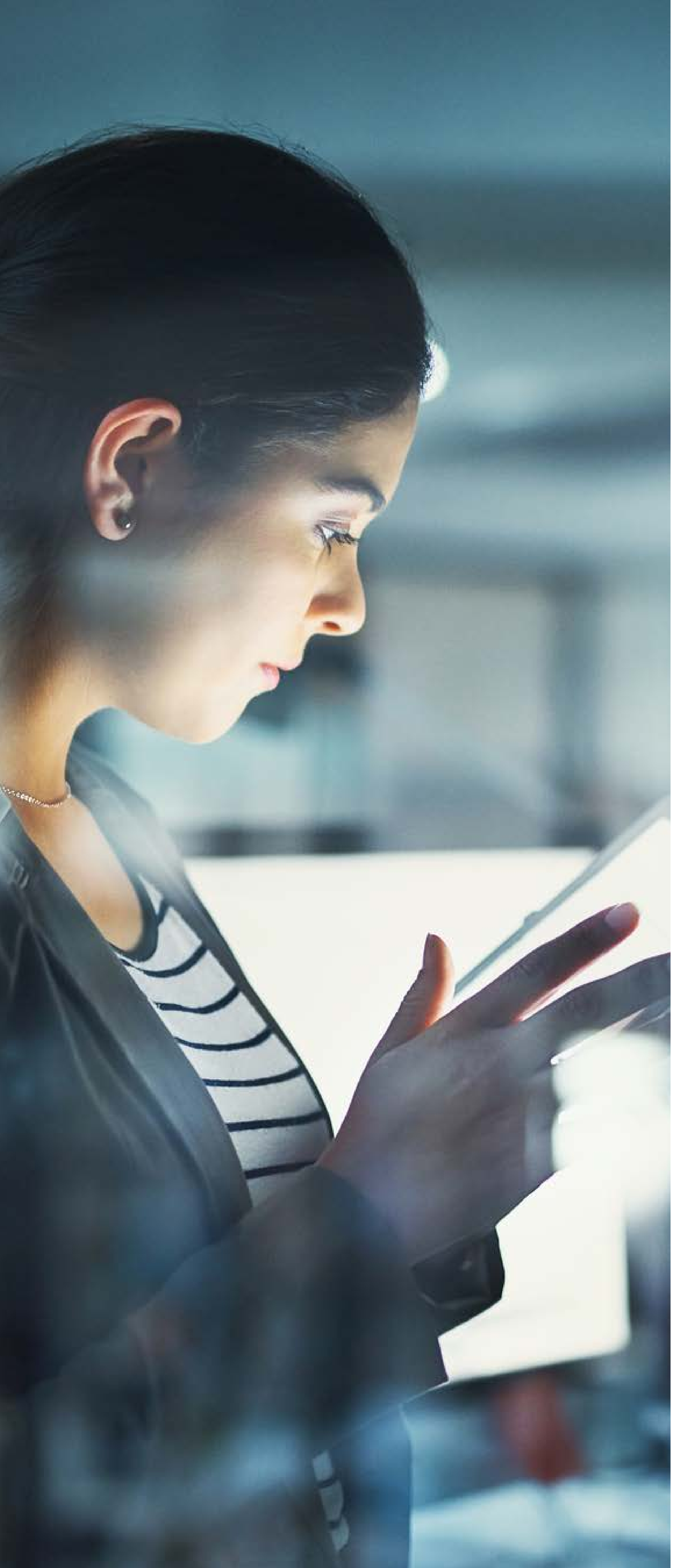
Enterprise Strategy Group™ by TechTarget

Building a Successful Cybersecurity Program

Strategies for the Midmarket

Dave Gruber, Principal Analyst

JULY 2023



Contents

Introduction

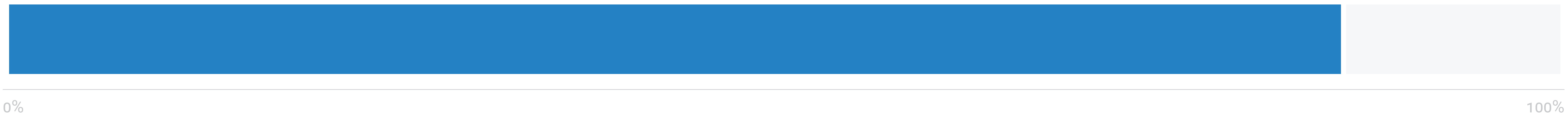
Technology now underlies virtually every aspect of modern business operations, from early customer awareness, consideration, and engagement to support. Connected devices further play a critical role in multiple aspects of business operations and service delivery, with new, more capable and compact offerings further increasing both operational and growth opportunities.

This technology-enabled operating model depends on the continuous availability of applications, services, and devices, escalating the importance of technology and cyber resilience. Any disruption in service can transform a good day into a day of crisis, shining a light on the criticality of continuous connectivity and access to cloud-delivered applications.

While this trend applies to companies of all sizes across all industries, midsize companies often struggle to find the budget, people, and skills needed to operationalize and secure critical infrastructure. Highlighting this issue is the rapid adoption of cloud-delivered applications by midsize organizations, where many are facing a steep learning curve when it comes to managing cloud application cyber-risk.

86%

of organizations are turning to managed detection and response (MDR) providers for help.[1]



The risk of a cyber attack threatens virtually every aspect of operations, increasing the relevance and importance of robust cybersecurity strategies. Research from TechTarget's Enterprise Strategy Group reports that 65% of IT and professionals expect their organization's cybersecurity spending for 2023 to increase compared to 2022.[2] But how can midsize companies effectively mitigate and manage cyber-risk as the use of connected technology accelerates and the cyberthreat landscape becomes more prolific and complex?

Enterprise Strategy Group research reports that more than 86% of organizations are turning to MDR providers for help.[2]

Source; Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.
Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

BACK TO CONTENTS

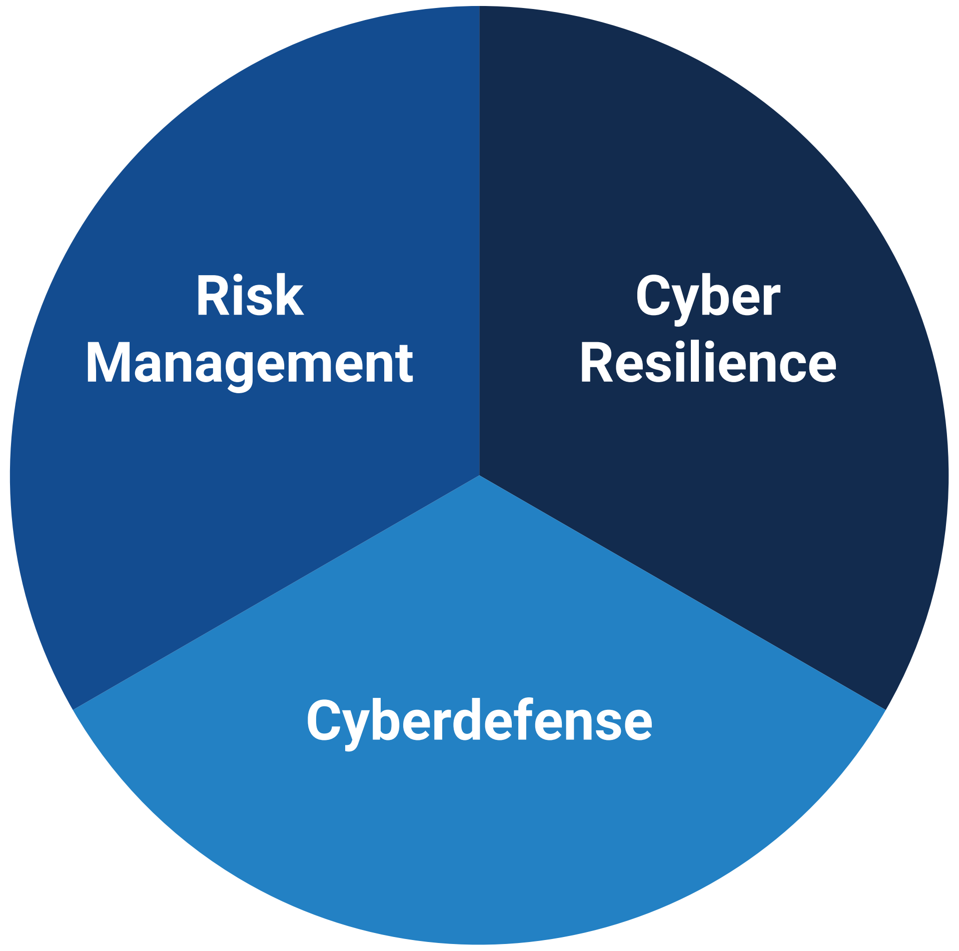
Security Program Fundamentals

Security Program Fundamentals: Resilience, Risk, and Cyberdefense

Security strategies seldom align to a one-size-fits-all model. Security can be very personal. From company to company, an organization's view on risk and priorities, its focus on technology, and its protection of intellectual property will significantly influence its security posture. Security program leaders must craft strategies to support the specific needs of their organization in alignment with their risk management strategies. For some, this means building out a fully customized, highly engineered strategy, architecture, and operational model that aligns to individual security objectives. For others, leveraging more standardized, readily available security frameworks, strategies, and technologies can provide the level of security needed to support the operation.

For all, security is a team sport. Security personnel must work closely with line-of-business leaders, risk management personnel, and all involved in the IT management function. While these functions must work together, each plays a specific role in achieving security programs objectives. Security leaders in midmarket organizations must clearly delegate specific responsibilities within each organization, guiding and measuring progress toward individual objectives.

Security Program Elements



IT teams are generally responsible for implementing and managing a cyber-resilient infrastructure. This means implementing, configuring, and managing networks, systems, applications, and services that are resistant to cyber attacks. In simple terms, IT teams close the front door and windows throughout the infrastructure to avoid knowingly operating vulnerable systems and infrastructure.

Business leaders are responsible for risk strategies, which include understanding critical systems and infrastructure required to maintain business operations and thinking through risk tolerance and risk management practices for each part of the overall operation. Cyber-risk management is now an executive-level responsibility and one that must involve all line-of-business leaders in preparedness activities.

Security teams must focus on cyberdefense and managing cyberthreats. They are responsible for all cyberdefense strategies and operations, which include understanding, identifying, investigating, and responding to cyber attacks that involve all aspects of the operation.

Security Operations Is Becoming More Difficult

Despite the critical importance of cybersecurity risk mitigation, Enterprise Strategy Group research reports that more than half (52%) think security operations is more difficult today than it was two years ago. When asked why, the top five reasons reported were:[3]

41%
The threat landscape is evolving and changing rapidly

40%
The attack surface has grown (i.e., more devices, applications, network traffic, etc.)

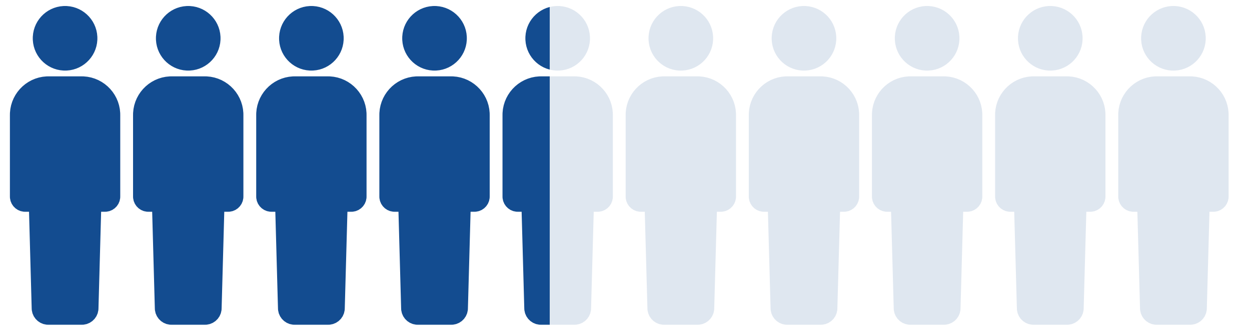
39%
The attack surface is continuously changing and evolving

37%
The volume and complexity of security alerts have increased

34%
My organization's increased use of public cloud services

Those investing in strengthening security strategies face additional headwinds with the continuing, industry-wide shortage of cybersecurity skills. Highlighted in Enterprise Strategy Group research, an acute shortage of experienced, cloud computing security resources are reported as the most difficult for organizations to fill over the last 12-18 months.[4] The use of cloud applications further adds new concerns around the protection of data, including PII, IP, and other sensitive data. Beyond theft of this data, ensuring cloud data is recoverable in the face of ransomware and other advanced threats is causing many to rethink data recoverability strategies.

The threat of ransomware is top of mind for both business and technical leaders, challenging organizations to prepare to respond. This has motivated 44% of organizations to make significant investments tied to ransomware preparedness over the past 12 months, focusing on proactive readiness for IT, security, and line-of-business leaders.[5] Despite these investments, Enterprise Strategy Group research reports that few are prepared for the impending ransomware threat.[6]



44%

of organizations made **significant** investments tied to ransomware preparedness over the past 12 months.

[3] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.
[4],[5] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.
[6] Source: Enterprise Strategy Group Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

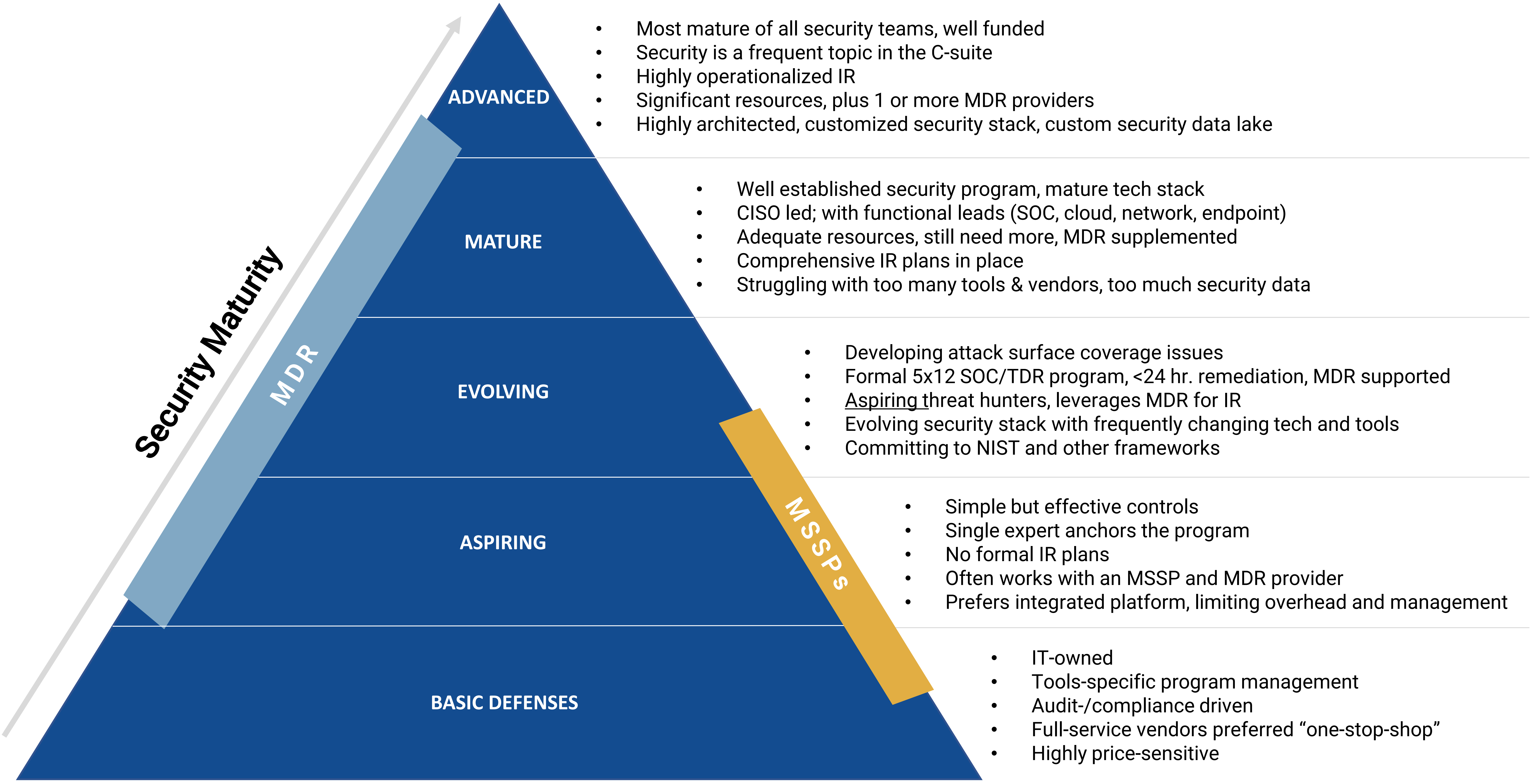
BACK TO CONTENTS

Security Maturity Matters

Security Maturity Model Levels Defined

Enterprise Strategy Group has developed a model categorizing five levels of security maturity that outlines strategies, challenges, and characteristics of how different types of organizations are approaching cybersecurity. While security maturity can, in many cases, be related to company size and the associated financial investment in security program development, Enterprise Strategy Group sees many large companies with relatively immature security programs and, conversely, many smaller companies with very mature security programs. Despite outliers, midsize organizations often fall into “Aspiring” or “Evolving” security maturity levels. As midmarket organizations seek to establish or grow their capabilities, partnering with strategic sourcing partners such as MSSPs and MDR providers offers access to expert-led capabilities.

Five Levels of Security Maturity



Security Maturity

MDR

MSSPs

ADVANCED

- Most mature of all security teams, well funded
- Security is a frequent topic in the C-suite
- Highly operationalized IR
- Significant resources, plus 1 or more MDR providers
- Highly architected, customized security stack, custom security data lake

MATURE

- Well established security program, mature tech stack
- CISO led; with functional leads (SOC, cloud, network, endpoint)
- Adequate resources, still need more, MDR supplemented
- Comprehensive IR plans in place
- Struggling with too many tools & vendors, too much security data

EVOLVING

- Developing attack surface coverage issues
- Formal 5x12 SOC/TDR program, <24 hr. remediation, MDR supported
- Aspiring threat hunters, leverages MDR for IR
- Evolving security stack with frequently changing tech and tools
- Committing to NIST and other frameworks

ASPIRING

- Simple but effective controls
- Single expert anchors the program
- No formal IR plans
- Often works with an MSSP and MDR provider
- Prefers integrated platform, limiting overhead and management

BASIC DEFENSES

- IT-owned
- Tools-specific program management
- Audit-/compliance driven
- Full-service vendors preferred “one-stop-shop”
- Highly price-sensitive

The Road to Cyber Transformation

Building an effective security program begins with building a case for change.

The process involves four phases:

1. MAKE A CASE FOR CHANGE

2. ACTIVATE A PLAN

3. INTEGRATE OPERATIONS

4. OPTIMIZE AND MATURE

1. **Make a Case for Change –** Drivers for change often come from other events or initiatives that are taking place in an organization. These can include IT investments in cloud applications and services, a change in leadership, a significant or near-miss cyberincident, regulatory audit or assessment findings, or a recognized gap in capabilities. Define a vision for what is needed, assess how far away from that vision the current state is, and determine what it will take to move from the current state to the future state.

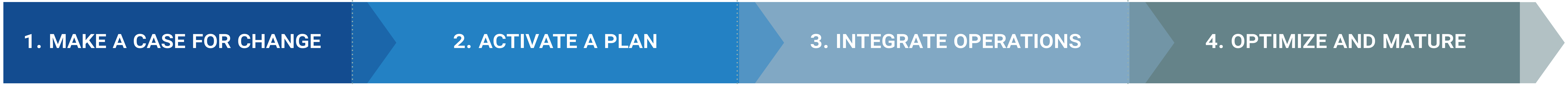
2. **Activate a Plan –** This phase is about outlining the journey that needs to be taken to achieve the desired outcomes. It begins with defining current capabilities and highlighting gaps and deficiencies. In this phase, a clear definition of the desired end state will be described, including what is to be protected, how effective current strategies are, and the beginning of a security roadmap. In this phase, the project scope will be defined, a sourcing strategy will be developed, and any external partners will be identified. This is needed to socialize the business case with all stakeholders to drive agreement on the approach and determine where funding will come from and the expected timeline. Appoint an internal executive owner of cyber-related business risk. Virtual chief information security officer (vCISO) and external security advisory services can be used to strengthen executive oversite.

3. **Integrate Operations –** Much of the implementation work happens in this phase, this includes both technology and process uplift. Talent, service provider partnerships, and technology acquisitions happen in this phase, together with the creation of an operating model and procedures. Focus on accelerating activities that will provide the highest impact measured in business risk reduction. MSSP and MDR providers can offer fully built functions that can accelerate security operations adoption.

4. **Optimize and Mature –** The final phase is a fully operational security function that meets the initial vision established in Phase One. Here, operational metrics are monitored with an eye on continuous improvement as the program progresses. Any gaps are identified and addressed during the process. Introducing continuous security testing capabilities will provide a mechanism to prioritize visibility gaps and program weaknesses.

BACK TO CONTENTS

A Blueprint for Cybersecurity Transformation



1. MAKE A CASE FOR CHANGE

OBJECTIVE

Establish a case for cybersecurity transformation and define a future state vision.

OUTCOMES

- What are we protecting?
- What does good look like, and how far are we from good?
- How quickly must we mature, and what resources will be needed?

2. ACTIVATE A PLAN

OBJECTIVE

Perform a security capabilities assessment and start an initial security program roadmap.

OUTCOMES

- Define cyber-risk ownership and program sourcing strategy.
- Select security service and technology partners.
- Document a near-term maturity roadmap.

3. INTEGRATE OPERATIONS

OBJECTIVE

Deploy critical program capabilities first with a focus on talent, technology, and process.

OUTCOMES

- Appoint and source core team members.
- Adopt foundational policies and procedures.
- Implement defensive and proactive technologies.

4. OPTIMIZE AND MATURE

OBJECTIVE

Adopt a continuous improvement mindset and continue to reduce cyber-risk through ongoing program maturity.

OUTCOMES

- Adopt key metrics.
- Test, validate, and harden defenses in a continuous manner.
- Define and action longer-term roadmap goals.

Getting Expert Help

Getting Expert Help

Organizations are planning services investments to assist with many aspects of cybersecurity, including services such as security operations-as-a-service, managed security services, incident response services, and compliance services.[7] Managed detection and response providers are widely utilized by organizations across all levels of security maturity, closing program gaps and providing experts, additional staffing, proven processes, and advanced security technologies that support organizations' security objectives.

Managed service providers (MDRs, MSSPs, etc.) often deliver multiple services in support of security program needs, such as:

- **Security program assessment.**
- **Security program strategy development.**
- **Security operations (alert assessment, triage, investigation, and response).**
- **Vulnerability assessment and management.**
- **Suspicious email investigations.**
- **Incident response services.**
- **Penetration testing and other offensive testing.**

Some providers bring their own tech stack while others can interoperate with existing security and IT tools. Industry specialization and experience can also play a role in finding the right provider for an organization.

Other considerations include where and how technology can fit into future operational objectives, ensuring that a provider can support both current and future requirements. A majority of service provider engagements continue and expand over time, with Enterprise Strategy Group research finding that 82% of organizations report using their MDR providers for three or more years,[8] so thinking about potential future needs in both capabilities and scalability are key considerations to ensure a provider can grow to support your program needs over time.

It is also important for organizations to consider what cybersecurity challenges are most acute currently. Enterprise Strategy Group research also shows that organizations often begin by supporting a portion of their infrastructure to fill immediate gaps, then expand services and coverage over time.[9]

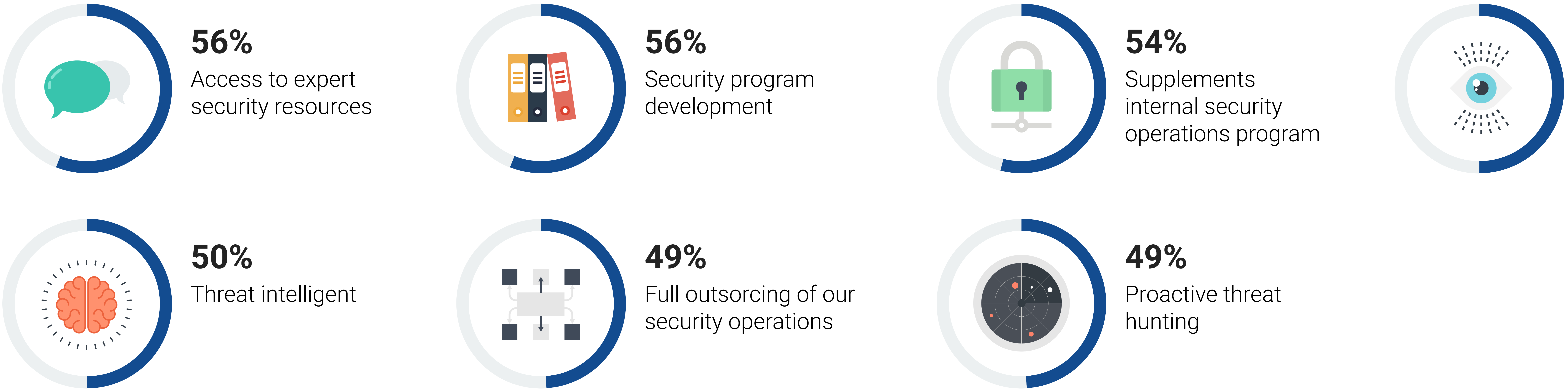
82%

of organizations report using their MDR providers for three or more years.

[7] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.
[8],[9] Source: Enterprise Strategy Group Research Report, *What Security Teams Want from MDR Providers*, March 2023.

BACK TO CONTENTS

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 intelligent

49% Full outsorcing of our security operations

49% Proactive threat hunting

Conclusion

Cyberthreats are accelerating faster than most corporate security teams can keep up. These security teams need help from a plethora of security technologies and skilled cyber-resources to help manage threats.

Security service providers are partnering with security program leaders in support of organizations’ business goals to close program gaps and accelerate overall security program development. Service providers bring security experts, proven processes, and advanced technology needed to modernize security programs, helping midmarket organizations accelerate maturing their capabilities and prepare for future growth.

Enterprise Strategy Group considers MDR a mainstream component for modern security program strategies and recommends midsize organizations leverage MDR and risk services from vendors like DeepSeas to accelerate security program development and transformation and ensure operational resilience. Often operating more as strategic partners, MDR providers can offer IT and security leaders long-term guidance and support of security program development, growth, and operationalization.

Introducing DeepSeas Managed Detection and Response

Bringing 30 years of experience, DeepSeas provides managed detection and response services that cover the entire converged attack surface for midmarket organizations, including OT, IT, cloud, and mobile. Leveraging deep expertise that combines world-class cyberthreat detection with industry-leading analysts, tailored threat intelligence, and accredited incident responders, DeepSeas is always on and always watching. Its Managed Detection and Response offerings, DeepSeas MDR+, and its full-spectrum cyberthreat monitoring service are award winning and backed by world-renowned researchers, data scientists, and mathematicians who have published over 250 papers and created a broad base of intellectual property while achieving a number of scientific breakthroughs in the areas of big data, machine learning, and artificial intelligence as they apply to the detection of advanced and unknown cyberthreats.

Leveraging their experience and backgrounds from serving the U.S. intelligence community and military, Fortune 500 cyberdefense teams, and world-class enterprise security consulting firms, DeepSeas experts help transform cyber programs for organizations of all sizes in both the public and private sectors. This includes both proactive assessment services to identify program maturity, gaps, and opportunities, together with ongoing operational capabilities to monitor and mitigate threats. DeepSeas handles the “last mile” of cyberdefense, providing capabilities often unavailable from other service providers.

Expertise Powered by a Proprietary Cyber Defense Platform

Armed with AI-based proprietary technology within the DeepSeas Cyber Defense Platform, DeepSeas experts use leading tradecraft to identify and respond to threats fast and efficiently. The DeepSeas platform includes comprehensive capabilities that supports the detection of both known and unknown threat vectors across all attack surfaces while integrating, orchestrating, and optimizing existing tools used to monitor and control attack surfaces. These platform and expert capabilities support both IT and OT environments, providing comprehensive, integrated defenses for all types of threats.

DeepSeas works together with other security tools and platforms, utilizing an open vendor ecosystem that includes support for best of breed security vendor solutions.

EXPLORE MORE

DEEP seas

Enterprise Strategy Group™ by TechTarget

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.