Uptycs Managed Detection and Response (MDR) Services

Monitor 1 → Contain 2 → Notify 3 → Recover 4

Uptycs

Customer

A Force Multiplier for Your Security Team

In today's complex and dynamic threat landscape, cyber attacks pose a significant risk to organizations of all sizes and industries. Hackers and cybercriminals are becoming more sophisticated, making traditional security measures less effective against advanced threats. Managed Detection and Response (MDR) services offer proactive threat detection and response capabilities, allowing organizations to identify and mitigate cyber threats before they can cause significant damage.

MDR services extend an organization's security team by bridging the cybersecurity resource gap facing many companies today. Uptycs MDR augments existing capabilities, delivering additional expertise and resources that may not be available in-house. MDR is an ideal solution for companies looking to enhance their cybersecurity posture and reduce risk without expanding their workforce.
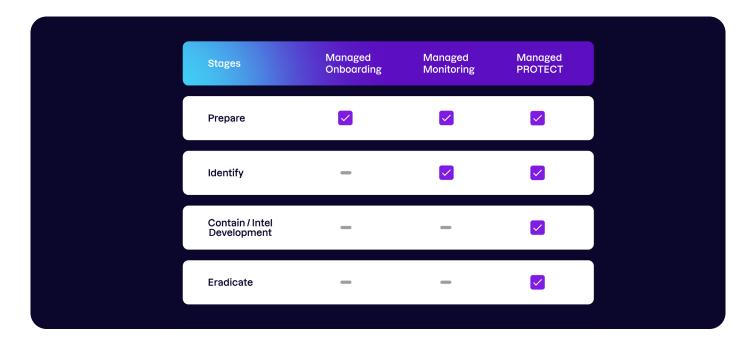
Why Choose Uptycs?

Uptycs is the only vendor in the market today that provides **Managed Detection and Response (MDR)** services for your on-premises, hybrid, and cloud environments, making it the optimal choice for organizations with complicated IT infrastructures. Uptycs' MDR services offer continuous monitoring, incident response, threat hunting, and incident investigation capabilities, ensuring that potential cyber threats are identified and resolved proactively. With Uptycs' MDR, your organization can have peace of mind, knowing that any cybersecurity issues can be promptly identified.

Key Business Benefits

- **Enhanced Security:** MDR offers real-time monitoring and response to threats, preventing data breaches and protecting your company's reputation.

- **Reduced Downtime:** Faster incident response and remediation minimize downtime, boosting productivity and preventing revenue loss.

- **Cost Efficiency:** MDR is a cost-effective alternative to in-house security teams, saving money while strengthening security posture.

- **Compliance Assistance:** MDR helps organizations meet regulatory requirements, avoiding fines and legal repercussions.

- **Customer Trust:** A strong commitment to security boosts customer confidence, attracting new clients and retaining existing ones.

- **Competitive Advantage:** Demonstrating dedication to security differentiates organizations in the market, appealing to customers seeking a secure partner.

Stages	Managed Onboarding	Managed Monitoring	Managed PROTECT
Prepare	☑	☑	☑
Identify	—	☑	☑
Contain / Intel Development	—	—	☑
Eradicate	—	—	☑

Uptycs Managed Detection and Response (MDR) Services Suite

Managed PROTECT

Managed PROTECT is Uptycs' premier MDR service. Fully managed to provide constant surveillance of your cloud and on-premises environments to identify, contain, and eliminate threats. Our expert team does the monitoring and actively contains any threat actors while you tend to the job at hand, ensuring peace of mind.

This service is especially valuable for customers who want expert monitoring and response capabilities to ensure ongoing protection, particularly those who lack the internal expertise to perform incident response and containment actions. With Managed PROTECT, you'll get a range of services tailored to your needs, including:

- **24/7 Monitoring and Response:** Our expert MDR team provides round-the-clock monitoring and quick response to any security incident, ensuring your systems stay protected at all times.

- **Remote Containment of Compromised Systems:** In the event of a security breach, we can remotely contain compromised systems to prevent further damage and minimize the impact on your business.

- **Customized Threat Hunting:** Our Uptycs Global Intelligence Collection enables us to perform customer-specific threat hunting, identifying, and neutralizing potential threats before they can cause harm.

- **Real-Time Reporting:** With our real-time reporting on active threats and high-criticality vulnerable systems, you'll always have a clear picture of your system's security status, allowing you to make informed decisions and take action as needed.

- **Auto-Tuned Detection Rules:** We auto-tune customer-based detection rules to ensure optimal performance and effectiveness, providing you with the most advanced and up-to-date security measures.

Managed Monitoring

Managed Monitoring is designed for customers needing specialized support to monitor and fine-tune the Uptycs platform to work in harmony with their unique environment. Expert staff is readily on-hand to triage detections and offer immediate guidance. It's important to note that Managed Monitoring is not for customers needing an immediate response to an active incident. It only "watches" and "notifies" of suspicious events, without actively responding to them. Services include:

- **Real-Time Threat Monitoring:** Our continuous, real-time threat monitoring provides complete coverage of your attack surface, ensuring your systems stay protected around the clock.
- **Advanced Detection Triage:** Our advanced triage team will use efficient threat identification and prioritization to provide you with the information you need to take immediate action and mitigate potential threats.

- **Customer Notifications:** In the event of high-confidence alerts, we provide customer notifications to ensure you are informed and equipped to take action as needed to protect your business.
- **Instant Vulnerability Alerts:** Our instant alerts notify you of new vulnerabilities, allowing you to stay ahead of emerging threats and proactively secure your systems.

Managed Onboarding

Managed Onboarding is a service designed for customers who've recently purchased Uptycs. This specialized service provides dedicated operational security staff experts in all aspects of Security Operation Center (SOC) and Incident Response activities. This service helps customers develop tailored detections suitable for their specific environment, as all organizations have different security monitoring requirements.

The Uptycs platform offers a full range of detections and alerts to suit customers from all industries, but correct tuning is crucial to quickly identify malicious activity. Managed Onboarding works alongside customers after Uptycs has been rolled out to their systems and before handover to an internal security operations team. Services include:

- **Customer Support:** We provide 60 days of customer support following agent deployment to ensure a smooth transition and address any concerns you may have.
- **Customized Alert Tuning:** Our expert team assists with customized alert tuning to ensure you receive only relevant and actionable alerts that match your business needs.

- **Initial Alert Triage Support:** We provide initial alert triage support to help you prioritize and address potential threats more efficiently.
- **Onboarding and Training:** Our onboarding and training program ensures a seamless transition to Uptycs, empowering you and your team to utilize our real-time threat monitoring and maximize your security posture.

Uptycs Digital Forensic Incident Response (DFIR) Service

Uptycs Digital Forensic Incident Response (DFIR) Service is your trusted partner in fortifying security across on-premises, cloud, or hybrid environments. We work closely with your team to detect, contain, investigate, and eliminate digital threats.

Our robust platform and seasoned experts join forces with your external consultants or internal team, providing unwavering support and collaboration during any incidents your organization encounters. With Uptycs DFIR, you're never alone in the battle against cyber threats – we're in the fight with you every step of the way. Services include:

- **Collaborative Incident Resolution:** Partner with Uptycs' experienced DFIR team, who can collaborate with external consultants or your internal staff to resolve security incidents promptly.

- **Expert-Led Investigation:** Engage Uptycs' DFIR experts to lead incident investigations alongside your internal team, ensuring that critical details are uncovered.

- **End-to-End Incident Response:** Trust Uptycs' dedicated DFIR professionals to manage the entire incident response process from start to finish, responding swiftly and effectively to security breaches.

Future-Proofing: MDR's Key Role in Security

MDR services provide advanced threat detection and response capabilities that many businesses lack due to limited resources or expertise. By leveraging MDR services, organizations can improve their security posture, reduce cyberattack risk, and benefit from specialized expertise and tools. With cost-effective options, MDR services are a wise and affordable investment to bolster your security defenses.

About SRC