Overview

Comodo Endpoint Security Manager

With the Industry's Only Virus-Free Warranty

Comodo's threat containment technology ensures that all viruses and malware are prevented from infecting your computer

COMODO
Creating Trust Online®

Comodo Endpoint Security Manager (CESM) protects against viruses and malware by focusing on prevention and not simply detection. Our threat prevention and containment technologies create an impenetrable shield that identifies safe, unsafe and questionable files (aka good, bad and unknown files).

Traditional antivirus solutions use a "detection"-based approach whereby they examine items against a "blacklist" (a list of known bad files/threats) to determine which programs or files are safe to run or to allow access to the system. The problem with this approach is that ALL threats must be known and your computer's blacklist file must be continuously, and instantly, updated. Given this limitation, it is impossible for a blacklist to be up-to-date 100% of the time for 100% of the threats.

Next Generation Prevention-Based Security

Defense+ – A collection of advanced security prevention technologies designed to preserve the integrity, security and privacy of your operating system and user data.

Host Intrusion Protection System (HIPS) – A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.

Behavior Blocker – Authenticates each executable and process running on your computer and prevents it from taking action that could harm your computer. Unrecognized processes and applications will be auto sandboxed and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but harmless) applications the freedom to operate while untrusted (and potentially malicious) applications are prevented from damaging your PC or data.

Comodo Firewall – Highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.

Secure Wireless Internet Connectivity – TrustConnect™ makes surfing the web safe from any public Wi-Fi location.

PRODUCT HIGHLIGHTS

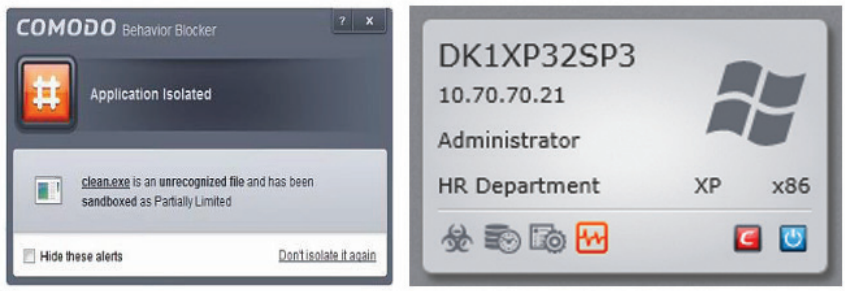
- Centralized management of Windows, Mac and Linux endpoints.
- Multilayered and integrated defense offering antivirus, firewall, auto sandbox, host intrusion protection, file reputation, URL filtering, and behavioral analysis.
- Unique, persistent, auto sandbox executes zero-day threats in a secure container, allowing Comodo to be the only vendor offering a $5,000 virus-free warranty*.
- Auto sandbox can be deployed independently alongside existing AV solutions to increase endpoint protection against unknown files until their true nature can be determined.
- One-click administration of quarantined, sandboxed and unrecognized applications.
- Dashboard displays 14 critical metrics per endpoint to provide clear and simple alerting and remediation of LAN and WAN managed systems.
- Manages endpoint processes, services, installed applications, resource usage, removable devices and power usage.
- Hierarchical deployment of CESM servers allows local or remote management of non-LAN endpoints.

Comodo Endpoint Security (CES) offers real-time protection against all malware threats. Other antivirus products depend on signature updates alone but Comodo's auto sandbox technology protects you from unknown threats. Thus enabling Comodo to be the only vendor to provide a $5,000* virus-free warranty against repair costs, should an endpoint in your enterprise become infected with a virus or malware and we are unable to restore you to working condition.

The Future of Endpoint Administration and Protection

CESM not only provides unrivalled protection against zero-day threats, it also grants administrators total visibility and control over the software, hardware and services of every machine. CESM is fully integrated with the Comodo Endpoint Security suite and provides centralized administration of antivirus and system health status.

Utilizing a unique patent-pending panoramic display, the web-based administration console presents each endpoint as a tile containing 14 critical metrics facilitating rapid alerting and remediation of issues requiring a minimum of administrative effort.



- Infection status
- Definition database status
- Security policy compliance
- System health status
- User assistance requests
- Security suite status
- Online status

The computer properties screen provides granular information about each endpoint, including OS version, service pack, installed applications, whether a reboot is required, networking statistics and CPU, RAM and hard-drive usage metrics. With just one click, the administrator is able to view and stop services and processes as well as browse and uninstall MSI-based applications.

Armed with this information, the administrator can make swift and accurate decisions to protect the infrastructure and ensure the smooth and efficient continuation of users' computing requirements.

Proactive administration is available through the configuration of policies or templates that dictate the endpoint's behavior. Controlling everything from the definition database update schedule and source, granular manipulation of critical security configurations, and file and vendor whitelisting to removable device control and power management, the user-friendly policy creation wizard can generate and enforce the administrator's configurations within minutes.

More Efficient, Effective and Easier Management

This ability to roll out and centrally manage security policies to a network that is protected with a proven and fully integrated

security suite can save thousands of man-hours per year. Administrator time that would otherwise be lost to repetitive configuration and vendor interoperability problems can be re-directed towards more productive and profitable core business interests. Furthermore, because CESM policies can be deployed immediately across all protected nodes, administrators can respond more quickly to protect an entire network against the latest, zero-day threats and CESM's intuitive interface provides fingertip access to task wizards, important network and task related data, and support resources.

A Total Solution for both SMBs and the Enterprise

- Centrally manage of Windows, Mac and Linux endpoints.
- Automatic threat containment – Prevents malware outbreaks by detecting then automatically containing unknown files in an isolated environment separate from the underlying operating system and user data.
- Whole host protection – Layered security ensures each **endpoint is protected** with a combination of antivirus, firewall, host intrusion prevention, URL filtering, behavior monitoring, and threat containment.
- Panoramic dashboard presents clear and simple view of 14 critical endpoint metrics for each endpoint; providing total security awareness and control.
- Powerful system management capabilities allow administrators to view and modify endpoint processes, services and installed applications.
- Supports "push" deployment via Active Directory®, Workgroup and IP addresses, and "pull" deployment via group policy or login script.
- Remote assistance feature allows admins to interact directly with users and remote desktop endpoints if required.
- Real-time notifications lower emergency response time to emerging threats.
- Location-aware policies allow granular definition of security configurations for endpoints inside and outside of the VPN.
- Go green with integrated power management functionality with Wake-on-LAN enabled systems advance.
- Minimal system requirements allow installation on non-dedicated Windows PCs or servers.

Next Steps

To download a 60-day, 600-user free trial or to access a product demo, visit **http://www.comodo.com/tryesm**

For more information on CESM, visit **https://enterprise.comodo.com/security-solutions/endpoint-protection/endpoint-security-manager/**

To speak with a regional sales representative, please contact us at: **cesmsales@comodo.com**

+ 1 (888) 266-6361 (North and South America)

+ 44 (0) 207 402 7278 (EMEA and APAC)

About Comodo

The Comodo organization is a global innovator and developer of cyber security 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 **www.enterprise.comodo.com**.

* Comodo's Protection Plan is included with Comodo Endpoint Security and is available for one (1) year from the date of your software registration and installation. Please see Comodo Endpoint Security Manager End User Subscriber Agreement (http://www.comodo.com/repository/eula/EULA-CESM-v2013.pdf) for complete details. Comodo Endpoint Security trials exclude Comodo Protection Plan.

**System only