

REPORT

PERSPEKTIVEN FÜR MSPS 2026

Einblicke von 800 MSPs zu
den Herausforderungen und
Chancen, die die Zukunft von
Cybersecurity-Services prägen.

SEPTEMBER 2026



Kurzfassung

Die Cybersicherheit steht vor einer Führungskrise. Weltweit kommt auf 10.000 Unternehmen nur ein einziger Chief Information Security Officer (CISO)¹. Der überwiegenden Mehrheit fehlt somit die gezielte Führung und Strategie, die für nachweisbare Sicherheit erforderlich sind. Währenddessen verschärfen steigende Vorfalldaten, höhere Sicherheitsausgaben und ein nach wie vor geringes Vertrauen in den Führungsetagen das Problem. Unternehmen und Organisationen investieren möglicherweise mehr denn je, aber viele haben immer noch Schwierigkeiten, grundlegende Fragen zu ihrem Risiko, ihrer Resilienz und ihren Investitionsergebnissen zu beantworten.

Diese Lücke bietet Managed Service Providern (MSPs) und anderen Channel-Experten eine große Chance, über die reine Bereitstellung hinauszugehen und zu Cyber-Leadern des Vertrauens zu werden. Die Forschungsergebnisse in diesem Report zeigen, dass Kunden zunehmend ihre Partner um Orientierung für ihr gesamtes Cyber-Programm bitten, von der technischen Implementierung bis hin zum vollständigen Management. Die Partner, die Komplexität überschaubar machen und ihren Kunden dabei helfen, zu erkennen, wo sie stehen, wie sie sich verbessern und wo weiterhin Risiken bestehen, sind am besten aufgestellt, um diese Führungslücke zu schließen.

Um jedoch in großem Maßstab eine führende Rolle im Bereich der Cybersicherheit einzunehmen, bedarf es mehr als nur Expertise. Wie auf Seite 19 dargestellt, **schätzen MSPs, dass sie mehr als die Hälfte der Zeit ihres Team einsparen könnten**, wenn Sicherheits- und Compliance-Aktivitäten über eine einzige, einheitliche Plattform verwaltet würden. Dies unterstreicht die entscheidende Bedeutung der betrieblichen Effizienz. Um der wachsenden Kundennachfrage gerecht zu werden, benötigen Anbieter ein Modell, das ihre Maßnahmen über den gesamten Kundenstamm hinweg wiederholbar, skalierbar und messbar macht.



Scott Barlow
VP, Chief Evangelist
Sophos

¹ <https://www.sophos.com/de-de/resources/report/2026-ciso-report>

Einleitung

Der Sophos Report „Perspektiven für MSPs 2026“ konzentriert sich auf drei strategische Bereiche des MSP-Geschäfts:

- Den Aufstieg der von MSPs bereitgestellten Cyber-Führung
- Compliance als Schlüsselkomponente der MSP-Servicebereitstellung
- Operationalisierung von Sicherheit und Compliance in großem Maßstab

Die Ergebnisse basieren auf einer unabhängigen, herstellernerutralen Befragung von 800 MSPs in den USA (200), dem Vereinigten Königreich (100), Deutschland (100), Frankreich (100), Singapur (100), Australien (100) und Brasilien (100). Die Befragten repräsentieren MSP-Stakeholder von der Führungs- bis hin zur Vorstandsebene.

Die Umfrage wurde von Sophos in Auftrag gegeben und vom Marktforschungsunternehmen Vanson Bourne im April 2026 durchgeführt.

800

MSPs

7

Compliance-Bereiche im Fokus

7

Länder

Wichtigste Erkenntnisse auf einen Blick

1. MSPs sind für ihre Kunden de facto zu CISOs geworden

- **88 %** der MSPs geben an, dass mindestens **20 %** ihrer Kunden von ihnen erwarten, als ihr CISO zu fungieren.
- **84 %** der MSPs erwarten, dass die Nachfrage nach CISO-Services in den nächsten 12 Monaten steigen wird.

2. Compliance-Services sind weit verbreitet, aber nicht ausgereift

- **99 %** der MSPs bieten Compliance Services an.
- **6 %** bieten ein umfassendes Compliance-Service-Portfolio an, was noch Raum für Wachstum lässt.

3. Compliance treibt Sicherheitsinvestitionen voran

- **50 %** der Kaufentscheidungen von Kunden werden durch Compliance-Anforderungen beeinflusst.
- Dieser Einfluss ist im Durchschnitt ein wesentlicher Faktor bei **33%** der Kaufentscheidungen.

4. Der Übergang zu kontinuierlicher Compliance verläuft schrittweise

- **62 %** der MSPs sind „sehr“ zuversichtlich in Bezug auf ihre Fähigkeit, die Compliance bei mehreren Kunden kontinuierlich zu überwachen, zu verwalten und zu dokumentieren.
- **33 %** sind „komplett zuversichtlich“, was unterstreicht, dass viele von Verbesserungen profitieren würden.

5. Toolbasierte Bereitstellung ist der Standard

- **53 %** der MSPs verwenden mehrere Tools oder Plattformen, um Cybersecurity-Compliance oder CISO-ähnliche Aktivitäten zentral zu verwalten.
- **36 %** verlassen sich auf nur ein Tool, was darauf hindeutet, dass MSPs und ihre Kunden in einem Modell agieren, das komplex, fragmentiert und potenziell unvollständig ist.

6. Sicherheits-Reporting wird automatisiert

- **86 %** der MSPs verwenden einen vollständig oder teilweise automatisierten Prozess zum Erstellen konsolidierter Security Posture Reports.
- **55 %** müssen immer noch manuell eingreifen, um Aktivitäten zu konsolidieren, was darauf hindeutet, dass die meisten Reporting-Prozesse nur teilweise automatisiert sind.

7. Erhebliche Effizienzgewinne bleiben ungenutzt

- **53 %** – so viel Zeit würden MSPs einsparen, wenn sie eine einzige, einheitliche Plattform für das Sicherheitsstatus- und Compliance-Management sowie das Reporting ihrer Kunden nutzen könnten.
- **81 %** der MSPs glauben, dass dies die Zeit, die sie derzeit für diese Aktivitäten aufwenden, um mehr als **30 %** reduzieren würde.

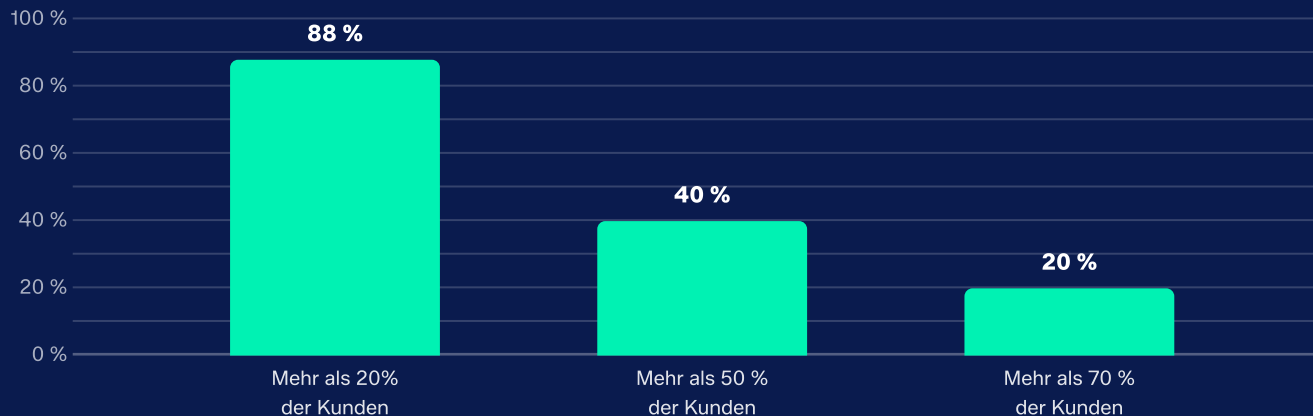
Teil 1: Der Aufstieg der von MSPs bereitgestellten Cybersecurity-Führung

1. MSPs sind für ihre Kunden de facto zum CISO geworden

Unternehmen sehen sich wachsendem Druck durch eine sich entwickelnde Bedrohungslandschaft, durch künstliche Intelligenz (KI) unterstützte Angriffe, zunehmende Vorschriften und den Mangel an Sicherheitsfachkräften gegenüber. Vielen fehlt auch die interne Führung, die erforderlich ist, um diese Herausforderungen durch ein koordiniertes Cybersecurity-Programm statt nur durch Technologiemanagement anzugehen. Als Reaktion darauf bewegen sich MSPs die Wertschöpfungskette nach oben und entwickeln sich von Anbietern taktischer Tools zu strategischen Beratungspartnern.

Die Daten des Reports zeigen, dass dieser Wandel bereits in vollem Gange ist. Im Durchschnitt schätzen MSPs, dass **46 %** ihrer Kunden sich jetzt für diese Art der Cyber-Führung auf sie verlassen. Dieses Modell ist weit verbreitet: **88 % der MSPs** fungieren für mehr als **20 %** ihres Kundenstamms als CISO, **40 %** für mehr als die Hälfte und **20 %** für mehr als **70 %**.

Kundenabhängigkeit von durch MSPs erbrachten CISO-Diensten



Wie hoch ist ungefähr der Prozentsatz Ihrer Kunden, die Ihr Unternehmen als ihren CISO einsetzen möchten, falls überhaupt? (Anzahl=800)

88 %

der MSPs fungieren für mehr als 20 % ihres Kundenstamms als CISO.

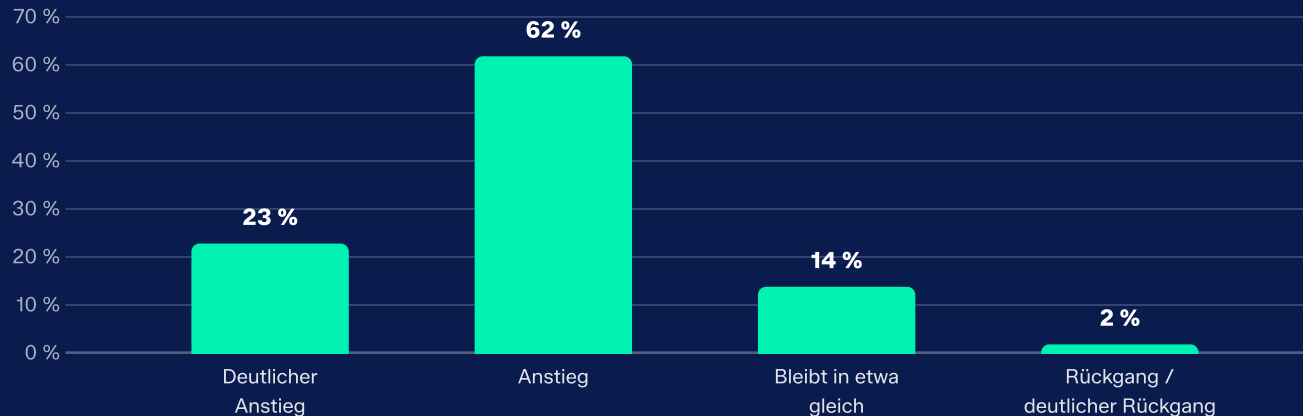
46 %

der MSP-Kunden erwarten im Durchschnitt von ihrem MSP, dass er in dieser Funktion tätig wird.

Die Nachfrage nach von MSPs bereitgestellten CISO-Services wird steigen

Diese Chance für MSPs wird weiter wachsen. **84 %** erwarten, dass die Nachfrage nach CISO-Services in den nächsten 12 Monaten steigen wird; **23 %** davon gehen von einem signifikanten Wachstum aus. Nur **2 %** erwarten einen Rückgang.

Erwartete Veränderung der Nachfrage nach CISO-Diensten



Wie wird sich dies Ihrer Erwartung nach in den nächsten 12 Monaten verändern, falls überhaupt? (Anzahl=800)

Die traditionellen Grenzen der MSP-Rolle verändern sich rapide und spiegeln die Herausforderungen wider, mit denen Unternehmen konfrontiert sind, denen es an Fachwissen, Ressourcen oder Mitteln fehlt, um eine dedizierte, interne Sicherheitsführungskraft zu unterstützen. Sie suchen nun bei ihren MSPs nach strategischer Cybersecurity-Beratung, Risikomanagement und Governance auf CISO-Ebene, die über das tägliche Technologiemanagement hinausgehen. Die Anbieter, die diese Lücke schließen und sich als erste Anlaufstelle etablieren können, sind gut positioniert, um die steigende Nachfrage zu bedienen.

84 %

der MSPs erwarten, dass die Nachfrage nach CISO-Services in den nächsten 12 Monaten steigen wird.

23 %

erwarten einen deutlichen Anstieg.

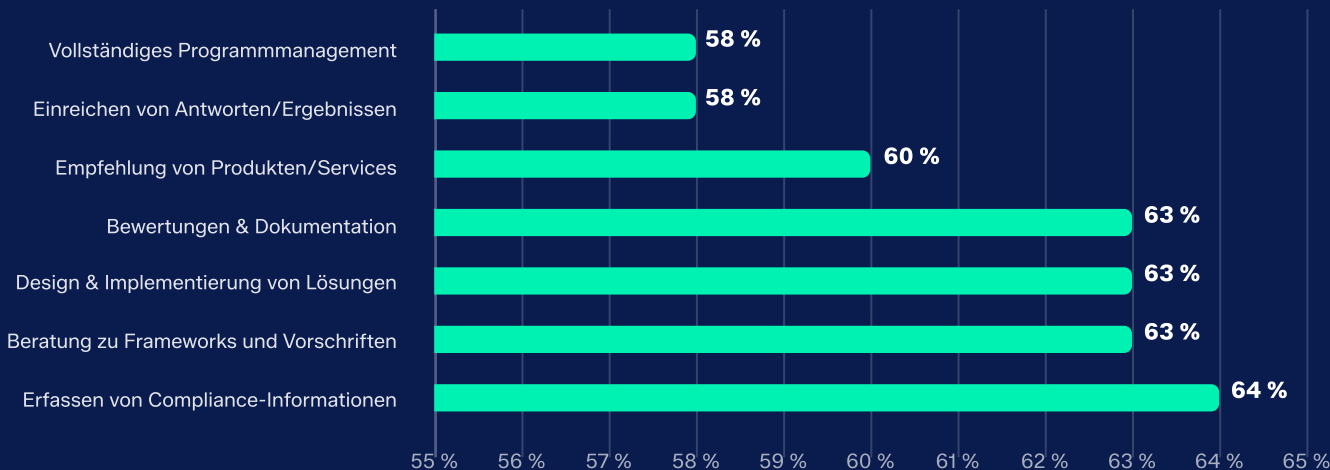
Teil 2: Compliance als Schlüsselkomponente der MSP-Servicebereitstellung

1. Compliance-Services sind weit verbreitet, aber nicht ausgereift

Cybersecurity-Compliance ist heute ein wesentlicher Bestandteil des Wertversprechens von MSPs, angetrieben durch zunehmende Vorschriften und Gesetze, die ein dediziertes, kontinuierliches Cyber Program Management erfordern. MSPs sind bestens aufgestellt, diese Serviceleistung zu erbringen.

Bei den sieben gemessenen Compliance-Aktivitäten ist die Abdeckung der Servicebereitstellung durchweg gut. Für jeden aufgeführten Servicebereich geben **58 % bis 64 % der MSPs** an, dass sie diese spezifische Serviceleistung Kunden bereits anbieten.

Prozentsatz der MSPs, die derzeit jeden der sieben Compliance-Bereiche abdecken



Welche der folgenden Aussagen beschreibt am besten das Engagement Ihres Unternehmens für die Cybersecurity-Compliance Ihrer Kunden heute und in der Zukunft? (Anzahl=800)

99 %

der MSPs bieten in gewissem Umfang Compliance-Services an.

58 %

bieten ein vollständiges Programmmanagement an.

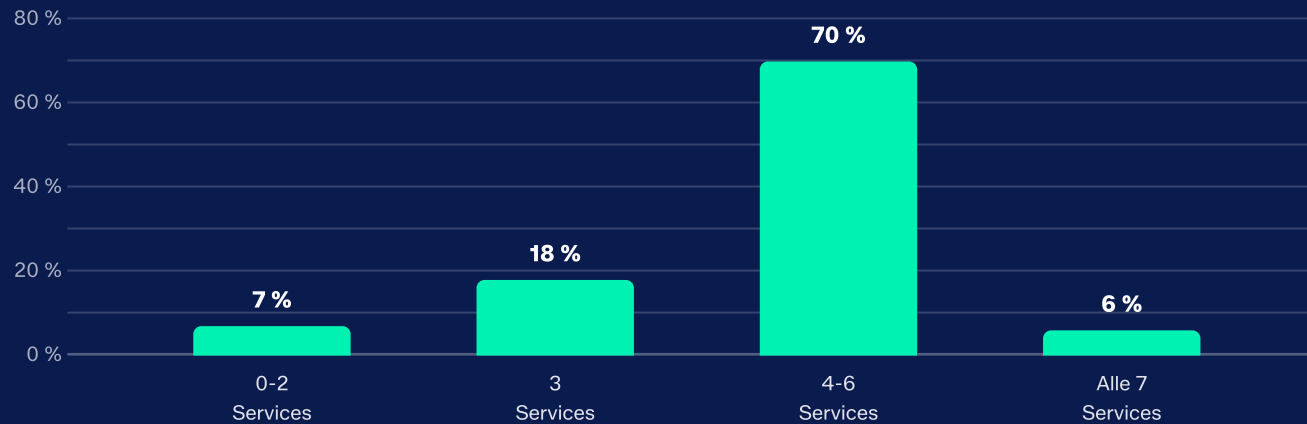
6 %

bieten ein umfassendes Compliance-Service-Portfolio an.

Nur wenige MSPs bieten die vollständige Palette an Compliance-Services an

Während einzelne Compliance-Services weit verbreitet sind, bieten die meisten MSPs nicht den vollständigen Compliance-Lebenszyklus an: **70 %** bieten zwischen vier und sechs der sieben gemessenen Aktivitäten an, nur **6 %** haben alle sieben im Angebot. Dies deutet darauf hin, dass viele MSPs ihr Angebot noch erweitern und diese Funktionen zu einem End-to-End-Compliance-Programm verbinden müssen, das die umfassende Überwachung bietet, die Kunden benötigen.

Umfang der angebotenen Compliance-Services

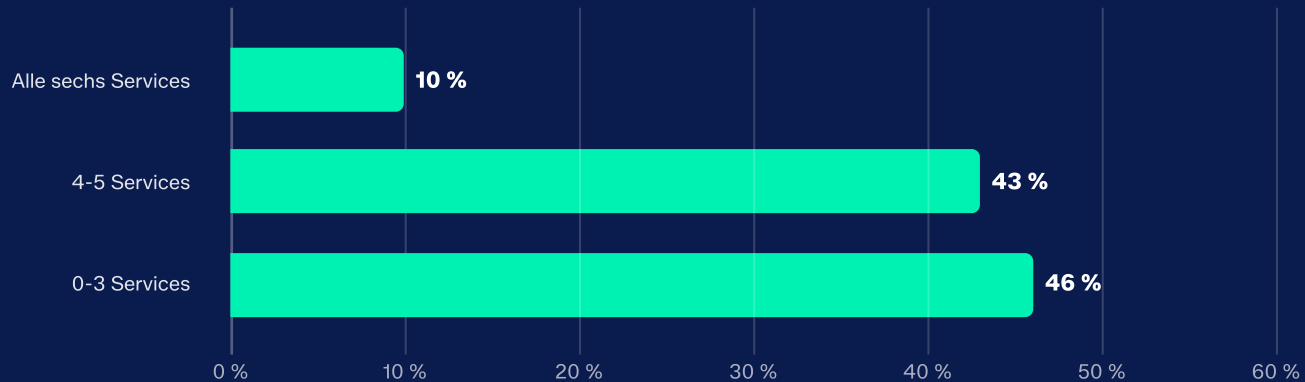


Welche der folgenden Aussagen beschreibt am besten das Engagement Ihres Unternehmens für die Cybersecurity-Compliance Ihrer Kunden heute und in der Zukunft? (Anzahl=800)

Viele MSPs, die Compliance-Programmmanagement anbieten, bieten nicht alle unterstützenden Services an

Ein Blick speziell auf MSPs, die das vollständige Compliance-Programm ihrer Kunden verwalten, offenbart eine ähnliche Lücke. Von den **58 % der MSPs**, die dies tun, stellen nur **10 %** auch die anderen sechs Services bereit. Dies deutet darauf hin, dass viele MSPs Verantwortung auf Programmebene übernehmen, bevor sie ein umfassendes Compliance-Service-Portfolio aufbauen. In der Praxis kann Compliance-Programmmanagement darin bestehen, die von Kunden oder externen Fachleuten durchgeführten Aktivitäten zu koordinieren, anstatt jede Serviceleistung direkt selbst zu erbringen. Infolgedessen gehen Programmüberwachung und Servicebereitstellungsfähigkeit nicht immer Hand in Hand.

Anzahl der von MSPs mit vollständigem Programmmanagement erbrachten Compliance-Dienste



Welche der folgenden Aussagen beschreibt am besten das Engagement Ihres Unternehmens für die Cybersecurity-Compliance Ihrer Kunden heute und in der Zukunft? MSPs, die ein vollständiges Compliance-Programmmanagement anbieten (Anzahl=465)

MSPs planen, ihr Compliance-Angebot auszubauen

Die gute Nachricht ist, dass die Nachfrage nach diesen Serviceleistungen wahrscheinlich zu einer weiteren Expansion führen wird. Viele MSPs, die derzeit keine Compliance-Services anbieten, planen, diese in Zukunft einzuführen. Das stärkste Wachstum wird im Bereich des umfassenden Compliance-Programmmanagements erwartet: Zusätzlich zu den 58 %, die diese Serviceleistung bereits anbieten, planen weitere 40 %, sie einzuführen. Dies deutet darauf hin, dass sich das Compliance-Programmmanagement schnell zu einem Standardbestandteil von MSP-Compliance-Angeboten entwickelt.

SERVICE	DERZEIT IM ANGEBOT	GEPLANTE EINFÜHRUNG	GESAMT
Empfehlung von Produkten/Services Beratung zu Sicherheitstools und -services, die Compliance-Ziele unterstützen.	60 %	38 %	99 %
Design & Implementierung von Lösungen Konfiguration und Bereitstellung von Sicherheitskontrollen zum effektiven Erfüllen von Compliance-Anforderungen.	63 %	37 %	100 %
Frameworks & Vorschriften Identifizierung anwendbarer Vorschriften, Standards und Frameworks, die die Compliance der Kunden betreffen.	63 %	36 %	99 %
Erfassen von Compliance-Informationen Bereitstellen von Nachweisen, die Kunden zum Erfüllen ihrer Compliance-Verpflichtungen benötigen.	64 %	35 %	99 %
Bewertungen & Dokumentation Durchführen von Assessments und Erstellen von Dokumentation, die den Compliance-Status und Lücken aufzeigt.	63 %	36 %	98 %
Einreichen von Antworten/Ergebnissen Erstellen und Einreichen von Antworten auf Audit-Anfragen, Fragebögen und Nachweisen zur Einhaltung der Vorschriften.	58 %	40 %	98 %
Vollständiges Programmmanagement Beaufsichtigen laufender Compliance-Aktivitäten, Erfassen von Nachweisen, Reporting und Governance.	58 %	40 %	99 %

Welche der folgenden Aussagen beschreibt am besten das Engagement Ihres Unternehmens für die Cybersecurity-Compliance Ihrer Kunden heute und in der Zukunft? „Weiß nicht“ nicht berücksichtigt (Anzahl=800)

Prozentsätze sind gerundet.

Compliance-Services sind ein Wachstumsbereich für MSPs jeder Größe

Die Reife des Compliance-Angebots von MSPs wird nicht durch deren Größe definiert. Während MSPs mit mehr als 51 Mitarbeitenden am ehesten alle sieben gemessenen Compliance-Services anbieten (**10 %**), sind kleinere MSPs dennoch wettbewerbsfähig. Diejenigen mit bis zu fünf Mitarbeitenden bieten mit höherer Wahrscheinlichkeit vier bis sechs der sieben Compliance-Services an (**77 %**) als jede andere Gruppe und melden die höchste durchschnittliche Anzahl der erbrachten Compliance-Services.

Die Einführung des vollständigen Compliance-Programmanagements ist ebenfalls relativ konsistent und reicht von **54 % bis 62 %**. Dies deutet darauf hin, dass Compliance für MSPs jeder Größe zu einem Wachstumsbereich wird, wobei sich der Wettbewerb von der Service-Verfügbarkeit hin zu Bereitstellungsgeschwindigkeit, Tiefe und Reife verlagert.

MSP-GRÖSSE	0-2 SERVICES	3 SERVICES	4-6 SERVICES	ALLE SIEBEN SERVICES	DURCHSCHNITTliche ANZAHL VON SERVICES	VOLLSTÄNDIGES PROGRAMMANAGEMENT
1-5 Mitarbeitende	5 %	11 %	77 %	7 %	5	62 %
6-25 Mitarbeitende	8 %	25 %	65 %	2 %	4	54 %
26-50 Mitarbeitende	8 %	17 %	70 %	6 %	4	59 %
51 und mehr Mitarbeitende	5 %	17 %	69 %	10 %	4	59 %

Prozentsätze sind gerundet.

Welche der folgenden Aussagen beschreibt am besten das Engagement Ihres Unternehmens für die Cybersecurity-Compliance Ihrer Kunden heute und in der Zukunft? „Weiß nicht“ nicht berücksichtigt (Anzahl=800)

MSPs haben beim Aufbau von Compliance-Praktiken erhebliche Fortschritte gemacht; fast alle Anbieter bieten inzwischen mindestens einen Compliance-Service an, und die Mehrheit liefert mehrere Funktionen über den gesamten Compliance-Lebenszyklus hinweg. Ein vollständiges Compliance-Programmanagement wird zum Mainstream und ist auf dem besten Weg, ein nahezu universelles Angebot zu werden, was die wachsende Kundennachfrage nach laufender Compliance-Unterstützung widerspiegelt.

Die Bandbreite des Service-Angebots sollte jedoch nicht mit der Reife verwechselt werden. Während viele MSPs ihr Angebot über grundlegende Advisory Services hinaus erweitert haben, haben relativ wenige ein wirklich vollständiges Compliance-Angebot entwickelt. Die meisten arbeiten weiterhin mit lückenhaften Service-Portfolios. Selbst unter denjenigen, die ein vollständiges Compliance-Programmanagement anbieten, erbringt nur eine kleine Minderheit die vollständige Palette an unterstützenden Compliance-Services.

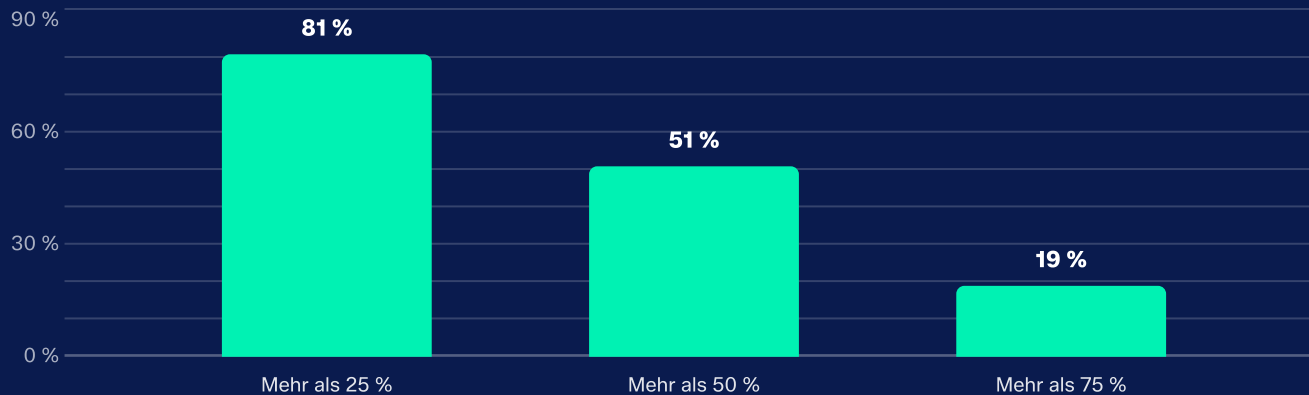
Da Compliance-Services immer breiter verfügbar werden, wird der Wettbewerbsvorteil zunehmend von der Geschwindigkeit, Tiefe, Qualität und Nahtlosigkeit der Bereitstellung abhängen und nicht mehr allein von der Bereitstellung selbst. **MSPs, die Advisory Services, Implementierung, Dokumentation, Reporting und Programmanagement zu einer kohärenten Compliance-Praxis verbinden können, werden am besten positioniert sein, um sich als Marktführer zu etablieren.**

2. Compliance treibt Sicherheitsinvestitionen voran

Compliance ist mittlerweile ein bedeutender Treiber für Cybersecurity-Investitionen. MSPs geben an, dass Compliance die Cybersecurity-Käufe von Kunden durchschnittlich zu **50 %** beeinflusst, wobei **33 %** der Entscheidungen „stark“ oder „maßgeblich“ geprägt sind. Dieser Einfluss ist weit verbreitet: **81 % der MSPs** geben an, dass Compliance-Anforderungen mindestens **25 %** der Kundenkäufe beeinflussen, und **51 %** sagen, dass sie mindestens die Hälfte davon beeinflussen. Mit anderen Worten: Compliance ist nicht mehr nur eine Reporting-Anforderung, sondern beeinflusst aktiv, wie Kunden ihre Sicherheitsausgaben priorisieren.

Die Chance besteht nun darin, diesen Einfluss strategischer zu gestalten. Nur **9 %** der MSPs geben an, dass Compliance einen signifikanten Großteil (**75 %**) der kundenseitigen Cybersecurity-Käufe „stark“ oder „maßgeblich“ beeinflusst. Dies bietet MSPs Spielraum, Compliance als Einstieg in umfassendere Beratungsgespräche, tiefgreifendere Services und strukturierte Sicherheitsprogramme zu nutzen.

Anteil der Kaufentscheidungen, die von Compliance beeinflusst werden



Wie viel Prozent der Cybersecurity-Kaufentscheidungen Ihrer Kunden werden zumindest teilweise durch regulatorische Compliance-Anforderungen beeinflusst, falls überhaupt? (Anzahl=800)

50 %

der Kaufentscheidungen von Kunden werden durch Compliance-Anforderungen beeinflusst.

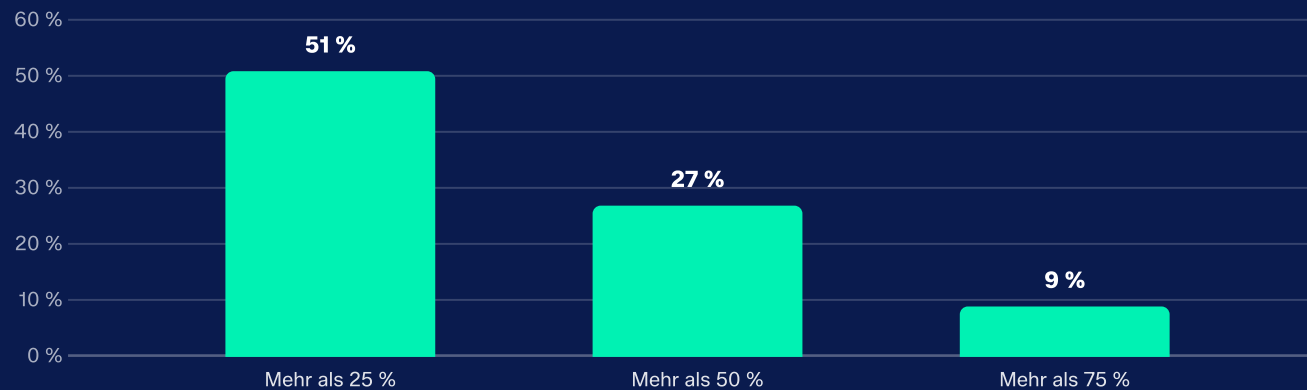
33 %

dieser Entscheidungen werden stark von regulatorischen Compliance-Anforderungen beeinflusst.

MSPs können die Compliance ihrer Kunden nutzen, um strategische Gespräche zu führen

Zusammengenommen zeigen die Ergebnisse, dass sich Compliance von einer regulatorischen Verpflichtung zu einem wichtigen Geschäftstreiber entwickelt. Sie hat bereits einen klaren Einfluss auf die Sicherheitsausgaben der Kunden. Allerdings haben bislang nur wenige MSPs das Thema Compliance als lukrativen Einstieg in weitreichendere Cybersecurity-Gespräche genutzt. Dies bietet ihnen Raum, die Lücke zu füllen und die durch Compliance gesteuerte Nachfrage in tiefere Beratungsbeziehungen und höherwertige strategische Services umzuwandeln.

Anteil der Kaufentscheidungen, die „stark“ oder „maßgeblich“ von Compliance beeinflusst werden

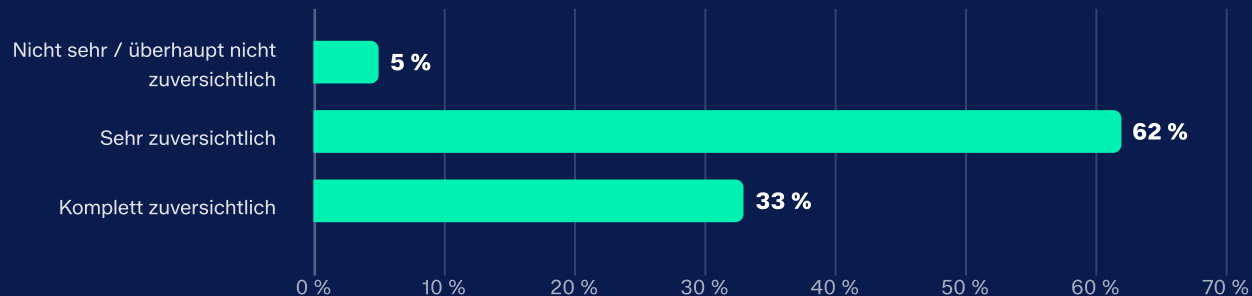


Wie viel Prozent der Cybersecurity-Kaufentscheidungen Ihrer Kunden werden stark oder maßgeblich durch regulatorische Compliance-Anforderungen beeinflusst? (n=800)

3. Der Übergang zu kontinuierlicher Compliance verläuft schrittweise

MSPs verfolgen zunehmend einen kontinuierlichen Ansatz beim Compliance-Management. Der Grad an Zuversicht deutet darauf hin, dass die meisten Anbieter glauben, gut gerüstet zu sein, um Kunden zu unterstützen, während sich die Compliance von periodischen Audits hin zu laufender Überwachung und Governance verlagert. Insgesamt sind **95 % der MSPs** entweder „sehr“ oder „komplett“ zuversichtlich in Bezug auf ihre Fähigkeit, die Compliance bei mehreren Kunden kontinuierlich zu überwachen, zu verwalten und zu dokumentieren.

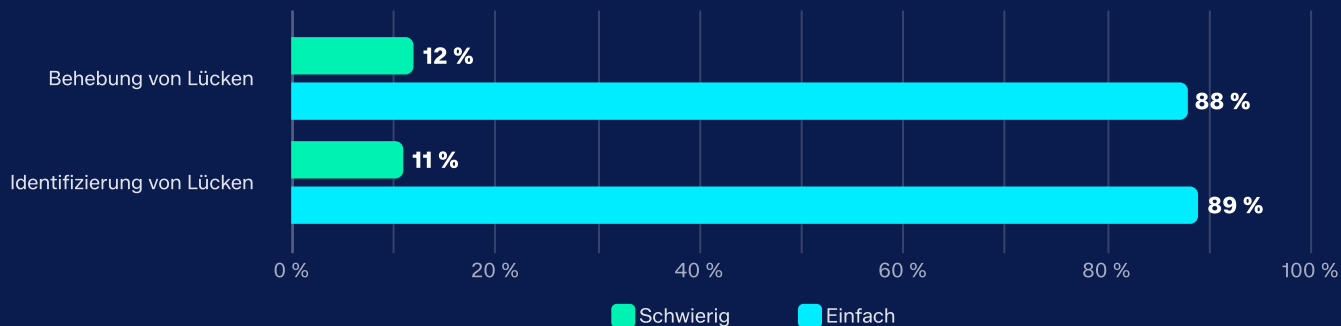
Zuversicht von MSPs bei der Verwaltung kontinuierlicher Compliance



Wie zuversichtlich sind Sie, dass Ihr Unternehmen derzeit in der Lage ist, Compliance-Anforderungen für mehrere Kunden kontinuierlich zu überwachen, zu verwalten und zu dokumentieren – sofern dies überhaupt der Fall ist? (Anzahl=800)

Dieses Vertrauen spiegelt sich auch darin wider, wie gut MSPs in der Lage sind, Compliance- und Kontrolllücken für ihre Kunden zu identifizieren und zu beheben, wobei nur eine kleine Minderheit von Schwierigkeiten bei beidem berichtet.

MSPs: Aufwand zur Identifizierung und Behebung von Compliance- und Kontrolllücken



Wie einfach oder schwierig ist es für Ihr Unternehmen heute, Compliance- oder Kontrolllücken für Ihre Kunden zu identifizieren und zu beheben? (Anzahl=800)

62 %

der MSPs sind „sehr zuversichtlich“ in Bezug auf ihre Fähigkeit, die Compliance bei mehreren Kunden kontinuierlich zu überwachen, zu verwalten und zu dokumentieren.

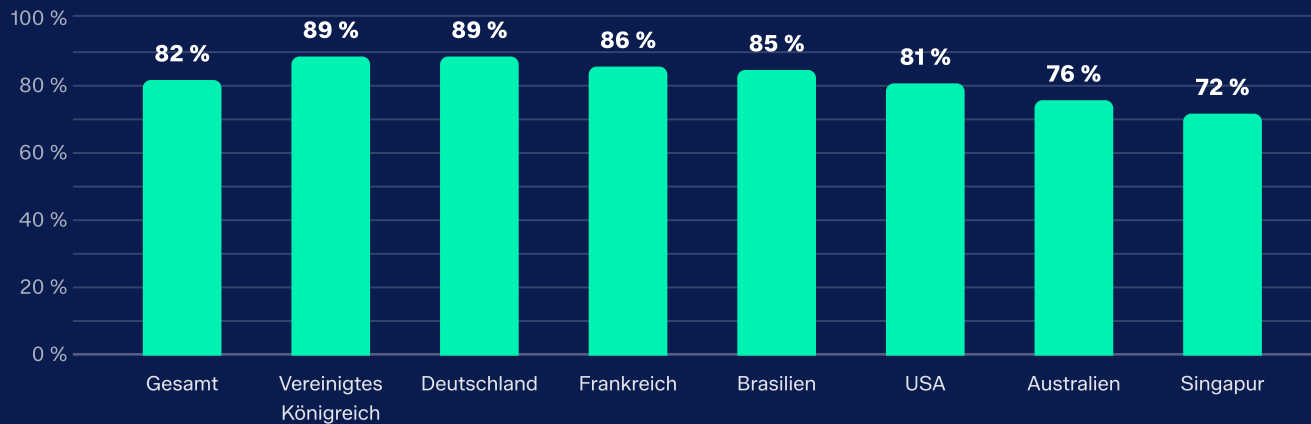
33 %

sind „komplett zuversichtlich“, was ihre Fähigkeiten angeht.

Die Zuversicht in die Fähigkeiten zur Verwaltung von Compliance- und Kontrolllücken variiert nach Land

Während die Verwaltung von Compliance- und Kontrolllücken für die meisten MSPs eine etablierte Serviceleistung ist, variiert die Zuversicht je nach Land. MSPs im Vereinigten Königreich und in Deutschland geben an, dass sie diese am ehesten sowohl leicht identifizieren als auch beheben können (**89 %**), verglichen mit **81 %** in den USA, **76 %** in Australien und **72 %** in Singapur. Diese Unterschiede deuten darauf hin, dass zwar viele Anbieter über operative Prozesse verfügen, die praktische Herausforderung, die Compliance aufrechtzuerhalten und Risiken zu reduzieren, jedoch in einigen Märkten größer ist als in anderen.

Der Aufwand zur Identifizierung und Behebung von Compliance-Lücken variiert je nach Land



Wie einfach oder schwierig ist es für Ihr Unternehmen heute, Compliance- oder Kontrolllücken für Ihre Kunden zu identifizieren und zu beheben? (Anzahl=800)

MSPs aller Größen sind zuversichtlich in Bezug auf ihre Fähigkeit, die Compliance ihrer Kunden kontinuierlich zu verwalten

Der Grad an Zuversicht ist bei MSPs aller Größen bemerkenswert konsistent. Kleinere Anbieter berichten von der höchsten Gesamtzuversicht, wobei **98 % der MSPs** mit 1–5 Mitarbeitenden angeben, „komplett“ oder „sehr“ zuversichtlich in Bezug auf ihre Fähigkeit zu sein, kontinuierliche Compliance zu verwalten, verglichen mit **92 %** der MSPs mit 51 oder mehr Mitarbeitenden. Die komplette Zuversicht bleibt in allen Größenklassen deutlich geringer und reicht von **30 % bis 36 %**. Die Lücke zwischen hoher Zuversicht und absoluter Gewissheit deutet darauf hin, dass sich zwar kontinuierliche Compliance-Fähigkeiten in der MSP-Community etablieren, viele Anbieter jedoch von Verbesserungen ihres aktuellen Modells profitieren würden.

ZUVERSICHT BEI DER VERWALTUNG KONTINUIERLICHER COMPLIANCE	GESAMT	1–5 MITARBEITENDE	6–25 MITARBEITENDE	26–50 MITARBEITENDE	51+ MITARBEITENDE
Komplett zuversichtlich	33 %	36 %	34 %	30 %	31 %
Sehr zuversichtlich	62 %	62 %	62 %	65 %	60 %
Nicht sehr zuversichtlich	4 %	2 %	4 %	5 %	7 %
Überhaupt nicht zuversichtlich	0 %	0 %	0 %	1 %	1 %
Komplett oder sehr	95 %	98 %	In 96 %	95 %	92 %

Wie zuversichtlich sind Sie, dass Ihr Unternehmen derzeit in der Lage ist, Compliance-Anforderungen für mehrere Kunden kontinuierlich zu überwachen, zu verwalten und zu dokumentieren – sofern dies überhaupt der Fall ist? (Anzahl=800)

Cyberresilienz hängt vom fortlaufenden Nachweis der Compliance ab und nicht von periodischen Zusicherungen. Für Kunden bedeutet das einen klaren Nachweis, dass Kontrollen funktionieren, Lücken aufgedeckt werden und im Laufe der Zeit Verbesserungen vorgenommen werden. Die Zuversicht der MSPs zeigt, dass sich diese Fähigkeit eindeutig entwickelt, aber das Fehlen absoluter Gewissheit unterstreicht sowohl Chancen als auch Risiken. Anbieter, die diese Lücke schließen und konsistente, skalierbare und wiederholbare Compliance-Services anbieten können, sind hervorragend positioniert, um in höherwertige Governance-Services zu expandieren. Diejenigen, denen dies nicht gelingt, könnten Schwierigkeiten haben, das Maß an Sicherheit zu bieten, das Kunden benötigen, während Bedrohungen, Vorschriften und Geschäftsrisiken weiter zunehmen.

Teil 3: Operationalisierung von Sicherheit und Compliance im großen Maßstab

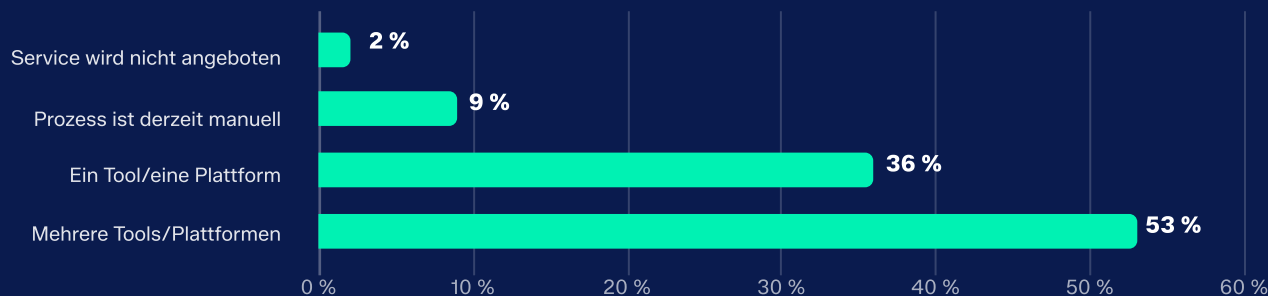
1. Toolbasierte Bereitstellung ist der Standard

Da MSPs ihre Rolle bei der Cybersecurity-Compliance und bei strategischen Advisory Services ausbauen, ist die toolbasierte Bereitstellung zur Standardpraxis geworden. **89 % der MSPs** nutzen heute ein oder mehrere Tools bzw. Plattformen, um Compliance- oder CISO-ähnliche Aktivitäten über ihren gesamten Kundenstamm hinweg zentral zu verwalten. Nur **9 %** verlassen sich weiterhin auf rein manuelle Prozesse, während **2 %** diese Compliance-Services überhaupt nicht anbieten.

Die Einführung dieser operativen Technologien hat nicht zu einer flächendeckenden Konsolidierung geführt. Mehr MSPs nutzen mehrere Tools oder Plattformen (**53 %**) als eine einzige Lösung (**36 %**), was darauf hindeutet, dass viele diese Services über eine Sammlung spezialisierter Plattformen bereitstellen, anstatt über ein einziges, einheitliches System.

Dies spiegelt möglicherweise die wachsende Komplexität bei der Verwaltung von Compliance-Anforderungen, Risikobewertungen, Reporting, Governance-Aktivitäten und Kundenkommunikation im großen Maßstab wider. Zudem wird auch eine häufige Herausforderung offensichtlich: Viele Tools können keine Daten in eine zentrale Reporting-Plattform einspeisen, sodass manuell Maßnahmen ergriffen werden müssen, um die Aktivitäten in einem einzigen, kundenorientierten Report zusammenzufassen. Die Ergebnisse deuten auf eine wachsende Nachfrage nach einheitlicheren Ansätzen für die Verwaltung und Berichterstattung von Compliance-Programmen hin.

Plattformansatz für die Bereitstellung von Compliance-/CISO-Services



Welchen Ansatz verfolgt Ihr Unternehmen derzeit bei der Bereitstellung von Cybersecurity-Compliance oder CISO-ähnlichen Aktivitäten für Ihren Kundenstamm? (n=800)

53 %

der MSPs verwenden mehrere Tools oder Plattformen, um Cybersecurity-Compliance oder CISO-ähnliche Aktivitäten zentral zu verwalten.

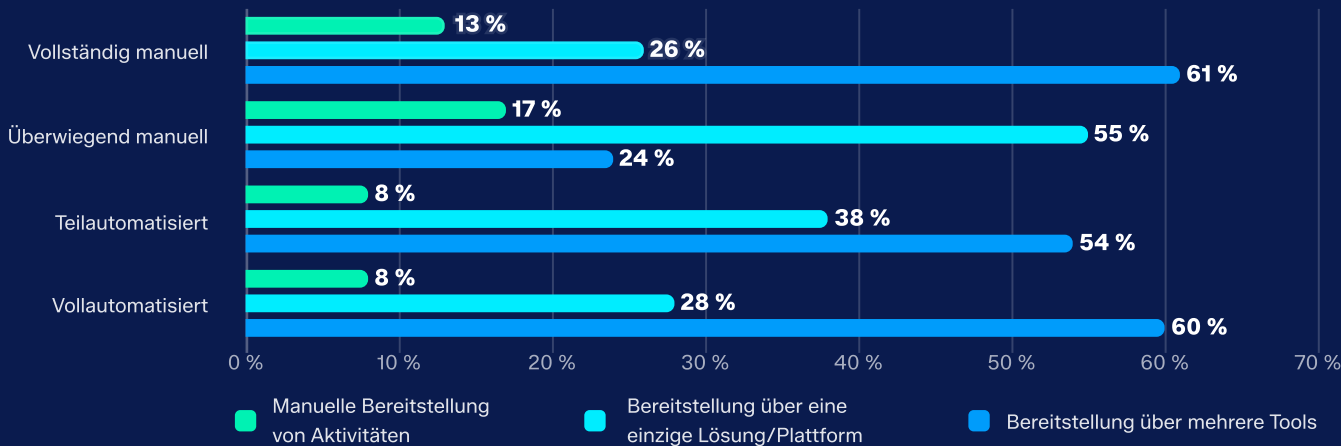
36 %

der MSPs verlassen sich auf nur ein Tool oder eine Plattform

2. Sicherheits-Reporting wird automatisiert

Die meisten MSPs haben sich von vollständig manuellen Reporting-Prozessen verabschiedet, wobei **86 %** entweder vollständig automatisierte oder teilautomatisierte Methoden verwenden, um konsolidierte Security Posture Reports zu erstellen. Eine vollständige Automatisierung ist jedoch noch nicht zum Standard geworden. Nur **31 % der MSPs** können Reports schnell über einen vollständig automatisierten Prozess erstellen, während **55 %** immer noch manuell eingreifen müssen, um Daten zu kombinieren, Kontext hinzuzufügen und Reports fertigzustellen.

Automatisierungsgrad des Reportings je nach Bereitstellungsmodell



Welchen Ansatz verfolgt Ihr Unternehmen derzeit bei der Bereitstellung von Cybersecurity-Compliance oder CISO-ähnlichen Aktivitäten für Ihren Kundenstamm im Vergleich dazu, wie automatisiert der Prozess Ihres Unternehmens zur Erstellung konsolidierter Security Posture Reports für Kunden ist, die den Cybersecurity-Status, Risiken und Empfehlungen aufzeigen? (Anzahl=800)

Dies zeigt, dass eine Plattformstrategie allein nicht gleichbedeutend mit Automatisierungsreife ist; MSPs auf allen Automatisierungsstufen verwenden mehrere Tools, was auf Prozessfragmentierung oder das Vorhandensein von mehr automatisierten Workflows über ein breiteres Toolset zurückzuführen sein könnte. So oder so ist der Bedarf an Automatisierung und der Wert, den sie für MSPs schaffen kann, weit verbreitet.

86 %

der MSPs verwenden einen vollständig oder teilweise automatisierten Prozess zum Erstellen konsolidierter Security Posture Reports.

31 %

können Reports mit Unterstützung von Automatisierung schnell erstellen.

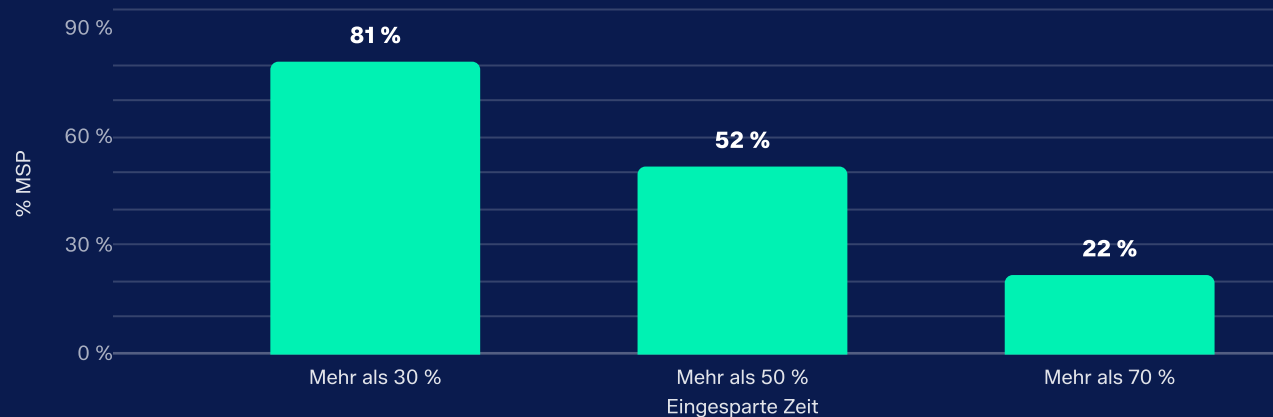
55 %

müssen noch manuell eingreifen, um Aktivitäten zu konsolidieren.

3. Erhebliche Effizienzgewinne bleiben ungenutzt

Eine Plattformkonsolidierung könnte MSPs erhebliche Effizienzgewinne eröffnen. Im Durchschnitt schätzen MSPs, dass eine einzige, vollständig vereinheitlichte Plattform die Zeit, die ihre Teams für die Verwaltung und Report-Erstellung zum Sicherheitsstatus und zur Compliance ihrer Kunden aufwenden, um **53 %** reduzieren könnte. Insgesamt **81 % der MSPs** erwarten Zeiteinsparungen von mehr als **30 %**, 52 % mehr als 50 % und 22 % mehr als 70 %.

Geschätzte Zeitersparnis durch eine einheitliche Plattform



Wie viel Zeit könnte Ihr Team einsparen, wenn das gesamte Sicherheitsstatus- und Compliance-Management sowie das Reporting für alle Kunden über eine einzige, vollständig integrierte Plattform abgewickelt würden? (n=800)

Die wahrgenommenen Einsparungen sind besonders hoch bei MSPs, die bereits ein vollständiges Compliance-Programmanagement anbieten; **84 % der MSPs** mit diesem Angebot geben an, dass sie mehr als **30 %** an Zeitersparnis erzielen könnten, verglichen mit **64 %** bei MSPs, die diesen Service weder anbieten noch planen anzubieten. Dies deutet darauf hin, dass diejenigen, die umfassendere oder integrierte Compliance-Aktivitäten verwalten, am meisten von einer Plattformkonsolidierung profitieren könnten.

Diese Ergebnisse unterstreichen die operative Belastung, mit der viele MSPs bei der Verwaltung von Reporting-, Compliance- und Advisory-Services über mehrere Plattformen und Workflows hinweg nach wie vor konfrontiert sind. Da die Nachfrage nach höherwertigen Services wie Compliance-Management und CISO-Beratung wächst, wird es immer wichtiger, Wege zu finden, das Cyber Program Management skalierbar neu zu strukturieren.

Die Ergebnisse deuten darauf hin, dass MSPs einen erheblichen Mehrwert darin sehen, ein einheitliches Modell zur Zusammenführung des gesamten Compliance-Programms zu nutzen. So müssen ihre Teams weniger Zeit für die Konsolidierung von Informationen aufwenden und können sich stattdessen stärker auf das Erzielen strategischer Ergebnisse für ihre Kunden konzentrieren.

53 %

so viel Zeit würden MSPs einsparen, wenn Sicherheitsstatus- und Compliance-Management sowie Reporting-Aktivitäten über eine einzige, einheitliche Plattform abgewickelt würden.

81 %

der MSPs geben an, dass ein einheitlicher Ansatz mehr als 30 % der Zeit ihres Teams einsparen würde.

22 %

geben an, dass sie mehr als 70 % dieser Zeit einsparen würden.

Fazit

Die MSP-Landschaft durchlebt einen bedeutenden Wandel. Kunden erwarten zunehmend von ihren Anbietern, dass sie neben Technologiemanagement auch eine strategische Cybersecurity-Führung bieten. MSPs reagieren darauf, indem sie ihr Angebot auf Compliance-Management, Cyber Advisory Services und andere CISO-ähnliche Rollen ausweiten. Da **84 % der befragten MSPs im nächsten Jahr eine steigende Nachfrage nach CISO-Services erwarten**, stellen diese höherwertigen Services eine wachsende Chance für Geschäftswachstum und Differenzierung dar.

Gleichzeitig bleibt die Verwaltung von Sicherheitsstatus, Compliance und Kunden-Reporting in großem Maßstab eine betriebliche Herausforderung. Während die meisten MSPs Plattformen und automatisierte Prozesse eingeführt haben, verlassen sich viele immer noch auf mehrere Tools und manuelle Arbeit, um diese Dienste bereitzustellen. In vielerlei Hinsicht spiegelt dies die Komplexität wider, mit der CISOs und Sicherheitsteams konfrontiert sind, was dazu führt, dass MSPs mit denselben Herausforderungen kämpfen, bei deren Bewältigung sie ihre Kunden unterstützen wollen.

MSPs, die skalierbare Cybersecurity-Führung, kontinuierliches Programmmanagement und messbare Sicherheitsergebnisse zuverlässig und effizient bereitstellen können, sind am besten positioniert, um Kundenbeziehungen zu stärken, den Umsatz zu steigern und von den nächsten großen Chancen zu profitieren.

Sophos CISO Advantage

[Sophos CISO Advantage](#) bietet MSPs die Möglichkeit, effektivere Cybersecurity-Gespräche anzustoßen: Gespräche, die sich auf Ergebnisse, Geschäftsrisiken, progressive Compliance und messbare Verbesserungen konzentrieren.

Bereitgestellt über [Sophos Fusion](#) – das KI-native Cybersecurity-Abwehrsystem von Sophos – wandelt Sophos CISO Advantage die CISO-Rolle, die die meisten MSPs bereits anbieten, in einen strukturierten, skalierbaren und abrechenbaren Service für Cyber Program Management um.

Durch agentische KI beschleunigte Workflows für Assessments, Reporting und Roadmaps ermöglichen es diesen wichtigen Partnern, ihrer gesamten Kundenbasis auf wiederholbare Weise vorlagefertige Erkenntnisse für die Geschäftsleistung, auf Frameworks basierende Nachweise und priorisierte Maßnahmenpläne bereitzustellen.

Sophos CISO Advantage schafft zudem einen klaren Weg zu neuen wiederkehrenden Umsätzen, Wachstumschancen und stärkeren Kundenbeziehungen innerhalb bestehender Projekte. Jedes Assessment deckt Sicherheitslücken auf, und jede Lücke eröffnet einen Weg zur Verbesserung, wodurch MSPs in die Lage versetzt werden, Folge-Lösungen bereitzustellen.

Sophos CISO Advantage reagiert auf eine Nachfrage, die die Sicherheits-Community seit Jahren hervorhebt. Durch die frühzeitige Einführung können MSPs vollständig in die Führungsrolle schlüpfen, die ihre Kunden offensichtlich von ihnen erwarten.

Weitere Informationen zu Sophos CISO Advantage finden MSPs im [Partner-Portal](#).

Möchten Sie Sophos-Partner
werden? [Hier registrieren.](#)

Sales DACH (Deutschland, Österreich, Schweiz)

Tel.: +49 611 58580

E-Mail: sales@sophos.de