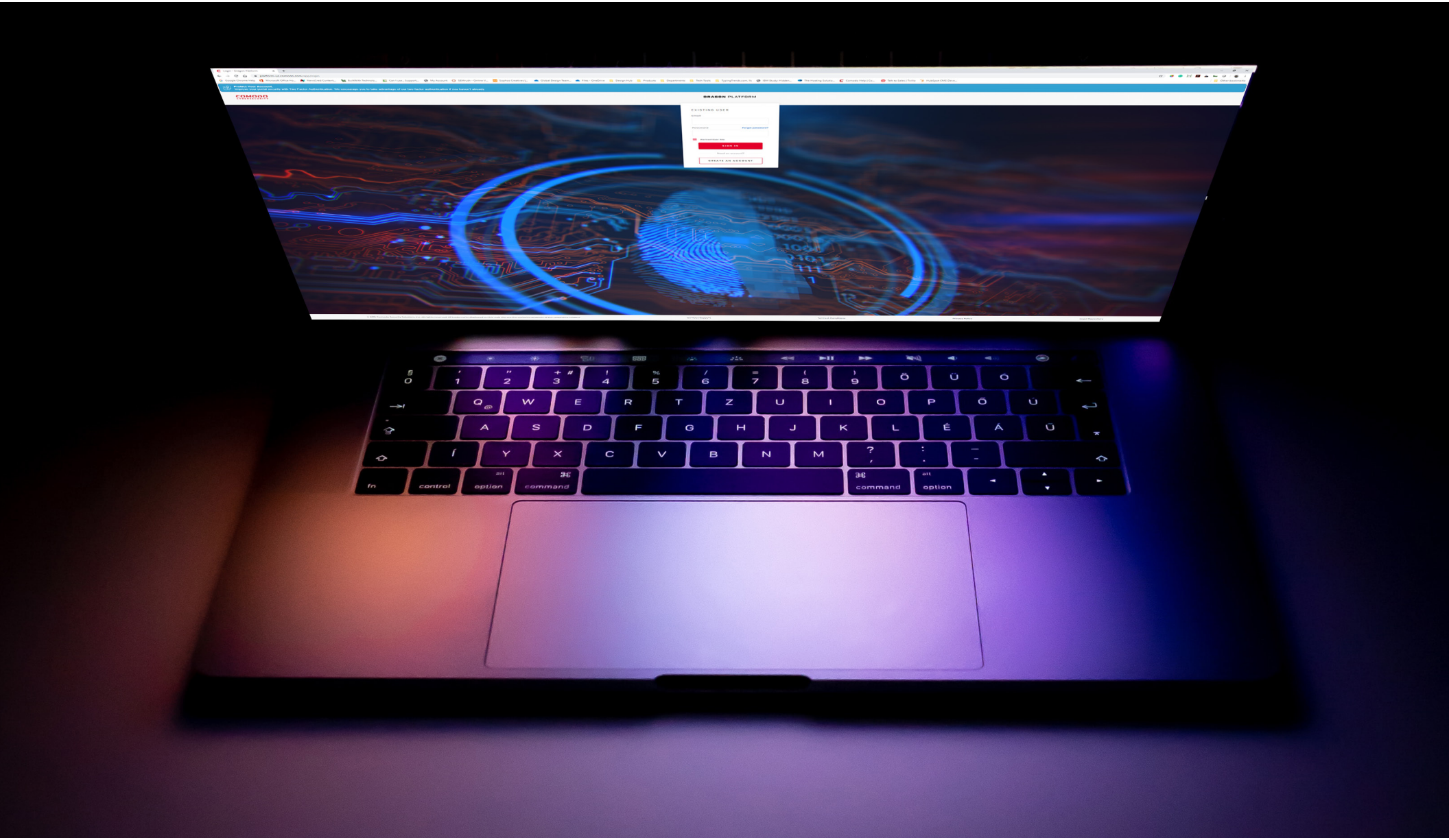
ADVANCED ENDPOINT PROTECTION

DATASHEET



COMODO

PROVEN SUCCESS IN PREVENTING BREACHES

TABLE OF CONTENTS

THE SOLUTION

100% Trust Verdict of every unknown file

Comodo Advanced Endpoint Protection (AEP) delivers patent-pending auto-containment, where 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 native system.

While running in auto-containment, unknown files are uploaded to a global threat cloud for real-time analysis, which returns a verdict within 45 seconds for 95% of the files submitted. The remaining 5% of cases are sent to researchers for human analysis who make a determination within SLA timelines. In short, Comodo AEP provides a 100% verdict 100% of the time. And because the global threat cloud is crowdsourced, the knowledge gained about one unknown file benefits all Comodo AEP users. You benefit from the network effect of 85 million users. The extremely lightweight Comodo client has no CPU dependencies and is completely application-agnostic.

THE RESULTS

Eliminate the damage from unknown threats

Good files can be safely run. Bad files can be blocked. But how do you deal with unknown files? If you run them and they're bad, you've put your company at risk. If you block them and they're legit, you prevent users from doing their jobs.

> ***Comodo AEP offers the broadest array of tools to identify known good and known bad files. For all the unknown, our auto-containment technology and verdict decision engine deliver a verdict—good or bad—every time, with zero impact on the user experience.***

GARTNER PEER INSIGHTS, CUSTOMER REVIEW ENDPOINT PROTECTION

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.

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.

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.

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.

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.

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.

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.

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.

MINIMUM HARDWARE REQUIREMENTS

Comodo provides technical support to customers who encounter issues with using and maintaining any of Comodo's products, including, but not limited to Advanced Endpoint Protection (AEP), Endpoint Manager (EM), Dome Products (such as Shield, SWG, ASG and DLP) and most other Comodo offerings.

Memory

384MB of available RAM

Storage

210MB HDD for 32-bit version or 64-bit version

Processor

CPU with SSE2 Support (Streaming SIMD Extensions 2)

Browser

Internet Explorer 5.1 or above

OPERATING SYSTEMS SUPPORTED

Windows Server

WINDOWS SERVER 2003 SP2

WINDOWS SERVER 2003 R2 SP2

WINDOWS SERVER 2008 SP2

WINDOWS SERVER 2008 R2

WINDOWS SERVER 2012

WINDOWS SERVER 2012 R2

WINDOWS SERVER 2016

WINDOWS SERVER 2019

Windows

WINDOWS XP (SP3 OR HIGHER) X86

WINDOWS 7 SP1 X86

WINDOWS 7 SP1 X64

WINDOWS 8 X86

WINDOWS 8 X64

WINDOWS 8.1 X86

WINDOWS 8.1 X64

WINDOWS 10 X86

WINDOWS 10 X64

macOS

10.11.X EL CAPITAN

10.12.X SIERRA

10.13.X HIGH SIERRA

10.14.X MOJAVE

iOS

7.X

8.X

9.X

10.X

11.X

12.X

4.X KITKAT

4.X (KNOX) KITKAT

5.X LOLLIPOP

5.X (KNOX) LOLLIPOP

6.X (KNOX) MARSHMALLOW

7.X NOUGAT

7.X (KNOX) NOUGAT

8.X OREO

8.X (KNOX) OREO

9.X PIE

GUARANTEED COMPATIBILITY:

LATEST UBUNTU 16.X LTS X64 RELEASE VERSION (WITH GUI)

LATEST UBUNTU 18.X LTS X64 RELEASE VERSION (WITH GUI)

LATEST DEBIAN 8.X X64 RELEASE VERSION (WITH GUI)

LATEST RED HAT ENTERPRISE

LINUX SERVER 7.X X64 RELEASE VERSION (WITH GUI)

LATEST CENTOS 7.X X64 RELEASE VERSION (WITH GUI)

UNCONFIRMED COMPATIBILITY:

UBUNTU, DEBIAN BASED:
MINT, ELEMENTARY OS, MX LINUX, ZORIN, KALI, ANTIX, LINUX LITE, ENDLESS OS, KDE NEON, LUBUNTU, PEPPERMINT OS, UBUNTU MATE, DEEPIN, SPARKYLINUX, XUBUNTU, TAILS, DEVUAN GNU+LINUX, Q4OS, PARROT SECURITY OS, LXLE, KUBUNTU, BODHI LINUX, FEREN OS

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.

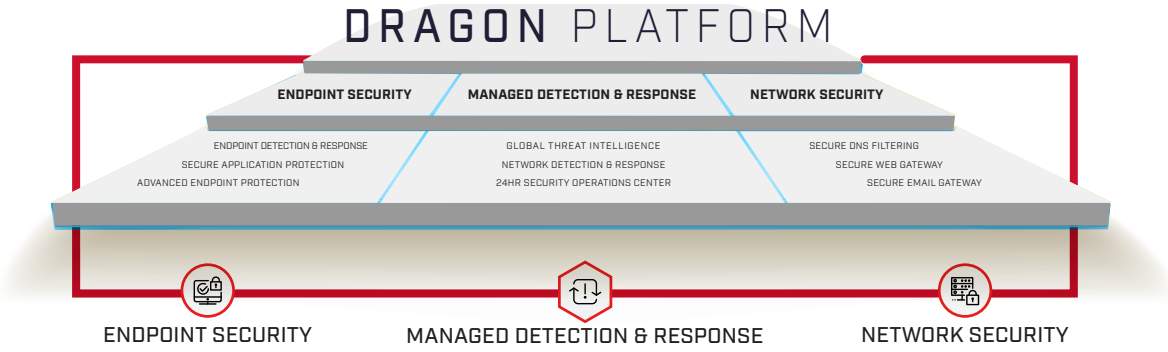
Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Bloomfield, New Jersey, Comodo has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide.

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