



Protect Your Network with Fully Managed Remote Resources

# MANAGED DETECTION & RESPONSE



## 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.

Comodo Cybersecurity’s 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.

## CSOC

### DELIVERING PEOPLE, PROCESS, AND TECHNOLOGY

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

Using Comodo SIEM and endpoint management technologies along with threat intelligence from the Comodo Threat Lab, our security experts hunt for vulnerabilities, continuously monitor your IT systems for indications of compromise, and contain advanced threats. We work closely with your IT team to prioritize and fix security flaws and remediate issues.

CSOC  
DETECT & FIND



CSOC  
THREAT HUNTING



CSOC  
MANAGED RESPONSE





## HOW COMODO MDR WORKS

### EVENTS AND INCIDENTS REMEDIATED FOR YOU

All components work in tandem to deliver your IT staff and administration the reports and remediation needed to handle every incident in the most effective manner

#### ON PREMISE SENSORS

Collect data from network logs, Active Directory, firewalls, and etc



#### DEFENSE-IN-DEPTH

Set correlation rules, alerting, configuration, risk monitoring, audits, threat intelligence

#### CLOUD CONNECTOR MONITORING

User activity, apps, data, infrastructure activity



#### DETECT & FIND

Our fully managed security starts with the Comodo Intrusion Detection System (IDS) via sensors. Security analysts continuously monitor your endpoints and network for malicious activities or policy violations that can lead to intrusions and the attacker's kill-chain. Artificial intelligence technologies within the Comodo SIEM aid the analysts in detecting compromises to stop them early in this progression.



#### THREAT HUNTING

Analysts use their experience to apply active cyber defense methods. These involve proactively searching client networks to detect threats that are resident in your network to yet be undetected. Threat hunting does not simply wait for correlation rules to alert. Our proactive nature of threat hunting recognizes that threats can still try to evade in-place security protections.



#### MANAGED RESPONSE

The solution is managed meaning that our analysts take the endpoint and network protections through the process of installation, tuning, learning and putting the defenses in place for the client system in the correct configuration. Managed also means maintaining the state with the addition of endpoints or the collection of other logs. The Response is the alerting and reporting, remediation of events or managing incidents through to resolution.



## MDR FEATURES

### OFF-SITE SECURITY EXPERTS

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

### ASSISTED MACHINE LEARNING

First AI designed specifically for MDR needs : Semi-supervised learning technology where AI learns from human security analyst decisions

### PRE-EMPTIVE AUTO CONTAINMENT

Patented 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

World's largest collection of threat intel. Multi-Sourced Integrated Security Intelligence from internal indicators and global external threats

## 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 Security Agents:

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



### LESS COMPLEXITY

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

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



### COMPLIANCE

Regulations such as GDPR, the California Consumer Privacy Act, HIPAA, 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



### IDENTIFY THREATS

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

- 100 million endpoints that find known and unknown files
- Ongoing threat hunting to detect & find weaknesses



### LOWER 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



### ON DEMAND EXPERTS

IT organizations face a growing shortage of cybersecurity experts. Comodo Cybersecurity'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

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. Comodo Cybersecurity has experts and analysts in 193 countries, protects 85 million endpoints and serves 200,000 customers globally. Based in Clifton, New Jersey, the company has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide. For more info, visit [comodo.com](http://comodo.com) or our blog. You can also follow us on Twitter (@ComodoDesktop) and LinkedIn.



## 200K SECURED CUSTOMERS

Delivering reliable, centralized, and fully scalable security solutions for today's business.

## 85 MILLION ENDPOINTS INSTALLED

With tens of billions of OS-VMs created in over 85 million endpoint installations, not a single infection!

## 193 COUNTRIES WORLDWIDE


Over 850 cybersecurity scientists and engineers analyzing 100,000 threats per day and reaching definitive verdicts around the world.

### **MDR** MANAGED DETECTION & RESPONSE



**SCHEDULE YOUR DEMO**



 For demo, pricing and other customer requests:  
**[sales@comodo.com](mailto:sales@comodo.com)**

For ISV and referral partners:  
**[channeloperations@comodo.com](mailto:channeloperations@comodo.com)**

For help and support inquires:  
**[c1-support@comodo.com](mailto:c1-support@comodo.com)**



**US and Canada**  
+1-888-551-1531  
+1-877-712-1309



**Headquarters**  
+1-973-859-4000

**Fax Line**

+1-973-777-4394