
# Comodo MDR:

# Protect Endpoint Services

## Scope and Statement of Work

# 1. Comodo Overview

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats harmless, across the LAN, web and cloud. The Comodo One platform enables customers to protect systems and data against even military-grade threats, including zero-day attacks. 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.

# 2. Management Summary

Comodo Cybersecurity provides managed security services that help companies to enhance operational management of enterprise security. These services are managed by a center of excellence where expertise and technology converge and are placed at the service of Comodo customers.

The Security Operation Center (SOC) is the core operational unit of Comodo Managed Security Solutions, dedicated to provision of services to customers. Its main task is to provide the ability toanalyze information and identify potential risks and/or intrusion attempts, as well as respond promptly to security incidents. An SOC also provides the tools necessary to measure performance of systems dedicated to security and to assess the level of risk/exposure to the company. An SOC can also provide Incident Response and manage information sharing with Computer Emergency ResponseTeams (CERTS). The provided services as given below.

- **Management:** All management activities related to Comodo security products targeting IT infrastructure (network, systems and applications) and the functionality of the systems are consolidated in the SOC.
- **Monitoring:** IT infrastructure and security are monitored in real time to quickly identify intrusion attempts, attack or misuse of systems.
- **Incident Response**: A team of specialists in collaboration with the customer identifies the best possible approach to mitigate an ongoing attack (incident handling, DDoS mitigation, crisis team).
- **Proactive Services:** services aimed at improving the security level of the organization (risk evaluation, security assessment, early warning, security awareness, event correlation).

The common services and scenarios are:

a. Protect Endpoint Services
b. Incident Monitoring, Handling and Response
c. Malware Analysis and Fraud Services
d. Threat Management and Intelligence
e. Log Management and Event Correlation

The Comodo SOC is comprised of teams located in the USA, Turkey, Ukraine and India. The Comodo SOC operates 24x7 and provides uninterrupted service delivery.

## 3. Protect Endpoint Service

Protect Endpoint Service offers the maximum in data security for Comodo Cybersecurity customers. In addition to award-winning advanced endpoint protection for Windows, MacOS, Linux and mobile clients, Protect Endpoint Service includes comprehensive group policy management to ensure adherence to your corporate guidelines and policies, even in complex networks.

**Scope**: Endpoint installation and management of Comodo AEP technologies such as

- Endpoint Monitoring
- Alerting
- Remote Access
- Mobile Security Management
- Anti-malware / Antivirus
- Application Control
- Personal Firewall
- Behavioral Monitoring
- Memory Protection
- Endpoint Detection and Remediation
- Application Sandboxing (Valkyrie)

**Description**: This service provides complete management of endpoint security requirements covering preventive measures, related working practices, policies, procedures, and evaluation risk.

Endpoint Security Management included with the Comodo service is comprised of the following lineitems:

- Creation and application of granular policies, based on users, locations, departments
- Troubleshooting and resolution of issues affecting the operation of Comodo advanced endpoint protection software.

- Upgrade, patching, configuration, and optimization of Comodo AEP (advanced endpoint protection) software
- Central monitoring of all endpoints enrolled in ITSM (IT Security Manager) with respect to Antivirus & Patch management solutions.
- Profiling in ITSM based on specifics customer requirements.
- Containment and remediation of suspicious hosts on demand.
- Live remote inspection capability on a host, including grabbing suspicious files for analysis.
- Tuning of monitoring rules for reduction of false positives.
- Analysis and reporting of unrecognized files submitted by customer.
- Monitoring of threat status and Malware Alerts triggered from endpoints as monitored under ITSM
- Incident Notification sent to the customer via Service desk
- File verdicting using Valkyrie to identify submitted files as malicious or benign.
- Active monitoring of endpoint logs for suspicious activity.
- Troubleshooting and resolution of operating system, application-level and network connectivity issues if caused by Comodo advanced endpoint protection
- Management false positives in malware detection
- Provision of forensic analysis upon request and/or post incident
- Bi-weekly (every two weeks) Anti-virus / ITSM agent patch update Status reporting
- Tri-weekly (every three weeks) Endpoint Compliance reporting

For clarity, customer responsibilities include

- Installation or configuration of any software or hardware other than Comodo product
- Configuration and applying OS-level patches
- Networking problems

Should infrastructure and network, cloud or otherwise not be under the control of the MSP / MSSP

## 4. Service Hours and Receipt of Service Requests:

Service will be provided as a “service desk” via telephone or email from 8:00 am-6:00 pm local time (extended business hours) or via the Comodo online service desk application https://one.comodo.com/service-desk/.

| | LOW | NORMAL | HIGH |
|---|---|---|---|
| **Priority Description** | Interruption to the work of individual users and/or an acceptable work-around is available | Interruption to critical processes affecting individual users with no acceptable work around is available | Interruption to critical business processes affecting many users with no acceptable work-around available |
| **90% must be assigned within** | 8 hours | 2 hour | 1 hour |
| **And resolved within** | 2 days | 24 Hours | 8 hours |

**Security Incidents:**

The service will be supported by the Security Operation Center 24x7x365. When incidents are detected, the SOC uses the following matrix to determine actions post analysis. Analysis results will conclude that either the alert is a False Positive, Suspicious, High Probability or Proven. The alert will only escalate to an incident if the corresponding action is “Record” or higher.

| | Suspicious | High Probability | Proven |
|---|---|---|---|
| Critical | Record | Notify | Escalate Call |
| Major | Increase Risk Level | Record | Notify |
| Medium | No Action | Increase Risk Level | Record |

All Escalate Calls are regarded as High Priority Tickets for service requests. If required, advanced forensic analysis will be performed. Notification will be accomplished via email. All notify events areregarded as Normal Priority Tickets.