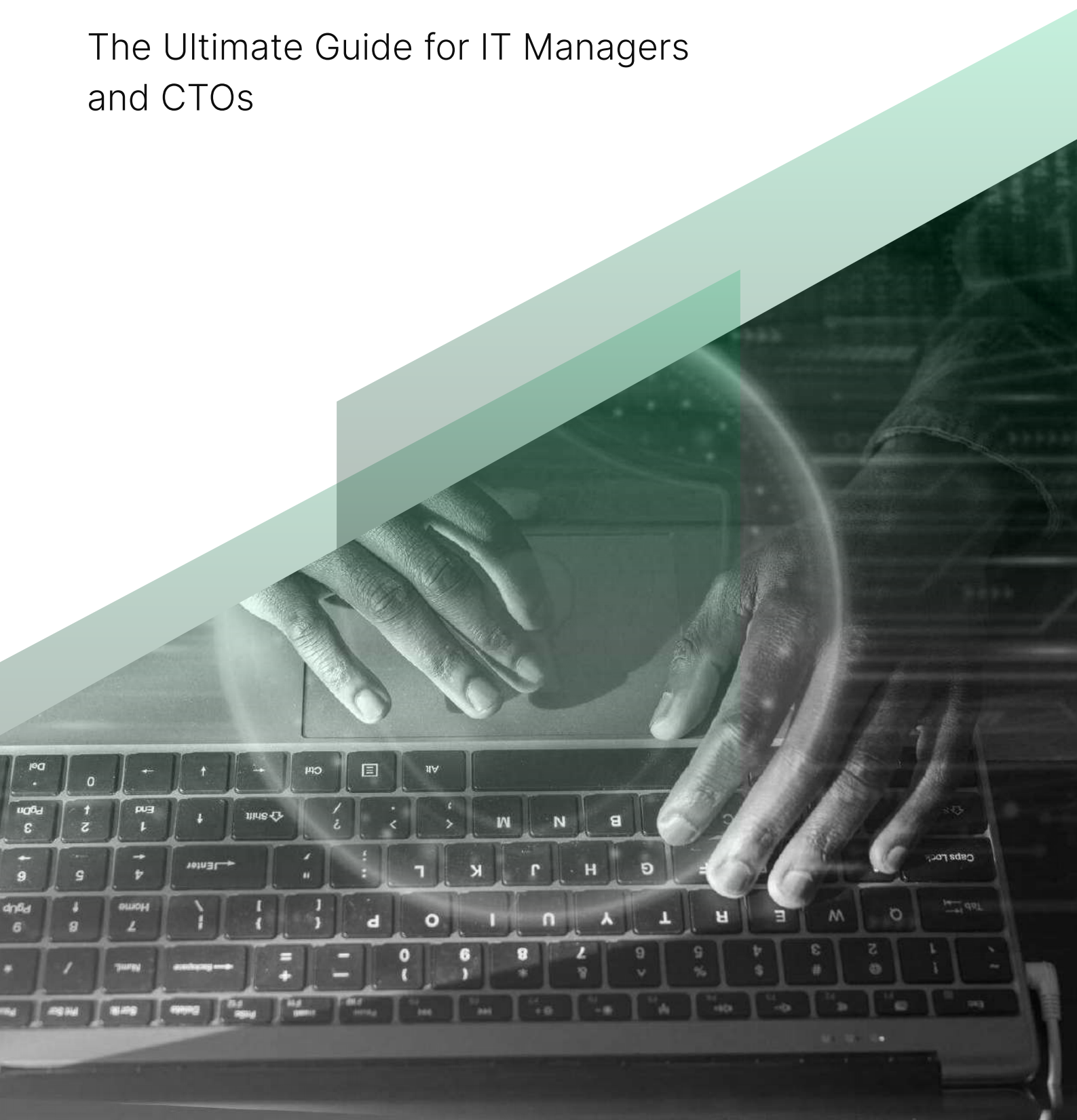
LINEARSTACK

The MDR Buyer's Checklist

The Ultimate Guide for IT Managers and CTOs



Introduction

As cybersecurity decision-makers, you're responsible for safeguarding your organisation's infrastructure against cyber threats. To do this effectively, you'll need Managed Detection and Response (MDR). However, choosing the right MDR can make a big difference in keeping you safe in the long run.

Besides, not all Managed Detection and Response (MDR) services are created equal. Some are reactive, others proactive, and some only monitor endpoints, while others cover the entire environment.

This guide gives you a clear, actionable checklist to evaluate MDR providers effectively. You'll understand how MDR differs from MSSPs, how to assess advanced services like XMDR, and what qualities separate exceptional providers from those that merely check the box.

By the end, you'll have a roadmap to help you make the right call for your organisation.

What Are MSSPs and MDRs?

Many organisations have an IRP on paper but fail when a real incident occurs. Why?

- ✓ **MSSP (Managed Security Service Provider)**

  Focuses on monitoring and alerting. They'll inform you when something's wrong, but the responsibility to respond typically falls back on your internal team.

- ✓ **MDR (Managed Detection and Response)**

  It's a cybersecurity service that spans **endpoints, networks, clouds, emails, and identity systems**. This level of coverage ensures security signals are detected across every part of your environment.

A common challenge in this space is providers over-promising and under-delivering.

Many MSSPs label themselves as "MDR" but only offer basic monitoring without real response or proactive capabilities.

Checklist – How to Evaluate MDR Providers

Many organisations have an IRP on paper but fail when a real incident occurs. Why?

Let's dive right in.

- ✓ **Comprehensive Detection and Response**

  Cyber threats don't just originate at endpoints anymore. Modern environments are interconnected across networks, clouds, and identities. The right MDR provider will offer full visibility and response capabilities across these layers.

- Do they cover EDR, NDR, IDTR and CDR?
- Can they handle threats in your email and identity systems?

Cyber threats don't just originate at endpoints anymore. Modern environments are interconnected across networks, clouds, and identities. The right MDR provider will offer full visibility and response capabilities across these layers.

✓ 24/7 Monitoring and Expert Threat Hunting

Cybercriminals don't stick to business hours, and neither should your MDR team. You need eyes on your systems 24/7 with real analysts—not just an automated dashboard.

- Is there a team actively threat-hunting and analysing incidents around the clock?
- How quickly can they respond to contain and neutralise a threat?

Some providers claim "24/7 support" but rely on skeleton teams. The best MDR services ensure someone with hands-on expertise is monitoring your systems, eliminating threats in real time, and hunting for potential risks before they escalate.

With a strong MDR partner, you'll have skilled analysts who are always on duty. They act faster. Whether it's detecting a threat, analyzing it, or containing it, you'll know someone is working to keep your systems safe at all times. They actively search for hidden threats in your environment, even when no alarms are raised. This means they can uncover potential risks that automated systems may miss.

✓ In-Depth Malware Analysis and Containment

If malware is detected in your environment, you need more than surface-level analysis. A full-scale MDR provider will dissect the malware, identify its origins, behaviours, and execution patterns, and take decisive action to contain it.

- Do they offer in-house malware reverse-engineering?
- Can they quarantine threats immediately and prevent lateral spread?

Detailed malware analysis saves critical time during an attack. It allows your organisation to understand the full scope of the threat while ensuring it's fully eradicated—not just quarantined temporarily.

✓ Scalability and Adaptability

Your environment isn't static, and neither are your security needs. Whether you're scaling operations, moving to the cloud, or undergoing a merger, your MDR provider should adapt seamlessly.

At this point, your considerations centre around two questions:

- Can they customise services to meet your unique infrastructure and workflows?
- How do they handle environments undergoing digital transformation?

Scalability isn't just about size. It all boils down to flexibility. If your environment evolves, your MDR provider should evolve with you without compromising performance.

✓ Proactive Threat Research and Hunting

A reactive defence isn't enough. Your MDR partner should be looking ahead, identifying vulnerabilities before they're exploited and applying those findings to improve your security posture.

- Do they perform ongoing threat research to uncover new vulnerabilities?
- How do they incorporate findings into your environment's detection rules?

Proactive threat hunting is what separates good MDR services from exceptional ones. Teams that research and simulate emerging threats can identify similar risks in your environment before they become real incidents.

✓ Incident Response Capabilities

When a threat occurs, the last thing you want is finger-pointing or vague responses. Your MDR provider should handle incidents with precision and transparency, including root cause analysis and clear reporting.

- Do they investigate the when, how, and why of every incident?
- How effectively do they communicate findings with your internal teams?

Clarity matters – during and after a threat. Incident response isn't just about fixing the problem but understanding what happened, why, and how to prevent it from recurring.

✓ Actionable Reporting and Metrics

Security decision-makers need clear, meaningful insights. Effective reporting provides visibility into threat trends, incidents, and your overall security posture.

- Are reports delivered in a format that aligns with executive and technical needs?
- Do they offer actionable KPIs and metrics for ongoing improvement?

A strong MDR provider simplifies reporting so that even complex incidents can be communicated effectively to your board, C-suite, and IT teams.

✓ Compliance and Data Residency

With privileged access to your systems and data, trust and compliance are non-negotiable. Your MDR provider must operate with transparency, certifications, and strong security processes.

- Are they certified, such as ISO 27001?
- How do they ensure data privacy and internal monitoring?

Providers that prioritise compliance don't just talk about security—they prove it through vetted teams, rigorous monitoring, and adherence to global standards.

For example, LinearStack ensures our team is thoroughly vetted and monitored. Police checks and verifications are conducted every six months, even after hiring. Our internal monitoring system analyzes team behaviour to maintain strict security standards.

When we're compliant, you get the peace of mind that your data is handled with the highest level of care and security. It means we follow strict standards to protect your sensitive information, reduce risks, and prevent mishandling.

✓ ROI: Cost vs. Value Assessment

An MDR service should not be viewed only from the cost perspective. It's an investment in your organisation's resilience. The right partner gives you measurable outcomes: fewer breaches, faster responses, and a stronger overall posture.

You should be asking these questions:

- Does the provider deliver tangible value, not just alerts?
- Are they committed to outcomes like speed, precision, and proactive improvement?
- Are they committed to outcomes like speed, precision, and proactive improvement?

When choosing an MDR partner, don't base decisions solely on price. Focus on the value of avoiding breaches, downtime, and reputational damage—outcomes that far outweigh the cost.

Why LinearStack Titan MDR Stands Out

At LinearStack, we understand what's at stake. That's why we combine these elements in our Titan MDR services

- 24/7 expert monitoring with proactive threat hunting and in-depth malware analysis.
- A full MXDR approach covering endpoints, networks, cloud, email, and identity.
- A Threat Research Unit (TRU) that anticipates emerging threats and strengthens defencess.
- Transparent reporting and flexible solutions that scale with your needs.

We don't just monitor; we act. Our experts become an extension of your team—ready to detect, respond, and prevent threats in real-time.

How LinearStack MDR Works?

Our MDR operates on a three-pronged framework—Reactive, Proactive, and Preventive.

01 → 02 → 03

Reactive

Immediate detection, response, and eradication of threats.

Proactive

Ongoing threat hunting and research through the Threat Research Unit (TRU) to identify emerging risks and vulnerabilities.

Reactive

Continuous risk assessments and IT hygiene recommendations to strengthen your security posture over time.