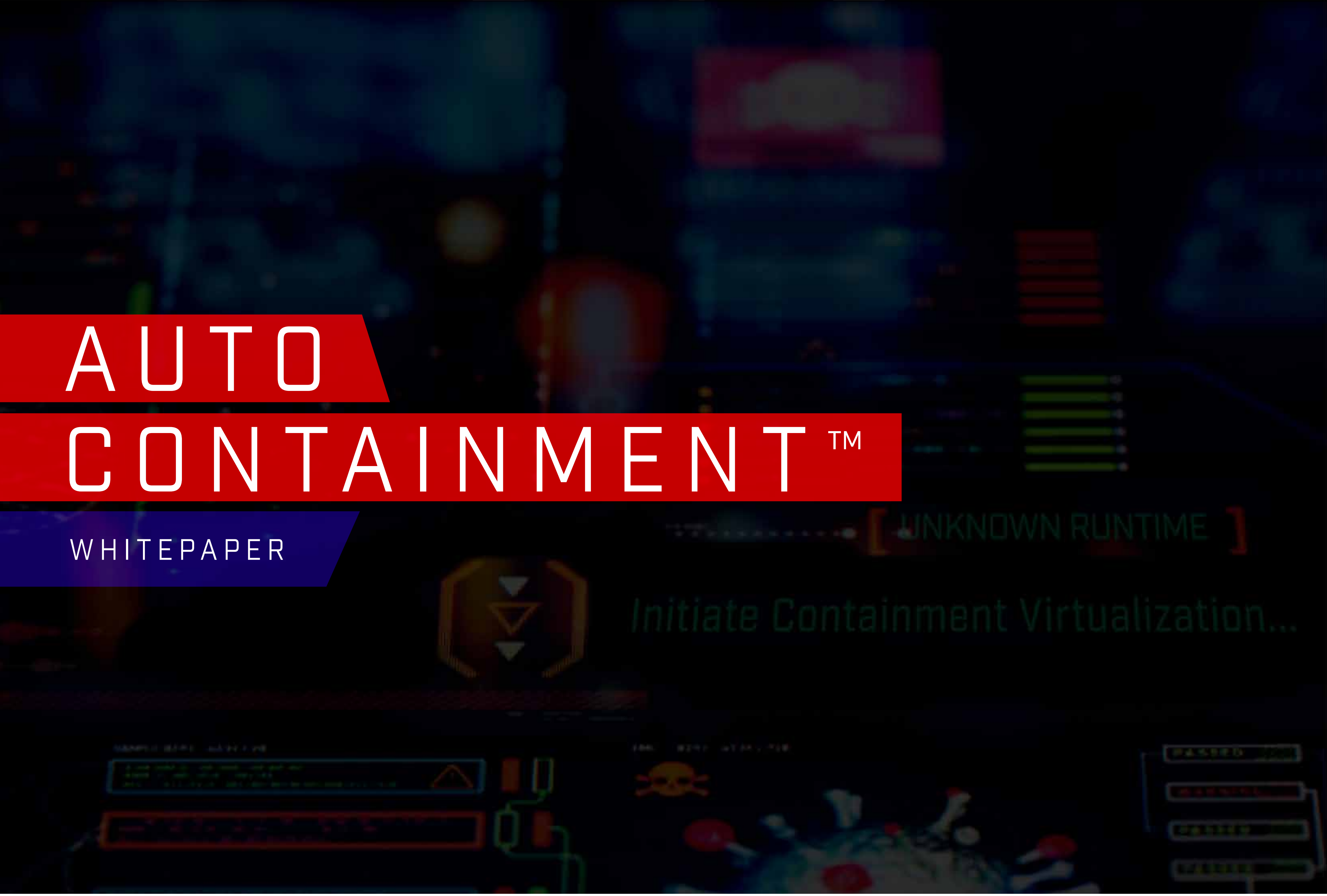
AUTO CONTAINMENT™

WHITEPAPER



COMODO

PROVEN SUCCESS IN PREVENTING BREACHES

TABLE OF CONTENTS

UNDERSTANDING WHY NOTHING ELSE WORKS

When it comes to securing your enterprise endpoints, it's important to have a foundational understanding that there are **three types of files**: the **good**, the **bad** and the **unknown**. Approaches such as Antivirus (both vendor-branded "next gen" and legacy detection-based), Blacklisting and Whitelisting handle the known good and the bad files – **but what about the unknown files**?

Regardless of the "next gen" nature and effectiveness of any new pre-execution, detection based solution, there will always be a certain number of unknown files, executables and code which by default are allowed to run on the host if not deemed malicious. The problem is that detection-based solutions will never detect 100% of what is malicious, or 100% known to be good. 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. Your cyber security solution must be able to detect the difference to both prevent breaches and enable productivity.

As a key component of Comodo Advanced Endpoint Protection (AEP), Comodo Auto-Containment technology defeats zero-day attacks with no impact to the end user experience, better than any other security technologies on the market today. Comodo's solution uses a combination of process virtualization, whitelisting, machine learning, behavior analysis, and advanced static and dynamic threat cloud analysis (Comodo Valkyrie) to accurately and quickly deliver a 100% trusted verdict for unknown files and processes. Pre-execution, our technology authenticates every executable and process that requests runtime privileges, and if not 100% known-good or known-bad, is deemed unknown, and launched inside a secure, virtual containment environment that does not allow access to system resources or user data.

HOW 'NEXT-GEN' AND LEGACY ANTIVIRUS WORKS

File Executed Inside Network with Traditional Endpoint Security

Attackers create payloads to deliver to targeted or global campaign.

Blacklist Allows to the New Signature to Pass

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

Machine Learning has not been trained the New Signature

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

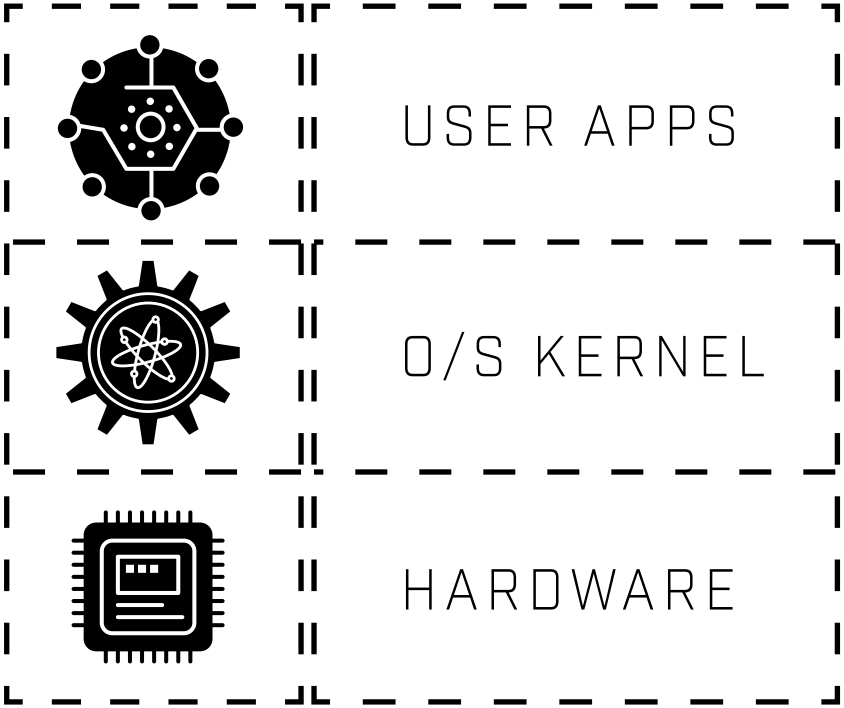
File Executes on the Endpoint to Infect the Network

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

THE ONLY SOLUTION TO STOP THE DAMAGE

Comodo Auto 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, our technology is architected so they run and perform in the autocontainment just as well as they would on the actual host 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.

Processes in containment read and write to a virtual registry, file system, OS core and hardware. Therefore, malware in containment cannot access user data or damage the protected system and are deleted by default upon receiving a "Malicious" verdict. Yet while in containment, a full forensic analysis is recorded, which may then be configured for delivery to your SIEM and Security Operations Center (SOC). A kill-chain style report for every malicious incident is then made available for review in the customer's Comodo Valkyrie console. Conversely, if unknown processes are given a final verdict of "Good" while in Containment, they are automatically allowed to run on the host in subsequent sessions, contingent upon the administrator's policy. This concept of intelligent containment (instead of perpetual containment) is essential to ensure the usability of the machine and user experience remains completely unchanged. Yet the user may now click on anything without the risk of infection and subsequent enterprise breach.

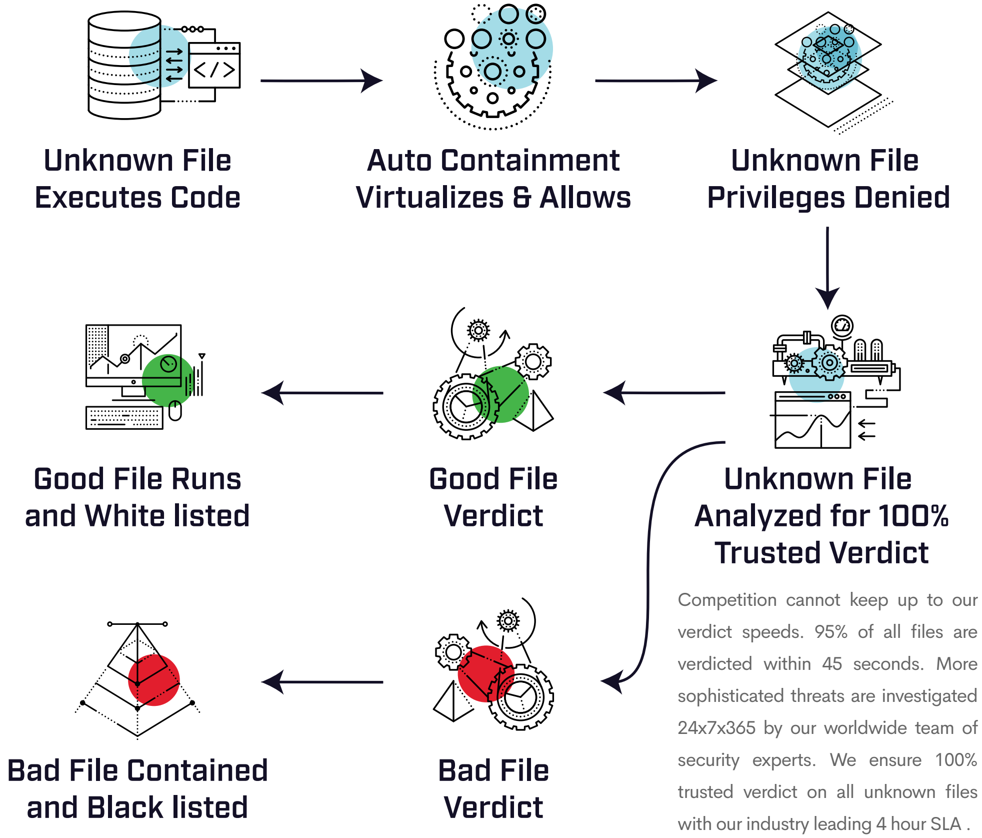


THE ONLY SOLUTION TO STOP THE DAMAGE

The idea to remove the burden of detection to completely secure the user, while not changing the user experience, over-burdening the machine and creating nightmare deployment scenarios, is not a new one. But it's a value proposition the endpoint security industry has failed to truly deliver. Other isolation and containment strategies that deny access the host by default (Default Deny), suffer from significant high-resource and usability challenges, and typically involve monthsto- years long deployments, incurring greater costs than the solution ultimately saves. These solutions launched in the market to great fanfare given the game changing potential to remove the burden of detecting what is bad from securing the endpoint.

Many enterprise security teams tested or partially deployed these solutions, and most ultimately were forced to abandon their default deny strategy. Some settled for next-gen, pre-execution detection endpoint protection solutions which employ advanced detection strategies beyond the traditional signature based approach. While these new solutions may detect at a better rate than legacy AV, unknown files and processes are still allowed to run on the host by default, due to the pressure enterprises have to preserve usability.

Comodo Advanced Endpoint Protection with patented Auto Containment has engineered the industry's first Default-Deny endpoint protection solution, which is practical and feasible for the enterprise to deploy. We call this "Default-Deny Security, with Default-Allow style usability."



Unknown File Executes Code

Auto Containment Virtualizes & Allows

Unknown File Privileges Denied

Unknown File Analyzed for 100% Trusted Verdict

Good File Verdict

Good File Runs and White listed

Bad File Verdict

Bad File Contained and Black listed

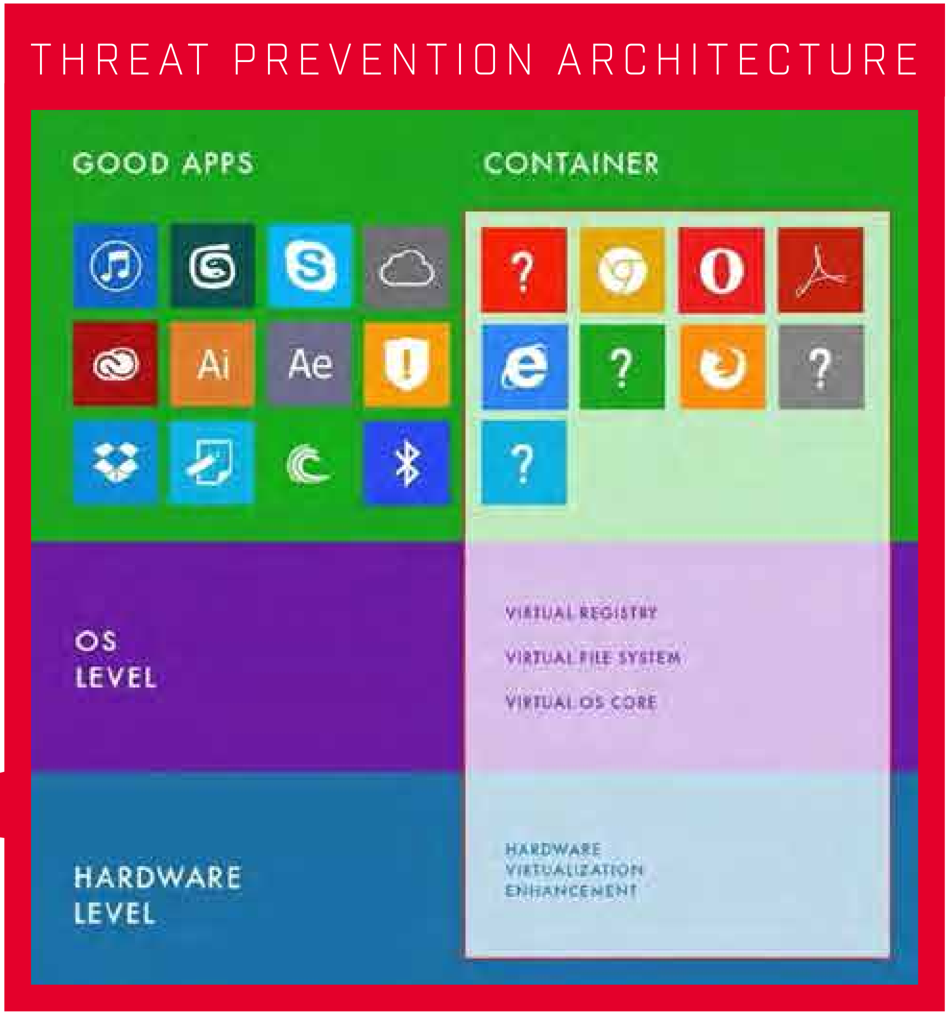
Competition cannot keep up to our verdict speeds. 95% of all files are verdicted within 45 seconds. More sophisticated threats are investigated 24x7x365 by our worldwide team of security experts. We ensure 100% trusted verdict on all unknown files with our industry leading 4 hour SLA .

COMPATIBILITY AND INTEGRATION

Comodo Auto Containment is not limited to specific applications. Comodo has the flexibility to fully support all use cases enterprise demand. Admins can specify Auto Containment for only specific applications (unknown files, executables, scripts, PDFs) or choose to Auto-Contain all files with no impact on performance.

Comodo Auto Containment is not dependent upon the CPU-virtualization technology to operate, yet can be deployed to leverage CPU-virtualization for additional security if required. Otherwise, Auto Containment uses runtime user-space process isolation. This technology benefits from the resource isolation offered by virtualization without the vulnerabilities. Auto Containment uses both software and hardware level virtualization technologies which makes it more secure and hardware agnostic. Moreover, Auto Containment is compatible with all remote desktop software.

THREAT PREVENTION ARCHITECTURE


THREAT PREVENTION ARCHITECTURE

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

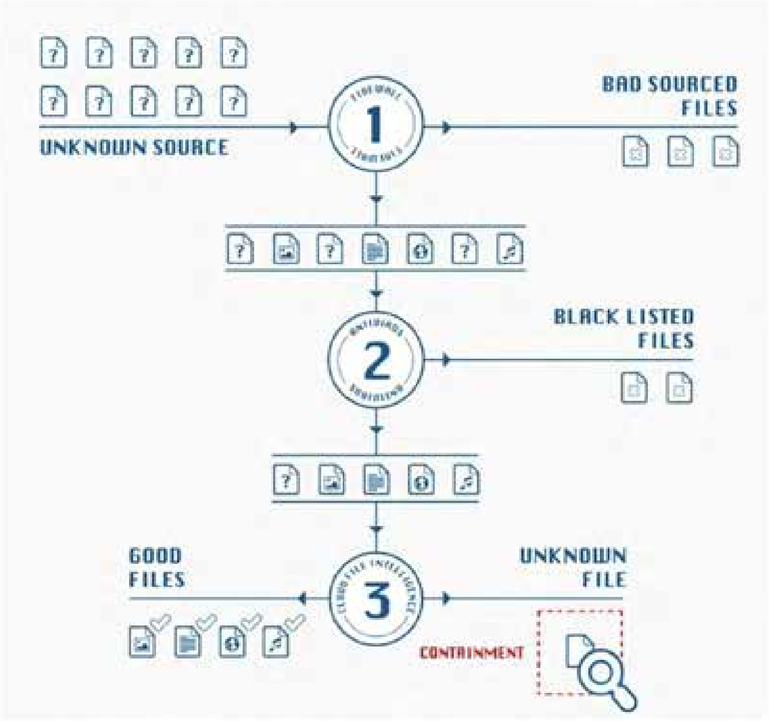
VALKYRIE: 100% TRUSTED VERDICT DECISION ENGINE

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 verdict decision engine, called Valkyrie, identifies and contains any and all non-whitelisted and nonblacklisted 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 Advanced Endpoint host monitoring, HIPS, firewall, 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 and endpoint passes through the following security inspections on the local machine:

ANTIVIRUS SCAN - HIPS HEURISTIC SCAN - BUFFER OVERFLOW CHECK



If the file is determined to be malicious, by customizable policy, it is quarantined or deleted and the administrator or SIEM is notified. If the file is not determined to be malicious, it passes onto another round of analysis.

IN DEPTH | FLS TECHNOLOGY

Next, 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.

- With 3% of all user base worldwide, 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 Comodo Auto Containment on the local machine.

While in Auto Containment, such unknown files are simultaneously uploaded to Comodo Valkyrie, where several static and dynamic forensic analysis tasks are performed in effort to quickly issue a trusted verdict, Good or Malicious:

- Each submitted process undergoes further real-time analysis powered by Valkyrie global threat cloud, which is constantly collecting machine learning and AI derived IOCs from the nearly 90 million enterprise and consumer user installations worldwide.

- 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 Valkyrie, a Malicious verdict is assigned, and a unique identifier IOC 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 Valkyrie, the file remains contained on the local endpoint and is submitted to our Global SOCs for in depth human analysis.

- To preserve the integrity of the global whitelist, automated behavior analysis can add signatures only to the global blacklist. The status of 'Good' 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).

CONTAINMENT IN 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 everchanging 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.

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.

CONTAINMENT IN THE REAL WORLD

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 specified their desktop and laptop fleet to include a 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 isolating 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 Advanced Endpoint Protection platform, with the essential Auto Containment, allows the enterprise to realize a practical Default Deny security posture at the endpoint without any compromise of user productivity. Default Deny Protection™ automatically contains and runs the unknown files in secure Auto Containment without any risk of infecting the host system. Comodo's innovative containment technology can finally deliver on the isolation and containment promise for the enterprise.

KEY 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 Dragon Platform 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.

START 30-DAY FREE TRIAL

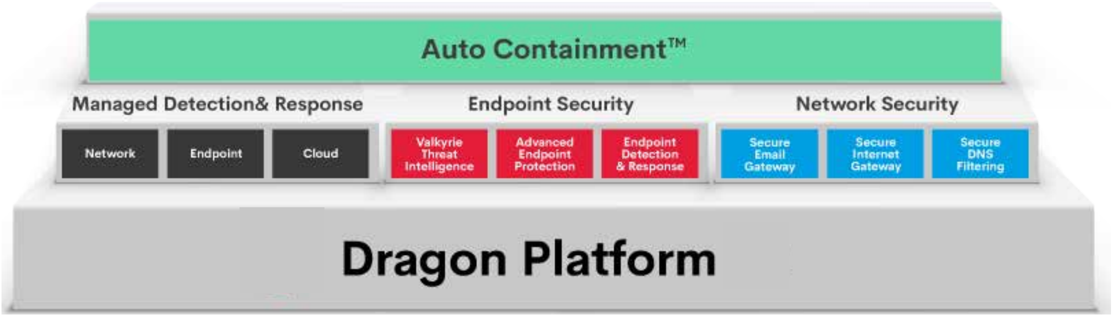
If you already have a CAM account, contact your Customer Success Manager for more information on how to integrate with Dragon Platform.

ABOUT US

In a world where cyber attacks are inevitable, Comodo provides active breach protection with its cloud-delivered, Zero Trust platform. The Comodo Dragon platform provides a Zero Trust security environment that verdicts 100 percent of unknown files. The platform renders an almost immediate verdict on the status of any unknown files, so it can be handled accordingly by software or human analysts. This shift from reactive to proactive is what makes Comodo unique and gives them the capacity to protect your business—from network to the web to cloud—with confidence and efficacy.

We have solved the malware problem with our patented technology, Auto Containment. Only Comodo stops damage from all malware, zero-day, unknown and known. We protect and defend your systems and data. We replace multiple solutions. Comodo can claim 100% effectiveness in eliminating cyber risk on endpoint, web, and cloud.

TRUSTED CUSTOMERS



COMODO CORPORATE HEADQUARTERS
200 BROADACRES DRIVE, BLOOMFIELD, NJ 07003 USA
Experienced a breach? Contact us at (888) 551-1531
Visit **comodo.com** for your free 30 day trial