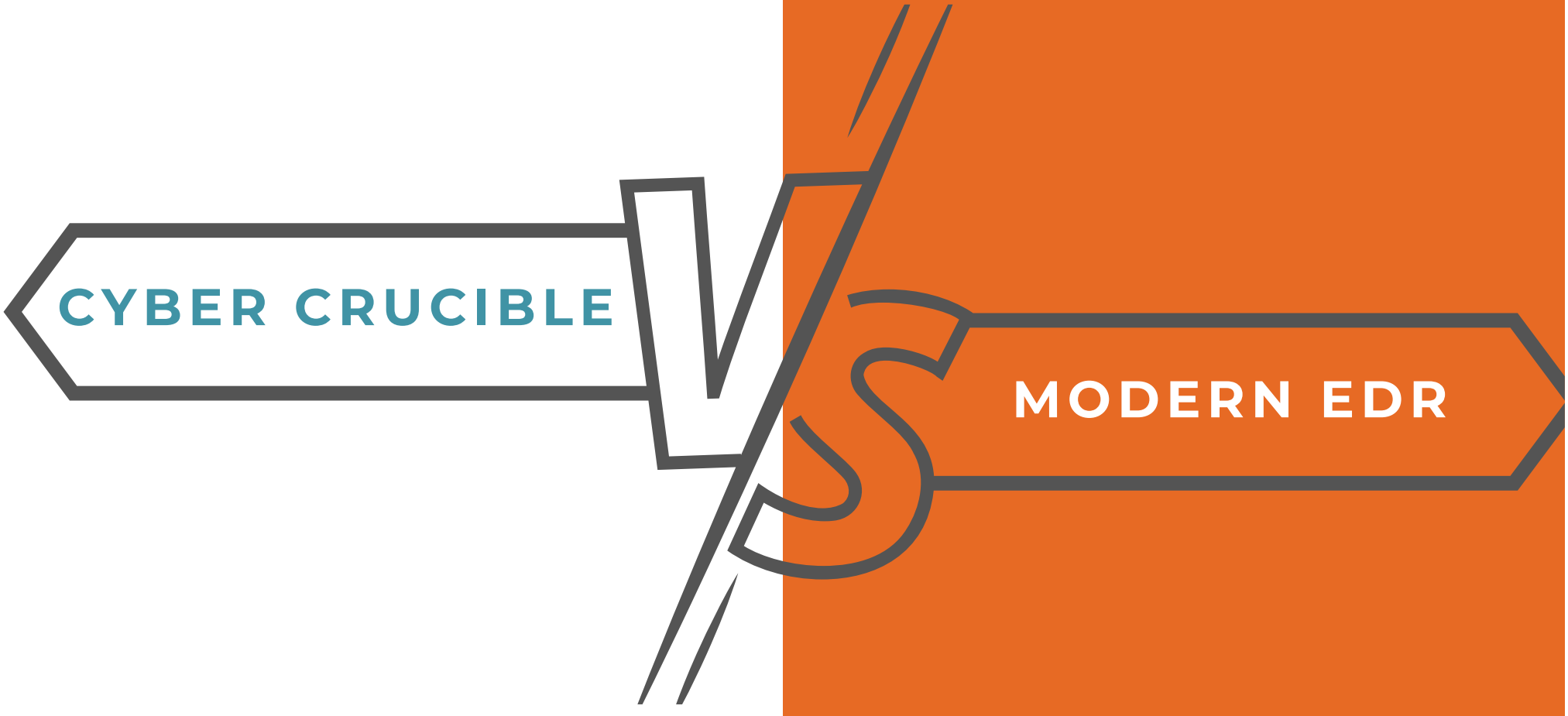

CYBER CRUCIBLE
VS
MODERN EDR

Modern Resilience

CYBER CRUCIBLE



Design

Built to counter hackers using automated techniques.



Defense Mechanism

Utilizes novel telemetry sources and a patented analytics engine for immediate defense.



Effectiveness

Provides advanced protection against zero-day attacks.

EDR/XDR



Design

Relies on predefined signatures and historical data.



Defense Mechanism

Analyzes endpoint data to identify suspicious activities.



Effectiveness

Useless against zero-day attacks due to reliance on known threat behaviors and patterns.

Cost & Efficiency

CYBER CRUCIBLE

Labor Costs

Automation reduces or eliminates labor costs.

Efficiency

AI-driven technology eliminates costs associated with false positives, manual configurations, and extra security staffing.

Outcomes

Automation gives back time and money, improving TCO and ROI.

EDR/XDR

Labor Costs

Requires significant human intervention for analysis and response, leading to higher labor costs.



Efficiency

Generates numerous false positives, requiring manual investigation and resolution.

Outcomes

High operational costs and labor-intensive processes reduce overall ROI.

Accuracy

CYBER CRUCIBLE

False Positives

Advanced AI and automated processes remove unnecessary variables, ensuring hyper-accurate detection.

Accuracy

Maintains 100% true positive performance with record-setting low false positives.

Outcome

Security teams can focus on real threats, enhancing overall security.

EDR/XDR



False Positives

High number of false positives due to rule-based detection.



Accuracy

Useless against new and sophisticated attacks.

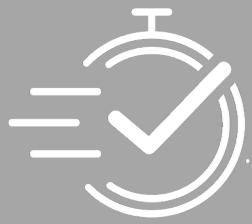


Outcome

High rate of false positives and manual investigation reduce efficiency.

CYBER CRUCIBLE

EDR/XDR



Detection and Response Time

Ensures real-time detection and mitigation of threats.



Detection and Response Time

Detects threats after infiltration, leading to delayed responses.



Automation

Identifies and neutralizes threats instantly, preventing potential damage.



Automation

Requires manual intervention to analyze and respond to threats.

Detection & Mitigation



Outcome

Allows security teams to focus on strategic tasks, ensuring continuous security and operational efficiency.



Outcome

Slower response time and increased risk of damage.

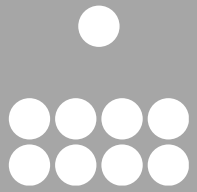
Business Continuity

CYBER CRUCIBLE



Workflow

Suspends only the affected malware processes, ensuring proactive defense and no business downtime.



Performance

Engineered to minimize system overhead and operate on the edge, reducing latency and reliance on external networks.



Outcome

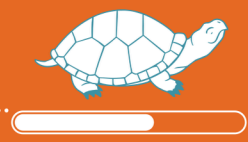
Operates seamlessly without business interruptions, maintaining high performance even under heavy loads.

EDR/XDR



Workflow

Requires manual intervention to respond to detected threats, potentially interrupting business operations.



Performance

Can be resource-intensive and relies on cloud services, which can introduce latency and dependency on external networks.



Outcome

Manual processes can lead to workflow disruptions and performance degradation.

Network Usage

CYBER CRUCIBLE



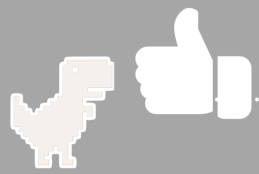
Network Dependence

Utilizes edge computing to operate at full capacity even when network connectivity is disrupted.



Performance

Operates autonomously, maintaining robust security without reliance on network connectivity.



Outcome

Ensures continuous protection and operational stability regardless of network conditions.

EDR/XDR



Network Dependence

Relies on network connectivity for data analysis and threat intelligence updates.



Performance

Centralized data processing introduces latency and vulnerability to network disruptions.



Outcome

Dependence on network connectivity can compromise effectiveness in isolated network environments.