

CYBEREASON MDR PACKAGES

Essentials & Complete

KEY BENEFITS

- » Optimize security operations and reduce TCO
- » Faster outcomes with 24x7x365 proactive threat hunting
- » Reduce enterprise security risk and time to response with zero-false positives to you
- » Fully hosted and managed by Cybereason - Active and operational-ready in minutes
- » Flexible offerings providing you and your team the right fit today and the enterprise's future requirements

AT THE FRONTLINE OF DEFENSE

PREVENTING DATA BREACHES

Cybereason MDR Essentials and Complete give your organization 24x7 protection backed by the Cybereason Defense Platform. With Cybereason's superior NGAV, award-winning EDR, and innovative security analytics technology to automate the detection and remediation of threats, Cybereason Defenders are armed with offensive and defensive techniques for a comprehensive defense. The Cybereason MDR team is ready to immediately contain threats, notify your team in the event of a malicious discovery, and provide you with the entire scope of the attack and recommendations to remediate.

24X7 CUSTOMER

FIRST COMMITMENT

The Cybereason MDR team is ready to act, no matter the circumstances. From monitoring to triage, to complete investigation and root cause analysis, to proactive alerting, we are committed to continuously updating you on any high-severity threats. We seek to foster open communication between our customers and our team for co-managed remediation assistance and guided response, collaboration on hunts, and any other questions your team might have.

ZERO FALSE POSITIVES FOR YOU

No one wants yet another alert or unnecessary flood of alerts during a suspicious event, regardless of how actionable it is. The Cybereason MDR approach means attacker's activities are mapped as part of a campaign and consolidated into a single Malop (Malicious Operation). Malops elevate alerting to a high-fidelity, context-rich description of an incident across all steps of MITRE ATT&CK. As part of Cybereason MDR's vigilant threat hunting, high severity Malops are handled first and fast. For every Malop generated, automatically or via 24x7 proactive hunting, a recommendation for immediate containment and threat remediation is either provided or applied on your behalf.

PUT CYBEREASON MDR TO THE TEST

[CYBEREASON.COM/MDR](https://cybereason.com/mdr) →

NEVER COMPROMISE

TAKE CONTROL

For every new piece of evidence identified and every Malop created, Cybereason Defenders provide a detailed investigation to identify compromised endpoints across all your enterprise-wide environment. Armed with the full scope of the malicious operation (Malop), a response recommendation to contain and eliminate the threat is provided or performed for you within minutes to hours, regardless of the organization's location.

FLEXIBLE OFFERINGS THAT BEST FIT YOUR SECURITY OPERATIONS

CYBEREASON MDR PACKAGES

» 24X7 TRIAGE & MONITORING

Augment your security team at any level to scope cyberattacks and accelerate detection and investigation activities for every potential threat across all endpoints. Enable your team to focus on further progressing the organization's security operations program. With SOCs in the United States, Israel, and Japan, Cybereason MDR provides an around-the-clock follow the sun model and 24x7x365 support to identify the most critical threats and respond immediately.

» AUTOMATED THREAT HUNTING

Harness cross-domain defensive and offensive security expertise infused with superior technology. Identify Indicators of Behavior (IOB), perform threat hunting, and get visibility into all endpoints, all users, all communications, all MITRE ATT&CK techniques, and most important, the complete compromise root cause.

» CONTEXTUAL NOTIFICATIONS

The Cybereason MDR Defenders provide you with notifications of threats prioritized by severity and enriched with the right context for remediation. Further, you control all of this within the Cybereason Defense Platform for ongoing communications and later audit use.

» DETAILED RESPONSE RECOMMENDATIONS

For every new Malop the Cybereason MDR team will provide you with the complete root cause investigation and a definite response recommendation for compromise containment.

CYBEREASON

MDR ESSENTIALS

- ✓ AUTOMATED THREAT HUNTING
- ✓ PROACTIVE EMAIL ALERTS
- ✓ DETAILED RESPONSE RECOMMENDATIONS
- ✓ MALOP ROOT CAUSE INVESTIGATION
- ✓ THREAT FINDINGS & STATE-OF-SERVICE REPORT
- ✓ CROSS-DOMAIN DEFENDERS EXPERTISE
- ✓ PROACTIVE PHONE NOTIFICATION FOR CRITICAL MALOPS
- ✓ PRE-NEGOTIATED REMOTE INCIDENT RESPONSE RETAINER

CYBEREASON

MDR COMPLETE

+ EVERYTHING INCLUDED IN ESSENTIALS

- ✓ ACCESS TO CYBEREASON DEFENDERS
- ✓ PROACTIVE TUNING & CONFIGURATIONS
- ✓ PREMIUM ONBOARDING
- ✓ NGAV PREVENTION ANALYSIS
- ✓ 24X7 PROACTIVE THREAT HUNTING
- ✓ ACTIVE RESPONSE & GUIDED COMPROMISE CONTAINMENT
- ✓ CRITICAL MALOP REPORT
- ✓ THREAT INTELLIGENCE REPORT
- ✓ PRE-NEGOTIATED REMOTE INCIDENT RESPONSE RETAINER

PUT CYBEREASON MDR TO THE TEST

[CYBEREASON.COM/MDR](https://cybereason.com/mdr) →

» PROACTIVE THREAT HUNTING

Proactively hunt for hidden adversaries using Cybereason technology, analytical expertise, and intelligence. Our team will apply 200+ hunting IOB techniques daily to uncover outlier anomalous activity, continually assess your data, and ensure you do not miss a threat.

» GUIDED & ACTIVE RESPONSE

The Cybereason Defenders will work directly with you and for you 24x7, to stop all threats. Cybereason MDR orchestrates response actions automatically or per request to isolate endpoints, block malicious persistent modules identified as root-cause, and prevent lateral movement.

» DIRECT ACCESS TO CYBEREASON DEFENDERS

For every question, Cybereason Defenders are ready to help with the right guidance.

» DETAILED THREAT, MALOP, & INTELLIGENCE REPORTS

The Cybereason MDR team will keep you apprised of your security posture with monthly cadence threat reports, detailed high-severity Malop reports, and a quarterly threat intelligence report for ongoing intel on the worldwide threat landscape, new research, and attacker techniques.

» PRE-NEGOTIATED REMOTE INCIDENT RESPONSE RETAINER

With no upfront commitment or cost, Cybereason includes a remote Incident Response Retainer. Get direct access to our experts when you need it the most.