CyberOne

The MXDR Buyer's Guide

A Practical Guide for IT, Security and Business Leaders to Plan, Evaluate and Implement MXDR With Confidence.

Introduction...

Managed Security for Leaders: Lower Risk, Faster Response, Predictable Ceost

Cyber attacks are getting quicker and more convincing. The priority is simple, find real threats faster, contain them with proof and keep the business running. Identity-led attacks are rising and phishing-resistant MFA still blocks the vast majority of unauthorised access [Microsoft Digital Defense Report 2025]. Breaches remain expensive at a global average of $4.44m [IBM Cost of a Data Breach – 2025].

Supply chain breaches have surged in 2025 to nearly double their usual rate [Cybersentriq 2025], underscoring what is at stake: We have seen production halted at Jaguar Land Rover after a supplier compromise and widespread airport disruption linked to a third-party check-in platform. These are not IT problems. They are continuity, customer and reputational risks that require clearer supplier assurance.

Most organisations are also carrying too many security tools. That adds unnecessary cost, complexity and delays action. The typical stack is about 83 tools from 29 vendors, while integrated platforms detect sooner and contain faster [IBM 2025]. Regulation is tightening with DORA now in force across the EU and the UK moving toward a Cyber Security and Resilience Bill.

Managed security is how you run this well. Clear roles. Evidence you trust. Supplier accountability you can enforce. Managed eXtended Detection and Response sits inside that model. MXDR monitors your estate 24x7 and takes direct action in your environment to isolate risky devices, lock compromised accounts, block malicious emails and stop attacks in your SaaS and cloud services, so detection and containment work together across endpoint, identity, email, SaaS and cloud.

Service providers are under tougher scrutiny and consequences are real. In October 2025 the Information Commissioner's Office fined Capita £14m after a 2023 cyber-attack exposed personal data for around 6.6 million people [Information Commissioner's Office]. That level of focus means boards must demand outcome commitments, monthly evidence and clear authority to act.

This buyer's guide is built for that job. Use the checklists, the weighted RFP score sheet and the 30-day proof-of-value plan to compare providers on outcomes. Test how they reduce time to detect and time to contain, prove coverage of critical assets and keep spend predictable without losing signal. Aim to land value by Day 90 with a simple 0-30-60-90 plan. Our commitment is simple: work in the open, align with your risks and be judged on clear outcomes.

If this guide helps protect revenue, reduce downtime and show ROI with confidence, it has done its job.

Dominic List | **CEO & Founder**

Understanding The MXDR Landscape

For most small to mid-market organisations, the threat landscape now resembles what only large enterprises faced a decade ago. Attackers target the same identity providers, cloud platforms and SaaS ecosystems, but these teams rarely have the people, visibility or maturity to defend at that level.

Most organisations already own a patchwork of point solutions: an EDR here, a SIEM there, some native cloud security controls and perhaps a handful of vulnerability scanners. These tools generate alerts, yet very few translate into decisive outcomes.

The Result?

- Alert fatigue
- A false sense of coverage
- Gaps across identity, SaaS and cloud
- Slow detection and even slower response

Meanwhile, attackers exploit misconfigurations, abused identities and unmanaged cloud workloads long before traditional tooling notices anything is wrong.

The global Managed Detection & Response market is valued at $4.19 billion in 2025 and projected to reach $11.30 billion by 2030, growing at a strong CAGR of 21.95%
Mordor Intelligence MDR Market Analysis 2025

the UK is now the 2nd most-affected country by cyber threats, showing how concentrated and persistent hostile activity has become across the region.
Microsoft Digital Defense Report 2025

What The Latest Data Shows

The Breach Reality in 2025

48% of UK organisations suffered a cyber breach in the last 12 months.

UK Government Cyber Security Breaches Survey 2025

The AI Challenge

74% of leaders say AI-powered threats are a major challenge for their organisation.

Darktrace State of AI Cybersecurity 2025

Yet, 60% of organisations have yet to implement any AI-specific controls.

Microsoft Digital Defense Report 2025

Why It Matters:

Attacks are no longer rare crises, they are routine operational events and are hit hardest because teams are thin, tooling is fragmented and attackers no longer distinguish between SME and enterprise infrastructure.

Identity Is The Front Door

Modern multi-factor authentication blocks over 99% of unauthorised sign-in attempts, yet more than 97% of identity attacks still involve brute-force or password spray. Identity-based attacks rose 32% in the first half of 2025, with attackers shifting to workload identities and token theft.

Initial Access Is Predictable

Microsoft incident response cases attribute 28% of breaches to phishing or social engineering, 18% to unpatched web apps and 12% to exposed remote services. Access brokers now industrialise this step, with 368 brokers impacting 4,000+ victims across 131 countries.

Cloud Is Under Fire

In Azure environments, Microsoft observed a 26% rise in incidents period-on-period, an 87% increase in disruptive campaigns such as mass deletions or ransomware and a 23% rise in credential-access attempts.

Data Theft Is The Norm

In the past year, responders observed data collection in 80% of engagements and confirmed exfiltration in 51% of engagements.

Attacker Scale Is Real

Just 20 internet backbones (ASNs) drive 80%+ of malicious password-spray traffic. AI-generated phishing drives 4.5× higher click-through rates (54% vs 12%) than standard attempts.

Microsoft Digital Defense Report 2025

The small- to mid-market organisation faces enterprise-grade attacks without the headcount to match. Success now depends on unified visibility; detections focused on attacker behaviour and responses that can act across identity, endpoint, SaaS and cloud in minutes, not days.

The Case For A Different Approach

Cybercrime is now a $10.5 trillion industry, on par with the world's third-largest economy, underscoring the scale of the challenge businesses face before any tooling or readiness is even considered.

Cyber Security Ventures Report 2025

Security has historically been reactive. Tools detect an event, analysts triage it and response happens only after impact. This approach is no longer fit for purpose.

Modern attacks begin with identity compromise, token theft, lateral movement across cloud services and privilege escalation inside SaaS platforms. These behaviours rarely trigger traditional signatures or simple alert rules.

Businesses Now Need:

- Unified visibility across endpoint, identity, SaaS, cloud and network
- Threat detection aligned with modern attacker behaviour
- Response that is fast, repeatable and trusted
- Outcomes that align with uptime, continuity, compliance and financial risk
- A solution that does not require growing headcount

MXDR meets this need by integrating people, technology, data and response into a single outcome-driven service.

MXDR in Plain English

Only 27% of UK firms have a board member explicitly responsible for cyber, down from 38% in 2021.
Gov UK - Cyber Breaches Survey 2025

With leadership oversight shrinking and capability gaps widening, the need to strip back complexity and explain security in real business terms comes sharply into focus.

Most organisations already own plenty of security tools, but these tools rarely work together, don't cover the whole environment and often fail to deliver fast action when something goes wrong. MXDR solves this by bringing technology, people and process together into one outcome-driven service.

- **Identities** - Every login, privilege change and access path that attackers routinely target.
- **Cloud Workloads & Platforms** - Where your most important data, systems and integrations now live.
- **SaaS Applications** - Every day, tools create hidden entry points and expose data.
- **Networks & Operational Technology (OT) Industrial Control Systems (ICS)** - Critical systems that must remain available for the business to operate.

To protect these areas effectively, MXDR brings together 5 essential ingredients:

1. **High-Quality Telemetry** - Comprehensive data from across the estate, not isolated alerts.
2. **Advanced Analytics & Detections** - Detection built on attacker behaviours, not outdated matching.
3. **Automation & SOAR** - Pre-approved actions that can cut off an attack in seconds.
4. **24×7x365 Security Operations** - People at the keyboard, verifying and responding at all hours.
5. **Incident Response Expertise** - Experienced specialists who understand the situation, impact and next steps.

Together these five ingredients drive board outcomes – measurable risk reduction, minutes-to-containment and predictable cost.

The Goal Is Simple:
Cut through the noise, identify real threats quickly, act fast and prevent disruption to customers, revenue or operations.

MXDR in Plain English

Almost half of UK businesses report basic cyber skills gaps.
DSIT, Cyber Skills in the UK Labour Market 2025

Where traditional security just produces alerts, MXDR delivers outcomes you can measure and hold to account:

- **Faster Time To Detect - Mean Time To Detect (MTTD)**
  How quickly a real threat is spotted. Faster detection means attackers have less time to move, steal data or cause damage.
- **Faster Time To Contain - Mean Time To Contain (MTTC)**
  How quickly access is cut off once a threat is confirmed. This is the difference between a minor incident and a major outage.
- **Lower False-Positive Rates**
  Fewer meaningless alerts that waste time, your teams stay focused on what genuinely matters.
- **Audit-Ready Evidence For Regulators, Insurers & Boards**
  Clear timelines, actions and proof that the incident was handled correctly. This reduces regulatory pressure and strengthens your insurance position.
- **Clear Accountability For Decisions & Actions**
  One partner is responsible for monitoring, investigating and containing threats, so there's no confusion about who does what, especially during an incident.

In Plain English:
MXDR turns scattered tools and constant alerts into an always-on security capability that prevents disruption and reduces real risk.

Further Reading:
What Is MXDR in Plain English

How to Use This Guide

Global Cyber Crime

2,200 cyber attacks occur globally each day in 2025, which averages to roughly one attack every 39 seconds.

Statista Data Breaches 2017-2025

This guide walks leaders through the commercial and technical considerations required to select and operationalise MXDR successfully.

We Cover:

- Business value and risk reduction
- Readiness and prerequisites
- What good MXDR looks like
- How to evaluate vendors with discipline
- How to run a Proof of Value (PoV)
- TCO/ROI modelling for finance teams
- Operational best practice
- How to secure internal approval
- Support materials you can drop directly into your process

It is written for CEOs, CFOs, CISOs, CIOs, Heads of IT and their teams who want MXDR explained in business English, with actionable tools, not bold claims.

Why MXDR?

Severity Is Surging

The UK saw a 50% increase in the most serious cyber incidents last year, including 204 nationally significant cases.

NCSC Annual Review 2025

With 48% of organisations struggling to keep up with increasingly sophisticated cyber threats, the gap between what businesses expect from their security tools and what they actually deliver is widening.

Annual SaaS spend now averages $4,830 per employee, up 21.9% year on year and much of this growth sits outside formal oversight through Shadow IT and emerging Shadow AI. This expansion increases the attack surface faster than most organisations can secure it (Zylo-SaaS Management Index 2025).

Top Causes of Failure in Today's Environments Include:

- **Identity Compromise** - Multi-factor authentication (MFA) fatigue, token interception, credential theft
- **Cloud Exploitation** - Misconfigurations, excessive privileges, unmanaged resources
- **Ransomware** - Leveraging Remote Desktop Protocol (RDP), phishing, supply chain compromise
- **SaaS Data Leakage** - Unsanctioned apps, accidental sharing, OAuth abuse

Why It Matters:

The baseline threat has moved. The question for boards is no longer "if" but "how fast" the organisation can detect, contain and recover when tactics normally associated with nation-state actors now appear in mid-market incidents.

Why You Need Managed Security Now

Downtime

- Systems and / or services are unavailable
- Staff prevented from working
- Customers prevented from ordering
- Service delivery delays

Loss of Revenue

- Immediate financial losses from theft of funds
- Expensive cost of recovery
- Disrupted normal operations / downtime
- Penalties tied to missed SLAs
- Customer churn, tougher renewals and slower deals

Legal & Regulatory Consequences

- Fines for data breaches and non-compliance
- Lawsuits from customers, clients or shareholders
- Contractual penalties with business partners
- Dismissal of senior management if they are held accountable for the breach

Loss of Intellectual Property

- Customer exposure
- Sensitive information stolen
- Risk of IP loss
- Long clean-up efforts.
- Counterfeit products

Reputational Damage

- Loss of customer trust
- Reduced confidence from employees and suppliers
- Damage to brand
- Difficulty in attracting / maintaining business partners

Challenges with Cyber Insurance

- Cyber Insurer does not pay out
- Higher premiums or difficulty finding insurance at all

How to Measure Value

These outcomes transform security into something measurable and board relevant.

Board-ready outcomes with targets: Report these by incident tier every month.

MTTD
(Mean Time to Detect)
Time from threat start to first detection.
Target: P1 <5 minutes.

MTTR
(Mean Time to Respond)
Time from confirming threat to completing first response action.
Target: P1 <15 minutes.

MTTC
(Mean Time to Contain)
Time to stop attacker access and lateral movement.
Target: P1 <30 minutes.

False-Positive Rate
Percentage of alerts closed as non-malicious.
Target: Trending down MoM

Evidence Quality & Investigation Depth
Case files complete, corroborated and audit-ready so stakeholders can see what happened, why and what was done.

Operating commitments that drive the outcomes: Provider behaviours and artefacts you should expect and review monthly.

SLA Compliance
Contracted SLAs and transparent reporting of adherence via dashboard or pack.
Why It Matters: Proves the provider honours commitments.

KPI Compliance
Clear view of MTTD, MTTR, MTTC, false-positives and recurrence trends.
Why It Matters: Links operations to risk reduction.

Service Reviews & Reporting
Named Customer Success Manager and monthly service review with actions and owners.
Why It Matters: accountability and continuous improvement.

Log Optimisation Activity
Ongoing ingestion and retention tuning to cut noise and cost, with a note of changes made.
Why it Matters: Reduces waste and sharpens detection.

Detection Engineering Activity
New rules and playbook tuning delivered, with rationale and test evidence.
Why It Matters: Sustains detection quality as the environment changes.

Threat Hunting Activity
Hunts completed and findings-to-detections recorded.
Why It Matters: Proactive discovery, not reactive alert chasing.

What good reporting looks like: Include these in the monthly board pack.

- **Per-Tier Metrics:** MTTD | MTTR | MTTC | False-Positive Rate | Incident Categories | Recurrence
- **Executive incident summaries for P1 within 2 hours and investigation dossiers within 24 hours**
- **Root Cause Analysis (RCA) examples with corrective actions and owners**
- **Cost and data clarity: ingestion baselines (GB/day), retention tiers and any overage explained**

Are You Ready for MXDR?

Read this with brutal honesty. If even one-point lands, MXDR is not optional.

01 Alerts, No Outcomes

Your tools keep warning you, but the problems don't get fixed. That is wasted spending. MXDR turns signals into decisions and actions.

02 No Credible 24×7x365

Nights, weekends and holidays (e.g. Christmas) rely on goodwill. Attackers do not. MXDR gives you continuous cover with authority to act.

03 Identity Gaps Linger

MFA exceptions, stale privileged accounts, weak partner access. MXDR treats identity as the primary control surface.

04 Cloud & SaaS Sprawl

Multiple tenants, shadow apps, inconsistent policies. MXDR unifies visibility and response across the lot.

05 Tuning Cannot Keep Up

Rules lag attacker behaviour. Engineers are stretched. MXDR brings detections-as-code and continuous refinement.

06 Board Asks, You Hide

You cannot show MTTD, MTTR or true containment time with confidence. MXDR makes these measurable and defensible.

07 Regulators & Customers Expect Proof

You are asked to provide continuous monitoring, but you cannot produce the evidence quickly. MXDR provides audit-ready cases.

08 Approvals are manual

Manual approvals stall containmenT, adopt named pre-authorised actions matrix with guardrails and audit regularly.

09 Insurance & Contracts Raise The Bar

Renewal terms or key deals require verified monitoring and response. MXDR meets the clause, not just the spirit.

10 Recent Breach Or Near Miss

You were lucky last time. Luck is not a plan. MXDR shortens the time to detect and the time to contain.

11 Big Changes Ahead

M&A, new products, rapid growth. MXDR absorbs the turbulence and keeps control.

If this reads like your reality, move MXDR from "nice to have" to the next funded step. It is the fastest route to fewer tools, clearer accountability and measurable risk reduction.

Minimum Prerequisites

Reality Check

MXDR is an amplifier of capability. It will not create visibility, access or governance where none exists. The right partner will meet you where you are, stabilise noisy areas quickly and deliver measurable improvement within 90 days.

If a provider cannot map clear milestones and act on your behalf, keep looking.

Even the best MXDR service will underdeliver if your foundations are weak. Before you sign a contract, be confident you can commit to the following. If any are missing, close the gap first or run a short readiness sprint with your provider:

1. Plug In Full Telemetry - Ensure your provider connects core signals across endpoints, identity, SaaS, cloud and networks. Partial feeds equal partial outcomes.

2. Grant Authority To Act - Provide appropriate administrative access for onboarding, tuning and integrated response. This should include the ability to isolate endpoints, deactivate accounts, revoke tokens and quarantine cloud resources under agreed runbooks.

3. Set The Operating Rhythm - Agree on clear channels and a firm cadence for triage, escalation and review, led by your provider. Define who is on point 24×7x365, how war rooms spin up and what constitutes an executive notification.

4. Put An Executive On The Hook - Appoint a sponsor who owns risk, budget and authority. They approve runbooks, remove blockers and make trade-offs explicit.

5. Know What You Are Defending - Maintain a usable asset and identity inventory, plus baseline configurations for critical systems. Accuracy beats perfection.

6. Strengthen Identity Basics - Enforce multi-factor authentication for all users, use single sign-on where possible and apply least privilege for admins and service accounts.

7. Align On Outcomes & Evidence - Set measurable goals up front: mean time to detect, true containment time, false-positive rate and the quality of case evidence for audit.

8. Commit To Remediation At Pace - Agree on who implements fixes, target SLAs and how changes are tracked to closure. Insight without action is wasted spend.

9. Nail Governance & Data Handling - Document data residency, retention and access logging. Confirm the provider's right to operate during incidents and the approvals needed.

10 Prepare For Integration - Allow integration with ITSM, collaboration tools and identity providers so detection leads to action without swivel-chair work.

Further Reading:
Are You Ready for MXDR?

MXDR Readiness Checklist

Category	Requirement	Why It Matters	Status
Environment	Hybrid or multi-cloud estate (Azure, AWS, on-premises, SaaS)	MXDR needs data across all domains to detect multi-stage attacks	
	Telemetry coverage across endpoint, identity, network and cloud	Weak data collection creates blind spots and missed detections	
	Regulatory or audit pressure present (NIS2, ISO27001, PCI DSS, DSPT)	Compliance compels measurable controls and monitoring	
People & Process	Internal SOC or IT operations with limited 24×7x365 coverage	MXDR fills out-of-hours and depth gaps	
	Clear communication and escalation procedures	Enables rapid triage and hand-off	
	Executive sponsor with budget and decision-making authority	Keeps the initiative funded and aligned to business outcomes	

Category	Requirement	Why It Matters	Status
Technology Readiness	Secure administrative access for onboarding and tuning	MXDR needs data across all domains to detect multi-stage attacks	
	Strong identity controls (Entra ID/SSO/MFA)	Weak data collection creates blind spots and missed detections	
	Automated log forwarding or integration into a central platform	Manual log collection slows detection and response	
Operational Maturity	Regular review of alerts and reports	Drives accountability and continuous improvement	
	Willingness to act on provider recommendations and remediation	Insight without action is wasted budget	
	MXDR metrics linked to business KPIs (MTTD, MTTR, risk reduction)	Demonstrates ROI and aligns security with business value	

Interpretation:

8 or more checks: You're ready and will extract value rapidly.

5 to 7 checks: You're close, but address visibility or process gaps when proceeding.

Fewer than 5 checks: Invest first in telemetry, governance and sponsorship before engaging MXDR.

MXDR Costs (and how to control them)

The cost drivers

Log Ingestion / Retention

3 Major Factors to Consider:

1. Ingestion Volume
(GB/day into the SIEM)

2. Ingestion Volume
(GB/day into a Data Lake)

3. Retention Period (90-days, 365-days, 12-years, hot vs. cold storage)

Be aware of overage charges for ingestion.

Managed Service

Which Pricing Model is Used?

- Per-User Per-Month
- Per-Device Per-Month
- Events Per Second

Add-On Services

Do You Require An Expanded Service?

- Incident Response
- Dark Web Monitoring
- Crisis Simulation Exercises
- Dedicated Analysts / Threat Hunters

Log Ingestion / Retention

Are there any additional or hidden charges?

- Custom Rules / Playbooks
- Additional Data Connectors / Integrations
- Threat Hunting & Threat Intelligence
- Incident Response & Containment Fees
- Out-of-Hours Fees
- Log Optimisation / Rule Tuning
- SLA Upgrades
- Root Cause Analysis (RCA) Reports

Always ask the question “How much do you charge for x?”.

Data Storage: Hot vs. Cold

🔥 **Hot Storage (Log Analytics)**

What it is: Fast, live workspace for immediate security threats.
Cost: Higher per GB (optimised for speed).
Speed: Instant queries (seconds).
Used For: Stopping active attacks and daily monitoring.
Retention: Short-term (e.g. 90 days).

❄️ **Cold Storage (Sentinel Data Lake)**

What it is: Low-cost, long-term archive for compliance and big data projects.
Cost: Significantly Lower per GB (optimised for volume).
Speed: Slower access, but can handle massive volume.
Used For: Regulatory compliance and massive scale data science/AI.
Retention: Long-term (e.g. years).

MXDR Costs (and how to control them)

The levers to control cost without sacrificing Security Operations.

Log Ingestion / Retention

- Prioritise ingesting high-value logs
- Move away from an “ingest everything” mindset
- Filter noisy high-volume logs prior to ingestion
- Use summarisation for high-volume logs
- Ingest non-security and low-priority logs directly into cold storage
- Retain logs for 90-days of hot storage, then move to cold storage
- Only retain logs for 12-years if mandated by compliance / regulations

Managed Service

- **Per-User Per-Month**

Organisations with a reasonable blend of users, devices, servers, cloud, on-prem, hybrid (majority of orgs fit well here).

- **Per-Device Per-Month**

May suit organisations who are ‘device heavy’ e.g. manufacturing with large numbers of IT and OT devices.

- **Events Per Second**

Very rarely cost-efficient, also causes unpredictable billing, not recommended in most cases.

Add-On Services

Consider negotiating bundled price for your preferred add-ons or invest in a future year.

Log Ingestion / Retention

Request all-inclusive pricing, that includes:

- 24x7x365 coverage
- Contractual and custom SLAs
- Control over your own data
- Monthly service reviews
- Measurable KPIs (MTTD, MTTR, MTTC)
- Custom rules / playbooks
- Additional data connectors / integrations
- Threat hunting and threat intelligence
- Incident response and containment
- Customised service
- Out-of-hours coverage, no exceptions
- Log optimisation / rule tuning
- Root cause analysis (RCA) reports
- Predictable pricing

Selecting an MXDR Provider

The market is crowded with providers claiming 24x7x365 monitoring, AI-powered detection and sub-15-minute response times. The problem is that most organisations approach MXDR selection the same way they've always procured services: with feature-tick RFPs that are gamed, product demonstrations that showcase best-case scenarios and evaluation criteria that measure claims instead of operational reality.

For MXDR, an RFP must make sure a provider is selected based on evidence, capabilities and accountability, evaluate areas that directly influence risk reduction, operational continuity and long-term value is crucial. Minimise risk by selecting providers with verified Microsoft credentials; Microsoft Solutions Partner for Security, Microsoft Intelligent Security Association membership, as well as deep Cyber Security recognition; ISO 27001, NCSC CIR and CREST SOC.

1. Detection Quality	Use behavioural analytics and cross-domain correlation to spot lateral movement, privilege abuse and data exfiltration early.	**6. Governance, Compliance & Data Sovereignty**	In-region storage, least-privilege access, audited logs and exit terms that return your data and content in a usable format.
2. Response & Containment	Named pre-authorised actions matrix, clear playbooks and 24x7x365 cover let analysts act fast with confidence. Show MTTD, MTTR and MTTC by incident tier.	**7. Incident Response**	Cyber Incident Response and recovery capabilities with retainer, surge capacity and regulator-ready processes for evidence handling and post-incident reporting.
3. Coverage	Identities, endpoints, email, SaaS, cloud and network signals flow into one coherent timeline with asset and user context, so priority is obvious.	**8. Provider Resilience & Stability**	A dependable partner with financial strength, resilient operations and managed third-party dependencies so your service stays available when others fail.
4. Stack Optimisation	Run on Microsoft Defender XDR, Microsoft Sentinel, Microsoft Entra and Microsoft Purview as one platform to cut latency, tool sprawl and cost.	**9. Cultural Fit & Communication**	Named team, business-aware communication and regular reviews that drive measurable improvement, not just status updates.
5. Transparency	Monthly reporting shows alert quality, false-positive trend, speed to contain and recurrence falling, with clear pricing, data volumes and retention.	**10. Exit Strategy**	No lock-in with a clear handover plan, open formats for rules and playbooks and a timed data return so you can move without disruption.

How to Score MXDR Providers

An MXDR evaluation should focus on ten categories, weighted by their impact on risk reduction and operational stability. The categories total 100 points, distributed across three strategic groupings that prioritise what drives measurable outcomes.

Critical Capabilities (55%)

These 3 categories determine whether the provider can deliver measurable risk reduction. They represent 55% of your evaluation because they directly impact your ability to detect and stop threats before they cause business interruption.

1. Detection Quality (23% of Evaluation)

The industry obsesses over detection rates, but what matters is precision: how many alerts are true positives that require action versus false positives that waste time.

Detection quality is measured across 3 dimensions:

1. **Precision** - What percentage of alerts are actionable?
2. **Recall** - What percentage of real threats does the system detect?
3. **Business Impact** - How quickly does detection translate to reduced interruption costs?

- **Score Focus:** Behavioural analytics across identity, endpoint, email, apps, cloud and data; false-positive trend; threat hunting results folded back into detections.
- **Ask For:** Top 10 detections with rationale, rules-as-code sample, quarterly hunt plan, findings-to-detections log.
- **Targets:** False-positives trending down month on month; ⩾2 new detections per month from hunts; end-to-end narratives for priority incidents.

2. Response Capability (18% of Evaluation)

Some providers sell you on detection but stop short of actual containment or response. The average time for cybercriminals to move from initial access to full network compromise is 48 mins (Reliaquest, 2025), a MXDR provider needs to outpace that.

Response capability depends on authority - If your provider needs to call you before isolating a compromised device, containment is delayed by hours, not minutes.
Require a delegated action catalogue - A matrix of pre-approved actions that the MXDR provider can execute without awaiting approval.

- **Score Focus:** Speed to first action and time to contain; pre-authorised actions; quality of playbooks and shift handover.
- **Ask For:** SLA extract, pre-authorised actions matrix, sample P1 playbook, shift handover pack.
- **Targets:** P1 MTTD <5 mins, MTTR <15 mins, MTTC <30 mins with evidence in reports.

3. Coverage (14% of Evaluation)

Coverage is about instrumentation, not visibility. What matters is whether the MXDR service has telemetry from every attack surface: identity, endpoint, email, apps and data. For Microsoft environments, this means: **Microsoft Defender XDR** for unified detection and response across endpoints, identities, email and cloud apps. **Microsoft Sentinel** for cloud-scale SIEM and threat hunting. **Microsoft Entra** for identity and access management. **Microsoft Purview** for data security and compliance

- **Score Focus:** Breadth of sources and depth of context; device and identity coverage; entity correlation quality.
- **Ask For:** Data sources list, coverage percentages by domain, entity-timeline examples.
- **Targets:** 90%+ device and identity coverage; unified timelines linking user, device, app and IP for P1–P2 incidents.

Operational Excellence (25%)

These two categories determine how effectively the provider operates and integrates with your existing security investments. They represent 25% of your evaluation and separate providers who deliver ongoing optimisation from those who simply monitor.

4. Stack Optimisation (15% of Evaluation)

How deeply does the MXDR service understand and optimise your security stack? Tools require configuration, tuning and continuous optimisation to be effective.

The 3 Maturity Layers:
1. **Integration Depth** - Can the provider deploy and configure the tools?
2. **Operational Consistency** - Can they maintain performance over time?
3. **Continuous Optimisation** - Do they improve detection and response as threats evolve?

- **Score Focus:** Native use of Microsoft Defender XDR, Microsoft Sentinel, Microsoft Entra and Microsoft Purview; minimal custom glue; plan to retire overlap.
- **Ask For:** Reference architecture, connector inventory, runbooks, tool consolidation plan.
- **Targets:** Sentinel as the primary analytics plane; measurable licence and tool reduction within 90 days.

5. Transparency (10% of Evaluation)

Pricing should be clear and transparent. Know what you are paying for: analyst hours, automation coverage, threat intelligence and incident response retainers. Storage costs should be predictable and optimisable, not a lever to inflate invoices.

Storage - Agree GB/day baselines, retention tiers and capped overage.
Operations - Documented playbooks, clear escalation paths and clear comms cadence.
Reporting - Incident summary within 2 hours of a P1 and analysis within 24 hours

- **Score Focus:** Board-ready reporting and pricing / data clarity.
- **Ask for:** A monthly report pack, root cause analysis samples, pricing schedule with ingestion baselines (GB/day), retention tiers and overage caps with examples.
- **Targets:** Reports by tier every month; all-in scope for hunts, playbooks and out-of-hours; capped overage and documented retention.

Trust & Governance (20%)

These 5 categories determine whether the provider meets regulatory, operational and partnership requirements. They represent 15% of your evaluation and ensure the relationship is sustainable, compliant and aligned to your risk tolerance.

6. Governance, Compliance & Data Sovereignty (7% of Evaluation)

Providers must evidence regulatory compliance and show how controls operate in your tenant. They should be be transparent about data flows, sub-processors and exit.

- **Score Focus:** Data residency, access, encryption and regulation alignment to compliance controls.
- **Ask For:** Data map, in-region processing, role-based access controls, audit log sample, retention and encryption policies.
- **Targets:** In-region storage, just in time access with audited logs, retention aligned to policy, annual control testing.

7. Incident Management (5% of Evaluation)

When a serious incident hits at 02:00, you need immediate DFIR support with authority to act and a single point of contact.

- **Score Focus:** Incident Response readiness beyond business as usual MXDR, evidence handling, regulator and legal interfaces, board-grade reporting.
- **Ask For:** In-house capability, NCSC CIR Certification, IR retainer terms, surge-hours SLA, single-point-of contact, forensic, regulator and legal playbooks.
- **Targets:** Named Incident Response lead, 1-hour engagement SLA for Priority 1, post-incident root cause analysis within 10 working days.

8. Provider Resilience & Stability (5% of Evaluation)

Evaluate SOC staffing levels and analyst retention rates, infrastructure redundancy and failover capabilities, incident escalation procedures and business continuity plans.Request Evidence of Operational Maturity: financial stability and funding history, customer retention rates, references from organisations similar to yours in size, vendor expertise; Microsoft Solutions Partner for Security, Microsoft Intelligent Security Association membership with Microsoft-Verified Managed XDR Solution Status.Supporting sector and industry Cyber Security accreditations (e.g. CREST, NCSC) gives peace of mind.

- **Score Focus:** Provider health and operational resilience, including third-party dependencies.
- **Ask For:** Financial summary, uptime metrics, business continuity plan, disaster recovery tests, list of critical suppliers and dependency SLAs.
- **Targets:** 99.9% platform availability, annual failover tests, supplier risk reviews with actions.

9. Cultural Fit & Communication (2% of Evaluation)

Cultural fit is an often overlooked factor that determines whether a partnership thrives or fails, you need to trust them, understand them and work with them under pressure.

Are notifications clear and actionable? Do exec summaries speak to business impact, not just technical detail? Does the provider adapt their style to your culture?

- **Score Focus:** Ways of working and senior access.
- **Ask For:** Org. chart with named team, comms cadence, RACI, service review agenda.
- **Targets:** Executive sponsor named; monthly service reviews with actions and owners.

10. Exit Strategy (1% of Evaluation)

The best providers make exit planning straightforward because they're confident in their service quality, those who resist exit planning are signalling future problems.

- **Score Focus:** Portability of data and content, and a clean handover.
- **Ask For:** Exit plan, data return formats, rules/playbooks export example, deprovision checklist.
- **Targets:** Confirmed export of rules and playbooks in open formats; data returned within 30 days of termination.

Due Diligence: What to Validate

Data Security, Privacy & Retention

How your data is protected, handled and kept.

- Encryption at rest and in transit, clear key ownership, role-based just-in-time access with audited actions
- How is access granted and logged
- In-country or in-region storage, DPA and sub-processor list with processing locations

Operational Resilience

Ability to run reliably under stress and recover fast.

- Uptime history inc. lessons learned
- Business Continuity Plan / Disaster Recovery test reports for the last 12 months with Recovery Time / Recovery Point Objective achieved.
- Supplier-failure drills and corrective actions tracked to closure

Supply Chain Security

How third-party vendors, tools and hosting are secured.

- Register of critical suppliers, regions and data flows
- Vetting, monitoring and renewal cadence with recent assessments
- Dependency Service Level Agreements, fallback plans and exit paths

Incident Response Capability

Depth and readiness when a serious incident hits.

- Named Incident Response lead, certifications and surge-hours Service Level Agreement
- 1-hour P1 engagement target, chain-of-custody workflow
- Sample post-incident report and regulator or legal playbooks

Accreditations & Certifications

Independent assurance of security operations maturity.

- ISO 27001; NCSC Cyber Incident Response; Microsoft Solutions Partner for Security; Microsoft Intelligent Security Association membership with Verified Managed XDR Solution status

Accreditations & Certifications

Independent assurance of security operations maturity.

- ISO 27001; NCSC Cyber Incident Response; Microsoft Solutions Partner for Security, Microsoft Verified MXDR and MISA membership
- Scope, boundaries and any exclusions, with renewal dates and any open findings

Pricing and Data Clarity

How costs behave and what is included.

- Ingestion baseline (GB/day), hot and cold retention tiers, overage caps with a worked example
- In-scope items listed: hunts, playbooks, out-of-hours and connectors
- Quarterly cost review with variance and optimisation actions

Customer References & Satisfaction

Proof the service delivers in environments like yours.

- References of similar size and sector
- Outcomes and satisfaction: MTTD, MTTA, MTTC, false-positive trend, board reporting, CSAT/NPS and renewal rate
- Named contacts with permission to discuss scope, issues and lessons

How to Structure an Effective Proof of Value (PoV)

The Proof of Value (PoV) is where any claims meet operational reality, without success criteria it is just a demo. It proves nothing about the provider's ability to detect threats in your environment, respond within your risk tolerance or integrate within your estate.

1. Define Success Criteria Before Deployment

Pre-defined success criteria transform the Proof of Value from a sales exercise into an accountability exercise.

Agree on:

- What threats the provider must detect (based on your threats, not their library)
- What response actions they must execute (and how quickly)
- What integrations they must demonstrate (e.g. your Microsoft Security tools)
- What documentation is required (playbooks, runbooks, configuration guides)

Pre-deployment success criteria are tied to business outcomes. For example: "Detect and contain a simulated ransomware attack within 30 minutes, with automated device isolation and executive notification."

2. Test Customer Threat Vectors, Not The Providers Library

The PoV should reflect your threat landscape, not the vendor's demo script.

Work with the provider to design scenarios based on:

- Threats your industry faces (phishing, ransomware, supply chain attacks)
- Current weaknesses (identity compromise, unpatched systems, shadow IT)
- Compliance requirements (data exfiltration detection, privileged access monitoring)

Kill chain validation tests MXDR across the entire attack progression: initial access, privilege escalation, lateral movement, data exfiltration and impact. If the provider only detects the final stage, they're too late.

3. Measure Evidence Translation

Technical metrics must translate to financial outcomes, convert minutes saved into avoided interruption cost for CFO.

An MTTR improvement of 30 minutes translates to reduced business interruption costs. A 12% improvement in protection efficiency translates to avoided loss and productivity savings.

A PoV should produce a business impact statement that converts operational gains into financial outcomes. This is language CFOs understand and it's the first capability that separates vendors who understand your business from those selling technology.

4. Evaluate the Handover Phase

The PoV should include a handover phase that simulates the transition from your current state to the MXDR service.

This tests:

- How the provider documents your environment
- How they train your team on escalation procedures
- How they handle incidents during the transition

A controlled transition is a make-or-break factor in any MXDR success.

5. Set a Time Limit

A PoV should last 2-4 weeks, not months. Longer PoVs create evaluation fatigue and delay decisions. Shorter PoVs don't provide enough data to assess performance under varied conditions.

Two pages maximum for the PoV report. If the provider can't summarise their findings and recommendations in two pages, they don't understand your priorities.

Common Pitfalls to Avoid

Even with a structured framework, organisations make predictable mistakes during MXDR selection. Avoid these six pitfalls:

Pitfall 1:
Equating Coverage with Visibility

Instrumentation Matters: Whether the provider has telemetry from every attack surface and can correlate signals across them.

Pitfall 2:
Accepting Vague Service Level Agreements

SLAs should mandate specific Service Level Objectives (SLOs) in RFPs, not generic commitments to "best effort" response. Require contractually committed MTTD and MTTC targets with financial penalties for breaches.

Pitfall 3:
Ignoring Data Hygiene

Data hygiene is the hidden multiplier in MXDR effectiveness. If logs are noisy, incomplete or misconfigured, even the best provider will struggle to detect threats. A provider should help improve this as part of the service.

Pitfall 4:
Treating the Proof of Value as a Formality

The PoV is not a box-ticking exercise. It's your opportunity to validate claims, test integration and assess cultural fit. Treat it seriously.

Pitfall 5:
Forgetting to define an Exit Plan

Every contract needs a contractual exit plan. If the relationship doesn't work, you need a clear path to transition without operational disruption.

Pitfall 6:
Unclear delegated actions

Without a signed actions matrix, containment requires approvals and response stalls.

Further Reading:
Avoiding Common Pitfalls When Selecting a Security Partner

What Good Looks Like

A well-selected MXDR provider delivers measurable resilience. You will see:

Reduced MTTD & MTTC:
Organisations with AI-powered detection systems identify breaches 80 days faster and save $1.9 million compared to manual detection methods. MXDR users typically see a 50% reduction in MTTD and MTTR (IBM Cost of a Data Breach – 2025).

Higher True Positive Rates
Your team spends less time investigating false positives and more time on strategic security initiatives.

Improved Protection Efficiency
A 12% improvement in protection efficiency translates to measurable cost savings and reduced business interruption.

Confidence In Your Security Posture:
You can defend your security investments to the board with evidence, not anecdotes.

Final Thought

MXDR selection is not a procurement exercise. It's a strategic decision that shapes your security posture for years. The framework in this article gives you a structured, evidence-based approach to evaluate providers, validate their capabilities and make a decision you can defend.

Start with outcomes, not features. Demand proof, not promises. Insist on transparency, not marketing. And remember: the best MXDR provider is not the one with the most impressive demo, but the one who can detect threats in your environment, respond within your risk tolerance and integrate with your Microsoft Security stack to deliver measurable resilience.

Security is not just about providing a service. It's about building a partnership and a secure foundation for your business to thrive.

CyberOne

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.

Assured Service Provider
in association with
National Cyber Security Centre

Assured Service Provider
in association with
National Cyber Security Centre
Cyber Incident Response: Standard Level

CREST

CREST
SECURITY OPERATIONS
Security Operations Centre

CREST
INCIDENT MANAGEMENT
Incident Response

CREST
SECURITY TESTING
Penetration Testing

Member of
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

Microsoft
Solutions Partner
Security
Specialist
Cloud Security
Identity and Access Management
Threat Protection

Microsoft
Solutions Partner
Modern Work

Microsoft
Solutions Partner
Infrastructure
Azure

Microsoft
Solutions Partner
Data & AI
Azure