SOPHOS

MSP のビジネス展望 2024 年版

350 社の MSP に対する調査から得られた、サイバーセキュリティツール、リスク、課題、ビジネス機会に関する知見。

ソフォス ホワイトペーパー 2024 年 5 月

はじめに

「MSP のビジネス展望 2024 年版 」レポートでは、MSP のビジネスの以下の 5 つの主な分野に関する知見を紹介します。

- RMM と PSA ツール
- サイバーセキュリティの管理
- MDR サービス
- MSP と MSP の顧客が直面する課題とリスク
- サイバー保険の影響

これらの結果は、米国 (200)、英国 (50)、ドイツ (50)、オーストラリア (50) の 350 社の MSP を対象に、独立した調査会社が実施した調査に基づきます。この調査は、ソフォスの委託を受けて調査会社の Vanson Bourne が 2024 年 3 月に実施しました。

4 か国の

350 以上 の MSP

米国
回答者 200 名

英国
回答者 50 名

ドイツ
回答者 50 名

オーストラリア
回答者 50 名

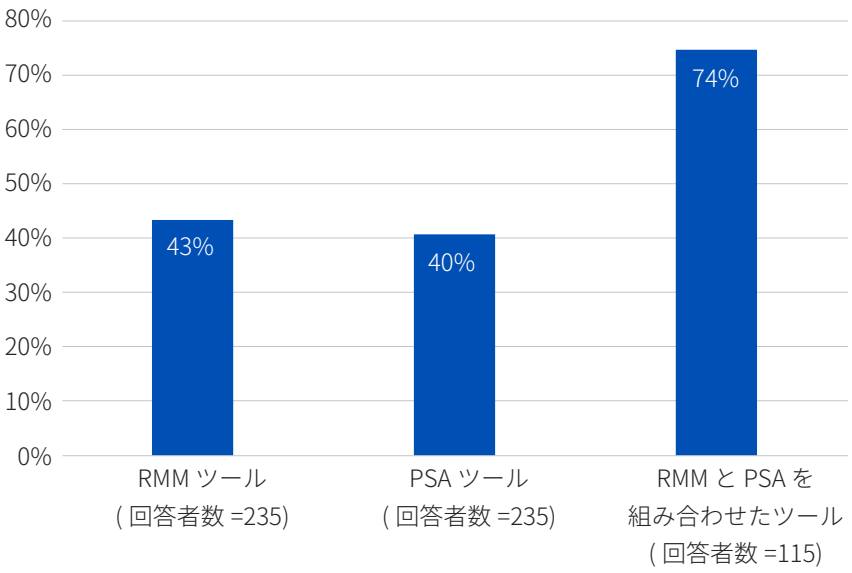
RMM と PSA ツール

リモート監視および管理 (RMM) とプロフェッショナルサービスオートメーション (PSA) ツールは、MSP がサービスを効率的かつ効果的に提供できるようにしながら、MSP の運用や管理を合理化します。この調査では、MSP を支援するこれらのテクノロジーに関して、2 つの重要な結果が明らかになりました。

RMM と PSA ツールを組み合わせると、ツールを個別に使用する場合に比べて、はるかに高い満足度が得られる

RMM と PSA ツールを組み合わせて使用している MSP のほぼ 4 分の 3 (74%) が、ソリューションに「非常に満足」と回答しているのに対し、この回答率は、スタンドアロンで RMM ツールを使用している場合には 43%、スタンドアロンで PSA ツールを使用している場合は 40% にとどまります。

既存の RMM および PSA ツールに「非常に満足」と答えた回答者

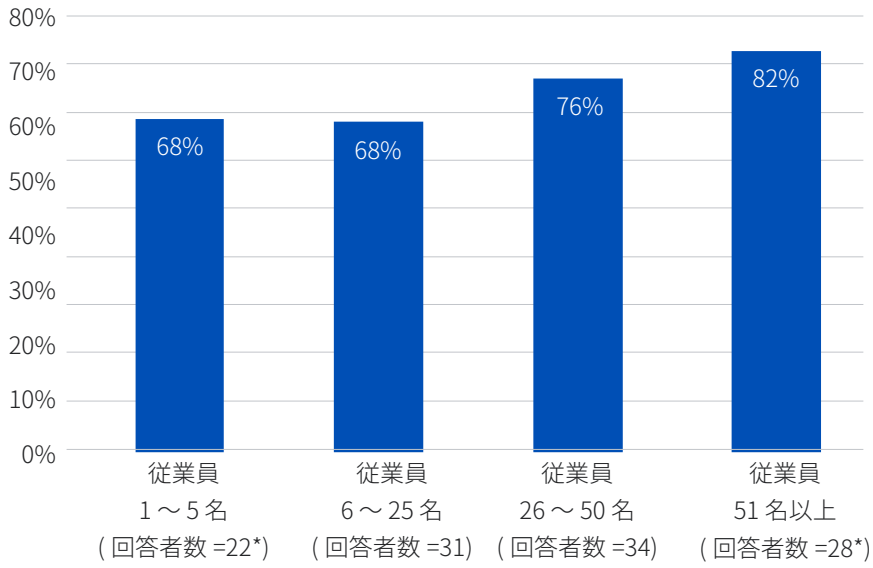


既存の RMM および PSA ツールにどの程度満足していますか？回答者数を図内に記載。

RMM と PSA を組み合わせた場合の満足度は、MSP の規模が大きくなるほど高まる

従業員数 25 名までの MSP の 3 分の 2 以上 (68%) が、RMM と PSA ツールを組み合わせて利用することに非常に満足しています。従業員数 26 ～ 50 名の MSP と従業員数 51 名以上の MSP を見ると、この回答率は、それぞれ 76% と 82% に上昇します。MSP の規模が大きくなるほど、多くの顧客を支援している可能性が高まります。この調査結果は、顧客がより多いほど、RMM と PSA ツールを同時に使用することによってもたらされる利益が大きくなることを示しています。

RMM と PSA ツールを同時に使用することに「非常に満足」と答えた回答者



既存の RMM および PSA ツールにどの程度満足していますか？回答者数を図内に記載。
* このセグメントの回答者数は少ないため、調査結果は統計的に有意ではありません。参照情報として扱ってください。

ソフォスの提言：RMM または PSA ツールをそれぞれスタンドアロンで使用している MSP は、特に顧客ベースの拡大を計画されている場合、満足度を高めるために RMM と PSA を同時に使用するソリューションに移行することを検討してください。

サイバーセキュリティの管理

サイバーセキュリティベンダーとの連携

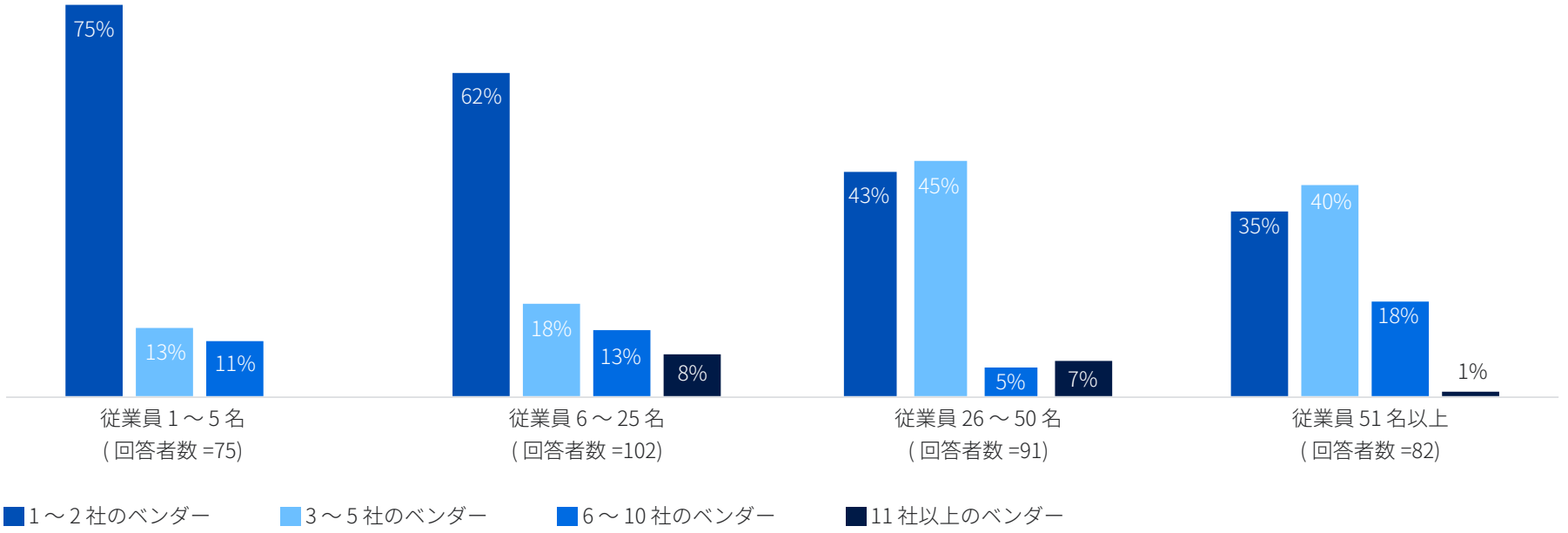
サイバーセキュリティは、多くの MSP にとって重要な基幹サービスです。今回の調査から、MSP は通常、少数のサイバーセキュリティベンダーと連携して顧客を保護していることがわかりました。

- 1 社または 2 社のサイバーセキュリティベンダーと連携している MPS は 53%。
- 1 社から 5 社のサイバーセキュリティベンダーと連携している MSP は 83%。
- 11 社以上のサイバーセキュリティベンダーと連携している MSP は 4%。

また、一般的に MSP 組織の規模が大きくなるほど、連携するサイバーセキュリティベンダーの数が増加することもデータが示しています。規模が最も小さな MSP (従業員数 1 ～ 5 名) の 75% が 1 社または 2 社のサイバーセキュリティベンダーと連携しているのに対し、従業員数 51 名以上の MSP では 1 社または 2 社のベンダーと連携しているのはわずか 35% にとどまっています。

逆に、規模が最も大きな MSP は、小規模な MSP と比較して、6 社以上のサイバーセキュリティベンダーと連携している割合が約 2 倍になっています (四捨五入した数値で 20% 対 11%)。連携するサイバーセキュリティベンダーの数が増えると、提供できるサービスの幅が広がる可能性はありますが、ベンダーを管理するための間接費や、異なるテクノロジーを統合しなければならないなどの課題も増加することがあります。

顧客を保護するために利用しているサイバーセキュリティベンダーの数



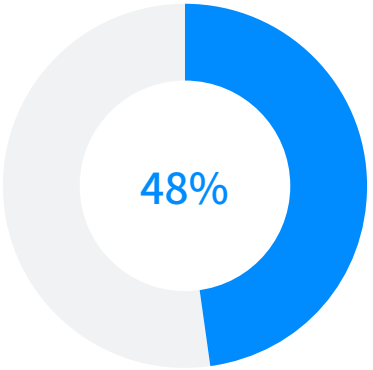
あなたの組織は現在、顧客を保護するために何社のサイバーセキュリティベンダーを利用していますか？回答数を図内に記載。「わからない」は除外。

サイバーセキュリティプラットフォームの統合

今回の調査では、MSP がサイバーセキュリティプラットフォームを統合することで、業務の効率性を向上し、間接費を削減できる大きな可能性があることもわかりました。

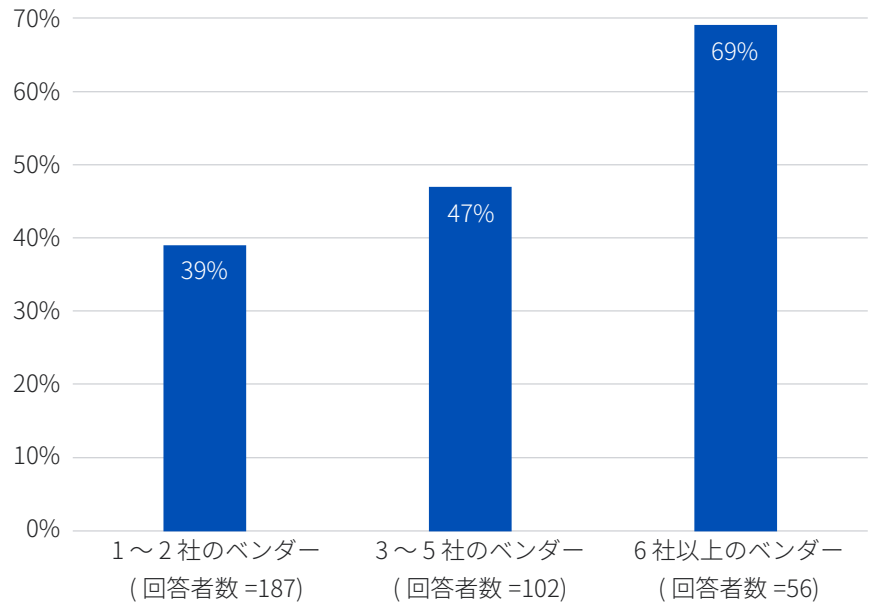
現在複数のプラットフォームを使用している MSP は、単一のプラットフォームですべてのサイバーセキュリティツールを管理できる場合に、日々の管理時間を平均で 48% 節約できると試算しています。

1 つのサイバーセキュリティプラットフォームに統合する場合に削減できると予測される日々の管理時間の割合



現在使用しているサイバーセキュリティベンダーの数が多いほど、管理時間を節約できる可能性も高くなります。6 社以上のサイバーセキュリティベンダーと連携している MSP は、単一のプラットフォームですべてのサイバーセキュリティツールを管理できる場合、日々の管理時間を 3 分の 2 以上 (69%) 削減できると予測しています。管理の間接費をこれだけ削減できれば、収益にも大きな影響をもたらし、同時に従業員は収益を上げるための別の活動に時間を費やすことも可能になります。

使用しているベンダーの数だけ分散しているプラットフォームを 1 つのサイバーセキュリティプラットフォームに統合することで、削減できると推定される日々の管理時間の割合



サイバーセキュリティツールのすべてを単一のプラットフォームで管理できる場合、日々の管理時間をどの程度削減できると予測しますか？回答者数を図内に記載。

ソフォスの提言：複数のサイバーセキュリティプラットフォームを使用している MSP は、統合の可能性を検討し、単一のプラットフォームですべてのサイバーセキュリティツールを管理して TCO を削減してください。

MDR サービス

MDR サービスの導入

サイバー脅威と、これらの脅威を防止するツールやテクノロジーの両方が複雑化したことで、MDR (Managed Detection and Response) サービスの需要が急速に増大しています。Gartner が最近公開したデータによると、MDR の市場総額は 75 億ドルであり、年平均成長率 (CAGR) は 25.8% に達しています。

このような需要の伸びと将来的な成長予測を背景にして、多くの MSP (81%) がすでに一定レベルの MDR サービスを提供しています。残りの 多くの MSP も、直近および将来的に MDR サービスを追加することを計画しています。しかし、今回の調査では、MDR サービスの導入の広がりについては、調査対象の 4 か国間でかなりの差があることが明らかになりました。

米国の MSP の 94% がすでに MDR サービスを提供しており、ドイツ (70%)、イギリス (62%)、オーストラリア (58%) を引き離しています。世界全体では、現在 MDR を提供していないほぼすべての MSP が今後数年間で MDR をポートフォリオに追加することを計画しており、英国の MSP のほぼ 3 分の 1 (32%) が 2024 年に MDR を追加することを計画しています。

現在 MDR サービスを提供している	**94%**	**62%**	**70%**	**58%**
2024 年に MDR サービスを追加することを計画している	5%	32%	20%	18%
2025 年以降に MDR サービスを追加することを計画している	2%	6%	10%	22%

あなたの組織は現在、顧客に MDR サービスを提供していますか？
回答者数 =350 (米国 200、英国 50、ドイツ 50、オーストラリア 50)、回答の選択肢の一部を除外。

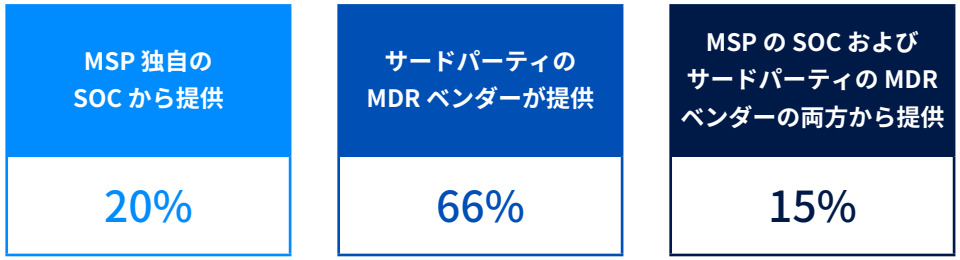
MDR サービスの提供

MSP が MDR サービスを提供する場合、MSP の自社のセキュリティオペレーションセンター (SOC) から提供する、サードパーティベンダーのサービスを利用する、MSP の SOC とサードパーティベンダーのサービスの両方を活用するという 3 つの主なモデルがあります。

今回の調査では、66% が MDR サービスを提供するためにサードパーティベンダーを利用し、20% が自社の SOC を利用し、15% が自社の SOC とサードパーティベンダーのサービスの両方を利用していることがわかりました。全体として、MSP の約 80% が、MDR サービスを提供するために何らかの形でサードパーティベンダーと連携しています。

MSP の約 34% が社内に SOC を設置しており、自社のみまたはサードパーティベンダーと連携して MDR サービスを提供しています。SOC を社内に設置している割合は、すべての規模の MSP でほぼ一致しています。SOC を社内に設置している割合が最も高いのは、従業員数 26 ～ 50 名の規模の組織であり、その割合は 37% でした。それ以外の規模の組織ではこの割合は 33% であり、その差はわずか 4 ポイントです。

MDR サービスの提供方法



あなたの組織は現在、顧客に MDR サービスを提供していますか？
回答者数 =MDR サービスを提供している 282 社。回答の選択肢の一部を除外。

MDR プロバイダーに求められる能力

これまで見てきたように、MSP の 5 社に 4 社が、MDR サービスを提供するためにサードパーティベンダーを利用しています。MDR サービスに対する需要が大きく伸びていることから、MSP は自社と顧客にとって最適なベンダーを選択することが極めて重要になっています。

MDR ベンダーは MSP が提供するサービスの能力を拡大することから、MDR ベンダーの資質と能力はそのまま MSP に反映されることになります。さらに、MDR ベンダーの能力は、MSP が顧客に提供できるサービスの範囲や、MSP が行う必要のある管理作業の負荷にも影響します。

*24 時間 365 日体制のインシデント対応サービス*は「必須」の能力として挙げられており、36% の MSP が「必要不可欠」と回答しています。この数値は従業員が 1 ～ 5 名の MSP では 49% に増加します。ランサムウェア攻撃の 91% は標準的な営業時間外に開始されていることから、[1] 顧客の組織を効果的に防御するためには、24 時間体制でサービスを提供できることが不可欠になっています。24 時間 365 日体制でサービスを提供できる MDR ベンダーと連携することで、MSP は社内でこのような高度なレベルの専門的なサービスを立ち上げる労力を背負うことなく、顧客を常に保護しているという安心感を得ることが可能になります。

2 番目に多く挙げられた能力は、*「Microsoft 365 や Google Workspace のアカウント乗っ取りの脅威を検出する能力」*でした。MSP の 3 分の 1 (33%) がこの能力を「必須」と回答し、43% が「非常に重要」と回答しています。

*「MDR ベンダーから、別のセキュリティツール (特にファイアウォール / ネットワークセキュリティとエンドポイントプロテクション) を利用できること」*も強く求められている能力であり、回答者の 4 分の 3 が「必須」または「非常に重要」と回答しています。単一プロバイダーからサイバーセキュリティツールと MDR サービスを利用することができれば、運用を合理化しながら、管理者の労力を削減することが可能になります。

同時に、MSP は柔軟性も求めており、使用できるツールを制限されたり、MDR ベンダーからサイバーセキュリティツールを購入することを強制されることは望んでいないことも、この調査で明らかになっています。71% の MSP は、*「脅威の検出と対応に既に導入しているセキュリティツールのテレメトリ (監視データ) を使用できること」*を「必須」または「非常に重要」と回答しています。

24 時間 365 日体制のインシデント対応サービスは、MDR ベンダーに求められている最大の要件

能力	「必須」	「必須」または「非常に重要」
24 時間 365 日体制の インシデント対応サービス	36%	74%
Microsoft 365 や Google Workspace アカウント乗っ取りの脅威を検出する能力	33%	77%
MDR ベンダーから**ファイアウォール / ネットワークセキュリティ**ツールを利用できること	31%	74%
MDR ベンダーからエンドポイントプロテクションツールを利用できること	28%	75%
MDR とその他のセキュリティソリューションを単一のコンソールから管理できること	28%	74%
セキュリティ侵害に**対する補償**	26%	70%
脅威を検出して対応するために既に導入しているセキュリティツールのテレメトリを利用できること	25%	71%

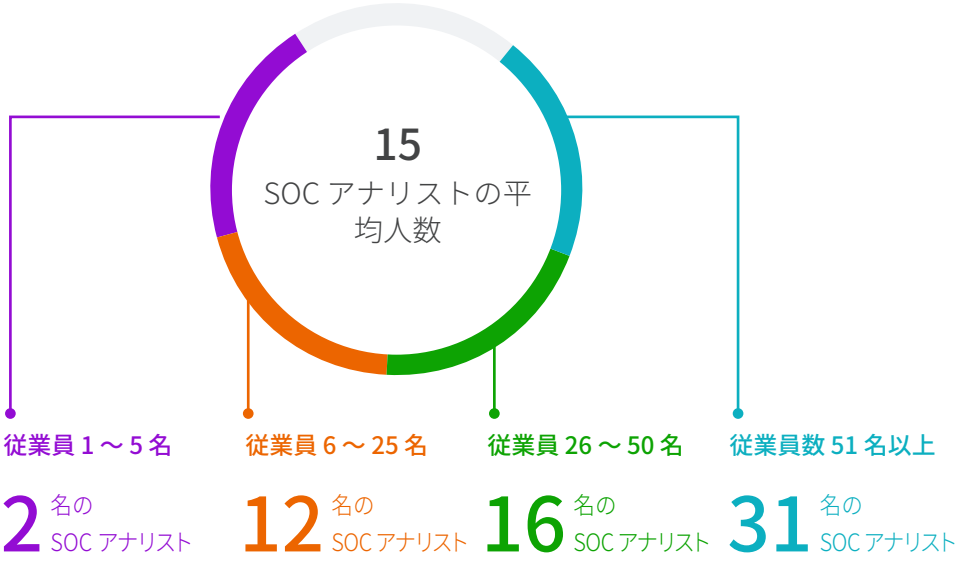
あなたの組織が MDR ベンダーを選択する必要がある場合、MDR ベンダーが提供する以下の機能はどの程度重要だと考えますか？
回答者数 =350 (米国 200、英国 50、ドイツ 50、オーストラリア 50)、回答の選択肢の一部を除外。

社内の SOC アナリスト

MDR サービスを提供している MSP の 34% は、社内に SOC を設置しており、社内で専門のアナリストを採用しなければなりません。今回の調査によると、一般的な MSP の SOC には平均で 15 名のアナリストが存在していました。しかし、この数値は、MSP の規模別に見ると、かなりのばらつきがあります。

従業員が 1 ～ 5 名の MSP は、平均して 2 名のアナリストが顧客の環境を監視し、脅威を検出して対応しています。アナリストの数は組織の規模が大きくなるにつれて増加する傾向が顕著であり、最大級の MSP では平均 31 名の SOC アナリストが存在していることが報告されています。各セグメントの回答者数は少ないため、調査結果は統計的に有意ではありません。参照情報として扱ってください。

サイバー攻撃者は、営業時間外となる深夜、週末、休日に攻撃を意図的に仕掛けており、防御効果を高めるためには、24 時間 365 日体制で MDR サービスを提供することが不可欠となっています。SOC アナリストが少ない小規模な MSP にとって、自社のリソースのみで MDR サービスを提供することは、限られているリソースに大きな負担を強いることになります。



あなたの組織の SOC について尋ねます。あなたの組織では、何名のアナリストが顧客の環境の攻撃が疑われるイベントを監視して対応していますか？

ソフォスの提言：現在 MDR サービスを提供していない MSP は、競争に取り残されることがないように早急に MDR サービスをポートフォリオに加えることを検討してください。サードパーティの MDR ベンダーを選定するときには、自社にとって重要な機能を見極めて、それらの機能を提供しているベンダーの能力を評価してください。

課題とサイバーリスク

MSP が現在直面している最重要課題

MSP を取り巻く環境は常に変化しています。脅威は進化を続けており、サイバーセキュリティ対策も進化し、顧客のニーズも変化しています。

今回の調査で、***最新のサイバーセキュリティソリューションやテクノロジーに追いつくこと***が、MSP が現在直面している最大の課題であることが明らかになりました。

この分野のイノベーションのスピードを考えれば、多くの MSP が最新のテクノロジーに追いつくことに苦労していることは驚くべきことではありません。脅威の進化に伴って、脅威を阻止するためのサイバーセキュリティ機能も進化しています。既存のテクノロジーに新たな機能が追加されている一方で、全く新しい製品も定期的に市場に投入されています。これらすべてのテクノロジーの動向を常に把握することは困難であり、多くの時間も必要となります。

十分なサイバーセキュリティアナリストを確保することが困難になっていることが、MSP が現在直面している最大の課題の第 2 位の主な要因です。

- ***夜間や週末を含む営業時間外の検出と対応***は、MSP が直面している最大の課題の第 2 位
- ***成長に合わせたサイバーセキュリティアナリストの増員***は、課題のトップ 3 の第 2 位

サイバーセキュリティを専門とするアナリストは慢性的に不足しており、高い給与を支払わなければ採用することができません。さらに、24 時間 365 日体制で脅威を監視して対応するためには、少なくとも 5 ～ 6 名のアナリストが必要となりますが、これだけのアナリストを採用することは多くの MSP にとって極めて困難です。

最大の課題

1 位	最新のサイバーセキュリティソリューションやテクノロジーを取り入れること
2 位	夜間、週末、休日などの営業時間外にも対応すること
3 位	新規顧客を獲得すること

トップ 3 の課題

1 位	最新のサイバーセキュリティソリューションやテクノロジーを取り入れること
2 位	顧客の増加に合わせてサイバーセキュリティアナリストを増員すること
3 位	最新のサイバー脅威に対応すること

あなたの組織が日々直面している重要な課題は何ですか？重要な課題を 3 つお答えください。

サイバーリスク

今回の調査では、MSP が自社と顧客の双方にとって最大と考えているサイバーリスクについても調べました。その結果、共通するリスクと相違するリスクの両方が明らかになっています。

MSP とその顧客の双方にとって、以下の 2 つのリスク要因が上位を占めています。

- アクセスデータや認証情報の窃取
- サイバーセキュリティに関する社内のスキルや専門知識の不足

実際には、攻撃者は組織に侵入しているわけではありません。ログインしてアクセスしています。窃取した、あるいは、ダークウェブで初期アクセスブローカー (IAB) から購入したアクセスデータと認証情報を使用して、正規の従業員になりすまして標的の組織にアクセスしています。ソフォスの「ランサムウェアの現状 2024 年版」レポートでは、昨年のランサムウェア攻撃の 29% が漏洩した認証情報が起点となっており、この問題が深刻な問題になっていることが示されています。

MSP

最大のリスク		重要な 3 つのリスク	
1 位 =	サイバーセキュリティに関する社内のスキルや専門知識の不足	1 位	アクセスデータや認証情報の窃取
1 位 =	安全でないワイヤレスネットワーク	2 位	セキュリティツールの設定ミス
3 位	サイバーセキュリティツールの不足	3 位	安全でないワイヤレスネットワーク

MSP クライアント

最大のリスク		重要な 3 つのリスク	
1 位	サイバーセキュリティに関する社内のスキルや専門知識の不足	1 位	アクセスデータや認証情報の窃取
2 位	パッチが適用されていない脆弱性	2 位	サイバーセキュリティツールの不足
3 位	リモートアクセスツール	3 位	パッチが適用されていない脆弱性

あなたの組織や顧客にとって、最大のサイバーセキュリティリスクは何ですか？

サイバーセキュリティテクノロジーと人工知能も絶え間なく進化していますが、効果的なサイバーセキュリティを実現する鍵は、依然として人間が握っています。熟達したプロフェショナルが、テクノロジーソリューションを設定、展開、管理、対応、更新しなければなりません。テクノロジーだけではすべての攻撃を自動的に阻止することはできません。スキルの高いプロフェショナルが不足していることは周知の事実ですが、この採用の問題を解消するために企業は MSP を利用するようになっており、この人材難の問題は悪化しています。

MSP とその顧客の双方が認識している最大のリスクは共通していますが、下位のリスクを見ていくと、その認識に違いがあることがわかります。

安全でない無線ネットワークは、MSP が認識しているサイバーリスクのトップです (「最大のリスク」で第 1 位、「トップ 3 のリスク」で第 3 位)。安全でないネットワークを使用すると、データが傍受され、ログインやパスワード情報が窃取され、サイバー攻撃者が個人や企業のアカウントにアクセスできるようになるなど、いくつかの危険性につながる可能性があります。

セキュリティツールの設定ミスもまた、MSP が認識している最大のリスクの 1 つです。ファイアウォールやエンドポイントプロテクションなどのツールは、正しく設定されなければ正しく機能しません。

パッチが適用されていない脆弱性は、MSP の顧客が認識している最大のリスクの 1 つです (「最大のリスク」第 2 位で、「トップ 3 のリスク」の第 3 位)。昨年発生したランサムウェア攻撃の 32% は、パッチが適用されていない脆弱性の悪用が起点となっていることから、MSP は、この問題は顧客にとって大きなリスクであることを認識しなければなりません。

ソフォスの提言：このような広範なリスクおよび課題に直面する中で、連携するベンダーの数を削減し、日々の管理作業を最小限に抑えるために、MSP はあらゆるサービスとツールを提供しているサイバーセキュリティのパートナーを探す必要があります。複雑な設定や展開を必要とせず、堅牢で適応型の保護機能を組み合わせたソリューションを展開し、進化する脅威に対応できるようになれば、最先端のテクノロジーに取り残されることもありません。さらに、MSP は、自社にとって最適なビジネスモデルをサポートし、変化や成長に合わせて自社のニーズに柔軟に適応できるパートナーを見つけて、社内のサイバーセキュリティスキルや専門知識を拡大および拡張するために、MDR ベンダーを活用すべきです。

サイバー保険の影響

ソフォスの調査によると、サイバー攻撃を受けた場合のリスクを分散するためにサイバー保険を利用するケースが着実に増加しており、現在では中堅企業の 90% が何らかの形で保険に加入しています。中堅企業の 50% がスタンドアロン型のサイバー保険契約に加入し、40% がより広範なビジネス保険契約 (一般賠償責任保険など) の一部としてサイバー保険に加入しています。

サイバー保険への加入が広がっていることは、チャネルパートナーによるエンゲージメントの強化にもつながっており、MSP の 99% がサイバー保険の要件を満たすためのサポートやソリューションへの需要が増加していることを報告しています。

世界全体では、MDR サービスを導入して保険契約の等級を向上させたいという顧客の要望が最も多くなっており (47%)、次いで保険申請の手続きを完了するための支援が必要という顧客の要望 (45%) が僅差で続いています。これらの要件はいずれも MDR の提供やプロフェッショナルサービスの請求によって大きな収益を生み出す機会を MSP にもたらします。

顧客のニーズ	グローバル				
MDR を利用して保険契約の等級を向上させる	**47%**	49%	38%	56%	36%
保険**申請手続きを**完了するための支援	**45%**	49%	46%	30%	42%
EDR を利用して保険契約の等級向上させる	**34%**	31%	32%	28%	52%
EDR/MDR 以外のテクノロジーやサービスを利用して、保険契約の等級を向上させる	**33%**	31%	22%	48%	40%

あなたの組織では、顧客のサイバーセキュリティ要件に対応するためのサポートやソリューションへのニーズが高まっていますか？
回答者数 =350 (米国 200、英国 50、ドイツ 50、オーストラリア 50)。

MSP の 3 分の 1 (34%) が、保険等級を向上するために、顧客が EDR (Endpoint Detection and Response) をセキュリティスタックに追加することを検討していることを報告しています。オーストラリア以外では、保険に関連する MDR へのニーズは、EDR よりも大幅に高くなっていますが、これは 24 時間 365 日体制で MDR サービスを提供する方が、リソースが不足している社内チームが MDR サービスを提供するよりも、大幅にリスクを削減できることを反映しています。

回答者の 3 分の 1 (33%) が、保険等級の向上を望む顧客からの EDR/MDR 以外のテクノロジーやサービスに対する需要が高まっていると回答しています。今回は、これ以上深く調査はしていませんが、すべての保険会社が多要素認証 (MFA) ツール、メール、ネットワークセキュリティを一般的に要求していることから、EDR/MDR 以外のテクノロジーやサービスには、これらの機能が含まれている可能性が高いと考えられます。

ソフォスの提言：MSP には、有利な補償を受けるために保険等級を向上させるサービスやテクノロジーを提供する大きなビジネス機会が広がっています。MSP はこの分野で顧客を最適な方法で支援し、収益性を最大化する必要があります。

結論

サイバー攻撃はあらゆる企業や組織にとって避けることができない問題です。これは、MSP がビジネスを成長させ、収益性を向上させる多くのビジネス機会につながっています。管理プラットフォームを統合することによって日々の管理業務を削減する、サードパーティの MDR ベンダーとの連携方法を最適化して提供するサービスを拡大する、そして、サイバー保険のニーズに対応するなど、MSP はランサムウェアやセキュリティ侵害への保護対策を強化しながら、さまざまなビジネスを推進できます。

MSP の市場は競争が劇化しています。MSP は、今回の調査から得られた知見を活用し、今後のビジネス機会を最大限に広げてください。

Sophos MSP プログラム

ソフォスは、MSP がビジネスを拡大し収益を向上できるように支援しています。ソフォスは、革新的でさまざまな環境に適応できる防御機能と、包括的な MSP 向けのサイバーセキュリティシステムを提供しており、自信を持ってサイバーセキュリティサービスを顧客に提供できるようにし、MSP のビジネスを成功に導きます。

- サイバーセキュリティサービスと製品の包括的なポートフォリオを一社のベンダーから利用できれば、顧客の現在および将来的なニーズにも確実かつ効率的に対応できます。
- Sophos Central セキュリティプラットフォームは、すべての顧客のセキュリティを単一のコンソールで管理できるため、日々の管理作業を最小限に抑え、貴重なリソースな時間を確保できるようになります。
- Sophos MSP プログラムでは、魅力的なマージン、収益性の高いインセンティブ、および一括請求を享受できます。

1 ビジネスリーダー向けのアクティブアドバーサリーレポート、ソフォス、2023 年

Sophos MSP プログラムの詳細については、sophos.com/MSP を、Sophos MDR については、sophos.com/MDR をご覧ください。

Sophos MDR：24 時間 365 日体制のインシデント対応を標準で提供

Sophos MDR は、世界で最も信頼されている MDR (Managed Detection and Response) サービスであり、世界中でどのベンダーよりも多くの組織を保護しています。24 時間 365 日体制の検出とアナリストによる手動の対応が標準で提供されるため、MSP とその顧客は、昼夜を問わずソフォスの専門家が攻撃を阻止しているという安心感を得ることができます。Sophos MDR サービスの内容については以下をご覧ください。

- アナリストによる 24 時間 365 日体制の手動の修復
- 包括的なインシデント対応
- 24 時間 365 日体制の直接連絡サポート
- 専任のインシデント対応の担当者
- 対応モデルの選択
- セキュリティ侵害に対する補償
- プロアクティブな脅威ハンティング
- ソフォスおよびソフォス以外ベンダーのエンドポイントプロテクションに対応
- Microsoft 365 や Google Workspace アカウント乗っ取りを検出
- その他の多数の機能

完全なアウトソーシングサービスを検討されている場合でも、社内の SOC を柔軟に拡張できるサービスを検討されている場合でも、Sophos MDR を利用すれば、ビジネスを成長させることができます。

「Sophos MDR は、壊滅的なビジネス障害になりえる可能性から数社のクライアントを救ってくれました。当社のマージンは 100% 増加し、収益は 300% 増加しました。」

The ITeam、社長、James Wagner 氏

2024-05-21 (WP-NP)

SOPHOS