ホワイトペーパー

MSP 向け Microsoft 365 成熟度モデル

ベースラインの設定、ギャップの解消、サービスのカスタマイズ

Microsoft 365 は、マネージドサービスプロバイダー（MSP）にとって難題であり続けています。サービスプロバイダーは、圧倒的な人気を誇るこのプラットフォームをサポートするために常に俊敏に対応しなければならず、収益を確保し、顧客を維持するのが困難です。しかしながら、Microsoft 365 を管理する新たなモデルが登場しつつあります。

2011 年に Office 365 として導入されて以来、現在 Microsoft 365 として知られるこのプラットフォームは爆発的な人気を博し、2024 年には有料ビジネスシートが 4 億に達しています。あらゆる規模の企業でこのプラットフォームの利用が拡大するにつれて、MSP は持続可能で収益性が高く、安全で効率的な方法で顧客にこのサービスを提供することに苦心してきました。

このホワイトペーパーでは、ツールの乱立、専門家を雇用する難しさ、Microsoft 365 におけるバックアップの不備、価格と利益の予測の問題など、MSP が Microsoft 365 向けのセキュリティサービスを提供する際に直面する課題について解説します。さらに、MSP がこれらの課題を克服し、財務上および運用上の障壁なしに包括的な Microsoft 365 保護を提供できるようにするための成熟度モデルを提示します。

Microsoft 365 サービスの提供と管理における課題

Microsoft 365 が、MSP にとってこれほどの難題をもたらす主な理由は、いくつかあります。おそらく最も困難な問題は、この業界を長い間悩ませてきた人材の確保でしょう。

ほとんどの MSP は、顧客ごと、またテナントごとに Microsoft 365 インスタンスを管理しなければなりません。そうすると、1 人の技術者を複数の顧客に割り当てることになります。その結果、サービスプロバイダーは、顧客基盤が拡大するにつれて、より多くの専門家を雇用する必要に迫られます。技術専門家を探すのが難しい時代において、この問題はさらに深刻化しています。

MSP が技術者を採用しようとする場合、いくつかの問題に遭遇します。ネットで検索してみると、そのひとつが分かります。サービスプロバイダーの技術者は、プレッシャーの大きい業務として認識されているのです。技術専門家に対する需要は常に高いため、望みの場所で待遇の良い職務に就くことができます。また、MSP で働くことの厳しさゆえに、一般企業での仕事の方が給与面で有利に感じられるため、MSP を敬遠するケースも増えています。

特に小規模 MSP にとって、人材確保が最大の問題となっています。また、従業員の採用や維持が困難な MSP にとって、顧客に Microsoft 365 サービスを提供することは困難です。このプラットフォームでは、MSP のスタッフが常時対応し続けなければならず、少人数のスタッフで効果的に管理するのは難しいでしょう。

また、技術者が他の MSP に転職する際に、自分の専門性や嗜好に応じて、Microsoft 365 を管理するために異なるサードパーティ製管理ツールを持ち込む可能性があります。こうした状況において、MSPは、技術専門家が組織内で入れ替わる中で、管理しきれないアプリケーションを抱えることになります。

Microsoft 365 は多層防御を提供できない

もし Microsoft 365 が万全なデータセキュリティとバックアップを提供するならば、MSP はMicrosoft 365 を設定した後は、何もせずに他の業務に移ることができます。さらに多くの顧客を獲得し、収益も上げることができるでしょうが残念ながら、Microsoft 365 の責任共有モデルは、データ保護に関して多くの不備を抱えています。

Microsoft は、Microsoft 365 プラットフォームを稼動させ続けることに責任をもちますが、セキュリティに関しては、限定的な Eメールセキュリティなど基本的な機能を提供するにとどまっています。Microsoft 自身は、これらの機能の多くをサードパーティに依存していますが、それらは顧客が通常必要とする機能に比べるとかなり見劣りします。たとえば、Microsoft 365 に内蔵されている Eメールセキュリティでは、頻度を増し深刻化するサイバー攻撃から MSP が顧客を適切に保護するために必要な追加のセキュリティレイヤーを提供できません。

今や多層防御は、サイバーセキュリティの世界で広く受け入れられている概念です。どのようなシステムであれ、複数のデータ保護レイヤーを持つことが重要ですが、Microsoft 365 は単一のソリューションであるため、複数レイヤーを提供することはできません。その結果、ほとんどすべての企業は、Microsoft の技術の運用によるリスクから逃れることができないのです。

Microsoft は顧客データのバックアップに責任を負わない

Microsoft は、世界で最も攻撃を被っている企業のひとつであり、その顧客は、毎日 6 億件という驚異的な数のサイバー攻撃に直面しています。そして、そのペースは衰えていません。2023 年半ばから 2024 年半ばにかけて、Microsoft は同社の顧客を狙ったランサムウェア攻撃が 275% 増加したことを確認しています。

しかし、Microsoft 365 のデータ保護における最大の欠陥は、同社が率直に認めているものです。同社のサービス契約書には、最新バージョンの Microsoft 365 でも、完全なデータ保護は提供されないと記述されています。

「Microsoft は、本サービスの稼動状態を維持するよう取り組んでいますが、すべてのオンラインサービスには中断および停止が時折発生します。結果としてお客様に生じることがある中断または損失について一切責任を負いません。停止が発生した場合、お客様は、保存しているお客様のコンテンツまたは本データの取得ができなくなることがあります。本サービスに保存しているお客様のコンテンツおよび本データは、定期的にバックアップするか、第三者のアプリおよびサービスを使用して保存することをお勧めします」

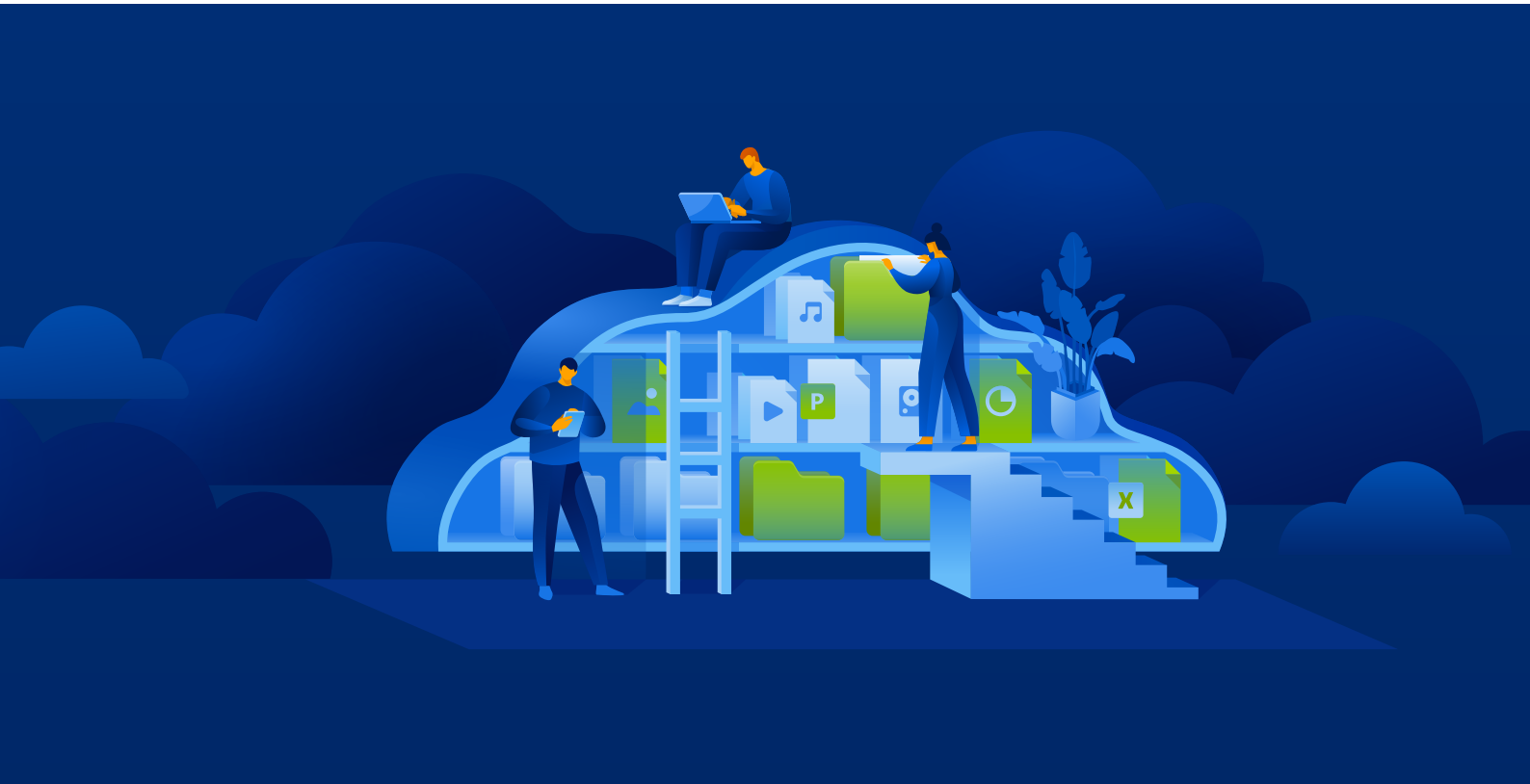
この部分に、責任共有モデルの特徴が最も顕著に表れています。Microsoft は顧客のデータに責任を負いません。実際、Microsoft はサードパーティのアプリやサービスでデータをバックアップすることを推奨しています。完全にバックアップされていず、すぐにリカバリできないデータは安全とは言えません。また、たとえ攻撃者にデータを盗まれなかったとしても、Microsoft 365 が唯一の保護手段である限り、重要な情報が消えてしまう恐れがあります。

ツールの乱立は混乱と統合の崩壊を引き起こす

MSP は、Microsoft 365 の顧客のデータセキュリティとバックアップを提供するために、サードパーティのツールを利用することになります。こうした手法は、すぐにツールの乱立につながり、新たな問題を引き起こします。Microsoft 365 を顧客ごとに管理するのは困難ですが、かといって他の複数ツールを同時に使いこなすのは基本的に不可能です。

技術者はしばしば入れ替わり、Microsoft 365 のセキュリティを強化する自分好みのツールを残して退社していきます。これらのツールを統合するには、法外な時間とコストがかかります。さらに、特定のツールに精通した技術者を割り当てなければなりません。こうした中で、コストが増加し、運用が複雑化する状況にすぐに陥ってしまいます。

その上、ほとんどのサードパーティ製ツールには互換性がありません。一般的には、API を使ってアプリケーションをリンクさせる必要があります。ここで問題となるのは、2 つの API がアプリケーション同士を結びつけたとしても、管理しやすい安定した統合にはならない点です。MSP は、その場しのぎの統合であっても、構築、保守、セキュリティ保護、トラブルシューティングのためにリソースを投入する必要があります。



結局、サービスプロバイダーが統合に費やした労力と費用は、一瞬にして価値を失い、接続の修復は、適切な専門知識がなければほぼ不可能です。多くの MSP は、脆弱な接続環境と手間のかかるテナント単位の設定で Microsoft 365 を運用していますが、そうした設定は不安定でリスクが高く、収益性が低くなります。

運用の問題が財務予測を不可能にする

Microsoft 365 の顧客にサービスを提供するために必要な時間、スタッフの数、全体的な労力を見積もることはほとんど不可能であり、財務上のリスクを伴います。サービスマネージャー、ソリューションアーキテクト、またはシステムエンジニアが Microsoft 365 の提供に必要なリソースを過小評価すると、MSP は損失を被り、複数のセキュリティサービスの販売による収益増加が打ち消されてしまいます。

逆に、サービスマネージャーが必要なリソースを過大評価すると、コストが高くなりすぎて、サイバー セキュリティサービスに対して顧客に過剰な料金を請求するリスクが生じます。そうなれば、MSP はサービスを販売することが難しくなり、最悪の場合サイバーセキュリティビジネスから撤退せざるをえません。

その結果、MSP は Microsoft 365 サービスをマネージドサービス契約（MSA）に組み込むことを躊躇しがちになります。コストの見通しが立たないため、このプラットフォームのサポートはリスクが高すぎますが、MSP の顧客のほとんどが Microsoft 365 を使用しており、MSP にその管理を求めているのも事実です。

Microsoft 365 で何か問題が発生した場合、顧客は MSP にその解決を期待します。信頼されるパートナーであろうとするために、MSP は問題を都度対応で解決し、1 回ごとに請求します。そして多くの場合、MSA に記載されていないため、修正費用は MSP が負担することになります。

たとえ MSP が顧客に請求する場合でも、修正するたびに利益は減っていきます。これでは、サービスプロバイダーのコストがすぐに膨れ上がり、顧客にとっても決して好ましい状況ではありません。顧客は、Microsoft 365 のような重要プラットフォームが、MSA で保証されることで、安心して利用できることを望んでいます。

MSP は Microsoft 365 の新時代に適応すべき

Microsoft 365 はかなり以前から提供されていますが、管理ツールには、MSP が複雑さや煩雑さを感じることなくサービスを顧客に提供するために必要な機能が備わっていません。

顧客は、セキュリティやデータ保護に関するこれまで以上に厳しい規制を遵守する必要があり、信頼性の高い Microsoft 365 サービスを求めています。また、急増し深刻化するサイバー攻撃から身を守る必要がありますが、多くの MSP はこうしたニーズに対応できるソリューションを備えていないため苦労しています。

20 年以上前にリモート監視・管理（RMM）が登場したとき、MSP はエンドポイントをプロアクティブかつ予測可能な形で管理できるようになり、サブスクリプションサービスの一環として、より収益性を高めることで、MSP ビジネスの方法を一変させました。

残念ながら、Microsoft 365 は同様のクラウドベースの機能を提供していましたが、現在では Exchange や SharePoint など、MSPが管理していたサーバーの多くを管理しています。しかし、管理し、セキュリティを確保し、データを保護する必要性が失われたわけではありません。MSP はユーザー、アプリ、データのサービスをクラウド上で提供することが求められました。しかし、RMM のような、自動化および顧客基盤全体にわたり単一のアクセスポイントで支援できるようなツールがありませんでした。

サービスプロバイダーは、単一のコントロールポイントで複数の Microsoft 365 テナントを管理する必要があり、Microsoft 365 のセキュリティとデータ保護のギャップを埋めるソリューションが求められています。

Microsoft 365 はかなり以前から提供されていますが、管理ツールには、MSP が複雑さや煩雑さを感じることなくサービスを顧客に提供するために必要な機能が備わっていません。

Microsoft 365 向けAcronis Cyber Protect Cloud 成熟度モデル

不完全でリスクの高い Microsoft 365 のカバレッジから脱却し、顧客に自信を持って提供できる環境を整えます。MSP がこのプロセスを実行するためには、 Microsoft 365 の保護に不可欠な要素を組み込める段階的なモデルを構築する必要があります。Acronis Ultimate 365 は、実装と保守が容易なネイティブに統合された単一のソリューションとして、成熟度モデルのあらゆる要素を提供することで、このプロセスを完了させます。

セキュリティのベースラインを設定する

サービスプロバイダーは、最初のステップとして、セキュリティのベースラインを設定することから成熟度モデルの導入を開始することができます。ここで言うベースラインとは、MSP が顧客に Microsoft 365 プラットフォームの保護を提供する際に、多くの MSP が抱える課題を回避するために必要な最低限の設定のことです。ベースラインには、以下が含まれています。

セキュリティ態勢管理: これは、複数のテナントを 1ヵ所に集め、集中管理の司令塔として Microsoft 365 の管理を可能にする重要な要素です。セキュリティ態勢管理により、MSP は 1 台のコンソールから複数の顧客を、アカウントを切り替えることなく管理できます。また、1 つのインターフェイスで複数顧客のオンボーディングとオフボーディングを一度に行うこともできます。

そのため、複雑なタスクを簡素化することができ、経験の浅い技術者でも上級技術者が処理していた責任範囲をカバーできるようになります。統一されたインターフェイスにより、より簡単な作業をより少ない人数で迅速に達成することで、MSP は有能な技術者を見つけるという困難な課題から解放されます。サービスプロバイダーは、少数の技術者でより多くの仕事をこなし、顧客環境の管理に費やす時間を大幅に短縮することができます。

MSP は 採用を管理し、リソースを割り当て、Microsoft 365 セキュリティ管理サービスを定義し、パッケージ化することで、MSA をシンプルにできます。採用の管理を強化し、顧客管理の負担を軽減することで、MSP は Microsoft 365 サービスを含む MSA を作成する際のリスクを減らすことができます。MSP は、Microsoft 365 のセキュリティとデータ保護サービスを利用して、コスト、売上、利益をより簡単に予測し、以前に直面していた財務リスクを負うことなく、MSA を構築することができます。

もちろん、顧客環境を保護する機能も求められます。統合型サイバーセキュリティソリューションは、Microsoft 365 に備わっていない機能を提供します。この統合型ソリューションにより、顧客をオンボーディングする際に、これまでは検出できなかった脆弱性を洗い出すことで、リスク検出機能を強化できます。また、ベースラインからの逸脱を継続的に監視し、リスクを自動的に修正することで、常時保護し、露出期間を最小限に抑えることができます。

これらの機能はすべて MSP を強化するものであり、Microsoft 365 に標準搭載された機能を超えた強固な防御とともに、多層防御を顧客に提供します。また、セキュリティ機能の周辺には、MSP が Microsoft 365 のセキュリティを提供する上で最も困難な局面を克服するための管理機能が実装されています。

バックアップとリカバリ: ほとんどの MSP はすでにバックアップとリカバリ機能を提供しています。しかし、サービスを提供する際に複数のアプリケーションを管理することに苦労しているケースが多くみられ、ツールを統合し、運用コストを削減する必要に迫られています。最終的には、バックアップとリカバリ、Eメールセキュリティ、セキュリティ態勢管理などの機能をネイティブに統合したソリューションが必要となります。

それでも、バックアップとリカバリは、MSP が提供すべき必須サービスであることに変わりありません。この機能により、MSP は Microsoft が積極的で解消しようとしない重大なギャップを埋めることができます。データバックアップは、MSP が迅速かつ最小限のビジネス中断でリカバリできる能力があってこそ価値があります。このデータ保護の要素は、Microsoft の責任共有モデルにおいて、顧客の責任の範疇に入ります。MSP は顧客にこの機能を提供しなければなりません。

バックアップとリカバリ機能は、ビジネス継続性という明確な価値を提供するだけでなく、規制要件を満たすためにも重要になります。GDPR、HIPAA、FINRA、SOX などの主要な規制には、データの保存、保護、リカバリに関する規定が含まれています。

Eメールセキュリティ: Eメールは、依然としてあらゆる種類の攻撃、特にランサムウェアやマルウェアの脅威の主要なベクトルです。IBM は、サイバー攻撃の 70% はエンドポイントから始まり、Eメールはエンドポイントへの主要な侵入口だと指摘しています。Microsoft の責任共有モデルでは、エンドポイントを保護する責任を、Microsoft ではなく顧客が負っています。

Microsoft 365 はある程度の Eメールセキュリティを提供しており、無償の Microsoft Defender アプリケーションは MSP に一定の価値を提供しています。しかし、それだけでは十分でありません。Microsoft には、ユーザーの受信トレイを保護する義務はありません。MSP には Eメールを保護するソリューションが必要であり、できればサイバー攻撃を未然に防ぐプロアクティブな監視機能を備えていることが望まれます。他の機能要素と同様に、サービスプロバイダーには、複数のテナントに対する Eメールセキュリティを単一のコンソールで管理する機能も求められます。

ベースラインは、 Microsoft 365 管理に必要な最低限の基準を、MSP に提供します。一旦、ベースラインが導入され、効率的で収益性の高いサービスを提供できるようになれば、次の段階に進み、サービスの幅を広げることができます。

セキュリティギャップを埋める

ベースラインは、 Microsoft 365 管理に必要な最低限の基準を、MSP に提供します。一旦、ベースラインが導入され、効率的で収益性の高いサービスを提供できるようになれば、次の段階に進み、サービスの幅を広げることができます。その一方で、サービスを拡大しながら、無節操にツールを増やしていけば、効率性と収益性の高い成長を持続させながら新サービスを構築することは困難になるでしょう。

だからこそ、ベースラインが不可欠なのです。MSP がベースラインを設定すれば、以下の拡張サービスを提供できるようになります。

セキュリティ態勢の監視と修復: この機能は、セキュリティ態勢管理を一歩進め、MSP が顧客環境におけるイベントの監視と修復の両方を自動化するのを可能にします。サービスプロバイダーは、複数テナントへのシングルビューアクセス機能は活かしたままで、技術者が介入することなく問題を発見し、修復できるシステムにアップグレードすることができます。

セキュリティ態勢の監視と修復により、MSP は顧客向けの Microsoft 365 の管理に費やす時間をさらに短縮し雇用する技術者の数を減らすことができます。また、この機能により、収益性を犠牲にすることなく、より多くの顧客を獲得し、売上を増やすことができます。

セキュリティ意識向上トレーニング: サイバーセキュリティにおいて最も脆弱なリンクは、常に人間です。2024 年 Verizon データ漏洩調査レポートによると、データ漏洩の約 70% はエンドユーザーのミスが原因です。顧客サイトでのユーザーミスが減れば、MSP が修復しなければならないインシデントも減ります。

サービスプロバイダーは、Microsoft 365 の顧客のリスクをプロアクティブに防ぐと同時に、すべてのサイバーセキュリティ、データ保護、エンドポイント管理サービスを、単一ポイントで制御する単一のソリューションで簡単に管理し、提供することができます。

MSP は、世界中の多くの政府規制に準拠するための要件となっているセキュリティ意識向上トレーニングを提供することで、自社を守り、売上を増やすことができます。トレーニングの実施と管理は、顧客環境を集中制御することで、シンプルで収益性の高いものとなります。セキュリティ意識向上トレーニングは、コンプライアンスやサイバー保険の必須要件となりつつあり、MSP が顧客にトレーニングを販売する際のセールスポイントになります。

しかし、セキュリティ意識向上トレーニングを効果的に実施するのは一筋縄ではいきません。情報があふれ、人の忍耐力が低下している時代において、トレーニングは簡潔かつ魅力的で、素早く理解できるものでなければなりません。そのため、MSP は、受講者が実際に教材を習得し、それに応じた行動を実践できるように、魅力的でゲーム化されたレッスンを提供できるトレーニングパートナーを採用する必要があります。

XDR 統合: Extended Detection and Response（XDR）は、エンドポイントの検出および対応（EDR）を新たなレベルに引き上げます。XDR により、MSP は Eメールや ID/アクセス管理を含む最も脆弱な攻撃対象領域を可視化し、Microsoft 365 のエンドポイントを保護することができます。サービスプロバイダーは、AI の支援により、脅威の分析と対応に必要な時間をわずか数分に短縮することができます。これまで以上に詳細な調査を実施し、迅速に対応し、大規模にリスクを軽減することができます。

XDR により、MSP は対応を自動化し、即座に修復できるようになりました。その結果、セキュリティ運用の拡張とコスト削減が可能になりました。ネイティブに統合されたサイバーセキュリティソリューションと連携することで、サービスプロバイダーは、Microsoft 365 の顧客のリスクを未然に防ぐと同時に、すべてのサイバーセキュリティ、データ保護、エンドポイント管理サービスを、単一ポイントで制御する単一のソリューションにより、簡単に管理し、提供することができます。

顧客の要件に合わせたソリューション

機能のギャップを埋め、自動化を進めることで、MSP は Microsoft 365 のサービスを細かくカスタマイズできるようになりました。

Eメールアーカイブ: MSP 向けに設計された Eメールアーカイブは、強力な検索機能と、迅速なセルフサービスアクセスをクライアントに提供します。Eメールアーカイブが提供されることで、顧客は規制要件を容易に遵守できます。

コラボレーションアプリケーションのセキュリティ: MSP は、Microsoft 365 のコラボレーションアプリケーションのセキュリティを提供することで、サービスを向上させることもできます。企業が、SharePoint、Teams、OneDrive、その他の Microsoft 365 クラウドコラボレーションアプリに急速に移行していることから、サイバー攻撃者にとって、ますます魅力的な標的となっています。

現在のコラボレーションアプリ向けの Microsoft 365 セキュリティは、包括的な保護を提供していません。適切なツールを導入することで、MSP は Microsoft のネイティブなセキュリティにとどまらず、悪意のあるコンテンツが検出された場合にアラートを設定して通知したり、すべてのファイルや URL を動的にスキャンしてエンドユーザーへの脅威の拡散を防止することができます。

重要なのはサイバーセキュリティ機能のネイティブな統合

MSP セキュリティモデルのすべての要素が重要であり、特にベースラインレベルは不可欠ですが、MSP にとってのサイバーセキュリティ成熟度の真の価値は、集中管理された単一のソリューションでモデルのすべての機能を提供/管理できる能力にあります。

Acronis Ultimate 365 を使用することで、サービスプロバイダーは従来のシステムの制約や煩雑さに悩まされることなく、Microsoft 365 のセキュリティと保護を顧客に提供することに集中できます。アクロニスのソリューションは、MSP が Microsoft 365 環境で顧客を保護し、リソースを再配布するために必要となる、包括的なネイティブに統合された機能を提供します。Microsoft 365 の RMM を効果的に実現し、さらに多くの機能を提供します 。

Acronis Ultimate 365 により、MSP は、バックアップ、XDR、Eメールセキュリティ、コラボレーションアプリセキュリティ、Eメールアーカイブ、セキュリティ態勢管理、およびセキュリティ意識向上トレーニングの 7 つの保護機能を、単一の直感的なマルチテナントプラットフォームに統合した、最も包括的な保護ソリューションを効率的に提供できるようになります。MSP は利用したサービスに対してのみ料金を支払い、顧客に最大限の価値を提供します 。

Acronis Ultimate 365 で、以下を提供します。

単一の統合プラットフォームで Microsoft 365 を包括的に保護

すべてを保護 — データ保護、サイバーセキュリティ、セキュリティ態勢管理、セキュリティ意識向上トレーニングをネイティブに統合することにより、顧客の Microsoft 365 シートのあらゆる要素を確実に保護します。

収益化への最短コース

製品選定、契約交渉、スタッフトレーニング、顧客オンボーディングにおけるあらゆる障壁を取り除きます。簡単な操作でサービスを販売、有効化し、すぐに収益につなげることができます。

きわめて効率的な管理

単一のプラットフォームですべての顧客とサービスを一元管理します。専門知識があまり必要でなくなり、作業時間を短縮できます。

自信を持ってMicrosoft 365 の保護を提供し収益化する体制が整っていない MSP は、すでに提供を進めている MSP に対して競争上不利な立場に立つことになるでしょう。Acronis Ultimate 365 を使用すれば、人気の Microsoft 365 プラットフォームの保護はもはや問題になりません。危機とリスクを商機に変えるのです。