



Impenetrable Cybersecurity Without Sacrificing Usability

ADVANCED ENDPOINT PROTECTION

REAL-WORLD PROOF THAT OUR ENDPOINT PROTECTION OFFERS SECURITY WITHOUT COMPROMISE

When a 2017 WikiLeaks data dump exposed the CIA's assessments of 20 security products, we got to see the unvarnished results of the intelligence community's attempts to foil the technologies that businesses rely on daily to protect themselves. While many of the biggest names in the market proved to be easily to moderately hackable, there was one solution that seemed to frustrate their best attempts.

Here's what the CIA—one of the best-funded, most expert hacking organizations in the world—had to say about Comodo AEP:

“Comodo is impossible to breach. A colossal pain in the posterior. It literally catches every payload sent through a network.”

That's good news for you. By deploying Comodo AEP, you can bulletproof your endpoints and your hardworking employees won't notice the difference.

100% TRUSTED VERDICT OF ALL UNKNOWN FILES

Cybercrime has come a long way from script kiddies looking for a little glory. Today's sophisticated attackers are after money and power. By 2019, ransomware will attack a business every 14 seconds and damage costs will soar to \$11.5 billion annually. In 2017, wide-ranging events from elections to North Korea nuclear threats and missile launches corresponded with major malware spikes in enterprise security, indicating the use of cyber “activism” to achieve geopolitical goals.

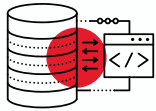
No business and no user can be considered safe. Having a comprehensive defense-in-depth strategy has never been more critical, and no security posture is complete without technology to protect endpoints. But security controls must not impede employees' ability to do their jobs—and ease of administration is critical to reduce the burden on your IT staff.





TRADITIONAL ENDPOINT SECURITY

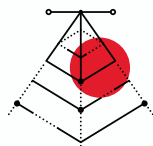
File Executed Inside Network



Attackers create payloads to deliver to targeted or global campaign.



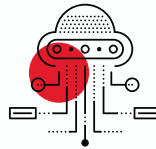
Blacklist Pass



Legacy AV doesn't detect malicious signature for newly created files.



Machine Learning



Machine Learning is not trained for newly bad indicators, bypassing statistical and behavioral models.



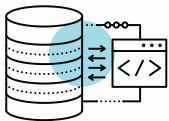
File Executed Infects Network



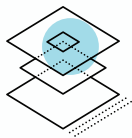
Endpoint is infected because all previous layers cannot identify relying on bad indicators.

COMODO ADVANCED ENDPOINT PROTECTION

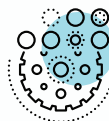
File Executed Inside Network



File Identified as Unknown



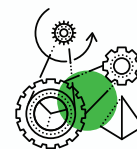
Auto Containment Triggers Instantly



File Analyzed for Trusted Verdict



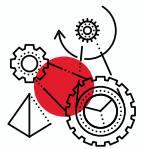
Known Good Verdict



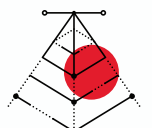
File Safe on Endpoint



Known Bad Verdict



File Blocked from Endpoint




Unknown executables and other files that request runtime privileges are automatically run in a virtual container that does not have access to the host system's resources or user data. They run just as well as they would on the host system, making it seamless from the end-user perspective, but they cannot damage or infect the system. Any unknown executables in containment do not have write privileges to the hard drive, COM interface or registry. Comodo's approach enables users to remain productive as usual without allowing unknown threats to harm their endpoints.

Competition cannot keep up to our verdict speeds. 95% of all files are verdicted within 45 seconds. More sophisticated threats are investigated 24x7x365 by our worldwide team of security experts. We ensure 100% trusted verdict on all unknown files with our industry leading 4 hour SLA.



AEP FEATURES


AUTO CONTAINMENT
Contain 100% of unknown threats instantly



COMODO ANTIVIRUS
Automatically detect, cleanse and quarantine suspicious files



COMODO HOST FIREWALL
Protect against inbound and outbound threats



VALKYRIE ANALYZER
Analyze and verdict 100% of unknown files


FILELESS MALWARE PROTECTION
Stop malware to write access


HOST INTRUSION PREVENTION
Monitor important operating system activities


VIRUS SCOPE BEHAVIOR ANALYZER
Monitor behaviors of all processes to identify harmful actions


FILE LOOKUP SYSTEM
Check the file reputation against Comodo's whitelist and blacklist


EXPERT HUMAN ANALYSIS
24x7x365 expert analysis of more sophisticated threats

AEP COMPATIBILITY



MINIMUM SYSTEM REQUIREMENTS

Windows 10, Windows 8, Windows 7, Windows Vista

- 384 MB available RAM
- 210 MB hard disk space for both x86 and x64
- CPU with SSE2 support
- Internet Explorer version 5.1 or above



MINIMUM SYSTEM REQUIREMENTS

Windows XP

- 256 MB available RAM
- 210 MB hard disk space for both 32-bit and 64-bit versions
- CPU with SSE2 support
- Internet Explorer version 5.1 or above



SUPPORTED OPERATING SYSTEMS

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2003 R2
- Windows 10 (both x86 and x64)
- Windows 8.1 (both x86 and x64)
- Windows 8 (both x86 and x64)
- Windows 7 (both x86 and x64)
- Windows XP (SP3 or higher) x86
- Android: 4.x, 4.x (KNOX), 5.x, 5.x (KNOX), 6.x (KNOX)
- Android: 7.x, 7.x (KNOX), 8.x, 8.x (KNOX), 9.x
- iOS: 7.x, 8.x, 9.x, 10.x, 11.x, 12.x
- macOS: 10.11x, 10.12x, 10.13x, 10.14x
- Latest Ubuntu 16.x LTS x64 (with GUI)
- Latest Ubuntu 18.x LTS x64 (with GUI)
- Latest Debian 8.x x64 (with GUI)
- Latest Red Hat Enterprise Linux Server 7.x x64 (with GUI)



STOP CYBER THREATS

COMODO HAS PROVEN RESULTS FOR CYBER SECURITY SOLUTIONS

Comodo has made a paradigm shift in its approach to the malware problem. We are the only company that prevents the damage by putting files into three categories, Good, Bad or unknown. Unknown or bad files are contained until they are verdicted.

GARTNER RECOGNIZED - MAGIC QUADRANT

The Gartner logo, consisting of the word "Gartner" in a blue sans-serif font, with a red horizontal line underneath.

***“ADVANCED CYBERSECURITY TECHNOLOGY
THAT PROTECTS YOUR DATA
AGAINST ALL **UNKNOWN THREATS.**”***

GARTNER PEER INSIGHTS - FEBRUARY 2019



COMODO CORPORATE HEADQUARTERS

1255 Broad Street, Clifton, NJ 07013 USA

info@comodo.com | sales@comodo.com | comodo.com

Experienced intrusion? Contact us at (855) 551-1531