

Keeping Your Endpoints Free of Malware

Comodo Advanced Endpoint Protection

Comodo AEP combines the best in endpoint security with comprehensive device control and endpoint management.

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

With malware proliferating at an astonishing rate of over one million unknown files per day, conventional **Default Allow** solutions that only detect/block “bad” files while allowing all other files to run provide inadequate security that leaves you vulnerable to attack by “zero day” and other unknown threats.

Comodo Advanced Endpoint Protection (AEP) delivers a cloud-enabled suite of protection and management that is both lightweight and scalable. Comodo AEP combines the best in endpoint security with comprehensive device control and management functions to deliver superior security and manageability across the endpoint spectrum.

On the endpoint, Comodo AEP provides a multi-layered defense that allows unfettered access to all known good files and content, **denies** access to any known to be malicious and automatically **contains** files and scripts found to be **unknown**. This “Default Deny” strategy that only permits the “known good” to run and contains the unknown maximizes productivity and security as the user can run and interact with these files while Comodo AEP protects critical endpoint resources from harm. This approach also maximizes IT Security staff productivity by avoiding time-consuming recovery and re-imaging of infected machines.

In addition to preventing endpoint infections due to malware, complete endpoint protection must also include the administration of security patches, OS updates and application control. Comodo AEP delivers all of this functionality along with automatic discovery, device inventory management and external device control for Windows, Android and iOS-based devices. All from an easy-to-use, cloud-based administration console.

Comodo AEP minimizes operational costs and maximizes security by providing the power to manage devices and stop malware from affecting your organization.

COMODO

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
<ul style="list-style-type: none"> Dynamic Security Containment 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 Persistent VPN 	<ul style="list-style-type: none"> Default Profile Over-the-Air Device Enrollment Remote Data Wipe Mobile Certificates Find My Device Features Data Isolation Enforce Strong Mobile Policies Sneak Peek AntiTheft Feature Policy-based Management VPN Aware Policies External Device Control
Remote Monitoring & Management	Application Security
<ul style="list-style-type: none"> Remote Access with Full Device Takeover Remote Management Patch Management 24x7x365 Support 	<ul style="list-style-type: none"> Application Inventory Blacklist Inventory Application Whitelist Store 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.

Comodo and the Comodo brand are trademarks of the Comodo Group Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The current list of Comodo trademarks and patents is available at comodo.com/repository