

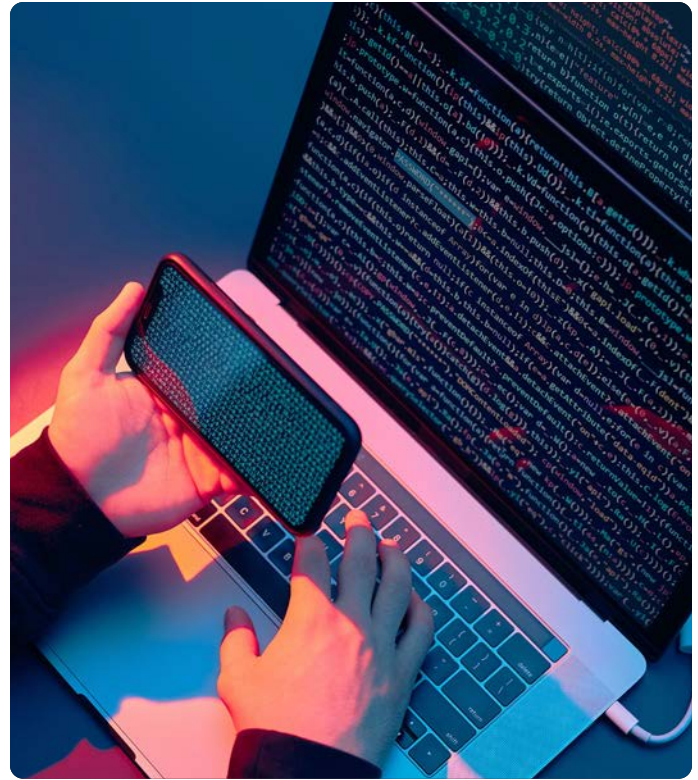
# HCLTech Universal Managed Detection and Response (UMDR)

Universal Detection.  
Rapid Response. Total Security

# Overview

HCLTech UMDR service is revolutionizing the way enterprises perceive and handle cyber threats. This service is built upon a foundation of inclusivity, collaboration, resilience, and adaptability, all aimed at mitigating the impact of sophisticated threats. With HCLTech UMDR, enterprises can make informed decisions, optimize security operations, meet regulatory and privacy requirements, and scale their quantitative cyber risk management programs.

Whether your security operations are handled in-house or outsourced, HCLTech UMDR can modernize your security operations by complementing and augmenting your existing investments. This adaptive approach to threat detection and response is designed to address the fundamental challenges that have long plagued traditional threat management approaches.



# Challenges

As cyber threats continue to evolve, organizations face a myriad of challenges in implementing and managing effective Managed Detection and Response (MDR) strategies. Here are some of the most common challenges:



## Lack of Visibility

Organizations often struggle with gaining full visibility into their enterprise environments that goes beyond just Endpoints. Without this extended visibility, it's difficult to detect and respond to threats effectively.



## Lack of Proactive Threat Hunting

Many organizations rely on reactive measures to deal with cyber threats. However, proactive threat hunting is essential for detecting and responding to threats before they can cause significant damage.



## Shortage of Skilled Personnel

Cybersecurity is a specialized field that requires a high level of expertise. Many organizations struggle to find and retain skilled cybersecurity personnel, making it challenging to manage an effective MDR strategy.



## Complexity of Threat Landscape

The cyber threat landscape is constantly evolving, with new types of threats emerging all the time. This makes it challenging for organizations to keep up and ensure they're protected against the latest threats.



## Piece-Meal Approach:

Many organizations use a variety of security tools and technologies, which can lead to integration challenges. Without proper consolidation, it's difficult to get a unified view of the organization's security posture and respond to threats effectively. This Disintegrated approach further leads to:-

- SOC teams getting overwhelmed with a large flow of false positives (Alert Fatigue Syndrome).
- Analysts lose time and energy investigating events and non-contextualized alerts.
- Lack of openness to cloud services and modern and hybrid infrastructures.



# Our Solution

HCLTech UMDR service backed by AI-Powered Fusion Platform is specifically designed to address an enterprises' current and future requirements with 24x7x365 coverage. The Modular platform delivers an always on managed detection and response solution that converges security signals across Endpoint, Network, Identity, OT/IoT, Apps and Cloud for automated attack confirmation, enrichment and investigation, triage, and remediation on a single consolidated platform and at no extra cost.

With UMDR, we take the ownership of all incidents through this end-to end AI and automation first platform and advise clients with a single touchpoint for all security needs. This is the crux of the HCLTech UMDR service. Our service is built on a foundation of streamlined processes, deep knowledge, and global presence, ensuring that your business is always protected.



## Deep Knowledge and Expertise

Our team of seasoned experts brings deep knowledge and expertise to your cybersecurity operations.



## Scalability and Predictability

We understand that in the world of cybersecurity, the only constant is change. That's why HCLTech UMDR service is designed to be both scalable and predictable.



## Proactive Detection and Hunting

HCLTech UMDR employs automated and human intelligence-driven hunting techniques for the detection and enrichment of threat signals.



## Streamlined SOC Processes

Our Security Operations Center (SOC) processes are designed to be efficient and effective. We supercharge your security analysts by providing them with the tools and information they need to quickly identify and respond to threats.



## Integration

HCLTech UMDR is designed with an open architecture and interoperability concept for extended visibility. This means it is compatible with almost every leading industry solution.



## Visibility

Our robust eXtended security analytics and response platform centralizes all security signals at cloud scale with the power of an advanced security data lake, providing full visibility across hybrid environments and eliminating blind spots caused by data silos, tool sprawls and cloud shift.



## Open Platform Approach

HCLTech UMDR service is built with the agility and openness of a SaaS ready to integrate and inter-connect with your existing security infrastructure & solutions.



## Cutting-edge Technology

HCLTech UMDR leverage advanced AI/ML capabilities with crafted use cases ensuring efficient threat detection and incident management.



## Global Cyber Security Fusion Centre

Our Global Cyber Security Fusion Centre provides a delivery presence that spans the globe. This ensures that no matter where your business is located, you can benefit from our MDR solution's superior protection.

## Key Features of the HCLTech UMDR Service

- AI & Automation capabilities that deliver comprehensive threat detection, hunting, investigation and response
- Built on HCLTech's proven SecIntAI and powered by HCLTech Collaborative Threat Intel
- Actionable threat insights from HCLTech's Cybersecurity Fusion Center (CSFC)
- Extensive threat visibility with a holistic view across enterprise systems
- Centralized analyst AI-workbench for UMDR Security Analysts to deliver continuous monitoring of all resources, applications, and security tools with real-time situational awareness
- Consolidated platform with advanced capabilities of a data lake, threat intelligence & security analytics platform, automation & orchestration engine and much more



## Value Delivered

Some of the key benefits of our comprehensive HCLTech UMDR service include:

- **6** global Cyber Security Fusion Centers & multiple regional satellite SOCs
- **150+** out of the box & custom developed integrations
- **3X** faster time to customer onboarding
- **200+** enterprise MDR Customers Supported
- **600+** ready to be deployed catalogue of automated playbooks
- **1500+** analysts Skilled in Delivering MDR

Whether you're looking to augment, extend, replace, or build your existing security threat detection and response operations from the ground up, HCLTech's MDR approach can help supercharge your enterprise security.

Contact us today to learn more

To know more, visit: [HCLTech UMDR page](#) or write to us at [Cybersecurity-GRC@hcltech.com](mailto:Cybersecurity-GRC@hcltech.com)

**HCLTech** | Supercharging  
Progress™

[hcltech.com](https://hcltech.com)