

# Suspected data leak

When sensitive data shows up in a response

## Real or false? Then stop it — or narrow it.

A data-leak-prevention (DLP) finding means **sensitive data appeared in a response the backend sent** — a card number, a national ID, a secret, a dump of records. The WAF caught it on the way out. This playbook decides whether it is real, then follows the right path.

### 1 decision

Real leak or false match

### 2 paths

Contain the leak · narrow the rule

### 1 record

For your incident log

**GajShield Infotech Private Limited**  
Mumbai, India

Version 1.0 · October 2026  
For GAJWAF analysts & administrators

#### LEGAL NOTICE

© 2026 GajShield Infotech Private Limited All rights reserved. This document is provided for the use of GAJWAF customers and partners. No part of it may be reproduced, distributed or transmitted in any form or by any means without the prior written permission of GajShield Infotech Private Limited

The information in this document is provided "as is", without warranty of any kind, express or implied, and is subject to change without notice. Features, menu labels and default values may differ between GAJWAF releases. While every effort has been made to ensure its accuracy, GajShield Infotech Private Limited accepts no liability for any loss, damage or service disruption arising from the use of, or reliance on, this document. This playbook is general operational guidance. It does not replace your organisation's own incident-response or change-control procedures, and GAJWAF is not a substitute for network-layer (L3/L4) DDoS protection.

GAJWAF and GajShield are trademarks of GajShield Infotech Private Limited Amazon Web Services, AWS and AWS Shield are trademarks of Amazon.com, Inc. or its affiliates. Microsoft and Azure are trademarks of the Microsoft group of companies. All other product and company names mentioned in this document are trademarks of their respective owners; they are used for identification purposes only, and their mention does not imply endorsement.

AT A GLANCE

# Real leak or false match?

GOLDEN RULE

First decide **real data vs. test data / false match**.  
Blocking a real leak protects the data — but the real fix is in the application. The WAF is masking a backend bug, not curing it.

STEPS 1-2 · TRIAGE

A DLP finding fired — read it, then decide

- What pattern matched? Which path? Blocked, or only detected?
- Is it **real sensitive data**, or **test data / a pattern coincidence**?

▼ REAL SENSITIVE DATA

PATH A · STEP 3

Real leak — stop it

- Set the DLP action: **mask** or **block**
- Tell the **application team**
- Preserve the evidence

▼ TEST DATA / COINCIDENCE

PATH B · STEP 4

False match — narrow it

- Narrow the **custom pattern**
- Or **exempt the path**
- Or lower the action for that data type

✗ DON'T

- **Don't** assume every DLP hit is real — confirm it's genuine data first.
- **Don't** treat the WAF block as the fix for a real leak — it's a stopgap until the application is corrected.
- **Don't** turn DLP off globally to clear one false match — narrow the pattern or exempt the path instead.

WHO **Analyst** to triage; **admin** to change DLP actions; the **application team** for the permanent fix.

CONTENTS

|   |                                 |   |
|---|---------------------------------|---|
| 1 | Read the finding .....          | 3 |
| 2 | Real leak or false match? ..... | 3 |
| 3 | If it's a real leak .....       | 4 |
| 4 | If it's a false positive .....  | 5 |
| ✓ | Verify & incident record.....   | 6 |

## STEP 1 OF 4

## 1 Read the finding

PATH **TRIAGE** WHO Analyst WHEN As soon as the event appears

Open the event. The finding category is **dlp** ("Sensitive data in the response"), and the action is often **response-block** ("response blocked"). Note three things:

| Note                               | Look for                                                                                                              | Write it in                   |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------|
| What pattern matched?              | Card number, national ID (Aadhaar / PAN), e-mail list, API secret, private key...                                     | Incident record — "Data type" |
| Which response / path produced it? | The request path and the response that carried the data.                                                              | Incident record — "Path"      |
| Was it blocked, or only detected?  | <b>response-block</b> = stopped. If the site or rule is in detect / report mode, the data <b>reached the client</b> . | Incident record — "Action"    |

**IMPORTANT**

If it was **only detected**, the sensitive data **was delivered to the client**. Treat a real match as an active leak.

**✓ MOVE ON WHEN**

You know the data type, the path, and whether the response was blocked.

## STEP 2 OF 4

## 2 Real leak or false match?

PATH **TRIAGE** WHO Analyst

Look at what actually matched, then take **one** of the two paths:

| If it's...                                                                                                        | Then it's               | Go to         |
|-------------------------------------------------------------------------------------------------------------------|-------------------------|---------------|
| <b>Real sensitive data</b> leaking to a client that shouldn't see it                                              | <b>A genuine leak</b>   | <b>Step 3</b> |
| <b>Test or sample data</b>                                                                                        | <b>A false positive</b> | <b>Step 4</b> |
| A <b>pattern coincidence</b> — a long number that isn't actually a card, a string that merely looks like a secret | <b>A false positive</b> | <b>Step 4</b> |

**✓ MOVE ON WHEN**

You have decided: **real leak** (Step 3) or **false match** (Step 4).

PATH A · STEP 3

### 3 If it's a real leak

PATH **REAL LEAK** WHO Admin + application team WHEN Immediately

WHERE Edit configuration → Response & limits → Data-leak prevention (`response.dlp.*`)

1. Set the DLP action for that data type — deliberately:

| Action | What happens                                            | Choose it when                                   |
|--------|---------------------------------------------------------|--------------------------------------------------|
| Mask   | The page goes through with the sensitive parts removed. | You need the application to <b>stay usable</b> . |
| Block  | The whole response is stopped.                          | You need the <b>strictest</b> protection.        |

2. Tell the application team. The WAF is now masking a real backend defect; the permanent fix is to stop the application returning that data.
3. Preserve the evidence — the Incident ID, the path and the time — for your incident record.

**IMPORTANT**

- Masking and blocking are **enforcement** — they only act while the site is in **Block** mode.
- The WAF block is a **stopgap**, not the fix. The leak is closed only when the application stops sending the data.

✓ **MOVE ON WHEN**

- The sensitive data no longer reaches clients.
- The application team has the bug, and the evidence is recorded.

PATH B · STEP 4

# 4 If it's a false positive

PATH FALSE MATCH WHO Admin

Fix it narrowly — **one** of these, the narrowest that works:

| Option                              | Where                                                                                | Use it when                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Narrow the custom pattern           | Response & limits → "Custom data-leak patterns" ( <code>response.dlp.custom</code> ) | One of <b>your own</b> patterns is matching too broadly.           |
| Exempt the path                     | Exclusions tab, for that path                                                        | That endpoint <b>legitimately</b> returns data that matches.       |
| Lower the action for that data type | Response & limits → Data-leak prevention                                             | That data type is matching benign content <b>across the site</b> . |

Then **re-test**: replay the response / path and confirm the finding no longer fires for the legitimate traffic.

✗ DON'T

- **Don't** turn DLP off globally to clear one false match — narrow the pattern or exempt the path instead.

✓ MOVE ON WHEN

- The legitimate page or endpoint works again, and the finding is quiet for it.
- DLP is **not** weakened for other paths.

## CLOSE THE INCIDENT

## ✓ Verify & incident record

|                                                 |                                                                                                              |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> <b>Real leak</b>       | The sensitive data no longer reaches clients, and the application team has the bug.                          |
| <input type="checkbox"/> <b>False positive</b>  | The legitimate page / endpoint works again and the finding is quiet — without weakening DLP for other paths. |
| <input type="checkbox"/> <b>App fix tracked</b> | For a real leak: the application fix has an owner and a date. The WAF setting stays until it ships.          |

## INCIDENT RECORD

|                                    |                                                                                                                                                                                                   |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Site / path                        |                                                                                                                                                                                                   |
| Detected at                        |                                                                                                                                                                                                   |
| Incident ID                        |                                                                                                                                                                                                   |
| Data type                          | <input type="checkbox"/> Card <input type="checkbox"/> Aadhaar <input type="checkbox"/> PAN <input type="checkbox"/> US SSN <input type="checkbox"/> Secret / key <input type="checkbox"/> Custom |
| Action at the time                 | <input type="checkbox"/> Blocked <input type="checkbox"/> Masked <input type="checkbox"/> Detected only (data delivered)                                                                          |
| Verdict                            | <input type="checkbox"/> Real leak (Path A) <input type="checkbox"/> False positive (Path B)                                                                                                      |
| Change made                        |                                                                                                                                                                                                   |
| Application team notified / ticket |                                                                                                                                                                                                   |
| Handled by / date                  |                                                                                                                                                                                                   |

## Related documents

| Document                                | Use it for                                                   |
|-----------------------------------------|--------------------------------------------------------------|
| Taming false positives (playbook)       | The general method for narrow fixes (Path B).                |
| GAJWAF Features & Configuration Guide   | Data-leak prevention settings (9.1) and Exclusions (ch. 10). |
| GAJWAF Troubleshooting & Support Manual | Chapter G — Data-leak prevention.                            |