Why Choose Comodo?

Our revolutionary Advanced Endpoint Protection enables Default Deny Security with Default Allow Usability.

Comodo secures the online transactions for thousands of businesses worldwide. With more than 85 million desktop security software installations, Comodo has the world's largest crowd-sourced threat intelligence of known good and bad files.

Comodo Advanced Endpoint Protection runs unknown files safely in containment at the endpoint--with negligible resource usage--to enable a Default Deny security posture with default allow usability.

Our multi-layered forensic analysis identifies unknown malware and prevents it from executing. Only Comodo-validated "good" files are allowed to run on your endpoints—and you know what each and every one of them is doing.

Plus, users can run unknown files in containment so workflow continues uninterrupted. This means you won't get a single support call because you denied someone access to their application. And the virtual client is transparent to end users and takes minimal resources to run...

Why would you choose a Default Allow security posture that lets unknown files run unfettered on your network, when you could choose Comodo's Default Deny Platform and know that all the files running on your network are good?

Buy Now

How We Achieve a Default Deny Security Posture

Comodo's **good and bad signature lists** are bigger and better than any other vendor because we are the world's largest certification authority. We know all the legitimate publishers. Our dynamic lists of good and bad files—together with the behavioral analysis of VirusScope and forensic intelligence from Valkyrie and our threat experts—allow us to analyze unknown files automatically and deliver a verdict in less than a minute, 95% of the time. And for the other 5%, our dedicated threat experts return a verdict in less than 2 hours.

Using the combined strengths of automatic containment, forensic intelligence from dynamic and static analysis and digital file signature-based whitelisting and blacklisting; Comodo® Advanced Endpoint Protection prevents malware from infecting your endpoints.

Unlike endpoint solutions that isolate files for analysis frustrating end users, our patented containment technology allows end users to continue working while the unknown file is analyzed in containment virtual container. If it's good, it's allowed onto your endpoint, and if it's bad, it's killed.

Comodo's Default Deny Platform let's, you sleep better at night knowing that malware will never run unfettered on your network again.

Comodo Advanced Endpoint Protection solves your malware problem with a revolutionary Default Deny Platform that enables productivity.

Prevent infection. **Learn More about Default Deny Security**

How We Do It

Multiple Layers of Forensic Analysis Provide Accelerated Verdicts

The big difference between Comodo's Default Deny Platform and other endpoint solutions is that it is a verdict-driven system designed to ensure no unknown process or executable has access to the CPU to exploit the endpoint.

The Comodo Advanced Endpoint Protection client runs on the endpoint to intercept and render a good/bad/unknown verdict on files and applications. When malicious files are identified, they are prevented from infecting endpoints and spreading across your network.

Multiple layers of analysis look at the behavior of unknown files and, while this is happening, users can run the files safely in containment...

Local Analysis within the Virtual Container. Comodo VirusScope™, a local behavioral analysis engine, uses machine learning to analyze what the file is doing within the container. If this engine determines the file is acting maliciously it's automatically killed, the container is closed and the bad file goes on the blacklist. If there is no malicious behavior, the good file goes on the whitelist.

Forensic Analysis in the Cloud and by Experts. In parallel with the local analysis, the unknown file is automatically sent to Valkyrie™, Comodo's cloud-based sandbox where another 200 or so static and dynamic checks are applied to assess the file as either good or bad, typically within 45 seconds. If no clear determination can be made, the file is sent to Comodo's lab for human analysis by our threat experts who return a verdict in less than 2 hours.

Valkyrie has a full dual verdict capability, which means it delivers a verdict of either good or bad on all unknown malware, 100% of the time. Only good files run on your endpoints. This is the difference between the Valkyrie cloud-based sandbox versus other endpoint solutions' sandboxes that deliver a partial single verdict on bad files only some of the time. They can't give a dual verdict so they allow unknown files to execute on the endpoint.

Complete awareness of every file on your network. We analyze 100 percent of the files on your endpoints so you know exactly what they are doing on your network. Both static and dynamic behavior is scrutinized and the outcome is doubly verified. With both automatic and manual analyses—performed by VirusScope, Valkyrie and our threat experts—only validated good files can run on your endpoints. And you can see and control every single one of them.

Comprehensive protection that lowers operational costs. Comodo Advanced Endpoint Protection secures your servers, desktops, laptops, and mobile devices without requiring signatures or updates. It identifies and automatically discards malware eliminating the need for costly remediation. And, Comodo Advanced Endpoint Protection solution also includes a unified IT and security management dashboard to simplify the jobs of IT operations and system administrators tasked with keeping all your endpoints protected.

Don’t you want to know every file that’s running on your network?

Run a forensic analysis. It’s fast and free