COMODO

DRAGON MDR

Solution Brief

200 Broadacres Dr,
Bloomfield, NJ 07003

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

www.comodo.com
platform.comodo.com

COMPREHENSIVE CYBERSECURITY AND REGULATORY COMPLIANCE AT AN AFFORDABLE COST

Growing numbers of more sophisticated cybersecurity attacks threaten your web applications, cloud infrastructure, networks, and endpoints. Failure to protect these resources will trigger costly penalties once a data breach occurs to your business.

Your best defense is a "defense-in-depth" strategy with multiple layers of cybersecurity protections. This approach requires technical experts who are knowledgeable across many security domains. But these days, demand for cybersecurity skills far surpass supply. Skilled resources have become too costly for many small-to-medium-sized, and even some larger, organizations.

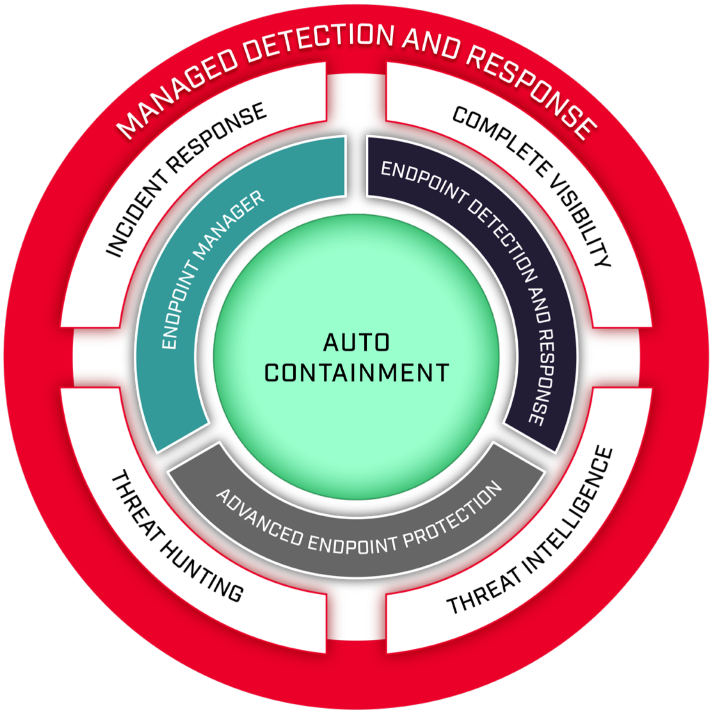
Dragon Managed Detection & Response (MDR) Solution delivers comprehensive cybersecurity protection at a price you can afford. Better still, our service frees your IT team to focus on strategic priorities with peace of mind, knowing your systems are defended from advanced threats.

DELIVERING PEOPLE, PROCESS, AND TECHNOLOGY

Dragon MDR is a 24/7 Security Operations Center delivered as a Service (SOCaaS). Our service provides a team of security analysts who extend your IT team to safeguard your IT systems and infrastructure.

Comodo works closely with your existing IT team to prioritize incidents, fix security flaws, and remediate issues. Our Global SOC and Threat Lab teams are comprised of analysts along with security experts hunting for vulnerabilities, continuously monitor your IT systems for indications of compromise, and contain advanced threats. These industry experts leverage Comodo's state-of-the-art SIEM, EDR, and Threat Intelligence to continuously manage, maintain, and patch your environment through our Endpoint Manager.

How Dragon MDR Works



DISCOVERY

Security analysts continuously monitor and report on your endpoint and network using AEP (Advanced Endpoint Protection) & our state-of-the-art Intrusion Detection System (IDS) via sensors. The Comodo IDS monitors your network traffic for any malicious activities or policy violations that may ultimately lead to a full-scale attack.

THREAT HUNTING

Security analysts leverage their extensive years of experience to apply active cyber defense methods. These involve proactively searching client networks to identify vulnerabilities and potential threats in your network, that have previously gone undetected. Comodo threat hunters do not simply sit back and wait for correlation rules to alert. Our proactive approach to threat hunting recognizes that threats can still try to evade in-place security measures.

MANAGED RESPONSE

As a fully managed solution, our analysts conduct endpoint and network analysis, through the mechanisms of installation, fine-tuning, and deploying the appropriate custom security configuration and measures for each client. Comodo response entails continuous alerting, reporting and remediation of security events. Additional steps for managing incidents from identification to threat mitigation.

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.

Dragon MDR Benefits

Remediation

If an incident occurs, IT and security teams may find themselves scrambling to remediate the issue. Taking them away from high priority projects.
Comodo's Advanced SOC Analysts:

- Focus on incident severity and advanced threat outcomes
- Deliver actionable remediation guides and detailed response plans

Compliance

Regulations such as GDPR, the California Consumer Privacy Act, and SOX impose hefty penalties for security breaches that threaten data privacy.

- Privacy standards like GDPR, HIPAA, and PCI
- Security standards like ISO 27001, PCI, SOC and NIST CSF

Reduced Costs

Managing endpoints and networks is costly in terms of staff, technology solutions, and time spent. Many solutions for outsourcing these functions are also tremendously expensive.
Comodo's Pricing Plans:

- Package licenses and services into one annual fee
- Plans cost to be affordable for small-medium-sized businesses

Minimal Complexity

Managing defense in-depth solutions is challenging. IT often administers multiple solutions from different vendors. Many solutions lack integration. Dragon MDR simplifies cybersecurity management with:

- One-pane-of-glass integration with Comodo technology
- Network / Cloud + Endpoint + Web protection supported by 3 tiers of analysts

Identify Threats

The number of sophisticated cybersecurity threats is increasing exponentially. MDR provides proactive threat hunting that delivers:

- The ability to identify known and unknown file
- Ongoing threat hunting to detect & find weaknesses

On Demand Experts

IT organizations face a growing shortage of cybersecurity experts. Comodo's Managed Detection & Response delivers security experts on-demand:

- We provide Tier 1 through 3 analysts on a 24 / 7 global basis
- We train and provide skilled "watchers" for your organization

Features

Global Security Experts

Cloud-based Security Operations Center (SOCaaS) with a global footprint on delivery to keep your network healthy and secure

Efficient Incident Service

Utilize a team of highly trained forensic analysts to conduct in-depth investigations that highlight attack timelines

Pre-Emptive Auto Containment

Patented auto-containment technology to stop malware threats with surgical precision by denying malicious activity while still allowing systems to operate

Powerful Threat Hunting

Extensive threat scanning platform,data visualization and analysis, statistical correlations, and data pivoting are among the supported techniques

Cloud Based SOC As-A-Service

No capital expenditure, no license, and no infrastructure to buy, designed particularly for threat detection and response automation

Threat Intelligence Feeds

Comprehensive, multi-sourced collection of threat intelligence from internal and external feeds, with the ability to incorporate your organization's intelligence for extra coverage

About Comodo

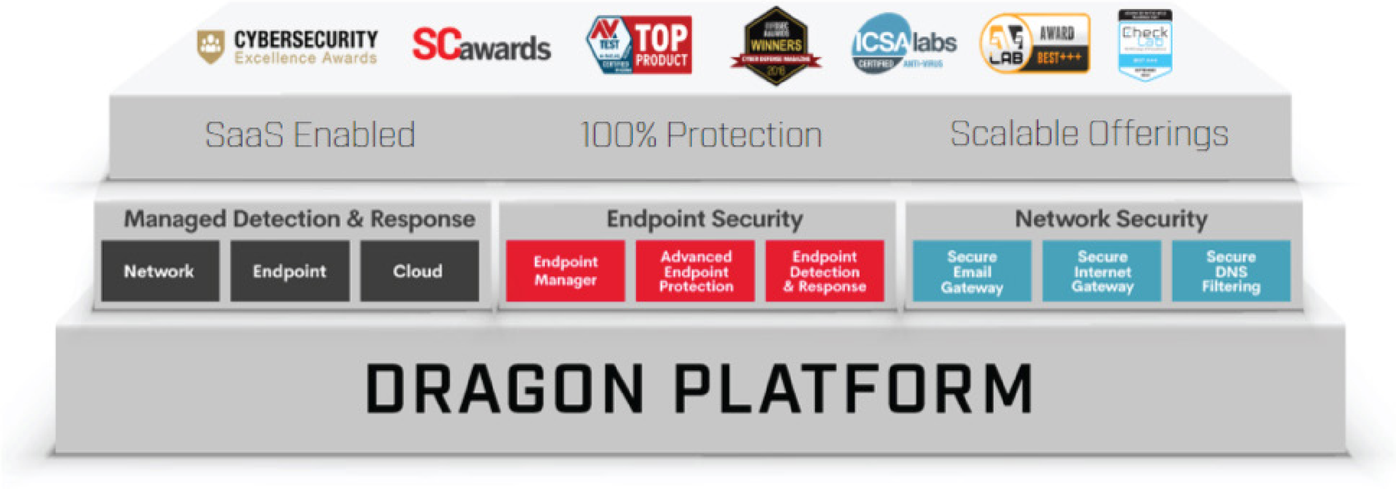
Comodo is the world's leader of next-generation open-source cybersecurity, with the industry's most disruptive innovations.

We help customers stop breaches with groundbreaking isolation technology that neutralizes ransomware, malware and cyber-attacks. Our complete cloud-native framework delivers a zero-trust architecture with active breach protection for the most comprehensive defense against zero-day threats. Comodo's cybersecurity products maximize intelligent sharing between every component of the platform, therefore providing superior security. We are the only company that analyzes and gives a trusted verdict for 100% of files on a network.

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