COMODO

24/7 Managed Detection & Response

Security Ops Center as a Platform

Transition your organization's security methodology from detection-based security products to the latest in prevention-based solutions. Our SOC as a Platform delivers zero-trust security prevention at the endpoint level with minimal impact to your organization's user productivity.

No minimum quantities, pay in arrears

No lock-in, simply month by month subscription

Deliver full SOC in 24 hours with ZERO upfront investment

Security Operations Center as a Platform:
24/7 Managed Detection, Response and Remediation
[Code Name // SOCaaP]

The world's first SOC-as-a-Platform that combines people, process, and technology to deliver a completely outsourced SOC with remediation at the endpoint for less than most EDR and MDR products. Comodo SOCaaP is fully managed by our industry certified security experts around the clock. Whose collective goal is to reduce attacker dwell time from hours, days, weeks or even months to just seconds and stop attacks against protected endpoints. The service is a fully managed defense-in-depth for the prescribed features. Event processing/remediation of external threat intelligence is included. This provides the client with visibility to threats that are within their own horizon (the IOCs) and for those threats that exist in the external horizon (the external threat). **This package includes detect, protect and remediation.**

These services involve the security analysts in a series of features to perform a deeper analysis of the detected events and when required to working with the client to remediate the detected events or incidents. This is licensed as the number of workstations being managed by the Comodo SOC team includes expanded Global SOC services to detect and resolve the IOCs within the endpoints.

200 Broadacres,
Bloomfield, NJ 07003

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

www.comodo.com
platform.comodo.com

Pre-Emptive Containment Management - Patented containment technology to pre-emptively stop threats with surgical precision by denying malicious activity while still allowing systems to operate. Unknown files are executed in containers and by no means hold a threat because their access is limited until they are given a good verdict.

Application Profiling (AI Support) - Based on normalization techniques and time series models, SOCaaP provides user-application related baselining which allows our SOC analysts to detect anomalous process behaviour likely to be caused by attacks such as memory exploits and file-less attacks. This covers one of the major modern-day attack types in which trusted applications legitimately serve for adversaries and yet not get caught by legacy AV solutions. Security Policy Management - SOCaaP comes with the Comodo recommended Security Policy, which is customizable to meet your individual needs. Our engineering team is available to work with you to tailor the policy around your requirements. The recommended policy covers behaviour-based alerts, which notify you about activities such as file-less attacks, advanced persistent threats (APTs), and privilege escalation attempts.

Proactive Threat Hunting (APTs, Lateral Movements, Suspicious Behaviors, ...) - SOCaaP provides security analysts with a suite of powerful tools to provide earlier detection, reduce dwell time, and improve defenses for future attacks.

Detect APT - The top benefits organizations derive from threat hunting include improved detection of advanced threats, followed closely by reduced investigation time, and saved time not having to manually correlate events.

Process Analysis Examination - SOCaaP excels at providing analysts actionable knowledge over the process hierarchies. Process hierarchies are given in tree structure and timeline view both providing all process-related events at a sequence and context. Endpoint MDR also provides details about any hash seen in the environment, including execution history, download summary, creation summary, execution trend, and basic attributes of the hash. File trajectory is also provided to show the hash's incidents as well as the alerts created by the hash and Valkyrie verdict.

Threat Validation from analysts - SOCaaP solves the alert fatigue problem, which is as dangerous as the attack itself, with its auto investigation and analyst threat validations. Our SOC experts perform well-defined alert triaging which leaves no room for unvalidated threats.

Eliminate False Positives - Act on all alerts on the endpoints, analyze and evaluate the alerts to eliminate false positives. So that MDR only escalates actionable incidents.

200 Broadacres,
Bloomfield, NJ 07003

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

www.comodo.com
platform.comodo.com

Integrated File Analysis (Cloud Sandbox) - Valkyrie, Comodo's advanced cloud sandboxing, and file-verdicting system, continuously checks files and processes executed in your environment and automatically uploads unknown files for static and dynamic analysis.

Host-Based Intrusion Detection - Endpoint MDR comes with Host Based Intrusion Detection capability that represents a preemptive approach and utilizes advanced techniques to detect and block attempts to breach an endpoint. HIDS incorporates signature, behavioural analysis and stateful inspection detection techniques. Additionally, Endpoint MDR provides file integrity checking, log monitoring, and rootkit detection capabilities.

24/7 Managed Network Detection and Response

Comprehensive 24/7 response of discovered network-based attacks

This will extend SOCaaP offering by monitoring additional logs from customer's network like firewall, Switch, UTM etc. whenever needed. The same service levels will be applied as other packages. It is being licensed as the number of network equipment where only up to 4GB of log per month is included.

Includes: Secure Policy Management, Proactive Threat Hunting (APTs, Lateral Movements, Suspicious Behaviors and more), Process Analysis Examination,

Threat Validation from analysis, eliminates false positives, integrated file analysis (Cloud Sandbox), host-based intrusion detection, early warning for emerging threats, Intrusion triage, breach (case) management, Incident analysis, combine network, endpoint, cloud and web platforms (situational awareness) for maximum effectiveness. It is deployed as a simple VM and licensed by the number of endpoints.

24/7 Managed IDS, DPI Network Detection and Response

Comodo Managed Network Detection and Response, including Intrusion Detection and Deep Packet Inspection.

This is our most comprehensive and extensive network protection solution. This service is an extension of the Global SOC services and enables to include Comodo's own Network Sensor where it does Network-Based Detection and Response for customers. The sensor runs as a probe on the customer network, sniffing network traffic, decoding more than 40 protocols including L7 and extracting meta-data information out of it. It also includes an on-prem log collector and vulnerability scanner as well. SOCaaP with IDS and DPI Network Detection and Response includes the managed network detection platform plus network intrusion detection which combines signature and heuristics-based IDSs and provides a strong mechanism that allows our SOC teams to do

comprehensive network analysis and security monitoring, daily signatures discovering and incidents detection rules management, Insider threat analysis, threat intelligence integration, full packet capture, protocol analyzers for 40+ different protocols such as TCP, UDP, DNS, DHCP, HTTP, HTTPS, NTLM, etc. with full decoding capability. It is deployed as a simple VM and licensed by the number of endpoints.

Advanced Endpoint Protection:
Auto Containment technology stops undetectable hacks
[Code Name // AEP]

Comodo's Industry unique **Auto Containment technology stops undetectable malware, hackers, ransomware** and supply chain breaches before damage can be done. To create any damage, hackers must write to the disk, COM Interface, or the Registry. All unknown malicious files trying to perform writes are instantly opened in a secure virtual container and an allow or deny verdict is returned within 45 seconds, 95% of the time.

Additionally, only Comodo delivers a trusted verdict for 100% of the files already in your network to prevent hidden or embedded malware or hacker code from launching from files already on your endpoints and creating damage.

AEP includes Comodo Auto Containment, Antivirus, Fileless Malware

200 Broadacres,
Bloomfield, NJ 07003

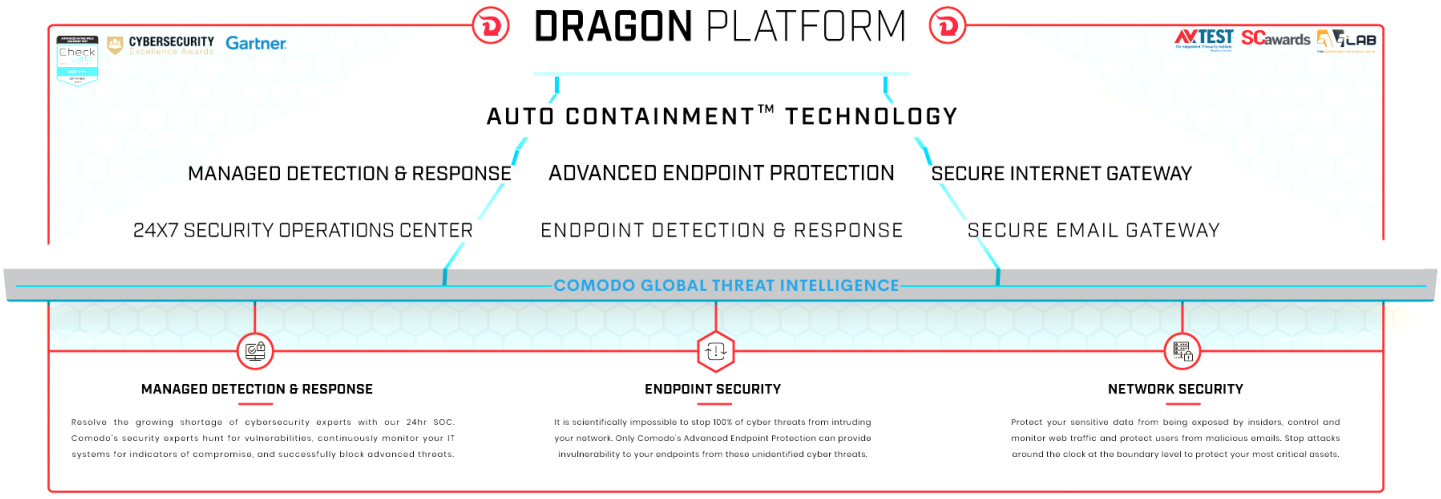
Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000

www.comodo.com
platform.comodo.com

Protection, Valkyrie AI Threat Intelligence, HIPS (Host Intrusion Protection System), Host Firewall (protects against inbound and outbound threats), Virus Scope Behaviour Analyser and File Lookup System (allow/deny lists), Comodo includes RMM capabilities that deliver Patch Management, Remote Control, Software Inventory, Service Desk and more.

About Comodo

We help customers stop breaches with groundbreaking auto containment 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.



Comodo's Dragon Enterprise platform with Advanced Endpoint Protection (AEP) is a complete cloud-native framework that delivers a **zero-trust architecture** to protect and defend endpoints. Its **auto containment technology** has **active breach protection** that neutralizes ransomware, malware and cyber-attacks.

200 Broadacres,
Bloomfield, NJ 07003

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

www.comodo.com
platform.comodo.com