Malware Problem Solved

Advanced Endpoint Protection

COMODO

Advanced Endpoint Protection

Why Traditional Endpoint Solutions Fail

Today, with malware proliferating at an astonishing rate of over 500,000 unknown pieces per day, the legacy approach has been rendered incapable of defending, with detection rates averaging only 45% success rate at stopping malware, and rapidly declining.

The result is you may be allowing the execution of unknown files to run with unfettered access - literally asking for your endpoints to become infected. This is the equivalent of blindly allowing a stranger access to your home, with the freedom to enter every room.

You wouldn't allow this in your home, so why allow this to happen on your devices? In today's world of targeted attacks and advanced persistent threats, all it takes is a single infection to cause damage.

PROBLEM ★★★ SOLVED
PROBLEM SOLVED

COMODO

> In today's world of targeted attacks and advanced persistent threats, sometimes all it takes is a single infection to cause damage.

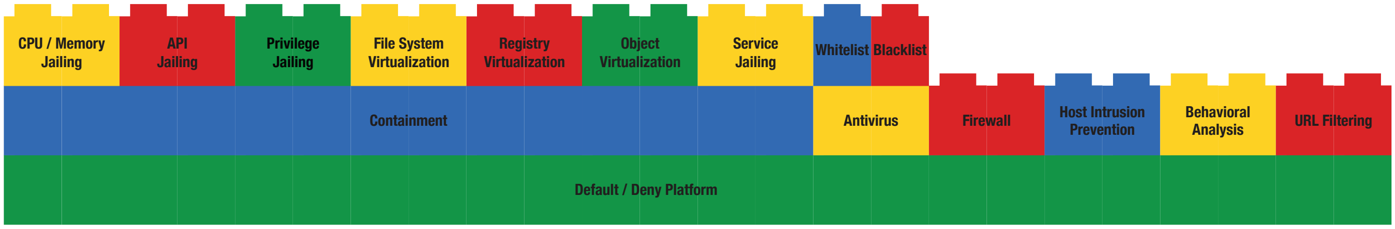
Why Some New Approaches Fail

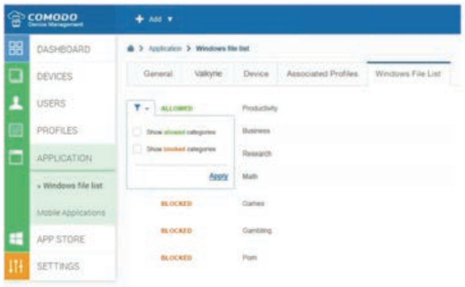
Recently developed approaches have evolved, seeking to expedite the identification of unknown malware and zero-day exploits. Automated behavioral analysis tools such as "sandboxes" run unknown files in virtual environments, in an effort to see if applications have malicious behavior or not. While this has improved the war, the victory comes at a cost in the form of decreased usability for the end user due to introduced delay. More concerning, many of these models allow a window for the initial "patient zero" infection while the automated study of unknown applications is taking place in the attempt to write a signature (vaccine). Unfortunately this patient zero is all an attacker requires to 'pivot' and gain access to sensitive assets in your network.

> "Before using Comodo, we were getting infected with malware and spyware at least 3 times a week. Since Comodo, we've had zero infections."
>
> - Enterprise Customer

Solution

Comodo's Advanced Endpoint Protection solution, utilizes a Default Deny Platform to provide complete protection against zero-day threats, while having no impact on end-user experience or workflows. All untrusted processes and applications are automatically contained in a secure environment, allowing safe applications the freedom to run while denying malware the system access they require to deliver their payloads. In addition, Comodo’s Advanced Endpoint Protection solution is integrated with Comodo’s local, and cloud-based Specialized Threat Analysis and Protection (STAP) engine. This provides an Accelerated Verdict of unknown files into either known good, or known bad, thus keeping unknown files in containment the shortest time of any solution on the market.





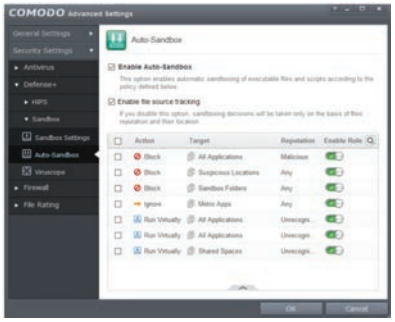
ALLOWED	Productivity
	Business
	Research
	Math
BLOCKED	Games
BLOCKED	Gambling
BLOCKED	Porn

Application Visibility and Control (*Coming Q2 2016)

Gain enterprise visibility and control into what applications users are installing across Windows-enabled endpoints with the new device management capabilities built into Comodo’s IT and Security Manager (ITSM). ITSM allows you to set mobile application policies based on groups such as productivity apps, utility apps, gaming apps, etc. Applications can also be permitted, blocked or allowed to run inside a secure container. Productivity is also increased by disallowing non-critical business applications to run during a specific time or day. ITSM provides for the security of corporate data through comprehensive application management.

Automatic Containment

You can feel confident that only safe applications are running on your network with Comodo’s automated containment technology built on our Default Deny Platform. Desktops are very dynamic. As your users introduce new unknown and possibly malicious applications externally from the device, you can automatically force them to run in isolation, never risking corporate data. Comodo’s automated containment technology is extremely lightweight, has no CPU dependencies, and is application agnostic unlike other containment solutions in the market.



Auto-Sandbox

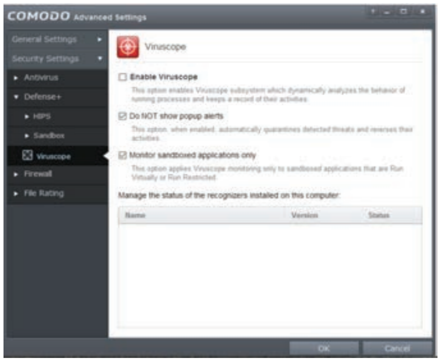
☑ Enable Auto-Sandbox

This option enables automatic sandboxing of executable files and scripts according to the policy defined below.

☑ Enable file source tracking

If you disable this option, sandboxing decisions will be taken only on the basis of files reputation and their location.

□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malicious	●
□	Block	Suspicious Locations	Any	●
□	Block	Sandbox Folders	Any	●
□	Ignore	Metro Apps	Any	●
□	Run Virtually	All Applications	Unrecogni...	●
□	Run Virtually	All Applications	Unrecogni...	●
□	Run Virtually	Shared Spaces	Unrecogni...	●



Viruscope

□ Enable Viruscope

This option enables Viruscope subsystem which dynamically analyzes the behavior of running processes and keeps a record of their activities.

☑ Do NOT show popup alerts

This option, when enabled, automatically quarantines detected threats and reverses their activities.

☑ Monitor sandboxed applications only

This option applies Viruscope monitoring only to sandboxed applications that are Run Virtually or Run Restricted.

Manage the status of the recognizers installed on this computer:

Name	Version	Status

Behavioral Analysis

Identify unknown software applications, quickly moving them to a verdict of known good or known bad with Comodo’s local, and cloud-based Specialized Threat Analysis and Protection (STAP) engine. Comodo’s local STAP layer, VirusScope, first analyzes application behavior and actions running inside or outside of containment, and leverages multiple techniques to determine any malicious intent. Valkyrie, Comodo’s second, cloud-based STAP layer correlates VirusScope’s local view of the file’s activity with a global view. This reduces false positives, false negatives provides an Accelerated Verdict of malware at the endpoint. The result is that unknown files stay in containment for the shortest time of any containment solution on the market.

COMODO

Product Development and Malware Research Teams

Comodo's Default Deny Platform places emphasis on allowing known good applications, denying everything else until a verdict is reached. In order to execute on this strategy, identifying known good and known bad applications is critical. As the #1 largest certificate authority brand in the world, Comodo is uniquely positioned to identify known good software publishers, applications (whitelists); while our installed base of over 85 million users provides the Comodo Threat Research Lab (CTRL) with one of the largest caches of known bad files (blacklists). Our global product development and malware research team has security professionals working 24x7x365 worldwide to ensure that unknown files are rapidly identified before they are able to cause damage.

Santa Clara
Kentucky
New Jersey
United Kingdom
Romania
Ukraine
Turkey
India
China
Philippines

Advanced Endpoint Protection

Comodo has combined our suite of award-winning enterprise-level security products to provide a complete Advanced Endpoint Protection solution. As a fully integrated combination of cloud, and on-premise delivered Mobile Device, Endpoint Security, and Inventory Management solutions, you now have the ability to stop any unknown executable from running on your network with unfettered access.

Comodo Client

Comodo Client delivers a layered suite of protection that is lightweight and scalable. Users can run any application on their endpoint with confidence, having only known good applications running on your network outside of containment. Comodo Client includes:

Endpoint Containment Firewall
Antivirus
Behavioral Analysis (VirusScope)
Specialized Threat Analysis and Protection (STAP)
Web Filtering
Host Intrusion Prevention (HIPS)
Valkyrie Cloud-based Static and Dynamic analysis

Comodo IT and Security Manager

Comodo Advanced Endpoint Protection solution brings a new Default Deny Platform to the table, leveraging automated containment technology as a temporary solution for analysis to verdict unknown files with dual STAP behavioral analysis engines, to determine each unknown file's true state.

In the past, organizations have had to deploy multiple solutions to accomplish these tasks. Today, Comodo has integrated these critical components under a single, unified cloud-accessible Advanced Endpoint Protection management platform.

Comodo's IT and Security Manager allows for the configuration of security policies and visibility into the security posture and health of your enterprise endpoints, while the ITSM Mobile Device Manager and Inventory Manager allow for the remote provisioning, configuration and control of android, iOS and Windows devices.

Perform tasks like restricting what a user can do on a corporate owned mobile phone, determine which unknown applications are running in containment enterprise-wide, remote wipe a device and identify the geographic location of a device.

With Comodo's ITSM, you can even conduct an enterprise-wide search for malware. **Malware Problem Solved.**

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
www.comodo.com/enterprise

COMODO