visit comodo.com

2018 Solution Brief

cWatch Endpoint Detection & Response

COMODO
CYBERSECURITY

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States
Tel: +1 (877) 712 1309
Tel: +1 (888) 551 1531
Fax: +1 (973) 777 4394
Inquire: sales@comodo.com
Support: c1-support@comodo.com

DELIVERING AN INNOVATIVE CYBERSECURITY PLATFORM TO RENDER MALWARE HARMLESS

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.

The World's First Free, Cloud-Based Endpoint Detection and Response Solution

Comodo Cybersecurity cWatch 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.

How it Works

The cWatch EDR lightweight agent 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. Here's what the process might look like, taken from real customer experience:

- Zero-day attack hits the customer environment.
- cWatch EDR immediately identifies a PowerShell command suspiciously attempting to disable auto update, alter registry keys to add a new DNS server, and alter firewall settings.
- cWatch EDR uses behavioral analysis to provide context to these events, which helps the customer see the "big picture" and take immediate remediation actions.

Because 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 cWatch EDR, the threat could have gone unnoticed, allowing the attacker to steal all the company's confidential data.

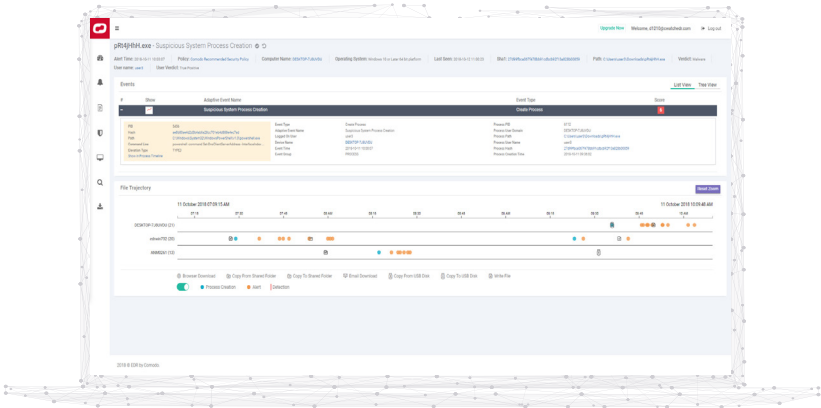


Figure 1: Alert Details

Comodo Recommended Security Policy

Every cWatch EDR license comes with the Comodo Recommended 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

The recommended policy covers behavior-based alerts, which notify you 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. Additionally, they can provide a verdict on the alerts, which is sent to the Comodo threat analysis team for further examination and to improve the security policy over time.

Attack Chain Visualizations

Attack vectors are shown on dashboard which, when combined with file trajectory and process hierarchy visualizations, aids in investigations (figure 2A). Process-based events are shown in a tree-view structure to help analysts better understand process behavior (figure 2B). Device trajectory details are provided with separate screens to drill down into devices (figure 2C).

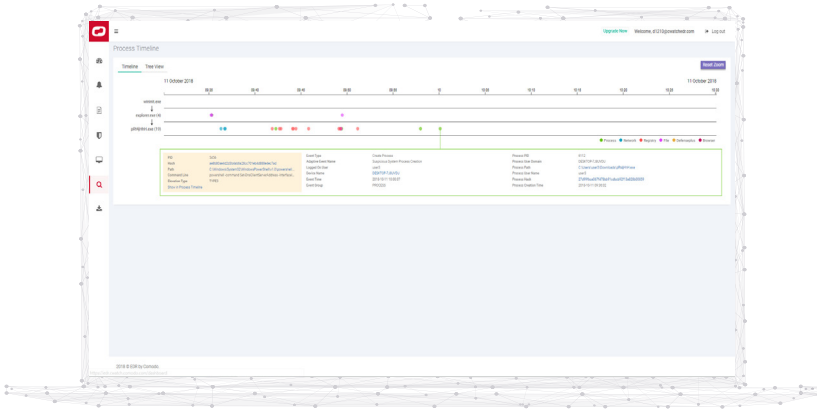


Figure 2A: Process Timeline View

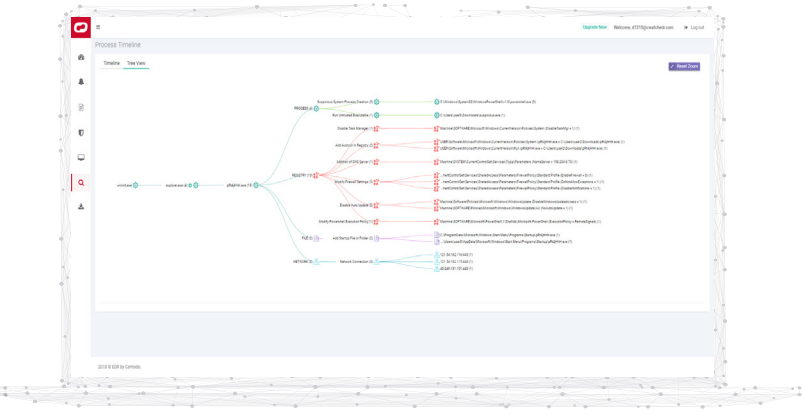


Figure 2B: Process Timeline Tree View

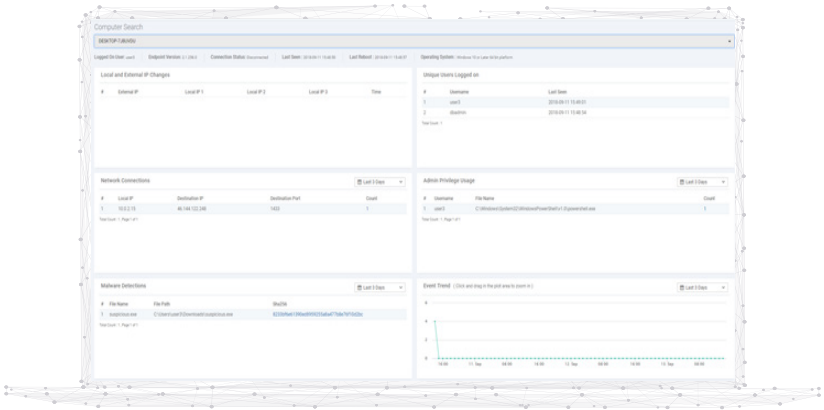


Figure 2C: Device Trajectory Details

Incident Investigation

The event search screen allows analysts to run queries to return any detail at base-event-level granularity, and these queries can be saved for future reference. Aggregation tables are clickable, letting investigators easily drill down into specific events or devices. cWatch EDR also provides details about any hash seen in the environment, including execution history, download summary, creation summary, execution trend, and basic attributes of the hash. File trajectory is also provided to show the hash's incidents as well as the alerts created by the hash and Valkyrie verdict.

Online File-Verdicting System Access

Valkyrie, Comodo's advanced cloud sandboxing and file-verdicting system, continuously checks processes executed in your environment and automatically uploads unknown files for static and dynamic analysis. You can log into the Valkyrie portal using your cWatch EDR credentials to review file verdicts and reports; report summaries are also available in the cWatch EDR portal (figure 3).

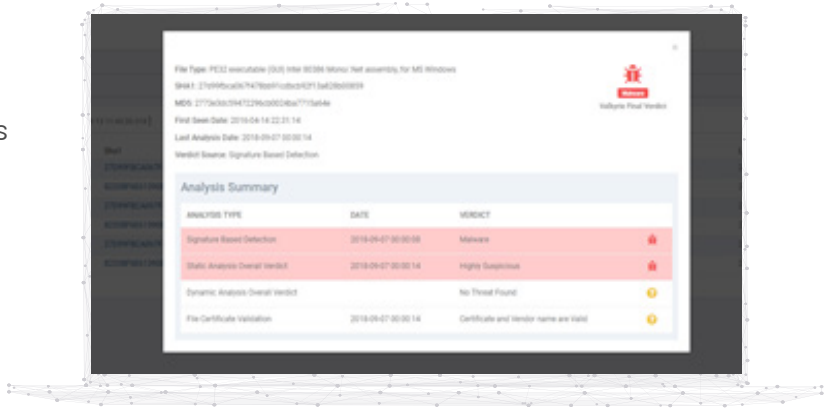


Figure 3: Verdict Report Summary

Instant Time to Value

Whether you're an enterprise with thousands of endpoints or an MSP serving hundreds of customers, the cWatch EDR agent can be instantly deployed via group policy object (GPO) or the Comodo Cybersecurity ITSM, and it automatically updates whenever a new version is released.

Lightweight Agent

cWatch 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.

The agent runs on:

- Windows 7 SP1 or later Enterprise and Business Edition 32- and 64-bit
- Windows 8.1 Enterprise and Professional, 32- and 64-bit
- Windows 10
- Windows Server Editions 2008 to 2016

The low-impact agent uses limited resources:rt

HDD I/O	Negligible
RAM	15-20 MB
CPU	Less than 1% (0.6-0.7% avg.)
HDD	20 MB

A Must-Have for MSPs

cWatch EDR is perfect for MSPs and is available on the Comodo One platform with all multi-tenancy features, including company dashboard and management (figure 4A), as well as single-pane-of-glass management of all Comodo Cybersecurity products (figure 4B).

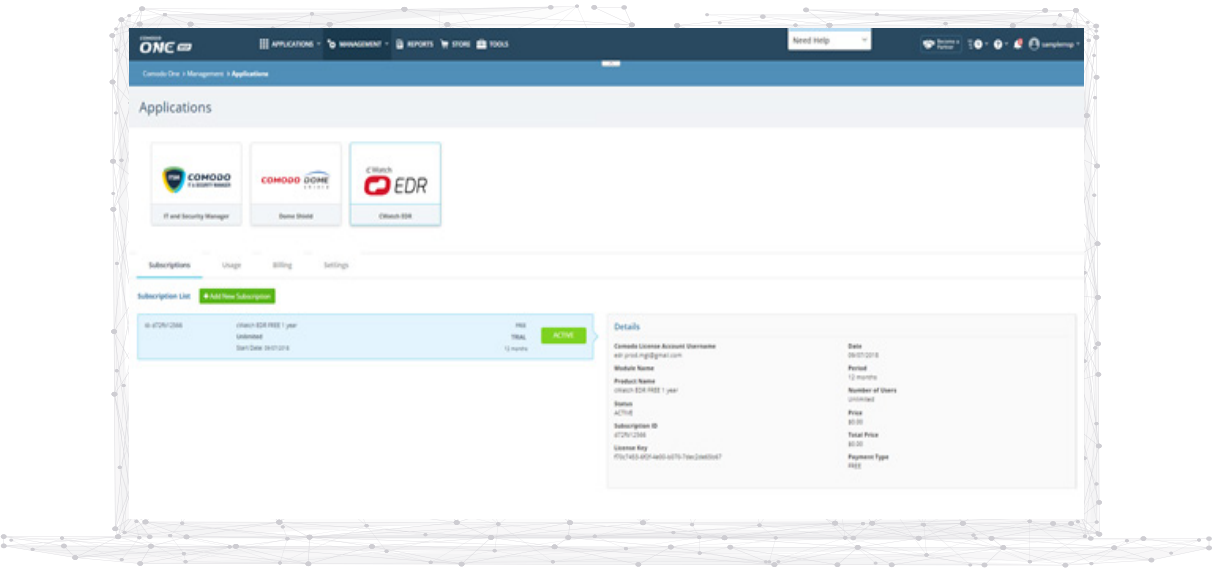


Figure 4A: Company dashboard and management

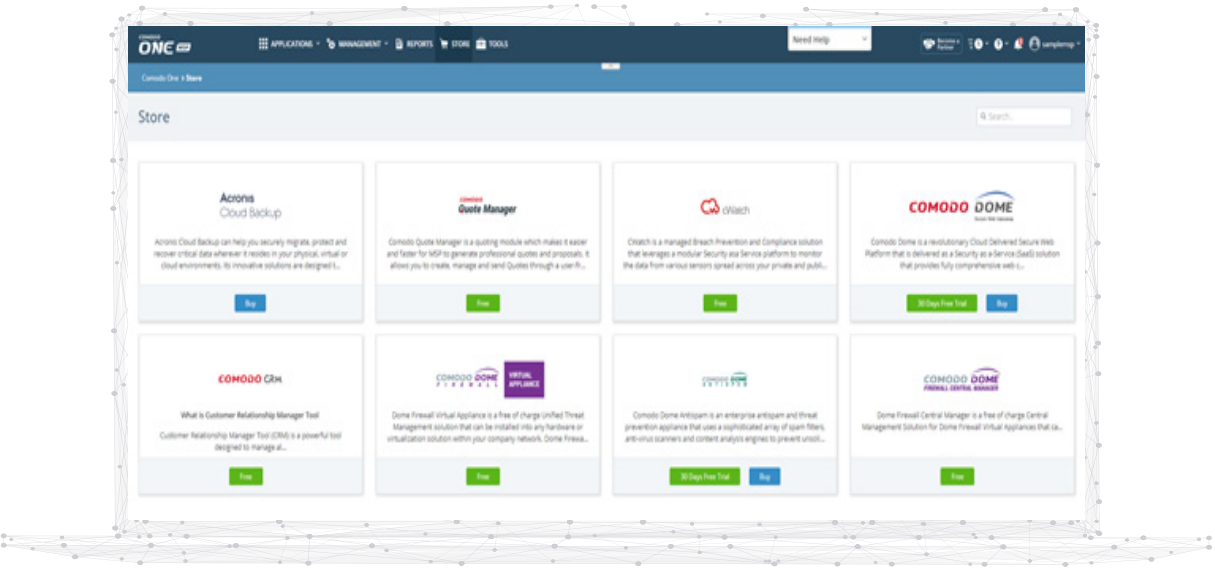


Figure 4B: Manage cWatch EDR and all other Comodo Cybersecurity products from a single pane of glass

Looking for a Managed Solution? We've Got You Covered

For organizations without skilled security analysts in-house, on a tight budget, or looking for a turnkey solution, a fully managed EDR service is available as part of the cWatch managed detection and response **(MDR)**.

You can even bundle in our Advanced Endpoint Protection (AEP) solution, which combines in-house SOC teams, cWatch EDR, and AEP in a fully managed service that provides:

- Customizable policy creation—Allows you to meet varying levels of "strictness"
- Alert prioritization and ticket management process:

1. Ticket is automatically created
2. Ticket is assigned to dedicated SOC staff
3. Case is resolved
4. Customer is informed of issue and resolution

- Constant elimination of false positives—The SOC and product development team collects user feedback to continuously improve security policy quality
- Proactive threat hunting for indicators of compromise (IOCs) performed by dedicated SOC operators
- Preemptive containment and quarantine—Our patented containment "default deny" technology stops malware instantly with surgical precision with "default allow" usability*
- Firewall rule update—Analysts continuously seek out the firewall rules that will provide the very best protection*
- AV scan—Automatic antivirus scan performed against the latest signatures*
- AV block—Known malware is automatically blocked and destroyed*
- Script execution and remote device connection—Comodo Cybersecurity Remote Monitoring and Management (RMM) service enables us to establish connections to remote devices to run any necessary scripts*
- Dedicated SOC personnel available 24/7
- Intrusion triage—Analysts investigate intrusions to decode attackers' modus operandi
- Email notifications—Transparency is critical and we provide email communications to inform you about alerts and the actions we take to resolve the case
- Incident reporting—After an incident, you receive a history of the case, including why it happened, what protections were in place, and suggestions for improving your overall security posture
- Briefings and recommendation sessions—Periodic reports on your assets and other tools and services are available to improve your security posture
- Process analysis examination—Continuous deep analysis of processes executing in your environment with recommendations for addressing potential dangers
- Compliance reporting
- Threat validation—Analysts assess every alert from your endpoints, no matter how many are raised; each is meticulously tracked to find and alleviate root cause
- Early warning for emerging threats—Early analysis of wide-spreading threats, such as ransomware like WannaCry, and immediate definitions of IOCs for fast protection

• Complete and actionable visibility into endpoints—Just because data shown graphically doesn't mean it helps you understand what to do; this is the cWatch EDR reason for being

• High scalability—The cloud architecture enables fast response

• Granular endpoint tracking—Drill down to the base-event level with details including file creation, registry key change, network connection, peripheral device access, etc.

• Visuals enabling correlation of complex attack scenarios—The full attack chain is visualized to deliver insight into what's happening in the environment at any given moment

• Extremely low dwell time—Get the information needed to take action fast

• Instant expertise—Highly skilled SOC operators are an extension of your team

• Real-time incident response—Incidents are addressed in near-real time to minimize damage

• Root-cause identification—The first step of remediation is to find the root cause with a deep understanding of what really happened

• Long data retention period—We retain telemetry data far longer (up to 90 days) than most in the industry, allowing us to perform retrospective analysis to detect attacks with a long dwell time and to improve training for AI models

• Fully managed threat hunting service—A turnkey solution

• Remote connection to any asset

• Default deny security posture with default allow usability

• Patch management and round-the-clock vulnerability assessment

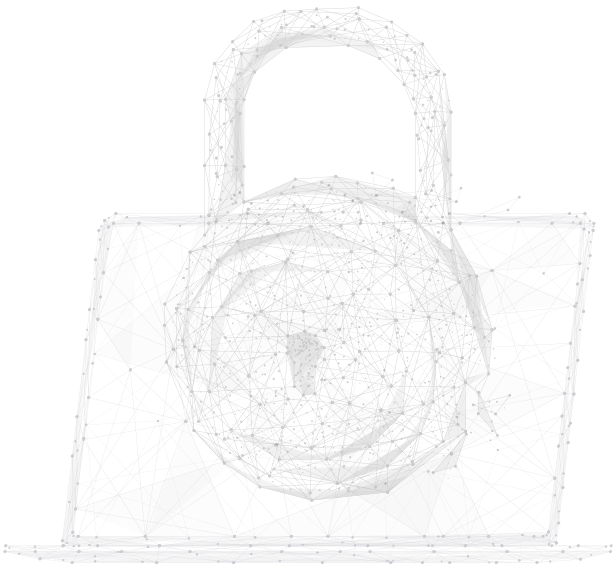
About Comodo Cybersecurity

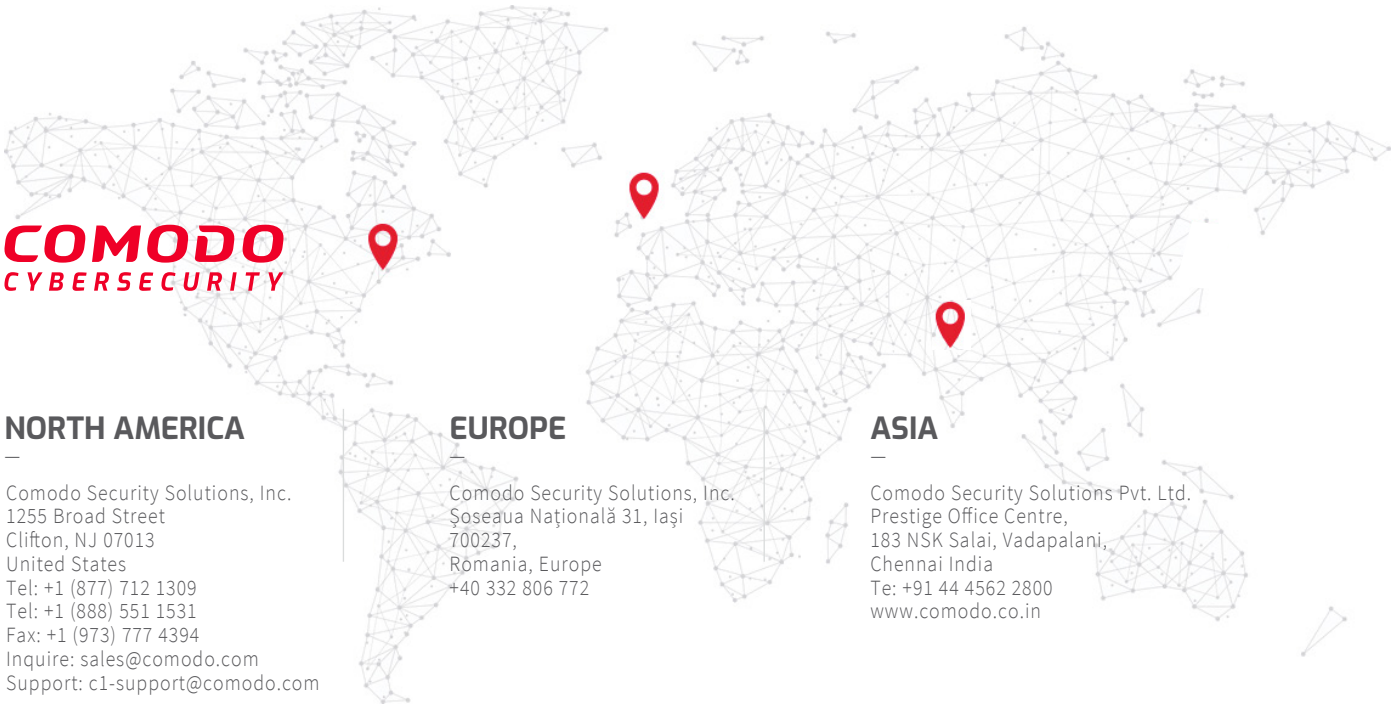
In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. Comodo Cybersecurity has experts and analysts in 193 countries, protects 85 million endpoints and serves 200,000 customers globally. Based in Clifton, New Jersey, the company has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide. For more info, visit comodo.com or our blog. You can also follow us on Twitter (@ComodoDesktop) and LinkedIn.

Try it for Yourself

cWatch EDR is free—get started today.

BEGIN YOUR TRIAL NOW





COMODO
CYBERSECURITY

NORTH AMERICA

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States
Tel: +1 (877) 712 1309
Tel: +1 (888) 551 1531
Fax: +1 (973) 777 4394
Inquire: sales@comodo.com
Support: c1-support@comodo.com

EUROPE

Comodo Security Solutions, Inc.
Şoseaua Națională 31, Iași
700237,
Romania, Europe
+40 332 806 772

ASIA

Comodo Security Solutions Pvt. Ltd.
Prestige Office Centre,
183 NSK Salai, Vadapalani,
Chennai India
Te: +91 44 4562 2800
www.comodo.co.in

VISIT COMODO.COM

REQUEST A DEMO

Try Comodo Cybersecurity by speaking with a security consultant to begin the process to set up a demo or proof-of-concept project. Contact us directly at +1 888-266-6361

Stay in the loop