



COMODO

DRAGON MDR

Managed Threat Hunting with Unified Managed Security



COMODO

UNIFIED MANAGED SECURITY

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

REAL-TIME RESPONSE

- > Automate Forensic Collection
- > Block Activity in Real-Time
- > Isolate Endpoint from Network
- > Execute Custom Commands

COMPLETE VISIBILITY

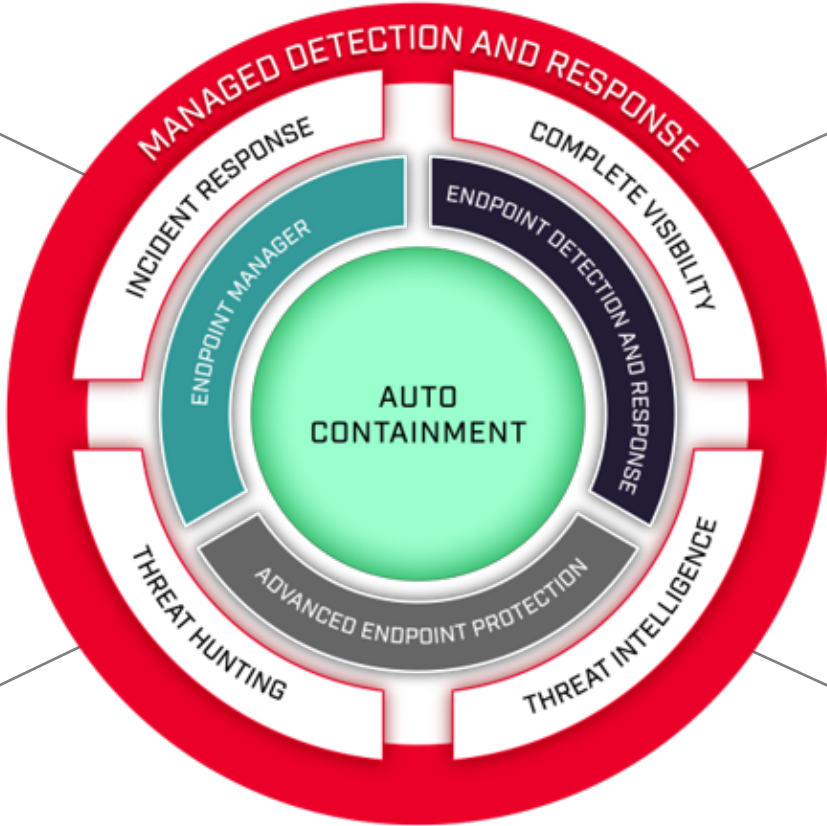
- > Continuously Record Activity
- > Anomalous Behavior & Trends
- > Identify Root Cause

THREAT HUNTING

- > Pivot Quickly Across Dragon Enterprise
- > Advanced Drill-Down Analysis
- > Threat Hunting Queries

THREAT INTELLIGENCE

- > Integrate with Open-Source Feeds
- > Leverage Internal Intelligence
- > 200+ Behavioral Alarms
- > VirusTotal Integration





Ongoing Expert Threat Hunting

KEY FEATURES

A highly trained team of cybersecurity experts will continuously hunt through generated logs looking for anomalous and suspicious activity across your organization

Front Line Incident Response

MDR

Real Time Alerting and Reporting

Your environment will be baselined for known good behavior and we'll alert you on deviations outside those recorded patterns

Threat Intelligence Integrations

Ongoing Expert Threat Hunting



Front Line Incident Response

MDR

Real Time Alerting
and Reporting

Threat Intelligence Integrations

KEY FEATURES

Leverage a team of highly skilled forensic analysts to conduct in-depth investigations

Receive a detailed timeline of attack activity derived from endpoint forensics. Includes analysis of artifacts such as MFT\$, Windows Event Logs, Registry, Web History, etc.

Threat Neutralization support provided during Incident Response to contain any possible breaches

Ongoing Expert Threat Hunting

Front Line
Incident Response

MDR

Real Time Alerting
and Reporting

Threat Intelligence Integrations

KEY FEATURES

Analysts will triage alerts & events generated by your environment and will notify you through the Dragon Enterprise Platform on any activity that may indicate a compromise

Receive high fidelity alerts on attacker activity, malicious programs and tune out false positives

MDR

Ongoing Expert Threat Hunting

Front Line
Incident Response

Real Time Alerting
and Reporting



Threat Intelligence Integrations

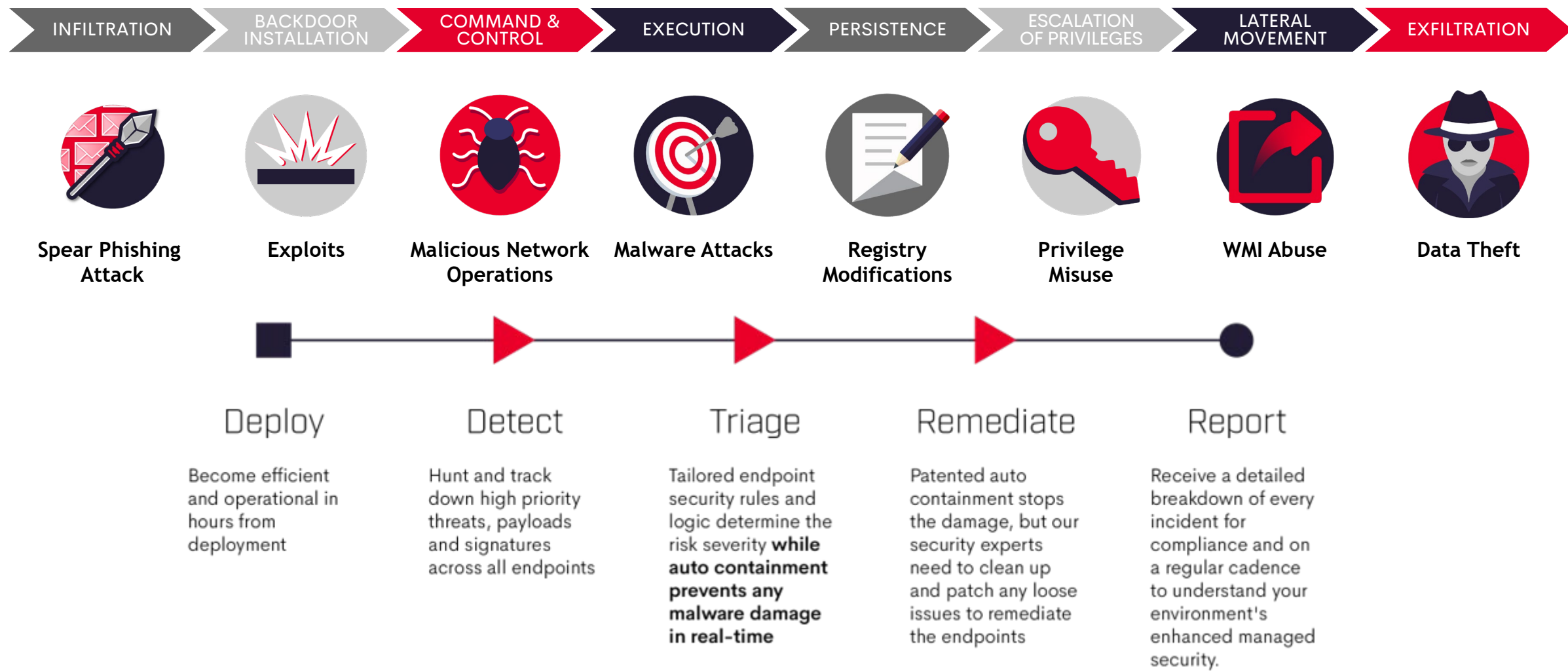
KEY FEATURES

Receive highly refined internal & external threat intelligence feeds to alert or block on Indicators of Compromise

Incorporate your companies own internal intelligence into Comodo's Dragon Enterprise for added coverage

Complete Valkyrie integration for checks on process execution via MD5 hash submission

Visibility Into All Phases of Attack Chain





HIGHLIGHTS OF FINDINGS

Detect lateral movement activity from an unprotected segment of the network / rogue devices that do not have our AEP installed.

<ul style="list-style-type: none">▪ Enforce policies / detect policy violations	<ul style="list-style-type: none">▪ Detecting pre-emptive attacks via network sensor logs and custom Intrusion Detection signatures	<ul style="list-style-type: none">▪ Identifying entrance vectors of attack and providing root cause analysis
<ul style="list-style-type: none">▪ Custom reporting and threat intelligence briefings	<ul style="list-style-type: none">▪ Behavioral-based emerging threat rule sets and IOC's catered to your business' industry	<ul style="list-style-type: none">▪ Baseline network activity to identify anomalous attack patterns when they do occur
<ul style="list-style-type: none">▪ Cloud attack detection via our 0365 & AWS log integrations	<ul style="list-style-type: none">▪ Decoding malware C2 (Command & Control) traffic with network sensor deployed	<ul style="list-style-type: none">▪ Decoding obfuscated command execution to determine intent
<ul style="list-style-type: none">▪ Significantly decrease your overall exposure to cyber security risks by leveraging our MDR's insights and recommendations	<ul style="list-style-type: none">▪ Receive high fidelity threat notifications and avoid being inundated with useless alerts	<ul style="list-style-type: none">▪ Tune noisy endpoint/network events to significantly reduce false positives



ANSWERING THE CHALLENGE

UNIFED MANAGED ENDPOINT SECURITY

What we do differently

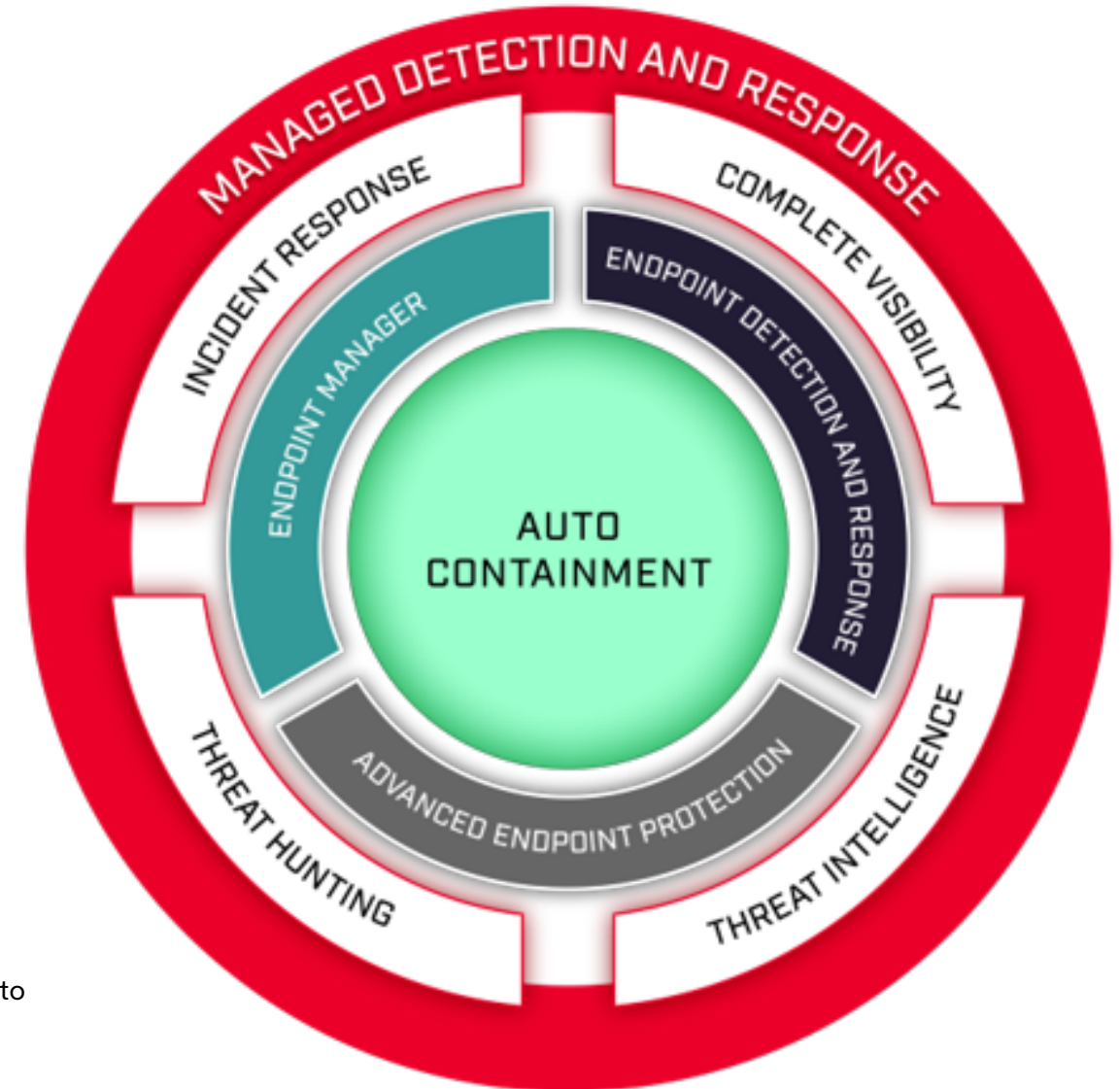
A centralized auto-containment feature is at the core of Active Breach Protection which allows you to reduce your time to detect and respond to zero.

How we eliminate threats

Our unique, patented auto-containment technology prevents known and unknown malware from doing harm at runtime. When an unknown file, a potential malicious threat attempts to execute on an endpoint, the file is immediately encapsulated by Comodo's Auto-Containment Technology, while users can immediately open files and run downloaded scripts and executables.

Why we solve the challenge

The combination of AEP, EDR and EMM – offering Active breach Protection through exploit prevention, advanced threat hunting, and endpoint management to stop ransomware, contain breaches, avoid data loss, and maintain system health.





COMPLETE SECURITY PACKAGE

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

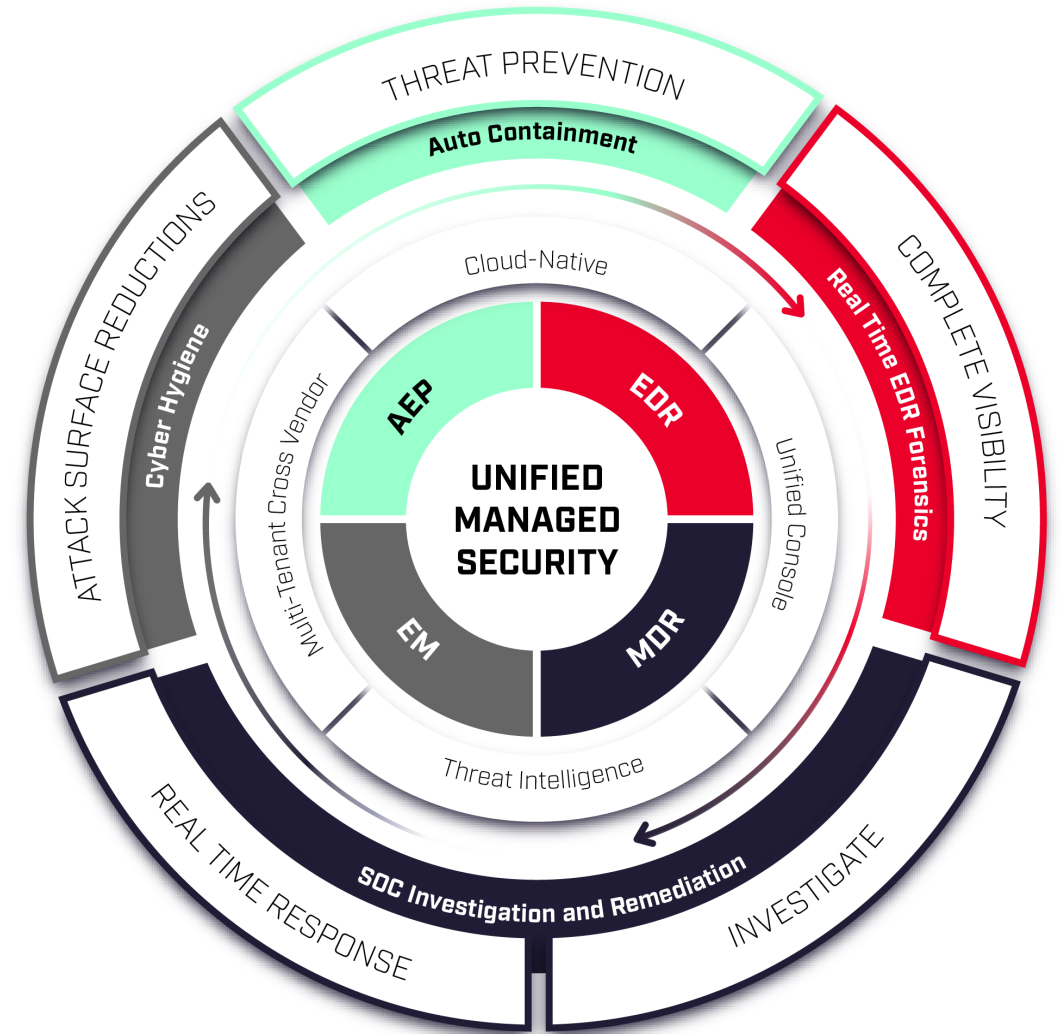
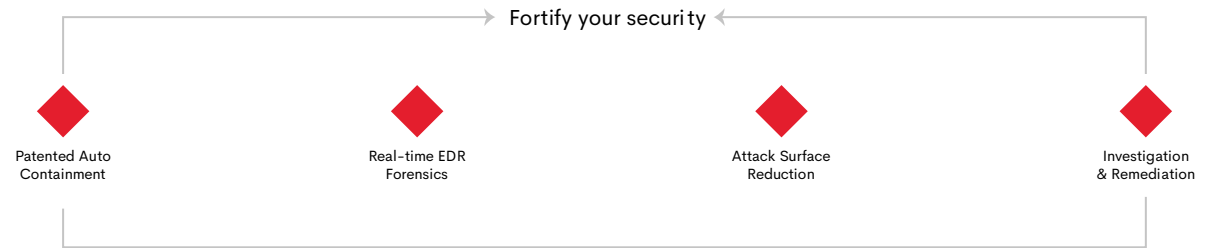
100% Cybersecurity Protection

UNIFIED TECHNOLOGIES FOR

Ultimate Endpoint Security

FULLY MANAGED

Around the Clock SOC Experts





ABOUT US

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/>.



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

