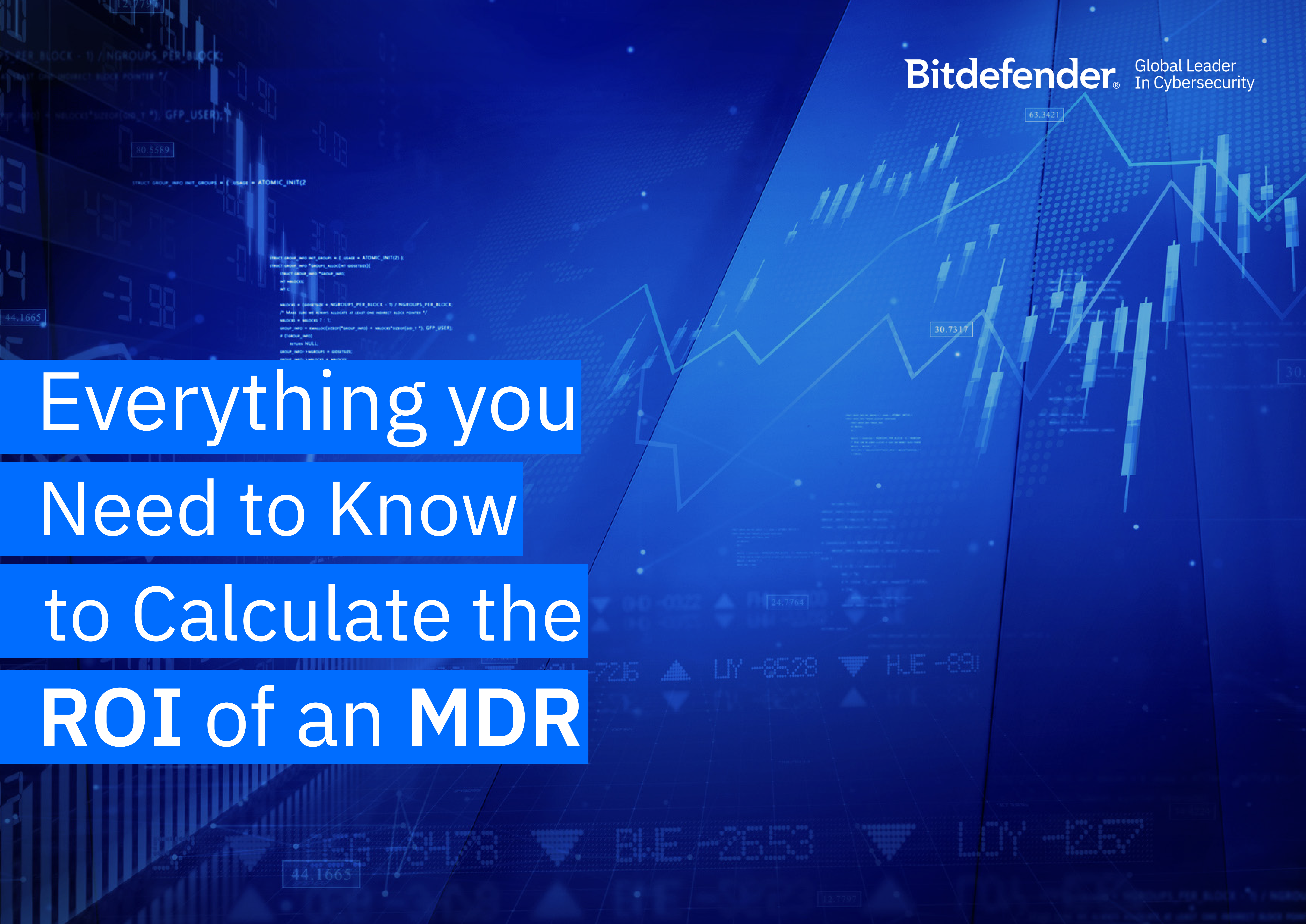


Bitdefender Global Leader In Cybersecurity

Everything you Need to Know to Calculate the **ROI** of an **MDR**

Table of contents

Introduction

In the face of increasing complex cybersecurity threats, organizations invest in plenty of security tools but often struggle to operationalize them. They are faced with a decision: Do they build out a cybersecurity team internally to monitor, detect and respond to threats or do they seek outside help looking to partner with a trusted security provider like a Managed Detection and Response company? How do organizations determine the Return on Investment (ROI) of each approach and maximize their cybersecurity investments without compromising security?

In this guide, we will go over the various factors organizations must consider when creating a cybersecurity program and how to think about the costs of the various options and approaches they can take. We'll lay out the variables that must be considered and how to calculate the values to the primary question of "Build vs Buy".

Minimum Salary Cost of a Security Team?

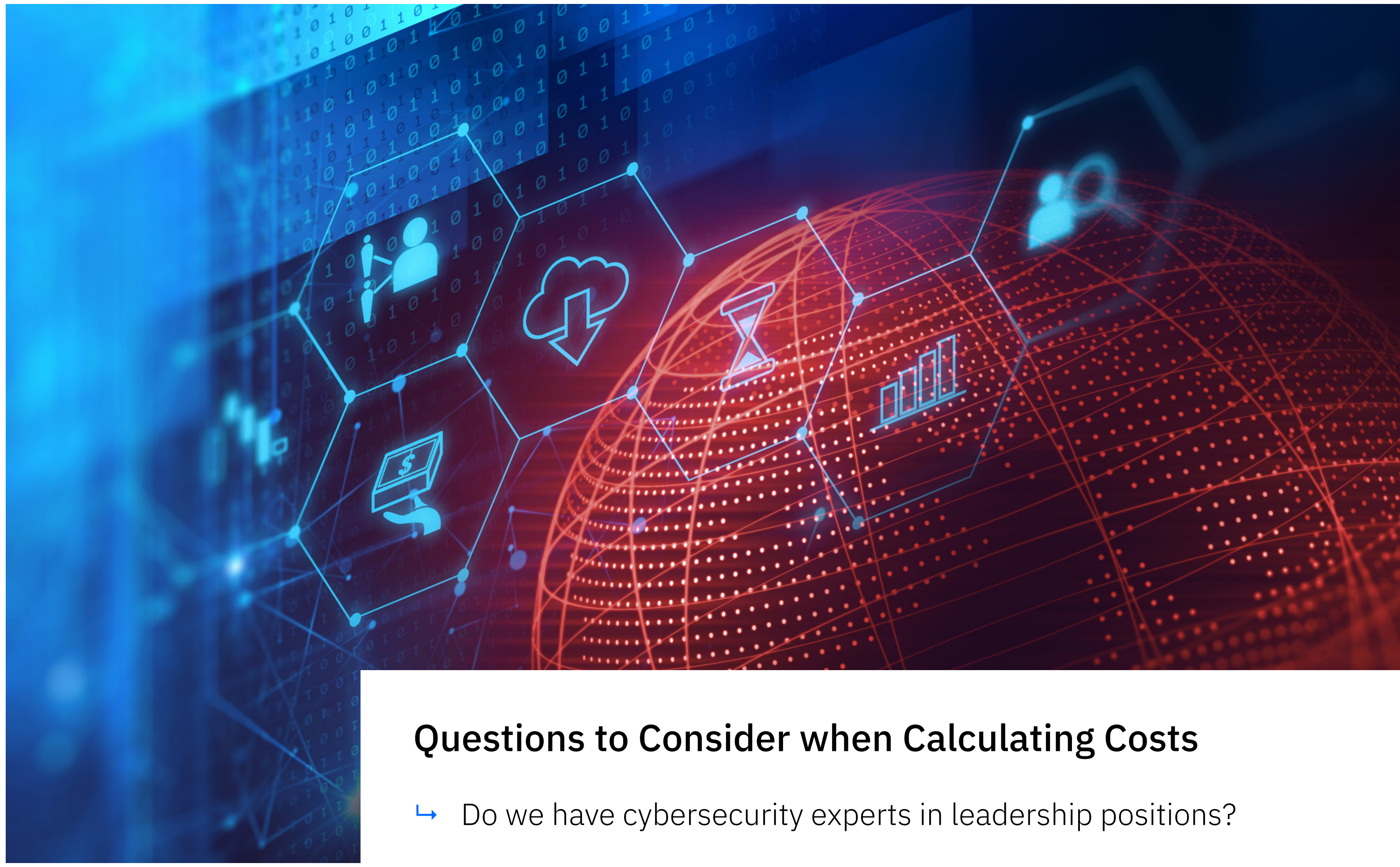
Cost Savings of an MDR?

The Foundations of a Cybersecurity Program

Before diving into the exact cost calculations, it's important to establish the components of what make up a proper cybersecurity program. While outside the scope of this eBook, cybersecurity frameworks, such as NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), can help organizations understand each area that they must protect and prioritize accordingly. NIST CSF 2.0 can provide a guide for identifying what components organizations have and which components they need and how to prioritize them.

Here's some sample responsibilities and requirements for each of the six functions that can be used as a starter guide:

Govern	Identify	Protect	Detect	Respond	Recover
Cybersecurity Knowledge / Leadership	Identifying Organizational Assets	Tools to Protect Assets	Tools to Monitor Events in Real-Time	Tools to Respond and Remediate Threats	Disaster Recovery / Business Continuity Plan
Ability to Develop and Implement a Cybersecurity Plan	Tools to Manage Assets	Identifying and Addressing Vulnerabilities (Pen Test, Red Teaming, etc)	Team to Monitor and Investigate Events: Threat Researcher, Detection Engineer, Security Analyst.	Team to Perform Response and Remedition: Threat Responder, Incident Handler	Team and Time to Test Plan
Hiring / Training a Team	Team to Manage the Tools	Team to Manage Tools and Vulnerabilities			Backup and Recovery Software
		Policies and Plans to Mitigate Risks			



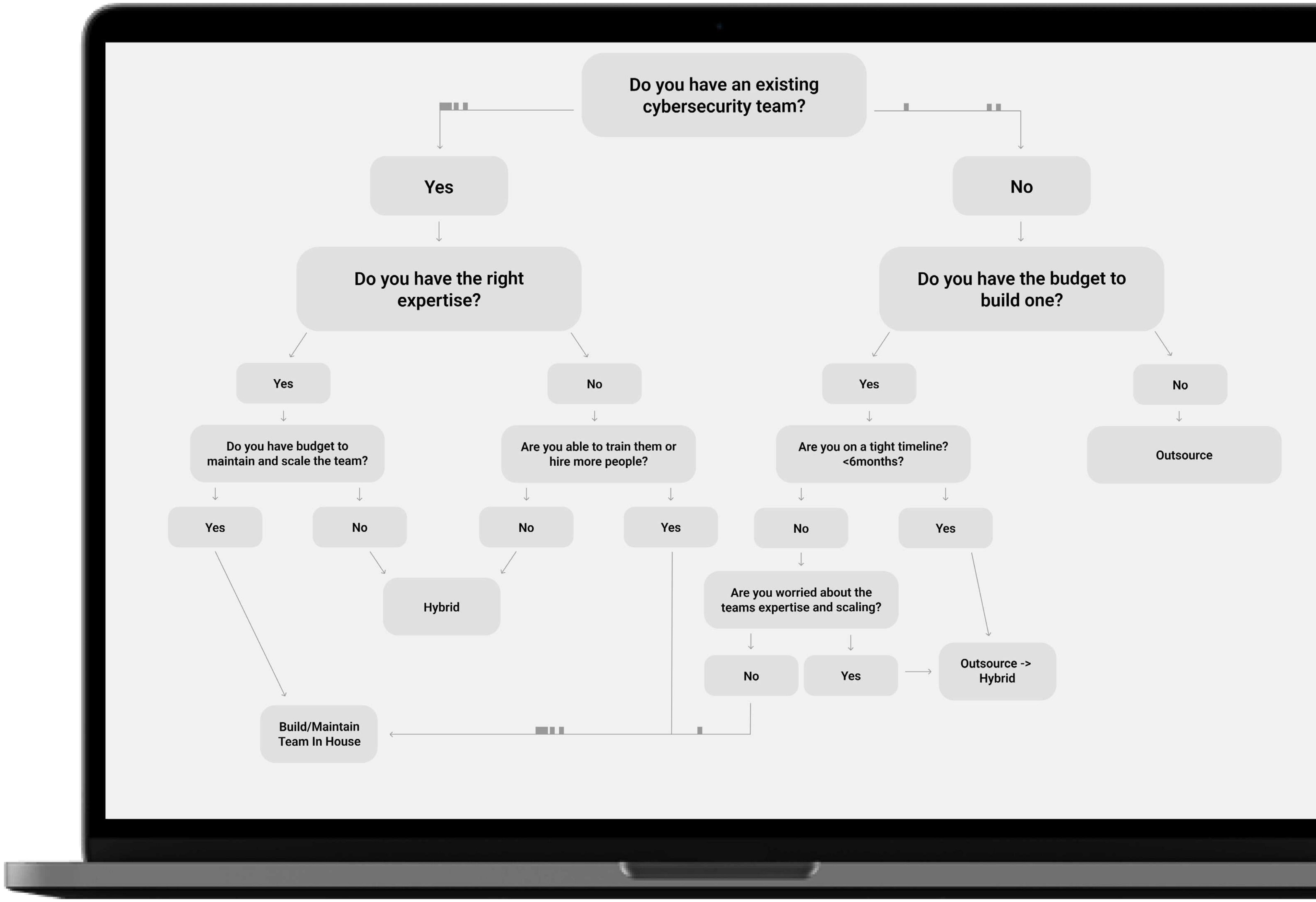
Questions to Consider when Calculating Costs

- Do we have cybersecurity experts in leadership positions?
- Do we intend to have 24/7 threat monitoring and response capabilities?
- Do we have the budget and resources to build a team in-house?
  - How big of a team do we need?
- What is our timescale for getting a program running?
  - How quickly do we need to move?
  - How long will it take to interview, hire, and onboard a team?
- What and how many security tools do we need
  - Is our team able to operationalize them?
- How will we test our defenses, identify security gaps, and apply continuous improvement?
- How are we accounting for the possibility of a breach?

The Options: In-House vs Outsourced vs Hybrid

Organizations have a few options in addressing cybersecurity needs: build a dedicated team in-house, outsource many of the cybersecurity responsibilities to a trusted third-party security partner, or a hybrid approach where they co-manage the responsibilities and tasks with a security partner. While there are many factors that play into this decision, it often comes down to the available budget and resources and the ability to hire and maintain a team of full-time equivalent (FTE) security experts across various roles.

Which approach works best will be unique and different for every organization. It's also worth noting that the costs are not just the direct cost of the salary of the employees on the team, but the indirect costs such as the time to build and maintain a team or predicting the cost (both monetarily and reputational) of a potential breach.



Do you have an existing cybersecurity team?

Yes

Do you have the right expertise?

Yes

Do you have budget to maintain and scale the team?

Yes

No

No

Are you able to train them or hire more people?

No

Yes

Hybrid

Build/Maintain Team In House

No

Do you have the budget to build one?

Yes

Are you on a tight timeline? <6months?

No

Are you worried about the teams expertise and scaling?

No

Yes

Yes

Outsource -> Hybrid

No

Outsource

Determining the Approach

Choosing which approach is best will be heavily dependent on the existing staff, budget, resources, and time available to each organization. Each option has its own pros and cons and organizations may prioritize or value the benefits differently based on their own unique circumstances. Here are some sample Pros and Cons, but are not an exhaustive list:

Building In-House

Pros	Cons
Improved Control and Customization	High Initial Cost
Agility and Quicker Response	Talent Retention and Scalability
Enhanced Visibility Over Org Infrastructure	Lack of Specialized Knowledge and Limited Threat Experience
Easier to Manage Confidentiality, Compliance, and Data Security	Lost Opportunities for Other Strategic Initiatives

Outsourcing / Hybrid

Pros	Cons
Cost - Effective Solution	Less Direct Control
Rapid Deployment, 24/7 Coverage, and Scalability	Dependence on Third - Party SLA Performance
Access to Advanced Security Expertise and Technology	Sharing Sensitive Data and Security Concerns with Third - Party
Lower Risk of Burnout and Turnover	Lack of Unique Organizational Knowledge
Broader Threat Intelligence and Ongoing Threat Research, Innovation, Improvement	Service Limitations or Gaps Based on Unique Organizational Needs

How to Calculate Cost and ROI

With the pros and cons of each option in hand, organizations now have a list of items they can compare against each other to calculate the cost savings and ROI they can get by partnering with the right security vendor.

Salary Cost of Building a Team

Building an internal security team that will monitor and be able to respond 24/7 will require a fairly extensive staff. Here is a quick calculation for the minimum required size of a team to get started:

Building a Team

Three 8-hours shifts

+ 7 days a week

+ 2-3 FTEs per shift

+ $100,000 - $150,000 Salary

$800,000-1,800,000 Cost of Team

Organizations looking to keep smaller cybersecurity teams can do so at the expense of coverage. For example, some organizations staffing five or less FTEs will likely not be able to support true 24/7 coverage, instead having the team only active during working hours and relying on team members receiving alert notifications to respond overnight or on the weekends. Risk appetites will need to be weighed by the organization and will factor into the cost of building a team or partnering with a trusted security vendor.

Sample Cost Comparisons

Components	250 Employees	1000 Employees	5000 Employees
FTE Staff	2 - 3	5 - 10	15+
Coverage	8 x 5	8 x 5 or 24/7	24/7
Salary (+benefits)	$100,000-$150,000	$100,000-$150,000	$100,000-$150,000
Cost of Team	$200,000-$450,000	$800,000-$1,800,000	$1,500,000-$2,250,000+
MDR Cost Savings	**60 - 90%**		

MDR

24/7 Coverage

+ MDR provides all FTEs

+ Only cost of the license subscription

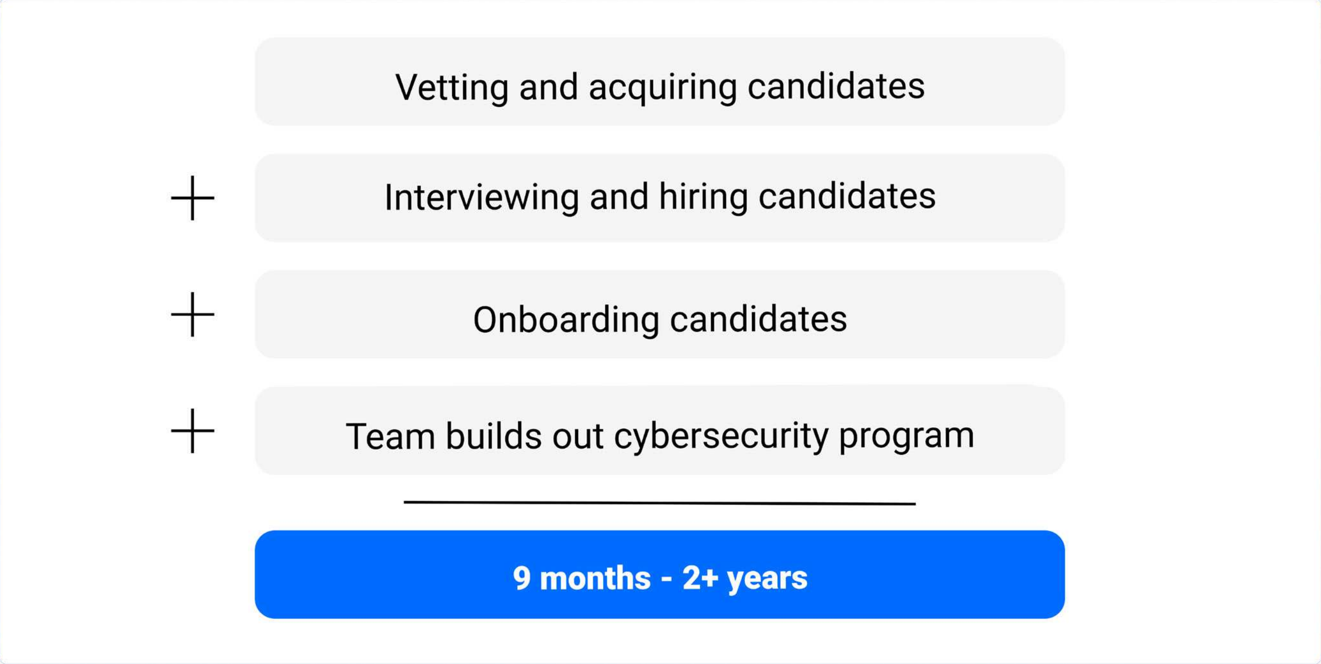
MDR Savings of 60 - 90%

Organizations can get greater security monitoring, detection, and response from accredited security experts at a fraction of the cost of attempting to build it out internally. MDRs provide equal or even greater security protection 24/7 saving companies up to 90% in direct costs.

Time and Resource Cost of Building a Team

Building an internal security team takes time and organizations are not guaranteed to find the best talent.

Building a Team



Vetting and acquiring candidates

+ Interviewing and hiring candidates

+ Onboarding candidates

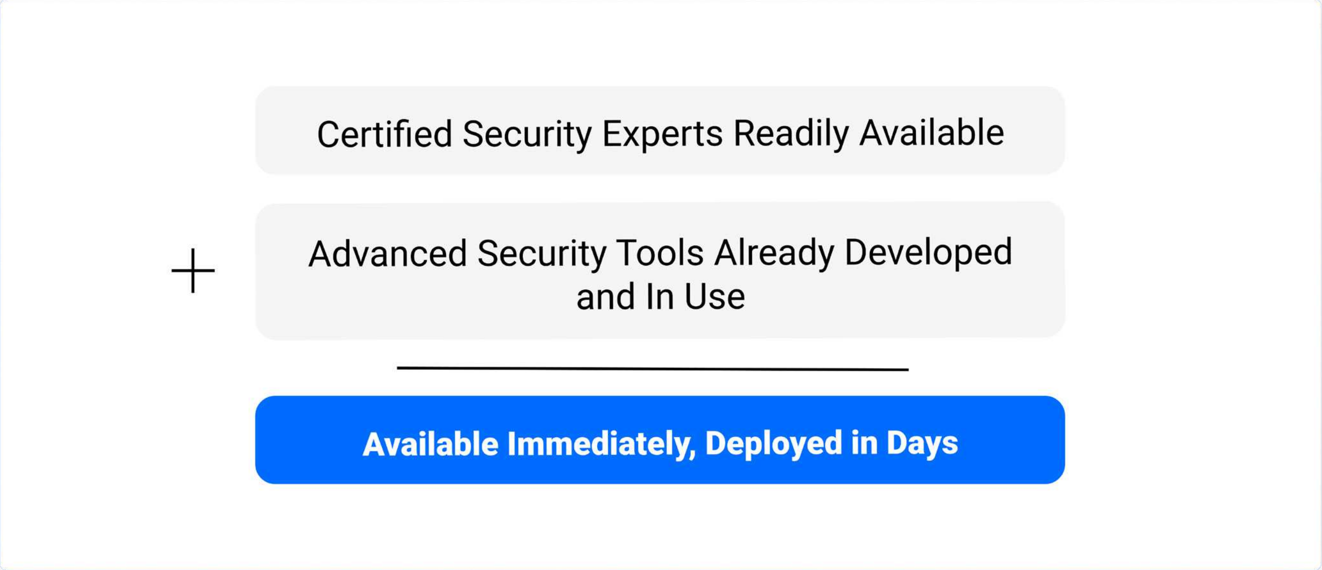
+ Team builds out cybersecurity program

9 months - 2+ years

Year over year, studies have shown that the cybersecurity skills shortage continues to grow with the workforce gap reaching 4.8 million globally. This increases the time to vet and interview candidates while also increasing the competition and minimum salary offer required. Even if a team can be fully hired for, it will still take time for onboarding and building the cybersecurity program from scratch. Organizations must calculate the risk cost of this downtime.

Year over year, studies have shown that the cybersecurity skills shortage continues to grow with the workforce gap reaching 4.8 million globally.

MDR



Certified Security Experts Readily Available

+ Advanced Security Tools Already Developed and In Use

Available Immediately, Deployed in Days

MDRs have the security teams and people in place allowing for quick and immediate deployment. They also have the internal tools necessary for threat detection and response and will help operationalize the organization’s security tools to achieve value within days, rather than months or years.

Cost of a Breach

While it's impossible to calculate the cost of a potential breach since each org is unique, using global research into breaches can help organizations understand the average cost resulting from breaches and use that to forecast their own possible cost and risk evaluation. Studies have consistently found that the cost of a data breach increases year over year.

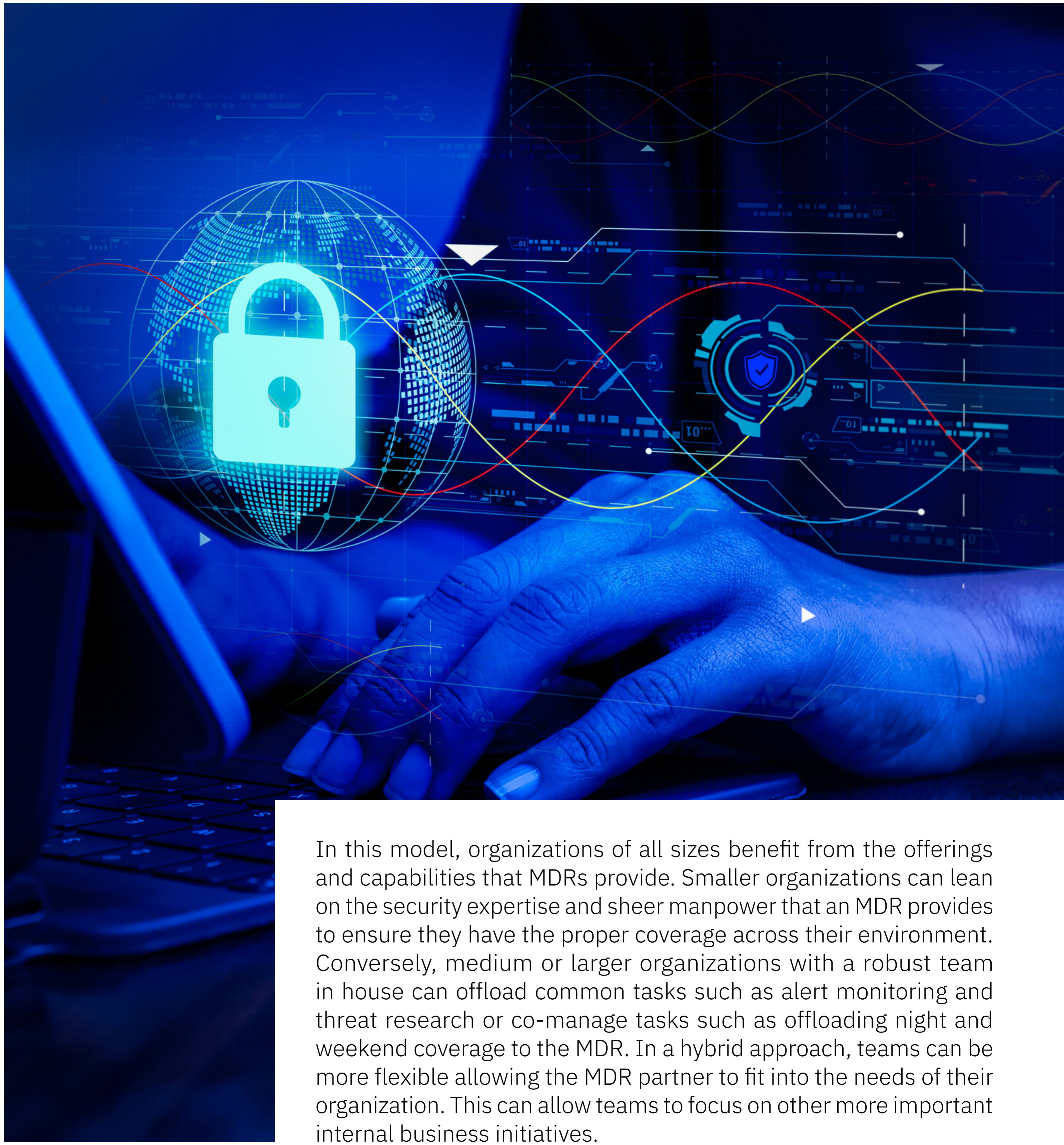
> According to Forrester's[1] data, "global security decision-makers reported that their organizations experienced 4.8 breaches on average in the past 12 months...[and] that the breaches that their organization experienced in the past 12 months averaged $3.6 million in total cumulative breach costs." Similarly, another Forrester report[2] notes that "global security decision-makers who cited a lack of adequate incident response preparation as a top information/IT security challenge at their organization spent a mean of $204,000 more on breaches over 12 months than all survey respondents. They also experienced almost one more breach annually."

In essence, the frequency and cost of breaches continue to rise and organizations without a proper cybersecurity program or organizations that are unprepared to handle detection and response, see more breaches on average with those breaches costing more. Organizations must prioritize their ability to detect and respond to threats and choosing the right option that meets their need will help mitigate breaches from occurring, saving them money in the long run.

Why a Hybrid/Co-managed Approach is Right for Everyone

A hybrid, or co-managed, approach combines elements of having a team in place to handle specific tasks or things that must be kept in house while partnering with an MDR or trusted security provider to outsource common tasks or to supplement the internal team.

In-House	Co-Manage / Outsource
Unique or Uncommon Threats	Common or Universal Threats
Involves Sensitive Internal Knowledge or Data	Resources, Budget, Time are Unavailable
Requires Sensitive, Internal Only Communication	Tasks are Common or Can be Offloaded
Involves High-Risk / High-Value or Strategically Important Tasks	Lack Experience or Security Expertise



In this model, organizations of all sizes benefit from the offerings and capabilities that MDRs provide. Smaller organizations can lean on the security expertise and sheer manpower that an MDR provides to ensure they have the proper coverage across their environment. Conversely, medium or larger organizations with a robust team in house can offload common tasks such as alert monitoring and threat research or co-manage tasks such as offloading night and weekend coverage to the MDR. In a hybrid approach, teams can be more flexible allowing the MDR partner to fit into the needs of their organization. This can allow teams to focus on other more important internal business initiatives.

The Bitdefender Difference

Bitdefender's MDR is comprised of over 280 security experts with a variety of security and technology certifications ready to protect organizations 24/7. Our MDR service sits on top of our industry leading GravityZone platform providing a unified security ecosystem. This combination of top-end security tools combined with highly trained experts offers our customers the most cost effective and comprehensive protection across their environment. By choosing Bitdefender MDR, organizations gain a trusted ally who prioritizes their security and empowers them to focus on growth with confidence.

Next Steps

With the information covered in this eBook, organizations should have a solid foundation for all the variables they must consider when calculating the cost of an MDR compared to building a security team internally. Here are some suggested steps for organizations to take to help them determine which option is best for them.

↳ Perform an internal self-assessment to discover the needs and priorities of the organization.

↳ Determine whether 24/7 coverage is a requirement or if 8x5 is sufficient.

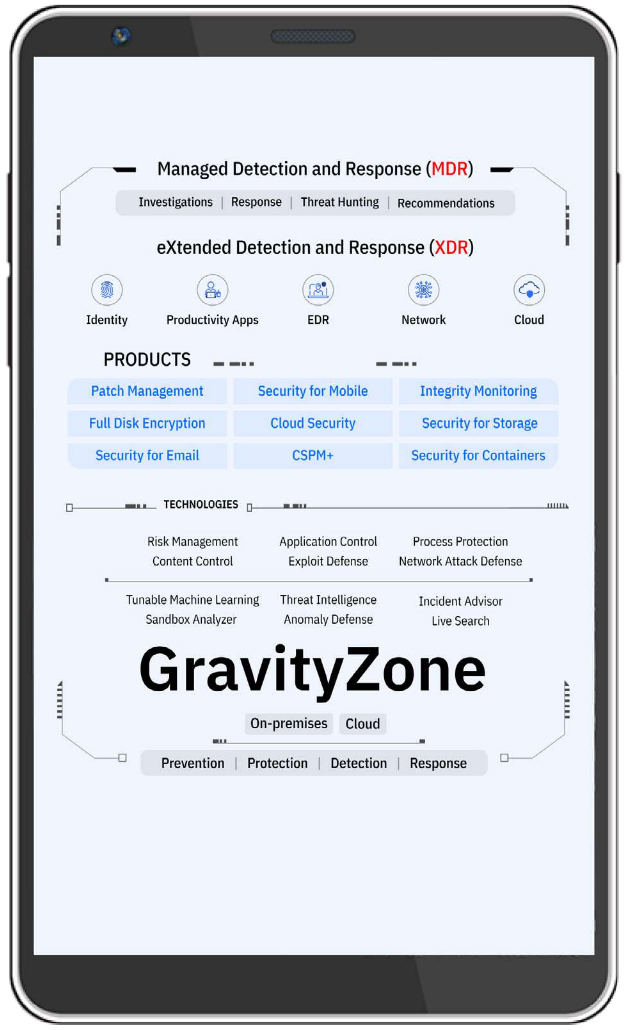
↳ Calculate the cost of building and maintaining an internal security team.
- Time to acquire, vet, interview and hire candidates.
- Time to onboard candidates and build out the security program.
- Cost of the team's salary (plus benefits) and additional tooling.
- Cost of maintaining team, training, and preventing burnout or turnover.

↳ Assess and evaluate MDRs and other managed service offerings.

↳ Learn about what Forrester expert analysts have to say about XDR and MDR.

↳ Weigh the pros and cons of building in-house vs out-sourcing. Consider a hybrid co-managed approach to provide balanced and comprehensive coverage.

Finally, for organizations that are ready to partner with a trusted security vendor can learn about how Bitdefender is ready to help.



Footnotes

[1] Forrester, 2023 Breach Benchmarks By Region by Allie Mellen with Merritt Maxim, Kathryn Bell, Liam Holloway, July 1, 2024.

[2] Forrester, Breaches Are More Expensive And More Frequent When Incident Response Teams Are Unprepared by Allie Mellen with Joseph Blankenship, Heidi Shey, Jess Burn, Kathryn Bell, Liam Holloway, July 8, 2024.

Bitdefender® Global Leader
In Cybersecurity

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Trusted. Always.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.