deepwatch™

Selecting the Right Managed Detection and Response Provider

The MDR Buyer's Guide to Enhanced Cyber Resilience

www.deepwatch.com

Table of Contents

01. **The Challenge of Cyber Resilience**

02. **Extend Coverage, Fill Skills Gaps and Maximize Security Investments with MDR**

03. **Key Benefits of MDR**

04. **An MDR Provider Checklist**

05. **The MDR Advantage Against Cyber Threats**
    - MDR Improves Threat Detection
    - MDR Improves Incident Response
    - MDR Improves and Strengthens Security Posture

06. **Why Deepwatch?**

07. **Take the Next Step**

01. The Challenge of Cyber Resilience

Automated systems alone are not enough to protect most organizations from modern cyber threats' volume and complexity. As long as human threat actors exist, security efforts will require human-led cyber defense.

The goal of cyber resiliency is to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. Cyber resilience embodies an organization's capacity to anticipate, withstand, and recover from cyber threats.

However, many organizations say they have a shortage of staff with the requisite skills to meet the challenge of cyber resilience. An estimated 750,000 U.S. cybersecurity jobs are open in 2023. Making matters worse, the competition for talent means many organizations don't have the budget to hire enough security staff for around-the-clock coverage.

At the same time, cloud and digital transformation has significantly increased cyber risk to enterprises of all sizes. The attack surface has expanded, and cyber attacks have increased, led by an alarming increase in business email compromise and ransomware attempts.

To help organizations improve their security posture, MDR services provide cybersecurity expertise, technology, and support when there are no existing internal capabilities, or when an organization must accelerate or augment existing security operations. As an extension of an organization's security efforts, MDR service providers help the internal team deliver the optimal value from existing cyber investments.

The right MDR provider will help strengthen your organization's cyber resilience through faster, more robust threat detection and response capabilities, improve visibility into threats so that others can understand risk, and increase the overall value of security investments and tools.

01

Cyber threat landscape expanding as attacker capabilities increase

7%

Global weekly attacks rose **7% in Q1 2023**

02

Organizations are using more SaaS apps than ever

18%

Net growth of SaaS apps is up **18% over last year**—organizations use 130 apps on average

03

Cybersecurity workforce gap continues to grow

3.4M

3.4 million cybersecurity workers needed to fill global gap

02. Extend Coverage, Fill Skills Gaps and Maximize Security Investments with MDR

Managed Detection and Response (MDR) services provide organizations with effective, efficient, remotely delivered, and human-led security operations center functions.

As a fully managed security service, MDRs include SIEM, SOAR, and identity management security tools. However, these services are most effective when security architects and analysts coordinate with a customer's in-house SecOps team for automated, manual, and on-demand response actions based on predefined and custom escalation workflows.

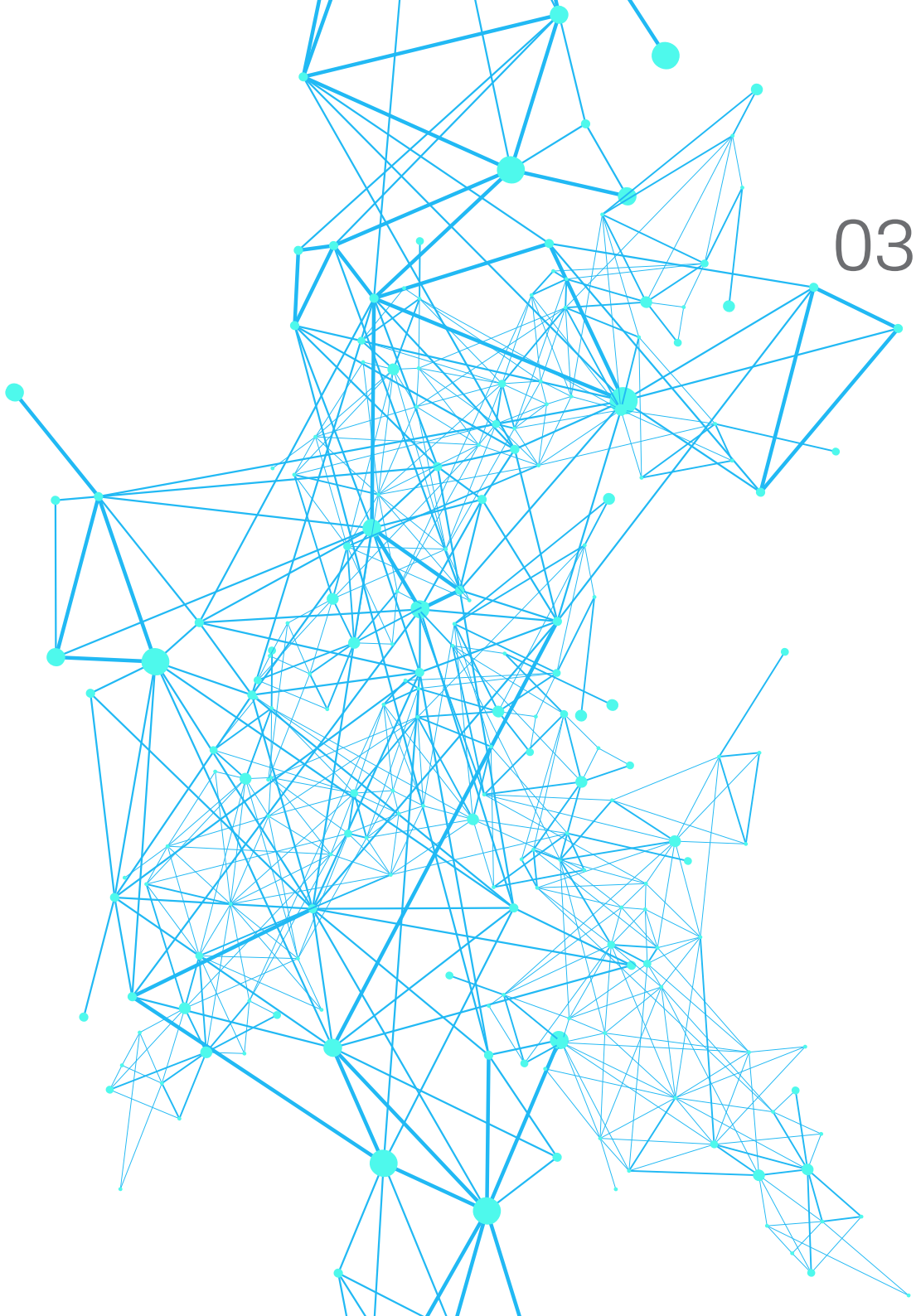
When choosing an MDR service provider, CISOs and SecOps leaders should look for partner organizations that look to maximize investments in security tools, taking an agnostic, risk-based approach and/or consolidating to reduce subscriptions. They should also strongly consider MDR providers that offer:

- Remote, mitigated response offering disruption and containment activities in addition to typical alerting and notification (i.e., quarantining hosts and deauthenticating users).
- Tier 1 and Tier 2 analyst functions, allowing security organizations to focus resources on engineering and architecture.
- Context-driven insights that directly impact business objectives, with data collected, sorted, and presented visually as board-ready reports.

By 2025, 60% of organizations will actively use remote threat disruption and containment capabilities that MDR providers deliver, up from 30% in 2023.

60%

In this MDR Buyer's Guide, we look at the key considerations for choosing an MDR provider and how Deepwatch's Managed Security Platform helps security organizations become more cyber resilient.



03. Key Benefits of MDR

Some managed service vendors have created confusion around the term MDR, selling alert technology features or automation as a way to reduce headcount or threat response time. But there is no replacement for human-centric analysis, enriched data analytics, and curated response playbooks that should be an MDR provider's core offering.

Security Solution Alternatives

An organization focused on improving its security posture has many options in the marketplace. Which is the right choice? Here's a look into the common solutions.

OPTIONS	SECURITY POSTURE IMPACT
Status Quo	Although cyber threats are increasing, economic uncertainty and scrutiny over IT expenses means resources may not be available to level up security.
Managed Technology (EDR, XDR, SIEM)	Overlay to existing technologies with little-to-no human expertise or intervention.
MSSP	Managed disruption and containment services plus alerting and notification
MDR	Provides human interpretation of security incidents, providing guidance, as well as performing the initial mitigation steps.

04. Your **MDR Provider Checklist**

As you consider the alternatives to improve your security posture, here are the essential functions you should expect from an MDR provider.

Remote, Mitigated Response

- Engages daily with an organization's unique set of data, security outcomes, and business-driven risk profile.
- Remotely delivers threat monitoring, detection, threat hunting, threat intelligence (TI), and hands-on incident response.
- Offers coverage around the clock, every day of the year especially nights and weekends and national holidays.

Extend Security Teams

With tighter budgets, reduced or frozen headcounts, and more scrutiny over IT/cybersecurity purchases, companies look to optimize their current investments. Customers expect the MDR provider to function as the entire SOC Tier 1 and 2 analyst cohort or as an extended part of their existing SOC to perform around-the-clock coverage.

- Engages daily with an organization's unique set of data, security outcomes, and business-driven risk profile.
- Remotely delivers threat monitoring, detection, threat hunting, threat intelligence (TI), and hands-on incident response.
- Offers coverage around the clock, every day of the year especially nights and weekends and national holidays.

Large enterprises spend an average each year of

$5.7M to staff a SOC team

Ponemon Institute & ESG research

Utilization, Efficiency, Consolidation

The average security organization uses more than 40 tools in their security tech stack. An MDR provider should help security teams optimize existing tools and look for opportunities to consolidate the security stack to reduce cost and improve visibility into the overall security posture.

01 A platform-agnostic MDR provider helps security teams utilize existing security investments, rather than a rip-and-replace technology solution.

02 Improve utilization of existing ticketing systems and their process for enriched data analysis.

03 Provide high-fidelity actionable findings to which internal teams can successfully respond.

04 MDR providers can help accelerate implementation of new tools, or help teams reduce subscriptions and ingest costs.

Nearly half of organizations say they have a problematic **shortage of cybersecurity skills**

"Why MDR?" -ESG/Deepwatch Survey 2022

45%

Avoid service providers who require migration to an exclusive set of tools to replace existing investments. Instead, **look for an open architecture approach that makes the best of what's in place so you're less dependent on any single security tool or platform.**

A Wall Street Journal/National Association of Corporate Directors survey found only **3 of 10 Boards of Directors highly rate their ability to respond to a cyber crisis.**

-WSJ March 23, 2023.

Security teams can improve efficiency through automation or by delegating time consuming or after-hours tasks to an MDR provider. An MDR provider should deliver Tier 1 and Tier 2 security analysis, freeing security engineers and architects to work on tasks that more directly impact business operations.

- **The MDR provider should add value to lean security teams with faster, deeper insights.**
- **Ask how the MDR provider can reduce alert fatigue through enriched data analysis.**
- **Ask how they will work with an organization's existing security team to prioritize analysis and incident response tasks.**

For teams looking to reduce the proliferation of security tools, MDR providers can help assess their most critical log sources and analytics platforms. They can often lower subscription fees and data ingestion costs. In coordination with an existing security plan, MDR service providers should help teams deliver high-fidelity alerts, and consolidate tasks, log ingestion sources, reporting, and ticketing systems to improve efficiency.

A Gartner Survey showed **75%** of organizations pursued security vendor consolidation in 2022, **with 65%** consolidating to improve risk posture. Only **29%** of organizations consolidate to reduce spending on licensing.

Gartner Infographic: Top Trends in Cybersecurity 2022

Visibility, Prioritization, and Business Impact

An MDR service provider's goal is to increase an organization's visibility into threats across endpoints, identities, and cloud environments, and help teams prioritize responses aligned to business-focused risks.

- Look for an MDR provider that delivers a prioritized, risk-based view of threat exposures, not simply an avalanche of technology outputs without further analysis.
- MDR reduces tooling costs by quickly implementing improved processes and security posture.
- Identify threats faster and reduce the cost of event response in the expanding threat landscape.

More Control Over Security Events and Actions

Large organizations can't adequately outsource every security operation, so ensure that an MDR provider's outputs and coverage aligns with internal incident response systems. Coordinated detection and response activities will reduce the time between detecting and responding to threats across the enterprise.

- Perform remote disruption and containment activities to support internal incident response processes.
- Adapt or integrate with existing technology while expanding security posture across the corporate architecture as well as endpoints.
- Offers a unified interface that delivers an advanced level of visibility and transparency to an organization's managed security operations.

Security Outcomes Tied to Business Objectives

MDR users must develop and implement their own internal incident response policies and procedures to prioritize response activities. The MDR provider can help develop policies and playbooks that reflect an organization's business-driven requirements. In the event of a threat, the MDR provider must deliver actionable findings that guide internal response as well provide remote mitigative response, investigation, and containment activities.

- Assess how a provider's containment approach and incident reporting will integrate with your organization and whether those actions align with business requirements as well as relevant compliance regulations.
- Select a provider that will triage, investigate, and manage responses to all discovered threats without limitations on time or volumes.
- Look for a provider with the capability to address threats across the entire modern infrastructure, with visibility and mitigative response to mission critical areas.

05. **The MDR Advantage** Against Cyber Threats

Managed detection and response offers unique solutions for comprehensive security management. Here's an overview of the threat detection and response models and how MDR strengthens an organization's security posture.

MDR IMPROVES **THREAT DETECTION**

Threat Detection	Why It Works
MITRE ATT&CK® framework, a global knowledge base of proven adversary tactics and techniques.	Used for threat modeling and use cases for established TTPs (Tactics, Techniques, and Procedures) to facilitate a rapid incident response.
Threat Intelligence for advanced detection and security risk mitigation.	Curation, application, and operationalization of threat intelligence offers visibility into real-time insights to accelerate responses.
Proactive Threat Hunting that leverages TTPs, Threat Intelligence, and IOCs to identify potentially malicious abnormal activity.	Expert Threat Hunters augment signature-based detections and create a feedback loop to improve existing controls.
Use ML, analytics, and advanced technologies to correlate data, assign alert priority, and provide business context for evaluating security incidents.	Reduces Mean Time to Respond (MTTR) by focusing on the most actionable alerts and integrating ML facilitates real-time alerts.

MDR IMPROVES **INCIDENT RESPONSE**

Response	Why It Works
Standardized, curated playbooks for procedures to respond to detected threats.	Playbooks organized according to the MDR provider's alert triage and workflow integration with the in-house security team.
24/7/365 human-led security monitoring supported by technologies and automation, who investigate alerts, escalate incidents, and manage cases and tickets.	Trained security analysts monitoring the network ensure that they identify threat actors and respond according to the playbook.
Endpoint Detection and Response (EDR) for real-time endpoint monitoring, mitigation, and remediation capabilities.	EDR captures data from network and provides remote incident response capabilities to contain, isolate, and remove threats.
Attack Surface Management (ASM) ensures a full understanding of the environment's assets and their susceptibility to attack and guides mitigation and patching efforts.	A proactive AMS program helps identify and patch security issues to deter threat actors scanning for unpatched systems and assets.

MDR IMPROVES **SECURITY POSTURE**

MDR Methods	Why It Works
Assessing the organization's security posture based on cyber resilience best practices, the current threat landscape, and criticality of business security risks.	Benchmarks compare the security posture against industry peers and provide a roadmap to help companies fill security gaps and improve key metrics.
Prioritization of data sources available in the environment, and tuning all data sources for maximum security fidelity.	Focus on high-priority data sources to reduce alert fatigue, lower storage costs.
24/7/365 access to security experts and best practices to address gaps in technology, policies, and procedures.	An in-house security team partners with the MDR provider to address identified issues, manage cases, and implement recommendations.
Use of up-to-date proprietary and comprehensive detection catalogs and response playbooks.	An MDR provider should offer a robust detection catalog advanced threat detection and develop incident response playbooks.

06. Why Deepwatch for MDR?

Deepwatch is the leading managed security platform for the cyber resilient enterprise. We provide visibility and contextual threat intelligence to rapidly identify, investigate, and resolve cyber threats, backed by a 24/7/365 team of experts.

Stay vigilant by leveraging our advanced security analytics, threat intelligence, and teams of expert security engineers, architects, and analysts to provide continuous monitoring and proactive threat hunting throughout your environment.

Deepwatch Experts

Deepwatch Managed Security Platform services are delivered by a human-led, U.S.-based team of security experts dedicated to your unique business-related security outcomes. With knowledge of your existing security environment and tools, our dedicated teams include a customer success manager, team directors, a detection engineer, a threat hunter, and security analysts. Deepwatch experts provide response recommendations or actions based on unique business-driven requirements.

Deepwatch Platform

The Deepwatch platform manages leading security technology solutions including Splunk, Cortex, and Okta. This visualization, communication, and reporting tool helps teams communicate risk throughout their organization in ways others can understand.

Deepwatch Security Center

The Deepwatch platform manages leading security technology solutions including Splunk, Cortex, and Okta. This visualization, communication, and reporting tool helps teams communicate risk throughout their organization in ways others can understand.

Deepwatch Security Index

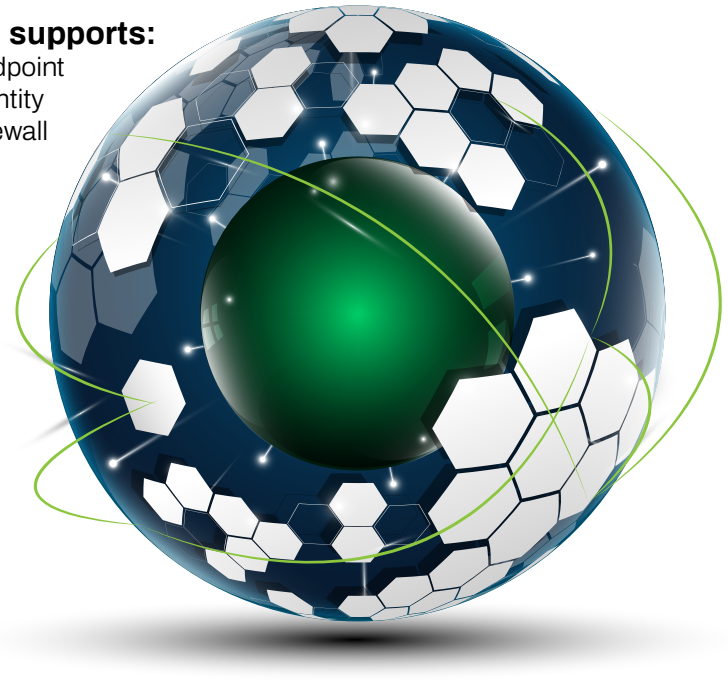
Quantify your security posture with the Deepwatch Security Index, a patented methodology that delivers real-time measurement and benchmarking of your security operations while providing next best actions and a roadmap for continuous improvement. It delivers daily board-level reporting, metrics, full transparency and unmatched visibility.

Deepwatch Active Response

Deepwatch's Active Response service is our open architecture cross-platform capability focusing on automated and orchestrated response actions across multiple technology types. Combined with in-house threat intelligence and contextual information, Active Response manages exceptions to high-fidelity alerts, manages the approvals for further actions and integrates with a variety of ticketing vendors to contain and remediate threats within a client's environment.

Deepwatch currently supports:

- Active Response for Endpoint
- Active Response for Identity
- Active Response for Firewall



Take the **Next Step**

Your organization doesn't have to fight cyber threats alone. A trusted MDR provider delivers faster detections and significantly reduces the number of security alerts that teams need to focus on, while leveraging existing security investments.

Look for an MDR provider with a cloud-based platform that combines advanced analytics, threat intelligence, detection, and both human and automated response capabilities and tailored guidance from security experts.

Deepwatch's 24/7/365 Managed Security Platform ensures a constant enhancement of your cyber resilience. By minimizing vulnerabilities and responding to emerging threats, we empower your organization to stay one step ahead in the face of cyber adversaries. We operate as an extension of your team with most comprehensive advanced threat detection and response capabilities backed by security experts.

Take the next step on your MDR journey by visiting www.deepwatch.com or by reaching out to us at **sales@deepwatch.com.**

ABOUT **DEEPWATCH**

Deepwatch is the leading managed security platform for cyber-resilient enterprises. Our comprehensive solution, expert practitioners, and AI-powered technology provide unparalleled threat detection and response capabilities, enhancing your security and reducing risk. Join leading brands relying on Deepwatch for cyber resiliency.posture, reduce risk, and provide peace of mind. Join the ranks of leading brands who rely on Deepwatch for cyber resiliency.

Visit **www.deepwatch.com** or reach out to us a**t sales@deepwatch.com.**