威インテリジェンス**
リアルタイム分析と、エンドポイント、ドメインネームシステム (DNS)、電子メールの脅威防御により、サイバー脅威を検知。

- ✓ **マルチテナントプラットフォーム**
顧客のデータを保護し、顧客のニーズや業界固有のコンプライアンスに応じて各クライアントのポリシーをカスタマイズ。

- ✓ **レポートिंगと分析**
レポートिंगとパフォーマンスに関するインサイトを提供し、ビジネスクリティカルなクライアントデータへのアクセスを容易にして、意思決定を向上。

ビジネスを成長させるビジネスに戻る

運が良ければ、クライアントはレガシーシステムを廃止しつつあるか、少なくともその方向に進めようとしているかもしれません。ただし、マイナス面もあります。こうした移行は、古いアーキテクチャを最新のツールに置き換えようと慌てる中で、アプリのクラスターにすり替わってしまう傾向があります。

組み込みの Platform Security Architecture (PSA) やその他の統合機能を備えた Secure Cloud は、データを一元化して集中管理することで統合されたプロビジョニング、導入、レポート、請求を可能にし、各クライアントの環境を迅速に把握できるようにします。

MSP の達成目標	課題	ソリューション
ツールセットの統合	ツールセットが増えるごとに、トレーニング、専門知識、管理するための時間が必要になり、その負担は新規顧客の獲得に応じてさらに大きくなる。	サポートとタスク管理の一元化により、チームは複数のツールについて学ぶことなく、クライアントを効率的に管理可能。
運用効率	プロビジョニング、導入、レポート、および顧客管理のプロセスが手動であるために、複数の環境を迅速かつ大規模に管理することが困難。	ワークフローの自動化により運用オーバーヘッドが削減されるため、チームは安心して多様な顧客環境に対応可能。
よりスムーズな拡張	ほとんど二次的な問題だが、おそらく最も重要な課題。他の課題の中でも、リソースを過剰に拡張せずに成長することはほぼ不可能。	Secure Cloud を使用して管理と請求を統合することで、社内チームに負担をかけずにビジネスを簡単に拡張可能。

管理をシンプルにすれば、成長も容易になる

新規クライアントと幸先の良いスタートを切るには、その環境を詳細に把握する必要があります。しかしご存知の通り、セットアップと設定には時間がかかります。すぐに対策を講じたいクライアントにとって、完全に機能するセキュリティを数週間あるいは数か月も待つことはできません。当社のプラットフォームなら、異なるシステムから取り込んだデータを簡単に整理できるため、よりすばやく移行できます。

OpenText Secure Cloud は、MSP に合わせられるように構築されているため、必要のない複雑なソリューションに縛られる心配をする必要はありません。製品とサービスのエコシステムから選択して、簡単に導入できます。当社が裏側の複雑さを管理し、成長のための時間を生み出します。



コストの削減と利益率の向上

請求の統合とタスクの自動化により運用コストが削減され、セキュリティソリューションのパッケージ化でクライアントにさらに多くの価値を提供。



顧客との関係の維持

イベントカレンダーや更新アラートなどの統合された顧客管理ツールにより、MSP は顧客のニーズを把握することが可能。



顧客ベースの拡大

製品のおすすめ機能を使ってクロスセルとアップセルの機会を提供。



規制コンプライアンスの維持

セキュリティスタックに適合するシンプルなライセンス体系、管理、統合により、安全性とコンプライアンスを維持。



MDR で脅威に対抗

自動化、24 時間 365 日の検知機能、対応、リカバリ、EDR、SIEM、SOAR、および SOC 専門チームによる可視化を実現²。



価値のある AI インサイトへのアクセス

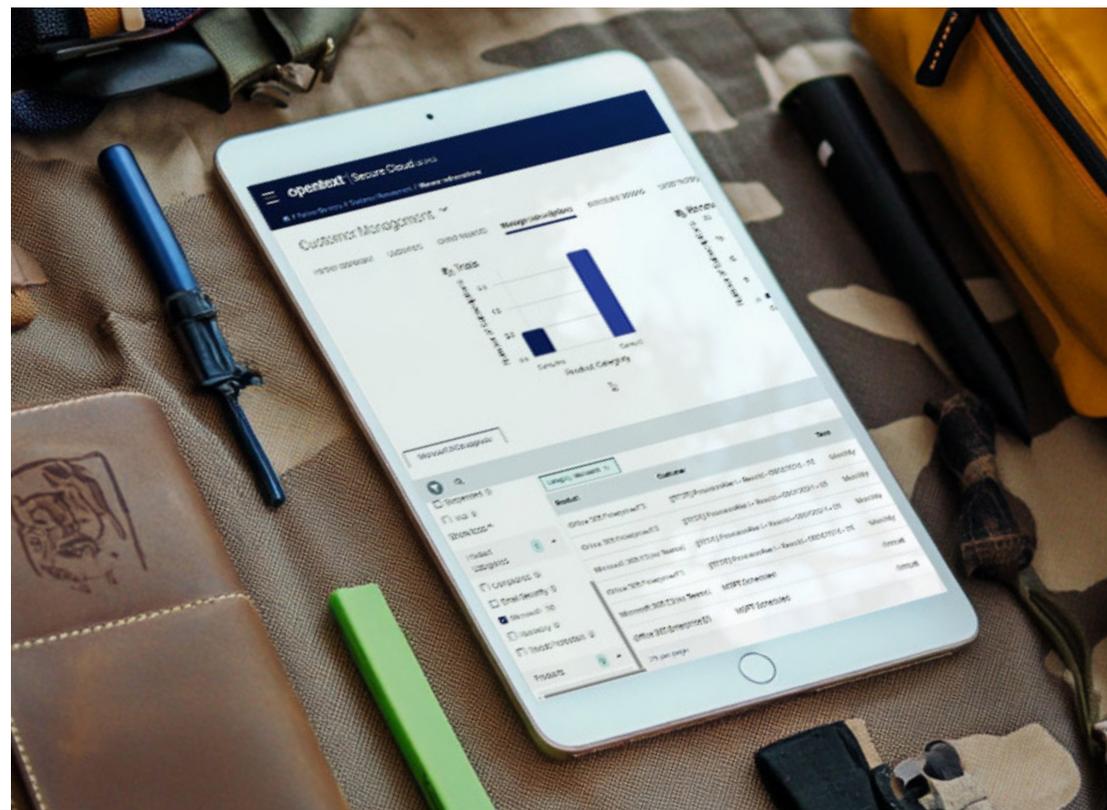
脅威同士の関係性を捉え、環境を守るためのサポートとなる重要なデータとインサイトを提供。

² エンドポイントでの検知および対応 (EDR)、セキュリティ情報およびイベント管理 (SIEM)、セキュリティのオーケストレーション、自動化、対応 (SOAR)、セキュリティオペレーションセンター (SOC)

品質を維持しつつ規模を拡大する

セキュリティ機能とフレームワークはベンダー間で共通であるため、最終的な判断は、貴社とクライアントのニーズが適合するかどうかになります。選択肢を検討する際には、柔軟性を重視しましょう。貴社組織がスタック以上に成長したときに、1年か2年でスタックを再度構築し直すことはだけは避けたいところです。

当社の幅広いサイバーセキュリティツールは、貴社ビジネスの重要な差別化要因となり、飽和した業界で一目置かれる存在となるのに役立ちます。他のベンダーの強みと当社の能力の比較をご覧ください。



ネットワークモニタリング

ネットワーク監視以上の機能を備えた統合インターフェイスを使用し、一連のサイバーセキュリティソリューションを管理。

クラウド中心の MDR

顧客管理、ベンダー管理、サイバーセキュリティ監視のための包括的なツールにアクセス。

インシデント対応

高度な自動化と、マルチソースのAI 駆動型インテリジェンスにより、サイバー脅威に事前に対処。

自動検知

統合型のエクスペリエンスを通じ、分析、ベンダー管理、顧客管理を一元化して集中管理。

安全な基盤を構築

MSP ビジネスを次のレベルに成長させる準備はいいですか？ IT 運用に革命をもたらす強力で全てを備えた当社のソリューションは、単なるサイバーセキュリティスイートではありません。SMB に合わせてカスタマイズされた基盤です。

OpenText Secure Cloud は、業界をリードする脅威インテリジェンス、自動化、および多様な製品セットを通じて、今日、明日、そして将来何が起ころうとも、組織が資産を守るようサポートします。ビジネスレジリエンスに向けて、一緒に次の一歩を踏み出しましょう。

