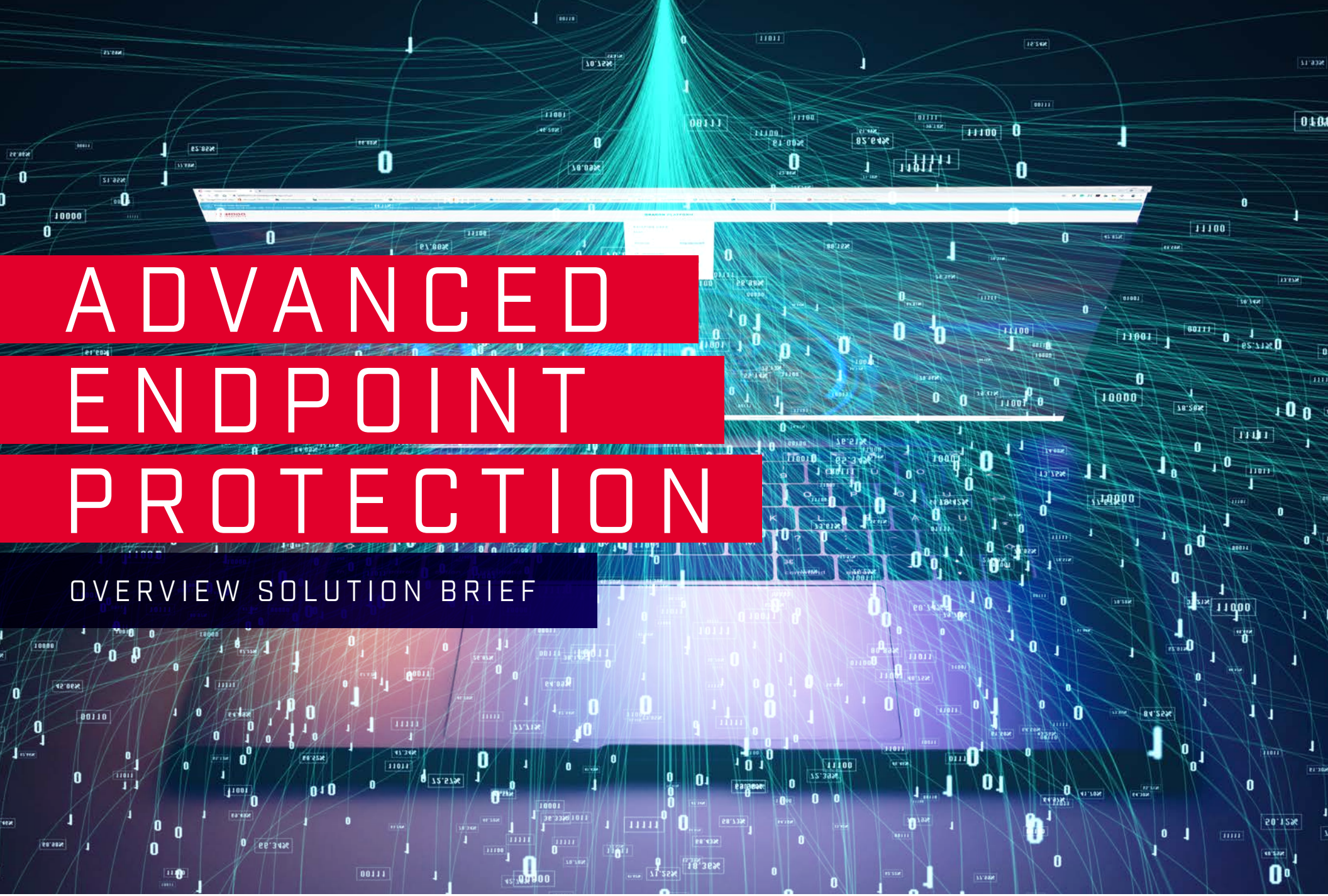


ADVANCED ENDPOINT PROTECTION

OVERVIEW SOLUTION BRIEF

COMODO

PROVEN SUCCESS IN PREVENTING BREACHES

TABLE OF CONTENTS

REAL-WORLD PROOF THAT OUR ENDPOINT PROTECTION OFFERS SECURITY WITHOUT COMPROMISE

When a 2017 WikiLeaks data dump exposed the CIA's assessments of 20 security products, we got to see the unvarnished results of the intelligence community's attempts to foil the technologies that businesses rely on daily to protect themselves. While many of the biggest names in the market proved to be easily to moderately hackable, there was one solution that seemed to frustrate their best attempts.

Here's what the CIA—one of the best-funded, most expert hacking organizations in the world—had to say about Comodo AEP:

> ***"Comodo is impossible to breach. A colossal pain in the posterior. It literally catches every payload sent through a network."***

That's good news for you. By deploying Comodo AEP, you can bulletproof your endpoints and your hardworking employees won't notice the difference.

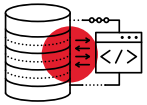
100% TRUST VERDICT OF ALL UNKNOWN FILES

Cybercrime has come a long way from script kiddies looking for a little glory. Today's sophisticated attackers are after money and power. By 2019, ransomware will attack a business every 14 seconds and damage costs will soar to $11.5 billion annually. In 2017, wide-ranging events from elections to North Korea nuclear threats and missile launches corresponded with major malware spikes in enterprise security, indicating the use of cyber "activism" to achieve geopolitical goals.

No business and no user can be considered safe. Having a comprehensive defense-in-depth strategy has never been more critical, and no security posture is complete without technology to protect endpoints. But security controls must not impede employees' ability to do their jobs—and ease of administration is critical to reduce the burden on your IT staff.

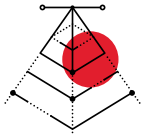
HOW TRADITIONAL ENDPOINT SECURITY WORKS

File Executed Inside Network with Traditional Endpoint Security



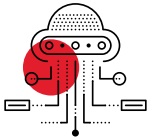
Attackers create payloads to deliver to targeted or global campaign.

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



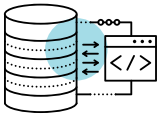
Machine Learning is not trained for newly bad indicators, bypassing statistical and behavioral models.

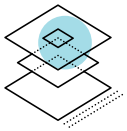
File Executes on the Endpoint to Infect the Network

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

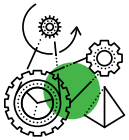
HOW ACTIVE BREACH PROTECTION WORKS TO PREVENT THE DAMAGE

File Executed Inside Network → **File Identified as Unknown** → **Auto Containment Triggers Instantly** → **File Analyzed for Trusted Verdict**

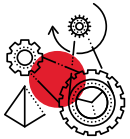


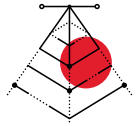


Known Good Verdict → **File Runs Safe on Endpoint**



Known Bad Verdict → **File Blocked from Endpoint**





Unknown executables and other files that request runtime privileges are automatically run in a virtual container that does not have access to the host system's resources or user data. They run just as well as they would on the host system, making it seamless from the end-user perspective, but they cannot damage or infect the system. Any unknown executables in containment do not have write privileges to the hard drive, COM interface or registry. Comodo's approach enables users to remain productive as usual without allowing unknown threats to harm their endpoints.

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 .

KEY CAPABILITIES

Auto Containment

Unknown executables and other files that request runtime privileges are automatically run in Comodo's patented virtual container that does not have access to the host system's resources or user data.

24x7 Human Analysis

In the 5% of cases where VirusScope and Valkyrie are unable to return a verdict, the file can be sent to researchers for human analysis who make a determination within SLA timelines.

Host Intrusion Prevention

Rules-based HIPS that monitors application activities and system processes, blocking those that are malicious by halting actions that could damage critical system components.

Fileless Malware Protection

Not all malware is made equal. Some malware do not need you to execute a file, it built-in the endpoint's memory-based artifact such as RAM. Comodo AEP completely stops write access against this threat.

Comodo Antivirus

Scans endpoints against a massive list of known good and bad files compiled from years as the world's largest certificate authority and from the 85 million endpoints deployed worldwide.

VirusScope Behavioral Analysis

Uses techniques such as API hooking, DLL injection prevention, and more to identify indicators of compromise while keeping the endpoint safe and without affecting usability.

Valkyrie Verdict Decision Engine

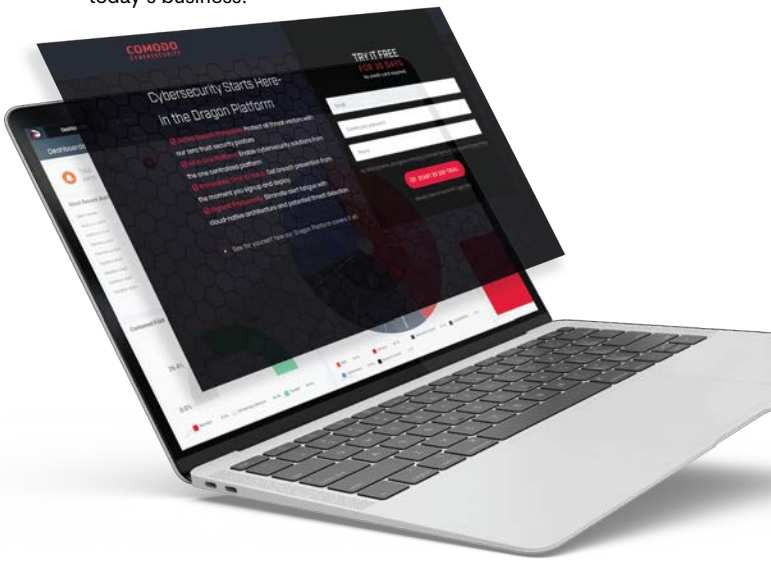
While running in auto-containment, unknown files are uploaded to a global threat cloud for real-time analysis, returning a verdict within 45 seconds for 95% of the files submitted.

Personal Packet Filtering Firewall

Provides granular management of inbound and outbound network activities, hides system ports from scans, and provides warnings when suspicious activities are detected.

Cloud-based Online Platform

Automatic signature updates that simplifies deployment across your entire environment to lower operational costs delivering reliable, centralized and fully scalable security solutions for today's business.



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.

COMODO

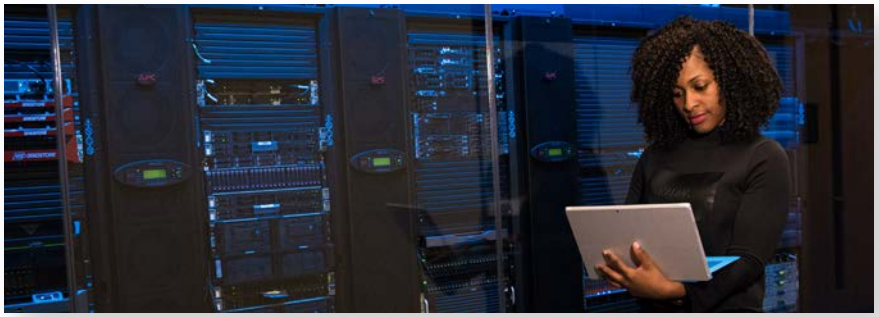
PROVEN SUCCESS IN PREVENTING BREACHES

SUPPORT BUSINESS HOURS

Our customer support has you covered

Our Level 1 and Level 2 Support Teams are available 24x7 to assist our customers' needs, no matter where they are located. Should your issue require escalation, we have our Level 3 Support Team, as well as development teams, available to assist.

Level 1	Level 2	Level 3
24 HRS ALL WEEK	24 HRS ALL WEEK	18 HRS WEEKDAYS



CONTACTING SUPPORT

Choose one of these 3 options

1 | **SUBMIT A TICKET**
support.comodo.com

2 | **CALL US DIRECT**
973-396-1232

3 | **SEND AN EMAIL**
support@comodo.com

Opening a ticket on our portal or sending an email to Support will result in a ticket being generated immediately. You will be notified of this ticket creation through the email address used. A Support representative will reach out to you within our defined SLA (see below). You may also search our knowledge base or help page for further support information.

ABOUT COMODO

In a world where preventing all cyberattacks is impossible, Comodo provides Active Breach Protection with its cloud-delivered cybersecurity platform. The Comodo Dragon Platform provides a zero trust security environment that verdicts 100% of unknown files. The platform 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 unique and gives us the capacity to protect your business – from network to web to cloud – with confidence and efficacy.

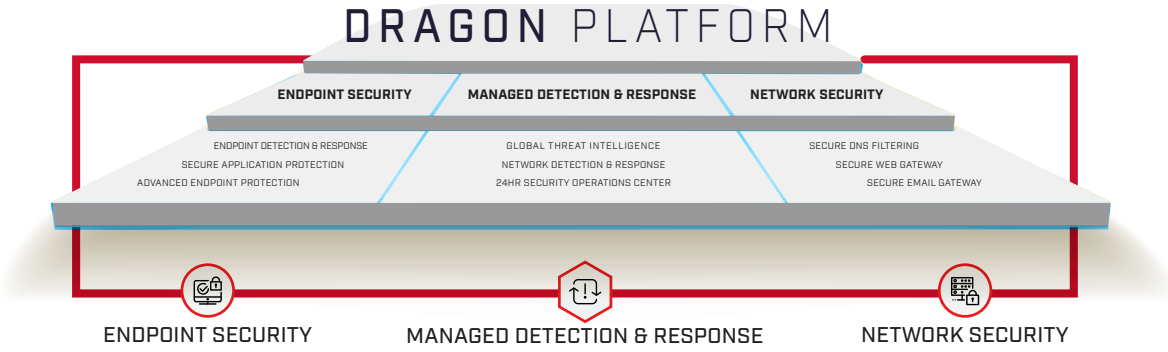
Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Bloomfield, New Jersey, Comodo has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide.

ACTIVE BREACH PROTECTION PREVENTS DAMAGE WITH THE INDUSTRY'S LEADING ZERO TRUST ARCHITECTURE

PROTECT THREAT VECTORS WITH OUR ZERO TRUST SECURITY POSTURE

ENABLE CYBERSECURITY SOLUTIONS FROM OUR ONE CENTRAL PLATFORM

ELIMINATE ALERT FATIGUE WITH CLOUD-NATIVE ARCHITECTURE & THREAT DETECTION



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

COMODO

PROVEN SUCCESS IN PREVENTING BREACHES