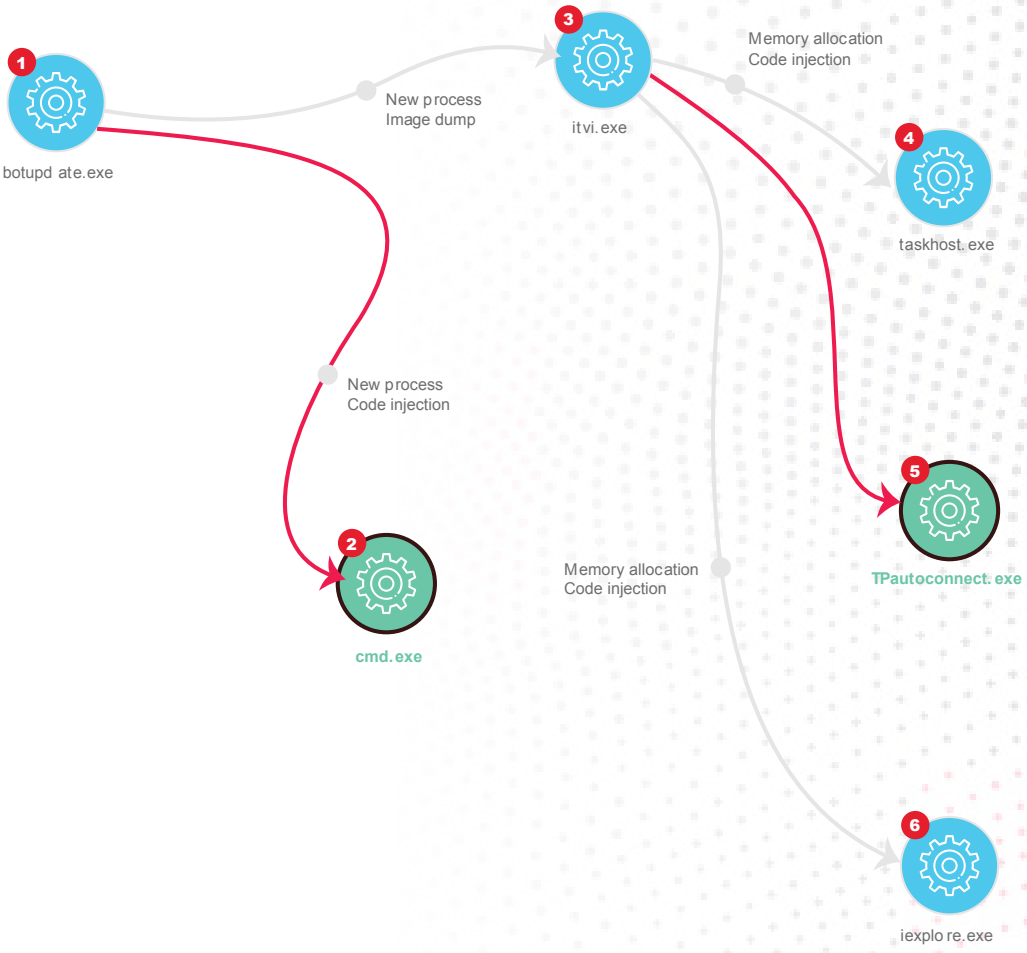
COMODO

Dragon EDR

Endpoint Detection and Response



200 Broadacres Dr,
Bloomfield, NJ 07003

Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000

www.comodo.com
platform.comodo.com

The Worldwide Challenge

Ransomware is a Sophisticated Business.

NEW MALWARE
300,000
CREATED DAILY

EDR IS NOT ENOUGH
99% Detection

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

NEW RANSOMS
11 Secs
PER INCIDENT

REPUTATION SERVICES
Unpredictable

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

VICTIMS PAID
$350M
IN RANSOMS

INSUFFICIENT
Expertise

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

The Comodo DIFFERENCE

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

CYBERSECURITY
100 %
EFFECTIVENESS

ENDPOINTS
ZERO
INFECTED

CYBERSECURITY
100 %
SCALABILITY

RANSOMS
ZERO
PAID

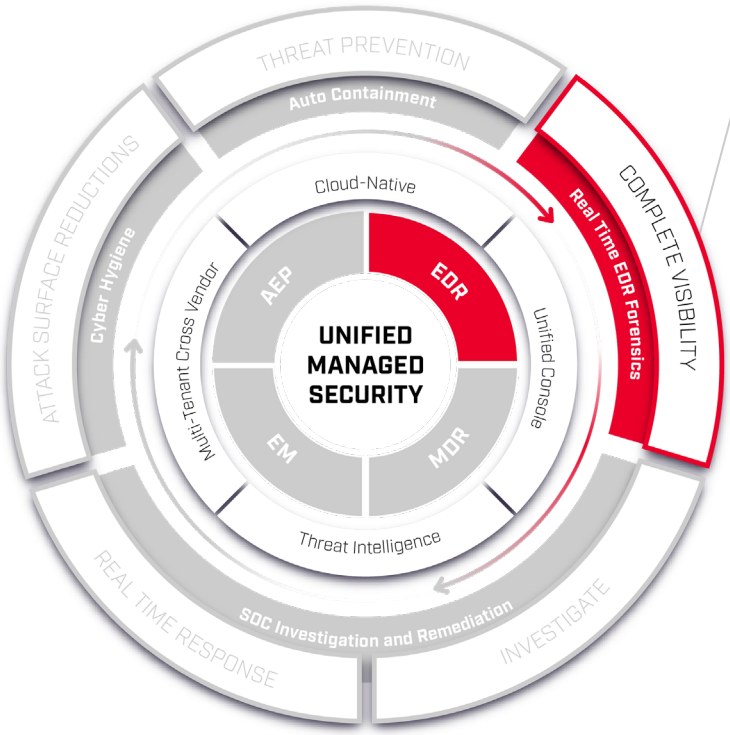
THE SOLUTION

Cloud-Based Endpoint Detection and Response

There's no question that you need to deploy endpoint security tools and platforms that are built for protection. But that's not enough. Attackers are smart. They understand how those solutions work and they continuously develop techniques to slip under their radars. You also need real-time, continuous visibility so you can identify zero-day and file-less attacks and that visibility must lead you to accurate root-cause analysis for effective remediation.

EDR allows you to analyze what's happening across your entire environment at a base-event level. This granularity enables accurate root-causes analysis needed for faster and more effective remediation. Process hierarchy visualizations, which are proven to be the best way to convey this type of information, provide more than just data, they offer actionable knowledge. Easy-to-navigate menus makes it easy to get details on endpoints, hashes, and base and advanced events. You get detailed file and device trajectory information and can navigate single events to uncover a larger issue that may be compromising your system.

Tel: +1 (888) 551-1531 | Tel: +1 (973) 859-4000 | Fax: +1 (973) 777-4394 | www.comodo.com | Inquiries: sales@comodo.com



THE RESULTS

Eliminate Threats & Resolve Recurring Events

EDR continuously collects events from your endpoints, centralizing them in our threat cloud that leverages Comodo Threat Laboratories intelligence and the Comodo Recommended Security policy. Our cloud-based sandboxing uses the Valkyrie file-verdicting system to isolate unknown files attempting to run on endpoints and return a fast good/bad verdict.

You get instant alerts based on your customizable security policy to notify you about suspicious activity that could represent ransomware, memory exploits, PowerShell abuse, and many other threats. Alerts are also triggered when the Comodo Recommended Security Policy is violated. The malicious behavior was performed by signed and trusted applications such as PowerShell and Regedit, a traditional endpoint tool would not have flagged it—which is exactly why the attacker used this approach. Without EDR, the threat could have gone unnoticed, allowing the attacker to steal all the company's confidential data.

KEY CAPABILITIES

ATTACK CHAIN VISUALIZATIONS

Attack vectors are shown on the dashboard which, when combined with file trajectory and process hierarchy visualizations, aids in investigations. Process-based events are shown in a tree-view structure to help analysts better understand process behavior.

RECOMMENDED SECURITY POLICY

Every EDR license comes with the Security Policy, which is customizable to meet your individual needs. Our sales engineering team is available to work with you tailor the policy to your requirements, including endpoint-specific policies.

SUSPICIOUS ACTIVITY ALERTING

Get notified about such activities as file-less attacks, advanced persistent threats (APTs), and privilege escalation attempts. Analysts can change status of alerts as they take counter-actions to dramatically streamline follow-up efforts.

INCIDENT INVESTIGATION

The event search screen allows analysts to run queries to return any detail at base-event-level granularity. Aggregation tables are clickable, letting investigators easily drill down into specific events or devices.

CLOUD-BASED ARCHITECTURE

EDR uses a lightweight agent to collect process, network, registry, download, upload, file system, peripheral device access, and browser events, and enables you to drill down into incidents with base-event-level granularity.

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 DETECTION

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 EDR can detect against this threat before it appears.

COMPATIBLE WITH 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.

ENTERPRISE LEVEL & MSP READY

Whether you're an enterprise with thousands of endpoints or an MSP serving hundreds of customers, the EDR agent can be instantly deployed via group policy object or the Comodo ITSM with automatic updates every release.

Tel: +1 (888) 551-1531 | Tel: +1 (973) 859-4000 | Fax: +1 (973) 777-4394 | www.comodo.com | Inquiries: sales@comodo.com

Unified Manage 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.

Advanced Endpoint Protection

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

Endpoint Detection and Response

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

Endpoint Manager

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

Managed Service

With 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.

About Comodo

Headquartered in Bloomfield, NJ, Comodo's mission is to help customers avoid breaches with groundbreaking isolation technology that fully neutralizes ransomware, zero-day malware, and cyber-attacks that other security providers can't do. We deliver active breach prevention with patented auto containment technology. Our Unified Endpoint integrates this technology with critical components like our highly rated advanced endpoint protection, endpoint detection and response, and endpoint management to offer a single cloud-accessible Active Breach Protection solution. Comodo's SOC as a Service team makes the solution a frictionless, high-security implementation. For more information, visit https://www.comodo.com/.

Tel: +1 (888) 551-1531 | Tel: +1 (973) 859-4000 | Fax: +1 (973) 777-4394 | www.comodo.com | Inquiries: sales@comodo.com