CRYTICA SECURITY

If you can't detect, you can't protect.™

PARTNER PROGRAM

Crytica Security offers a unique and patented technology for detecting and alerting on malware and ransomware within seconds of intrusion. This detection engine seamlessly integrates into existing cyber stacks, SOCS, MDR, EDR & XDR solutions currently deployed to enhance and strengthen an organization's cyber defenses.

COMPETITIVE DIFFERENTIATION:

"If you can't detect" malware at time of injection **"you can't protect"**! Most all cyber solution use basically the same tools to search for malware.

- Artificial Intelligence
- Virus Signature Matching
- Previously Identified Malicious Behavior
- Threat Intelligence Compilations

Yet numerous successful cyber and ransomware attacks occur every day. The number one reason for this is due to a detection gap that current MDR, XDR, or EDR don't resolve.

Organizations can now find and alert on malware at time of injection!

Crytica Security has developed a patented detection engine that is unique in the industry. Instead of searching for malware with AI or other tools which often miss never -before seen malware or the evolving threat of APTs ...

... Crytica monitors "unauthorized changes to executable code" which by definition must be malware. That is how we can find never-before-seen malware and APTs when other solutions cannot.

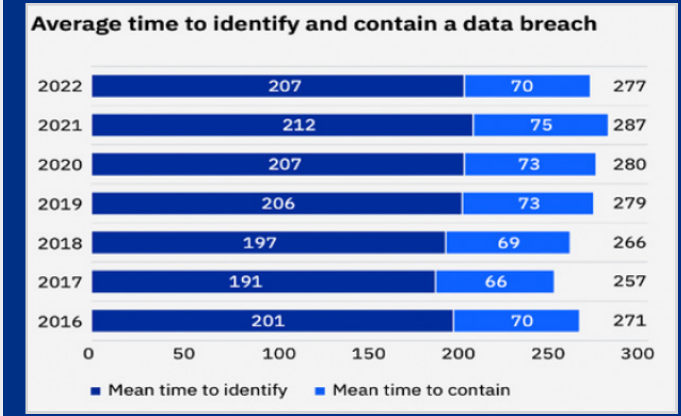
Crytica's **unique detection** engine seamlessly integrates into your existing cyber security stack improving and accelerating your existing malware detection capabilities.

In the war against cybercriminals and malicious state actors, some of the most powerful defensive tools are:

MDR (Managed Detection and Response)

EDR (Endpoint Detection and Response)

XDR (Extended Detection and Response)

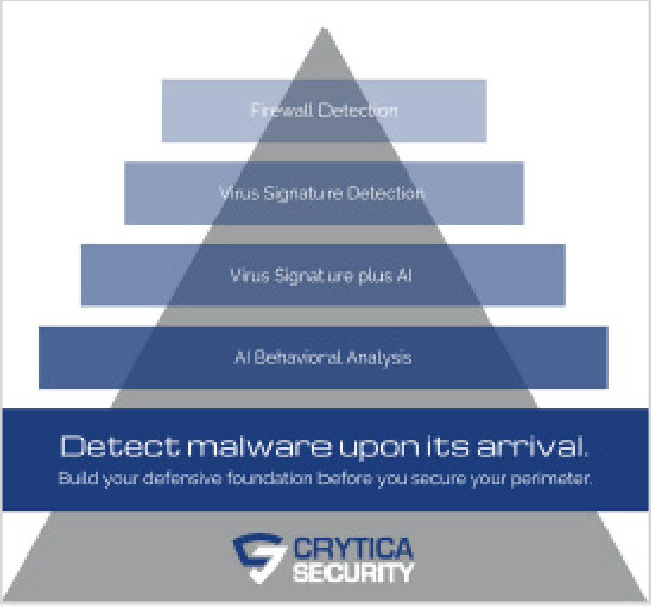

Average time to identify and contain a data breach

Up until now, there has not been effective Detection. Without Detection, there can be no Response.

CRYTICA SECURITY

If you can't detect, you can't protect.™

In the hierarchy of protective measures, Crytica is the foundation, the detector that detects the malware that others miss.


Firewall Detection
Virus Signature Detection
Virus Signat ure plus AI
AI Behavioral Analysis
Detect malware upon its arrival.
Build your defensive foundation before you secure your perimeter.
CRYTICA SECURITY

KEY VERTICALS & PERSONAS

- Healthcare, Finance, Federal/SLED, government contractors.
- MSP, MSSP, MDR/EDR/XDR providers (put "Crytica Inside").
- Firewall companies (put "Crytica Inside").
- CEO, CFO, CIO, CISO, SOC leader and program managers

WHAT TO LOOK FOR IN THE FIELD

- Any organization that is at high risk of cyber and ransomware attacks.
- Any organization that has been the victim of a cyber security or Ransome Ware attack.

OPPORTUNITY ALIGNMENT

- A perfect fit for your existing customer base of cyber companies.
- You bring genuine value to new and/or future customers.
- Builds credibility around your customer base.

TECHNOLOGY ALLIANCE

SentinelOne™

QUALIFYING QUESTIONS

- By the nature of your business are you at risk for a cyber or ransom ware attack?
- Has your enterprise been breached in the past?
- Does your current cyber protection include:
  - Malware detection at time of injection?
  - Find new and never-before-seen malware?
  - True continuous monitoring?
  - Require you to manage numerous daily false positives?
  - Allow you to protect IoT devices at the edge?
  - Alert and absorb attacks on itself?

HOW WE WIN

- Demonstrate our unique capabilities via a "live demo"
- Initiate a Proof of Concept in prospects IT environment
- Show prospects a Breach Analysis of recent attacks and how Crytica would have caught it before it could launch.
- Seamless integration into an existing cyber stack makes it an easy add to their protection

CRYTICA SECURITY

If you can't detect, you can't protect.™

INDUSTRY ACKNOWLEDGMENT

> **"The detection gap in cybersecurity leads to a continuous drain on security operations teams, and high costs for organizations. Closing the detection gap requires a change in posture towards cybersecurity and can be addressed through better technology and solutions like Crytica Security".**
>
> **~ February 2, 2023 | Ben Bajarin - Creative Strategies & WSJ**

Zero-Day Malware Detection

Blazingly Fast - continuous - Device Scanning

Elimination of False Positives

Instantaneous Alerting & Notification

Resouce-efficient probe processing

Rapid onboarding and deployment

CUSTOMER GAINS

- Strengthen existing cyber security solutions ability to defend and defeat cyber attacks and ransomware.
- The ability to detect and alert on malware within seconds at time of injection.
- Eliminate the cost and maintenance of managing false positives.
- Gain ability to detect malware in IoT devices at the edge.
- Conduct true continuous monitoring with a <70KB agent.
- Seamless integration into existing cybers stacks including MDR, XDR and EDR solutions.
- Significantly enhanced protection against cyber threats at a low cost.
- A more complete compliance profile to minimize risk of lawsuits and/or cyber insurance termination.
- Cyber protection not affected by the changing threat posed by new malware variants.
- Detection and alerts sent to existing remediation platforms eliminating the need for another "pane of glass" to monitor.
- Peace of mind.

USE CASES

- Advanced Persistent Threat Detection (APT)
- Cyber protection for IoT devices
- Polymorphic malware
- Preemptive malware
- 5th Column malware
- AI generated malware

SCHEDULE A DEMO

to see Crytica's Detection Engine in action

☎ 877-614-9300

✉ info@cryticasecurity.com