Endpoint Security Problem Solved

Comodo Client
Advanced Endpoint Protection

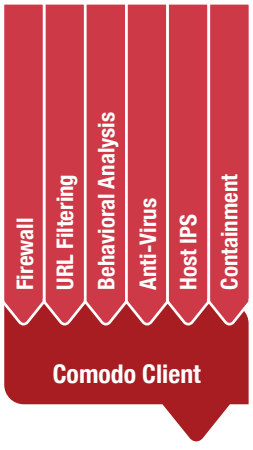
Only Comodo Client combines the complete coverage of a Default Deny Platform in a lightweight 10MB client, deployed and managed in a cloud-based unified IT and Security Management Platform.

Complete Security from Malware Attacks

The Comodo Client solves the problem of malware on both Windows endpoints and mobile devices. Comodo Client uses a multi-layer, modular approach that uses automation to isolate unknown files in a secure container, while an accelerated verdict is determined for unknown files, All while using multiple Specialized Threat Analysis and Protection (STAP) methods identified as essential by IDC to protect against advanced threats.

Thanks to a Default Deny Platform, Comodo Client is lightweight - as little at 10MB - and is able to allow all known good, and block all know bad files, automatically containing the remaining unknown, while local and cloud components deliver an accelerated verdict. This provides the most robust protection on the market, without sacrificing usability or scale even in virtual environments.

No need to 'solution stack' unproven point solutions, on your legacy AV. Comodo Client can increase your security posture, in a competitively priced offering.



"Cybercrime is not something that is just a nuisance to IT organizations around the world anymore, it has ripple effects across multiple global problems such as economic decline, identity theft and how it is used to fund terrorism, human and drug trafficking. Our advance Advanced Endpoint Protections are intended to eradicate malware, once and for all."

~ Melih Abdulhayoglu, Comodo CEO

COMODO

Comodo Client

Summary of Features

Known Good/Bad: Comodo is the largest Certificate Authority brand in the world, providing for the most comprehensive library of all known "good" code producers. Comodo Threat Research Labs (CTRL) provide the largest library of known "bad" files, battle tested solution with over 85 million Windows PC users.

Automated Containerization: Comodo's patent pending automated containerization technology has been proven to stop zero-day attacks, 'jailing' unknown processes until an accelerated verdict is decided. Say goodbye to 'Patient Zero.'

VirusScope: Using behaviorial analysis based on knowledge or indicators of compromise (IOC) of how malware exploits an endpoint, analysis occurs on the local workstation. A virtualized container 'jails' files' attempting to contact the CPU, Memory, Filesystem, Registry, and more. This keeps your device safe, without affecting usability. VirusScope also uses techniques such as APIhooking, DLL injection prevention, and much more.

Valkyrie: To provide an accelerated verdict, the Comodo Client may be configured to contact the Comodo cloud for static and dynamic malware analysis that typically returns a verdict in as little as 30-45 seconds - >5x's 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 to ensure you have 100% Verdict, and 100% Coverage.

Features		
Automated Containerization	VirusScope Behavior Analyzer	Valkyrie Static & Dynamic Analyzer
Certificate-based Whitelisting	Comodo AntiVirus (blacklisting)	Jailing Protection
Comodo Host Firewall	Host IPS	Integrated Human Analysis
File Reputation	URL Filtering	

Device Controls		
Default Profile	Data Isolation	Mobile Certificates
Find My Device Features	Remote Data Wipe	Sneak Peak AntiTheft Feature
Over-the-Air Device Enrollment	Enforce Strong Mobile Policies	Policy Based Management
VPN Aware Policies		

Application Security		
Application Inventory	Blacklist Applications	Application Whitelist Store
Integrated Device, Application and Security Coverage	Comodo Mobile Apps	BYOD

Remote Monitoring and Management		
Remote access with full device takeover	Remote Management	Patch Management

Supported Operating Systems
Microsoft Windows Pro 7, 8, 8.1 & 10
Microsoft Windows Server 2008, 2008 R2, 2012 & 2016, all service packs
Android Jellybean, Kitkat & Lollipop
Apple iOS 6.x, 7.x, 8.x & 9.x

Minimum System Requirements
64 bit, 1.3GHz or greater, 2GB RAM or greater, minimum 10MB, TLS over port 443 (ITSM)
64 bit, 1.3GHz or greater, 2GB RAM or greater, minimum 10MB, TLS over port 443 (ITSM)

About Comodo

The Comodo organization is a global innovator and developer of cybersecurity solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information. With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1 (888) 266-6361
Tel: +1 (703) 581-6361
Fax: +1 (973) 777-4394

sales@comodo.com
www.comodo.com/enterprise

COMODO

CCDSWEB022416