

ENDPOINT DETECTION & RESPONSE (EDR/XDR).



Antivirus asks whether a file matches a known bad signature — **EDR and XDR ask whether behavior looks malicious**. They watch what processes actually do on the endpoint, then correlate that activity across identity, email, and cloud to catch what static signatures miss.

- BEHAVIORAL DETECTION
- ENDPOINT TELEMETRY
- AUTOMATED RESPONSE
- CROSS-DOMAIN CORRELATION

01 THE MECHANISM



Continuous Telemetry
Recording process, file, and network activity on every endpoint, **not just scanning at a point in time**.



Behavioral Detection
Flagging patterns of malicious behavior — **not just known bad file signatures**.



Automated Response
Isolating a compromised endpoint or killing a malicious process **the moment confidence is high enough**.

02 THE FLOW

The Detection Cycle CONTINUOUS

1

Endpoint agents stream process, file, and network telemetry to a **central analysis engine** in real time.

2

Behavioral analytics and threat intelligence **correlate that telemetry** against known attack patterns.

3

High-confidence detections **trigger automated containment** before an analyst opens the alert.

The XDR Cycle CROSS-DOMAIN

1

Signals from endpoints, identity, email, and cloud workloads are **normalized into one data model**.

2

Correlation engines link related signals across domains into a **single incident**, not dozens of alerts.

3

Analysts investigate **one correlated story** instead of piecing fragments across five tools.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Endpoint Telemetry	Continuously records process, file, and network activity on every managed device.
Behavioral Detection	Flags malicious patterns of activity rather than relying on known signatures alone.
Automated Response	Isolates endpoints or kills processes automatically at high detection confidence.
Cross-Domain Correlation	Links endpoint, identity, and cloud signals into a single investigable incident.

04 ENDPOINT DEFENSE APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Signature-Based Antivirus Alone	No	Misses novel malware and fileless attacks with no matching signature.
EDR Without Cross-Domain Context	No	Sees the endpoint but misses the identity or cloud pivot around it.
Manual Alert Triage Only	No	Analysts drown in isolated alerts faster than they can correlate them.
Prevention Tools With No Visibility	No	Blocks what it recognizes but can't investigate what it doesn't.
EDR/XDR (Telemetry + Behavior + Correlation)	Yes	Turns fragmented signals into one story with automated containment.

ENDPOINT DETECTION.

DETECT · CORRELATE · CONTAIN

05 PROGRAM OPERATIONS

Dwell time is the real cost metric.

The faster detection-to-containment closes, the less an attacker can do with access.

Alert fatigue kills detection programs.

Thousands of unprioritized alerts get ignored, not investigated.

Automated response needs guardrails.

Aggressive auto-isolation on the wrong system can cause its own outage.

Coverage gaps are where attackers live.

An unmanaged endpoint is invisible to the tool meant to protect it.

06 CONTROL MAPPING

NIST SP 800-61

Incident handling guidance that EDR/XDR detection and response directly support.

MITRE ATT&CK

Adversary tactics framework used to build and validate detection logic.

NIST CSF 2.0

Detect and Respond functions covering endpoint and cross-domain threats.

CIS CONTROL 10

Malware defenses guidance for endpoint detection and response programs.

07 WHAT THIS DOES NOT SOLVE

Living-off-the-land techniques

Attackers using legitimate admin tools generate less anomalous behavior to flag.

Unmanaged and shadow devices

A tool can't protect an endpoint it was never installed on.

Alert-response gaps

Detection without staffing to act on it just produces a longer alert queue.

Supply chain & firmware attacks

Threats below the OS layer are largely invisible to endpoint agents.

08 MYTHS VS. REALITY

MYTH	REALITY
"EDR replaces the need for antivirus."	Modern EDR platforms typically include and build on signature prevention, not skip it.
MYTH	REALITY
"XDR is just EDR with a new name."	XDR specifically adds cross-domain correlation that endpoint-only tools can't do.
MYTH	REALITY
"More alerts mean better detection."	Unprioritized alert volume buries the real threats analysts need to see.
MYTH	REALITY
"Automated response is always safe to enable."	Auto-containment on critical systems needs deliberate guardrails first.
MYTH	REALITY
"Deploying the agent everywhere finishes the job."	Tuning detection logic and playbooks is the ongoing work.

09 SPEAK THE PROGRAM — KEY TERMS

EDR

Endpoint Detection and Response: continuous monitoring and response on individual devices.

XDR

Extended Detection and Response: correlates signals across endpoints, identity, and cloud.

DWELL TIME

The time between initial compromise and detection or containment.

BEHAVIORAL DETECTION

Identifying malicious activity by what it does, not by matching a signature.

MITRE ATT&CK

A knowledge base of adversary tactics and techniques used to build detection coverage.

CONTAINMENT

Isolating or restricting a compromised endpoint to stop further spread.