

ENDPOINT PROTECTION WITHOUT COMPROMISE

The cyber-threat landscape has evolved and so has endpoint protection. Different solutions use different approaches and before you make a decision for your organization, you need to understand the options—and the tradeoffs.

Containment

Containment is similar to the concept of sandboxing, but addresses the usability issue by making it virtually invisible from the end-user perspective. With this approach, a processor- and OS-agnostic container runs right on the endpoint to analyze the file without allowing access to the underlying system. If the file is determined to be malicious, it's blocked. If the verdict is that it's safe, the next time the file is run, it will be run outside of the container.

Sandboxing

Sandboxing emerged as a way to evaluate files as being “bad” or “good” before they enter the network by isolating them in a tightly controlled virtual environment on a server, and only those that pass are then released to the endpoint. This provides a safe way to test unverified programs that could contain malicious code. In some cases, sandboxing quarantines the file and only releases it to the user when it's deemed safe. This offers a high level of security, but can have a significant impact on user experience and business productivity. In other cases, while the file is being analyzed in the sandbox, the original file remains on the endpoint. This addresses the usability and productivity issues, but the user is now vulnerable to malicious code.

“Signature- and behavior-based detection tools use a “default allow” approach to endpoint security. They let everything in and then determine if there is any malicious code being run. In contrast, sandboxing and containment take a “default deny” stance, preventing anything from running until it’s deemed safe. While this offers much tighter security, what happens between the time the file enters the system and when a safe file is cleared and passed back to the end user? Security is critical, but it can’t come at the expense of business productivity. Comodo Advanced Endpoint Protection (AEP) solves this problem.”

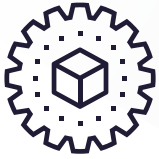
Signature-based detection

In the early days, antivirus companies would document the “signatures” of known malware. Any files that matched the signatures would be flagged as malicious. The problem with this approach is that it only works for known malware. But all malware starts out as unknown software, so when a new piece of malicious code was unleashed, companies were vulnerable until the threat was discovered and its signature captured (known as “zero-day”). It's the cyber equivalent of closing the barn door only after the horse is gone. When attackers began using techniques to encrypt or mutate the code, the simplistic approach of signature-based detection, while still valuable, simply couldn't keep up.

Behavior-based detection

A new wave of solutions looked to solve the problem by focusing not on the signatures of malicious files but on the behavior of network traffic. Behavior-based systems understand what “normal” looks like, and then identify abnormal behavior that could represent an attack. This approach helps address the zero-day problem by alerting IT to potential attacks within seconds, but comes with its own challenges. There can be a high number of false positives, making administration of the system time-consuming. And behavior-based tools can add significant traffic on the network, so organizations need to ensure their systems can support the additional bandwidth demands. While this approach is far better equipped than signatures to keep pace with today's sophisticated malware, the fact is that no matter how quickly it identifies malicious behavior on the network, it can only identify it once it's already inside.

Key Features



Lightweight client

At as little as 10 MB, the Comodo client provides the most robust protection on the market without sacrificing usability or scale.



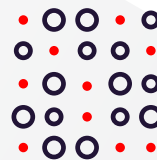
Website filtering

Set up specific rules—which can be user-specific and time-dependent—to block access to specific websites.



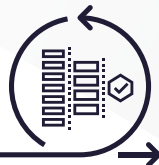
Host intrusion prevention

Rules-based IPS that monitors the activities of applications and system processes, blocking malicious behaviors by halting actions that could damage critical system components.



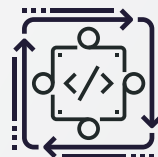
Personal packet filtering firewall

Can be administered locally or remotely and provides granular management of inbound and outbound network activity, hides system ports from scans, and provides warnings when suspicious activities are detected.



File lookup service

Provides a cloud-based file rating system to quickly determine the status of a file if it appears on the file list, the trusted software vendors list, or Comodo's own safelist. These trusted files are excluded from further monitoring, reducing system resource consumption.



Interoperability

A solid defense-in-depth security strategy requires enterprises to deploy a diverse security toolkit using technologies from a range of vendors. In a heterogeneous-by-design environment, interoperability is crucial. Comodo AEP containment technology has no known incompatibilities with productivity or security software.

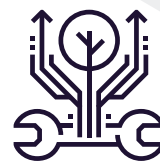
Remote monitoring and management



Remote access with full device takeover



Remote management



Patch management



24 x 7 x 365 Support

HOW IT WORKS

From a cybersecurity perspective, there are three types of files: those that are known to be good, those that are known to be malicious, and the unknown. When you know a file is good, you can let it run. When you know a file is bad, you can block it. It's the unknown files that create the challenge—and all malware starts out as unknown code. Comodo AEP uses auto-containment to automatically isolate unknown files while the verdict decision engine makes a good/bad determination.

AUTO-CONTAINMENT

Comodo leverages the world's largest signature whitelist of known good files to identify processes which are safe to run on an endpoint.¹

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 processes in containment read and write to a virtual registry, file system, OS core, and hardware. This allows safe files to run as needed while preventing malicious files from accessing the system to deliver their payloads.

While the file is in containment, the system records a full forensic analysis, which can be configured for delivery to your SIEM and SOC. Any unknown processes that are given a "good" verdict are automatically allowed to run on the host in subsequent sessions.

¹ Files can only be added to this list after undergoing intense testing by Comodo Threat Intelligence Lab. Known good processes are still subject to strict behavior and virus monitoring during runtime but are permitted to run on the local machine because they have been thoroughly authenticated as presenting no threat.

How Comodo AEP Compares to Other Containment Approaches

One vendor's approach uses selective containment, which isolates just certain targeted applications, such as browsers, PDF readers, and office applications. The drawback is that it does not provide mechanisms to detect and contain malicious processes from other sources. Administrators have to lock down the applications and services that users are allowed to run, and setup requires constant fine-tuning. In contrast, Comodo AEP offers a completely hands-off way to contain files from all sources.

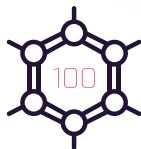
Another vendor creates multiple "micro VMs" to contain each user-generated process, spawning separate virtual instances of the guest OS for every contained process, all controlled by a hypervisor running on the host OS. This increases the demand on the endpoint's resources and can lead to system slowdown and workflow interruptions. In contrast, Comodo AEP's containers have zero impact on the user's experience.

Advanced Control for Security Teams

Comodo auto-containment uses runtime user-space process isolation and is not dependent on CPU-virtualization technology to operate, but it can be deployed to leverage CPU-virtualization for additional security if desired. Comodo auto-containment uses both software- and hardware-level virtualization technologies and is compatible with all remote desktop software.

Comodo auto-containment isn't limited to specific applications, giving it the flexibility to fully support all the use cases your organization requires. Admins can, however, specify auto-containment for only specific applications or choose to auto-contain all files. Either way, there's no impact on performance.

Real-Time Analysis



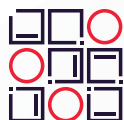
100% Verdict 100% of the time

Every file receives a verdict—good or bad—every time.



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.



Behavioral analysis

Comodo uses behavioral analysis on files running in containment. Comodo VirusScope 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.



Anti-virus scanning

Comodo's sophisticated antivirus engine actively 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. This quickly catches and eliminates easily detected known malicious software.



Verdict decision engine

While running in auto-containment, unknown files are uploaded to Comodo Valkyrie in the cloud for real-time analysis. This global threat cloud, which analyzes 73 billion file queries and 300 million unique unknown files annually, returns a verdict within 45 seconds for 95% of the files submitted. 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.

Frustrate the Hackers, Not Your Users

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 same technologies that businesses rely on every day 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:

"A colossal pain in the posterior. It literally catches everything until you tell it not to."

That's good news for you. And there's more good news. By deploying Comodo AEP, you're only thwarting bad actors; your hardworking employees won't notice the difference.

Source: Cuthbertson, Anthony. "How CIA Hackers Rate Your Computer's Antivirus." Newsweek. March 19, 2017.

Advanced device controls

- Default profile
- Over-the-air device enrollment
- Remote data wipe
- Mobile certificates
- "Find my device" features
- Data isolation
- Strong mobile policy enforcement
- "Sneak Peek" pictures to recover lost devices
- Policy-based management
- VPN-aware policies
- External device control