Comodo Containment Technology

COMODO
ENTERPRISE™

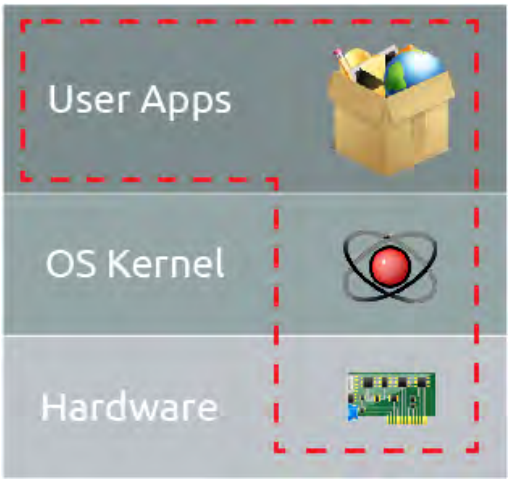
There are three types of files: the *good*, the *bad* and the *unknown*. Approaches such as antivirus, blacklisting and whitelisting handle the known *good* and the *bad* files – but what about the *unknown* files?

Unknown files may be perfectly harmless and required for system functionality or they may be dangerous zero-day threats or APTs that cause mega breaches. These unknown files are being recognized as one of the biggest security threats to organizations today, catching the attention of chief executive officers, chief information officers and chief security officers, as well as the board of directors. Your cyber security solution must be able to detect the difference to both prevent breaches and enable productivity.

Comodo's Solution: Containment Technology

Comodo containment technology defeats zero-day attacks better than any other security technologies on the market today. Comodo's solution uses a combination of process virtualization, whitelisting, file lookups, behavior analysis and traditional AV scans to intelligently, accurately and quickly identify unknown files and processes. Our technology authenticates every executable and process that requests runtime privileges and prevents them from taking actions that compromise user or system data.

Once identified, any unknown processes are launched inside a secure, virtual environment that does not allow access to system resources or user data. Processes in containment read and write to a virtual registry, file system, OS core and hardware. Malware in containment cannot access user data or damage the protected system and are deleted as soon as the user closes the container. If the processes are determined to be good, they are automatically released out of the secure container, contingent upon the administrator's policy.



Comodo containment technology meets the key business deliverable of providing total protection against zero-day threats *while having no impact on end-user experience or workflows*. Whether the unknown files are malicious or safe, they run in the sandbox just as well as they would on the system. However, they cannot damage or infect the systems because they cannot access the underlying system. This allows safe applications the freedom to run as needed while denying malicious applications the system access they require to deliver their payloads.

Comodo Auto Sandbox

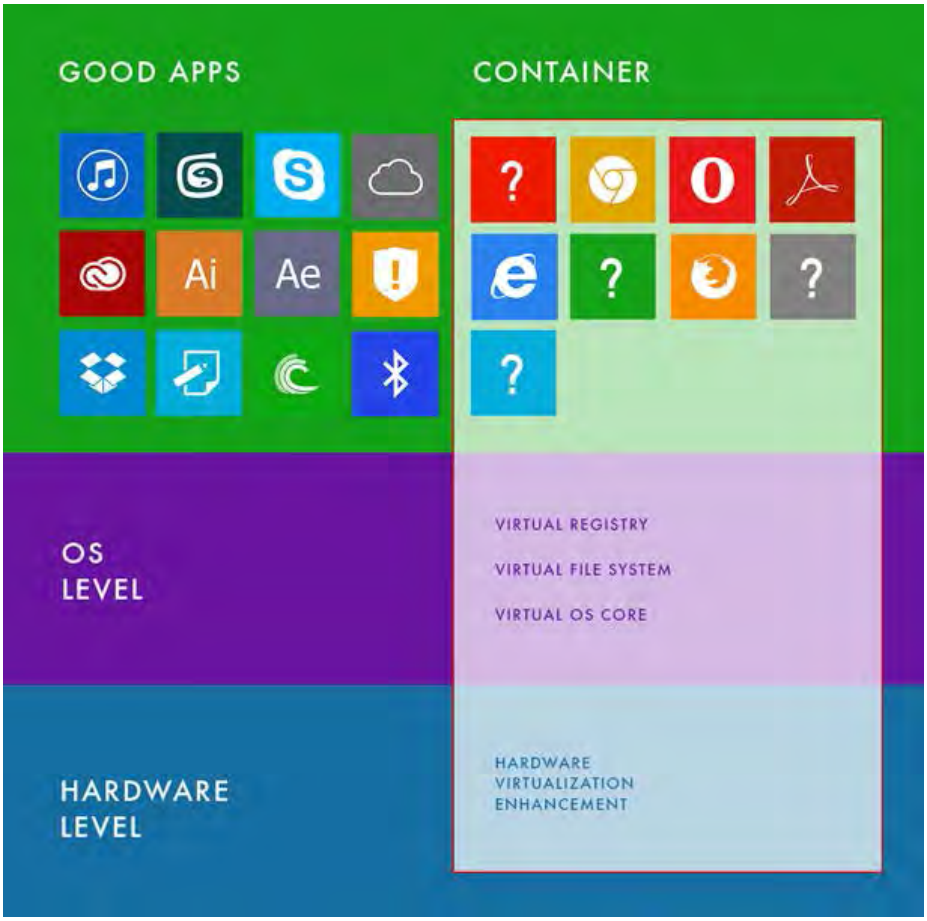
Comodo Auto Sandbox is not limited to specific applications. Comodo has flexibility on use cases. User can specify to auto sandbox only specific applications (unknown files, executables, scripts, PDFs) or choose to auto sandbox all files with no impact on performance.

Comodo Auto Sandbox leverages CPU virtualization for additional security if available but otherwise it uses runtime user-space process isolation and is not dependent upon the CPU virtualization technology to operate. This technology benefits from the resource isolation offered by virtualization without the vulnerabilities.

Comodo Auto Sandbox uses both software and hardware level virtualization technologies which makes it more secure and hardware agnostic.

Comodo Auto Sandbox is compatible with all remote desktop software.

Comodo Threat Prevention Architecture



Legacy security applications, by default, allow access to the host system. Contrarily, Comodo's containment technology automatically runs any unknown files in a virtual container without access to outside resources.

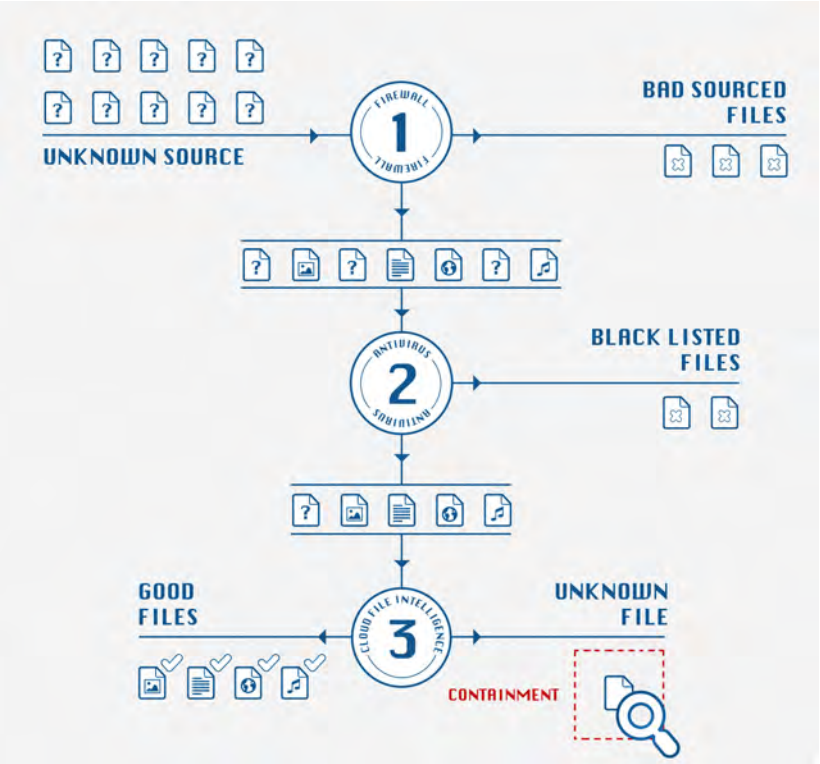
The Trust Decision Engine

Comodo's holistic security architecture leverages numerous threat prevention technologies to intelligently classify and route all unknown files and processes to our secure container. Rather than containing *all* user processes of a certain type, Comodo's proven and trusted decision engine identifies and contains any and all non-whitelisted and non-blacklisted processes that have not yet exhibited malicious behaviors. This delivers a secure threat prevention strategy for unknown files without overcommitting system resources to contain safe processes which present no danger. Security is further enhanced by the fact that even whitelisted processes running on the host are still subject to policy-driven behavior monitoring from Comodo's AV and Defense+ systems.

When a file is requested from an external source, it first passes through Comodo's packet filtering firewall which is installed on every endpoint. As a first layer of protection, this eliminates any threats housed within malformed data packets.

After that, every single file that enters an endpoint passes through the following security inspections on the local machine:

- Antivirus scan
- HIPS heuristic check
- Buffer overflow check



If the file is determined to be malicious, it is quarantined or deleted and the administrator is notified. If the file is not determined to be malicious, it passes onto another round of analysis – Cloud File Intelligence.

Comodo's File Look-Up Server (FLS) checks the very latest whitelist and blacklist databases. These checks are run in real-time and deliver near instantaneous feedback to the local machine – end users do not experience delay.

A digital hash of the unknown process or file is created and uploaded to the FLS to check whether the file signature is present on the latest databases which contain the global blacklist of all known malware signatures and a whitelist of known safe file signatures.

- If the hash is discovered on the blacklist then it is malware. The result is sent back to the endpoint and the process is quarantined or deleted.
- If the hash is not on the latest blacklist, its signature is checked against the latest global whitelist. If the hash is discovered here then the file is considered safe to run on the host machine. The local whitelist will be updated accordingly.
- Comodo has one of the world's largest whitelists.

Files and processes that emerge from the inspections above with a status of "unknown" will be automatically launched in the sandbox on the local machine. If the administrator enables the option, such unknown files are simultaneously uploaded to Comodo's Instant Malware Analysis servers for another round of checks:

- Each submitted process undergoes further antivirus scans on our servers.
- Our remote servers submit each file through behavior analysis to identify malicious intent. Unknown executables are detonated in a virtual, cloud-based environment; all actions are monitored and analyzed. Processes spawned, files and registry key modifications, host state changes, and network activity are recorded. Such proactive behavior analysis can often accelerate the identification of zero-day malware.
- If a process is found to be malicious by our Instant Malware Analysis servers, the signature is immediately returned to all networked endpoints. The file is quarantined or deleted from all managed endpoints (depending upon policy) and the local and global blacklists are updated.
- If no malicious behavior is recorded by Instant Malware Analysis, the file remains contained on the local endpoint and is submitted to our technicians for in-depth analysis. To preserve the integrity of the global whitelist, automated behavior analysis can add signatures only to the global blacklist. The status of 'safe' can only be granted to a file after in-depth checks by our technicians (or if the local administrator adds it to the local whitelist).

Comodo's containment technology can be deployed alongside any third party AV, firewall and file lookup technologies.

Comodo Containment Technology For the Real World

There are many container-based solutions on the market today, with each vendor claiming to provide automatic and complete protection against threats while simultaneously reducing how much time administrators need to spend dealing with malware. All this is supposedly achieved without interrupting end-user workflows, without requiring additional expense and without hogging network or system resources. However, the ability of any solution to deliver on these promises is predicated on the core architecture of their containment technology.

Contain only what needs to be contained.

Comodo's solutions delivers all-encompassing protection for endpoints at a fraction of the bandwidth of competing solutions by detecting all unknown processes and focusing containment on these items.

Our solution leverages the world's largest signature whitelist of known good files to identify processes which are safe to run on an endpoint. Files can only be added to this list after undergoing an intense testing process run by Comodo's renowned research labs. 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. This provides significant resource efficiencies over solutions that aim to contain 'all user initiated tasks and content' with little to no attempt to differentiate between good, bad and unknown files.

Intelligent Containment

Both Vendor A and Vendor B present virtualization technology as a malware silver bullet to disguise the absence of other security technologies from their products.

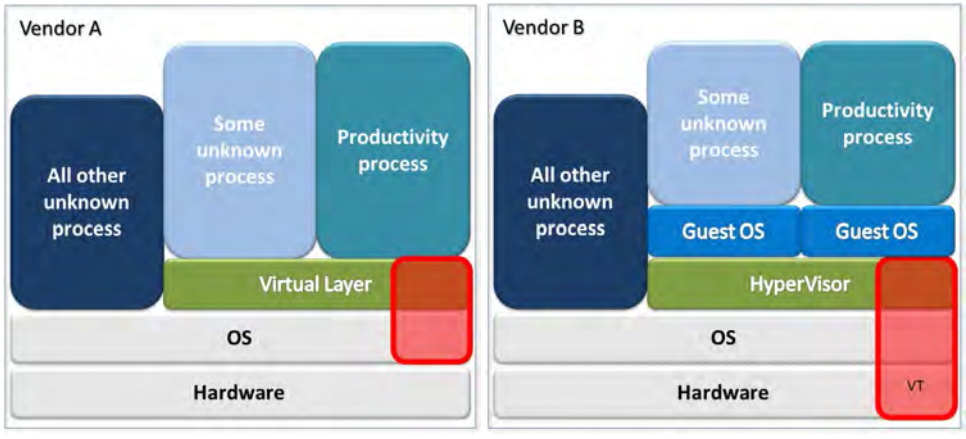
Vendor A's strategy is one of selectively containing 'targeted applications' such as browsers, PDF readers and office applications. The drawbacks are that its solution only supports certain browsers and applications, and that it does not have mechanisms in place to detect and contain malicious processes from other sources. While Vendor A's solution may work fine under laboratory conditions, it does not fare in the real world with a large number of end users running a unique and ever-changing set of applications. The setup requires constant fine tuning and may require administrators to 'lock down' the applications and services that users are allowed to run. Comodo's containment technology allows administrators to selectively run any application they choose inside a virtual container and has no 'supported applications' restriction. Additionally, Comodo's solution leverages several real-time technologies to detect and automatically contain unknown processes *anywhere* on the host system. Comodo contains ALL unknown processes, not just some.

Vendor B solution uses a different approach, one of creating multiple 'Micro VM's' to contain each user generated process. Vendor B is type II VM which spawns running a separate, virtual instance of the guest operating system for every single contained process, all controlled by a Xen Hypervisor running on the host operating system.

Despite its claims, each instance of a virtual environment running on an endpoint increases the demand on the resources of that endpoint. This can lead to system slowdown, workflow interruptions and often to the expense of upgrading endpoint hardware. While this may not cause undue concern on a single machine, it leads to significant additional costs if the solution is deployed on a network of hundreds or thousands of machines. Vendor B requires approximately 1.5 GB of *free* memory to launch their microvisors. If this memory is not available, *then the virtualization does not take place* – threats are allowed into the host environment. Worse still, there are no real-time warnings to alert the administrator that the application is not being virtualized. To run correctly, Vendor B will require every Windows 7 machine to have 8 GB of RAM, which presents a huge problem to many enterprises who have specced their desktop and laptop fleet to 4 GB max.

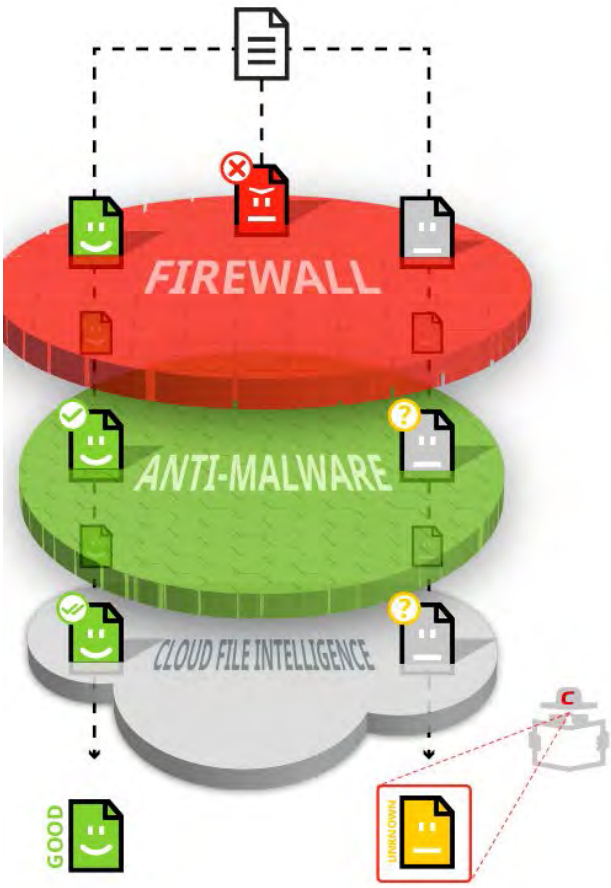
The Vendor B solution also suffers from other significant hardware and software dependencies. Vendor B only supports Windows 7 and requires the Xen hypervisor and Intel VT CPUs in order to work correctly. If the CPU VT extensions are not present, Vendor B's solution does not operate and allows all unknown files into the host environment. Comodo's solution is hardware agnostic and can be readily deployed to PCs and servers running on any processor type. Comodo's containment technology uses the CPU VT extensions for additional security if they are present, otherwise, uses run-time user-space process isolation to effectively contain unknown files.

Like Vendor A, the Vendor B solution has no means to identify unknown files and relies on sandboxing processes from a *limited* set of supported applications and file formats (this is phrased as "Email attachments and all common document formats), which leaves potentially malicious processes uncontained from other sources. The absence of mechanisms to control unknown processes throughout the host relegates both Vendor B and Vendor A to the status of partial solutions which have been erroneously marketed as panaceas for all threat vectors.



Unlike other vendors, Comodo's containment technology is genuinely proven in the field and can be introduced to an enterprise network without additional investment in hardware or software. It is already being used to protect over 85 million users worldwide via our enterprise and consumer security products. Our technology has consistently topped the Proactive Security Challenge by Matousec, security testing firm, and regularly achieves perfect protection scores and Editors' Choice Awards from magazine reviews. To illustrate the strength of our conviction, we have introduced a "$5,000 virus-free guarantee" and have never once had to pay out.

The Importance of Solution Interoperability



It is well documented that today's malware landscape is a dynamic and unpredictable environment which confronts even the best prepared CSOs with unique challenges on a daily basis. Best practices and preparation are everything; to many administrators this strategy necessitates the deployment of a diverse security toolkit using technologies from a range of vendors. Such a heterogeneous mix of solutions is not only the de-facto reality of most networks, it is an approach that should be wholly applauded. It mitigates any single point of failure that could allow a threat to execute because of a flaw running through a single-vendor suite of software. Each solution will be deployed to meet a specific threat and, while some of these security technologies may functionally overlap, it is the better strategy to go with more rather than less. This brings us to a key requirement of any enterprise security software – interoperability.

Any new security technology must harmonize well with the tenured portfolio of solutions running in a network and any new solutions the administrator chooses to deploy in the future. Because any potentially damaging processes are isolated in their own operating environment, our product is 100% compatible with any other security solutions that administrators choose to run on the endpoint or at the network level.

Many vendors go to lengths to stress their products are compatible with products X, Y and Z. Comodo's containment solution, on the other hand, has no known incompatibilities with major productivity or security software. Purely in the interests of addressing compatibility, our containment technology is compatible with all Adobe applications, all Microsoft Office applications, all Open Office applications, all versions of Java, all versions of Silverlight, all major mail clients and all major antivirus solutions.

Comodo is the Trustworthy, Proactive Choice

In response to the next-generation level of cyberattacks, Comodo offers the next generation of cyber security solutions. Comodo's fully integrated platform, Run-Time Automatic Threat Containment (RATC), uses Comodo Antivirus, or leverages existing antivirus, with whitelisting to filter out the known bad and good files from the unknown files. Then Default Deny Protection™ automatically contains and runs the unknown files in a secure container without any risk of infecting the host system. Comodo's innovative containment technology bolsters and protects business networks.

Additional Information

Visit our website www.enterprise.comodo.com

Discuss your security needs with a Solutions Consultant, email EnterpriseSolutions@comodo.com

BENEFITS

Automatic threat containment: Prevents local and network malware outbreaks by detecting and automatically containing unknown files in an isolated environment separate from the underlying operating system and user data.

Application containment: Administrators can elect to run popular but frequently-targeted applications inside our secure virtual container with no loss of usability. Examples include browsers, mail clients, Java and popular productivity suites such as MS Office.

Whole host protection: All processes running inside or outside the container are subject to strict behavior monitoring to identify anomalous and malicious activity patterns.

Integrated threat intelligence: Administrators have the option to upload suspicious files or potential false positives to Comodo's Valkyrie malware labs for additional analysis and verification.

Complete awareness and control: When paired with Comodo Endpoint Security's management console, Comodo containment solution gives administrators panoramic visibility and control over incidents across all local and remote networks.

Interoperability: Comodo containment technology runs without conflict with any existing security or productivity solutions that may already be installed on a network. Users are free to use their systems as they wish under complete protection without interruption.

Resource friendly and ready to go: Intelligent containment and real-time identification of unknown processes anywhere on the host make Comodo the only solution to offer complete protection without the need for additional hardware investments.

Reduce IT overheads: With Comodo's 360o threat prevention solution, administrators no longer need to devote excessive staff time to the investigation and remediation of malware outbreaks.

Hardware agnostic: Comodo's containment solution is not dependent on a company exclusively using certain processor types in their endpoints.

Battle tested in the real world. Comodo's containment technology is borne out of over 10 years' experience perfecting a holistic security system which is currently being used by over 85 million real-world users.

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 Security Solutions, Inc.

1255 Broad Street
Clifton, NJ 07013
United States

Comodo CA Limited

3rd Floor, 26 Office Village
Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ
United Kingdom

Comodo Turkey

Büyükdere Caddesi Yapı Kredi Plaza C
Blok No:40
41 Kat 17 Levent, Istanbul
Turkey

1-888-256-2608

enterprisesolutions@comodo.com