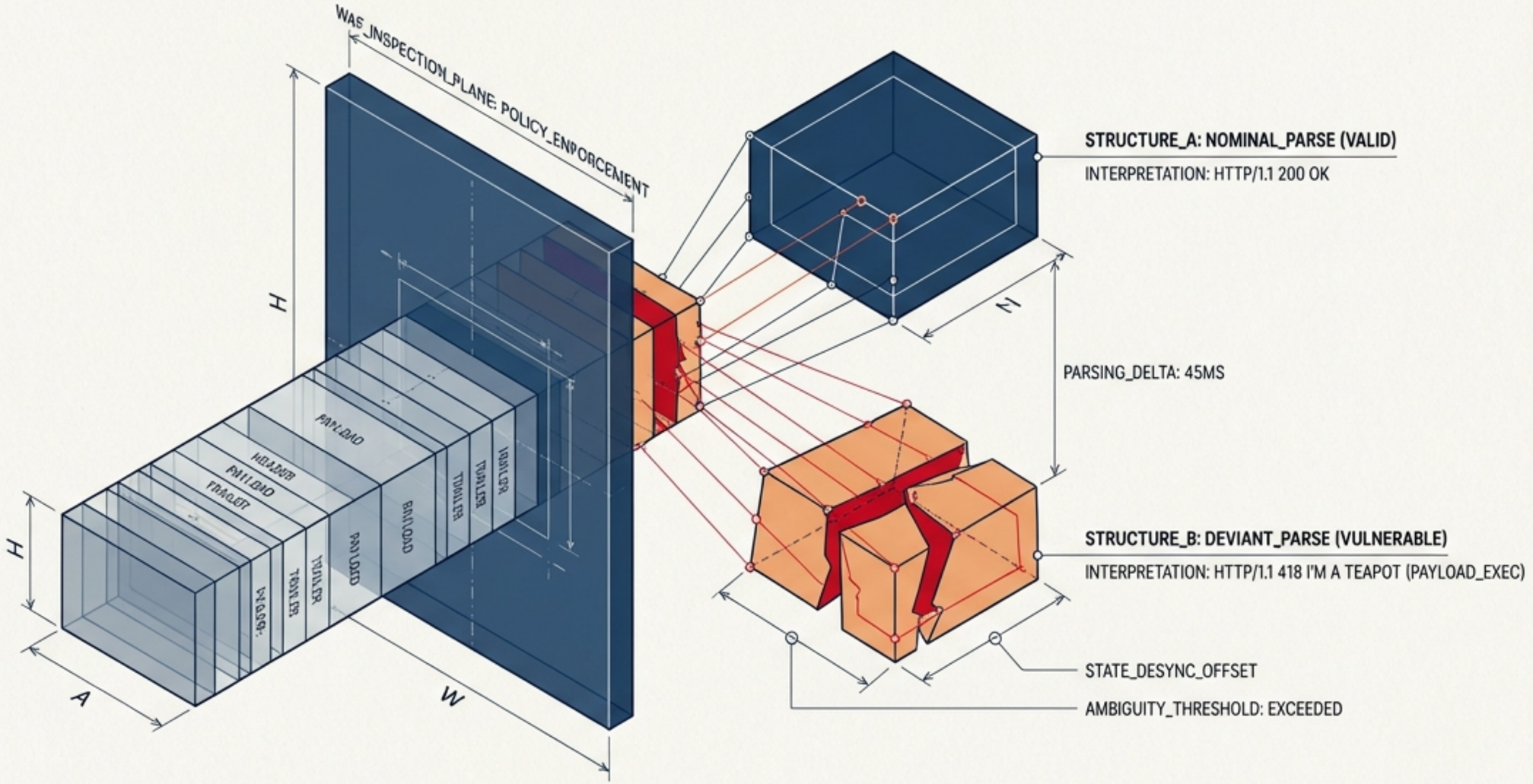
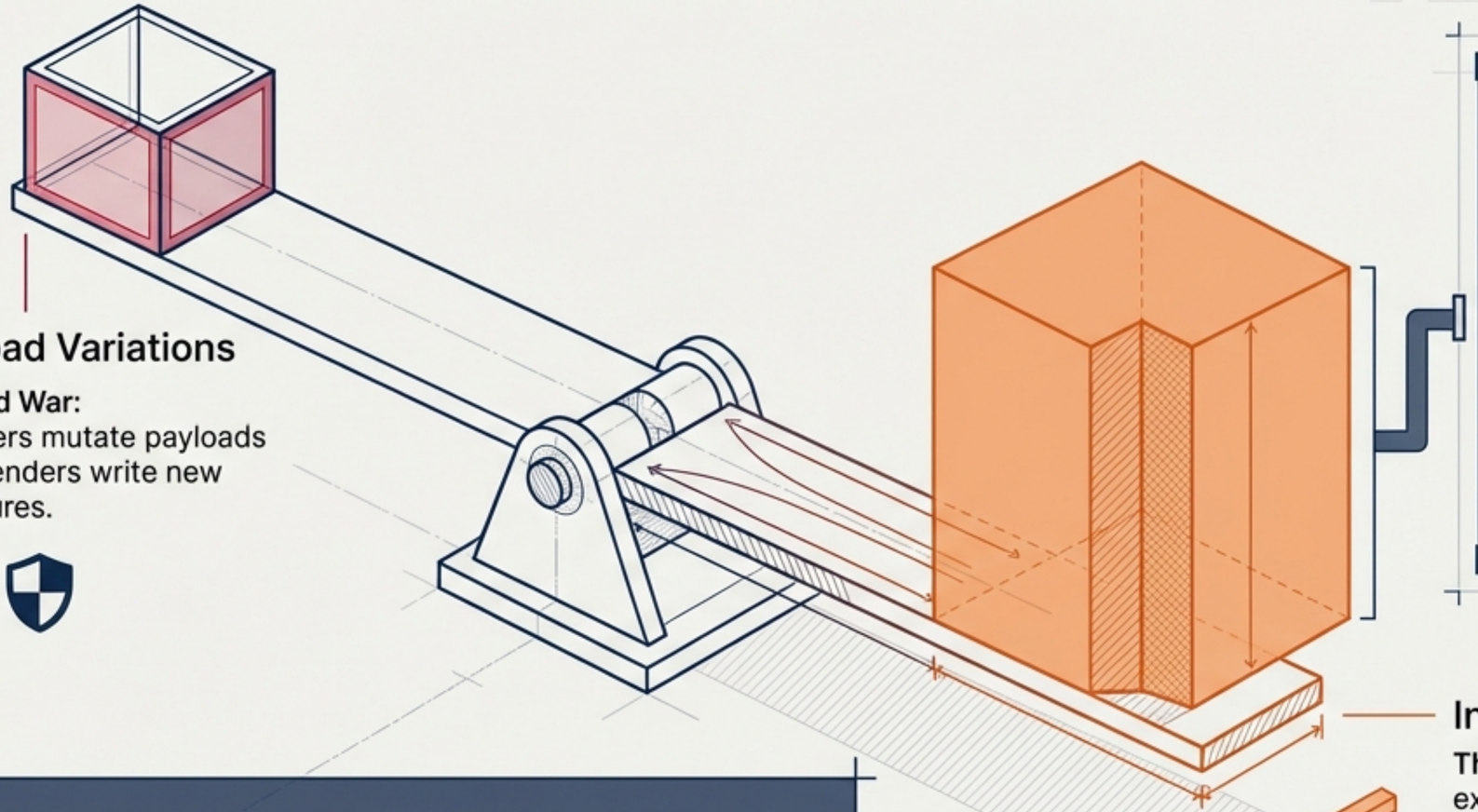
# WAF & IPS Detection Gaps: The Parsing Discrepancy Crisis

## Moving Beyond Signatures to State Machine Reinforcement




Analysis based on 2025/2026 Field Research & Incident Data (PortSwigger, WAFFLED, & Enterprise Red Team Findings).

# The Root Cause of Breaches is Structural, Not Syntactic



## Payload Variations

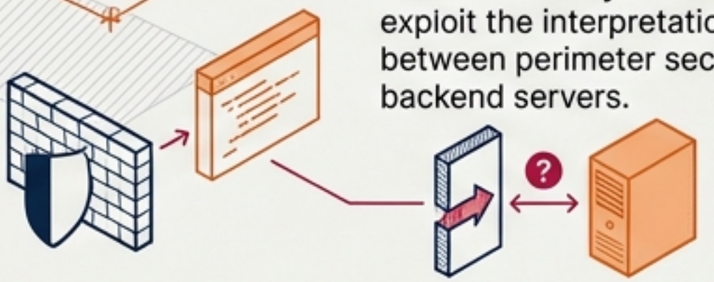
**The Old War:**
Attackers mutate payloads → Defenders write new signatures.

**1,207**

unique bypasses confirmed via structural parsing discrepancies across major WAF and framework combinations (WAFFLED 2025).

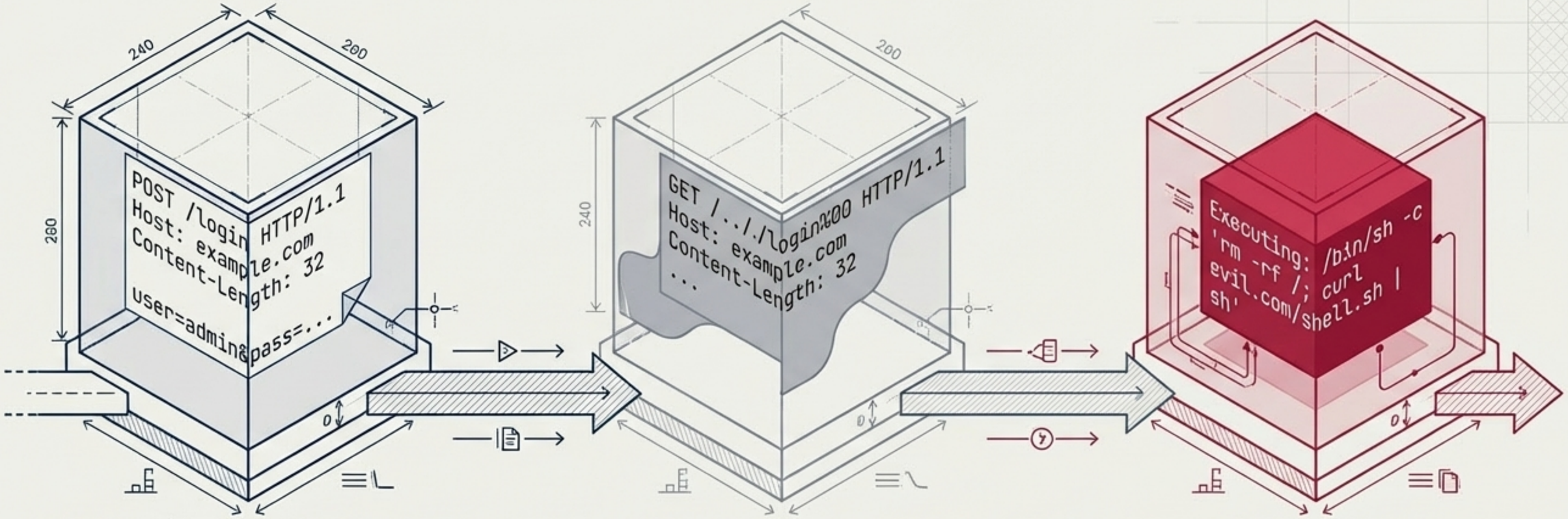
## Interpretation Gaps

**The New Reality:** Attackers exploit the interpretation gap between perimeter security and backend servers.



A signature is useless if the inspection engine is looking at the `wrong parser branch`, hitting a `size limit`, or evaluating a `pre-normalized string`.

# Anatomy of a Parsing Discrepancy




## Edge WAF View

Evaluates pre-normalization raw bytes. Fails to decompress or hits body size limits.

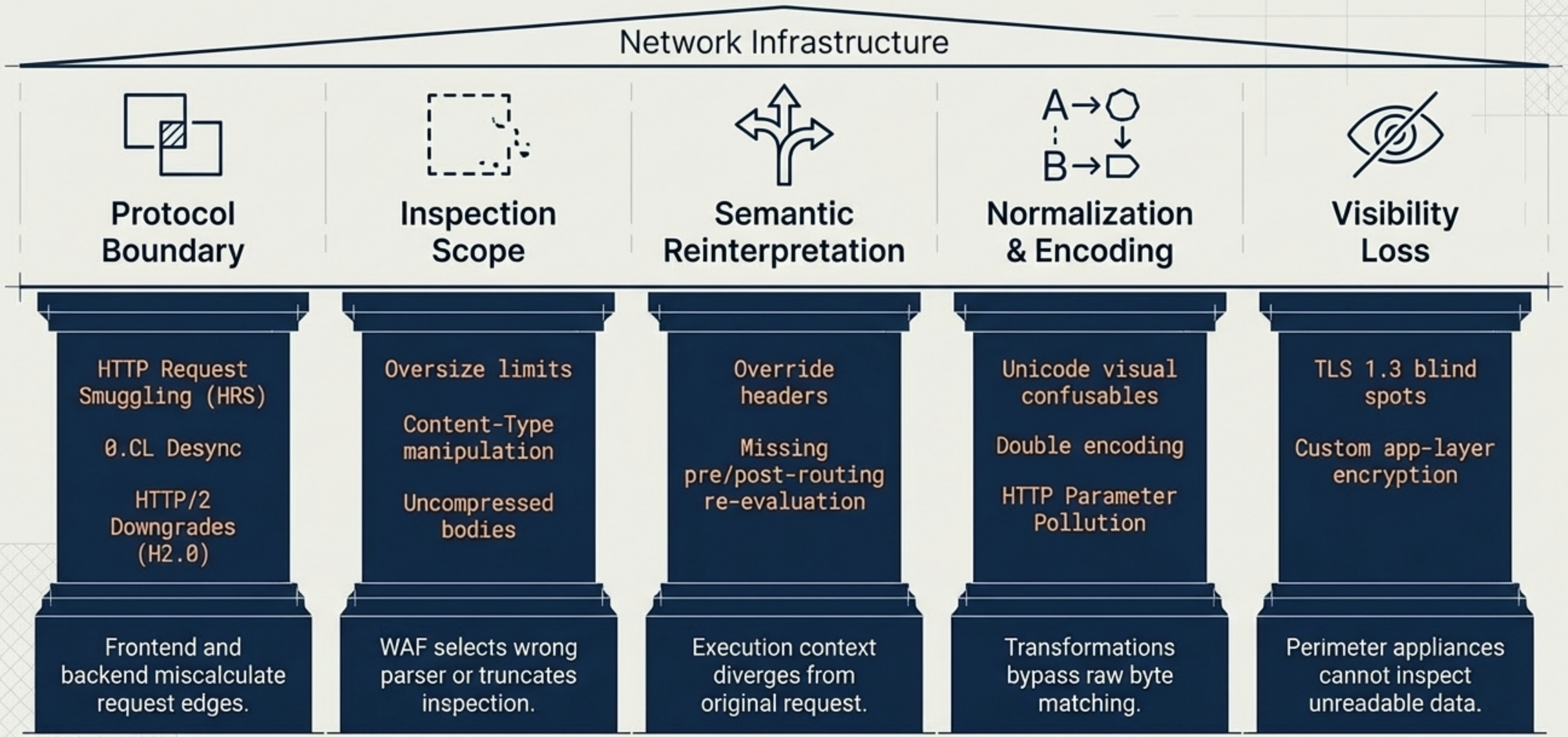
## Middle-Tier View

Alters request boundaries and semantic meaning (e.g., path normalization mismatches like Traefik CVE-2025-66490).

## Backend Reality

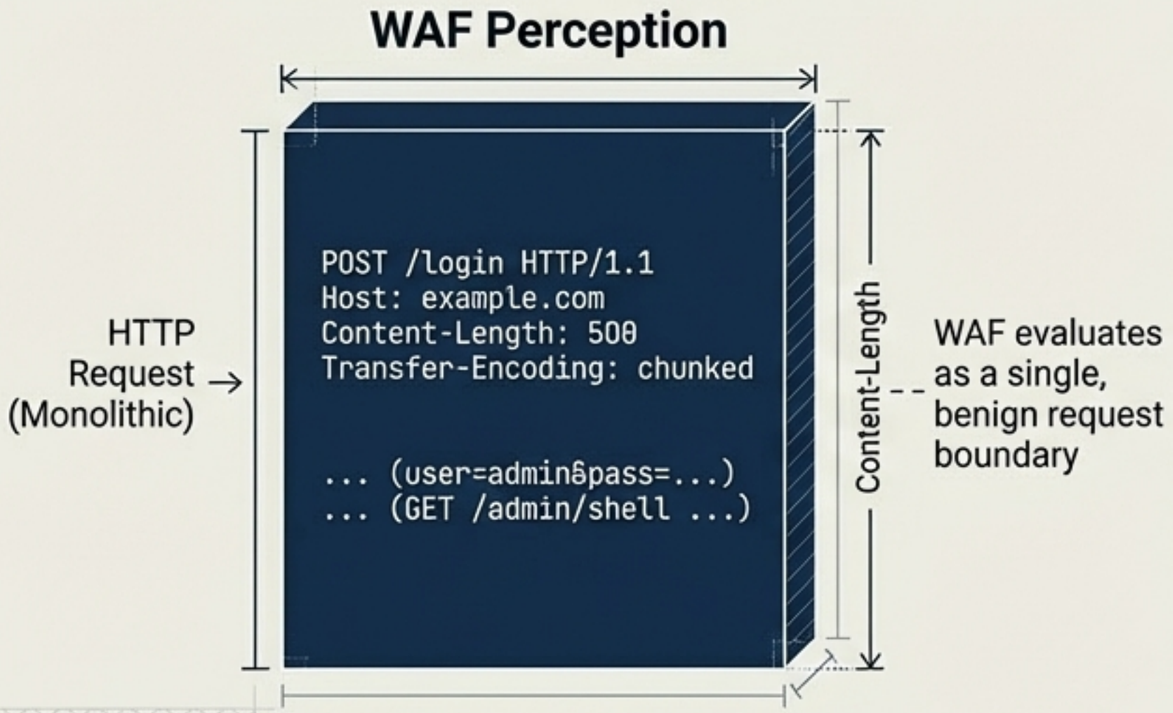
The final execution context. Processes the fully assembled, weaponized payload entirely unseen by the edge.

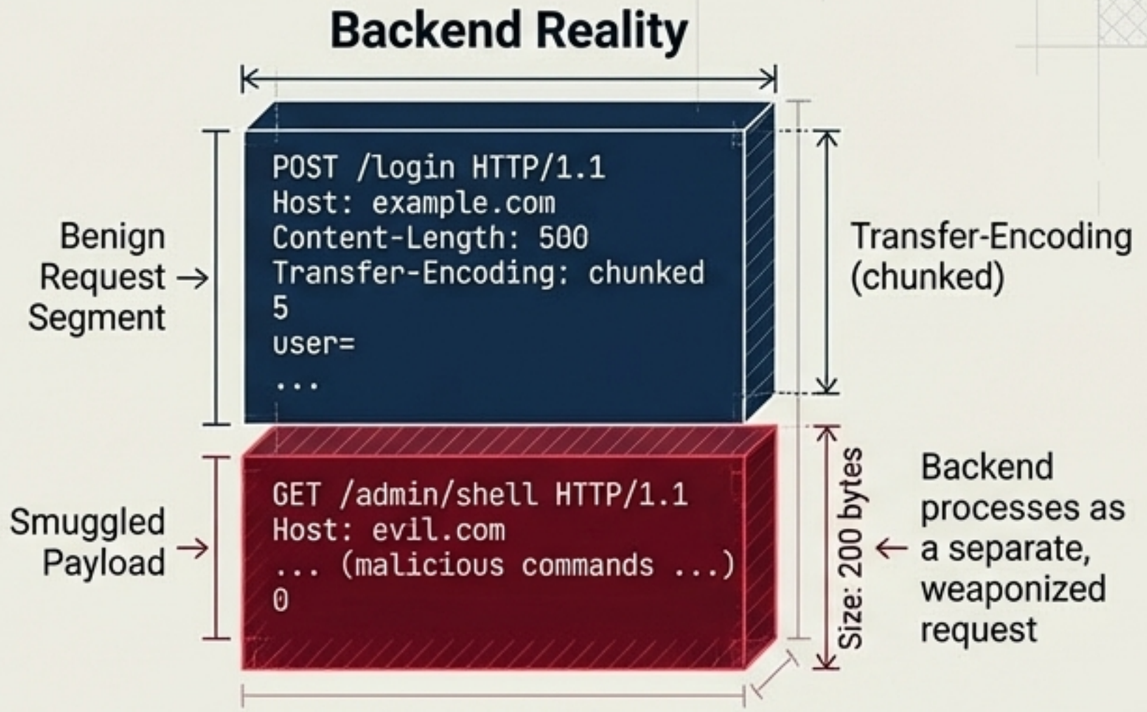
# The 5 Pillars of Structural Gaps



# Protocol Boundaries & The Desynchronization Threat

The Mechanism: HTTP header interpretation priority differences (e.g., Content-Length vs. Transfer-Encoding) between edge and backend cause boundary mismatches.




## Modern Variants

0.CL Desync (Frontend ignores `Content-Length: 0`), HTTP/2 Downgrade Desync (Header parsing divergence when downgrading H2 to HTTP/1.1).

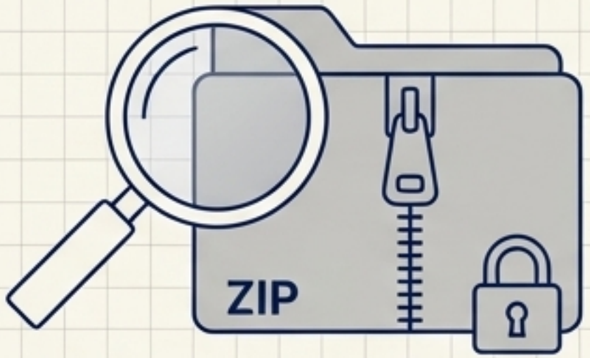
## The Impact

Malicious requests hide inside legitimate traffic, completely bypassing ACLs and enabling session hijacking.

# The Compression Blind Spot & Scope Truncation

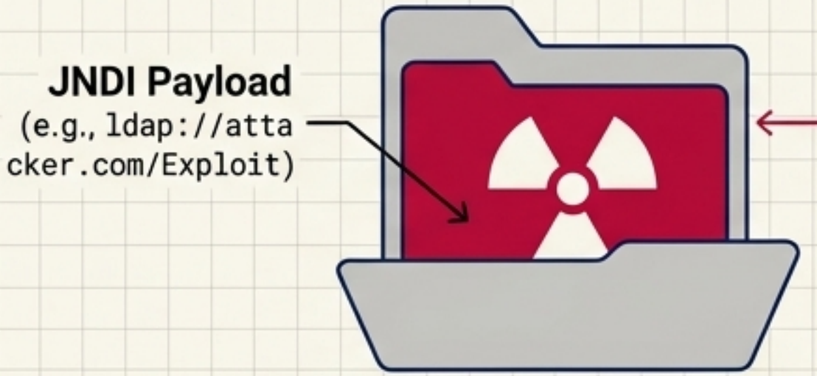
## Expectation vs. Reality

### Expectation / WAF




WAF inspects compressed body as a single, opaque object.

### Reality / Backend




Backend decompresses payload, exposing hidden threat.

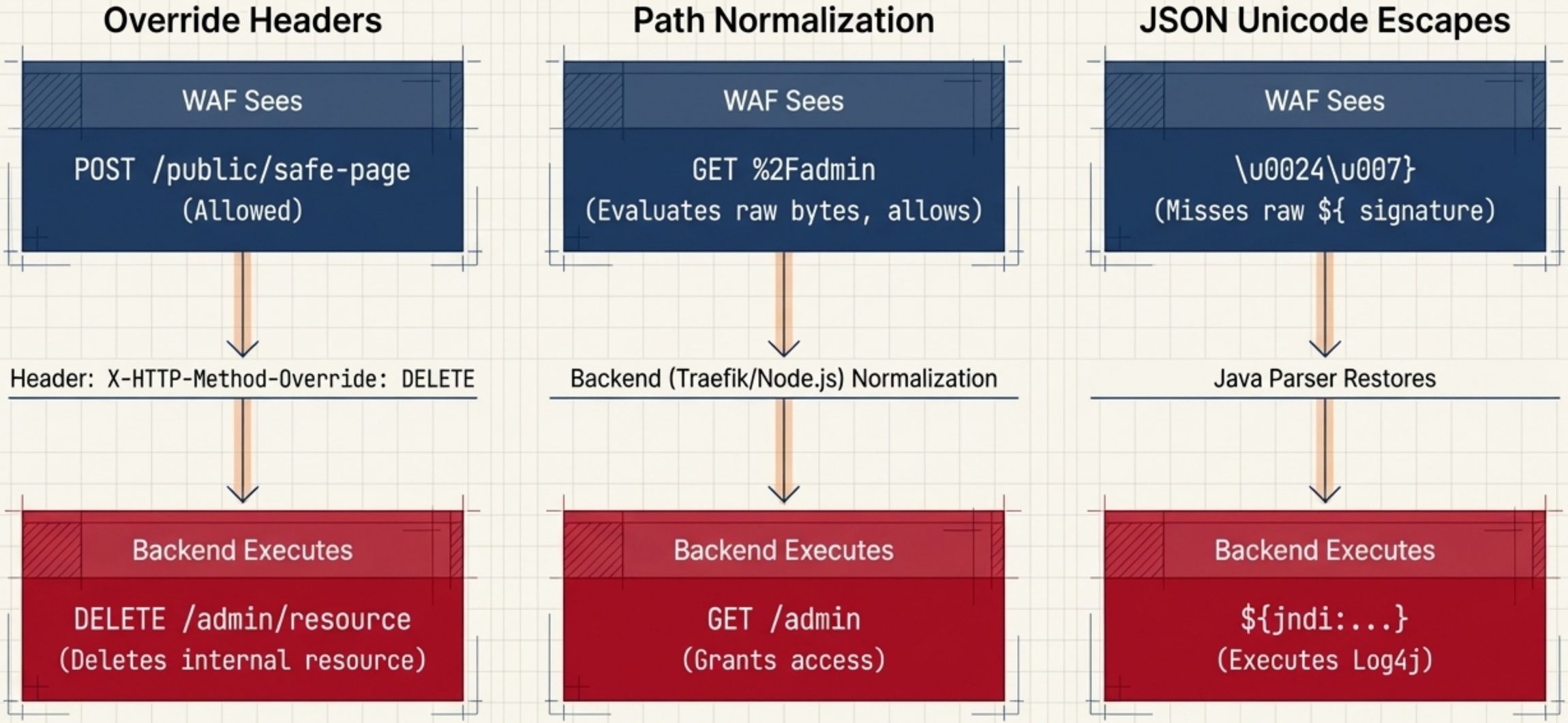
## Empirical Proof: Service-B Field Test (March 2026)

| Payload Type | Outcome |
|---|---|
| `Plaintext JNDI Body` | IPS Timeout (Successfully Blocked) |
| `Gzip/Deflate JNDI Body` | 302 Success (Completely Bypassed) |

**The Flaw:** WAFs skip inspection when body size limits are exceeded or fail to decompress payloads prior to raw byte matching.

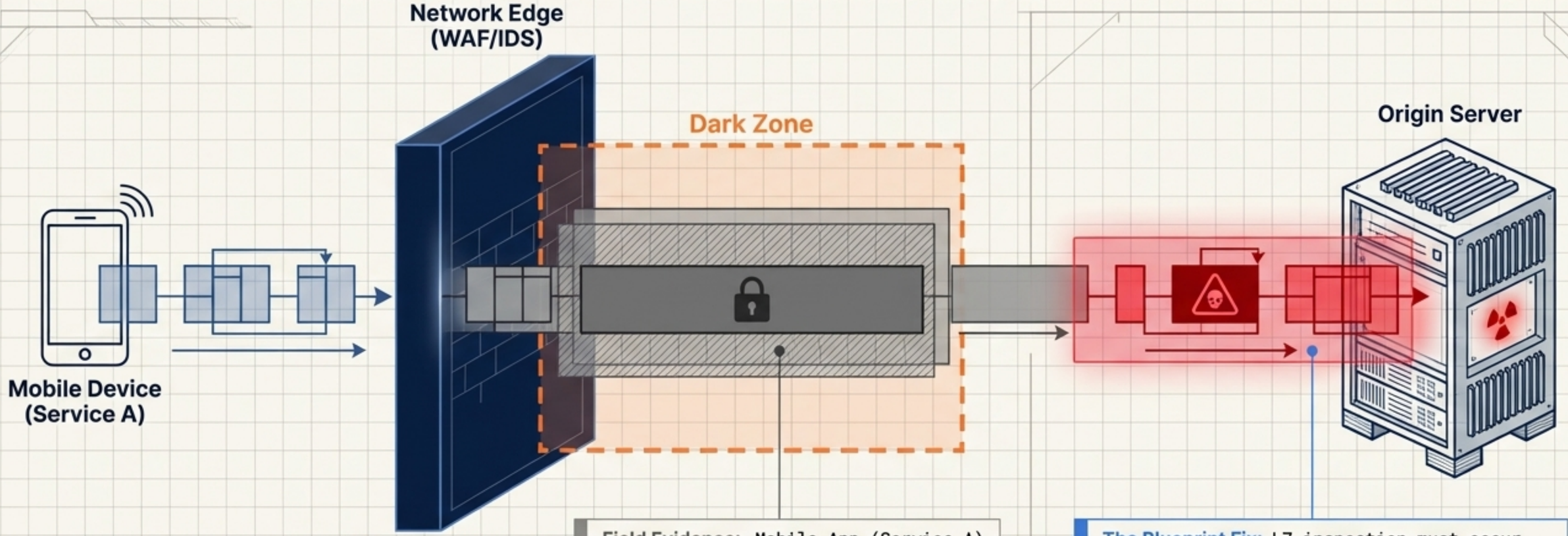
**The Remediation:** Explicitly activate Content-Encoding decompression (e.g., decompress_gzip). Set oversize handling to strict MATCH (block).

# Semantic Reinterpretation & Normalization Discrepancies



# The Visibility Void: Custom Encryption & TLS 1.3

Perimeter appliances cannot inspect what they cannot read.

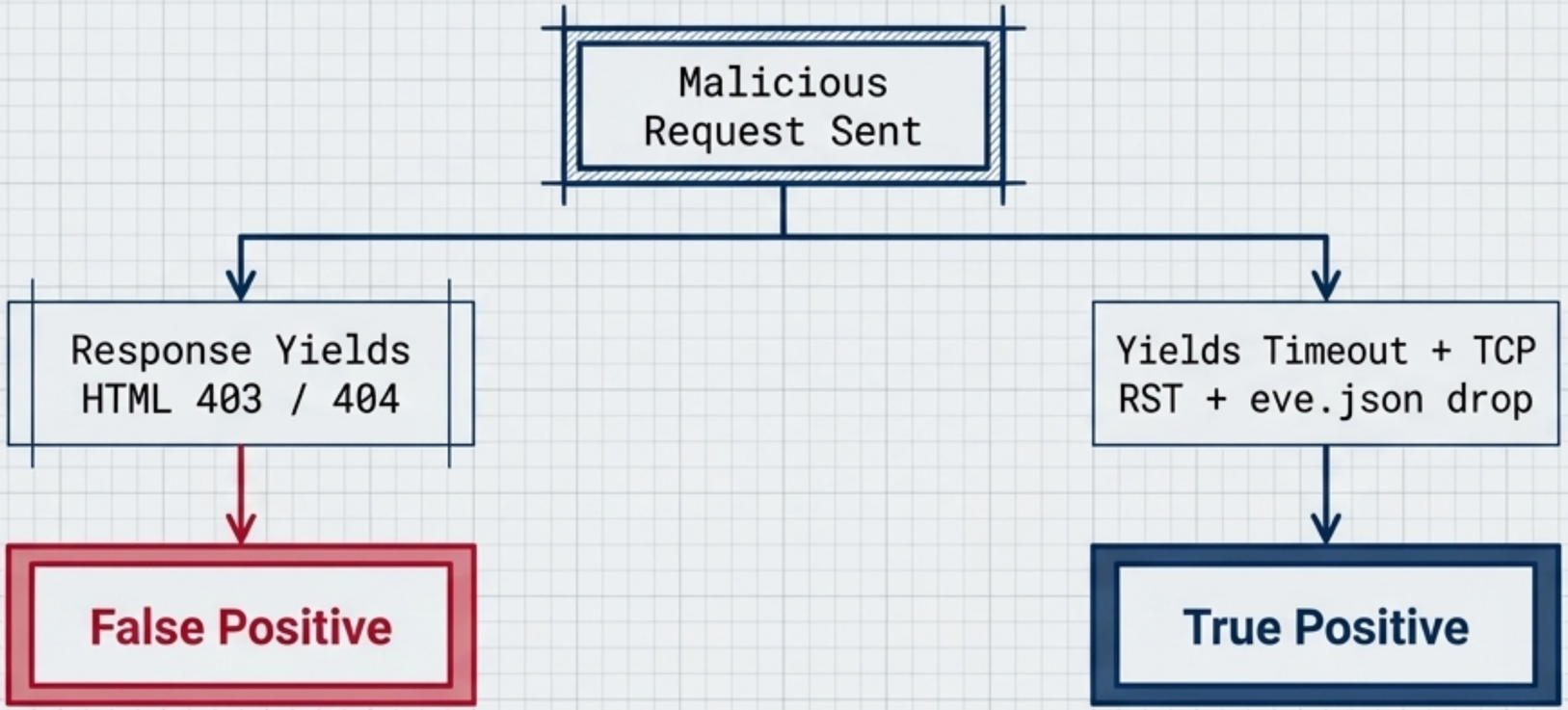



**Field Evidence:** Mobile App (Service A) encrypts body via KISA SEED ECB. IDS only sees enc={base64}. Attack payload is completely invisible.

**The Blueprint Fix:** L7 inspection must occur post-TLS termination. Mandate SSL Mirror coverage SLOs, and deploy server-side RASP/EDR where custom encryption creates network blind spots.

# Field Reality: The Fallacy of the 403 Forbidden

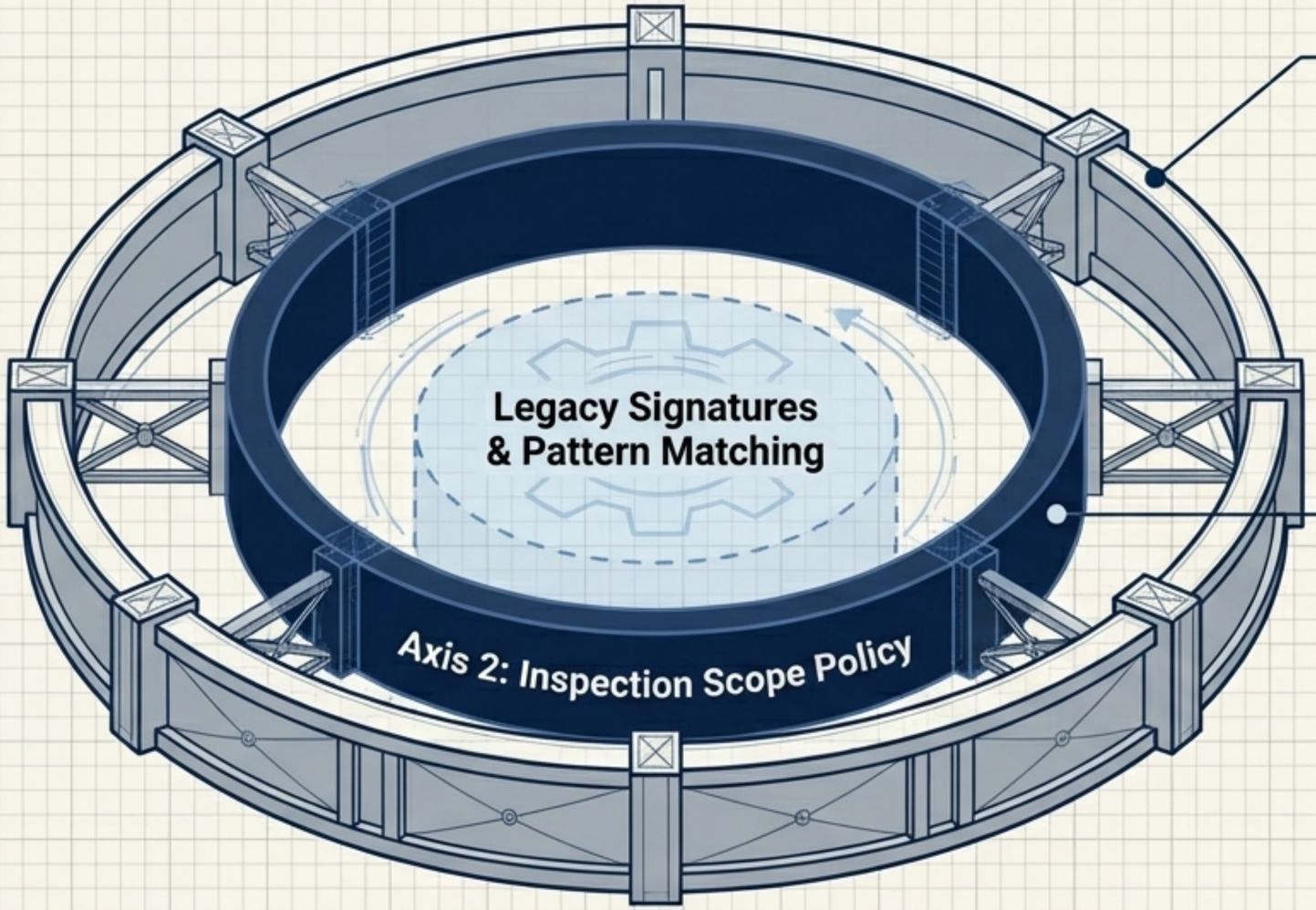
The Myth: "We received a 403 response, therefore the IPS successfully blocked the attack."




The Mandate: Stop misattributing 403s. Cross-reference appliance events, flow logs, and reset traces before confirming an IPS block.

# The Remediation Paradigm: State Machine Reinforcement

Beyond Signatures: Stop relying purely on Generic Patterns and raw byte Normalization Enhancements.




## Inspection Entry Control

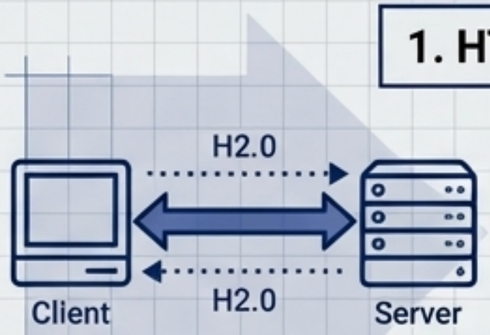
- Conservative block/quarantine on abnormal or missing `Content-Type`.
- Unconditionally strip externally-sourced override headers at the edge.
- Strict HTTP/2 end-to-end policies.

## Inspection Scope Policy

- Enforce mandatory MATCH (block) on size limit overflow.
- Explicitly define invalid JSON fallback behavior.
- Mandatory decompression prior to inspection.

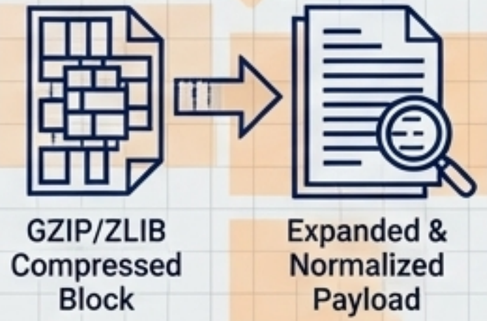
# Tactical Blueprint: 4 Critical Fixes

## 1. HTTP/2 End-to-End (Protocol)




Eliminate **downgrade parsing gaps**.
Restrict downgrades and prohibit upstream header concatenation to kill **H2.0 desyncs**.

## 2. Decompress & Decode (Payload)



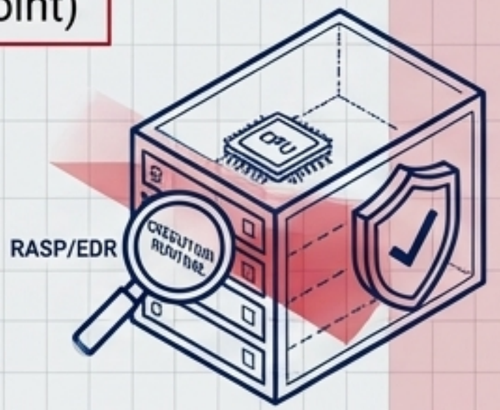

Enable **decompress_gzip (Snort/Suricata)**.
Mandate **NFC/NFKC** Unicode normalization before rules are evaluated.

## 3. Positive Security for APIs (API)


Abandon continuous signature expansion. Use OpenAPI/Swagger **schema validation** at the gateway to block unknown fields and type mismatches outright.

## 4. Deploy RASP/EDR (Endpoint)

Reclaim payload visibility. When app-layer encryption (SEED/ECB) blinds the network, validation must happen inside the **execution runtime**.



# The Validation Arsenal: Testing Structural Gaps

| Tool | Repository | Target Gap | Capability |
| --- | --- | --- | --- |
| WAFFLED | sa-akhavani/waffled JetBrains Mono | ✔ Inspection Mode | Fuzzes Content-Type, NUL byte injection, and boundary splitting via raw sockets. |
| Smuggler | defparam/smuggler JetBrains Mono | ✔ Protocol Boundaries | Tests 60-300+ Transfer-Encoding variations for timeout-based CL.TE/TE.CL detection. |
| Cortisol | toxy4ny/cortisol JetBrains Mono | ✔ Normalization | Automates double/triple URL encoding and Overlong UTF-8 tamper chains. |
| WAF-Bypass | nemesida-waf/waf-bypass JetBrains Mono | ✔ Scope & Encoding | Tests Base64/HTML-Entity/UTF-16 encodings across 7 request zones. |

# The State Machine Manifesto

## HIGH PRIORITY - CRITICAL MANDATES

### 01 Protocol Boundary Control

Enforce HTTP/2 end-to-end and block `Content-Length: 0` / non-standard `Expect` variations.

### 02 Semantic Reinterpretation Blocking

Unconditionally strip override headers (`X-Original-URL`, `X-HTTP-Method-Override`) at the edge.

### 03 Inspection Scope Assurance

Mandate **gzip/deflate** decompression and enforce MATCH on body oversize limits.

## STANDARD OPERATIONAL MANDATES

### 04 Normalize-Then-Inspect

Resolve **Unicode escapes**, double **encodings**, and visual confusables before applying signatures.

### 05 Sensor Health SLOs

Monitor IDS reassembly limits and memory spikes; appliance packet drops directly equal detection blind spots.

### 06 Cache Key Consistency

Ensure edge, proxy, and origin adopt the exact same canonical forms to prevent cache poisoning.