COMODO
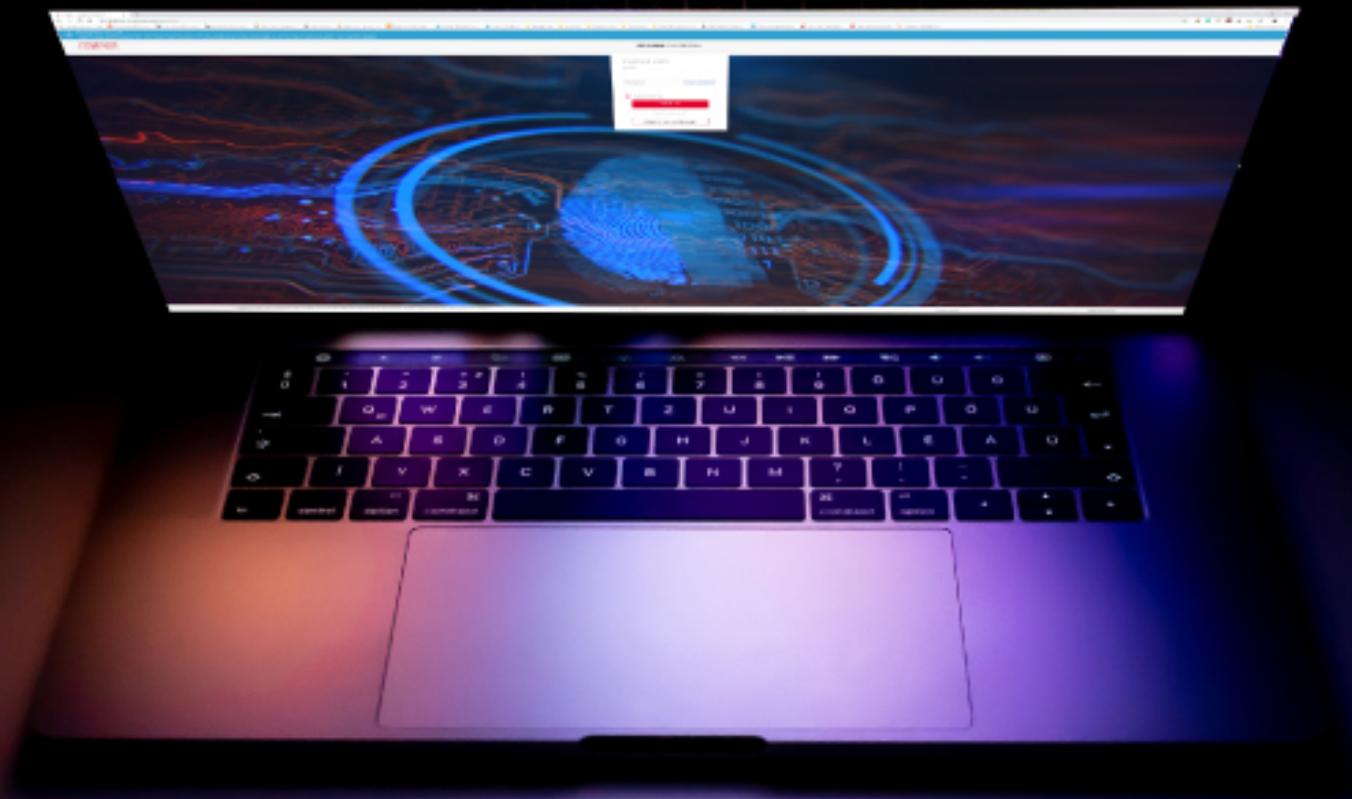
COMODO ADVANCED ENDPOINT PROTECTION PREMIUM FEATURES

ADVANCED

ENDPOINT

PROTECTION

IT MANAGEMENT CAPABILITIES

Comodo Advanced Endpoint Protection – Premium (AEP) Features:

Comodo Anti-Virus A Proactive Anti-Virus engine that automatically detects and eliminates viruses, worms, and other malware.

Comodo Containment Comodo's threat containment provides total protection against zero-day threats while having no impact on end-user experience or workflows. All untrusted processes and applications are automatically contained in a secure environment, allowing safe applications the freedom to run while denying malware the system access they require to deliver their payloads.

Valkyrie Valkyrie is a cloud-based file verdict service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. CCS on managed Windows computers can automatically submit unknown files to Valkyrie for analysis. The results of these tests produce a trust verdict on the file which can be viewed from the ITSM interface. Detecting, investigating, and mitigating suspicious activities and issues on hosts and endpoints.

Comodo Firewall Highly configurable packet filtering firewall that

constantly defends inbound and outbound internet attacks

Host Intrusion Prevention System (HIPS) Constantly monitors system activity and only allows executables and processes to run if they comply with security rules that have been enforced by the Windows profile applied to the managed computer.

Virus Scope Monitors the activities of processes running at the endpoints and generates alerts if they take actions that could potentially threaten privacy and/or security of the end user. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core
process-monitoring functionality of the CCS by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide you with more granular control over otherwise legitimate software which requires certain actions to be implemented to run correctly.

Website Filtering Create website filtering rules which let you

determine which sites certain users can or cannot access.

Mobile Device Management For the purposes of this guide, a mobile device is any Android or iOS smart phone or tablet that can connect to the enterprise network through a wireless connection.
Comodo IT and Security Manager allows network administrators to remotely configure device access rights, security settings, general preferences and to monitor and manage the device. Mobile devices may be employee or company owned.

Windows Endpoints For the purposes of this guide, a Windows Endpoint is any Windows laptop, desktop or server computer that can connect to the enterprise network through a wireless or wired connection. Comodo IT and Security Manager allows administrators to install Comodo Endpoint Security, manage security settings on them, view and manage installed applications, run antivirus scans manage OS update/security path installation and more. Windows Endpoints may be employee or company owned.

Comodo Client Security Comodo Client Security (CCS) is the remotely managed endpoint security software installed on managed Windows devices. Each component of CCS can be configured to offer the desired security level by applying configuration profiles.

File Lookup Service (FLS) A cloud-based file lookup service that ascertains the reputation of files checking them against Comodo's master whitelist and blacklist.

Patch Management The Patch Management module monitors Windows OS updates and patches for 3rd party Windows software. It identifies patches appropriate for the OS version of each managed Windows device and. If required, automatically installs them.

Remote Monitoring and Management The Remote Monitoring and Management (RMM) Module is an efficient endpoint monitoring application that allows administrators to monitor and manage multiple endpoints from one centralized console. RMM is available as an ITSM extension to Comodo One customers and can be accessed from the ITSM interface.

Mac Endpoints Allows administrators to view OS and software details, installed applications, security information from Comodo Antivirus, network connection details and more. Administrators can also manage configuration profiles in effect on the endpoint, remotely install OSX packages and manage group membership.

External Device Control manage external devices you can control data transfer capabilities and protect valuable organization/customer data from loss or theft via removable devices. Admins can now open or block access to devices such as data storage media, including removable devices, CD/DVDs and other data transfer devices.

Comodo Service Desk - Fully featured ticket management system which allows enterprises to implement strong and effective work-flows for internal and customer-facing support departments. The support ticketing management system allows administrators and help desk staff members to keep track of tickets raised by users, attend to them, reassign them to appropriate department or organizations, generate reports, create projects by integrating tasks and tickets and more. The interface has two panels, Admin Panel and Staff Panel, and admins with appropriate permissions can access both the panels.

VISIT COMODO.COM
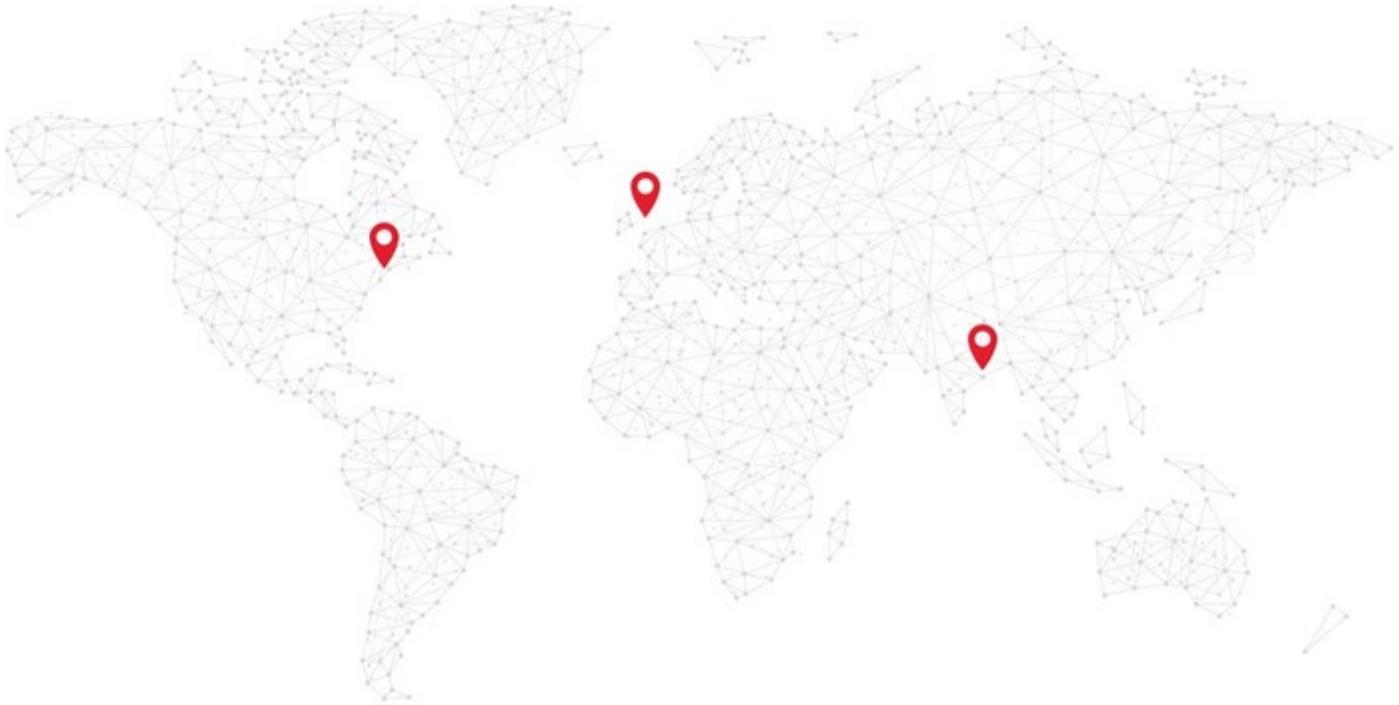
COMODO

NORTH AMERICA
—
Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013 United States
Tel: +1 (877) 712 1309
Tel: +1 (888) 551 1531
Fax: +1 (973) 777 4394
Inquire: sales@comodo.com
Support: c1-support@comodo.com

EUROPE
—
Comodo Security Solutions,
Inc. Șoseaua Națională 31, Iași
700237, Romania, Europe
+40 332 806 772

ASIA
—
Comodo Security Solutions Pvt.
Ltd. Prestige Office Centre,
183 NSK Salai, Vadapalani,
Chennai India
Tel: +91 44 4562 2800
www.comodo.co.in