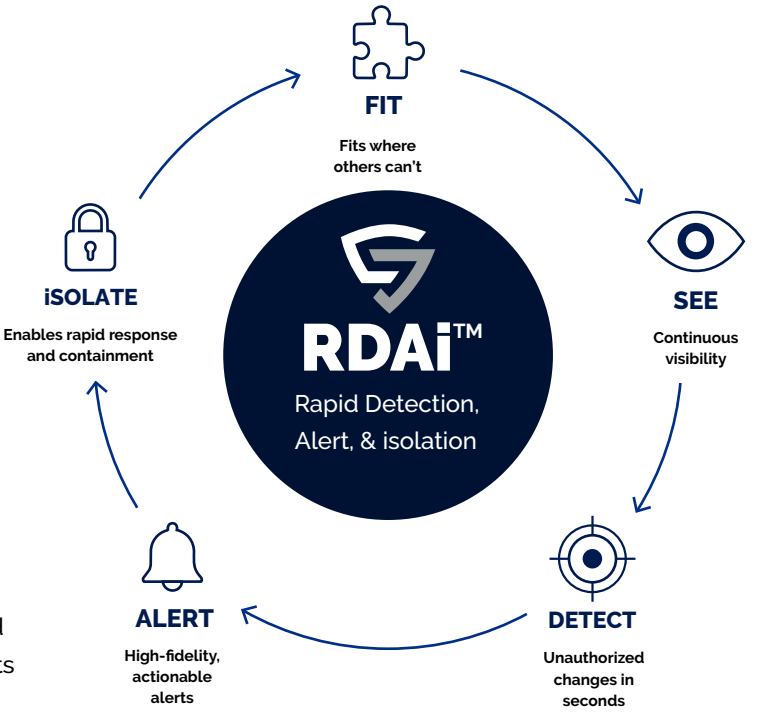
CRYTICA SECURITY

RAPID THREAT DETECTION

Purpose Built to Fit, See, Detect, Alert, and isolate in Seconds.

Crytica's patented RDAi™ system embeds inside OT, IoT, and IT devices to detect unauthorized changes to instruction sets and deliver deterministic, actionable alerts in seconds.



70 KB Probe size at its smallest for edge devices

180 Seconds or less to detect threats versus months

≤10% Or less CPU usage for constrained environments

THE CHALLENGE

Traditional cybersecurity wasn't built for every device.

Critical infrastructure environments rely on OT, IoT, embedded systems, industrial controllers, and legacy devices where conventional security solutions often cannot operate.

Without visibility, unauthorized changes become hidden risks.

Cybersecurity Begins with Trusted Rapid Detection

Every cyberattack begins with an unauthorized change. Powered by Instruction-Set Integrity Monitoring (iNSiM™), Crytica delivers deterministic, high-fidelity alerts that help organizations detect threats faster, respond with speed and confidence, and strengthen operational resilience.

IF YOU CAN'T DETECT, YOU CAN'T PROTECT.®

WHY ORGANIZATIONS CHOOSE CRYTICA

Deterministic Detection
Detects threats and performance anomalies within seconds without false positives.

Compact, Robust Code
Runs in OT, IoT, and IT environments with a footprint as small as 70KB with nominal performance impact.

Actionable Alerts
Generates deterministic Threat Alerts and Performance Alerts from unauthorized system changes and operational anomalies.

Built to Integrate
Delivers deterministic alerts into existing cybersecurity platforms, enabling rapid SOC response within familiar workflows.

Resilient Architecture
Maintains continuous detection through a distributed, mutually monitoring mesh.

Intelligent isolation
Triggers response workflows to isolate compromised devices based on alerts.

Continuous Visibility
Provides continuous insight into protected systems where traditional security solutions cannot operate.

Reduce average malware dwell time from months to seconds.
Schedule a demonstration to see deterministic detection in action.

Scan to learn more or visit:
www.cryticasecurity.com

HOW RDAi™ WORKS

Rapid Detection, Alert, and isolation

1 FIT

Deploys across the environments you need to protect.

OT / ICS | SCADA | IT SYSTEMS | IoT DEVICES | EMBEDDED SYSTEMS | EDGE ENVIRONMENTS

One architecture. Any environment.

2 SEE

Continuously observes protected devices

PROBE
OBSERVES CONTINUOUSLY

Instruction Sets (iNSiM™)
Detects unauthorized instruction-set changes.

Operational Performance
Detects operational performance anomalies.

- Minimal Footprint
- Signed Scans

3 DETECT

Compares each scan to a trusted baseline.

DETECTOR

INCOMING SCAN from Probe

BASELINE COMPARISON Trusted Baseline

DETECTION ENGINE Deterministic Analysis

UNAUTHORIZED CHANGE?

or

PERFORMANCE ANOMALY?

DETECTED ELEMENTS (Examples)

Element Added | Element Deleted | Content Modified | Permissions Modified | Ownership Modified | Modification Time Changed

HEARTBEAT MESH
(Always On)

- Mutual Monitoring
- Continuous Health Validation
- Automatic Recovery

4 ALERT

Generates trusted threat and performance alerts.

THREAT ALERTS
Unauthorized change detected.

RDAi™
TRUSTED ALERTS

PERFORMANCE ALERTS
Operational anomaly detected.

High-fidelity. Deterministic. Actionable.

5 iSOLATE

Trusted Alerts integrate with your existing security stack.

YOUR EXISTING SECURITY STACK RESPONDS:

SIEM | SOAR | XDR | AI/ ANALYTICS | DATA PLATFORMS | ITSM | CUSTOM APIS

Powered by Crytica Trusted Alerts

INVESTIGATE → *ESCALATE* → *iSOLATE* → *REMEDIATE* → *REPORT*

WHY IT MATTERS

REDUCE UNCERTAINTY
Know what actually happened.

ELIMINATE NOISE
Remove guesswork and false positives

INCREASE CONFIDENCE
Trusted deterministic alerts you can trust.

ACCELERATE RESPONSE
Act faster with accurate, actionable alerts.

MAXIMIZE INVESTMENT
Leverage existing security tools.