COMODO
CYBERSECURITY

2019

SECURITY AS A SERVICE

PROTECT YOUR NETWORK WITH REMOTE RESOURCES

MDR MANAGED DETECTION & RESPONSE

SECURITY AS A SERVICE

COMODO CYBERSECURITY

PROTECT YOUR NETWORK WITH REMOTE RESOURCES

Sales: + 1(888) 551-1531 Visit mdr.comodo.com

COMPREHENSIVE CYBERSECURITY AND REGULATORY COMPLIANCE AT AN AFFORDABLE COST

Your organization faces cybersecurity threats to your web applications, cloud infrastructure, networks, and endpoints that keep increasing in velocity, volume and sophistication. At the same time, growing numbers of regulations impose stiff penalties for data security breaches.

Addressing these challenges requires multiple layers of cybersecurity solutions from many vendors—along with experts knowledgeable in multiple security domains to integrate and manage these solutions. Yet with demand for cybersecurity skills far outstripping supply, rising costs have rendered skilled resources unaffordable for small-to-medium-sized and even some larger organizations.

Comodo Cybersecurity's Managed Detection & Response Solution delivers the comprehensive cybersecurity protection your organization demands with the appropriate controls to meet regulatory demands at an economical price. Our solution frees your internal IT organization to focus on strategic priorities while having peace of mind of knowing your systems are protected from advanced threat actors.

DELIVERING PEOPLE, PROCESS, AND TECHNOLOGY

Comodo MDR is a 24/7 Security Operations Center delivered as a Service (SOCaaS). Our SOCaaS provides a team of security researchers who extend your IT organization 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 with your IT team to prioritize security flaws and remediate issues.

MDR MANAGED DETECTION & RESPONSE

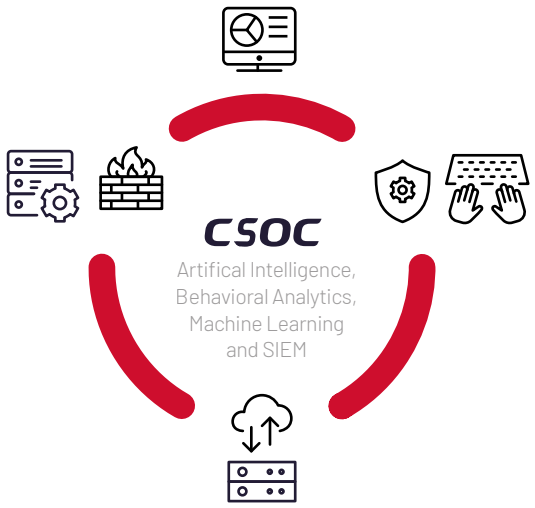
HOW COMODO MANAGED DETECTION & RESPONSE WORKS

INCIDENTS AND EVENT REPORTS DELIVERED TO YOU

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

ON PREMISE SENSORS

Collects Network Flow of Log Data, Active Directory, Firewalls, etc...



GLOBAL OPS TEAM

Security Engineers, SOC Analysts for 24 / 7 incident responses

VIRTUAL SENSORS FOR CLOUD MONITORING

User activity, apps, data, infrastructure activity

Microsoft Azure · amazon web services · salesforce · G Suite · Office 365 · box

DETECT

Sensors continuously monitor your network and systems for malicious activities or policy violations that can lead to network intrusions. Artificial intelligence within the Comodo SIEM combines correlation rules our Threat Lab develops for known attacks with rules customized for your environment to proactively alert our SOC to any possible endpoint compromise.

INVESTIGATE

Dedicated incident response analysts within the Comodo SOC continuously monitor your environment. Three tiers of analysts investigate any incidents by integrating relevant networking log and security sensor events, correlating, analyzing, and enriching data as necessary. They then evaluate the impact of the incident on the customer's environment and develop a detailed incident response plan.

RESPOND

Our service automatically generates timely and meaningful alerts based on your infrastructure requirements. Your IT team no longer needs to undergo the arduous process of defining custom rules, queries or reports. Our analysts give your internal team collected logs and reports to help them evaluate any events and manage remediation for any attacks.

SECURITY AS A SERVICE

COMODO CYBERSECURITY

PROTECT YOUR NETWORK WITH REMOTE RESOURCES

Sales: + 1(888) 551-1531 Visit mdr.comodo.com

MDR FEATURES

- SOC performs continuous 24 / 7 / 365 monitoring, threat hunting and investigation to proactively detect and resolve incidents or quickly remediate attacks.
- Security experts evaluate incident severity, create tailored alert reports, investigate advanced threats, deliver actionable remediation guides, and provide hands-on remediation support.
- Passive sensors (mirror port / hub or tap), on-premises network sensors (physical or virtual), and other vectors (DNS traffic, NetFlow data) collect data about your network, endpoints, cloud and web applications.
- MDR collects data from agents on endpoints and cross references it against threat intelligence from Comodo Threat Laboratories. Violations of recommended security policies trigger alerts.
- Artificial intelligence within our SIEM automates the analysis and correlation of events, alerts and network data to identify advanced attacks and minimize false positives.
- Proactive threat hunting identifies advanced persistent threats and zero-day threats in your network and devices.
- Customizable admin portal gives Comodo security experts and customers a single pane-of-glass interface to provision, deprovision and manage endpoints, perform network configuration, access cloud-based security and event management information, and create reports.
- Client-specific SLAs provide tiered notifications for alerts and support for incident response.
- Weekly summary and monthly service reports tailored for customers.

MDR BENEFITS

REMEDIATION

If an incident occurs, IT and security teams often find themselves scrambling to remediate the issue, which takes them away from high priority projects. Our advanced security agents:

- Focused on incident severity and advanced threat outcomes
- Actionable remediation guides and detailed response plans

COMPLIANCE

Regulations like GDPR, the California Consumer Privacy Act, HIPPA, SOX and more impose hefty penalties for security breaches that threaten data privacy. MDR delivers controls that simplify compliance with:

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

REDUCE COSTS

Managing endpoints and networks is costly in terms of staff, technology solutions, and time while many solutions for outsourcing these functions are also tremendously expensive. cWatch MDR:

- Packages licenses and services into one annual fee
- Designs costs to be affordable for small-medium-sized businesses

CUT COMPLEXITY

Managing defense in-depth solutions is challenging. IT must administer multiple solutions from different vendors. Many solutions lack integration. Some solutions generate many false positives masking events that turn out to be costly incidents. MDR simplifies cybersecurity management with:

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

MINIMIZE CYBERSECURITY 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 (zero day) malware files
- Ongoing scenario-based threat hunting to find weaknesses to external threat intel

SECURITY EXPERTS ON DEMANDS

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 by 7 global basis
- We train and provide skilled "watchers" for your organization

COMODO
CYBERSECURITY

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 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.

DIRECTORY

For demo, pricing and other customer requests:
sales@comodo.com

For ISV and referral partners:
channeloperations@comodo.com

For help and support inquires:
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

MDR MANAGED DETECTION & RESPONSE

SCHEDULE YOUR DEMO

Sales: + 1(888) 551-1531