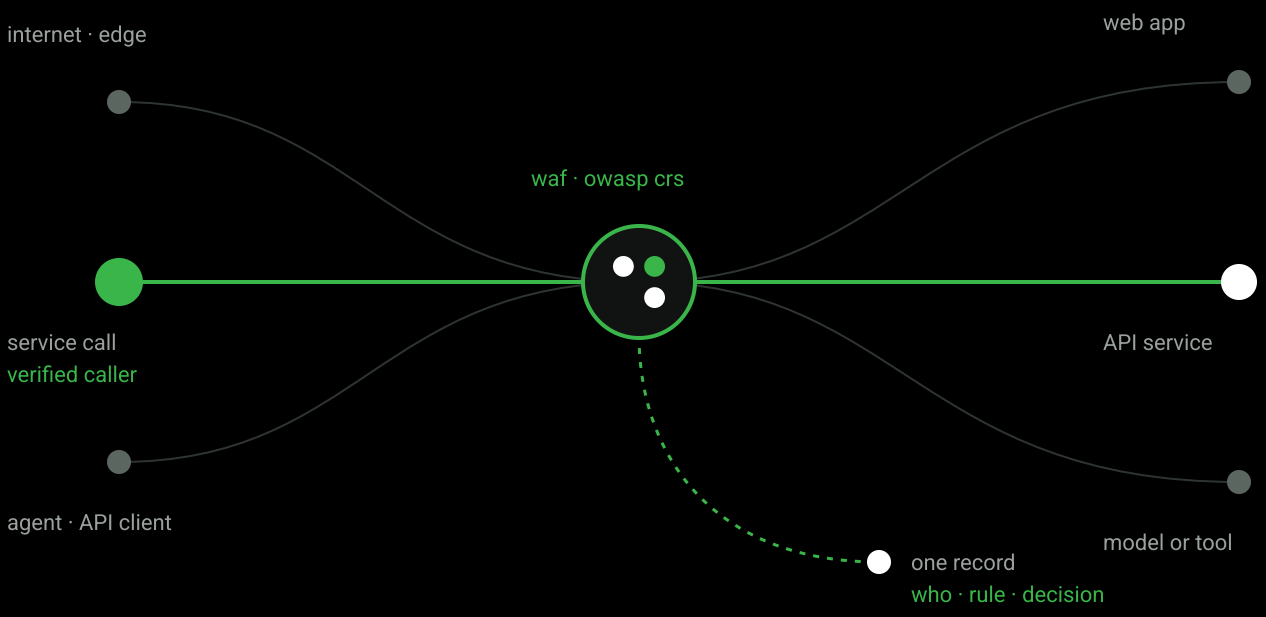
Greymatter.io

WHITE PAPER
GREYMATTER 2.5.0 · NOVEMBER 2026



The web application firewall, at the edge and inside the mesh

How Greymatter puts the OWASP Core Rule Set at the edge and on the services a team picks, tests it, and records each decision.

© 2026 Greymatter.io, Inc.

Contents

	SECTION		PAGE
THE CASE	1	Executive summary	1
	2	The perimeter is not enough	3
	3	One data plane, three engines	4
THE FIREWALL	4	The rule set	5
	5	Detect, test, then enforce	6
	6	What enforcement does	7
EVIDENCE	7	The record	8
	8	Reporting, forensics and Ask Greymatter	9
PROOF	9	Limits, stated precisely	11
	10	How this differs	12
	11	Operational and mission benefits	13
	12	Evidence for security frameworks	14
	13	Ask Greymatter	15

How to read the status marks

Every capability in this paper carries one mark. Nothing marked Fielded is aspirational.

FIELDED

Ships in Greymatter 2.5.0 today.

PREVIEW

Ships in 2.5.0 as a technology preview.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

1

Executive summary

Greymatter builds a web application firewall into its data plane as a native filter. A team turns it on at edge gateways and on any service it chooses, with no appliance, plugin or extra hop.

IN BRIEF

The OWASP Core Rule Set runs in the same data plane as the mesh. Teams test it on real traffic before it blocks, and every decision goes to one record with the caller.

WHO THIS IS FOR

Security architects, application owners and assessors who must show that web attacks are stopped inside the network as well as at its edge.

A perimeter firewall inspects the traffic that crosses the perimeter. Most traffic in a modern system never does. Services call services, agents call APIs, and one compromised workload can attack its neighbors without ever touching the edge.

Greymatter puts the firewall where the traffic already flows. The same data plane that encrypts and attributes each connection runs the OWASP Core Rule Set (CRS) on the requests it carries. A team can turn it on at an edge gateway, on a service, or both. Each can carry its own custom rules, tailored to the application or API it protects.

The firewall starts in detect mode. It reports what it would block while traffic flows as before. A team can replay recorded traffic against the rules before any change ships, and relax the rules for the paths that need it. Then it turns on enforcement.

Each decision goes to the same record as Guardrails, DLP and the rest of the platform. The record names the caller and the rule, and it never stores a raw credential.

THE CENTRAL POINT

A firewall at the edge protects the edge. Greymatter puts the same protection on any service a team chooses, with the caller attached.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Six properties a program office can test

Native in the data plane

FIELDED

A native filter built into the data plane, not a plugin. A team turns it on at edges and on the services it chooses.

An open, proven rule set

FIELDED

The OWASP Core Rule Set ships inside the data plane, so it works in disconnected networks too.

Detect, test, then enforce

FIELDED

Detect mode is the default. A team replays real traffic against the rules before it enforces.

Blocked before it reaches the service

FIELDED

In enforce mode, a denied request never reaches the service, not even its headers.

The caller on every finding

FIELDED

Each event names the verified caller, the rule and what the firewall did.

No raw secrets on file

FIELDED

The record fingerprints or withholds every credential in a request. No setting changes that.

STATED PRECISELY, SO IT IS NOT OVER-READ

The firewall blocks only in enforce mode. In detect mode it records what it would block and lets the traffic through.

The firewall inspects requests up to a size the team sets, and response bodies only when the team turns that on. Section 9 states each limit.

PART OF A SERIES

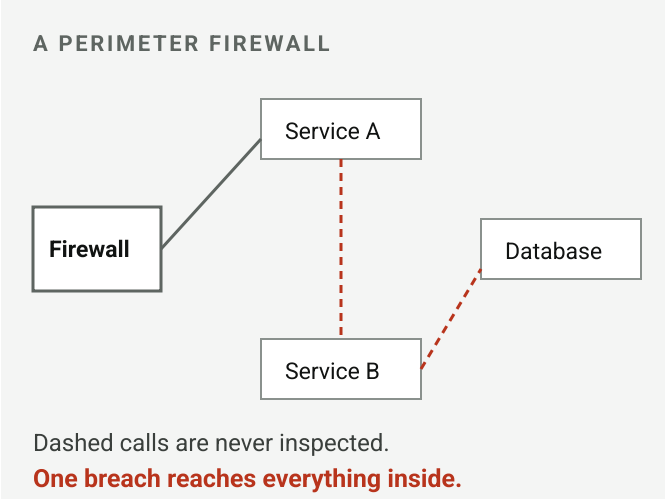
The firewall covers classic web attacks. Guardrails and DLP cover attacks on AI systems and sensitive data, and their own paper covers them. All three share one data plane and one record.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

2 The perimeter is not enough

Most requests in a modern system travel between services. A firewall that inspects only the edge misses them.

FIGURE 1 · WHERE THE FIREWALL RUNS



LATERAL MOVEMENT

An attacker who gets one foothold moves sideways. Internal calls are the path, and a perimeter firewall never inspects them.

MORE PRODUCTS, MORE SEAMS

A separate firewall per service means separate appliances, separate rules, separate logs and more open seams.

A web application firewall is a mature control. The rules that catch SQL injection, cross-site scripting and command injection are well known and well tested. The problem is placement. A firewall at the edge protects the services the internet can reach. It does nothing for the calls that service A makes to service B.

Those internal calls now carry the most sensitive traffic. AI agents call internal APIs. Batch jobs move data between systems. One service with a flaw in its input handling becomes the way in for everything behind it.

Greymatter runs the firewall in the data plane that already sits beside every service. A team turns it on for the services it chooses, and internal calls to them get the same inspection as calls from the internet.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

3 One data plane, three engines

The firewall, Guardrails and DLP run side by side in the same data plane. Each has its own job. FIELDED

	WEB APPLICATION FIREWALL	GUARDRAILS	DLP
Stops	Classic web attacks on applications and APIs	Attacks on AI systems, such as prompt injection	Nothing. It records sensitive data
Rules	OWASP Core Rule Set, plus a team's own rules	Modules mapped to the OWASP Top 10 for LLM Applications	Personal, health, logistics and marking detectors
Modes	Detect or enforce	Detect, enforce or off, per module	Detect or off
Default	Detect	Detect	Detect
Where	Edge gateways and service listeners, where a team turns it on	Workloads by label, listeners and egress	Workloads by label, listeners and egress

NATIVE, NOT A PLUGIN

The firewall is a native filter built into the data plane. It is not a WebAssembly plugin or an add-on, so no sandbox sits between it and each request.

RUNS AFTER IDENTITY

The firewall runs after Greymatter verifies the caller. Every event names who sent the request.

Greymatter added the firewall to the data plane itself, as compiled code in the request path. The firewall is built on OWASP Coraza, an open-source engine, and the OWASP Core Rule Set (CRS). Both are OWASP projects with wide use and open review. The rule set ships inside the data plane, so the firewall needs no download at run time and works in disconnected and air-gapped networks.

A team attaches the firewall to an edge gateway, to a service's listener, or to both. A route can turn the firewall off for itself when a listener carries it. The firewall inspects HTTP, gRPC and the start of each WebSocket connection.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

4

The rule set

The OWASP Core Rule Set is the most widely used open rule set for web application firewalls. It ships inside the Greymatter data plane, ready to turn on. FIELDED

ATTACK CLASS	WHAT THE RULES CATCH
Injection	SQL injection, command injection, and code injection for PHP, Java and other platforms
Cross-site scripting	Script injected into pages, parameters and headers
File access	Local and remote file inclusion and path traversal
Protocol abuse	Malformed requests, request smuggling and abuse of multipart uploads
Scanners and probes	Known attack tools and automated probing
Session attacks	Session fixation
Method and content limits	Methods and content types the service does not accept
Leaks in responses	Database errors, stack traces and web shells, when response inspection is on

A TEAM'S OWN RULES

A team can add rules in the standard SecLang rule language, next to the rule set, in the order it chooses.

UPDATES

A Greymatter release can carry a newer rule set. The team's own rules and exceptions stay as they are.

The rule set scores each request. Each rule that matches adds to an anomaly score. In enforce mode, a request whose score passes the threshold is blocked. This scoring keeps a single weak match from blocking a real user, and it lets several weak matches together stop an attack.

The default policy turns on the full rule set in detect mode. A team can tune the policy in the same rule language the rule set uses.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

5

Detect, test, then enforce

A firewall turned straight to enforce blocks something legitimate on day one. Greymatter makes the safe path the default. FIELDED

DETECT BY DEFAULT

A new firewall starts in detect mode. It records every rule it would fire and blocks nothing.

PER PATH, NOT GLOBAL

An exception relaxes the rules for one path only. The rest of the service keeps full protection.

Detect. The firewall runs every rule on live traffic and records what it would block. The record shows which rules fire, on which paths, for which callers, before any user is affected.

Test. The Greymatter CLI replays a file of recorded HTTP requests against a service's firewall policy, offline. It reports how many requests the policy would allow, deny, redirect or drop. A team tests a policy change before it ships.

Tune. A team writes exceptions for the paths that need them. An exception can add allowed methods or content types, or stop body inspection for an upload path. It can also remove specific rules or rule targets on that path.

Enforce. The team switches the mode to enforce. The record shows every block from then on.

AN EXCEPTION CAN	FOR EXAMPLE
Add allowed methods	Accept PUT and PATCH on an API path
Add allowed content types	Accept a custom JSON media type
Turn off body inspection	Stream large uploads to an object store path
Remove rules or rule tags	Drop a rule that misreads a search field
Remove a rule target	Stop one rule from reading one parameter

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

6

What enforcement does

In enforce mode, the firewall decides before the service acts. A denied request never reaches it. FIELDED

HELD UNTIL DECIDED

The data plane holds the request, body included, until the rules have run. The service receives nothing of a denied request.

When body inspection is on, the data plane holds the request and its body until the rules decide. The connection to the service opens only after that. A request the rules deny never reaches the service, not even its headers.

A rule decides what happens to a request it stops. The team sets this in its own rules, and the rule set uses deny by default.

CORRECT FOR EACH CLIENT

A gRPC client gets a gRPC error status, never a false success.

ACTION	WHAT THE CLIENT RECEIVES
Deny	An error status, 403 unless the rule names another
Drop	The error status, then the connection closes
Redirect	A redirect to the address the rule names
gRPC deny	The matching gRPC status, such as permission denied

WebSocket and streaming

DIVISION OF LABOR

The firewall guards the connection. Guardrails and DLP inspect what flows over it.

The firewall inspects the request that opens a WebSocket connection, and its response. It can also inspect each message, when a team turns that on. Messages in AI and notebook traffic are often code, which web rules misread as attacks. For that traffic, Guardrails and DLP read each message instead.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

7

The record

Every firewall decision goes to the same record as the rest of the platform, with the caller attached. FIELDED

NO RAW CREDENTIALS

The record keeps who, what, when and how. It fingerprints or withholds every token, password and key. No setting changes that.

ONE VIEW

The Console shows firewall, Guardrails and DLP findings for each listener, side by side.

A firewall log that cannot say who sent a request leaves the analyst guessing. Greymatter runs the firewall after it verifies the caller. Each event carries that identity, so an assessor can trace a blocked attack to a workload and, where known, to a person.

THE EVENT RECORDS	DETAIL
Who	The verified caller and, where known, the person
Where	Service, listener, method and path
What fired	Each matching rule, its message and its tags
What happened	Whether the firewall blocked, and with what status
Credentials	A summary of each credential seen, fingerprinted or withheld, never raw

READ IT THREE WAYS

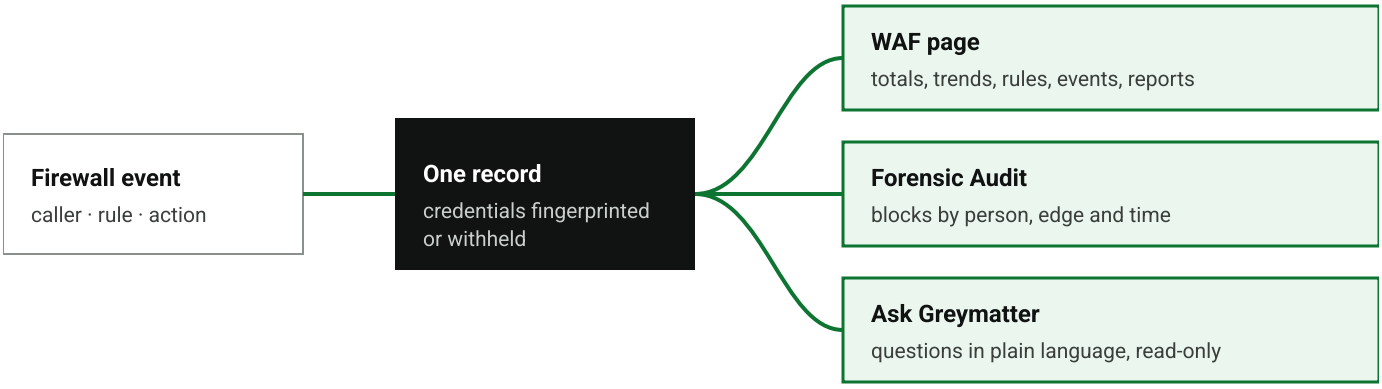
The same events feed the WAF page, the Forensic Audit and Ask Greymatter. Section 8 shows each one.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

8 Reporting, forensics and Ask Greymatter

A blocked attack is only useful if someone can find it, explain it and follow it. Greymatter puts firewall events where analysts already work. FIELDED

FIGURE 2 · ONE RECORD, THREE WAYS TO READ IT



MESH-WIDE OR ONE SERVICE

The page covers the whole mesh, chosen namespaces or one service. Each service's own view has the same tab.

DETECT MODE COUNTS

The totals show what was blocked and what detect mode would have blocked, so a team can measure the effect of enforcement in advance.

The WAF page. The Console gives the firewall its own page. It shows the totals for the range a reader picks, each against the previous period, and says when no listener is enforcing. A chart shows outcomes over time, and a grid shows which namespaces had findings when.

A reader filters by namespace, service, rule or attack category. The rules window groups every rule the firewall fired by the categories of the OWASP Core Rule Set. A built-in explainer shows how anomaly scoring works. Each event opens a full report in its own tab.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Connected to the Forensic Audit

FOLLOW THE CREDENTIAL

A credential on a firewall event shows as a fingerprint. It links to every audit record that carries the same fingerprint, so an analyst can follow a stolen token across the mesh.

The Forensic Audit shows requests over time with a lane for requests the firewall blocked, beside the requests that access policy denied. Its identity tables count firewall blocks by person and workload. A card shows firewall events at each edge over time, with a link straight to the WAF page.

Asked in plain language

READ-ONLY

Every tool reads. None can change a rule, a policy or a mode.

SAFE BY DESIGN

The tools leave out client addresses, headers, bodies and matched data. They also leave out rule messages, which can echo an attack payload.

Ask Greymatter takes questions about the firewall and reads the same records through its tools. A reader can ask where the firewall is on, what it did across the mesh or on one service, and which events matched a rule. Each reply cites the records the tools read.

ASK GREYMATTER TOOL	WHAT IT REPORTS
Coverage	Which engines have records, which services had findings, and how each listener is set
Summary	Totals against the previous period, outcomes over time, and the busiest rules and attack groups
Service	One service's findings, outcomes, top rules and top paths
Events	The findings newest first, filtered by rule or tag, or one event by its ID
Request trace and identity findings	One request's path across services, and the people and workloads with enforcement events

Firewall data is read only by roles that hold security viewing rights, mesh-wide or for chosen namespaces. The default policy gives those rights to security viewers, not to platform administrators. A service outside a reader's reach returns no events.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

9 Limits, stated precisely

Every limit has a defined result that the team controls, and the record shows it. FIELDED

WHEN THIS HAPPENS	GREYMATTER DOES THIS
A request body is larger than the size the team sets	Inspects up to that size. The team chooses whether the rest passes or the request is refused.
Response bodies	Not inspected unless the team turns response inspection on
An upload path is exempt from body inspection	Inspects the request line and headers, and streams the body
The firewall is in detect mode	Records what it would block, and blocks nothing
A rule set update arrives	Applies with a Greymatter release. The team's own rules and exceptions stay

WHY THE SIZE LIMIT

Holding a whole body costs memory for every request in flight. The team sets the trade between depth and cost.

NOT A SUBSTITUTE

A firewall stops known attack patterns. It does not replace secure code, patching or authorization.

For a team, an app or an API that needs the strictest posture, the firewall can refuse any body it cannot inspect in full. Where an app or an API moves large files, a team can exempt only the upload paths and keep every other path fully inspected.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

10

How this differs

A firewall at the perimeter guards one entry point. Greymatter can guard any service a team chooses.

ONE PRODUCT

The firewall ships in the same data plane, policy, record and Console as the mesh. There is nothing extra to deploy or run.

Perimeter firewalls and cloud firewall services protect what the internet can reach. They are a sound first layer. They cannot inspect the calls between services, and they rarely record which workload or person sent a request.

Greymatter adds the same class of protection inside, on the services a team chooses, without a new hop. The table compares the approaches as a class. Products within a class vary.

	PERIMETER FIREWALL	GREYMATTER
Where it runs	At the perimeter, as an appliance or a cloud service	In the data plane, at the edge and on the services a team chooses
Calls between services	Not inspected	Inspected, on the services where the firewall is on
Who sent it	A client address	The verified caller and, where known, the person
Rollout	Often switched on in one step	Detect by default, offline replay, per-path exceptions
Record	A separate log in a separate product	The same record as Guardrails, DLP and the mesh
Disconnected networks	Often needs a vendor feed	The rule set ships in the data plane

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

11 Operational and mission benefits

Each outcome, what produces it, and its status.

OUTCOME	WHAT PRODUCES IT	STATUS
Inspection inside the network	The firewall in the data plane, on the services a team chooses	FIELDED
A proven rule set	The OWASP Core Rule Set, shipped in the data plane	FIELDED
Safe rollout	Detect by default, offline replay and per-path exceptions	FIELDED
Attacks stopped before the service	Requests held until the rules decide	FIELDED
Correct errors for every client	HTTP and gRPC replies that match the rule	FIELDED
Attribution	The verified caller on every event	FIELDED
A record that is safe to keep	Credentials fingerprinted or withheld, always	FIELDED
Disconnected operation	No rule download at run time	FIELDED
Reporting without assembly	The WAF page, the Forensic Audit and Ask Greymatter, on one record	FIELDED
No plugin to manage	A native filter in the data plane, not a WebAssembly add-on	FIELDED
One product to run	Same data plane, policy, record and Console as the mesh	FIELDED

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

12

Evidence for security frameworks

Security frameworks require controls that run and records that prove they ran. The firewall supplies both, from the data plane. FIELDED

EXTEND, DO NOT BUILD

A team turns the firewall on in the mesh it already runs. It buys no appliance and builds no logging pipeline.

Frameworks for payment data, information security and critical services share a pattern. They require protection for web applications, monitoring of the network, and a log an assessor can review. The firewall supplies all three on the services where a team turns it on.

FRAMEWORK	WHAT IT REQUIRES	WHAT GREYMATTER SUPPLIES
PCI DSS v4.0	Requirement 6.4.2: an automated solution that detects and prevents web attacks on public-facing applications, with audit logs	The firewall at edge gateways, in enforce mode, with a record of every decision
OWASP Top 10	Protection against common web application risks	The OWASP Core Rule Set: injection, cross-site scripting, file access and protocol abuse
ISO/IEC 27001:2022	Annex A 8.20 networks security, 8.16 monitoring activities, 8.15 logging	Inspection in the data plane, findings on live traffic, and one record
EU NIS2 Directive	Article 21: secure maintenance and vulnerability handling, and checks that measures work	Detect mode and offline replay show what a policy does before it enforces
NIST SP 800-53 Rev. 5	SC-7 boundary protection, SI-4 system monitoring, AU-2 event logging	The firewall at the edge and inside, the WAF page, and the record
United States CISA Zero Trust Maturity Model	Applications and workloads pillar, with visibility and analytics	Protection beside the services a team chooses, with the caller on every event
United States DoD Zero Trust Strategy	Applications and workloads, and visibility and analytics pillars	The same controls, and the Forensic Audit view of blocks by person and edge

Using Greymatter does not make a system compliant with any framework. It supplies controls and evidence an assessor can test. National rows come last.

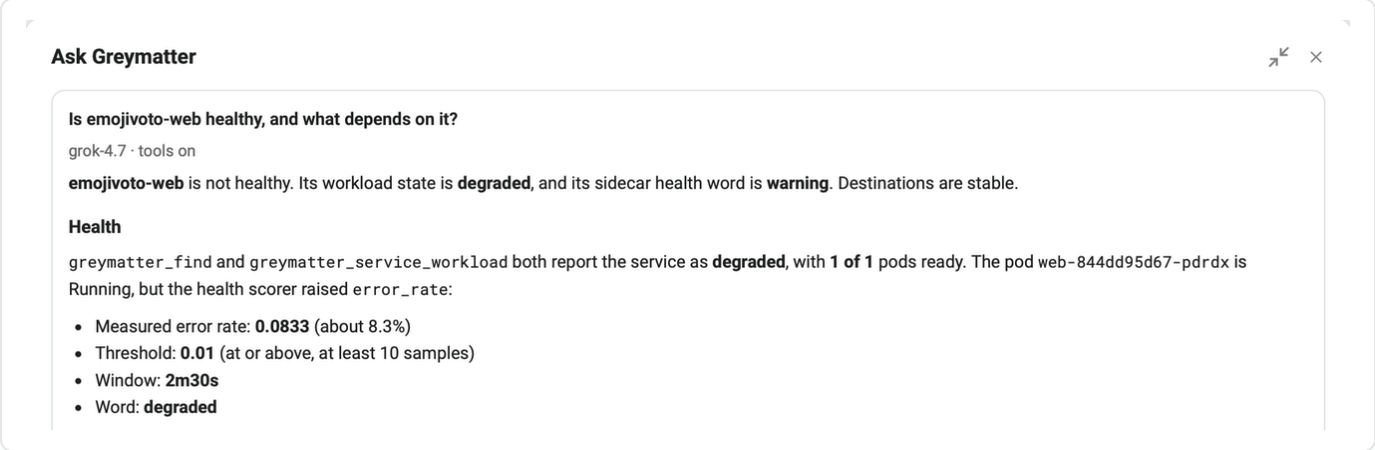
© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

13

Ask Greymatter

Ask Greymatter answers questions about what the firewall blocked or would block, and why, from the same record as the WAF page. FIELDED

FIGURE 3 · ASK GREYMATTER IN THE CONSOLE



READS AS YOU

Each tool reads the platform as the person who asked, and only reads. An answer holds only what that role allows.

GOVERNED LIKE ANY AI USE

Guardrails and DLP check each model call. The audit trail names the person and the agent.

Ask Greymatter is on every page of the Console. A person types a question in plain language. A model the organization chooses answers it from the platform's own data, through read-only tools.

For the firewall, it reads where the WAF runs and in which mode, what it blocked, its busiest rules and each event. These tools need a security viewer role.

Tools come in groups: Health, Security, Traffic, Changes and Docs. Health and Docs are on by default. A person turns on the others in the Tools menu.

Questions a team can ask

“What did the WAF block across the mesh in the last 24 hours?”
`Security` · blocked, would-block and audited totals

“Which WAF rules match most often this week?”
`Security` · the busiest rules and attack groups

“Is the WAF on for the orders service, and in which mode is each listener?”
`Security` · WAF coverage and each listener's mode

“Which rule blocked the most on orders today? Show me one of those requests.”
`Security` · top rules, then the events

“Is anyone probing the payments namespace?”
`Security` · callers denied on some paths and served on others

“How do I allow large uploads through the WAF?”
`Docs` · the Greymatter documentation

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Key takeaways

1

The edge and inside

A team turns the firewall on at the edge and on the services it chooses, so internal calls to them are inspected too.

2

A proven rule set

The OWASP Core Rule Set ships in the data plane and works in disconnected networks.

3

Detect, test, enforce

Detect mode is the default. Offline replay and per-path exceptions make enforcement safe.

4

Blocked before the service acts

In enforce mode, a denied request never reaches the service.

5

The caller on every event

The firewall runs after identity, so each event names who sent the request.

6

Reported where analysts work

The WAF page, the Forensic Audit and Ask Greymatter all read the same record.

IN ONE SENTENCE

Greymatter puts the OWASP Core Rule Set at the edge and on the services a team picks, and records every decision with the caller.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Greymatter.io

At the edge. Inside the mesh. One record.

LEARN MORE

greymatter.io

Greymatter.io is a trademark of Greymatter.io, Inc.

© 2026 Greymatter.io, Inc.