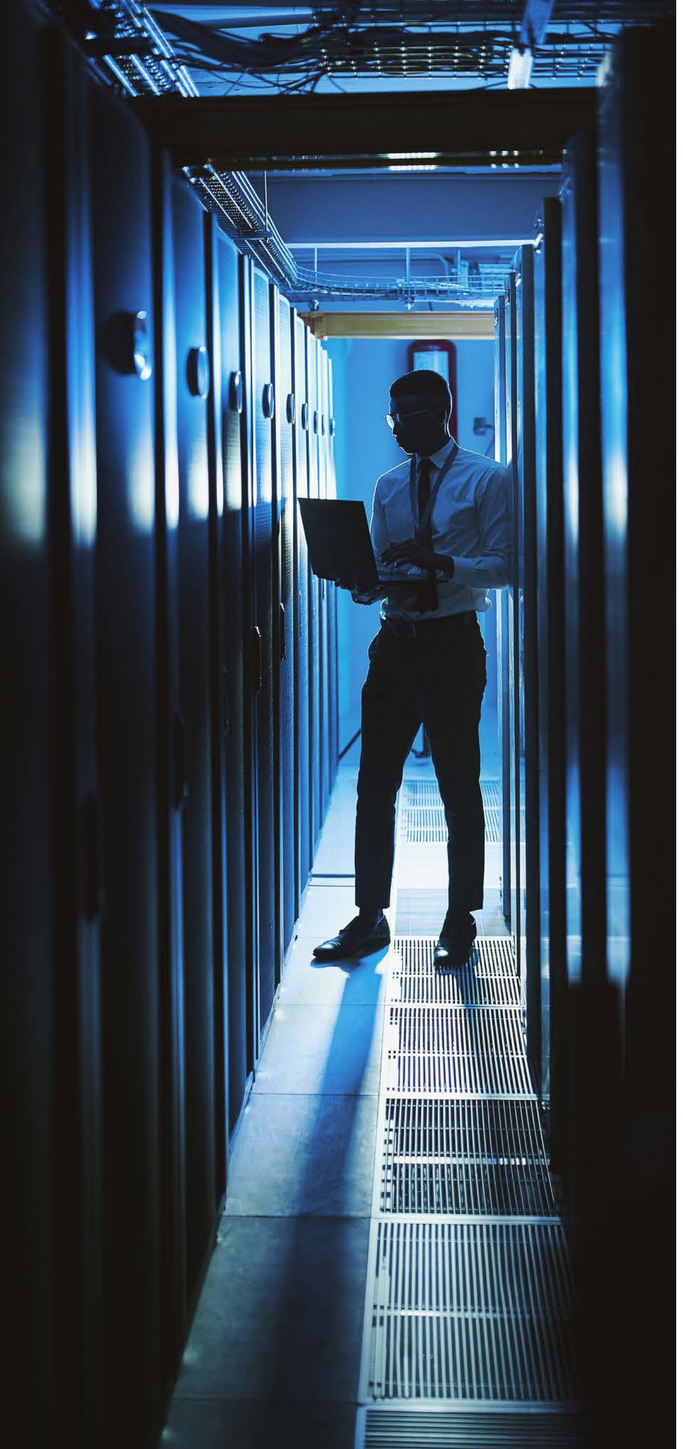
Enterprise Strategy Group | Getting to the bigger truth.™

What Security Teams Want from MDR Providers

Dave Gruber, Principal Analyst

SEPTEMBER 2022



Research Objectives

The use of managed detection and response (MDR) services has become a mainstream strategy in modern security programs. But IT organizations shouldn't be fooled by the name: MDR providers are delivering much more than basic detection and response, helping IT and security leaders accelerate program development and improve security posture. With no end in sight for the cybersecurity skills shortage, MDR services can bring immediate expert resources online, together with proven, best-of-breed processes and tools that can help security teams gain control and set themselves up for future security program success.

In order to understand these trends, as well as assess the general state of managed detection and response service offerings, ESG surveyed 373 cybersecurity professionals personally involved with cybersecurity technology, including both products and services, and processes.

THIS STUDY SOUGHT TO:

Determine how, where, and why MDR services are used to support security programs.

Gain insights into what matters most for IT operations, LoB executives, and end-users.

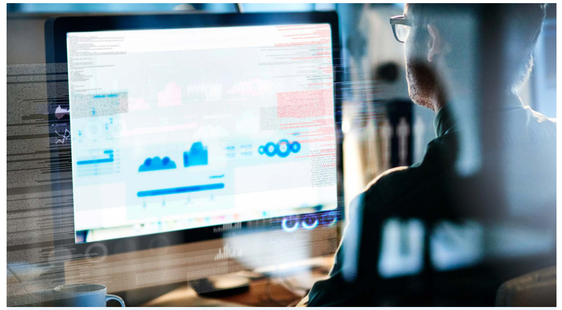
Isolate specific MDR use cases and the organizational profiles of those who use them.

Establish which industry megatrends are impacting MDR provider selection.

BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW



Three Key Factors Drive Initial MDR Engagement

Organizations are spurred by proactive assessments, operational gaps, and IR engagements.

Multiple Use Cases Are Supported by MDR

Experts, threat intelligence, skills training, coverage, program development, and more are driving ongoing engagement.

MDR Is Driving Positive Security Outcomes

Organizations see advanced maturity, fewer successful attacks, improved cyber-skills, and increased executive confidence.

An Open Tech Stack Is Expected, but MDR Must Bring All Mechanisms

Providers are expected to have a full tech stack if needed but must integrate with existing infrastructure to win.

MDR Customer Engagement Models Matter

While models vary, trust is built through regular, human-centric communications.

Industry Megatrends Are Impacting MDR Selection

The XDR movement, MITRE ATT&CK support, and SOC modernization are important.

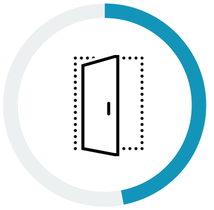
Three Key Factors Drive Initial MDR Engagement

Proactive Assessments More Likely to Initially Spawn MDR Engagement

What causes IT and security teams to pursue a managed detection and response service provider? Thinking about MDR as its most literal interpretation, gaps in security operations skills, coverage, or processes would be an obvious answer. However, it turns out that more than half (57%) of organizations cited proactive security assessments as a factor that drove their initial MDR engagement. Indeed, engagements with MDR providers often begin with security assessments, including vulnerability assessments, as they can serve to expose weaknesses in security posture in terms of programs, tools, coverage, and skills. The third big driver is a crisis/incidence response that reveals security program gaps. Operational needs like incident response are also common drivers of MDR engagements.

Factors that drove initial engagements with MDR provider(s).

57%
Security assessments

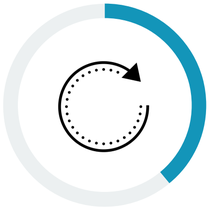


47%
Vulnerability assessment and management

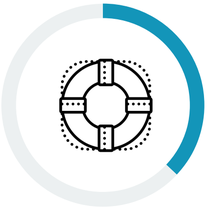
46%
Threat intelligence services

39%
Incident response/ mitigation

39%
Incident detection



39%
Incident remediation/ recovery



37%
Breach or major incident response engagement

36%
Crisis/breach incident response that revealed gaps in our program

34%
Incident investigation

33%
Daily alert triage and prioritization

30%
Threat hunting

25%
Red teaming and breach and attack simulation

BACK TO CONTENTS

Motivating Factors for Current MDR Service Engagement

As security teams struggle to scale security programs to meet both attack surface and threat landscape growth and complexity, many are engaging MDR providers to accelerate and scale their operating models. Organizations see MDR as a path to accelerate program development and fill gaps. More than four in ten think that MDR service providers can simply do a better job than in-house resources can. One-third report immature security programs, also lacking the tools and systems needed. But other important drivers include an escalating list of security controls and processes required to acquire cybersecurity insurance, together with regulatory compliance requirements.

When it comes to skills and coverage shortfalls, some report gaps, but these rank low on the list compared with overall program growth and development objectives.

Motivating factors for organizations to engage with their current MDR provider(s).

BACK TO CONTENTS

Multiple Use Cases
Are Supported by MDR

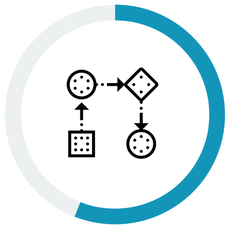
> Almost half leverage an MDR provider **to fully outsource security operations.”**

Key Use Cases: Access to Expert Resources and Security Program Development

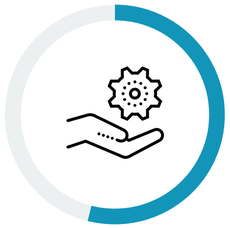
MDR providers offer an array of services that are used to fulfill multiple use cases. While accelerating security program development and gaining access to expert security resources lead the list, almost half leverage an MDR provider to fully outsource security operations. The other half uses MDR to supplement their in-house program, closing coverage gaps, gaining access to additional threat intelligence, and adding threat hunting capabilities. It’s also worth noting that nearly half of organizations fully outsource their security operations or aspire to do so.

MDR use cases within organizations’ security programs.

56%
Access to expert security resources



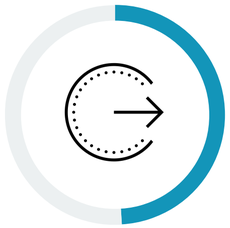
56%
Security program development



54%
Supplements internal security operations program

50%
Coverage

50%
Threat intelligence



49%
Full outsourcing of our security operations

49%
Proactive threat hunting

BACK TO CONTENTS

MDR Engagements Commonly Grow over Time

MDR engagements typically grow over time, adding new services to strengthen incident investigation, mitigation, and response for anything from a major crisis/breach event to day-to-day response activities. Modern MDR providers extend capabilities beyond traditional mainstream reactive SecOps functions, offering proactive services supporting threat intelligence, threat hunting, attack simulations, security assessments, and vulnerability management. Looking at this broad collection of services, MDR providers are delivering so much more than basic detection and response and are instead becoming full-scale security program partners that help organizations of all sizes scale their security programs.

Security activities added since initially engaging with MDR provider(s).

> MDR providers are delivering **so much more than basic detection and response.”**

BACK TO CONTENTS

More than Detection and Response: MDR Providers Are Long-term, Strategic Operating Partners

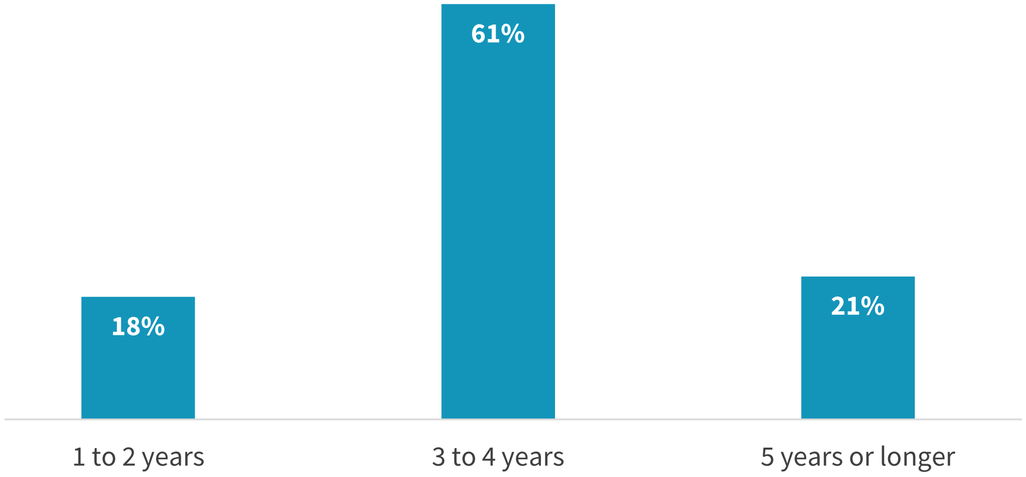
As MDR engagements persist and relationships grow, MDR providers will take on a more strategic role. This is clearly demonstrated by the fact that more than three-quarters (77%) of organizations describe their MDR provider as a strategic operating partner in terms of aligning with their security program. These relationships endure, with 82% of organizations reporting that they've been engaged with an MDR provider for at least three years, and a majority are using more than one MDR provider, with 34% partnering with three or more MDR service providers to support the use cases and assets that make up their attack surface.

How organizations view their current MDR provider(s).

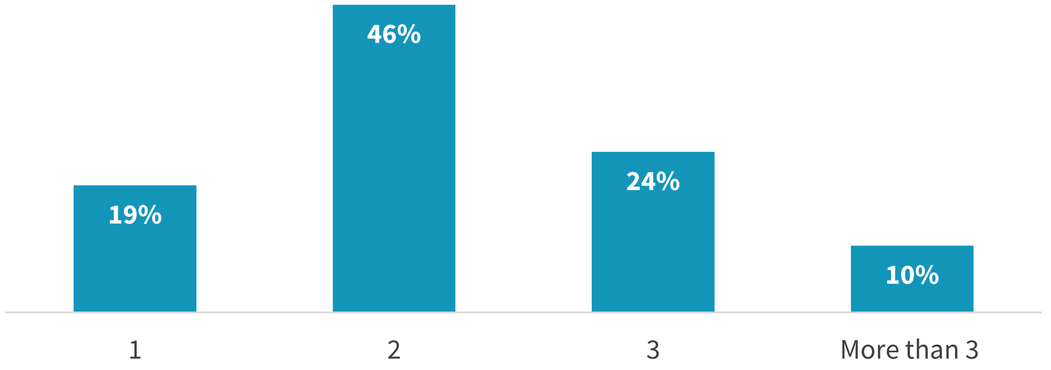
77%

A strategic operating partner **that has improved our overall security program**

Length of time organizations have been working with an MDR provider.



Number of MDR service providers organizations work with.



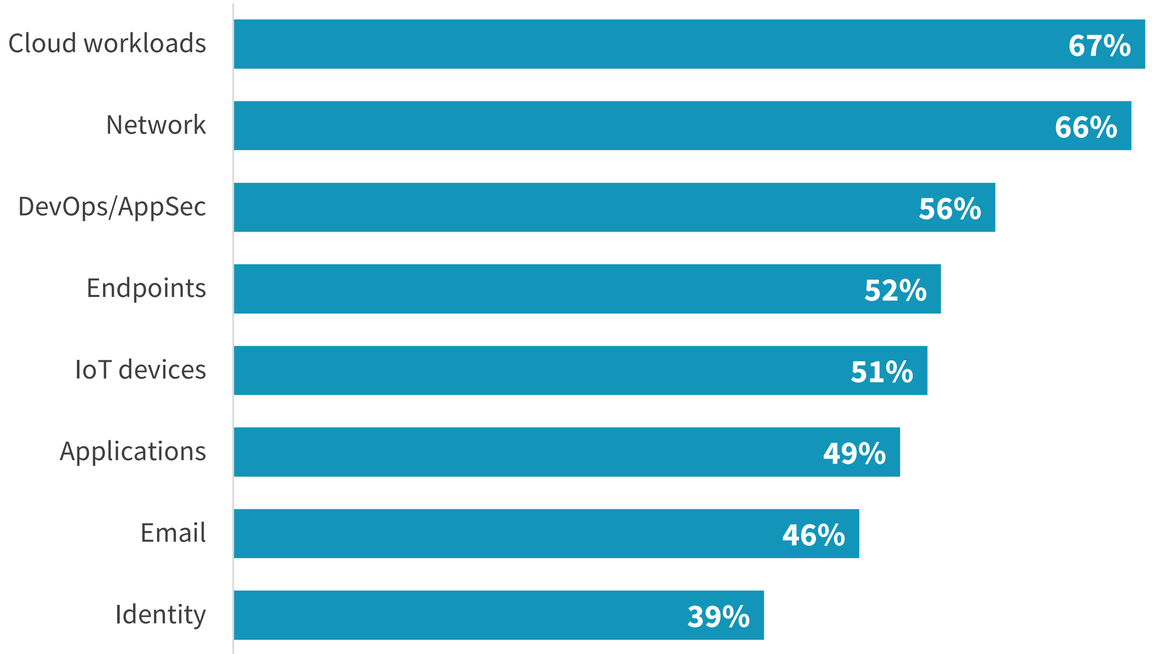
BACK TO CONTENTS

> “Few engage MDR providers **to cover their entire attack surface.”**

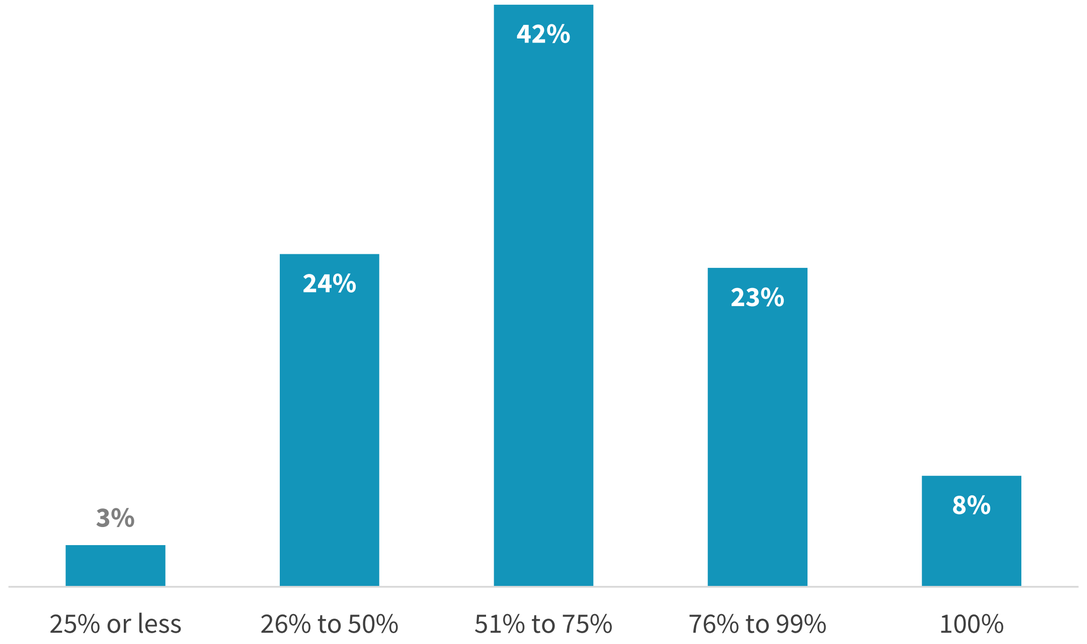
MDR Providers Expected to Monitor All Types of Assets, but Seldom the Entire Estate

When it comes to attack surface coverage, most expect MDR providers to support security operations for all types of IT assets. Yet few engage MDR providers to cover their entire attack surface. Specifically, more than two-thirds report their MDR provider is responsible for covering no more than 75% of their estate, while only 8% indicate their MDR provider covers 100%.

Scope of coverage for organizations’ current MDR provider(s).



Percentage of attack surface MDR provider(s) is responsible for covering.



BACK TO CONTENTS

MDR Is Driving **Positive Security Outcomes**

MDR Providers Are Helping to Improve Onsite Resources and Security Program Maturity

When it comes to actual outcomes achieved, MDR providers are helping organizations experience fewer successful attacks, accelerate overall security program development, and open up investment opportunities in more strategic security initiatives. Specifically, half say that their MDR provider is helping to improve the security skills of their internal resources, and 45% have been able to invest in more strategic security initiatives. More than four in ten report experiencing significantly fewer successful attacks and/or a general improvement in their security program. From a line-of-business perspective, 42% say executives' and/or board of directors' confidence has increased, while 38% report being able to meet compliance objectives or cyber-insurance requirements. Corroborating these positive business outcomes, there was a significant increase in the number of organizations categorizing their security programs' maturity as very mature after engaging with an MDR provider.

Outcomes achieved by leveraging an MDR provider

50%
Improved security personnel skills learned from MDR provider

45%
Investment in more strategic security initiatives

42%
Significantly fewer successful attacks

42%
Significant security program improvement

42%
Increased executives' and/or board of directors' confidence

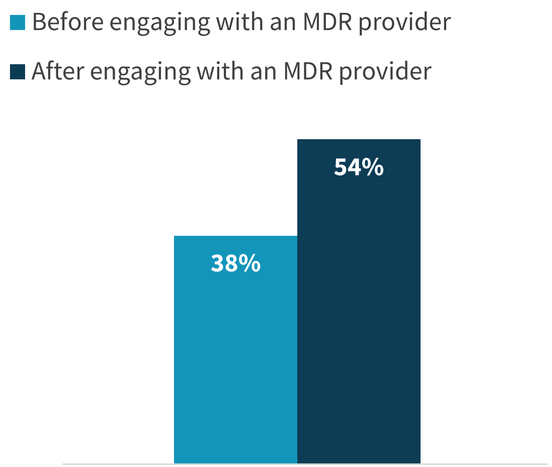
38%
Met compliance/cyber-insurance requirements

38%
Lowered security operating costs

35%
Less stress on in-house security team

32%
Reduced cyber-insurance fees

MDR program maturity.



Very mature (i.e., formal, operationalized processes, experts on staff, full coverage and visibility of the attack surface, risk profiles, formal, rehearsed IR program, IT collaboration, highly effective security tools and analytics, etc.)

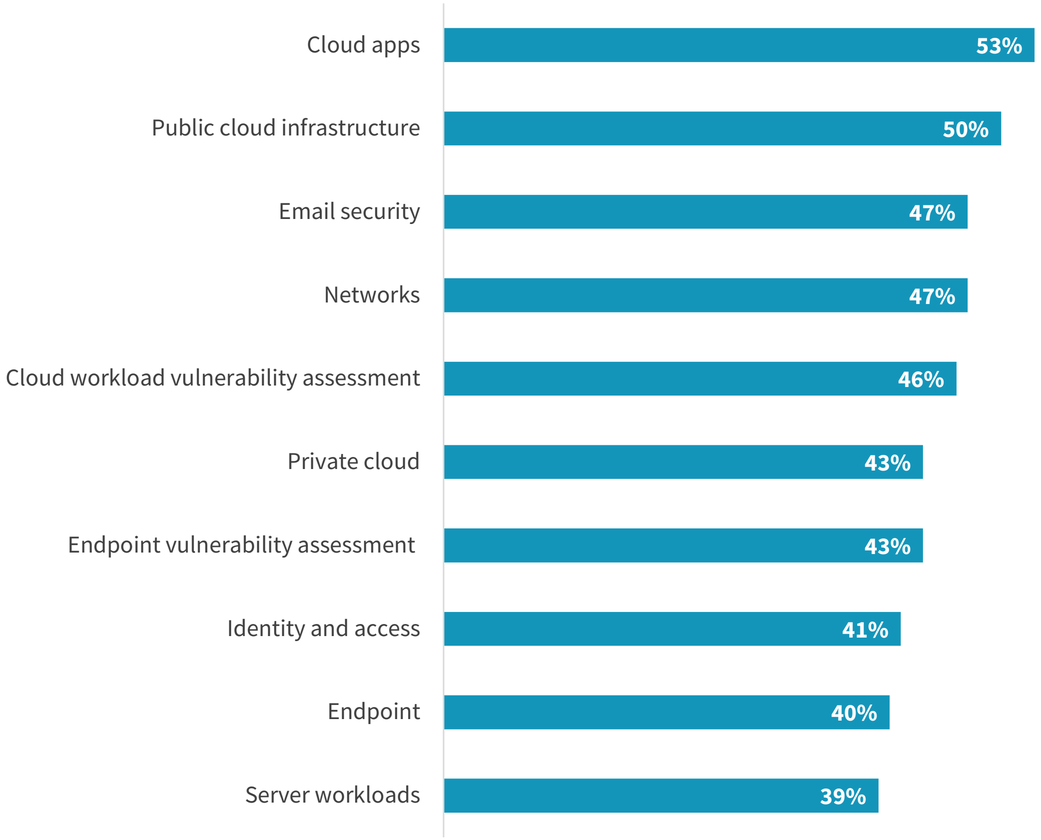
BACK TO CONTENTS


An Open Tech Stack
Is Expected, but
MDR Must Bring All
Mechanisms

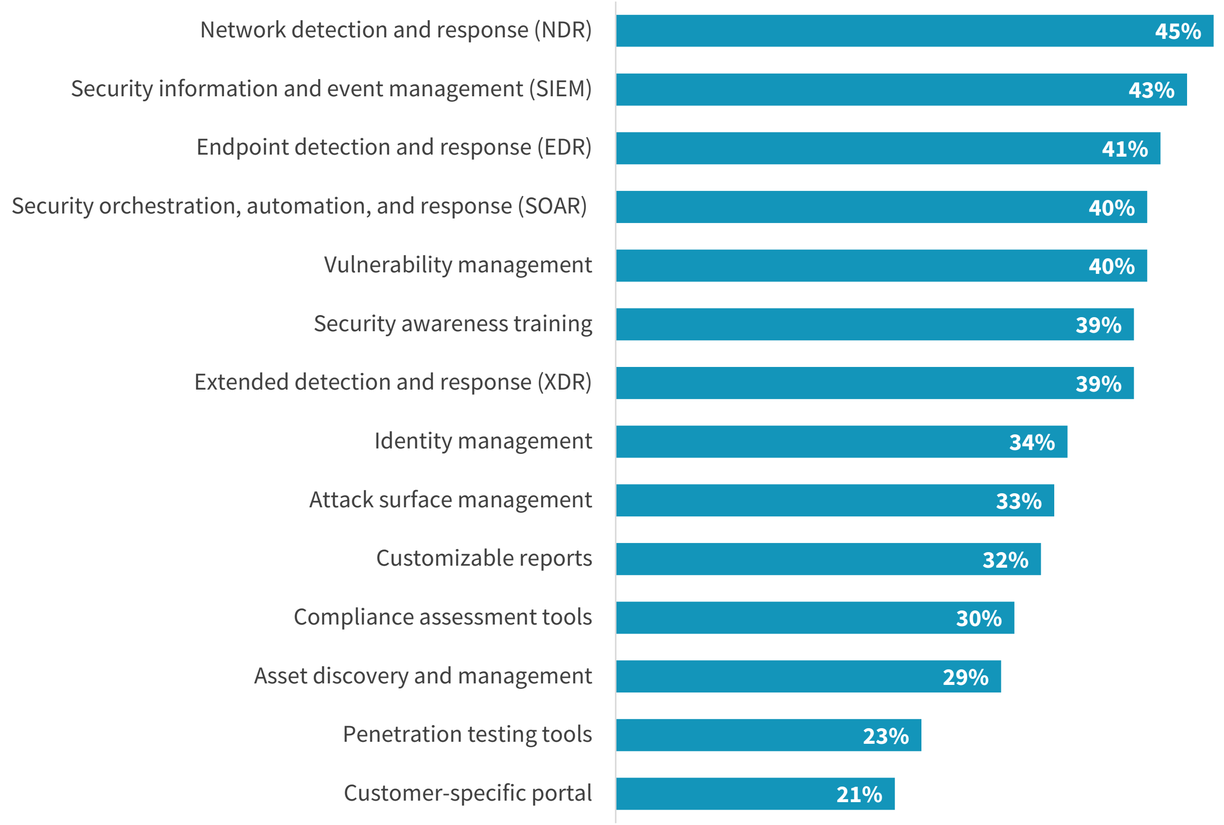
Cloud and Security Operations Are Key Technology Criteria for MDR Selection

MDR customers expect their provider to show up with comprehensive security coverage across all attack vectors. But in addition, MDR users expect their provider to work together with the security mechanisms that are already in place, ranging from a full set of security controls including endpoint, network, cloud, and email, to a full stack of security operations tools including SIEM, SOAR, EDR, NDR, XDR, attack surface management, asset discovery, and vulnerability management.

Detection/agent technologies organizations expect from an MDR provider.



Security operations technologies organizations expect from an MDR provider.



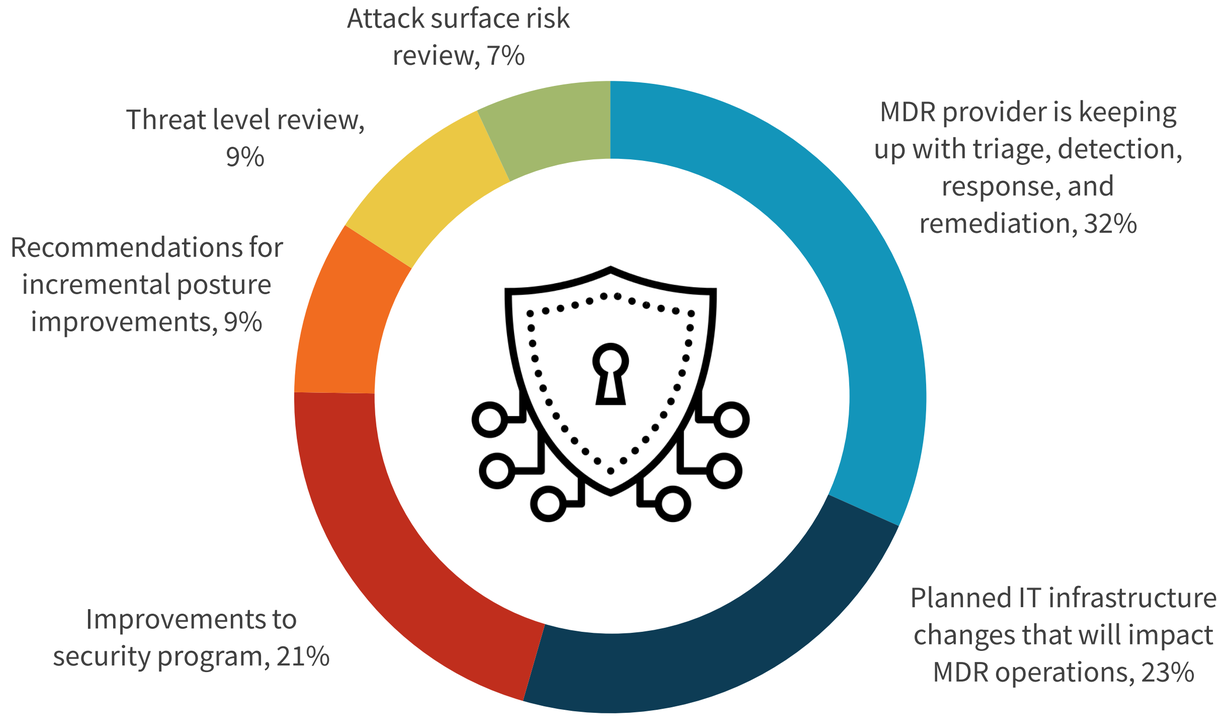
BACK TO CONTENTS

MDR Customer Engagement Models **Matter**

MDR Operational Reviews: What's Most Important

Security leaders stress that MDR engagement models matter a lot, asking MDR providers to not only keep up with their triage detection, response, and remediation, but also stay current with planned IT infrastructure changes, ongoing security program improvements, attack surface risk review, and threat level review—all while recommending actions for incremental security posture improvement. These expectations are high but demonstrate why most organizations consider their MDR provider a strategic partner.

Most important aspect of MDR provider operational reviews.



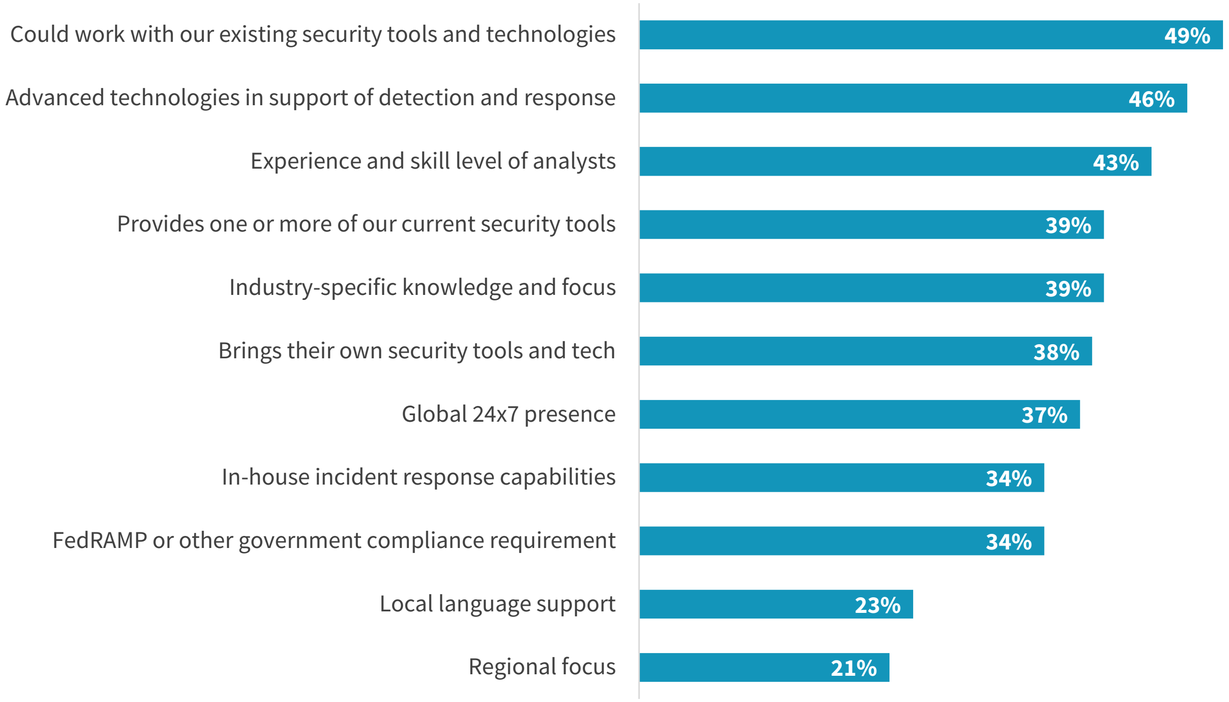
> Security leaders stress that **MDR engagement models matter a lot.”**

BACK TO CONTENTS

Skills and Advanced Tools Have the Ability to Drive MDR Provider Change

What considerations are important to organizations when they are evaluating and selecting an MDR provider? Nearly half (49%) said they must work with their existing security tool and technology ecosystem, while 46% want advanced detection and response capabilities. Another 43% want their MDR provider to have expert security resources, which is also the most commonly cited factor that would cause organizations to change their current provider. Other reasons include more advanced security tools and improved detection and resolution rates, though price and operating models matter, too.

Important selection criteria for MDR providers.



Factors that would motivate organizations to change MDR providers.

BACK TO CONTENTS

Industry Megatrends **Are Impacting MDR Selection**

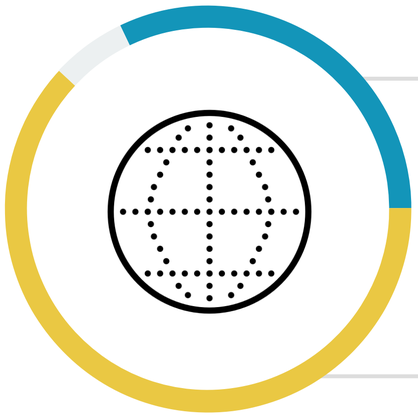
More than nine in ten

organizations identify MITRE ATT&CK support as critical or very important.

MITRE and XDR Support Are Key for Most in MDR Provider Selection

Choosing an MDR provider often involves more than a checklist of capabilities and coverage. Broad industry agendas are further impacting MDR provider selection, with more than nine in ten organizations identifying MITRE ATT&CK support as critical (32%) or very important (62%). Additionally, nearly three-quarters (73%) report extended detection and response (XDR) security technology was considered in the selection process for MDR services. Secure service access edge (SASE) and attack surface management (ASM) were also considered important by two-thirds.

Importance of MDR provider supporting MITRE ATT&CK framework.



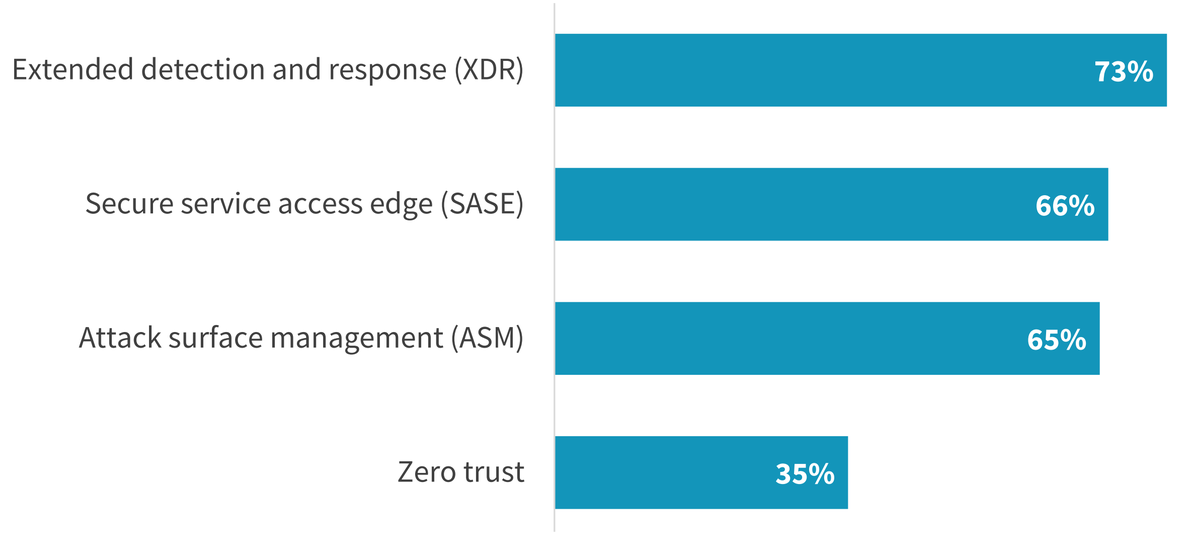
32%

Critical –we would not consider an MDR provider that doesn't support the MITRE ATT&CK framework

62%

Very important –we prefer to work with an MDR provider that supports the MITRE ATT&CK framework but will consider others

Security megatrends considered in the selection process for MDR services.



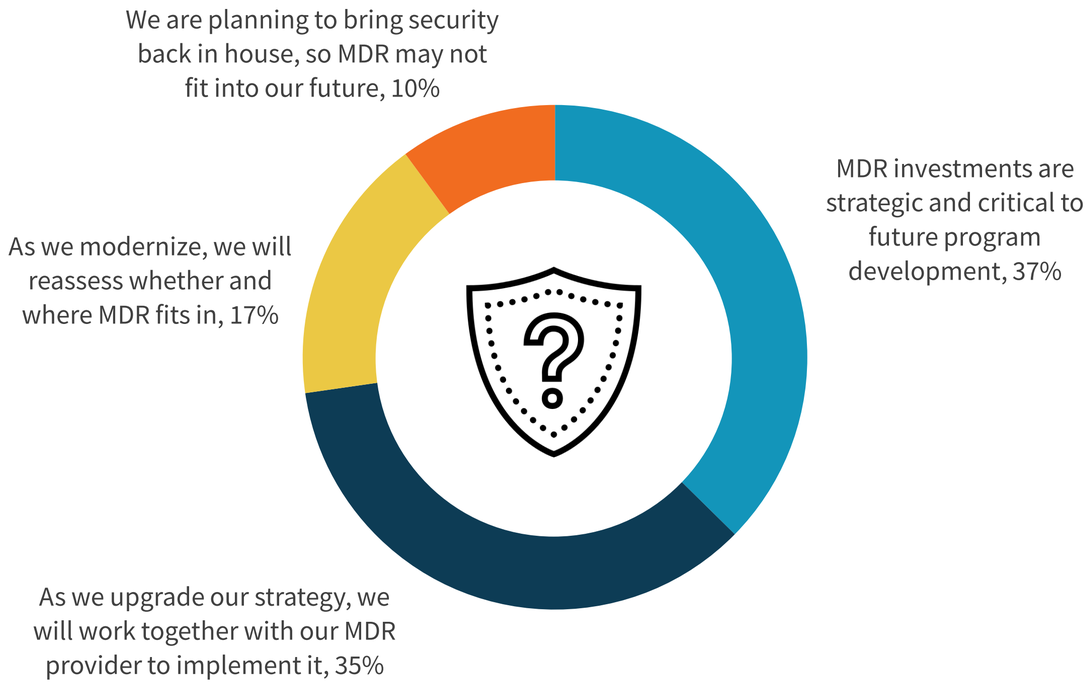
BACK TO CONTENTS

MDR Is Becoming a Mainstream Security Strategy

The use of MDR services has become a core security program strategy component, elevating MDR providers to strategic partners. They help security and IT teams accelerate program development, improve security posture, and reap less visible benefits such as compliance objectives support, cyber-insurance acquisition, and internal security skills and processes improvement. As such, most see MDR as a continuing part of their security program investment, with 37% reporting MDR as strategic and critical, and another 35% planning to work with their MDR provider as they upgrade and implement future security strategies.

ESG considers MDR an important and mainstream security strategy and recommends that organization further explore additional use cases that can accelerate security program development and posture.

Where MDR fits in the broader context of SOC modernization.

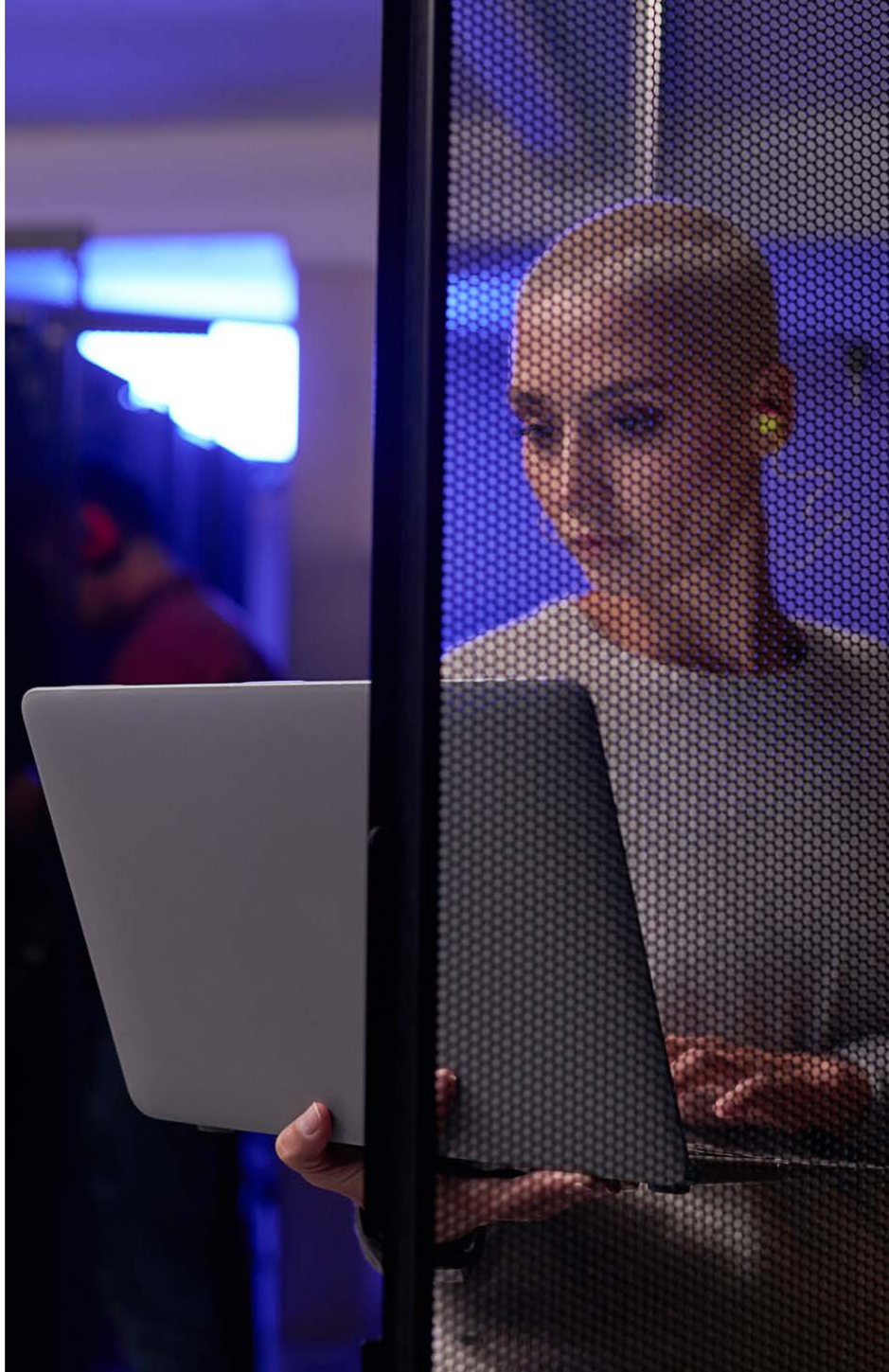


> Most see MDR as a **continuing part of their security program investment.”**

ARCTIC WOLF

Arctic Wolf® is a global leader in security operations, delivering a premier cloud-native security operations platform designed to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes more than two trillion security events a week across the globe, helping enable critical outcomes for security use cases and optimizing customers' disparate security solutions. The Arctic Wolf® Security Operations Cloud delivers automated threat detection and response at scale, and empowers organizations of virtually any size to establish world-class security operations with the push of a button.

LEARN MORE



ABOUT ESG

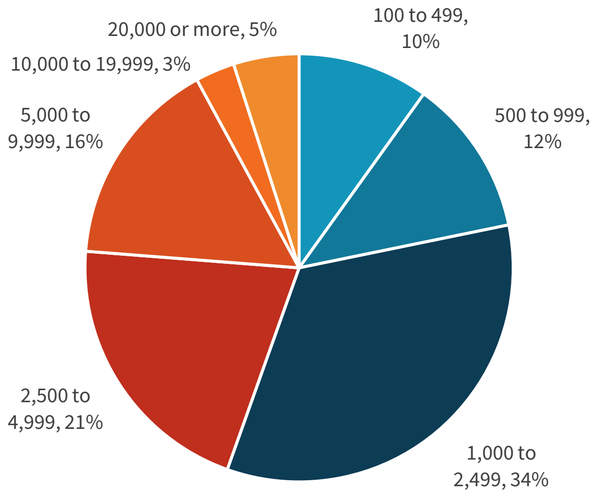
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

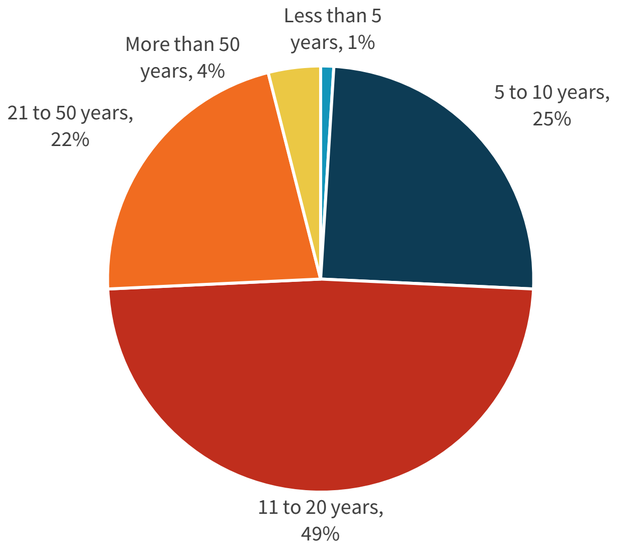
To gather data for this report, ESG conducted a comprehensive online survey of cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between August 3, 2022 and August 14, 2022. To qualify for this survey, respondents were required to be cybersecurity professionals personally involved with cybersecurity technology, including both products and services, and processes. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 373 cybersecurity professionals.

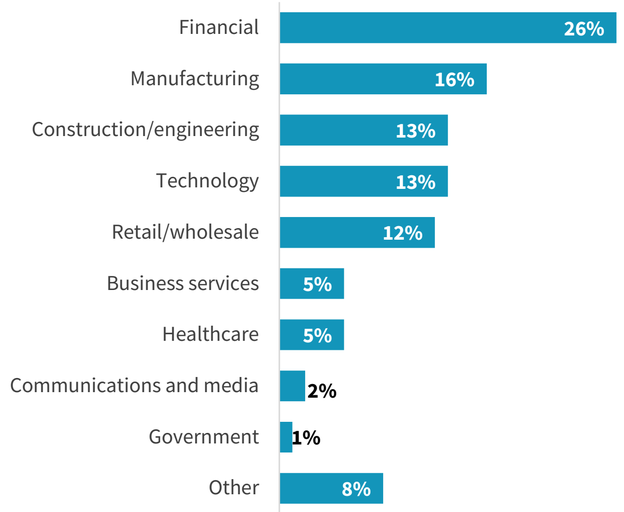
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.