ENDPOINT DETECTION & RESPONSE

SOLUTION BRIEF

COMODO

PROVEN SUCCESS IN PREVENTING BREACHES

TABLE OF CONTENTS

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.

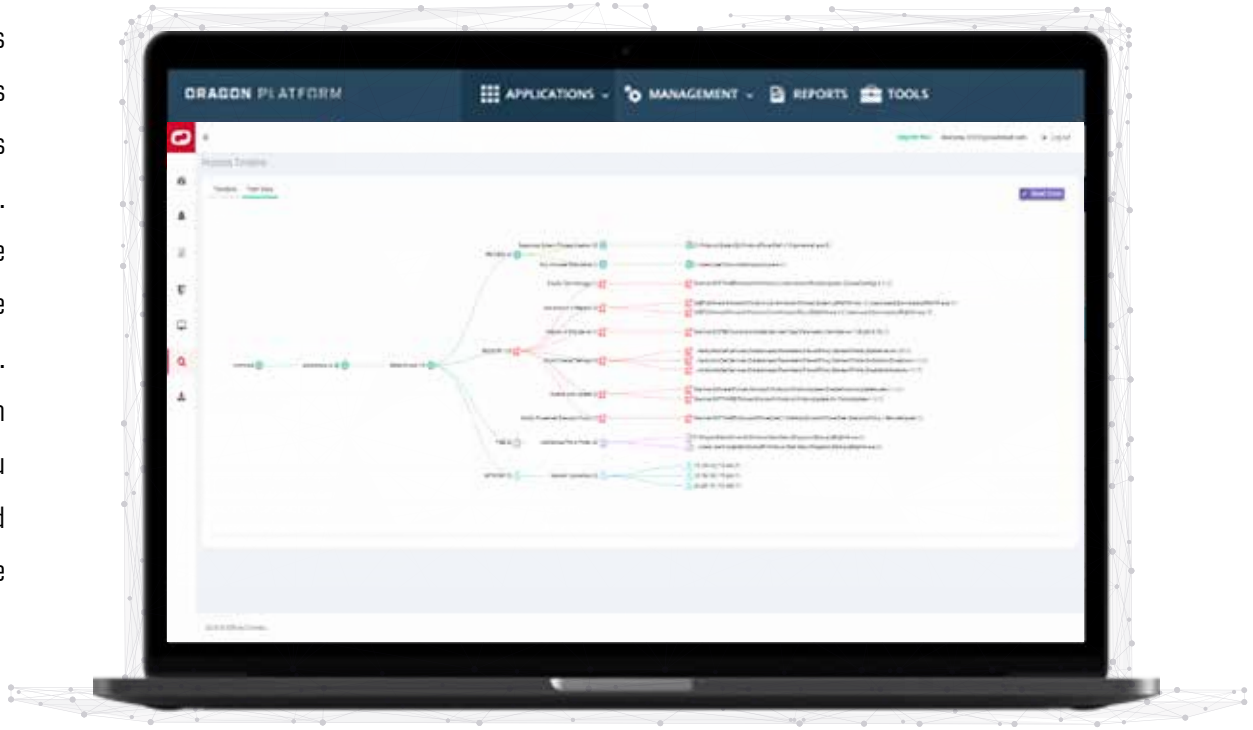


Figure: Process Timeline Tree View

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.

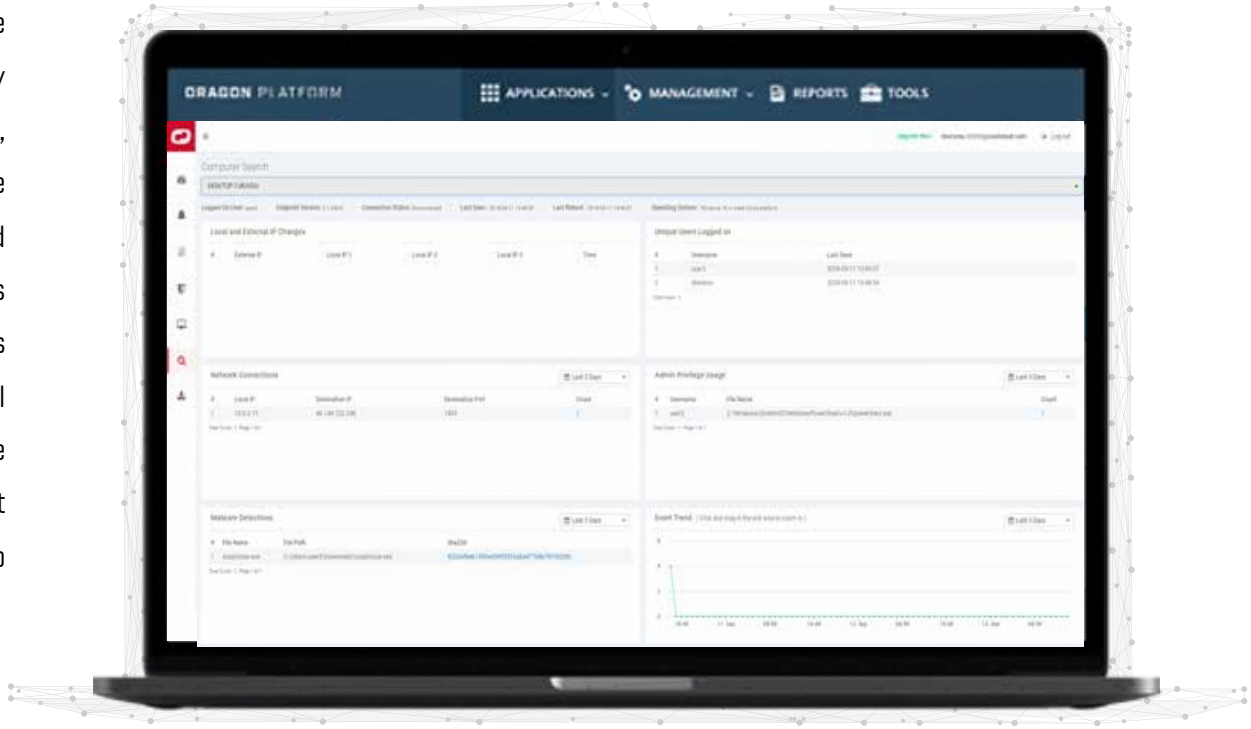


Figure 2C: Device Trajectory Details

KEY CAPABILITIES

Attack Chain Visualizations

Attack vectors are shown on 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.

MINIMUM HARDWARE REQ.

EDR detects the 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.

SUPPORTED OPERATING SYSTEMS

Windows Server

- WINDOWS SERVER 2008 SP2
- WINDOWS SERVER 2008 R2
- WINDOWS SERVER 2012
- WINDOWS SERVER 2012 R2
- WINDOWS SERVER 2016

Windows

- 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

Processor

Under 1% CPU Usage

Browser

Compatible All Major Browsers

Memory

20MB of RAM Usage

Storage

20MB of HDD Space

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	24 HRS	18 HRS
ALL WEEK	ALL WEEK	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.

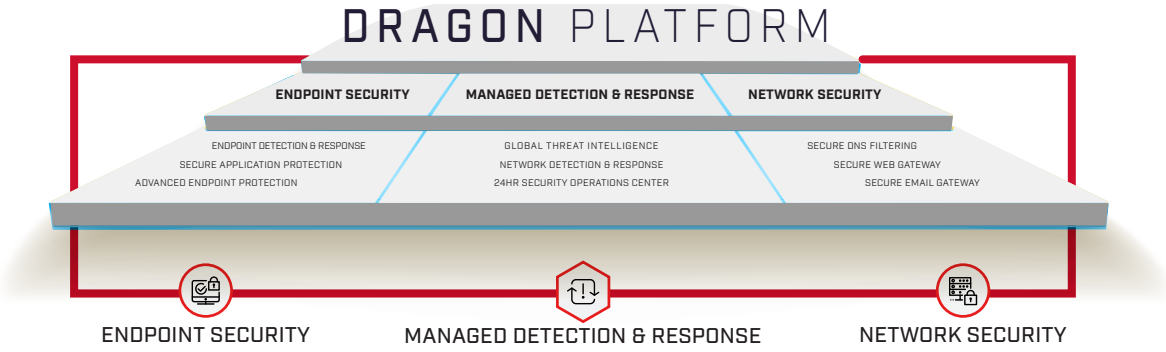
Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Bloomfield, New Jersey, Comodo has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide.

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