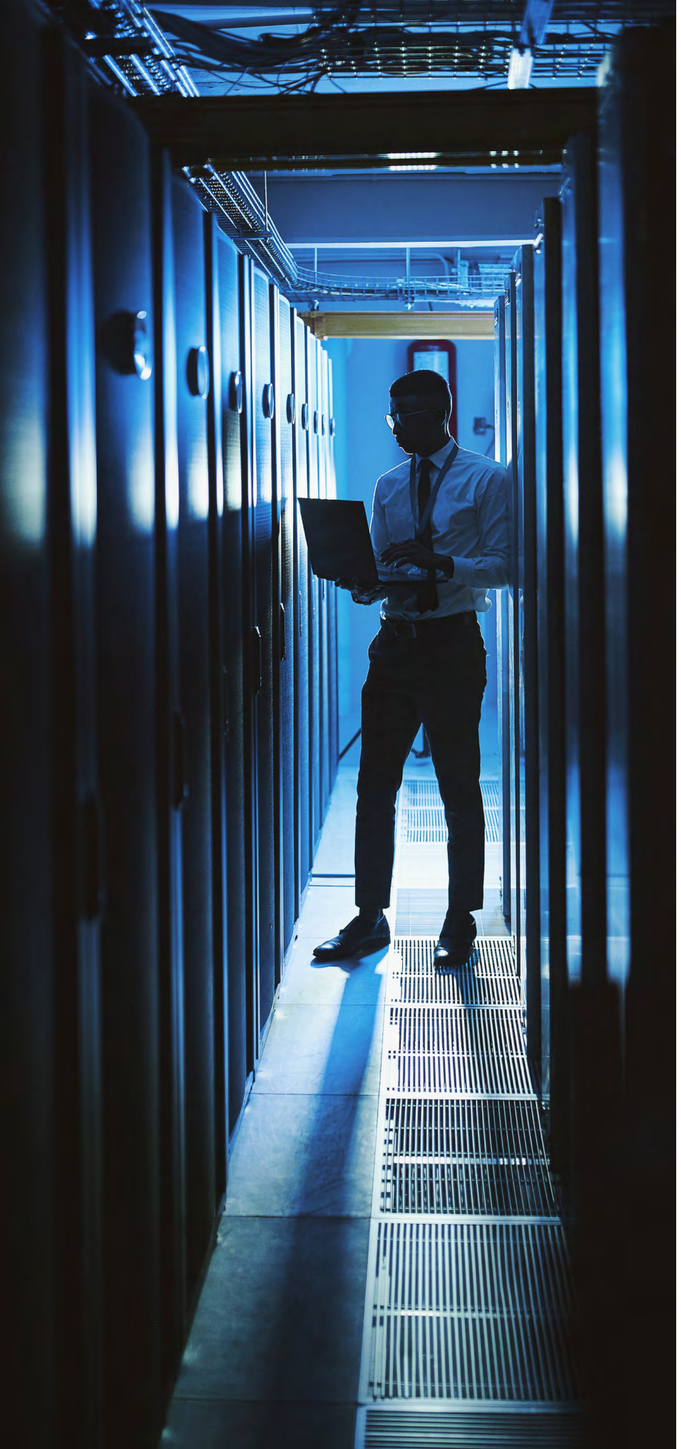
Enterprise Strategy Group | Getting to the bigger truth.™

Was sich Sicherheitsteams von MDR-Anbietern wünschen

Dave Gruber, Principal Analyst

SEPTEMBER 2022



Ziele der Studie

Die Nutzung von MDR-Services (Managed Detection and Response) ist zu einer Mainstreamstrategie bei modernen Sicherheitsprogrammen geworden. IT-Abteilungen sollten sich jedoch nicht vom Namen täuschen lassen: MDR-Anbieter bieten weit mehr als nur grundlegende Erkennung und Reaktion. Sie unterstützen IT- und Sicherheitsführungskräfte dabei, die Programmentwicklung zu beschleunigen und ihren Sicherheitsstatus zu verbessern. Mit MDR-Services profitieren Unternehmen angesichts der Tatsache, dass kein Ende des Mangels an Cybersicherheitskompetenzen in Sicht ist, von einer sofortigen Bereitstellung von Expertenressourcen – zusammen mit bewährten Best-of-Breed-Prozessen und -Tools, die Sicherheitsteams dabei unterstützen können, die Kontrolle zu gewinnen und den Erfolg des künftigen Sicherheitsprogramms sicherzustellen.

ESG hat 373 CybersicherheitsexpertInnen befragt, die persönlich mit Cybersicherheitstechnologie, einschließlich Produkten und Services sowie Prozessen, zu tun haben, um die Trends zu verstehen und den allgemeinen Status der Managed Detection and Response Service-Angebote zu bewerten.

DIESE STUDIE HATTE FOLGENDE ZIELE:

Ermitteln, wie, wo und warum MDR-Services zur Unterstützung von Sicherheitsprogrammen verwendet werden

Gewinnen von Einblicken in die wichtigsten Faktoren für den IT-Betrieb, LOB-Führungskräfte und EndnutzerInnen

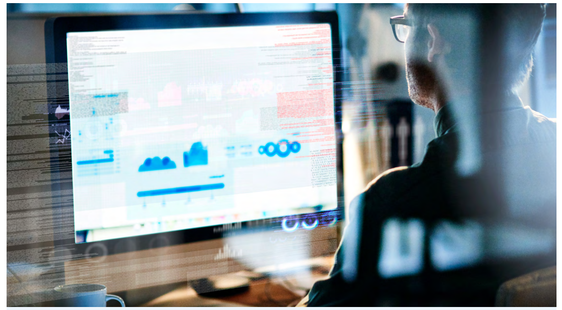
Isolieren spezifischer MDR-Anwendungsbeispiele und der Profile von Unternehmen, die diese nutzen

Herausfinden, welche Megatrends in der Branche die MDR-Anbieterauswahl beeinflussen

ZURÜCK ZUM INHALT

DIE WICHTIGSTEN **ERKENNTNISSE**

FÜR WEITERE INFORMATIONEN KLICKEN



Drei Hauptfaktoren als treibende Faktoren für ein erstes MDR-Projekt

Unternehmen werden durch proaktive Bewertungen, betriebliche Lücken und IR-Projekte vorangetrieben.

MDR unterstützt mehrere Anwendungsbeispiele

ExpertInnen, Threat Intelligence, Kompetenzschulungen, Absicherung, Programmentwicklung und mehr sind entscheidende Faktoren für die Fortsetzung der Zusammenarbeit.

MDR fördert positive Sicherheitsergebnisse

Unternehmen profitieren von einem erweiterten Reifegrad, weniger erfolgreichen Angriffen, verbesserten Cyberkompetenzen und einem größeren Vertrauen der Führungskräfte.

Ein Open-Tech-Stack wird erwartet, aber MDR muss alle Mechanismen umfassen

Von Anbietern wird erwartet, dass sie bei Bedarf über einen vollständigen Technologiestack verfügen. Sie müssen aber auch Integrationen in die vorhandene Infrastruktur bereitstellen, um erfolgreich zu sein.

MDR-Kundenbindungsmodelle sind wichtig

Auch wenn sich die Modelle unterscheiden, wird Vertrauen durch regelmäßige, menschenorientierte Kommunikation aufgebaut.

Branchentrends wirken sich auf die MDR-Auswahl aus

Der XDR-Trend, die Unterstützung für MITRE ATT&CK und die SOC-Modernisierung spielen eine wichtige Rolle.

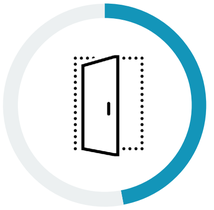
Drei Hauptfaktoren als treibende Faktoren für ein erstes MDR-Projekt

Proaktive Bewertungen als wichtiger Faktor für ein erstes MDR-Projekt

Warum wenden sich IT- und Sicherheitsteams an einen Managed Detection and Response-Serviceanbieter? Bei einer wortwörtlichen Interpretation von MDR sind Lücken bei Sicherheitsbetriebskompetenzen, Absicherung oder Prozessen eine offensichtliche Antwort. Es zeigt sich jedoch, dass mehr als die Hälfte (57 %) der Unternehmen proaktive Sicherheitsbewertungen als einen entscheidenden Faktor für ihr erstes MDR-Projekt nannten. Tatsächlich beginnt die Zusammenarbeit mit MDR-Anbietern oft mit Sicherheitsbewertungen, einschließlich Sicherheitslückenbewertungen, da diese Schwachstellen im Sicherheitsstatus in Bezug auf Programme, Tools, Absicherung und Kompetenzen aufzeigen können. Der dritte große treibende Faktor ist eine Reaktion auf Krisen/Vorfälle, die Lücken im Sicherheitsprogramm aufzeigen kann. Betriebliche Anforderungen wie die Reaktion auf Incidents sind ebenfalls gängige Faktoren für MDR-Projekte.

Faktoren, die zu ersten Projekten mit MDR-Anbietern führten

57 %
Sicherheits-bewertungen

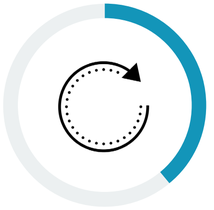


47 %
Bewertung und Management von Sicherheitslücken

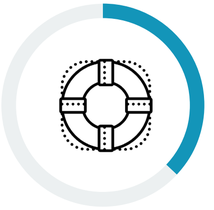
46 %
Threat-Intelligence-Services

39 %
Incident-Reaktion/-Abmilderung

39 %
Incident-Erkennung



39 %
Incident-Korrektur/ Recovery



37 %
Reaktionsprojekt bei Sicherheitsverletzungen oder größeren Incidents

36 %
Incident-Reaktion bei Krisen/ Sicherheitsverletzungen, die Lücken in unserem Programm aufgedeckt haben

34 %
Incident-Ermittlungen

33 %
Selektierung und Priorisierung täglicher Warnmeldungen

30 %
Bedrohungssuche

25 %
Red Teaming sowie Simulation von Sicherheitsverletzungen und Angriffen

ZURÜCK ZUM INHALT

Motivierende Faktoren für das aktuelle MDR-Serviceprojekt

Sicherheitsteams haben Schwierigkeiten mit der Skalierung von Sicherheitsprogrammen, um sowohl das Wachstum als auch die Komplexität der Angriffsfläche und Bedrohungslandschaft zu bewältigen. Deshalb beauftragen viele Unternehmen MDR-Anbieter, um ihre Betriebsmodelle zu beschleunigen und zu skalieren. Unternehmen betrachten MDR als einen Weg, die Programmentwicklung schneller voranzubringen und Lücken zu schließen. Mehr als 4 von 10 Unternehmen sind der Ansicht, dass MDR-Serviceanbieter einfach bessere Arbeit leisten als interne Ressourcen. Ein Drittel berichtet von unausgereiften Sicherheitsprogrammen sowie fehlenden Tools und Systemen. Zu anderen wichtigen Faktoren zählen jedoch auch eine ausufernde Liste von Sicherheitskontrollen und -prozessen, die für eine Cybersicherheitsversicherung erforderlich sind, sowie behördliche Complianceanforderungen.

Einige Unternehmen berichten auch von Lücken bei Kompetenzen und Absicherung, aber diese stehen im Vergleich zum Ausbau und der Entwicklung des allgemeinen Programms weiter unten in der Liste.

Faktoren, die Unternehmen motiviert haben, mit ihren aktuellen MDR-Anbietern zusammenzuarbeiten

ZURÜCK ZUM INHALT

MDR unterstützt **mehrere Anwendungsbeispiele**

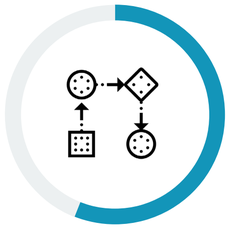
> Fast die Hälfte nutzt einen MDR-Anbieter, **um Sicherheitsabläufe vollständig auszulagern.“**

Wichtige Anwendungsbeispiele: Zugang zu Expertenressourcen und Entwicklung eines Sicherheitsprogramms

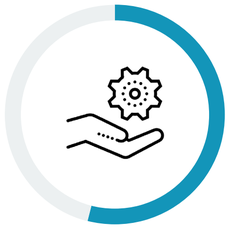
MDR-Anbieter stellen eine Reihe von Services bereit, die zur Realisierung mehrerer Anwendungsbeispiele verwendet werden. Während die Beschleunigung der Entwicklung eines Sicherheitsprogramms und der Zugang zu erfahrenen Sicherheitsressourcen ganz oben auf der Liste stehen, nutzt fast die Hälfte einen MDR-Anbieter, um Sicherheitsabläufe vollständig auszulagern. Die andere Hälfte verwendet MDR, um das interne Programm zu ergänzen, Absicherungslücken zu schließen, Zugang zu zusätzlicher Threat Intelligence zu erhalten und Funktionen zum Aufspüren von Bedrohungen hinzuzufügen. Bemerkenswert ist auch, dass fast die Hälfte der Unternehmen ihre Sicherheitsabläufe vollständig auslagert oder dies tun möchte.

MDR-Anwendungsbeispiele in den Sicherheitsprogrammen von Unternehmen.

56 %
Zugang zu erfahrenden Sicherheitsressourcen



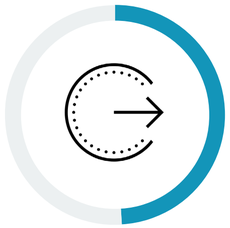
56 %
Entwicklung eines Sicherheitsprogramms



54 %
Ergänzung des internen Programms für Sicherheitsabläufe

50 %
Absicherung

50 %
Threat Intelligence



49 %
Vollständiges Outsourcing unserer Sicherheitsabläufe

49 %
Proaktive Bedrohungssuche

ZURÜCK ZUM INHALT

MDR-Projekte werden in der Regel im Lauf der Zeit ausgeweitet

MDR-Projekte werden in der Regel im Lauf der Zeit ausgeweitet. Dabei werden neue Services hinzugefügt, um Incident-Ermittlungen, -Abmilderung und -Reaktion zu verstärken. Das reicht von schwerwiegenden Krisen/Sicherheitsverletzungen bis hin zu alltäglichen Reaktionsaktivitäten. Moderne MDR-Anbieter erweitern Funktionen über herkömmliche reaktive SecOps-Mainstreamfunktionen hinaus. Sie bieten proaktive Services zur Unterstützung von Threat Intelligence, Bedrohungssuche, Angriffssimulationen, Sicherheitsbewertungen und Sicherheitslückenmanagement. Angesichts dieser breiten Palette an Services bieten MDR-Anbieter so viel mehr als nur grundlegende Erkennung und Reaktion. Stattdessen entwickeln sie sich zu umfassenden Sicherheitsprogrammpartnern, die Unternehmen jeder Größe bei der Skalierung ihrer Sicherheitsprogramme unterstützen.

Sicherheitsaktivitäten, die seit der ersten Zusammenarbeit mit MDR-Anbietern hinzugefügt wurden

> MDR-Anbieter bieten **so viel mehr als nur grundlegende Erkennung und Reaktion.“**

ZURÜCK ZUM INHALT

Mehr als Erkennung und Reaktion: MDR-Anbieter sind langfristige, strategische Betriebspartner

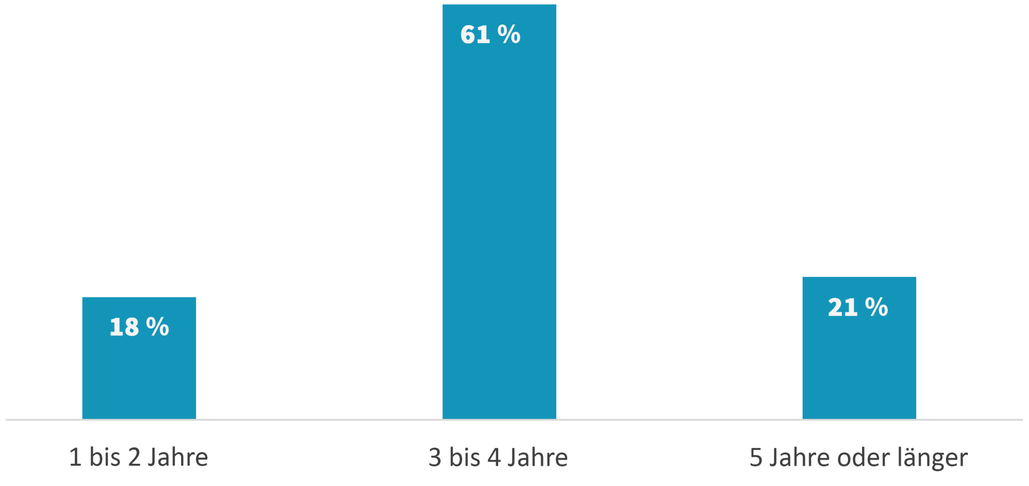
Wenn MDR-Projekte fortdauern und die Beziehungen vertieft werden, übernehmen MDR-Anbieter eine eher strategisch ausgerichtete Rolle. Dies zeigt sich deutlich daran, dass mehr als drei Viertel (77 %) der Unternehmen ihren MDR-Anbieter in Bezug auf die Ausrichtung an ihrem Sicherheitsprogramm als strategischen Betriebspartner beschreiben. Die Beziehungen haben Bestand. 82 % der Unternehmen geben an, dass sie seit mindestens 3 Jahren mit einem MDR-Anbieter zusammenarbeiten. Eine Mehrheit nutzt außerdem mehr als einen MDR-Anbieter. Dabei arbeiten 34 % mit 3 oder mehr MDR-Serviceanbietern zusammen, um die Anwendungsbeispiele und Ressourcen zu unterstützen, die ihre Angriffsfläche bilden.

Wie Unternehmen ihre aktuellen MDR-Anbieter betrachten

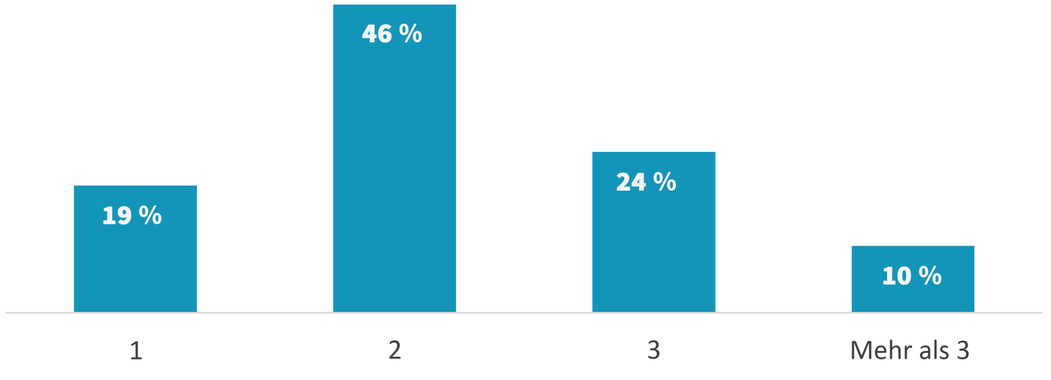
77 %

Ein strategischer Betriebspartner, **der unser allgemeines Sicherheitsprogramm verbessert hat**

Zeitdauer seit Beginn der Zusammenarbeit mit einem MDR-Anbieter



Anzahl der MDR-Serviceanbieter, mit denen Unternehmen zusammenarbeiten



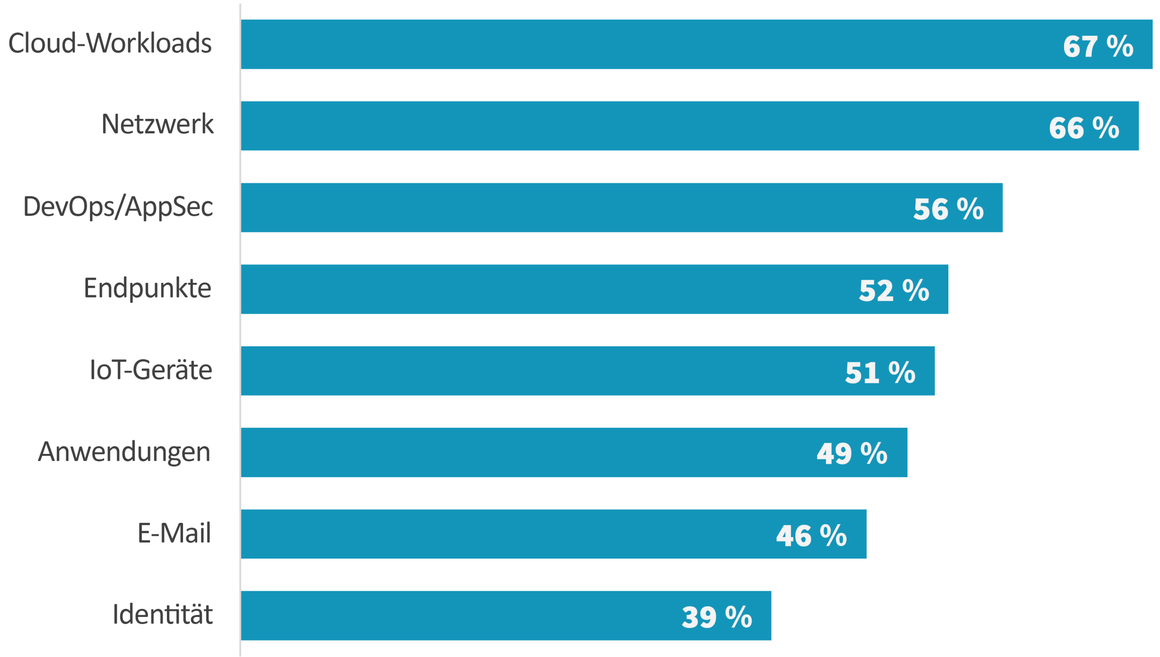
ZURÜCK ZUM INHALT

> Nur wenige beauftragen MDR-Anbieter **mit der Absicherung ihrer gesamten Angriffsfläche.“**

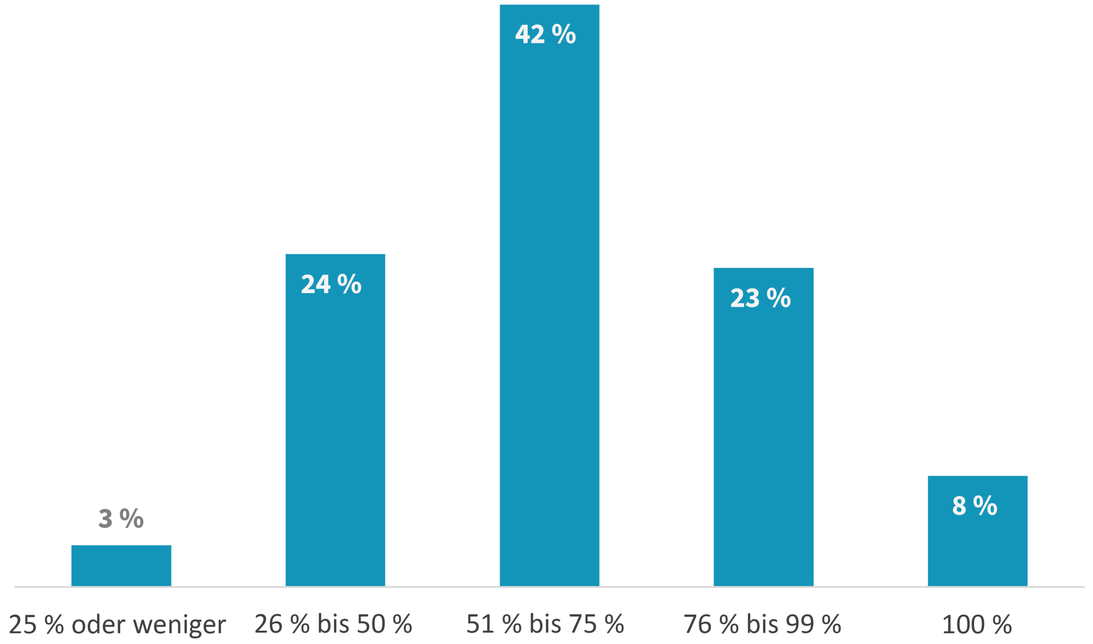
Von MDR-Anbietern wird erwartet, dass sie alle Arten von Ressourcen überwachen können, wobei nur selten der gesamte Bestand überwacht wird

Wenn es um die Absicherung von Angriffsflächen geht, erwarten die meisten Unternehmen, dass MDR-Anbieter Sicherheitsabläufe für alle Arten von IT-Ressourcen unterstützen. Aber nur wenige beauftragen MDR-Anbieter mit der Absicherung ihrer gesamten Angriffsfläche. Im Einzelnen geben mehr als zwei Drittel an, dass ihr MDR-Anbieter nicht mehr als 75 % ihres Bestands absichern, während bei nur 8 % der MDR-Anbieter 100 % übernimmt.

Umfang der Abdeckung für die aktuellen MDR-Anbieter von Unternehmen



Prozentsatz der Angriffsfläche, die der bzw. die MDR-Anbieter absichern



ZURÜCK ZUM INHALT

MDR fördert **positive Sicherheitser-gebnisse**

MDR-Anbieter tragen dazu bei, den Reifegrad der Vor-Ort-Ressourcen und des Sicherheitsprogramms zu verbessern

In Bezug auf die tatsächlich erzielten Ergebnisse unterstützen MDR-Anbieter Unternehmen dabei, die Anzahl erfolgreicher Angriffe zu reduzieren, die allgemeine Entwicklung von Sicherheitsprogrammen zu beschleunigen und Investitionsmöglichkeiten in eher strategisch ausgerichtete Sicherheitsinitiativen zu eröffnen. Spezifisch sagt die Hälfte, dass ihr MDR-Anbieter dazu beiträgt, die Sicherheitskompetenzen ihrer internen Ressourcen zu verbessern. 45 % konnten in eher strategisch ausgerichtete Sicherheitsinitiativen investieren. Mehr als 4 von 10 berichten von deutlich weniger erfolgreichen Angriffen und/oder einer allgemeinen Verbesserung ihres Sicherheitsprogramms. Im Hinblick auf den Geschäftsbereich geben 42 % an, dass das Vertrauen von Führungskräften und/oder Vorständen gestiegen ist. 38 % sagen, dass sie Complianceziele oder Cyberversicherungsanforderungen erfüllen können. Diese positiven Geschäftsergebnisse werden durch eine deutliche Zunahme der Anzahl der Unternehmen bestätigt, die den Reifegrad ihrer Sicherheitsprogramme nach der Zusammenarbeit mit einem MDR-Anbieter als sehr ausgereift kategorisieren.

Durch die Zusammenarbeit mit einem MDR-Anbieter erzielte Ergebnisse

50 %
Verbesserte, vom MDR-Anbieter vermittelte Kompetenzen der SicherheitsmitarbeiterInnen

45 %
Investitionen in eher strategisch ausgerichtete Sicherheitsinitiativen

42 %
Deutlich weniger erfolgreiche Angriffe

42 %
Deutliche Verbesserung des Sicherheitsprogramms

42 %
Steigerung des Vertrauens von Führungskräften und/oder Vorständen

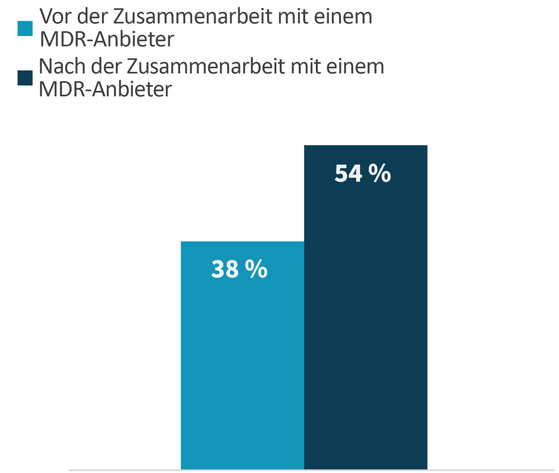
38 %
Erfüllung der Compliance-/Cyberversicherungsanforderungen

38 %
Niedrigere Sicherheitsbetriebskosten

35 %
Weniger Belastung für das interne Sicherheitsteam

32 %
Geringere Gebühren für Cyberversicherungen

MDR-Programmreifegrad



Sehr ausgereift (d. h. formale, operationalisierte Prozesse, ExpertInnen im Personal, vollständige Absicherung und Transparenz der Angriffsfläche, Risikoprofile, formales, geprüftes IR-Programm, IT-Zusammenarbeit, hocheffektive Sicherheitstools und Analysen usw.)

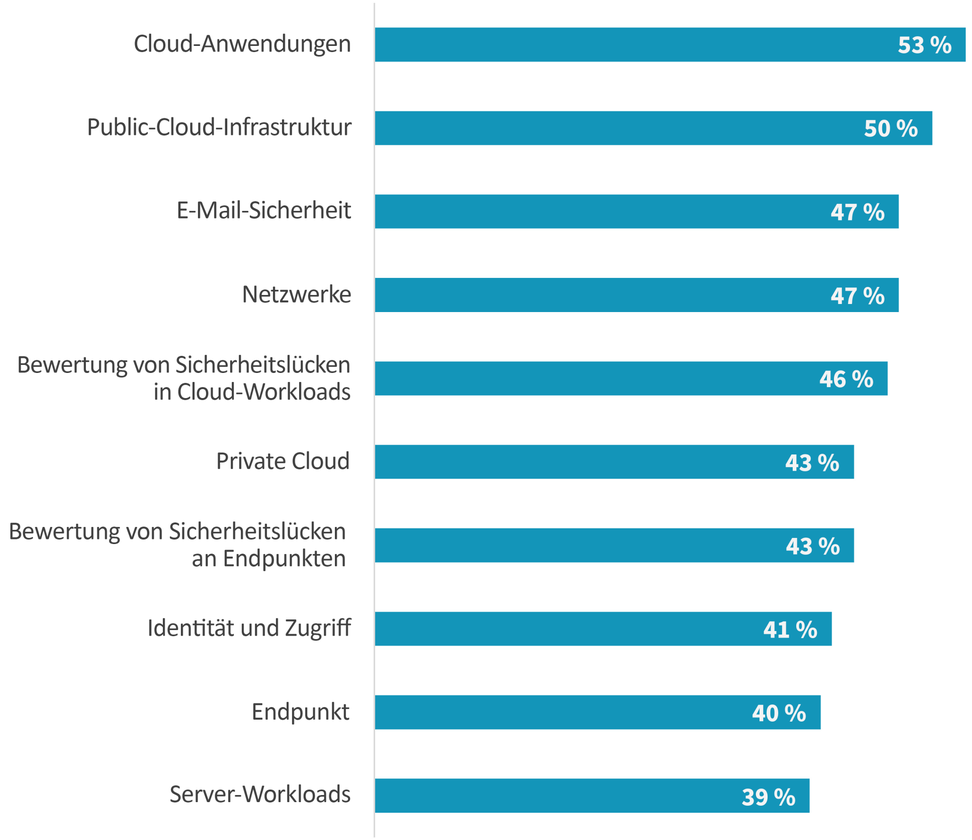
ZURÜCK ZUM INHALT

Ein Open-Tech-Stack wird erwartet, aber **MDR muss alle Mechanismen umfassen**

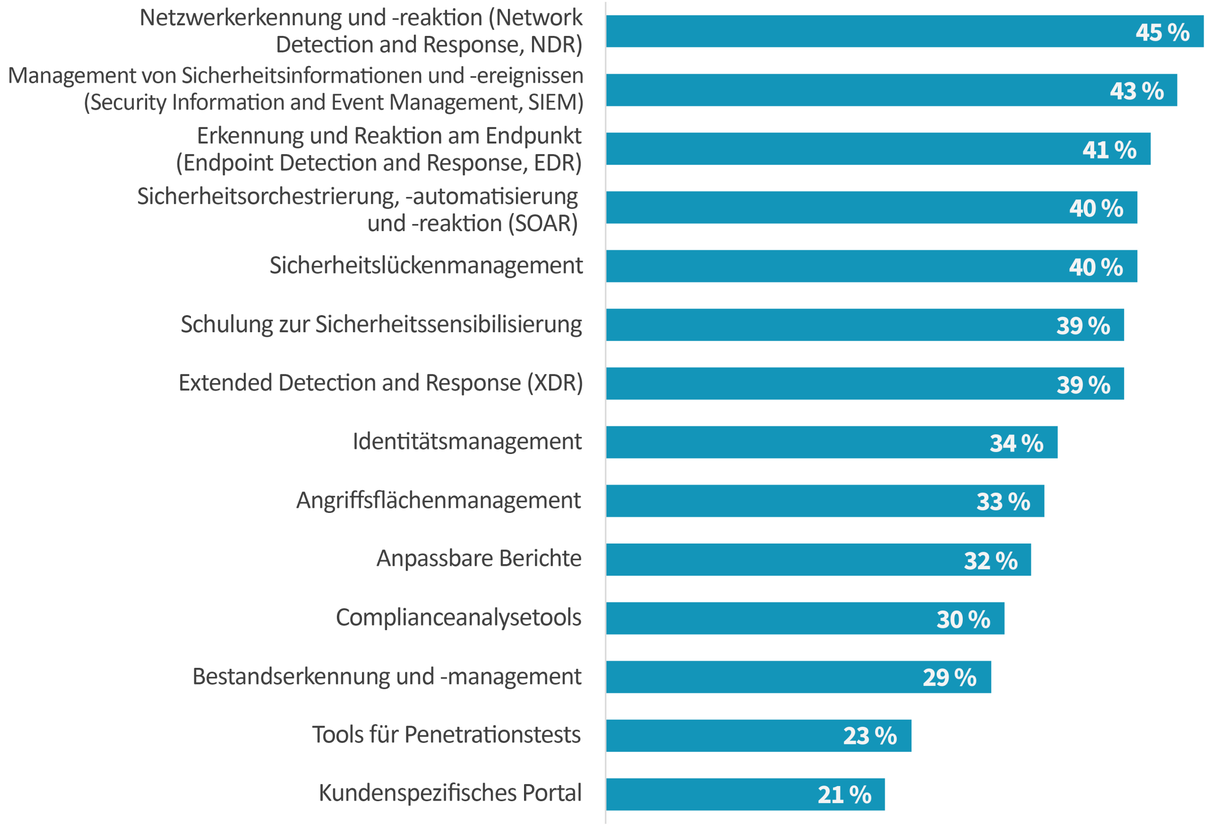
Cloud- und Sicherheitsabläufe sind wichtige Technologiekriterien für die MDR-Auswahl

MDR-Kunden erwarten von ihrem Anbieter eine umfassende Sicherheitsabdeckung über alle Angriffsvektoren hinweg. Darüber hinaus gehen MDR-NutzerInnen jedoch auch davon aus, dass ihr Anbieter mit den bereits vorhandenen Sicherheitsmechanismen zusammenarbeitet. Diese reichen von einem vollständigen Satz von Sicherheitskontrollen einschließlich Endpunkt, Netzwerk, Cloud und E-Mail bis hin zu einem vollständigen Stack an Sicherheitsbetriebstools wie SIEM, SOAR, EDR, NDR, XDR, Angriffsflächenmanagement, Ressourcenerkennung und Sicherheitslückenmanagement.

Erkennungs-/Agent-Technologien, die Unternehmen von einem MDR-Anbieter erwarten



Sicherheitsbetriebstechnologien, die Unternehmen von einem MDR-Anbieter erwarten



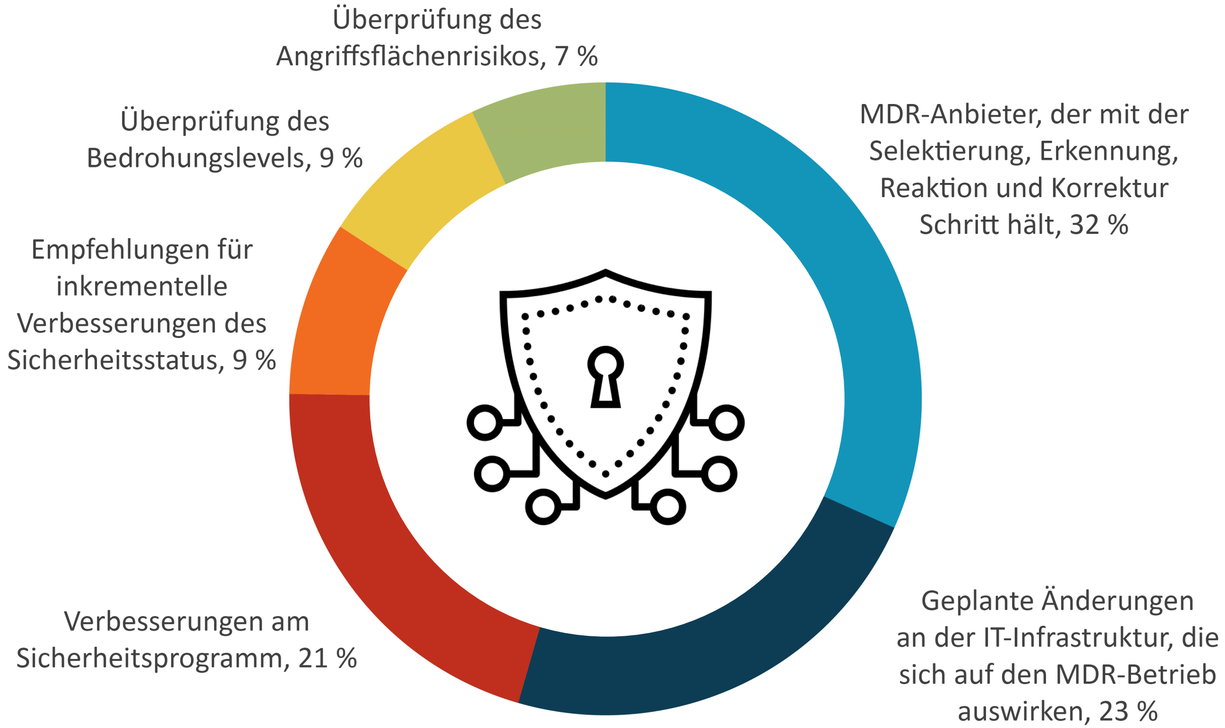
ZURÜCK ZUM INHALT

MDR-Kundenbindungs-modelle **sind wichtig**

MDR-Betriebsprüfungen: die wichtigsten Faktoren

Sicherheitsführungskräfte betonen, dass MDR-Kundenbindungsmodelle eine große Rolle spielen. MDR-Anbieter sollen nicht nur mit ihrer vorselektierten Erkennung, Reaktion und Korrektur Schritt halten, sondern auch mit geplanten Änderungen an der IT-Infrastruktur, der fortlaufenden Verbesserungen des Sicherheitsprogramms sowie der Überprüfung der Angriffsfläche und des Bedrohungslevels auf dem Laufenden bleiben – und gleichzeitig Maßnahmen für eine inkrementelle Verbesserung des Sicherheitsstatus empfehlen. Diese Erwartungen sind hoch, verdeutlichen aber, warum die meisten Unternehmen ihren MDR-Anbieter als strategischen Partner betrachten.

Wichtigster Aspekt der betrieblichen Überprüfungen des MDR-Anbieters



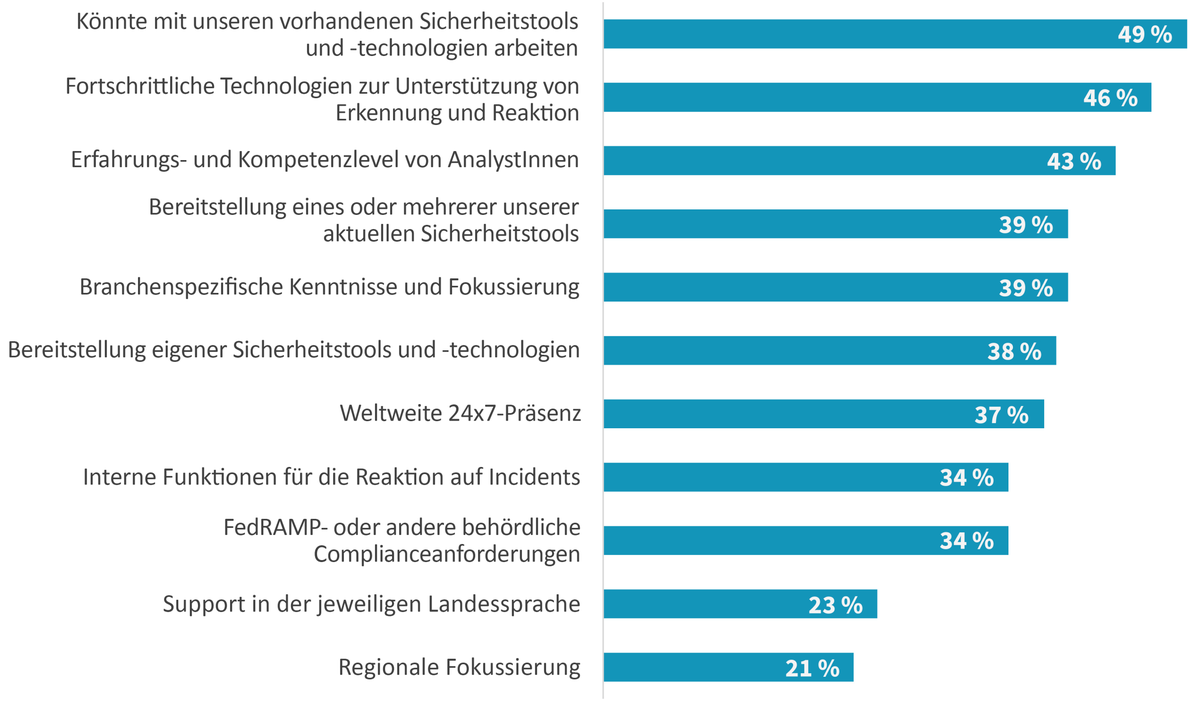
> Sicherheitsführungskräfte betonen, dass **MDR-Kundenbindungsmodelle sehr wichtig sind.“**

ZURÜCK ZUM INHALT

Kompetenzen und erweiterte Tools können einen MDR-Anbieterwechsel vorantreiben

Welche Überlegungen sind für Unternehmen wichtig, wenn sie einen MDR-Anbieter bewerten und auswählen? Fast die Hälfte (49 %) gab an, dass er mit ihrem vorhandenen Sicherheits- und Technologieökosystem arbeiten muss, während sich 46 % fortschrittliche Erkennungs- und Reaktionsfunktionen wünschen. Weitere 43 % möchten, dass ihr MDR-Anbieter über erfahrene Sicherheitsressourcen verfügt. Dieser Faktor wird auch als häufigster Grund für einen Wechsel des aktuellen Anbieters genannt. Weitere Gründe sind fortschrittlichere Sicherheitstools und verbesserte Erkennungs- und Auflösungsraten, obwohl auch Preise und Betriebsmodelle wichtig sind.

Wichtige Auswahlkriterien für MDR-Anbieter



Faktoren, die Unternehmen dazu motivieren würden, ihren MDR-Anbieter zu wechseln

ZURÜCK ZUM INHALT

Megatrends der Branche **beeinflussen die MDR-Auswahl**

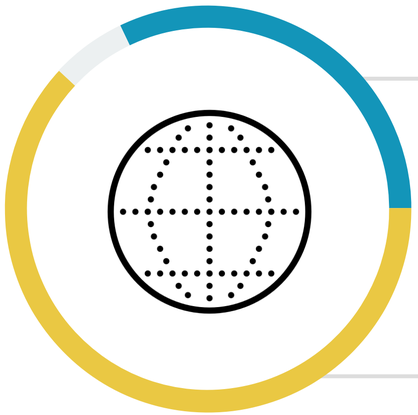
Mehr als 9 von 10

Unternehmen bezeichnen die Unterstützung für MITRE ATT&CK als kritisch oder sehr wichtig.

MITRE- und XDR-Unterstützung sind für die meisten Unternehmen bei der MDR-Anbieterauswahl entscheidend

Die Auswahl eines MDR-Anbieters umfasst oft mehr als eine Prüfliste der Funktionen und Absicherung. Auch umfassende Branchenthemen wirken sich auf die MDR-Anbieterauswahl aus. Mehr als 9 von 10 Unternehmen bezeichnen beispielsweise die Unterstützung für MITRE ATT&CK als kritisch (32 %) oder sehr wichtig (62 %). Darüber hinaus geben fast drei Viertel (73 %) an, dass die XDR-Sicherheitstechnologie (Extended Detection and Response) beim Auswahlprozess für MDR-Services eine Rolle gespielt hat. Secure Service Access Edge (SASE) und das Angriffsflächenmanagement (Attack Surface Management, ASM) wurden ebenfalls von zwei Dritteln als wichtig betrachtet.

Bedeutung der Unterstützung für das MITRE ATT&CK-Framework durch den MDR-Anbieter



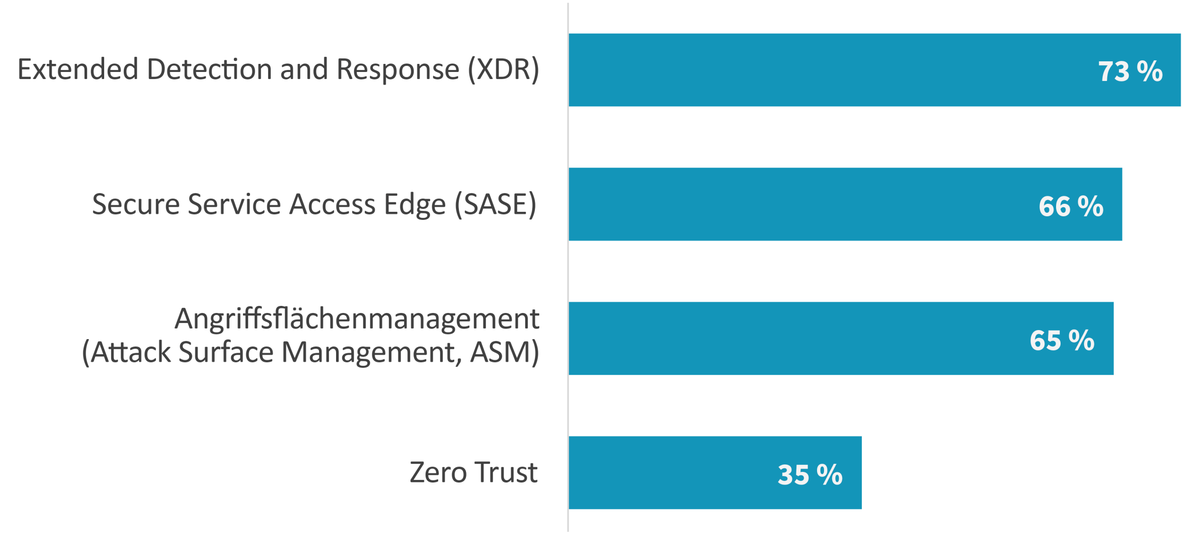
32 %

Kritisch: Wir würden keinen MDR-Anbieter in Betracht ziehen, der das MITRE ATT&CK-Framework nicht unterstützt.

62 %

Sehr wichtig: Wir würden bevorzugt mit einem MDR-Anbieter zusammenarbeiten, der das MITRE ATT&CK-Framework unterstützt, ziehen aber auch andere Anbieter in Betracht.

Sicherheitsmegatrends, die beim Auswahlprozess für MDR-Services berücksichtigt werden



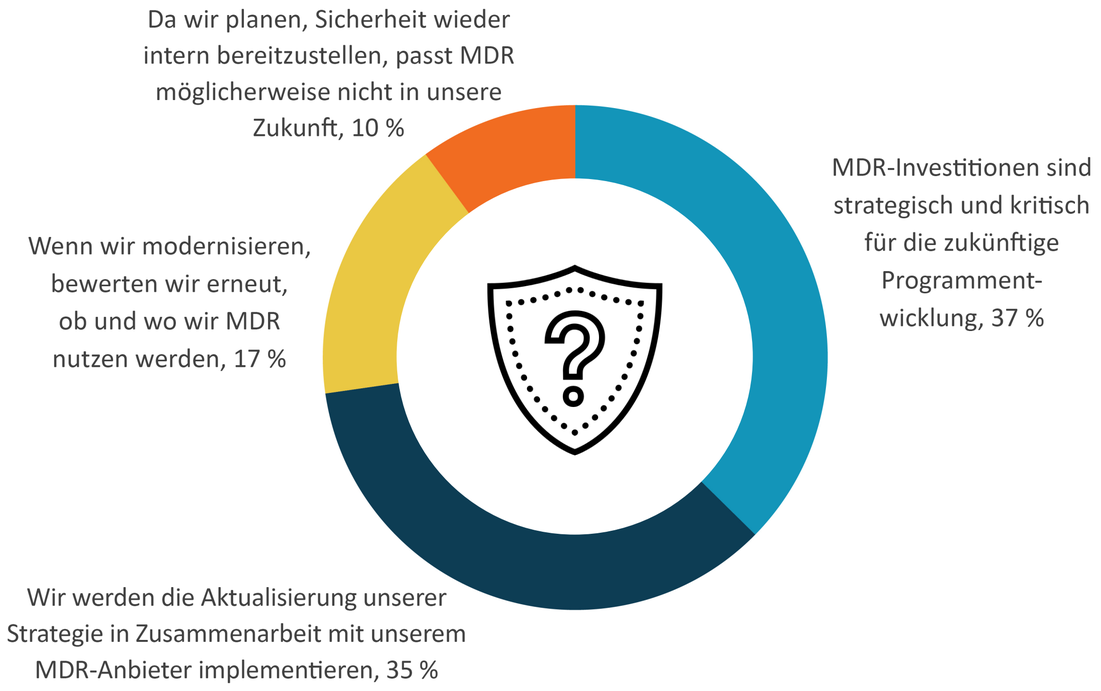
ZURÜCK ZUM INHALT

MDR wird zu einer etablierten Sicherheitsstrategie

Die Nutzung von MDR-Services ist zu einer Kernkomponente der Sicherheitsprogrammstrategie geworden, sodass MDR-Anbieter jetzt strategische Partner sind. Sie unterstützen Sicherheits- und IT-Teams nicht nur dabei, die Programmentwicklung zu beschleunigen und den Sicherheitsstatus zu verbessern, sondern auch weniger sichtbare Vorteile zu erzielen. Dazu zählen die Unterstützung von Compliancezielen, der Abschluss von Cyberversicherungen und die Verbesserung interner Sicherheitskompetenzen und -prozesse. Daher betrachten die meisten Unternehmen MDR als kontinuierlichen Teil ihrer Investitionen in das Sicherheitsprogramm. 37 % bezeichnen MDR als strategisch und kritisch und weitere 35 % planen, mit ihrem MDR-Anbieter zusammenzuarbeiten, wenn sie zukünftige Sicherheitsstrategien aktualisieren und implementieren.

ESG betrachtet MDR als wichtige und etablierte Sicherheitsstrategie und empfiehlt Unternehmen, weitere Anwendungsbeispiele zu erkunden, die die Entwicklung des Sicherheitsprogramms und die Verbesserung des Sicherheitsstatus beschleunigen können.

Stellung von MDR im breiteren Kontext der SOC-Modernisierung



> Die meisten betrachten MDR als **fortlaufenden Teil ihrer Investitionen in das Sicherheitsprogramm.“**

ZURÜCK ZUM INHALT

ÜBER ESG

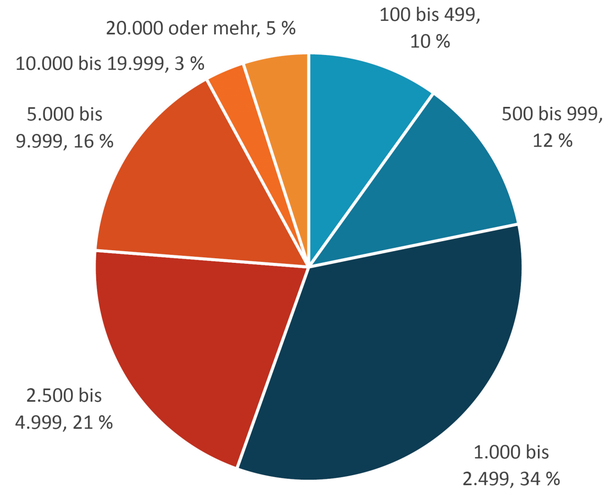
Die Enterprise Strategy Group ist ein integriertes Technologieanalyse-, Forschungs- und Strategieunternehmen, das Marktinformationen, verwertbare Erkenntnisse und Go-to-Market-Contentservices für die globale Technologiecommunity bereitstellt.

Studienmethodik und demografische Daten

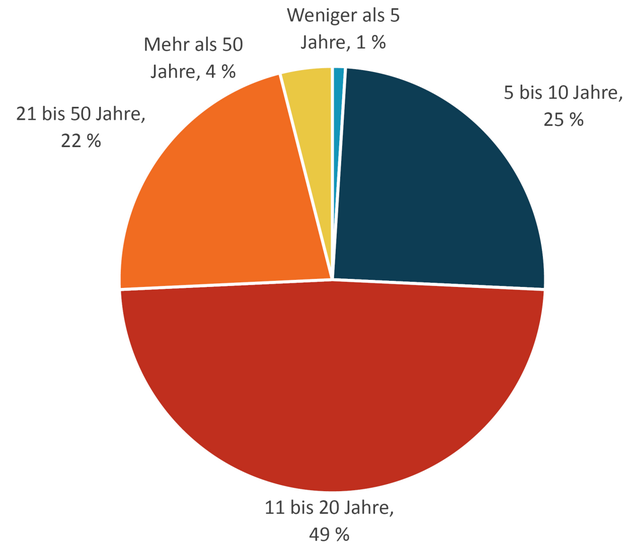
Für die Erfassung von Daten für diesen Bericht führte ESG zwischen dem 3. August 2022 und dem 14. August 2022 eine umfassende Onlineumfrage unter CybersicherheitsexpertInnen aus Unternehmen des privaten und öffentlichen Sektors in Nordamerika (USA und Kanada) durch. Um sich für diese Umfrage zu qualifizieren, mussten die Befragten CybersicherheitsexpertInnen sein, die persönlich mit Cybersicherheitstechnologie, einschließlich Produkten und Services sowie Prozessen, zu tun haben. Alle Teilnehmer erhielten Incentives in Form von Bargeld und/oder Barwerten für die Teilnahme an der Umfrage.

Nach dem Herausfiltern von nicht qualifizierten TeilnehmerInnen, dem Entfernen von doppelten Antworten und dem Überprüfen der verbleibenden bereitgestellten Antworten (nach verschiedenen Kriterien) auf Datenintegrität blieb letztendlich eine Auswahl von 373 CybersicherheitsexpertInnen übrig.

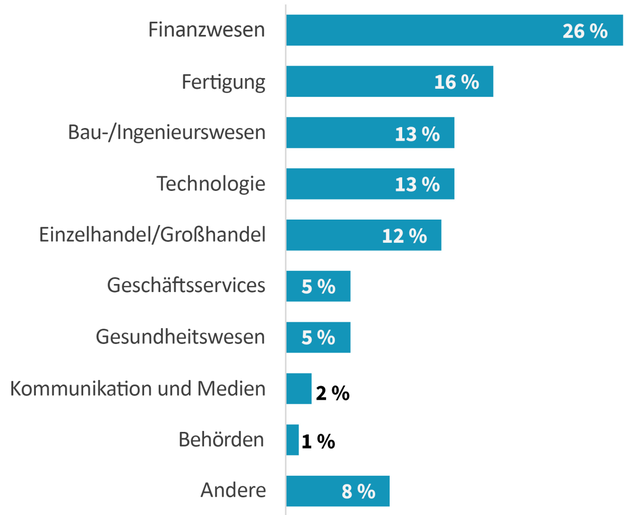
BEFRAGTE NACH ANZAHL DER MITARBEITERINNEN



BEFRAGTE NACH ALTER DES UNTERNEHMENS



BEFRAGTE NACH BRANCHE



ZURÜCK ZUM INHALT

Die Enterprise Strategy Group ist ein integriertes Technologieanalyse-, Forschungs- und Strategieunternehmen, das Marktinformationen, verwertbare Erkenntnisse und Go-to-Market-Contentservices für die globale Technologiecommunity bereitstellt.