COMODO

MDR 101

200 Broadacres Dr,
Bloomfield, NJ 07003

Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000

www.comodo.com
platform.comodo.com

What is Dragon MDR?

Leading analyst firm, Gartner defines Managed Detection and Response (MDR) as the process of providing real-time detection, analysis, investigations, and active response, all delivered remotely through a security operations center (SOC) type of function on a 24x7x365 basis.When set up with precision, insights, and experience, MDR can truly function as a dynamic extension of your wider security foundations. But **not all managed detection and response services are built the same**.

Dragon MDR provides a variety of supplementary benefits and becomes critical for organizations with limited or almost no resources dedicated to proactively monitoring, securing, and responding (even hunting) for **known and unknown threats**.

Complete Threat Prevention

Protection with patented Auto Containment technology is the world's only active breach protection that stops ransomware, malware, or cyber-attacks from causing damage. This allows protection of the systems without having to rely on detection of any sort.

Real-Time Forensics and Behavioral Analysis

Proactive in-built capability for endpoint detection and response-level forensics that offers continuous visibility and insight into the applications and processes running in your environment. Enabling you to rapidly detect threats before they become breaches, reducing dwell time and gaining a full understanding of the means, methods and root cause associated with suspicious activity and/or malware.

Dragon MDR has been built around these four foundational pillars.

Hunting-on-the-go:
Comodo's highly skilled team of security specialists are dedicated to continuously hunting for anomalies suspicious activity and threats across your organization's endpoints, network, and cloud environments.

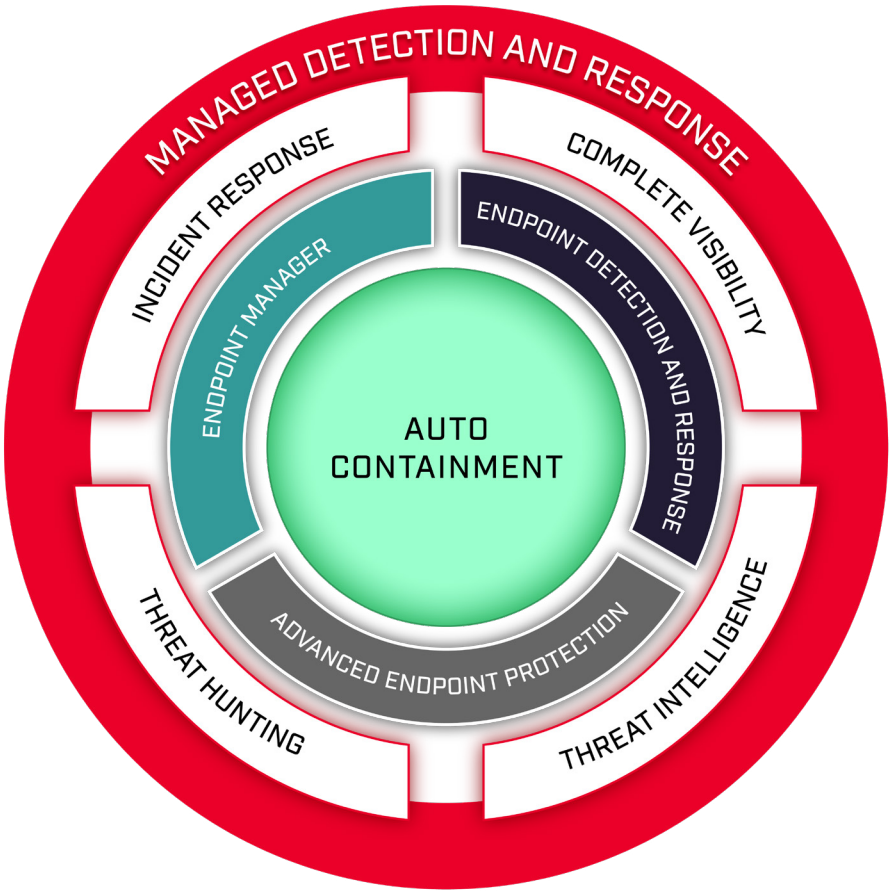
Full visibility with real-time alerting:
Routed to our state-of-the-art Dragon Platform, triaged events, alerts, and harmful behavior can be presented and addressed quickly.

Incident Response:
Leverage a team of highly skilled forensic analysts to conduct in-depth investigations. Receive a detailed timeline of attack activity derived from endpoint forensics. Includes analysis of artifacts such as MFT$, Windows Event Logs, Registry, Web History, etc.

Unification of threat intelligence:
Double-down on numerous internal and external threat intelligence feeds, providing wide coverage of threat data that contributes to halts and alerts on Indicators of Compromise (IoC).

How Dragon MDR Works

The illustration highlights the tightly integrated nature of Dragon MDR, combining the appropriate technology, people, and processes that the mid-market can gain from.



Deploy

Become efficient and operational in hours from deployment

Detect

Hunt and track down high priority threats, payloads and signatures across all endpoints

Triage

Tailored endpoint security rules and logic determine the risk severity **while auto containment prevents any malware damage in real-time**

Remediate

Patented auto containment stops the damage, but our security experts need to clean up and patch any loose issues to remediate the endpoints

Report

Receive a detailed breakdown of every incident for compliance and on a regular cadence to understand your environment's enhanced managed security.

Why you need Dragon MDR

1. Security has never been a process of setting and forgetting, even in the days when attacks were sporadic. In the modern era, where attack intensity has increased dramatically, it becomes even more important to stay ahead of the bad guys. However, there are certain realities that organizations must grasp before engaging in a truly managed detection and response initiative.

2. **Growing Threat Landscape:** Threats and attacks alike have become more advanced and increasing at an alarming rate. Ransomware attacks such Colonial Pipeline and JBS Foods are just a few examples of notable-size organizations that have suffered first-hand. Organizations, regardless of size are highly likely to experience an attack or breach, and it is a matter of when it will happen, not if it will happen.

3. **Limited Person-Power:** There are no shortcuts that can be taken to ensure an elevated level of dedicated security measures. You know your business and your customers better than anyone. Similarly, an MDR provider also knows its strengths in this line of business. With the lack of dedicated security expertise that may be present with your organization, partnering with an experienced MDR provider ought to become a must-have, not a nice to have.

4. **Time and Cost:** When deciding to undertake the mundane process of building an internal team for your holistic security or committed teams for incident response or threat hunting, the time and cost required can be significant. By allowing you to focus on your business needs, a dedicated MDR provider can focus their efforts entirely on analyzing events, conducting investigations and round-the-clock monitoring.

5. **Critical business value:** With MDR-type services that include continuous monitoring and remediation guidance, organizations are provided with a level of comfort that their employees, IP, and infrastructure are at a lower risk to threats, which subsequently helps to boost business productivity.

Business Benefits

- Real-time monitoring and alerting for suspicious activity
- Advanced Endpoint Protection using our 'Auto-Containment' technology to identify knowns, unknowns and reduce the attack surface
- Real-time aggregation and correlation of telemetry sensor data for endpoints
- Security event / alert management
- Endpoint management
- Incident response management and investigation
- Leverage Comodo's dedicated SOC analysts for responding to threats
- Managed hunting capabilities to recurrently to expose and pinpoint threats
- Advanced analytics highlighting file, user, and endpoint data
- 24x7 SOC support through numerous geographical centers

About Comodo

Headquartered in Bloomfield, NJ, Comodo's mission is to help customers avoid breaches with groundbreaking isolation technology that fully neutralizes ransomware, zero-day malware, and cyber-attacks that other security providers can't do. We deliver active breach prevention with patented auto containment technology. Our Unified Endpoint integrates this technology with critical components like our highly rated advanced endpoint protection, endpoint detection and response, and endpoint management to offer a single cloud-accessible Active Breach Protection solution. Comodo's SOC as a Service team makes the solution a frictionless, high-security implementation. For more information, visit https://www.comodo.com/.

ACTIVE BREACH PROTECTION FOR YOUR BUSINESS

Comodo provides Active Breach Protection in a single platform. No one can stop 100% of threats from entering their network so Comodo takes a different approach to prevent breaches.

Experienced intrusion? Contact us at 1 (888) 551-1531
Visit comodo.com for your free 30-day trial

200 Broadacres Dr,
Bloomfield, NJ 07003

Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000

www.comodo.com
platform.comodo.com