DRAGON ENTERPRISE

ENDPOINT PROTECTION PLATFORM

COMODO

PROVEN SUCCESS IN PREVENTING BREACHES

TABLE OF CONTENTS

THE EPP SOLUTION

100% Trust Verdict of every unknown file

Comodo Cybersecurity Dragon Enterprise allows you to analyze what's happening across your entire environment at base-event level. This granularity enables accurate root-causes analysis needed for faster and more effective remediation. Proven to be the best way to convey this type of information, process hierarchy visualizations 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. Dragon Enterprise eliminates completixy, reduces operational costs and time to deploy with its' cloud native infrastructure. While reducing total cost of ownership, full deployment would be limited to days! Dragon's security architecture simplifies breach detection, protection and visibility by working for all threat vectors without requiring any other agent or solution.

> ***"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

COMODO

PROVEN SUCCESS IN PREVENTING BREACHES

FULL VISIBILITY AT BASE EVENT LEVEL

Real-time visibility and continuous analysis are the vital elements of the entire endpoint security concept. Dragon Enterprise enables you to perform analysis into what's happening across your environment at base event level granularity. This allows accurate root cause analysis leading to better remediation of your compromises.

Integrated Security Architecture of Dragon Enterprise delivers Full Attack Vector Visibility including MITRE Framework. Dragon Enterprise provides full EDR and EPP. This unique approach provides visibility on all attack vectors and delivering active prevention in all. Dragon Enterprise will extend endpoint security with its' network security components, adding additional layer of security and visibility for all your endpoints. Network component adds DNS layer protection, Secure Browser Isolation, Email On-Click Analysis, Email Containment and Encryption.

CLEAR VISUALIZATION OF EVENT TIMELINES

Providing visualizations along with list of view detailed data is by far the best way of presenting information that will imminently be followed by effective counter actions. Our goal is to provide actionable knowledge rather than just arbitrary information.

SUSPICIOUS ACTIVITY ALERTING

Providing visualizations along with list of view detailed data is by far the best way of presenting information that will imminently be followed by effective counter actions. Our goal is to provide actionable knowledge rather than just arbitrary information.

INCIDENT INVESTIGATION

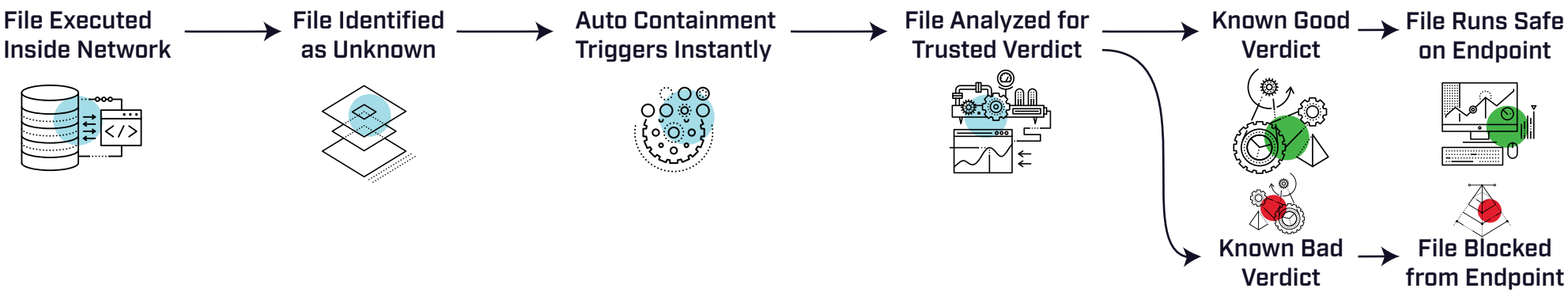
Providing visualizations along with list of view detailed data is by far the best way of presenting information that will imminently be followed by effective counter actions. Our goal is to provide actionable knowledge rather than just arbitrary information.

UNKNOWN FILE CONTAINMENT

Detection and Protection goes hand in hand with Dragon Enterprise. Unlike solutions in market Dragon focuses on delivering Active Breach Protection by combining Endpoint and Network Security. Dragon prevents any breach at its' core by patented Unknown File Containment Technology. Other solutions ' detection capabilities are focused on detection first hence creates risk for Zero-Day Attacks. Dragon Enterprise covers the loose ends with Containment Technology providing 100% protection againt Zero-Day Attacks and Unknown Files even if you are the Patient Zero.

At its' core, Dragon Enterprise provides full EPP functionality and Active Breach Protection with patented Unknown File Containment. Dragon combines Detection and Prevention in a unique method, while preventing attacks that may come from any threat vector, provides full attack chain visibility. Dragon's prevention capabilities are unmatched in market providing 100% coverage for Zero-Day attacks, and in the meantime delivers most powerfull and extensive detection and Threat Hunting capabilties.

Dragon Enterprise delivers Zero Trust Architecture at its' core automatically not trusting anything the system faces and uses patented Unknown File Containment. Dragon Enterprise will run every single unknown file within a low overhead container and will only let them live after tested and verified within our Dynamic and Behavioral Malware Analysis System. Dragon Enterprise's Zero Trust Analysis system will run every single file within customer environment with our Static and Behavioral Analysis System and verdict every single file it faces. This system is the most complicated analysis engine in the World even backed by real human analysts.



ANALYSE AND MANAGEMENT

Unified Policy and Report Management makes Dragon Enterprise easy to manage and reduce operational costs. The product will also cover Managed Detection and Response services which could help reduce opex of customers even further. Our Security Services offer, MDR Threat and Asset Modelling, Risk Management, Anomaly Detection by Profiling, Dark Web Analysis and Automated Reponse.

As user is the weakest link in every security system, Dragon Platfrom provides a unique User Behaviour Analysis and Detection feature, which enables our users to analyze single users based on their behavioral anomalies regardless of the number of machines they use, off-network or even offline usage.

Dragon Enterprise's Threat Intelligence harnesses World's biggest database and updated every minute, will be accessible for Threat Hunting. Combining not only endpoint related data points Dragon uses network, email and DNS based data helping our customers to make better analysis.

ANALYSE AND MANAGEMENT

Dragon Enterprise users are privileged to have access into easy to navigate menus that provided details on endpoints, hashes as well as base and advanced events. Users are provided with detailed file and device trajectory. Plus, they navigate on single events to decode the bigger problems causing compromises.

UNRIVALLED CUSTOMIZATION FOR ALERT DEFINITIONS

Infinitely many IOCs can be created via fully customizable COMODO Recommended Policy. Users are free to make any modifications on the recommended policy as well being able create new ones. These policies create alerts for non-malware attacks such as PowerShell exploits, ransomware and advanced persistent threats.

ALL PACKAGES INCLUDE

COMODO RECOMMENDED SECURITY POLICY

All Dragon Enterprise license holders have access to Comodo's Recommended Security Policy which is fully customizable and covers almost all malware behavior including APTs, file-less attacks, memory and PowerShell abuse.

CUSTOM ALERT DEFINITIONS

Infinitely many IOCs can be created via fully customizable COMODO Recommended Policy. Users are free to make any modifications on the recommended policy as well being able create new ones. These policies create alerts for non-malware attacks such as PowerShell exploits, ransomware and advanced persistent threats.

AUTOMATED NOTIFICATIONS

All Dragon Enterprise license holders have ability to construct their own notification policies as we believe dwell time is a very important parameter in cyber security.

EXTREMELY LOW DWELL TIME

Get the information needed to take action fast.

COMPLETE AND ACTIONABLE VISIBILITY INTO ENDPOINTS

Just because data shown graphically doesn't mean it helps you understand what to do; this is the Dragon Enterprise reason for being

HIGH SCALABILITY

Cloud architecture allows a complete ease of scalability and deployment.

GRANULAR ENDPOINT TRACKING

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

24x7x365 SUPPORT

Comodo customers depend on our outstanding and reliable customer service. Our support team exceeds the standards that are set.

ALL PACKAGES INCLUDE

COMODO GLOBAL THREAT INTELLIGENCE

Comodo verdict systems respond 200 million file queries per day and more than 300 million unknown files each year through tightly integrated Comodo solutions and our active global community of threat researchers. Dragon Enterprise aggregate Comodo's global threat intelligence and managed threat hunting services with information collected from the ultra-lightweight endpoint agent leads to imminent success in fighting with any form of malware.

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. Device trajectory details are provided with separate screens to drill down into devices.

SIMPLE AND FAST DEPLOYMENT

Regardless of how many endpoints you have, it is extremely easy and fast to deploy Dragon Enterprise either via GPO (Group Policy Object) or remote script execution on Comodo ONE portal. Once you make your decision, your time to value is almost non-existent.

Dragon Enterprise embodies everything that is required to stop breaches and requires no reboot or additional configuration! Just by installing the lightweight agent, all features provided with Dragon can be activated and will work on and off network!

INSTANT TIME TO VALUE

Whether you’re an enterprise with thousands of endpoints or an MSP serving hundreds of customers, the Dragon Enterprise 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.

NEED HELP?

LOOKING FOR A FULLY 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 Comodo Managed Detection and Response (MDR).

You can even bundle in our Dragon Enterprise solution, which combines in-house SOC teams, EDR component, and Advance Endpoint Protection in a fully managed service that provides:

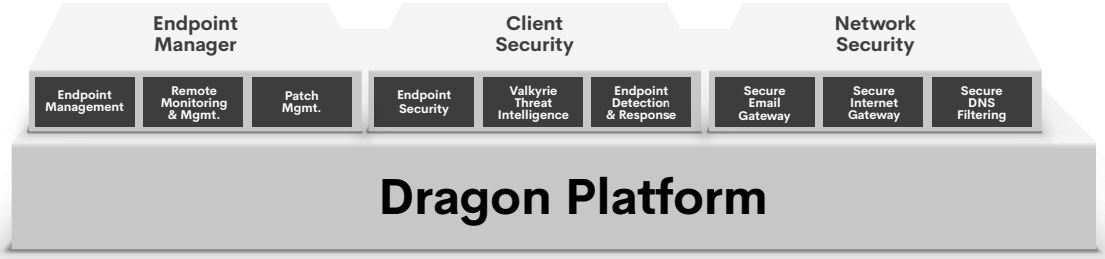
- Customizable policy creation—Allows you to meet varying levels of "strictness"
- Alert prioritization and ticket management process:
- Constant elimination of false positives—The SOC and product development team collects user feedback to continuously improve security policy quality
- Proactive threat 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

**When combined with Comodo Cybersecurity AEP*

ABOUT COMODO

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity provides Active Breach Protection with its cloud-delivered cybersecurity platform. The Comodo Cybersecurity 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 Cybersecurity 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 Clifton, New Jersey, Comodo Cybersecurity 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
1255 BROAD STREET, CLIFTON, NJ 07013 USA

Experienced a breach? Contact us at (888) 551-1531
Visit **comodo.com** for your free 30 day trial