Comodo Client Security

Advanced Endpoint Protection

Comodo Client Security Includes:

- Dynamic Security Containment
- Antivirus
- Personal Firewall
- Web Filtering
- File Lookup Service
- Host Intrusion Prevention (HIPS)
- Behavioral Analysis (VirusScope)
- File-less Malware Prevention
- Integration with Valkyrie Cloud-based Static, Dynamic and Human Expert Analysis

Endpoint Security and Management

Comodo Client Security is the Comodo Advanced Endpoint Protection client application, running directly on the endpoint and delivering a suite of protection that is both lightweight and scalable. Comodo Client Security provides a multi-layered defense that **allows** unfettered access to all known good files, **denies** access to any known malicious files and automatically contains files found to be unknown.

Comodo Advanced Endpoint protection allows the user to run unknown files on the endpoint but automatically wraps them in a self-contained file system. This “container” allows the user to run and interact with these files but protects critical endpoint resources from harm. While an unknown file is contained, Comodo Client Security is using local and cloud-based file analysis tools and resources to determine its true character. The process is transparent to the end users. If the file is good, it goes on the whitelist, and if it’s bad, it’s eliminated. Comodo Client Security’s Dynamic Security Containment functionality is extremely lightweight, has no CPU dependencies and is completely application agnostic.

COMODO

Comodo Client Security Advanced Endpoint Protection

Highlighted Features

- **Dynamic Security Containment –** Comodo's patent-pending automated containerization technology wraps unknown files in a self-contained file system that allows for end user interaction but denies access to critical system resources.
- **Antivirus –** Actively scans endpoints using Comodo's sophisticated antivirus engine that leverages knowledge acquired not only as the world's largest certificate authority but also from the 85 million deployed endpoints – creating an enormous list of known good and known bad files.
- **Personal Packet Filtering Firewall –** Provides granular management of inbound and outbound network activity, hides system ports from scans and provides warnings when suspicious activities are detected. Can be administered remotely or by local administrator.
- **Website Filtering –** Set up specific rules to block access to specific websites. Rules can be created for specific users and can be time-dependent. Comodo Client Security comes with three preset categories that can be added to the rules and also includes the ability to create custom lists.
- **File Lookup Service –** Cloud-based file rating system quickly determines the status of a file if it appears on the file list, the Trusted Software Vendors list or on Comodo's own safelist. These trusted files are excluded from further monitoring, reducing system resource consumption.
- **Host Intrusion Prevention –** Rules-based intrusion prevention system that monitors the activities of applications and system processes, blocking the activities of malicious behaviors by halting actions that could damage critical system components.
- **Behavioral Analysis –** VirusScope, Comodo's Behavior and Actions based knowledge subsystem, looks for indicators of compromise (IOC) around how malware exploits an endpoint. Analysis occurs on the local workstation in a virtualized container that 'jails' a file's attempt to contact the CPU, Memory, Filesystem, Registry, etc., keeping your device safe without affecting usability. VirusScope also uses techniques such as API hooking, DLL injection prevention and much more.
- **Cloud-Based File Analysis –** Providing an Accelerated Verdict, the Comodo Client may be configured to contact Valkyrie, Comodo's cloud-based Static and Dynamic file analysis system that typically returns a verdict in as little as 30-45 seconds – ***over 5 times faster than leading solutions!***
- **Human Analyst –** In cases where VirusScope or Valkyrie are not able to determine a verdict, the option to send analysis to researchers who return a verdict based on SLA timelines ensures you have a 100% Verdict and 100% Coverage.

Features	Device Controls
▪ Dynamic Security Containment	▪ Default Profile
▪ VirusScope Behavior Analyzer	▪ Over-the-Air Device Enrollment
▪ Valkyrie Static & Dynamic Analyzer	▪ Remote Data Wipe
▪ Certificate-based Whitelisting	▪ Mobile Certificates
▪ Comodo AntiVirus (Blacklisting)	▪ Find My Device Features
▪ Jailing Protection	▪ Data Isolation
▪ Comodo Host Firewall	▪ Enforce Strong Mobile Policies
▪ Host IPS	▪ Sneak Peek AntiTheft Feature
▪ Integrated Human Analysis	▪ Policy-based Management
▪ File Reputation	▪ VPN Aware Policies
▪ URL Filtering	▪ External Device Control
▪ Persistent VPN	

Remote Monitoring & Management	Application Security
▪ Remote Access with Full Device Takeover	▪ Application Inventory
▪ Remote Management	▪ Blacklist Inventory
▪ Patch Management	▪ Application Whitelist Store
▪ 24x7x365 Support	▪ Integrated Device, Application and Security Coverage
	▪ Comodo Mobile Apps
	▪ BYOD

Supported Operating Systems	Minimum System Requirements
Microsoft Windows Pro 7, 8, 8.1 and 10	64 bit, 1.3GHz or greater, 2GB RAM or greater, minimum 10MB, TLS over port 443 (ITSM)
Microsoft Windows Server 2008, 2008 R2, 2012, 2016 and all service packs	64 bit, 1.3GHz or greater, 2GB RAM or greater, minimum 10MB, TLS over port 443 (ITSM)
Android Jellybean, Kitkat & Lollipop	Google Play Supported Device List Supported OS versions
Apple iOS 6.x, 7.x, 8.x and 9.x	Official Apple iOS version 5 and later manufactured devices
Apple OS X	Official Apple manufactured devices

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals, to mid-sized companies, to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in New Jersey and branch offices in Silicon Valley, Comodo has 12 international offices across Europe and Asia.