



COMODO

Discover Active Breach Prevention

Comodo Stops What Others Miss



HEARD OF US?

WHO WE ARE

Comodo is the world's leader of next-generation cybersecurity, with the industry's most disruptive innovations.

FOUNDED IN

2018

EMPLOYEES

150+

CUSTOMERS

3,500+

PATENTS

27

PRIMARY DIFFERENTIATION

Only Comodo can claim 100% effectiveness in preventing ransomware and zero-day's from causing harm!

CYBERSECURITY EFFECTIVENESS

100%

CYBERSECURITY SCALABILITY

100%

ENDPOINTS INFECTED

0

RANSOMS PAID

0

INDUSTRY RECOGNITION

We help customers avoid breaches with groundbreaking isolation technology that neutralizes ransomware, malware and cyber-attacks.

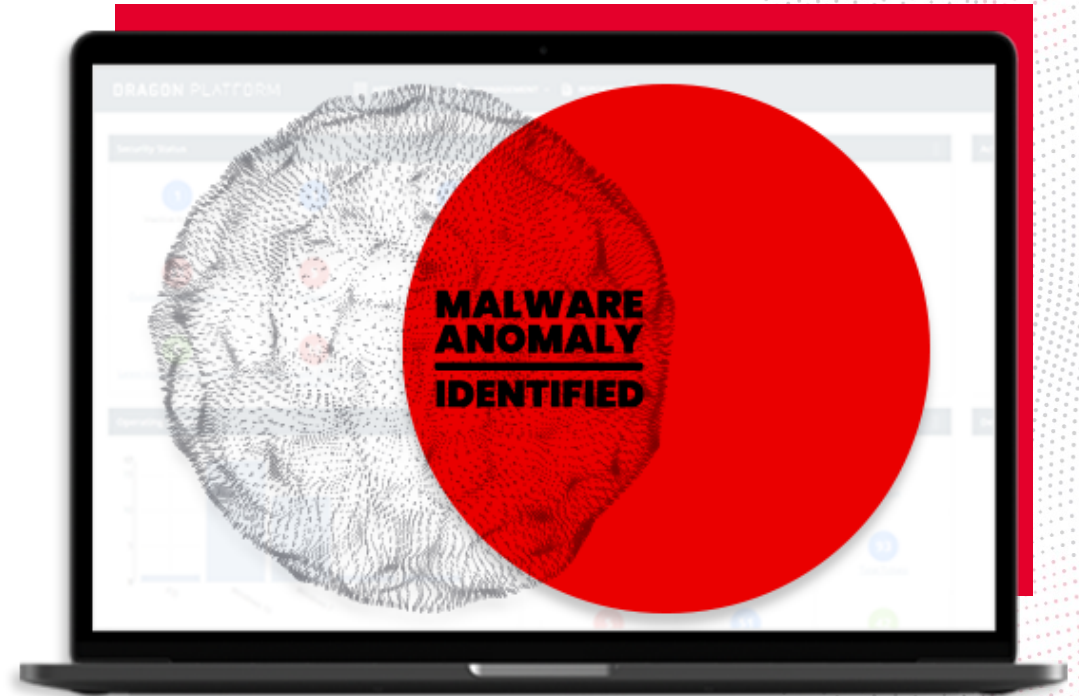


TIME TO FACE THE TRUTH

No one can stop zero-day malware from entering your network, but Comodo can prevent it from causing any damage.

Zero infection.

Zero damage.



“ All files were encrypted and could not be restored, except for two PCs running Comodo AEP ”



Andrew Cunningham, CEO Data Central

THE WORLDWIDE CHALLENGE

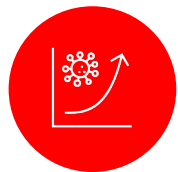
Ransomware is a Sophisticated Business.



NEW MALWARE

300,000

CREATED DAILY



[Source](#)



NEW RANSOMS

11 Secs

PER INCIDENT



[Source](#)



VICTIMS PAID

\$350M

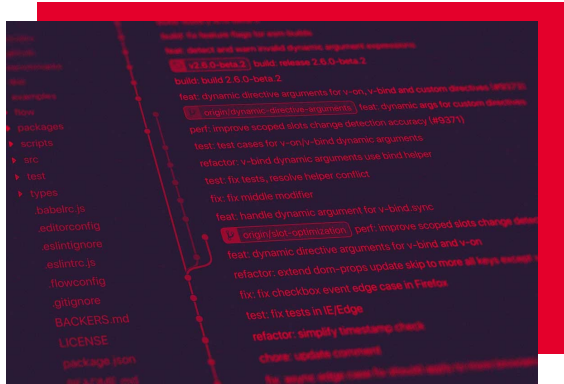
IN RANSOMS



[Source](#)

THE CHALLENGE EXASPERBATED

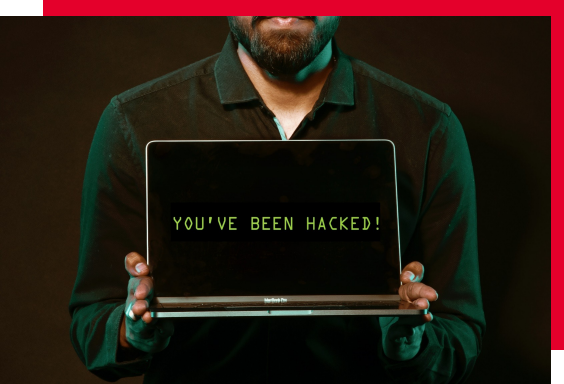
You're Against All Odds



EDR IS NOT ENOUGH

99% Detection

Current security solutions depend upon detection before they can prevent. Detection efficacy rates are not good enough.



REPUTATION SERVICES

Unpredictable

Third-party intelligence services fuel the detection world but remain too slow and inefficient to be relied upon all the time



INSUFFICIENT

Expertise

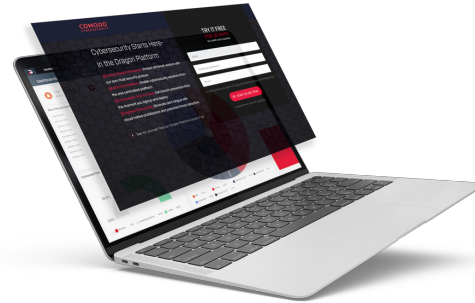
Limited cyber training, a high learning curve, and finite number of available experts to address your risk



THE CHALLENGE ACCEPTED

One Solution, Uniquely Bundled = Total Effectiveness

A single unified endpoint solution offering exploit prevention, advanced threat hunting, and endpoint management to stop ransomware, avoid breaches, and sustain your business.



STOP RANSOMS IN REAL TIME

100% Protection

Comodo is disrupting the market with our patented approach to stopping breaches and the damage malware and ransomware can cause. Devices remain protected even if they're infected by an unsecured device.

UNIFIED TECHNOLOGIES FOR

+ Endpoint Security +

Our **cloud native platform** works in real time to communicate threats between EDR, AEP, MDR, EMM, and MDM to give you enterprise grade protection at affordable fixed rates.

24HR FULLY MANAGED

SOC Experts

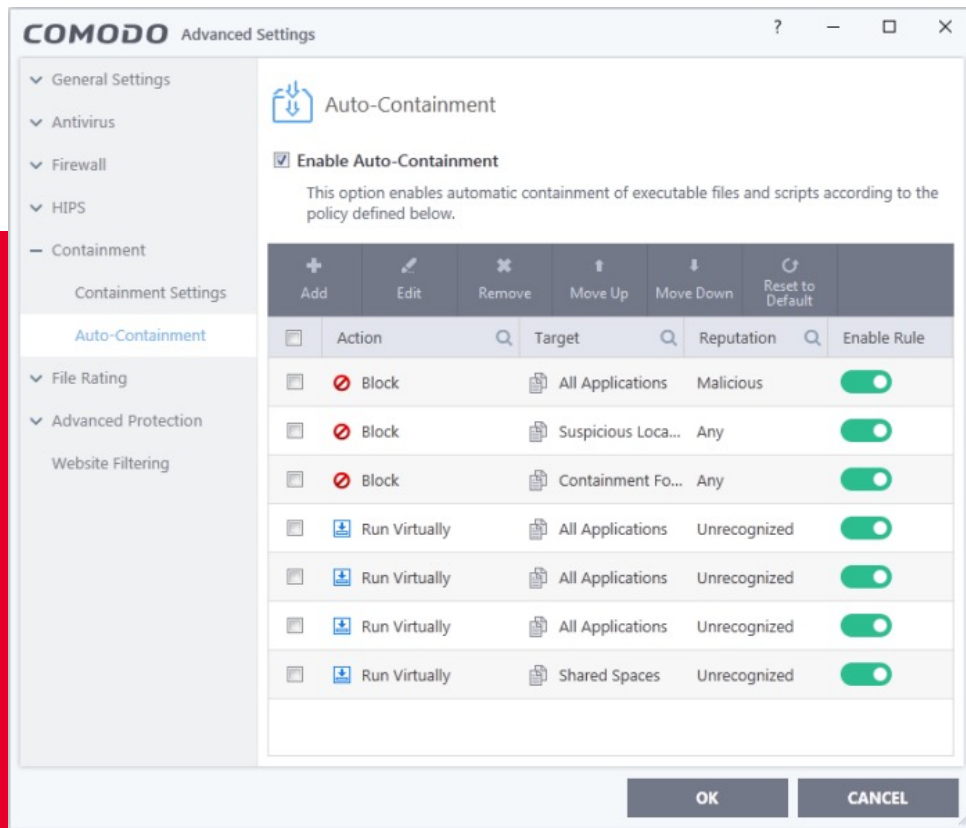
Our Security Operations Centers and teams of analysts work around the clock globally. These veteran threat hunters do not assess your business size, they simply love eliminating malware attacks and threats.



ADVANCED ENDPOINT PROTECTION

Auto Containment

Move from Detection to Prevention With Auto Containment™ to isolate infections such as ransomware & unknown threats.



Traditional AV and detection fail to stop threats from executing



Unknown Files

Malware requires write access to critical system resources



Hard Drive

Ransomware overwrites company data



Registry

Malware persists by adding code to registry



COM Interface

Malware injects malicious code to good processes

Our Technology Isolates and Disables the Threat at Runtime



Unknown Files

Isolation virtualizes your critical system resources



Hard Drive

File and File-less attacks are unable to damage or steal data



Registry

No persistence ensuring hackers not active in organization



COM Interface

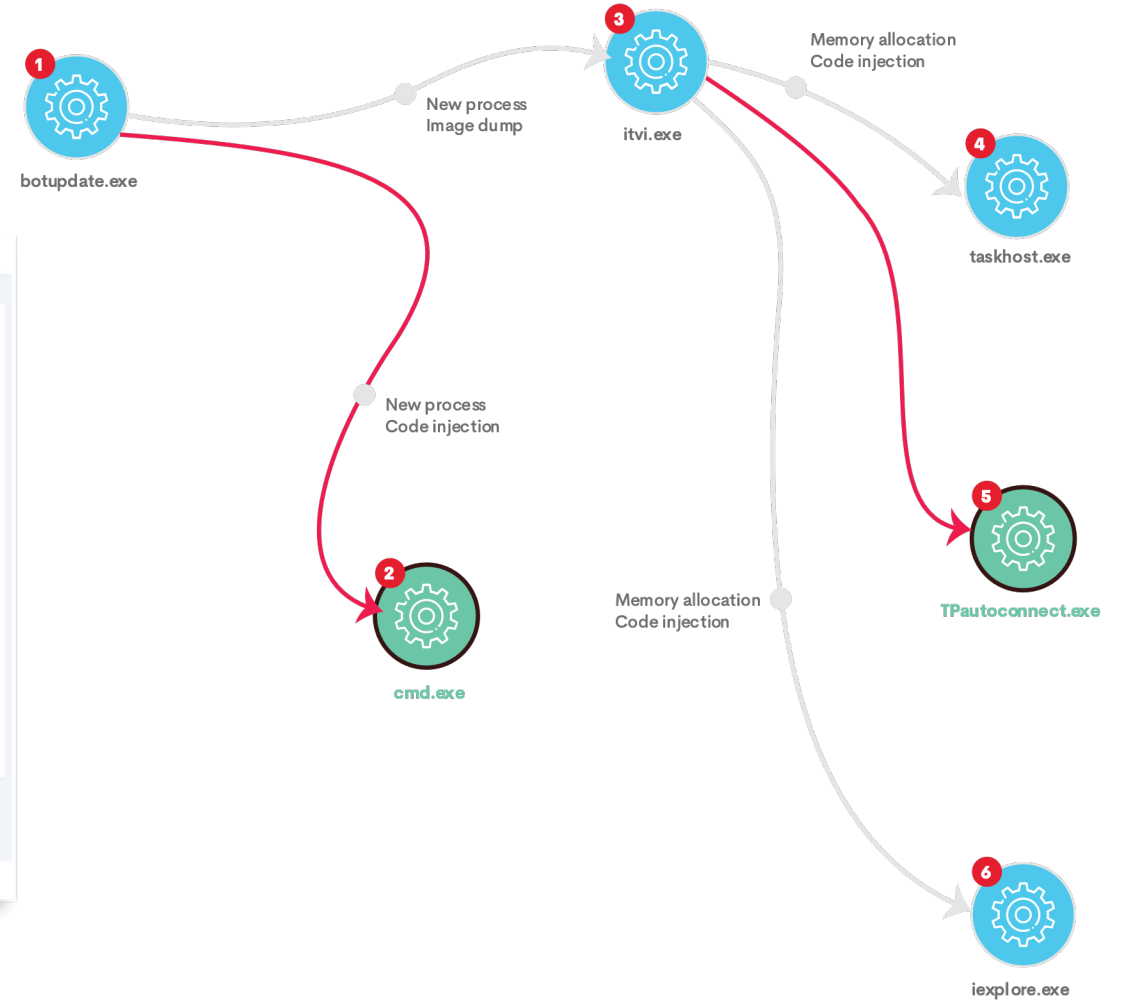
Memory protection to prevent injections and memory attacks



ENDPOINT DETECTION & RESPONSE

Real-time EDR Forensics

Gain full context of an attack to connect the dots on how hackers are attempting to breach your network.





Attack Surface Reduction

Practice cyber hygiene to reduce the attack surface by identifying applications, understanding the vulnerabilities and remediating patches.



COMODO IT & Security Manager

Patch Management

Paquete acumulativo de actualizaciones de calidad mensual de seguridad (enero de 2017) para Windows Server 2008 R2 sistemas basados en x64 (KB3212646)

Security Patch Info

General Vendor Security Patch info Bulletin CVE IDs

Supercedes

- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=5b92ccf0-3865-4ff9-828f-ff8cf1a4d985>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=3f887b75-cdea-4153-9135-9415b80bbc4c>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=9ecc576d-3654-411c-96c2-8c9836c4f33f>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=aa54d8bc-8043-4719-8b8c-a9ea86afe30a>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=0043e623-5876-4536-841b-f067d49121b7>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=71b467b-f842-43e6-aba4-868230ba297d>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=b1ec46dc-0bb9-4bce-8049-488b16aa9534>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=63e6442c-7a8b-4a8b-8134-848484848484>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=155>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=755>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=867>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=99f>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=18f>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=4f9>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=a12>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=f8b>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=ef7>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=dac>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=98b>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=f65>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=ebf>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=25f>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=aa5>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=ddc>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=a4e>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=af9>
- <http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=c26>

Downloads and updates

You're good to go
All your trusted apps and games from Microsoft Store have the latest updates.

Recent activity

App	Version	Modified
Telegram Desktop	App 1.6.7.0	Modified today
Dropbox	App 19.47.0	Modified yesterday
Surface	App 38.602.139.0	Modified 13/04/2019
Microsoft To-Do: List, Task...	App 1.542.992.0	Modified 12/04/2019
App Installer	App 1.0.30732.0	Modified 12/04/2019
Messenger (Beta)	App 196.2265.1966.0	Modified 11/04/2019
Spotify Music	App 1.104.197.0	Modified 11/04/2019
Feedback Hub	App 1.1811.10962.0	Modified 11/04/2019

Bulletin

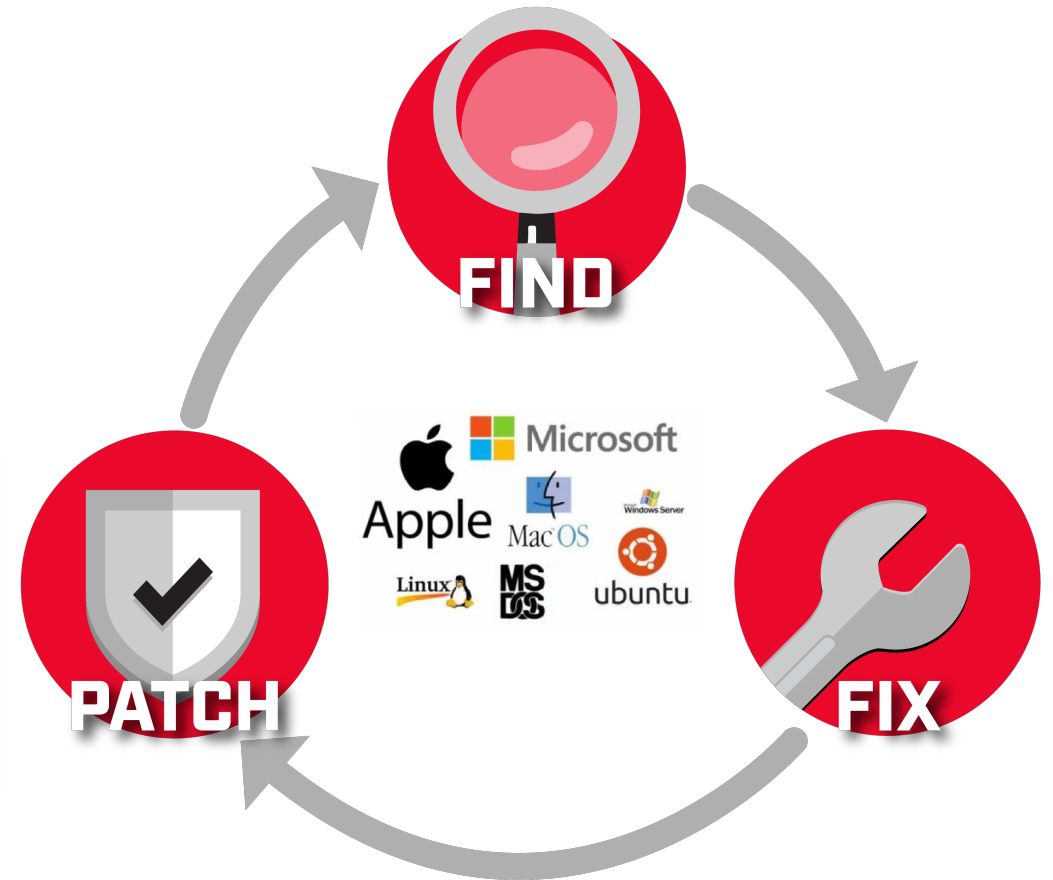
<https://technet.microsoft.com/en-us/library/security/MS17-004>

Supercedes bulletin ID

<https://support.microsoft.com/en-us/kb/3212646>

Release date

2017-01-10

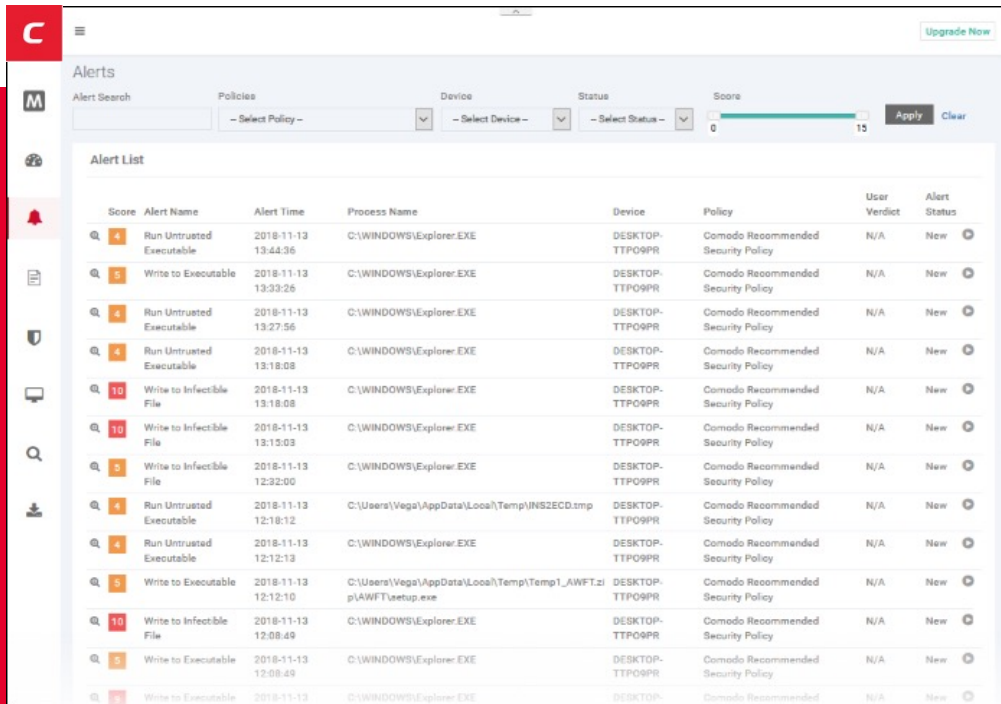


MANAGED SERVICE

24 • 7 • 365

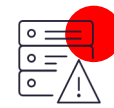
SOC Investigation and Remediation

Your vulnerabilities are due to lack of resources, processes, and possibly the technology to maintain all these technologies.



The screenshot displays a security management interface with a sidebar on the left containing navigation icons. The main area is titled 'Alerts' and includes a search bar and filter options for Policies, Device, Status, and Score. Below this is an 'Alert List' table with the following data:

Score	Alert Name	Alert Time	Process Name	Device	Policy	User Verdict	Alert Status
4	Run Untrusted Executable	2018-11-13 13:44:36	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Executable	2018-11-13 13:33:26	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 13:27:56	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 13:18:08	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
10	Write to Infectible File	2018-11-13 13:18:08	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
10	Write to Infectible File	2018-11-13 13:15:03	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Infectible File	2018-11-13 12:32:00	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 12:18:12	C:\Users\Vega\AppData\Local\Temp\INS2ECD.tmp	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 12:12:13	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Executable	2018-11-13 12:12:10	C:\Users\Vega\AppData\Local\Temp\Temp1_AWFT.zi	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
10	Write to Infectible File	2018-11-13 12:08:49	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Executable	2018-11-13 12:08:49	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New



Continuous Monitoring

Security analysts continuously monitor alerts for malicious activities or policy violations that can lead to attempted breaches.



Proactive Threat Hunting

Our proactive nature of threat hunting recognizes that threats can still try to evade in-place security protections.



Managed Response & Reporting

Providing remediation guidance on mitigating the threat, and orchestrating immediate triage and response



UNIFIED MANAGED SECURITY

DRAGON PLATFORM

A single unified endpoint solution offering exploit prevention, advanced threat hunting, and endpoint management to stop ransomware, avoid breaches, and sustain your business.

STOP RANSOMS IN REAL TIME

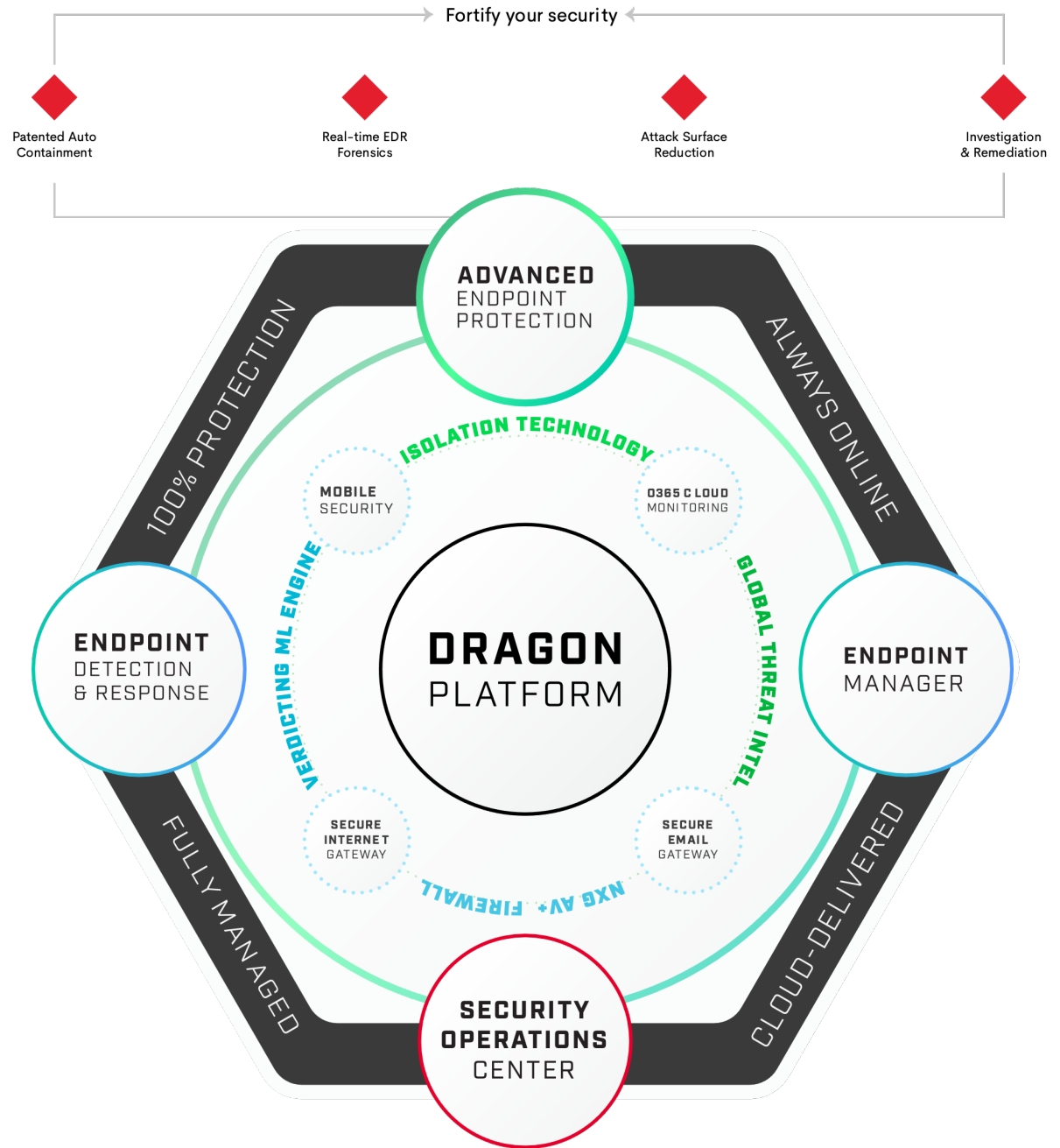
100% Cybersecurity Protection

UNIFIED TECHNOLOGIES FOR

Ultimate Endpoint Security

FULLY MANAGED

Around the Clock SOC Experts



THE PROOF

ENDPOINTS
INFECTED

0

CYBERSECURITY
EFFECTIVENESS

100%

RANSOMS
PAID

0





ABOUT US

Comodo is the world's leader of next-generation cybersecurity, with the industry's most disruptive innovations.

We help customers stop breaches with groundbreaking isolation technology that neutralizes ransomware, malware and cyber-attacks. Our complete cloud-native framework delivers a zero-trust architecture with active breach protection for the most comprehensive defense against zero-day threats. Comodo's cybersecurity products maximize intelligent sharing between every component of the platform, therefore providing superior security. We are the only company that analyzes and gives a trusted verdict for 100% of files on a network.

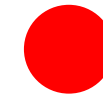
Comodo leverages innovation to celebrate and support the cybersecurity community by offering the very first open-source endpoint detection and response (EDR). We believe an open-source model using community-powered collaboration will ensure every organization has access to the industry's most sophisticated EDR.



Contact us

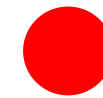
Tel: +1 (888) 551-1531

Tel: +1 (973) 859-4000



Email us

sales@comodo.com



200 Broadacres Drive,
Bloomfield, NJ 07003
United States



PRODUCT INFO

Resources

Need to review the product? Start with these informative documents.

[Download Solution Brief](#) →

[Download Datasheet](#) →

[Compare Products](#) →

PRODUCT DEMO

Schedule

Schedule a demo with one of our cybersecurity sales engineers.

[Schedule a custom demo](#) →

PRODUCT TRIAL

Signup

Get a dedicated Comodo Sales Engineer to guide your account setup quickly.

[Start Dragon trial for free](#) →

