The Role of Automated Containment™ in Comodo Advanced Endpoint Protection's Default Deny Platform™

The Role of Automated Containment™ in Comodo Advanced Endoint Protection's Default Deny Platform™

This paper is the direct result of a simple question that a customer asked us recently:

"What if a malicious file were to escape Comodo's containment technology, wouldn't it be 'game over'?"

In point of fact, while Comodo's patent-pending Automatic Containment™ is an integral part of Comodo's Default Deny Platform,™ the short answer is no, Automatic Containment is only one – albeit very important – piece of the Comodo protection puzzle.

Our true Default Deny Platform™ has been carefully designed to protect organizations from known, unknown and advanced attacks, and the quite reasonable question allows us, indirectly, to highlight the resiliency of the entire platform and its value to you as a customer. We genuinely believe this platform provides rock-solid Default Deny security with Default Allow usability.

The cybersecurity industry is seeing a spike in advanced attacks – sophisticated malware capable of evading detection and analysis by various systems including bare metal and hybrid virtualization systems, emulation systems, intelligence based systems and more. Several recent malware and vulnerability proof of concepts show real world defeats of such systems. If we look at well-publicized exploits such as VENOM and other recent malware campaigns that have been designed to escape and take over hybrid virtualized systems such as we saw in the well-publicized KVM, Xen and VirtualBox cases, we can clearly say that malware creators are far from being beaten into submission. In *these* systems, once malware escapes the guest OS and gains access to the host OS running the hypervisor, it is, essentially, ***game over.***

The container's main purpose is not detection, but simply to isolate an unknown process or executable until Comodo's local and cloud-based analysis solutions can determine a verdict.

Unlike most systems, however, Comodo's Automatic Containment has no hypervisor, nor the unique attributes that malware needs to identify the security system it's trying to defeat in order to escape. Comodo Advanced Endpoint Protection™ includes our patent-pending automatic containment technology, which, justifiably, continues to garner a lot of attention thanks to its innovative design and outstanding functionality, but it is in many ways just one of a number of interlocking pieces that together form the foundation for Comodo's true Default Deny Platform. The container's main purpose is not detection, but simply to isolate an unknown process or executable until Comodo's local and cloud-based analysis solutions can determine a verdict.

Inside *Automatic Containment*™

Comodo AEP implements a single container (OS virtualization) model that includes an exact copy of the endpoint machine, including the kernel. This is one of the main reasons startup performance is so fast, in stark contrast to almost all CPU-draining, system-slowing VM systems. In the Comodo model, whenever a process or executable (PE) is run in containment, often referred to as "jailing", the analysis system sits between the PE and the shadow resources it calls – including CPU, memory, registry, file system and more.

Endpoint Protection
Automated Containment
Global Threat Intelligence
True Default Deny Platform
Endpoint Detection and Response

If the PE turns out to be malicious code and attempts to exploit the machine, that action will occur *entirely within the container,* and affect only the shadow resources provided and NOT the native machine, *nor any of the native resources required to actually compromise the endpoint itself*.

That being said, in defensive security it's wise to assume that all systems will, eventually, be compromised. Relying upon any one strategy – whether heuristic pattern matching, sandboxing, signatures or cloud intelligence (IOC/IOA) – ensures that the system *will be exploited*, the only real question is *when*.

In contrast, Comodo's true Default Deny Platform is both designed to efficiently detect and prevent attacks in our tightly integrated model of EPP, EDR, Automated Containment and global threat intelligence, *but has also been carefully architected to continue working if any individual component fails or is defeated*.

If the Default Deny Platform is the whole, then Automatic Containment is a part of that whole. Again, an important part to be sure, but those who think that Automatic Containment is the entire story are missing the bigger picture. We believe that trying to perpetually contain all unknowns is insufficient and unrealistic. Full system-wide security architecture is required, and thus has been built into Comodo Advanced Endpoint Protection and our other cybersecurity solutions.

Outside of Containment

When the Comodo Client™ is installed on the endpoint system, the majority of components apply system-wide, while others only exist within the container, sometimes both (if so configured).

Application Control

Comodo is the world's largest certificate authority. This provides unique visibility into known good publishers, applications and hashes that match bona fide software available for download and installation. Such system processes and executables receive a verdict of **Trusted** after they have been verified as non-malicious by our proprietary local and cloud-based file assessment systems (more on those in a moment).

Unlike malware detection-based systems that interrogate everything, thus negatively impacting usability and performance, our deep intelligence on known good executables improves the user experience and increases the scalability of our security solution. *This process occurs on the native system, outside of our Automatic Containment*.

Integrated Threat Intelligence

Leveraging over 85 million endpoint installations and Comodo Threat Intelligence Labs™ (CTRL)'s real time global intelligence, Comodo AEP is the beneficiary of a truly remarkable knowledge base. With an extremely robust blacklist and whitelist, and the corresponding deep intelligence regarding known good and known bad files, all that's left are the unknown PEs, which are automatically contained and assessed using static, dynamic and human intelligence (when needed), leading to a good or bad verdict, 100% of the time.

Within AEP, the Comodo Client is able to crowdsource global threat intelligence in real time to ensure that malware and adversaries seen elsewhere by our install base, or by our research community, are fully blocked from compromising your endpoints. This complements local blacklisting of known threats and ensures a verdict of ***malicious***, preventing malware the chance to run unfettered on Comodo AEP-protected endpoints. Again, this process occurs on the native system outside of our automated containment. In the unlikely instance of an escape or an incorrect positive verdict, Comodo AEP would apply local and global threat intelligence to detect, protect and notify IT of any unusual activity.

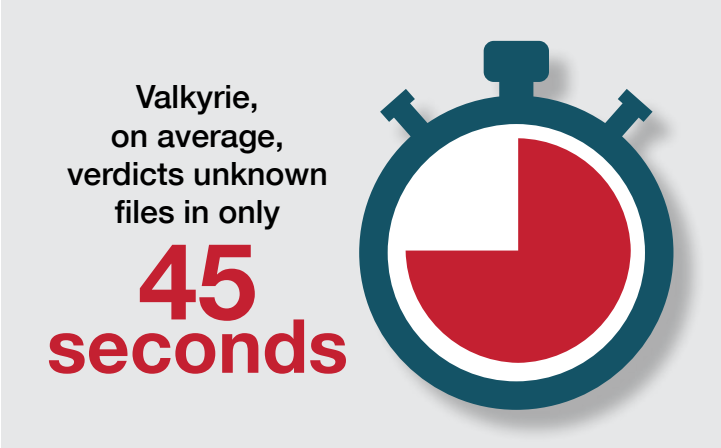
Machine Learning/AI

Comodo AEP includes VirusScope™ on the local level, which applies machine learning and algorithmic based detection – in essence, math – using multiple techniques such as vector machines, naïve bayes, decision trees, random forest classifier, linear discriminant analysis, stochastic gradient descent, hidden markov models, neural networks and more. VirusScope uses these recognizers to analyze behavior and actions indicating malicious intent or behavior, and thus a pending attack. By default, VirusScope employs machine learning only inside of the container. However, VirusScope may also be enabled, by profile, to monitor the entire system both ***inside*** and ***outside*** of Automatic Containment.™ Machine learning is able to identify both escape attempts from inside the container and, in a hypothetical case of escape, from outside of the container – again, providing IT with detection, protection and notification of the incident.

Cloud Integrated Sandboxing and Expert Human Analysis

Unknown PEs are placed into Automatic Containment while being submitted simultaneously to VirusScope, as discussed above, as well as to Valkyrie,™ Comodo's cloud-based file analysis platform for rapid assessment. Valkyrie provides an accelerated verdict to limit the time a PE spends in containment. Without even running the executable, Valkyrie uses more than 26 groups of over 1,000 static analysis detectors to identify embedded links, malicious libraries, system calls, extractable links, unpackers and more. In parallel, Valkyrie's dynamic analysis performs behavioral and environmental analysis (in the cloud) to detect anti-VM evasion,

escape attempts, mass sleep calls, registry changes, API calls and more. Fully automated, Valkyrie delivers the great majority of verdicts, on average, in only 45 seconds.



No Expensive Managed Services

Comodo AEP is the first solution to fully integrate expert human analysis without requiring an expensive managed service. This is possible by leveraging Comodo's robust whitelist and blacklist to limit the analysis target down to just unknown files. And so, in the event that static or dynamic analysis fail to reach a verdict, Comodo AEP uniquely sends those few unknowns to our expert human analysts to determine the final verdict. Furthermore, when the initial endpoint verdict is returned, your entire enterprise deployment is automatically updated. So, at some time in the future, if the same malware attempts to enter the network, it will now be recognized as *malicious* and will be blocked from running on any endpoints on all Comodo-protected networks. This all occurs VERY quickly in the Valkyrie file analysis platform, usually within 45 seconds for over 90% of the verdicts, and within 2 hours for human expert assisted verdicts. In essence, this is a second layer of analysis alongside VirusScope's local analysis and all takes place while the unknown file is, briefly, in Automatic Containment.

Traditional EPP Security

Comodo AEP integrates a comprehensive suite into Comodo's true Default Deny Platform. This includes an award-winning Host Firewall and mature Host Intrusion Prevention System (HIPS). Both of these components provide a robust set of access controls, heuristic analysis, detection and prevention that include disk, memory, processor, kernel and network-based protections. HIPS, in particular, monitors inter-process memory access, OS event hooks, device driver installations, process executions and terminations, DNS/RPC client calls and Windows Message Service between executables. HIPS also monitors COM interfaces, registry keys and protected files/folders. As part of HIPS' standard default protections, critical object access is blocked directly to physical memory by an executable, as well as to the monitor and disks in addition to attempts by the PE to access keyboard and mouse. Both the Host Firewall and HIPS run on the native system, outside of our Automatic Containment.

All of which is to say that while no malicious file has yet escaped our lightweight but powerful containment system, if that WERE to happen, the rest of Comodo Advanced Endpoint Protection's interlocking defenses would kick in and tackle the problem, keeping things **game on** vs. **game over**.

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals, to mid-sized companies, to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in New Jersey and branch offices in Silicon Valley, Comodo has 12 international offices across Europe and Asia.

Comodo Group, Inc., 1255 Broad Street, Clifton, NJ 07013 United States
Tel: +1 (888) 266-6361 | Tel: +1 (703) 581-6361 | Fax: +1 (973) 777-4394
sales@comodo.com | enterprise.comodo.com