COMODO
CYBERSECURITY

# RENDER ATTACKS USELESS ACROSS THE LAN, WEB & CLOUD

# Comodo Cybersecurity

## Innovative Cybersecurity to Render Malware Useless

### The Problem

Some things in life are unavoidable, and malware is quickly becoming one of them. According to experts, emerging viruses, worms, Trojans, and other malicious "wares" generate approximately one million new specimens of hostile and intrusive software each day. Although many cybersecurity vendors will promise full protection against threats —the truth is, they can't. No one can. Businesses and people must accept that malware cannot be successfully blocked 100% of the time, nor can it be mitigated through mere defensiveness. Undetected threats are now a reality of digital age. And as such, the fight against this robust enemy will require a far more innovative and holistic approach to protection.

### The Effect

Data surveys offer a glimpse into just how far down the attack cycle today's malware has travelled, and the statistics are unsettling at best. As companies continue to zero in on the silver bullet of "protection" without considering the redundancy and impotence of their security layers, the result is a porous security posture with limited capabilities.

*An attack cycle consists of four key stages:*

1. **Delivery of malware**
2. **Pre-execution**
3. **Runtime as malware attempts to execute**
4. **Post-damage remediation**

While a great deal of this threat can be prevented in the first phase, the defense in depth ability to block malware execution in real time—and repair the damage—hovers around 85%. This number simply isn't high enough to beat the greatest enemy to the world of computing.

### The Comodo Cybersecurity Solution

As a leader in cybersecurity for over twenty years, Comodo Cybersecurity seeks to protect businesses by understanding the true nature of the digital environment and what malware needs to survive. Without unfettered access and the ability to execute its malicious program, it has no power to breach other systems. But malware does that have the capability to penetrate initial security measures, which means it cannot be fully prevented or denied—instead, it must be mitigated through the acceptance of its ability to penetrate even the most well-guarded systems. While Comodo Cybersecurity solutions offer comprehensive detection services, our real prowess comes from the ability to determine if unknown files entering the system are good or bad, with no sandbox lag time or delayed productivity.

Comodo Cybersecurity's automatic threat containment technology does not block malware, but rather holds unknown executables in a virtual container, all the while allowing businesses to safely run their critical applications regardless of whether the platform has been compromised. Using a preemptive, surgical approach to containment, Comodo Cybersecurity's technology is precise, vigorous, and tailored to solve problems without downtime or undue stress. It renders an almost immediate verdict on the status of any unknown file, so it can be handled accordingly by either software or human analysts. This shift from reactive to proactive is what makes Comodo Cybersecurity unique and gives them the capacity to protect all domains of business activity and threat—from network to web to cloud—with confidence and efficacy. This fast and competent technology provides a seamless user experience and promotes ongoing customer trust. And, it recognizes an important reality: while you cannot prevent 100% of malware – you can render malware useless.

### Endpoint Security

Unlike conventional methods, Comodo Cybersecurity's approach to endpoint security supplements centralized measures with additional layers of needed protection on the endpoints. Safeguarding all endpoint devices, as well as the world's ever-growing IoT demands, is critical to keeping data safe and giving administrators the insight and control they need to form a strong defense posture. Comodo Cybersecurity's endpoint security manager utilizes its containment technology to make this goal a reality through automatic containment technology, which allows all files types, including potentially malicious ones, to run locally on the endpoints all while a definitive verdict is determined in the cloud in less than one minute.

### Secure Cloud and Internet Access

As enterprises leverage the many benefits of cloud-based technologies, they must also address the cybersecurity risks inherent in digital transformation. Cloud-based applications and other Internet-based services open up channels of communication to and from the corporate network that make businesses vulnerable to cyber threats and enable the exposure of critical data. Comodo Cybersecurity offers Comodo Dome, a Secure Cloud & Internet Access Suite that meets the enterprise-level business security needs in order to fully embrace the opportunities of digital transformation.

Comodo Cybersecurity's Secure Cloud & Internet Access Suite delivers a combination of capabilities which include: Secure Web Gateway, DNS Filtering, DLP, Firewall, and Antispam.

### Managed Detection and Response (MDR)

Under the umbrella of cWatch Network, Comodo Cybersecurity's MDR is able to detect, monitor, and correlate events to offer the most comprehensive and effective threat response on the market. As a security solution, Comodo Cybersecurity is the only provider who connects all three domains of the web, network, and cloud to protect critical infrastructure with real-time threat intelligence monitoring. In combination with extensive analysis and correlation capabilities, MDR reports all activity and access information related to networks, systems, users, and data.

### Managed Security Services (MSS)

Companies who need to oversee complex securi-ty systems often outsource this task to providers who can define, implement, monitor, and manage the evolving cyber threats of today. These efforts include proper configuration, pen testing, updat-ed solutions, maintenance, fine tuning, and reme-diation of all security products to ensure a seam-less and safe user experience. As compliance with major security regulations becomes increasingly mandatory, the need for capable experts with both insight and skill will also grow in demand, pushing businesses to find providers who can ensure full legal adherence.

COMODO
CYBERSECURITY