

# **The CRITICALSTART® Buyer's Guide for Managed Detection and Response**

**How to choose the right MDR provider to help you achieve greater risk reduction, improve security posture, and enhance security operations**



# Table Of Contents

---

**03** Executive Summary

---

**04** The Evolution of MDR: From Table Stakes to New Foundational Requirements

---

**06** How MDR Differs from MSSP Services

---

**07** Main Categories of MDR Services

---

**08** Common Pitfalls to Avoid in the MDR Decision-Making Process

---

**09** The Top 10 Questions to Ask a Potential MDR Provider

---

**10** How to Confidently Compare Leading MDR Providers

---

**13** Why Consider Critical Start for Your MDR Needs

---

**17** Conclusion



## Traditional security measures are no longer sufficient in today's rapidly evolving threat landscape.

This Buyer's Guide will help you navigate the complex world of Managed Detection and Response (MDR) services, ensuring you make an informed decision that aligns with your organization's unique needs and challenges.

**Critical Start's 2024 Cyber Risk Landscape Report** highlights the continuing trend of organizations placing increasing priority on proactive risk reduction strategies to strengthen their defense. With **83%** of organizations experiencing breaches within the last two years despite traditional security measures and **99%** planning to offload cyber risk reduction workstreams, it's more critical than ever for a reimagined MDR solution that:

- Includes enhanced visibility to drive MDR effectiveness
- Integrates with diverse data sources and environments and addresses diverse business needs and
- Provides human-driven contextual understanding

**MDR continues to transform information security by integrating proactive security intelligence – such as comprehensive asset inventories, Endpoint Detection and Response (EDR) and vulnerability scanner coverage gaps, overlooked Security Information and Event Management (SIEM) log sources and ingestion health monitoring, asset criticality, and MITRE ATT&CK® Mitigations – with traditional, reactive threat detection and response for enhanced visibility that delivers the greatest risk reduction of a breach and minimizes business disruption.**

Use this guide to explore the key factors to consider when evaluating MDR services, including the critical importance of complete signal coverage and the real-world benefits of responding to every alert, regardless of criticality, for complete protection that eliminates blind spots and enables real-time response actions to mitigate impacts.

This guide also provides information on evaluating MDR services for organizations with industrial operations. These services can effectively bridge the gap between diverse technology ecosystems (Information Technology (IT) and Operational Technology (OT) environments) for seamless protection across the organization's entire infrastructure.

**Use this guide to explore the key factors to consider when evaluating MDR services, including the critical importance of complete signal coverage and the real-world benefits of responding to every alert, regardless of criticality.**

# The Evolution of MDR: From Table Stakes to New Foundational Requirements



## As the digital landscape evolves, organizations face increasingly sophisticated cyber threats.

The **IBM 2024 Cost of a Data Breach Report** highlights that the average cost of a data breach reached **\$4.88 million**, a **10%** increase from **\$4.45 million** in 2023. Business disruption costs contributed significantly to the overall breach costs, with organizations experiencing higher disruption seeing an average breach cost of **\$5.01 million**. Looking ahead, emerging threats such as AI-driven attacks and advanced ransomware variants are expected to further increase these costs, making robust MDR solutions more critical than ever.

This upward trend underscores the need for comprehensive security solutions like MDR to manage and mitigate risks effectively.

BASELINE CAPABILITIES OF TRADITIONAL MDR	
Capability	What the Buyer Receives
<b>24x7x365 Monitoring, Detection, and Response</b>	Continuous monitoring and response, staffed by experienced security analysts who can investigate, respond to, and contain threats at any time of the day or night.
<b>Analysis and Investigation of Security Events</b>	Data augmentation, high-fidelity detections, and threat correlation and mapping to the <b>MITRE ATT&amp;CK® Framework</b> for deeper understanding of threat Tactics, Techniques, and Procedures ( <b>TTPs</b> )
<b>Threat Hunting</b>	Human-led investigation to find Indicators of Compromise ( <b>IOCs</b> ) before they become a breach
<b>Delivery of Active Threat Disruption and Containment Actions Based on Rules of Engagement (ROE)</b>	Customized response actions (assist with or perform response actions, e.g., isolating endpoints, blocking malicious IP addresses, or disabling user accounts), usually with an audit trail, resulting in rapid threat mitigation
<b>Reduction of False Positives</b>	Automatic resolution of known-good behaviors to reduce alert fatigue on security teams
<b>Direct Analyst Accessibility</b>	Ability to get in touch with a live human 24x7x365
<b>Contractual Service Level Agreements (SLAs)</b>	Assurance that alerts are identified, quickly contained and resolved within the agreed-upon terms
<b>Information Technology (IT) Data Source Integration and Coverage</b>	Log ingestion and integration with security tools covering EDR/Endpoint Protection Platform ( <b>EPP</b> ), SIEM, Identity, Email, and Cloud
<b>Automation and Orchestration</b>	Playbooks to route events that do not require direct investigation and escalation; Visibility into what is being applied to the customer environment specific to the tools being monitored
<b>Threat Detection Engineering</b>	Creating new threat detection rules specific to the organization to increase threat detection and response effectiveness
<b>Metrics and Reporting</b>	Clear and actionable metrics and reports that demonstrate service effectiveness
<b>Incident Response (IR) Services</b>	Either comes as part of the service or as an add-on, IR services offer direct support in case of a major security incident

# The Evolution of MDR: From Table Stakes to New Foundational Requirements (cont.)



MDR is the cornerstone for developing a resilient cybersecurity program and these capabilities are fundamental to your defense. The MDR provider you choose needs to meet, at a minimum, your expectations of what their baseline capabilities can deliver.

What data is showing us, however, is that MDR solutions are only as good as the security signals they receive. The Ponemon Institute reports that **68% of organizations have experienced one or more successful endpoint attacks** – frequently from threat actors exploiting insufficient visibility to gain network access – with **82% of security leaders admitting to being surprised by breaches or threats** that had managed to evade security controls they assumed were correctly in place.

**Now, best-in-class MDR must meet and exceed the traditional baseline expectations in addition to providing organizations with all expected telemetry and monitoring high-risk attack vectors as part of its foundational service.**

Even with an MDR in place, attackers can leverage hidden and unmonitored assets, creating undetected threats that evade security controls and monitoring. Security leaders – and MDR buyers – need assurance that the threats they believe their MDR has always been detecting...are truly being detected.

This has resulted in a shift to the starting line for what was once considered table stakes for MDR. Now, best-in-class MDR must meet and exceed the traditional baseline expectations in addition to providing organizations with all expected telemetry and monitoring high-risk attack vectors as part of its foundational service.

Modern MDR solutions are incorporating advanced features that transform how organizations manage and respond to security threats, including:

- **Visibility and Validation:** Ensuring all unmonitored assets are identified, threat signals align with asset inventories and are received, and log sources are ingested

- **Enhanced Response Workflows:** Customizable Rules of Engagement (**ROE**) to define precise response actions and investigation procedures based on alert and asset criteria, ensuring responses align with business priorities
- **Intelligent Alert Management:** Advanced capabilities like **Benign True Positive** identification help reduce alert fatigue by properly categorizing legitimate security testing and expected actions
- **Comprehensive Vulnerability Intelligence:** Integration of vulnerability scanner data to identify coverage gaps across assets, even without dedicated vulnerability management solutions

The **Gartner® Market Guide for Managed Detection and Response**<sup>1</sup> states, “Increasingly, MDR buyers are asking providers to extend their requirements beyond the detection of and response to threats, to include the proactive identification of threat exposures and preemptive security responses.”

Organizations planning for the future or in a position to scale their security program today are also considering how to address the need to prioritize, address, and patch every vulnerability across their security ecosystems. In today’s data-rich environments, there is also an expectation that MDR providers can seamlessly integrate with a **Vulnerability Management Service (VMS)** to help organizations uncover and mitigate exposures.

This increased visibility across current threats targeting vulnerabilities on critical assets makes MDR more effective. MDR providers integrating with a VMS take the burden out of vulnerability management with turnkey program operationalization that manages and prioritizes vulnerability scans and customer workloads.

Furthermore, as the convergence of IT and OT environments accelerates, MDR services are expected to provide comprehensive coverage across both domains, aligning with frameworks such as the **SANS ICS Critical Controls** and the **Purdue model** for Industrial Control Systems (**ICS**).

Considering the evolution of new foundational requirements for MDR, let’s more closely examine how to evaluate leading MDR providers.

<sup>1</sup> Gartner, Market Guide for Managed Detection and Response, Pete Shoard, Andrew Davies, Mitchell Schneider, Angel Berrios, Craig Lawson, 24 June 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

# How MDR Differs from MSSP Services



While both MDR and Managed Security Service Provider (MSSP) services aim to enhance an organization's cybersecurity posture, there are distinct differences in their approach and capabilities:

- ✓ **Continuous Threat Hunting:** Unlike MSSPs, which primarily focus on managing security tools and alerting organizations of potential issues, MDR services focus on identifying core adversarial behaviors within specific industries and actively hunt for threats within the network, enabling quicker detection and response.
- ✓ **Proactive Security Intelligence:** Some MDR services use asset visibility to identify at-risk threat vectors within the network (such as **Endpoint, vulnerability scanner, and SIEM coverage gaps**), enabling quicker detection and response.
- ✓ **Focus on Detection and Response:** MDR is specifically designed to detect and respond to active threats, with a focus on real-time response and minimizing dwell time. MSSPs often have a broader scope, including managing firewalls, VPNs, and security appliances, but they may lack real-time detection and remediation focus and often rely on the client to manage incident response.
- ✓ **Human-Led Investigations:** MDR solutions leverage experienced security analysts to investigate, validate, and respond to alerts, providing in-depth analysis. MSSPs, on the other hand, often provide less hands-on investigation and rely more on automated tools, including escalating alerts with little to no response guidance or recommendations.
- ✓ **Technology Agnostic:** MDR services are designed to integrate with multiple security tools across different environments (including endpoint, network, cloud, and OT), while MSSPs are typically focused on managing specific security technologies.





MDR offers defined services around detection and response (and now proactive security intelligence capabilities) to meet growing customer needs for advanced threat detection, incident response, and continuous monitoring combined with human expertise.

MDR services can cover multiple threat vectors (endpoint, server, user, identity, on-premises infrastructure, applications, hybrid, cloud, and Operational Technology (OT) / Industrial Control Systems (ICS) environments) and integrate disparate data into one centralized platform to create a robust, in-depth defense strategy that ensures comprehensive threat detection and response to quickly stop a breach and minimize business disruption.

Understanding the flexibility of MDR helps organizations determine where it can be used to best suit their needs.

## MDR FOR INFORMATION TECHNOLOGY (IT) ENVIRONMENTS AND DATA SOURCES

MDR for IT focuses on data confidentiality and integrity – keeping data safe from unauthorized access. Its mandates include protecting business applications and data and using more active response measures, such as isolating hosts or resetting user passwords, to do this. It usually consists of a centralized IT security team handling alerts, and it covers a broad scope across various IT systems and networks, including:



### Endpoint Detection and Response (EDR)

MDR services focused on endpoint protection leverage Endpoint Protection Platform (EPP) and EDR tools to continuously monitor endpoints (such as workstations, servers, and mobile devices) for suspicious activities. These services provide detailed forensic analysis and response capabilities to contain and remediate endpoint-based threats.



### Security Information and Event Management (SIEM)

MDR providers integrate with SIEM systems to deliver enhanced detection and response capabilities. SIEM-based MDR services use the data aggregation and correlation capabilities of a SIEM to provide visibility across the entire organization, allowing for more holistic threat detection and incident response. SIEM solutions ingest source data across all users, devices, applications, and infrastructure, including **Identity, Email, Cloud, and Network** security logs.

Some MDR providers offer SIEM management in addition to MDR services to maximize the SIEM system's operational security potential through value-added services such as tuning, customization, configuration, and more.



### Managed Extended Detection and Response (XDR)

Managed XDR services extend detection and response capabilities beyond the endpoint, integrating data from multiple security layers, including Identity, Email, Cloud, and Network systems. Managed XDR provides a broader view of the threat landscape and offers advanced detection and response capabilities across multiple vectors. It also provides customers with the benefit of hot and cold log storage to meet log storage compliance needs.

## MDR SERVICES FOR OPERATIONAL TECHNOLOGY (OT)

OT environments (such as **Industrial Control Systems (ICS)** and **Supervisory Control and Data Acquisition (SCADA)** systems) require specialized MDR services due to their unique risks and requirements. OT-focused MDR provides monitoring and response tailored to the specific needs of critical infrastructure and industrial environments, ensuring that operational technology systems are protected from both traditional IT threats and OT-specific attacks.

# Common Pitfalls to Avoid in the MDR Decision-Making Process



Choosing the right MDR provider is a critical decision that can have lasting impacts on your organization's security posture. Here are some common pitfalls to avoid when evaluating and selecting MDR solutions:

## 1. OVERLOOKING INTEGRATION CAPABILITIES

Ensure that an MDR provider can integrate with your existing security tools and infrastructure. Make sure the provider is vendor-agnostic and can work with your current technology stack, including SIEM, EPP/EDR, and cloud security tools. A lack of integration can lead to visibility gaps and inefficiencies.

## 2. FOCUSING SOLELY ON COST

While budget is important, choosing the cheapest option can result in inadequate coverage or slower response times. Focus on the total value provided by the service, such as comprehensive coverage, proactive threat hunting, and quality of the SOC team, rather than just the price tag.

## 3. ASSUMING AUTOMATION IS ENOUGH

Automated detection systems are efficient, but without human oversight, they can miss complex threats or generate false positives. Avoid assuming that automation alone will provide sufficient protection – ensure that the MDR service combines automation with human-led investigations to properly assess and mitigate threats.

## 4. IGNORING RESPONSE AND CONTAINMENT CAPABILITIES

Some MDR providers may excel at detecting threats but lack the ability to respond effectively to or contain them in real time. Ensure that the MDR solution includes incident response capabilities, and that the provider can contain threats quickly to minimize potential damage.

## 5. NEGLECTING SERVICE LEVEL AGREEMENTS

Many organizations overlook the importance of clear SLAs when evaluating MDR providers. Ensure that the vendor offers contractual SLAs for detection, response, and containment times (not Service Level Objectives), so you know exactly what to expect in terms of service and support.

## 6. FAILING TO ASSESS THE SOC TEAM'S EXPERTISE

Not all SOC teams are equally skilled. The effectiveness of the MDR service depends heavily on the experience and expertise of the SOC analysts who monitor and respond to threats. Be sure to evaluate the qualifications of the SOC team, team retention rate, and ensure they have experience dealing with the types of threats your organization faces.

## 7. UNDERESTIMATING SCALABILITY REQUIREMENTS

Your security needs will evolve as your organization grows. Some MDR services may not scale easily, resulting in coverage gaps or performance degradation. Ensure that the MDR provider offers scalability to handle additional endpoints, cloud services, and new environments (this includes tool migration should you change software or services) without compromising service quality.

## 8. NEGLECTING DATA PRIVACY AND SOVEREIGNTY

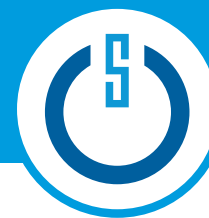
Ensure the MDR provider complies with relevant data protection regulations and can handle data in accordance with your geographic and industry-specific requirements.

## 9. OVERLOOKING IT-OT INTEGRATION CAPABILITIES

For organizations with both IT and OT environments, failing to consider an MDR provider's ability to monitor and protect both domains seamlessly can lead to security gaps. Ensure the provider has experience in both IT and OT security and can offer integrated, end-to-end coverage across your entire infrastructure.



# The Top 10 Questions to Ask a Potential MDR Provider



When evaluating MDR providers, it's critical to ask the right questions to ensure the service aligns with your organization's needs and goals. Here are the top 10 questions you should ask:

**1. What types of threats and environments do you specialize in?**

Make sure the provider has expertise in handling the types of threats your organization faces and can support your specific environment, including endpoints, networks, cloud, and OT systems.

**2. How does your MDR service integrate with my existing security tools and infrastructure?**

Ask about customized response workflows and the flexibility of response actions based on alert and asset criteria. Ensure compatibility with your existing SIEM, EDR, vulnerability scanning, firewalls, and cloud services. A vendor-agnostic solution that can integrate smoothly with your technology stack is essential for maximizing your security investments.

**3. Do you offer 24x7x365 monitoring and real-time response, and how quickly can you respond to threats?**

Ensure the provider offers around-the-clock monitoring and response. Ask about their average response times and whether they are backed by contractual SLAs for incident detection, containment, and resolution.

**4. How does your service combine automation with human analysis?**

It is crucial to understand how the provider balances automated detection tools with human expertise. A service that combines machine learning and AI with skilled human analysts is more effective at detecting and responding to complex threats.

**5. How scalable is your solution, and what are the costs associated with growth?**

As your organization grows, your security needs will increase. Ensure the provider can scale the MDR service to accommodate more endpoints, cloud environments, or locations without significantly increasing costs or requiring a complete overhaul of the service.

**6. How can I mitigate the risk of unprotected assets being compromised?**

Proactive security intelligence provides data to ensure all your assets are accounted for and that you are receiving full alert coverage across all your endpoints. Ask whether the provider includes proactive threat intelligence as part of their standard MDR service.

**7. What metrics and reporting will I receive, and how often?**

Ensure the provider offers detailed reports with actionable insights. Ask about key metrics like Critical alert notification, Mean Time to Detection (**MTTD**), Median Time to Resolution (**MTTR**), false positive rates, and incident summaries, and how frequently they provide these reports.

**8. How experienced is your Security Operations Center team, and what qualifications do they have?**

The effectiveness of an MDR service heavily depends on the skills and experience of the SOC team. Ask about the team's background, certifications (such as Certified Information Systems Security Professional (**CISSP**) and Certified Ethical Hacker (**CEH**), and experience with the types of threats your organization may face.

**9. What is your incident response process, and how do you handle a major breach?**

Understand the provider's process for detecting, investigating, and responding to alerts. Can they contain threats directly, and how involved are they in remediation? It's important to know whether they can assist during a major breach or if they escalate to a third-party incident response team.

**10. What kind of Service Level Agreements do you provide, and what happens if you fail to meet them?**

SLAs should cover response times for various threat levels. Ask about the consequences if the provider fails to meet these agreements and whether there are penalties or other guarantees.

# How to Confidently Compare Leading MDR Providers



Unfortunately, it's not as easy as weighing "apples to apples" when comparing technology-enabled services companies that provide 24x7x365 Security Operations Centers (SOCs) with round-the-clock alert monitoring of customer environments.

**The inability to conduct a like-to-like comparison creates a challenge when evaluating how, and to what degree, an MDR service can reduce pain points and benefit your organization and teams based on the unique criteria that align with your security needs, operational goals, and technology stack.**

We suggest creating and completing a **Buyer Evaluation Matrix** listing your Key Performance Indicators (KPIs) and required outcomes following the example below. This will make it easier to compare MDR providers and the features and functionalities you need to help you achieve them.

SAMPLE BUYER EVALUATION MATRIX		
Expected Buyer Outcomes	Buyer KPIs	Vendor Features and Functionalities that Drive Buyer KPIs
Risk Reduction	Detect and respond to threats faster	<ul style="list-style-type: none"> <li>Contractual Mean Time To Detection (MTTD) and Median Time To Resolution (MTTR) SLAs across 100% of alert priorities</li> <li>SLA for expedited notification of critical alerts</li> <li>iOS and Android mobile app for both triage and remediation</li> </ul>
	Enhance threat mitigation effectiveness	<ul style="list-style-type: none"> <li>Aggregate, normalize, correlate, and analyze security alerts alert priorities</li> <li>Continually updated automated response playbooks</li> </ul>
	Ensure and improve security posture	<ul style="list-style-type: none"> <li>Security alert, investigation, and response metrics</li> <li>Identify hidden assets and unmonitored infrastructure</li> <li>Vulnerability coverage gap detection with scanner data integration</li> </ul>
	Ensure business continuity	<ul style="list-style-type: none"> <li>Integration with both IT and OT environments for comprehensive protection</li> <li>25x7x365 monitoring and response capabilities</li> <li>Rapid containment of threats to minimize operational disruption</li> </ul>
	Increase compliance	<ul style="list-style-type: none"> <li>Schedule, generate, export, and email reports</li> <li>Identify unmonitored and hidden assets (Assure Host assets are secured)</li> <li>Continuous (versus point-in-time) asset monitoring</li> </ul>
	Increase proactive risk reduction	<ul style="list-style-type: none"> <li>Identify unmonitored and hidden assets</li> <li>Complete signal coverage aligned with asset inventory</li> <li>Log source and ingest monitoring</li> </ul>
	Continually reduce risk over time	<ul style="list-style-type: none"> <li>Continuous refinement of detection rules and response strategies</li> <li>Cyber Risk Reviews to assess and improve security posture</li> <li>Ongoing threat intelligence updates and continuous threat hunting</li> </ul>
	Improve threat intelligence	<ul style="list-style-type: none"> <li>Enhance ability to anticipate and prepare for emerging threats</li> </ul>



SAMPLE BUYER EVALUATION MATRIX		
Expected Buyer Outcomes	Buyer KPIs	Vendor Features and Functionalities that Drive Buyer KPIs
<b>Productivity Increase</b>	Leverage automation of security processes	<ul style="list-style-type: none"> <li>Trusted behavior registry (Uses false-positive reducing playbooks that provide confirmed and automated investigations)</li> <li>Benign true positive identification for reduced false positives</li> </ul>
	Increase security team productivity	<ul style="list-style-type: none"> <li>Customizable response authorization workflows</li> <li>Performance, effectiveness, and efficiency dashboards</li> <li>Scheduling coordination</li> <li>Transparent, unified platform using APIs to ingest alerts</li> <li>Transparency into audit logs and timeline of alert handling and response actions</li> </ul>
	Maintain a skilled workforce	<ul style="list-style-type: none"> <li>Reduced burnout risk for internal security teams by offloading routine tasks</li> <li>Access to a team of expert analysts</li> </ul>
<b>Cost Optimization</b>	Maximize use of existing security investments	<ul style="list-style-type: none"> <li>Security service efficiency metrics</li> <li>Metrics for the technological effectiveness of supported products</li> <li>Vendor agnostic integration</li> <li>Unified platform for analysis, response, and investigation with consolidated views</li> </ul>
	Minimize tech stack	<ul style="list-style-type: none"> <li>Portfolio solution</li> </ul>



## Additional Buyer and User Considerations

Once you've completed your Buyer Evaluation Matrix, also note broader MDR service capabilities important to your organization. These may include the types of threat vectors covered, additional training provided to security analysts, the availability of direct human communication, scalability, and even the flexibility to take your custom threat detections with you if you choose to switch providers.

CAPABILITIES	
<p><b>MDR with Proactive and Reactive Security Intelligence</b></p> <ul style="list-style-type: none"> <li>• Provides customers complete signal coverage by identifying hidden and unmonitored assets and log ingestion issues, assuring the SOC receives all expected threat telemetry.</li> <li>• Vendor-agnostic to integrate with your existing security tools and processes (such as EDR, SIEM, and firewalls) without forcing the use of proprietary tools.</li> <li>• Simplifies security across complex networks and threat vectors (e.g., IT with Cloud and Identity, OT).</li> </ul>	<p><b>Flexible Deployment for Security That Works the Way You Do</b></p> <ul style="list-style-type: none"> <li>• Define critical assets and operational priorities for faster threat mitigation that matches your risk tolerance and business needs.</li> <li>• Adaptive alert handling and response protocols that evolve and scale with your organization.</li> <li>• Eliminate the noise of redundant alerts and escalations and ensure that alerts are meaningful and actions are impactful.</li> </ul>
<p><b>Human-Driven Analysis</b></p> <ul style="list-style-type: none"> <li>• Provides nuanced analysis that automated, bot-driven analysis alone cannot accomplish. Human-driven analysis is critical for interpreting complex threats, while automation can improve efficiency for routine tasks, including minimizing false positives.</li> </ul>	<p><b>Security Operations Center Expertise</b></p> <ul style="list-style-type: none"> <li>• Evaluates the experience and expertise of the provider's SOC team and considers ongoing training initiatives and certification processes.</li> </ul>
<p><b>Security Support, SLAs, and Training</b></p> <ul style="list-style-type: none"> <li>• Supports direct communication with human analysts to collaborate, make quick decisions, and act with confidence.</li> <li>• Contractual SLAs particularly around escalation procedures and detection, response, and threat resolution times, ensuring your MDR service meets your business needs.</li> <li>• Hands-on training provided to your internal team to maximize the value of the MDR service.</li> </ul>	<p><b>Cost, Scalability, and Customization</b></p> <ul style="list-style-type: none"> <li>• Flexible pricing models that provide of scalability for both organizational growth and security posture maturity allow organizations add coverage for additional assets, cloud environments, or OT systems through a unified platform without incurring prohibitive costs.</li> <li>• Offers personalized onboarding and tailored ROE.</li> <li>• MDR tailored to your specific industry threats and compliance requirements.</li> </ul>
<p><b>Threat Hunting and Investigation</b></p> <ul style="list-style-type: none"> <li>• Proactive threat hunting is a valuable service that goes beyond reactive monitoring, allowing security teams to search for hidden threats that might not trigger alerts.</li> </ul>	<p><b>Incident Response</b></p> <ul style="list-style-type: none"> <li>• Expert service that limits attacker dwell time by taking immediate action to minimize the impact on your business.</li> </ul>

# Why Consider Critical Start for Your MDR Needs



At Critical Start, we help organizations stay secure by eliminating blind spots to prevent breaches and avoid business disruption.

Critical Start MDR finds and protects organizations from hidden threats that would normally be missed, ensuring no infrastructure is unmonitored, and no signals are overlooked.

By providing visibility across all assets, our customers can be confident that every potential threat is detected and addressed. We reduce risk and maximize security investments – without adding complexity or new tools – by combining proactive security with MDR to ensure that no threat slips through the crack.

## MDR FOR DIVERSE TECHNOLOGY ENVIRONMENTS, DATA SOURCES, AND BUSINESS NEEDS

Critical Start MDR maximizes your existing infrastructure to reduce complexity and optimize costs. Our holistic approach, combining proactive security intelligence with our MDR services, ensures that no part of your security infrastructure is left unmonitored.

**Complete signal coverage** results in **SOC signal assurance** (confidence the SOC is receiving all expected threat telemetry) by identifying hidden assets and unmonitored infrastructure. This ensures that no potential threat goes unnoticed, addressing a critical pain point for CISOs and security leaders, and ensuring the most value per dollar invested.

## PROACTIVE RISK REDUCTION

Unlike traditional security solutions that focus solely on detection and response, Critical Start integrates proactive security intelligence into its MDR platform. By identifying threat exposures and addressing vulnerabilities early, we help organizations stay ahead of evolving threats.

## SEAMLESS INTEGRATION WITH YOUR EXISTING INFRASTRUCTURE

At Critical Start, we understand that in order to be effective, MDR must work in harmony with your existing security ecosystem. Our solution is designed to integrate seamlessly with your current tools and processes, maximizing the value of your security investments. Our integration capabilities include:

- Seamless integration with existing security tools and environments
- Vendor-agnostic approach to maximize your current security investments
- Unified platform for streamlined operations and enhanced visibility

This flexible, integrated approach ensures that Critical Start MDR enhances your security posture without disrupting your existing workflows or requiring significant changes to your infrastructure.

### CRITICAL START MDR SERVICES

#### MDR for IT Environments

- Endpoint Detection and Response (**EDR**)
- Security Information and Event Management (**SIEM**)
  - Includes Managed SIEM capabilities
- Managed Extended Detection and Response (**XDR**)

#### MDR for OT Environments

- Operational Technology (**OT**) and Industrial Control Systems (**ICS**)

# Why Consider **Critical Start** for Your MDR Needs (cont.)



## How MDR Provides Better Protection in Today's Environment



MDR offers a significant advantage in today's complex threat landscape. Organizations extensively using AI and automation **reduced breach costs by an average of \$2.2 million** compared to those not using these technologies. This highlights the critical role of advanced technologies in identifying and containing threats quickly and efficiently.

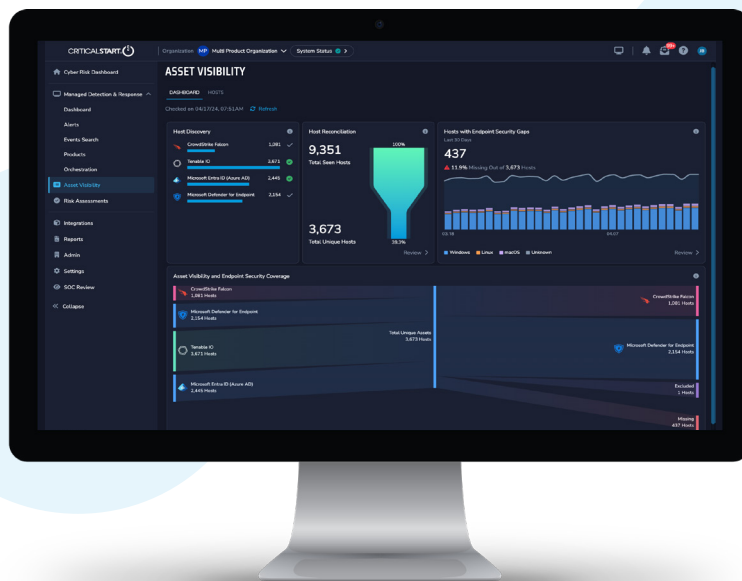
Critical Start's MDR goes beyond detecting threats — it also proactively identifies threat exposures before they can be exploited. Using MITRE ATT&CK® Mitigations, **asset visibility**, and **endpoint** and **SIEM monitoring**, Critical Start ensures that organizations are prepared to face evolving threats by reducing the potential for attacks at every stage. Our approach addresses current threats and helps organizations adapt to emerging cybersecurity challenges.

## How Critical Start Achieves These Results

At Critical Start, our mission is to help organizations minimize business disruption by preventing breaches. We do this by starting your threat protection before Detection and Response by creating an asset inventory and eliminating blind spots for comprehensive defense available nowhere else. Our comprehensive approach goes beyond traditional security solutions through:

### KEY DIFFERENTIATORS

-  **SOC Signal Assurance:** Leverages complete signal coverage to ensure the SOC receives all expected threat signals for trusted threat detection.
-  **Complete Asset Inventory and Signal Coverage:** Ensures signals from one of the highest-risk threat vectors (endpoints) are being received across the organization. Identifies hidden and unmonitored assets, endpoint and vulnerability scanner coverage gaps, and overlooked SIEM log sources and maintains a continuous, accurate inventory of assets (visible as a data source in your **Cyber Risk Dashboard**). SIEM health monitoring is also included to monitor for interrupted data ingestion. This prevents blind spots and enables organizations to mitigate potential threats before they can cause harm.



# Why Consider Critical Start for Your MDR Needs (cont.)



## KEY DIFFERENTIATORS (cont.)



**Cyber Operations Risk & Response™ (CORR) Platform:** Our proprietary **CORR Platform** integrates advanced security intelligence, including comprehensive **asset inventories**, **EDR/SIEM coverage gaps**, **asset criticality assessments**, and MITRE ATT&CK® Mitigations. Our platform provides a unified view of your security ecosystem, enabling more effective threat detection and response.



**Risk-Ranked Recommendations:** Uses real-time data to personalize risk-reduction recommendations. This allows you to prioritize improvements that deliver the greatest risk-reduction impact (like high-risk threats to critical assets) so you can minimize potential disruptions and maximize operational efficiency.



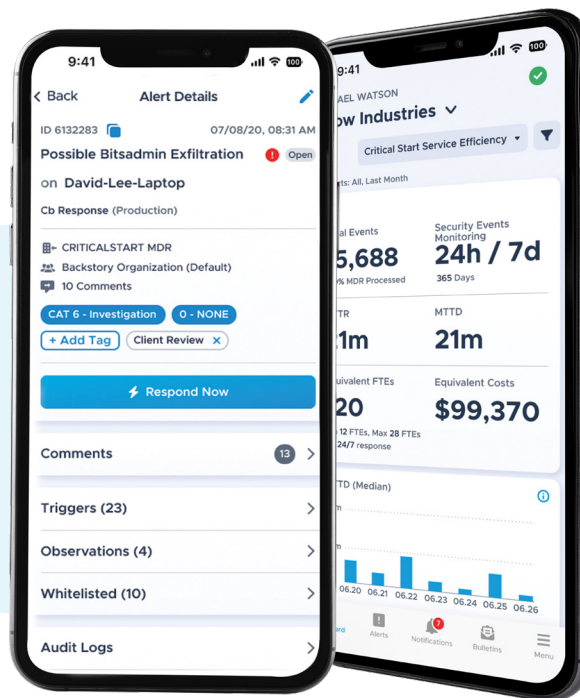
**Human-Driven Monitoring and Response:** **24x7x365** monitoring is powered by a dedicated team of security experts who provide in-depth investigation and true response mitigation. It provides nuanced, contextual threat detection and response by combining advanced automation with human expertise. Our human-led approach also includes a **2-person integrity review** on every action to be taken, ensuring every threat is accurately assessed and managed to avoid disruption to your operations. Our SOC team boasts a **90% annual retention rate**, ensuring consistent, expert service.



**Flexible Deployment:** Our MDR is built around your unique business processes to capture critical business context, **eliminating redundant escalations** and **reducing alert fatigue** while customized response strategies adapt with your organization to improve your security posture.



**MOBILESOC® for Remote Threat Containment:** Enables clients to investigate, contain, and respond to threats directly from mobile devices. This unique feature allows for quick response and minimal downtime during incidents.



# Why Consider Critical Start for Your MDR Needs (cont.)



## KEY DIFFERENTIATORS (cont.)



### IT and OT Integration

- **End-to-End Coverage:** Our MDR service provides unified protection across both IT and OT environments, ensuring no security gaps between these traditionally separate domains.
- **Non-Intrusive Monitoring:** Given the critical nature of OT systems, our MDR service for OT operates in a read-only mode to avoid any potential disruption to industrial processes.
- **IT-OT Boundary Monitoring:** We recommend monitoring and securing the boundary between IT and OT networks to prevent the lateral movement of threats.
- **SANS ICS Critical Controls Alignment:** Our approach supports the SANS ICS Critical Controls, including defensible architecture, ICS network visibility and monitoring, secure remote access, and risk-based vulnerability management.
- **Purdue Model Support:** While we align and support full Purdue model deployments, our flexible approach also accommodates simpler setups, starting with basic IT-OT segregation and scaling up as needed.
- **Experienced Security Professionals:** Our team understands the unique challenges of OT security, including the criticality of availability and the potential physical consequences of security breaches in industrial environments.

## KEY METRICS

- **MTTD (Mean Time to Detection):** Early threat detection reduces MTTD and allows for faster threat identification.
- **MTTR (Median Time to Resolution):** Fast resolution ensures threats are contained quickly, minimizing damage.
- **False Positive Reduction:** Our **Trusted Behavior Registry® (TBR®)** auto-resolves known good behaviors, minimizing false positives and unnecessary escalations.
- **ROI Metrics:** We provide clear, quantifiable metrics demonstrating the value and cost-effectiveness of our MDR services.

## Delivering Exceptional Results to Our Customers

Critical Start's MDR not only detects and responds to threats but also provides continuous improvement in security posture through **incident response** and **risk assessments**. Our commitment to transparency, expert-led services, and comprehensive coverage makes us a trusted partner in enhancing your organization's security maturity and reducing cyber risk.

### Compliance and Regulatory Support

Our MDR services can help organizations meet and maintain compliance with various regulatory standards. We provide detailed reporting and documentation to support audit requirements and demonstrate ongoing compliance efforts.

**Critical Start's MDR is more than a cybersecurity service – it's the foundation for your journey to stronger defenses and increased risk resilience.**





## Next Steps

As cyber threats evolve in complexity and frequency, choosing the right Managed Detection and Response (MDR) provider is crucial for your organization's security posture. This Buyer's Guide has outlined the key factors to consider, common pitfalls to avoid, and essential questions to ask when evaluating MDR services.

Critical Start stands out in the MDR landscape by elevating the traditional MDR model. We integrate proactive security intelligence – including **comprehensive asset inventories, EDR/VMS/SIEM coverage gaps, asset criticality**, and MITRE ATT&CK® Mitigations – with our transparent **Cyber Operations Risk & Response™ (CORR)** platform and **MOBILESOC® application**. Our approach ensures complete signal coverage, eliminating blind spots that could leave your organization vulnerable.

Our team of experts, with a **90% annual retention rate**, delivers **24x7x365 investigation** and **true response mitigation**. We offer **flexible deployment options** across all **IT and OT environments**, backed by industry-leading **contractual SLAs**. This comprehensive approach not only detects and responds to threats but continuously improves your security posture, delivering the greatest risk reduction and helping you confidently minimize business disruption and maximize operational efficiency.

Let us show you how we can enhance your security posture, reduce cyber risk, and provide you with the peace of mind that comes from knowing your defenses are always one step ahead of emerging threats. [Contact us today](#) for a personalized consultation and demonstration of our MDR capabilities. We offer a streamlined onboarding process and can ensure you start seeing value quickly.





Contact us for more information about Critical Start MDR, or schedule a demo at:  
[www.criticalstart.com/contact/request-a-demo/](http://www.criticalstart.com/contact/request-a-demo/)