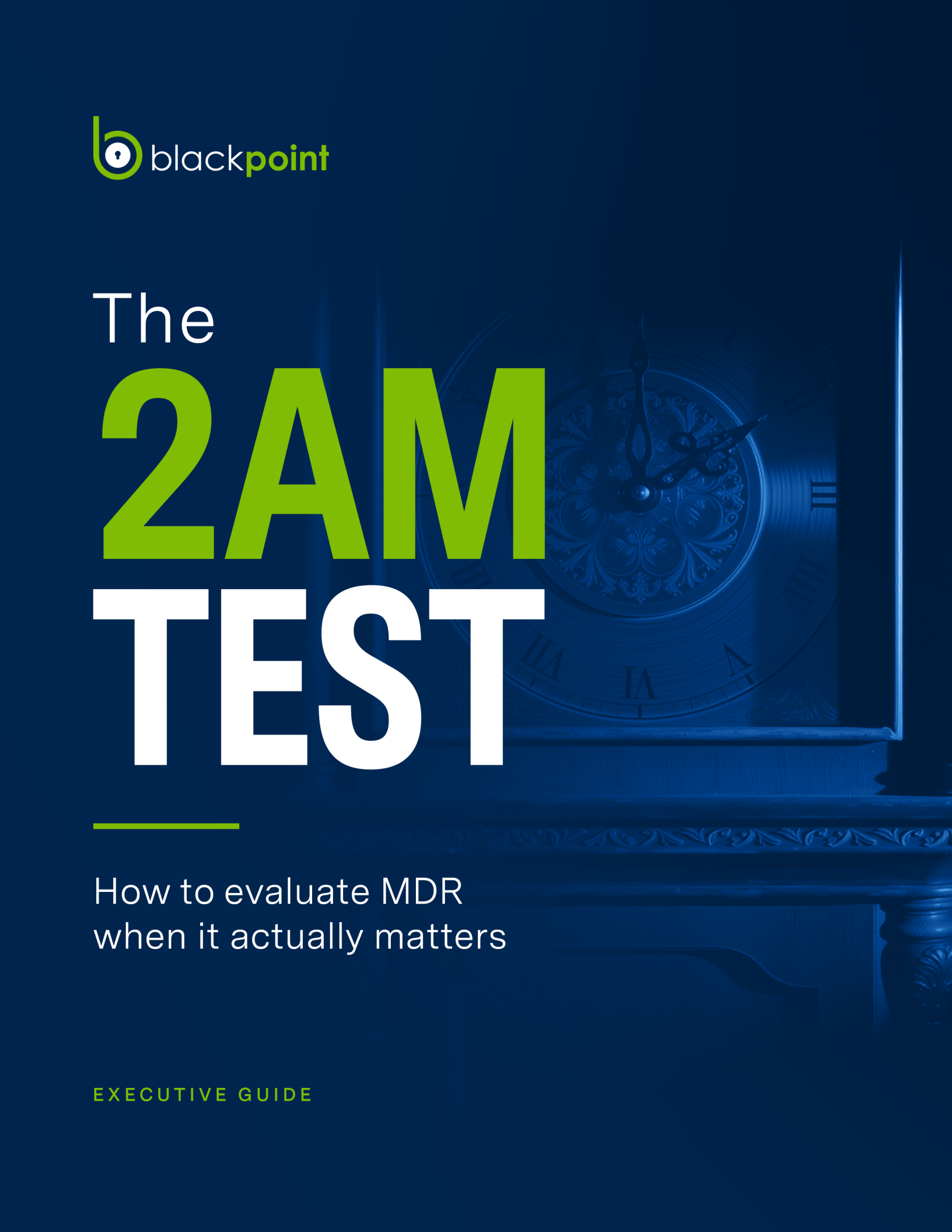
blackpoint

The 2AM TEST



How to evaluate MDR when it actually matters

EXECUTIVE GUIDE

Executive Summary

Whether you're evaluating MDR for the first time or reassessing your current provider, the category itself is no longer up for debate. Market analysts have codified it, platforms have matured, and most buyers realize that some form of MDR is necessary.

What rarely gets examined is what happens after a threat is detected. With 67% of security decision-makers reporting at least one breach in the past 12 months, the question is no longer whether incidents happen — the real question is whether your MDR provider acts when they do.[1]

The MDR category has matured, but the buying process hasn't kept pace. Most evaluations focus on dashboards and detection capabilities, not on what a provider will actually do at 2AM when something is live and moving. That gap between a good demo and a good response is where this guide lives.

What follows is a practical framework for evaluating MDR on the criteria that matter most: authority, speed, surface coverage, and proof. The goal is to give you the questions, metrics, and case context to tell the difference between a provider built for visibility and one built for outcomes.

67%

of security decision-makers reporting at least one breach in the past 12 months.

1 Forrester — Security Decision-Maker Survey, 2025

Table of Contents

Introduction

The 2AM Test:
What It Means for Your Business

When your clients sign on for 24/7 security, they're not just buying a monitoring service. They're buying the peace of mind that if something goes wrong at 2 AM on a Sunday, someone capable is already handling it. Whether your current MDR partner can actually deliver on that is the question this guide is built to help you answer.

The timing pressure is real. Sophos research puts 88–91% of ransomware attacks outside standard business hours. Attackers choose those windows deliberately: slower human response means more time to move, more data to take, and a much larger recovery bill for your client. The gap between when a threat is detected and when it's stopped is measured in business impact, not just minutes.

88-91%
of ransomware attacks occur outside business hours.

The Test Happens at 2AM

At 2:07 in the morning, nobody cares what was on the demo slide.

They care whether the compromised endpoint got isolated, the attacker's session token was revoked, and the mailbox rule that set up the business email compromise was disabled before finance woke up. They care whether the MSP that sold '24/7 protection' actually did something, or opened a ticket and waited for morning.

The cybersecurity industry has spent years teaching buyers to value visibility. Fair enough: visibility is a prerequisite. But seeing the threat and stopping it are two different things.

01

The Numbers Are Worth Taking Seriously

The Microsoft Digital Defense Report 2024 puts identity attack volume at more than 600 million per day, with over 99% of those attacks being password-based. The scale is staggering, but it's the response window that puts real pressure on MDR models. Verizon's 2025 DBIR found that third-party involvement in SMB breaches doubled from 15 to 30% in a single year. That means the compromise often arrives through a trusted tool or vendor before your team knows anything is wrong. If your MDR escalation chain requires customer approval before anyone acts, you're already behind the moment the alert fires.

Mandiant's M-Trends 2025 data shows a median global dwell time of 11 days, but dwell time measures discovery, not damage. The destructive phase of a modern intrusion can unfold within hours and, sometimes, even minutes. Attackers stay quiet for days, then move fast once they do.

Attackers Have Already Read the Calendar

Ransomware operators treat the calendar as an attack surface. Hitting on a Friday night, a holiday weekend, or during a shift change is a deliberate choice. Every hour between compromise and containment is an hour the adversary moves laterally, deepens access, exfiltrates data, and makes recovery more expensive.

Verizon's 2025 DBIR SMB snapshot makes the business exposure specific. Ransomware showed up in 44% of all breaches, and 88% of SMB breaches. Third-party involvement doubled in the same period, from 15 to 30%. Smaller organizations are getting hit on two fronts at once: direct ransomware targeting and compromise arriving through vendors and managed tools sitting upstream of them.

88%

of small and medium-sized business breaches involved ransomware in 2025.

Four Questions That Matter More Than the Demo

Effective MDR reduces the time between detecting malicious activity and containment. The '2AM test' is the cleanest way to evaluate that promise. By the end of any provider conversation, you should be able to answer these four questions with confidence.

Too many MDR evaluations end up focused on dashboards, portals, and monthly reports, things that are easy to show in a demo. The harder questions involve disabling identities, isolating hosts, blocking outbound traffic, killing malicious processes, removing mailbox rules, and rotating credentials at 2AM, without delegating responsibility back to the MSP. Those are the questions that reveal the actual service.

The Four Questions

Who acts after hours?

What authority do they have to act?

What can they actually contain?

How will you know if it was done?

Detection is Where Response Should Begin

Not all MDR providers that claim around-the-clock coverage are built the same.

Despite similar acronyms, pitches, and promises, the difference becomes visible only when an incident is live and moving. Detection is the starting point. What separates providers is what happens in the seconds and minutes that follow: whether someone is already acting, or whether an alert just entered a queue.

02

Two Models, One Name

An alert-led model works like this: the provider ingests telemetry, correlates signals, investigates and triages, and notifies with a ticket, phone call, chat message, and/or portal notification to the customer. Sometimes it offers recommendations or can take an automated action if someone approves it quickly. The customer is still the last link in the response chain.

A response-led model is built around pre-negotiated authority. Before an incident ever happens, the provider and customer agree on a defined set of allowed actions: isolate the device, disable the account, revoke risky sessions, remove persistence, block known-bad indicators, and initiate a defined workflow. When that type of response is needed at 2AM, the provider acts. Then it communicates. It still documents, escalates, and keeps the customer informed, but it doesn't stall containment waiting for notification.

Getting Past the Demo

The question that reveals most about an MDR service isn't 'how does your team work with ours?' It's 'what will you do before you talk to us?' Most teams are already managing response with partial automation and too many manual steps. An MDR service that routes the alert back into that same queue hasn't changed anything; it's just added a vendor. The real differentiators are cross-surface investigation, action within the tools you already have, and SLAs to back it up.

Alert-Led MDR	Response-Led MDR
Detects, validates, notifies	Detects, investigates, contains, then informs
Ticket or phone call at 2AM	Bounded action already underway at 2AM
Customer approves most actions	Pre-authorized actions for defined scenarios
Strength: Visibility and triage	Strength: Operational loss reduction
Gap: Delay between detection and containment	Gap: Requires governance and trust model upfront
Identity coverage: Often lighter or add-on	Identity coverage: Core of service design
Best for: Mature in-house IR teams	Best for: Lean MSP or security team needing execution leverage
Ask: How will you notify us?	Ask: What will you do before notifying us?

What Effective Response Actually Looks Like

Most MDR conversations get stuck on features.

The better question is: what will actually happen in the first 15 minutes of a live incident, and how do you hold a provider accountable to that answer? That starts with understanding what you're measuring and why it matters.

03

Cut Through the Alert Noise First

Before any metric means anything, there's a more immediate problem: 59% of security leaders say they have too many alerts, and more than half say too many are false positives (Splunk, 2025). A provider that adds volume without adding clarity hasn't improved your security posture. The first job of a good MDR partner is signal quality, giving your team the confidence to act decisively when something real fires.

59%
of security leaders say they have too many alerts

Response Time Is Four Different Clocks

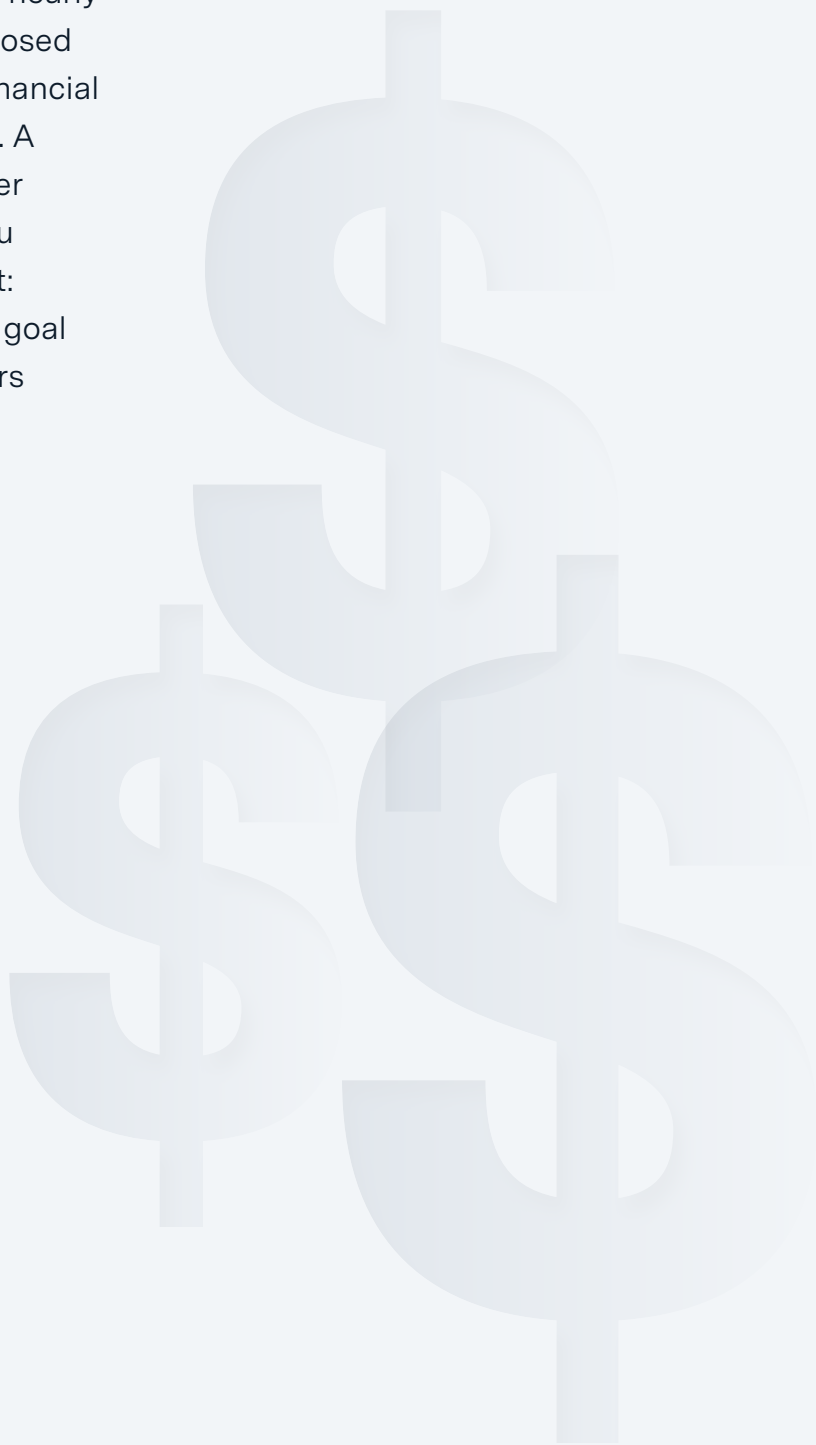
When a provider quotes a response time, that number only means something if you know what it's measuring. Acknowledgment, investigation, containment, and action scope each start and stop at different points, and a provider can look fast on one while being slow where it counts. Here's what to pin down:

- **Mean Time to Acknowledge (MTTA):** How long before a real person or validated automation owns the issue.
- **Mean Time to Respond (MTTR):** How long before investigation and active response begin.
- **Mean Time to Contain (MTTC):** How long before the attacker is actively stopped.
- **Mean Time to Detect (MTTD):** How long it takes to discover a security incident after it occurs.
- **Action Scope:** What can be done without waiting for customer approval.
- **Coverage Depth:** Whether actions work across endpoint, identity, email, cloud, and network.
- **Severity Logic:** Whether Service Level Objectives (SLOs) are tiered and documented.

SANS' research puts the current state in context: only 8.3% of organizations begin scoping and containment within seconds of a confirmed threat, 41.4% get there within minutes, and 32.8% take hours. Most defenders are operating in the minutes-to-hours window. The right MDR partner compresses that, and should be able to show you exactly how.

The Financial Case for Acting Faster

IBM's 2024 Cost of a Data Breach research found that internal detection shortened breach lifecycle by 61 days and saved nearly $1 million compared to incidents disclosed by the attacker. Speed changes the financial outcome, not just the operational one. A partner that acts in the first hour rather than the next morning is a number you can put in front of a board. The caveat: fast and imprecise is its own risk. The goal is fast and right, and the best providers can show you how they balance both.



Why the MSP Model Changes Everything

Most MSPs already know that building genuine 24/7 response coverage in-house doesn't pencil out.

The staffing costs alone are prohibitive, and that's before accounting for the multi-tenant complexity that makes every incident harder to triage than it would be in a single-tenant enterprise. The industry has recognized this, which is why external MDR support has become the default. The question isn't whether to use a partner. It's whether the one you have actually changes what happens when something hits after hours.

04

What 24/7 Coverage Actually Costs

The Sophos 2024 MSP Perspectives survey found that providing out-of-hours coverage was MSPs' second biggest operational challenge. The math behind that isn't complicated: genuine 24/7 SOC coverage requires a minimum of five to six analysts. That's the floor, before sick days, turnover, training, or the management overhead of running a shift structure. A single analyst per shift works fine until two serious incidents hit simultaneously, which is exactly the scenario attackers engineer when they target multiple customers of the same MSP at once.

The talent market makes self-sufficiency even harder. The World Economic Forum's 2025 Cybersecurity Outlook found that two in three organizations face moderate-to-critical cyber skills gaps, with only 14% confident they have the talent they need. For most MSPs, that gap isn't closing. It's widening.

5-6

analysts, at minimum, required to provide genuine 24/7 SOC coverage.

What the Market Is Actually Buying

81% of MSPs already offer MDR, and 80% use an external partner to deliver it (Sophos MSP Survey). The priorities driving those decisions are consistent: 74% say 24/7 incident response is essential or very important. 77% rank Microsoft 365 and Google Workspace account-takeover detection at the top of their list. 71% require the provider to work with their existing telemetry rather than replace it. These aren't wish-list items. They're the baseline. The gap is between MSPs who have a provider that checks these boxes on paper and those who have verified it holds up in practice.

Not All MDR Is Built the Same for MSPs

Three tiers of service operate under the same MDR label, and for a single-tenant enterprise with a full internal IR team, tier one or two might be enough. For an MSP managing dozens of client environments, it almost never is. Tier one gives you better triage. Tier two gives you faster escalation paths. Tier three absorbs execution entirely, handing back a managed incident with documentation rather than a queue item that still needs someone to act on it. The economics only work if your partner is doing the work you can't staff for at 2 AM.

MSPs Are The Entry Point, Not Just the Target

Blackpoint Cyber's 2026 Annual Threat Report found MSPs to be the third most targeted industry in 2025, but the goal is rarely the MSP itself. A single compromised technician account or RMM instance can silently unlock access to dozens of downstream client environments. You're not the destination; you're the master key.

When the compromise originates in your tooling or credentials, the downstream exposure is already in motion before anyone opens a ticket. An MDR partner that understands the MSP model acts across that entire chain, not just the endpoint where the first alert fired. That scope is what makes the difference between containing an incident and inheriting one.

The Playbook Attackers Keep Using

The path of least resistance never goes out of style.

Trusted software, open management ports, unmonitored credentials, holiday weekends: attackers gravitate toward whatever works. The five cases below show the specific gap that separates real response from alert escalation.

05

Kaseya VSA: When the Management Plane Is the Attack Path

In July 2021, timed deliberately to land on Fourth of July weekend, attackers used Kaseya's VSA software to push a fake update through MSP clients to downstream companies. The timing was no accident. Holidays and long weekends are among the most favorable conditions for ransomware operators: skeleton crews, delayed detection, and hours of uncontested dwell time before anyone notices. A Friday before a federal holiday handed REvil exactly that runway.

According to U.S. government materials from the National Counterintelligence and Security Center, fewer than 60 direct customers were compromised, but the blast radius reached up to 1,500 downstream businesses. REvil's initial demand was $70 million for global decryption.

MDR for MSPs has to cover upstream administrative tooling risk, and has to be operational when attackers expect no one is watching. When a trusted RMM becomes the delivery mechanism, effective response means rapidly identifying every exposed customer, taking containment measures fleet-wide, and coordinating threat hunting across all affected downstream environments. A service scoped only to endpoint triage runs out of road the moment the management plane itself becomes the attack path.

ConnectWise ScreenConnect: Speed Beats Polish

In February 2024, ConnectWise disclosed critical ScreenConnect vulnerabilities, including an authentication bypass rated CVSS 10.0. Cloud instances were patched within 48 hours. On-premises customers had to act immediately. CISA added the primary CVE to the Known Exploited Vulnerabilities catalog on February 22.

What that moment demanded was execution under pressure: identify unpatched instances, initiate emergency mitigations, and cut off attacker access before the exploit became commodity tradecraft. Polished reporting comes later. Blackpoint's 2026 Annual Threat Report adds relevant scale: ScreenConnect appeared in 71.5% of all rogue RMM incidents the SOC handled in 2025, tied to an ongoing campaign named Rogue ScreenConnect. This attack surface is well-established and actively exploited.

Snowflake: The Endpoint Isn't Always the Problem

In June 2024, Mandiant investigated a campaign targeting Snowflake customer instances for data theft and extortion.

Every case traced back to stolen customer credentials, often harvested by infostealer malware. The compromised accounts in analyzed cases had no MFA enabled. Mandiant and Snowflake ultimately notified approximately 165 potentially exposed organizations.

Effective response in that scenario started with the cloud identity: disable the account, revoke tokens, examine authentication anomalies, constrain trusted locations, and hunt for unusual data egress. MDR that frames response primarily as endpoint isolation is working from an outdated playbook. This connects directly to what Blackpoint's 2026 Annual Threat Report identifies as a dominant 2025 attack pattern: AiTM (Adversary-in-the-Middle) phishing, which targets authenticated session tokens rather than credentials.

MGM Resorts: Containment Has a Real Price

MGM's October 2023 SEC filing is one of the most useful public documents on what response decisions cost. The company reported approximately $100 million in negative Adjusted Property EBITDAR impact in September, and incurred less than $10 million in one-time third-party and legal costs. The case makes visible something buyers often skip past: good containment can still be painful, and the MDR conversation should include 'how do you help us choose the least-bad option under time pressure?'

3CX: When the Trusted App Is the Problem

In April 2023, 3CX disclosed that a malicious actor had exploited its product and advised customers to uninstall the 3CX Electron Desktop Application. Mandiant's subsequent analysis found that the 3CX compromise originated through an earlier compromise of Trading Technologies' X_TRADER software—the first documented case of one software supply-chain attack initiating another.

Response in that scenario required breaking trust fast. Uninstall the signed application. Block the update channel. Quarantine the executable that every security tool had been treating as safe. Providers should be asked: how do you handle high-confidence compromise in trusted software?

The Common Thread

In each case, detection wasn't the problem. The organizations could see what was happening. What they lacked was a partner with the authority and pre-established scope to do something about it. That's the gap that made the difference between an incident and a news story.

How to Buy MDR That Passes the Test

The threat data, staffing challenges, and incident cases all point to the same buying criteria.

The only real question is whether the provider you're evaluating can close the gap between detection and containment without waiting for your call.

06

Five Things to Evaluate, In Order of Importance

Push on all five in every MDR conversation. Strong providers give specific, contractual answers.

1. Authority

The foundation of any MDR partnership is pre-approved action. Understand what the provider is authorized to do before contacting you: what's automatic, what requires analyst judgment, and what needs your sign-off. The clearer that model is upfront, the faster everything moves when it matters.

2. Surface Area

Modern intrusions rarely stay on one surface. Look for a provider that can investigate and act across identity, email, endpoint, cloud, and network in a single workflow. 77% of MSPs rank account-takeover detection for Microsoft 365 and Google Workspace as essential or very important (Sophos MSP Survey), and for good reason. Identity is part of the blast radius in most modern intrusions.

3. Proof of Speed

Ask how the provider defines MTTA, MTTR, and MTTC and what starts each clock. Ask how SLOs are tiered and documented. Strong providers are specific about what's automated, what's analyst-led, and what requires your input.

4. Workflow Fit

The best MDR services are built to work within the environment you already have. 71% of buyers consider existing-tool integration essential or very important (Sophos MSP Survey). Look for a provider that integrates into your current stack and simplifies your workflow.

5. Identity and Logging Hygiene

MFA, logging, and SSO are baseline expectations in any well-defended environment. Microsoft's Digital Defense Report 2024 shows MFA alone reduces identity compromise risk by 99.2%. But Forrester found that 80% of modern breaches still involve compromised or stolen identities, meaning controls alone aren't enough without active detection behind them. A strong MDR provider can speak fluently to authentication anomalies, token theft signals, mailbox abuse, and risky OAuth consent grants.

The Bottom Line

Providers who answer every question in this chapter specifically, in writing, backed by references, are worth a serious conversation. Providers who get vague about authority, can't define what starts their response clock, or dodge the after-hours staffing question are also telling you something. Listen to that too. Use the toolkit that follows as your filter. The right partner will welcome every question on it.

Practical Evaluation Toolkit

07

RFP Question Bank

Use these in vendor conversations, RFPs, and evaluation scorecards. The providers who answer these questions with confidence and specificity are the ones worth a closer look.

Theme	Question to Ask	Why It Matters
Authority	Which containment actions can you take without prior customer approval?	Separates response from escalation.
Severity Logic	What are your SLAs by severity for acknowledgment, investigation, containment, and customer communication?	"Fast" or "rapid" needs to be a defined contract term.
Clock Definition	What event starts your MTTA and MTTR clocks?	Vendors measure speed differently.
Identity	Can you disable accounts, revoke sessions, remove malicious inbox rules, and investigate OAuth abuse?	Identity compromise is the primary attack path now.
Endpoint	Can you isolate hosts, kill processes, remove persistence, and collect forensic artifacts remotely?	Endpoint containment is table stakes.
Cloud	How do you handle cloud control-plane abuse, suspicious data egress, and risky admin changes?	Snowflake-style incidents need cloud-native response.
Telemetry	Which third-party security and IT tools can you ingest and act through today?	Stack replacement shouldn't be a prerequisite for service.
After-Hours Execution	Walk us through a Friday night ransomware scenario. Who does what in the first 15, 30, and 60 minutes?	Scenario fluency exposes real maturity.
Human vs. Automation	Which actions are automated, which analyst-approved, which requires customer sign-off?	This is where the real workflow friction lives.
Reporting	What does the customer receive after an after-hours incident by the next business morning?	Artifacts, not reassurance.
False Positives	How do you define a true positive and measure false-positive volume?	Noise reduction is a material value driver.
Staffing	How is your 24/7 operation staffed by shift, geography, and analyst role?	Coverage claims need to be resourced.
Tabletop Support	Do you participate in IR planning and tabletops with partners?	Pre-alignment makes the 2AM response cleaner.
Third-Party Tooling Risk	How do you respond when an RMM, remote support, backup, or identity platform used by your customers is compromised?	Upstream tooling is a primary attack path in MSP environments.
References	Provide three references from after-hours incidents involving identity, endpoint, and cloud.	Generic references are easy to produce. Relevant ones build credibility and trust.

Executive Checklist

Score your current or prospective provider against these 13 criteria. Each one represents a real capability difference between alert escalation and managed response.

Coverage and Authority	
☐	24/7 staffed response with analysts, not just monitoring infrastructure
☐	Pre-approved containment actions for defined scenarios, in writing
☐	Endpoint isolation authority
☐	Account disable and session token revoke authority
☐	Email and SaaS response actions
☐	Cloud control-plane and data-plane investigation

Workflow and Fit	
☐	Works with existing tools and telemetry sources
☐	Provides MTTR, MTTA, and MTTC
☐	After-hours incident communication workflow documented
☐	Multi-tenant MSP operating model support

Evidence	
☐	Partner accountability framework with documented operating standards
☐	Sample incident report reviewed
☐	After-hours reference customer validated

Below 8 checks	Likely alert support only, not response
8-10 checks	Viable, with real gaps
11-13 checks	Passes the 2AM Test

Industry Evidence Snapshot

Reference data for vendor conversations and internal stakeholder alignment.

Signal	What the Data Says	What to Ask Your MDR Provider
Identity attack volume	600M daily attacks, 99%+ password-based (Microsoft DDFR 2024)	How do you detect and respond to credential abuse and token theft?
Ransomware prevalence	Ransomware in 88% of SMB breaches (Verizon 2025 DBIR)	What does your ransomware playbook look like at 2AM?
Third-party exposure	Third-party involvement in SMB breaches doubled to 30% (Verizon)	How do you respond when an upstream tool or vendor is the attack path?
Alert volume	59% of leaders report too many alerts; 55% too many false positives (Splunk)	How do you reduce noise, and what's your true-positive rate?
Automation gap	Only 16% have fully automated response (SANS 2024)	What percentage of your containment actions require human approval?
Off-hours timing	88–91% of ransomware launches occur off-hours (Sophos)	Who is staffed and authorized to act on Saturday night?
MSP delivery model	80% of MSPs use external MDR support (Sophos MSP Survey)	How is your service designed for multi-tenant MSP environments?
Staffing economics	24/7 coverage requires 5–6 analysts (Sophos MSP Survey)	How is your 24/7 operation staffed, and what's your coverage model?
Talent gap	2 in 3 organizations face skills gaps; 14% confident in their talent (WEF 2025)	How does your service reduce the response burden on our team?
Breach frequency	67% of security leaders reported at least one breach in the past 12 months; 33% experienced three or more (Forrester 2025)	How does your service reduce breach recurrence, not just alert on it?

Conclusion

The 2AM test is a certainty.

At some point tonight, this weekend, or next quarter, an alert will fire outside business hours. A live adversary will be active, and the window to contain them will already be closing. In that moment, your MDR provider shows its true value through action or delay.

The MSPs and security leaders who succeed with MDR treat it as an operational capability. They define authority in advance, validate response through real scenarios, and hold partners accountable to outcomes instead of activity. When something triggers at 2AM, execution is already underway.

This is the standard Blackpoint Cyber was built around. A response-led model with pre-authorized action, multi-surface visibility, and a 24/7 SOC designed to act first and communicate alongside response. The goal stays simple: reduce the time between threat detection and containment across every environment an MSP is responsible for.

When your phone lights up, one question defines the outcome: Is the situation already under control, or already escalating?

That answer determines whether your security promise holds or becomes a conversation you have to manage the next morning.

Research Cited

Blackpoint Cyber — Annual Threat Report, 2026

Verizon — Data Breach Investigations Report, 2025

Forrester — Security Decision-Maker Survey, 2025

Mandiant (Google Cloud) — M-Trends Report, 2025

Splunk — State of Security, 2025

World Economic Forum — Global Cybersecurity Outlook, 2025

Microsoft — Digital Defense Report, 2024

IBM — Cost of a Data Breach Report, 2024

Sophos — MSP Perspectives Survey, 2024

SANS Institute — Incident Response Survey, 2024

blackpoint