BlackBerry Cybersecurity

BUYER'S GUIDE

INSIDE THIS BUYER'S GUIDE, YOU'LL LEARN:

- *The key components to consider when searching for an MDR solution*
- *The benefits of an MDR solution*
- *All about buying an MDR solution vs. building your own SOC*
- *How to choose the best solution for your organization*

How to choose a ***MANAGED DETECTION AND RESPONSE SOLUTION***

Cybercrime is on the rise and worldwide costs are expected to reach **$10.5 trillion USD** by the end of the 2025.[1]

As new threats develop, organizations of every size in every industry are being targeted.

With the ever-evolving threat landscape, it is difficult for organizations of any size to keep pace and fully secure their infrastructure. Some cybersecurity challenges for organizations include staffing challenges, cost and complexity of the tools, compliance and regulatory requirements, and strategic planning for the unknown.

To address these obstacles, organizations will benefit from effective and affordable turnkey solutions like managed detection and response (MDR) that deliver world-class cybersecurity at a manageable cost in a fraction of the time required to build an in-house security operations center (SOC).

KEY COMPONENTS TO CONSIDER

Businesses can use MDR to augment their own SOC or as a turnkey solution for all cybersecurity operations. MDR services differ, so it is important to know what capabilities to look for and choose the one that best fits your needs. MDR services typically offer the following capabilities.

01

WHITE-GLOVE IMPLEMENTATION

Getting started with MDR should be seamless and simple. Project managers and technical personnel should work together to design and deploy a custom, outcome-based MDR solution that meets your current needs and can scale as your business grows.

02

ADVANCED AI-BASED PROTECTION

Effective MDR relies on innovative AI and machine learning to monitor and protect all endpoints—including computers, servers, mobile devices, and local, hybrid, and cloud-based environments—and detect and prevent threats early in their lifecycle. Extended telemetry and advanced analytics should automatically block sophisticated adversary behavior before data, operations, or reputation is compromised and reduce alert noise that drives analyst fatigue.

03

24X7X365 MONITORING

Because threat actors don't take nights, weekends, or holidays off, businesses without around-the-clock security staff may not learn about breaches immediately. An MDR solution can monitor, detect, and respond to threats at any time without interruption.

04

SUPPORT FROM SKILLED SECURITY PROFESSIONALS

MDR services can include access to security professionals who can answer questions, make recommendations, customize playbooks, and help test security for new technologies and services.

05

CRITICAL ALERT AND ASSURED COMMUNICATIONS

Attackers often compromise the communication channels that their targets need to mount an effective response. An effective MDR offering should provide a resilient out-of-band communication fabric so you can easily communicate across your security team and user base in the event of an incident.

06

THREAT INTELLIGENCE

Threat actors are constantly changing their techniques, tactics, and procedures (TTPs) and the number of new threat actors is increasing. Effective MDR solutions continually incorporate new strategic, operational, and tactical threat intelligence to identify threats and quickly neutralize attacks.

07

THREAT HUNTING AND DETECTION

MDR offers more than first-rate cybersecurity software—an ideal MDR solution also includes robust threat hunting and detection by skilled professionals that make it faster and easier to flag and contain potentially malicious files and activities before they can impact the environment.

08

INCIDENT MANAGEMENT

MDR can deliver comprehensive incident management that incorporates preparing for events, identifying and containing breaches, eradicating malware, recovering and restoring the affected environment, and incorporating lessons learned from an incident into future response plans.

09

RAPID RESPONSE

When an environment has been breached, the speed at which threats are detected and neutralized is critical. An ideal MDR solution offers faster-than-average metrics for mean time to detection (MTTD), mean time to investigate (MTTI), and mean time to response (MTTR).

10

FULL TRANSPARENCY AND COMPLIANCE

The right MDR vendor will keep you fully informed about every aspect of your security operations and help you maintain regulatory compliance.

11

OPTIMAL OPERATIONS

For any security organization, optimizing and orchestrating the technologies in your cybersecurity solution portfolio can be challenging. With MDR, your cybersecurity solutions are harmonized at launch to deliver organization-wide visibility and response capabilities that remain up to date without in-house administrative burden.

MDR BENEFITS

The right solution can deliver a range of benefits that include the following:

- In addition to eliminating or reducing breach costs, financial benefits include faster return on investment (ROI) and significantly lower startup costs compared to resourcing a SOC on your own. More information on cost is in The SOC Build vs. Buy Decision section below.
- MDR delivers nonstop protection, closing the cybersecurity skills gap to deliver business continuity without the cost and coverage challenges associated with hiring, training, and retaining in-house staff.
- An MDR solution can increase attack surface visibility to reduce incidents and speed threat response, resulting in greater business continuity and uninterrupted operations.
- By protecting personal, financial, and proprietary data, an effective MDR solution helps strengthen customer and partner trust.

BENEFITS BY STAKEHOLDER

MDR can deliver measurable benefits for stakeholders throughout the organization.

SOC TEAM

By reducing false positives, aggregating threat data, and prioritizing information, MDR helps reduce alert fatigue so staff can quickly identify and focus on legitimate potential threats.

IT TEAMS

MDR can eliminate the need for 24x7x365 in-house cybersecurity teams, freeing IT staff to focus on core competencies and strategic business objectives.

CEO/CFO

With the average cost of a data breach climbing above $9.4 million,[2] an MDR prevention-first cybersecurity solution can save an organization millions of dollars with every successful defense.

CIO

MDR services deliver continuous cybersecurity coverage at a fixed price, enabling CIOs to dedicate budget and personnel to other mission-critical tasks.

CISO

By integrating with your organization's existing cybersecurity solutions, MDR enables organizations to preserve the value of existing investments while strengthening overall security posture.

THE SOC BUILD VS. BUY DECISION

To help evaluate whether an organization can benefit from MDR, we developed a composite model of an average mid-size organization and compared the first-year costs to build and staff a minimal, mid-size, and optimally sized SOC to the cost of a complete turnkey MDR solution. Depending on the size of the in-house SOC and the number of endpoints to protect, organizations can save up to millions of dollars by outsourcing cybersecurity to a team of dedicated professionals. Put simply, businesses that implement MDR can achieve enterprise-wide protection and 24x7x365 monitoring with 85 percent less capital outlay than by going it alone.[3]

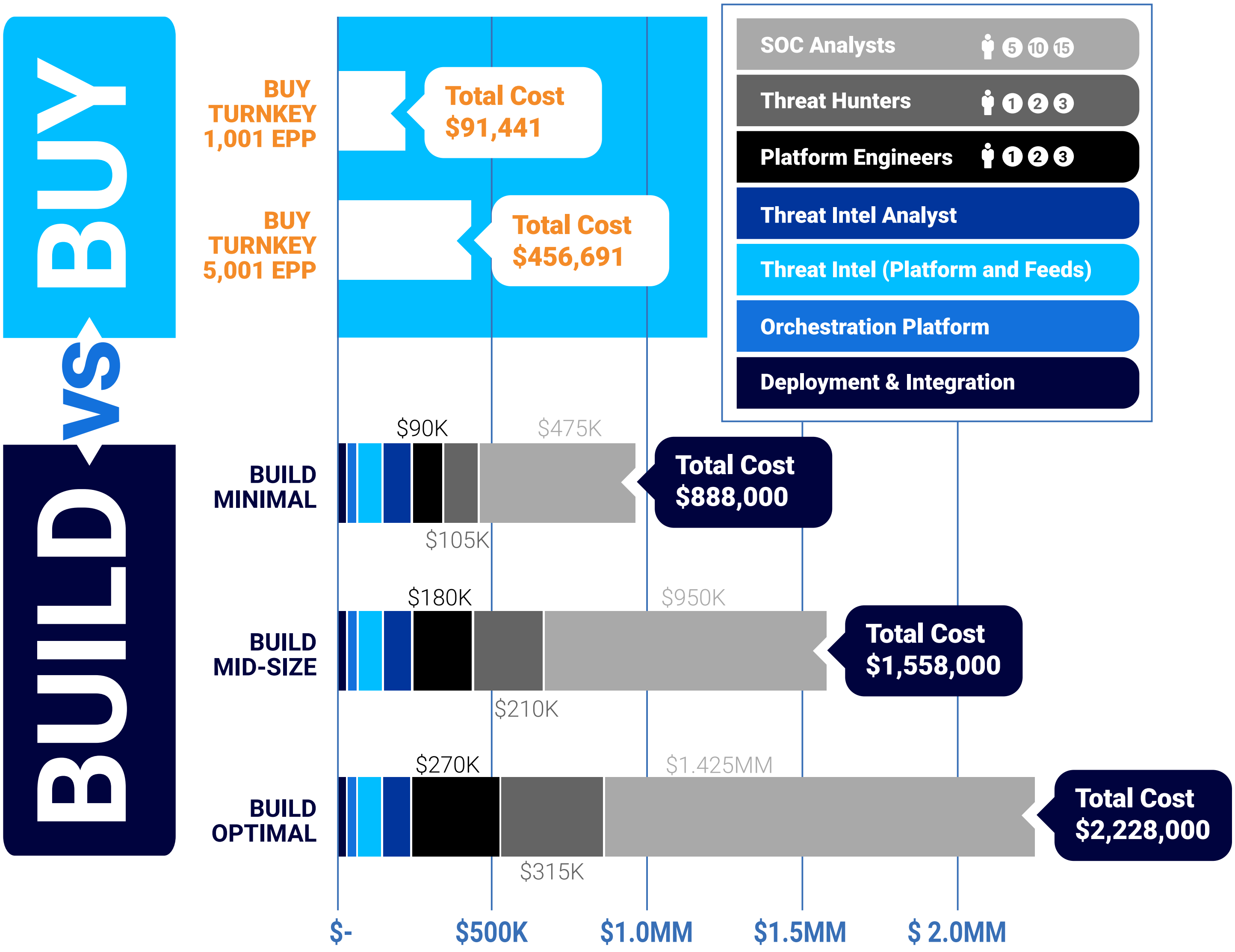


Figure 1: Comparing build vs. buy costs for an MDR solution

CHOOSING THE RIGHT MDR SOLUTION

Factors to consider when evaluating MDR solutions include technology and response capabilities, services, vendor information, and a roadmap to ensure that your cybersecurity solution will remain on the forefront as new technologies evolve and the threat landscape grows.

TECHNOLOGY AND RESPONSE

- Advanced AI-informed threat identification and remediation
- Ongoing technology updates and contextualized cyber threat intelligence to detect and eliminate new TTPs
- Integration of MITRE ATT&CK® mapping, third-party data, and threat telemetry for greater protection
- Faster-than-average operational metrics for MTTD, MTTI, and MTTR
- Alert classification and prioritization based on your rules and labels with automated capabilities to reduce alert fatigue
- Delivers comprehensive security without consuming significant CPU resources

SERVICES

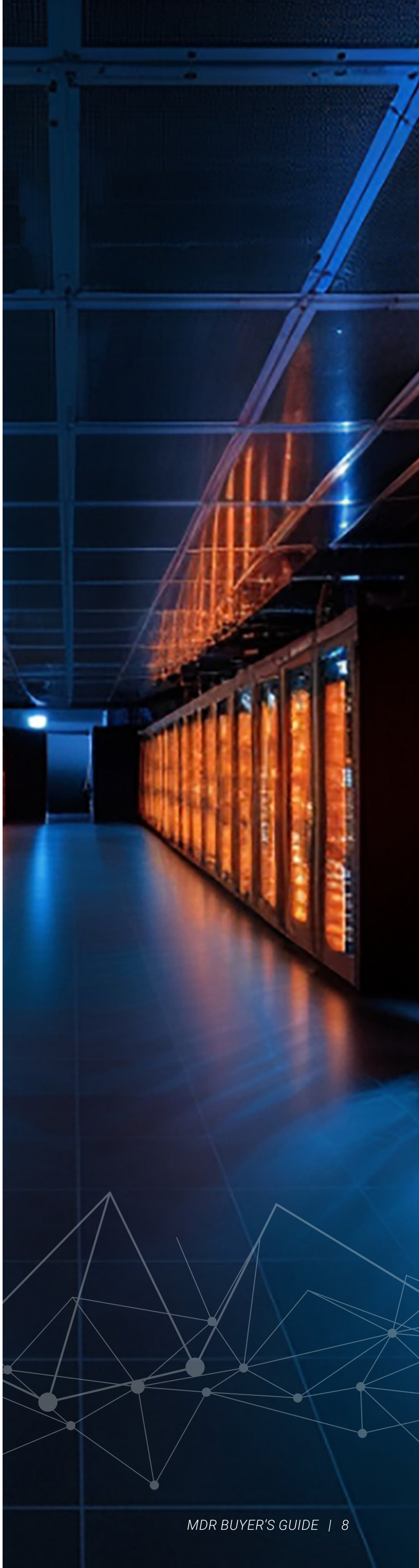
- 24x7x365 coverage
- Custom response playbooks for your unique environment
- Complete transparency about how your organization is secured
- A collaborative partnership with in-house teams to answer questions, sync playbooks, provide tabletop and technical exercises, and deliver hands-on training
- Documentation of regulatory compliance

VENDORS

- Overall corporate history and track record
- Excellent client references
- An established team with low turnover and years of industry experience
- Commitment to meeting or exceeding protection-level agreements (PLAs)

FUTURE-PROOFING

- Understanding and supporting changing regulations and compliance requirements
- Increasing numbers and types of endpoints, including support for remote, mobile, and hybrid work as well as "bring your own device" (BYOD) policies
- Continuous authentication and other technologies that support a transition to zero-trust architecture
- Pervasive security for Internet of Things (IoT) devices and operational technology (OT)



CYLANCEGUARD BY BLACKBERRY STRENGTHENS CYBER RESILIENCE

CylanceGUARD®, the BlackBerry® MDR solution, delivers world-class security around the clock at a fraction of the time and cost of going at it alone. Our award-winning team serves as an extension of your staff, closing the cybersecurity skills gap and handling monitoring, threat hunting, and alerts so your team can focus on strategic goals and projects. CylanceGUARD delivers industry-proven benefits including the following:

- ***Exceptional security.*** AI-driven CylanceGUARD MDR reduces mean time to detection (MTTD), mean time to investigate (MTTI), and mean time to respond (MTTR) to eliminate false positives and utilize BlackBerry cybersecurity solutions to neutralize more than 98 percent of threats before they compromise your environment. And, this powerful security doesn't compromise performance: BlackBerry cybersecurity solutions can reduce CPU consumption by approximately 95 percent compared to other vendors.[4]

- ***Rapid ROI.*** CylanceGUARD delivers a state-of-the art SOC that costs 85 percent less than building and maintaining an in-house operation.[5] Implementation typically requires weeks instead of months, helping businesses achieve a faster time to value. In fact, Forrester estimates that BlackBerry products deliver 100 percent ROI in six months and save millions of dollars across three years.[6]

- ***Award-winning expertise and solutions.*** BlackBerry took first place in the *SOC X world championship* and won both the first and third spots at the *DEF CON 29 Network Defense Competition*. BlackBerry received eight 2023 Cybersecurity Excellence Awards including Best Cybersecurity Company, Cybersecurity Research, Extended Detection and Response, and Artificial Intelligence Security.

To learn more about CylanceGUARD, request a demo.

Sources:

1. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
2. https://www.ibm.com/reports/data-breach
3. Based on calculations using the total cost to build and staff a SOC vs buying CylanceGUARD from actual customers and analyst findings
4. https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/resources/blackberry-com/resource-library/en/cyber/2023/standard/rp/rp-tolly-group-cylanceendpoint-by-blackberry-comparative-endpoint-protection-test-report.pdf
5. Based on calculations using the total cost to build and staff a SOC vs buying CylanceGUARD from actual customers and analyst findings
6. https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/resources/blackberry-com/resource-library/en/cyber/2022/standard/rp/rp-forrester-total-economic-impact-study-of-cylance-protect.pdf

BlackBerry® | Cybersecurity

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 195M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear – to secure a connected future you can trust.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*