COMODO
CYBERSECURITY

Advanced Endpoint Protection
Datasheet

IMPENETRABILITY WITHOUT SACRIFICING USABILITY

100% Verdict 100% of the Time

Comodo Advanced Endpoint Protection (AEP) delivers patent-pending auto-containment, where 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 native system.

While running in auto-containment, unknown files are uploaded to a global threat cloud for real-time analysis, which returns a verdict within 45 seconds for 95% of the files submitted. The remaining 5% of cases are sent to researchers for human analysis who make a determination within SLA timelines. In short, Comodo AEP provides a 100% verdict 100% of the time. And because the global threat cloud is crowdsourced, the knowledge gained about one unknown file benefits all Comodo AEP users. You benefit from the network effect of 85 million users.

The extremely lightweight Comodo client has no CPU dependencies and is completely application-agnostic.

Eliminate Fear of the Unknown

Good files can be safely run. Bad files can be blocked. But how do you deal with unknown files? If you run them and they're bad, you've put your company at risk. If you block them and they're legit, you prevent users from doing their jobs.

> "Comodo AEP offers the broadest array of tools to identify known good and known bad files. For all the unknown, our patented auto-containment technology and verdict decision engine deliver a verdict—good or bad—every time, with zero impact on the user experience."

Key Capabilities

Antivirus scanning: Scans endpoints against a massive list of known good and bad files compiled from years as the world's largest certificate authority and from the 85 million endpoints deployed worldwide.

Auto-containment: Unknown executables and other files that request runtime privileges are automatically run in Comodo's patented 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.

VirusScope behavioral analysis: Uses techniques such as API hooking, DLL injection prevention, and more to identify indicators of compromise while keeping the endpoint safe and without affecting usability.

Valkyrie verdict decision engine: While running in auto-containment, unknown files are uploaded to a global threat cloud for real-time analysis, returning a verdict within 45 seconds for 95% of the files submitted.

Human analysis: In the 5% of cases where VirusScope and Valkyrie are unable to return a verdict, the file can be sent to researchers for human analysis who make a determination within SLA timelines.

Host intrusion prevention: Rules-based HIPS that monitors application activities and system processes, blocking those that are malicious by halting actions that could damage critical system components.

Personal packet filtering firewall: Provides granular management of inbound and outbound network activities, hides system ports from scans, and provides warnings when suspicious activities are detected. Can be administered remotely or by a local administrator.

COMODO CYBERSECURITY

Advanced Endpoint Protection
Datasheet

Features

- Automated containerization
- Certificate-based whitelisting
- Comodo host firewall
- File reputation
- VirusScope behavior analyzer
- Comodo Antivirus (blacklisting)
- Host IPS
- URL filtering
- Valkyrie static and dynamic analyzer
- Jailing protection
- Integrated human analysis
- Fileless malware protection
- Command-line analysis
- Embedded code detection

Device Management

- Default profile
- Find-my-device features
- Over-the-air device enrollment
- VPN-aware policies
- Data isolation
- Remote data wipe
- Enforce strong mobile policies
- External device control
- Mobile certificates
- “Sneak Peek” antitheft feature
- Policy-based management

Application Security

- Application inventory
- Integrated device, application, and security coverage
- Blacklist applications
- Comodo mobile apps
- Application whitelist store
- BYOD

Supported Operating Systems

- Windows 10 Support (both 32-bit and 64-bit versions)
- Windows 8 (both 32-bit and 64-bit versions)
- Windows 7 (both 32-bit and 64-bit versions)
- Windows Vista (both 32-bit and 64-bit versions)
- Windows XP (both 32-bit and 64-bit versions)
- Android: 4.x, 4.x (KNOX), 5.x, 5.x (KNOX), 6.x (KNOX), 7.x, 7.x (KNOX)
- iOS: 7.x, 8.x, 9.x, 10.x, 11.x

macOS: 10.11.x, 10.12.x, 10.13.x

- Windows server: Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016
- Linux: Ubuntu 16.04.2 LTS x64, Debian 8.8 x64, Red Hat Enterprise Linux Server 7 x64

Minimum System Requirements

Windows 10, 8, 7, Vista	Windows XP
384 MB available RAM	256 MB available RAM
210 MB hard disk space for both 32-bit and 64-bit versions	210 MB hard disk space for both 32-bit and 64-bit versions
CPU with SSE2 support	CPU with SSE2 support
Internet Explorer version 5.1 or above	Internet Explorer version 5.1 or above

Remote Monitoring and Management

- Remote access with full device takeover
- Remote management
- Patch management