

EDR & XDR SECURITY.



A signature can only catch what's already been seen before — **modern detection has to watch what a process actually does, and increasingly, whether the detection agent itself is still alive to watch it.**

- BEHAVIORAL TELEMETRY
- CROSS-LAYER CORRELATION
- ATT&CK-MAPPED DETECTION
- REMOTE CONTAINMENT

01 THE MECHANISM



Behavioral Detection vs. Signature Matching

Signature-based antivirus checks a file against known-bad hashes, which a single byte change defeats entirely — **EDR instead watches what a process actually does**, catching malicious behavior chains regardless of whether the file has ever been seen.



Living-Off-the-Land Techniques

Attackers increasingly carry out malicious actions using legitimate, pre-installed tools like PowerShell and WMI rather than dropping custom malware to disk — **there's no malicious file for a signature to ever match.**



EDR Agent Tampering

Sophisticated attackers specifically target the detection agent itself, exploiting a vulnerable signed driver to gain kernel-level access and blind the EDR before deploying a payload — **disabling the alarm is now a standard attack step.**

02 THE FLOW

The Correlated, Cross-Layer Program

CONTAINED

- Telemetry from endpoints, identity, email, and network is correlated centrally, so **a low-signal event at any single layer is evaluated alongside everything else happening to that user or asset.**
- Detection logic is mapped against a structured framework of known adversary techniques, catching behavior chains rather than waiting for a specific malicious file to appear.
- A confirmed threat triggers automated containment, isolating the endpoint or killing the process directly from the console, so **response happens in minutes, not after manual investigation.**

The Siloed, Endpoint-Only Program

EXPOSED

- Endpoint telemetry is reviewed in isolation, with no visibility into what the same user's identity or email activity looked like around the same time.
- Detection relies on known-bad signatures, so **living-off-the-land activity using legitimate system tools generates no alert at all.**
- Response depends entirely on an analyst noticing and manually acting on an alert, so **a validated threat can sit unaddressed for hours while it spreads.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Continuous Behavioral Telemetry	Records process execution, file, registry, and network activity on every endpoint, providing the raw data behavioral detection actually depends on.
Cross-Layer Signal Correlation	Combines endpoint telemetry with identity, email, and network signals, surfacing multi-stage attacks invisible at any single layer alone.
MITRE ATT&CK-Mapped Detection Logic	Structures detection rules against a documented taxonomy of adversary techniques, rather than an ad hoc list of known-bad indicators.
Remote Containment & Response	Enables isolating a host, killing a process, or rolling back changes directly from a central console, without waiting for physical access to the machine.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Signature-Based Antivirus Alone	No	Misses any malware that hasn't already been cataloged, and living-off-the-land activity using legitimate tools never matches a signature.
Endpoint Telemetry Reviewed in Isolation	No	Misses multi-stage attacks where each step looks unremarkable alone and only forms a pattern when correlated with identity or email activity.
Detection With No Response Automation	No	Identifies a threat but still depends on a human to manually contain it, leaving a validated compromise active while it waits for attention.
Unmonitored, Unmanaged Devices	No	Provides no visibility into BYOD, IoT, or ephemeral cloud workloads that never had an agent installed on them in the first place.
Cross-Layer Telemetry + ATT&CK-Mapped Detection + Automated Containment	Yes	Covers visibility, detection logic, and response speed together, rather than any one alone.

EDR & XDR SECURITY.

DETECT · CORRELATE · CONTAIN

05 PROGRAM OPERATIONS

EDR generates far more telemetry than any team can manually review.

A program's real effectiveness depends on detection tuning that separates genuine threats from noise, not just how much data is collected.

XDR's value is correlation, not more sensors.

Adding more data sources without a way to connect signals across them just produces more isolated alerts, not better detection.

Disabling the EDR agent is now a documented attack step, not an edge case.

Techniques like BYOVD, exploiting a legitimate signed driver for kernel access, exist specifically to blind detection first.

An EDR agent only sees what it's installed on.

Unmanaged devices, OT equipment, and ephemeral serverless workloads remain a structural blind spot regardless of agent quality.

06 CONTROL MAPPING

MITRE ATT&CK FRAMEWORK

The industry-standard taxonomy of adversary tactics and techniques used to structure EDR/XDR detection logic and evaluate product coverage.

MITRE ATT&CK EVALUATIONS

An independent testing program that measures how well EDR/XDR products detect emulated real-world adversary behavior.

NIST SP 800-61

Incident handling guidance that frames how detection and containment capabilities fit into a broader incident response process.

CISA ENDPOINT DETECTION GUIDANCE

Federal guidance promoting EDR adoption and visibility as a baseline expectation for civilian agency networks.

07 WHAT THIS DOES NOT SOLVE

Unmanaged & Unmonitored Devices

An EDR agent only provides visibility into systems it's actually installed on, leaving BYOD, IoT, and OT equipment structurally invisible.

Application-Layer Vulnerabilities

Detecting malicious endpoint behavior doesn't fix a vulnerability in the application code an attacker exploited to get there.

Credential-Based Access, No Malicious Behavior

An attacker using stolen but valid credentials through entirely normal-looking actions may never trigger behavioral detection at all.

Analyst Capacity & Alert Fatigue

Better detection still depends on a team with capacity to actually investigate what it surfaces, which no amount of tooling alone fixes.

08 MYTHS VS. REALITY

MYTH

"EDR replaces the need for antivirus entirely."

REALITY

Most EDR platforms **still include signature-based detection as one layer** — the shift is toward behavioral analysis as the primary layer, not eliminating signatures entirely.

MYTH

"More telemetry always means better detection."

REALITY

Telemetry nobody has the capacity to tune or review **just becomes noise that buries the alerts that matter**, rather than improving detection outcomes.

MYTH

"Living-off-the-land attacks are rare and theoretical."

REALITY

Using legitimate tools like PowerShell and WMI is **one of the most common techniques in real-world intrusions**, precisely because it evades signature-based detection.

MYTH

"If an EDR agent is installed, that endpoint is protected."

REALITY

Attackers specifically target **disabling or blinding the agent itself**, using techniques like exploiting a vulnerable signed driver, before deploying their actual payload.

MYTH

"XDR is just EDR with a new name."

REALITY

XDR's defining capability is **correlating signals across endpoint, identity, email, and network layers** — EDR alone only sees the endpoint.

09 SPEAK THE PROGRAM — KEY TERMS

EDR (ENDPOINT DETECTION & RESPONSE)

Continuous **behavioral monitoring and response capability** on individual endpoints, built to catch what signature-based antivirus misses.

XDR (EXTENDED DETECTION & RESPONSE)

Correlates telemetry **across endpoint, identity, email, and network layers** into a unified detection view, rather than analyzing each in isolation.

LIVING-OFF-THE-LAND (LOTL)

Using **legitimate, pre-installed system tools** to carry out malicious actions, avoiding the need for a custom malicious file a signature could catch.

MITRE ATT&CK

A **documented taxonomy of adversary tactics and techniques**, used to structure detection logic and evaluate product coverage.

BYOVD (BRING YOUR OWN VULNERABLE DRIVER)

An attack technique that **exploits a legitimately signed but vulnerable driver** to gain kernel-level access and disable EDR protections.

ALERT FATIGUE

The operational risk of **too many low-value alerts causing analysts to miss or deprioritize a genuine threat** buried among the noise.