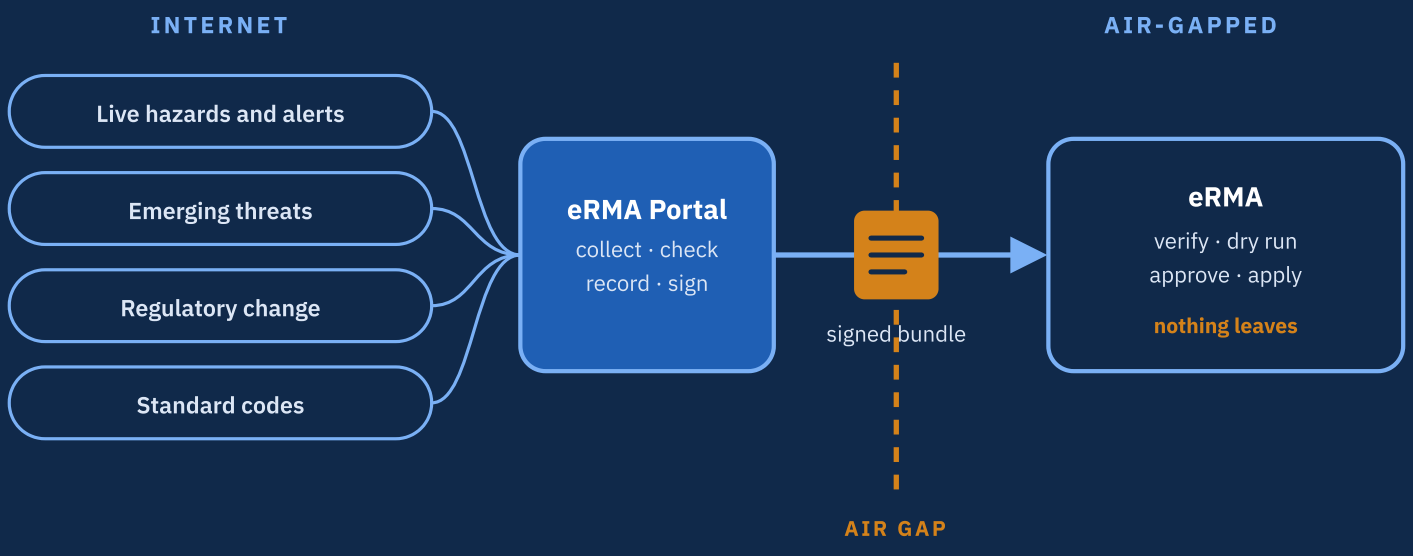
eRMA Portal Services

Eyes and ears on the world, for your resilience programme.

Live hazards, emerging threats and regulatory change from trusted sources worldwide, brought to your eRMA, air gap included. The outside facts that keep a resilience programme honest and reliable.

EDITION PS-01 · OCTOBER 2026



Every source fetched once, worldwide. Every file signed, addressed to one deployment, and checked before it is used.

EYES AND EARS · EMERGING THREATS · REGULATIONS · HONEST AND RELIABLE

WHAT PORTAL SERVICES DOES

A resilience programme is only as good as its view of the world outside.

Your BIA, risk ratings and plans were set on a picture of the world taken at one moment. The world keeps moving. Portal Services watches it for you and brings what matters into eRMA, where it meets your services, sites and obligations.

Eyes and ears

Live warnings from national weather and emergency services, filtered to your countries and shown on the eRMA map against your sites and what depends on them.

→ **Know as the authority knows**

Emerging threats and regulations

What is coming, not only what is here: new and changed rules from regulators, cyber advisories, sanctions and new hazards in your footprint, each raised for review.

→ **See change before an audit does**

Honest and reliable

Outside facts test your assumptions. Every fact is signed, sourced and dated, and data that is late or missing is shown as such, never hidden.

→ **A programme you can stand behind**

KEEPING THE PROGRAMME HONEST

What the programme assumes	What the outside world says	What eRMA shows
A site is safe to work today	A flood or storm warning is issued for that area	The alert on the map against the site and what depends on it
Hazard ratings still hold	Warnings keep arriving for a place rated low	The evidence to revisit the rating, alert by alert
Obligations match the rule in force	The regulator publishes a new edition or circular	*Source changed, review* against the obligations you loaded; never a silent update
Controls cover today's threats	A national CERT lists a newly exploited vulnerability	An advisory to check against your applications and controls
Records are coded alike	A standards body revises a code set	One standard set, with its version, in every deployment
The data is current	A source has stopped updating	The channel marked Stale, with the reason, so no one plans on old facts
"How did you know?"	The auditor asks for the basis of a decision	Every item traced to its original document and fetch time

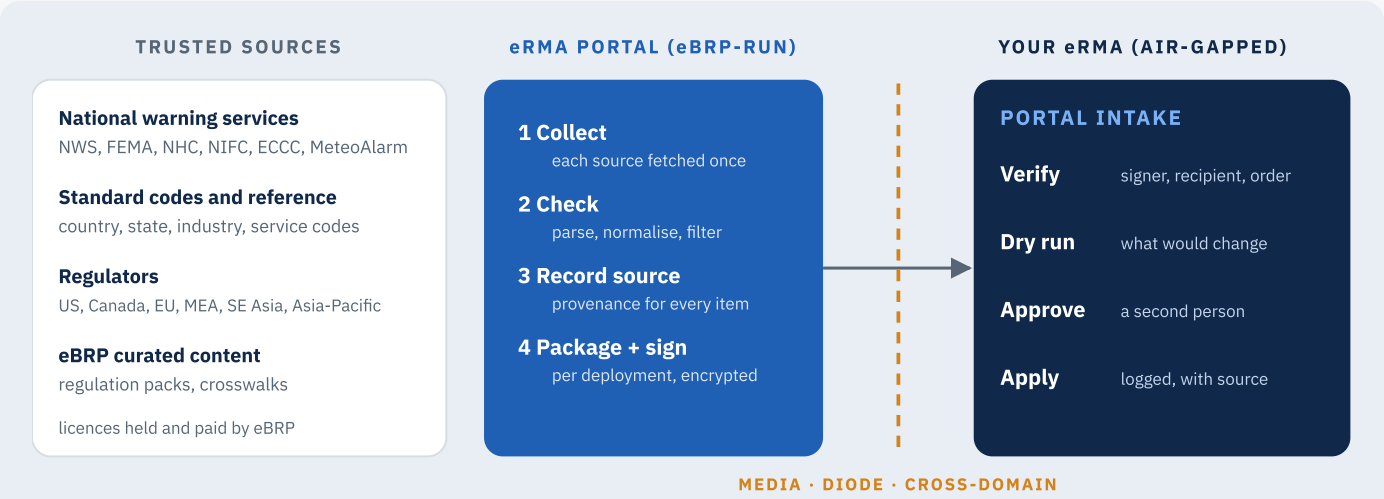
Reliable because every fact is signed, sourced and dated. **Honest** because what is late, missing or switched off is shown, not hidden. **Secure** because it reaches your eRMA without opening a single connection.

© 2026 eBRP Solutions. All rights reserved.

HOW IT REACHES YOU

Outside intelligence, for an eRMA with no route outside.

eRMA is deployed air-gapped: the server holding your dependency graph, recovery objectives and plans has no connection to the internet. Portal Services collects and checks the outside data on the internet side, then delivers it as a signed file that your team carries across.



The bundle is the only thing that crosses. eRMA never calls the Portal, and nothing leaves the high side unless you choose to carry it.

Air-gapped by design

Every feature works when the only link is a person carrying a file. Faster links carry the same file; they never add a different feature.

→ No firewall rule to defend

Nothing leaves the high side

Your site list, your register and your applicability decisions stay in eRMA. The Portal knows only the countries and sectors you choose to tell it.

→ Your footprint stays yours

eRMA keeps working

Every page fed by the Portal shows *data as of* and a state per channel: Fresh, Ageing or Stale. Late data is flagged, never removed.

→ A delay, never an outage

One global source

Each source fetched once, worldwide, with every licence held by eBRP. Countries, states, industries and services carry one standard code in every deployment.

→ One source of truth, one agreement

© 2026 eBRP Solutions. All rights reserved.

1 How a bundle crosses the gap

A bundle is one signed file made for one eRMA deployment. It answers two questions before any record changes: *did eBRP make this?* and *was it meant for us, untouched, and in order?*



Low side on the left, high side on the right. Steps 5 to 8 run inside eRMA, on your hardware, under your teams.

Signed and addressed

Every manifest is signed (ECDSA P-384) by a Portal key certified by eBRP's offline root, and names one recipient deployment. eRMA refuses a bundle addressed to anyone else, and any file the manifest does not list.

→ **Proof of origin on every file**

Encrypted when it matters

Licensed content is encrypted with AES-256 to your deployment's own key, generated on your side and never sent to eBRP. Public-only bundles can stay readable for your transfer officer.

→ **Only your eRMA can open it**

Ordered and replay-proof

Each bundle carries a sequence number, the hash of the one before and an expiry date. Old, replayed or out-of-order bundles are refused, and a gap is shown. A snapshot bundle starts a new deployment or closes a long gap.

→ **Data can never be rolled back by a file**

Two people to apply

One person stages a bundle, another approves it. On by default for every channel that changes records; switching it off is audited with who and when. Live feeds may be set to apply once verified.

→ **Segregation of duties at the gap**

A switch for every feed

Each feed has a key that eBRP or your administrator turns on or off, with dates. The key list travels signed in every bundle, so eRMA also refuses data for a feed that is switched off.

→ **You decide what reaches the high side**

Intake log

Every bundle seen is logged: file, hash, sequence, signature and recipient checks, who staged, who approved, what changed per channel and any error. Kept seven years by default.

→ **Every change traced to its file**

Three ways across, one file format. Carry bundles on approved media or through your cross-domain solution into a drop folder, through a one-way data diode fed by a Portal Relay in your DMZ, or, where policy allows, by a restricted pull from the Relay over mutual TLS.

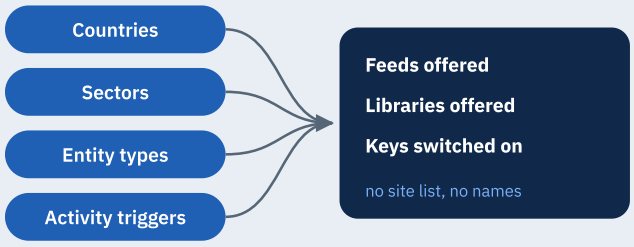
© 2026 eBRP Solutions. All rights reserved.

2 What the Portal delivers

Hazards, threats and regulatory change travel in channels. Each lands where eRMA already looks: the map, Location Operations, risk and compliance.

Channel	What it carries
Live feeds	Hazard and alert feeds filtered to your countries: US (NWS, FEMA, NHC, NIFC), Canada (ECCC), Europe (MeteoAlarm, 39 countries). More national warning services are added in your footprint's order.
Boundaries	Country boundaries for the world or a deployment's scope. Where a country's law prescribes how its borders are drawn (India, for example), a deployment there gets that point of view.
Reference	Public holidays from sources that allow commercial redistribution, time zone data, currencies and units.
Map	Base map tiles rendered from OpenStreetMap for your area of interest, served by eRMA, and an offline gazetteer so address lookup never leaves the high side.
Regulatory	Signed regulation packs curated by eBRP, every release kept and adopted by your choice; change notices from regulators in the US, Canada, the EU, the Middle East and Africa, Southeast Asia and Asia-Pacific, raised for review.
Standard codes	The single source for the codes every record uses, each with scheme and version: countries and regions (ISO 3166-1, UN M49), states and provinces (ISO 3166-2), industries (NAICS, ISIC), services and products (UN CPC, NAPCS), time zones and currencies; LEI for the entities you register.
Cyber and third party	National CERT advisories, exploited-vulnerability lists, and sanctions lists linked to vendor records.
Your own channel	Your low-side data for your high side, such as an internal threat feed or your own map layers. Encrypted; never visible to other customers or to eBRP staff.

YOUR FOOTPRINT DECIDES WHAT IS OFFERED



Declared on the Portal at country level. Detailed applicability is decided in eRMA, on the high side.

Scope per deployment

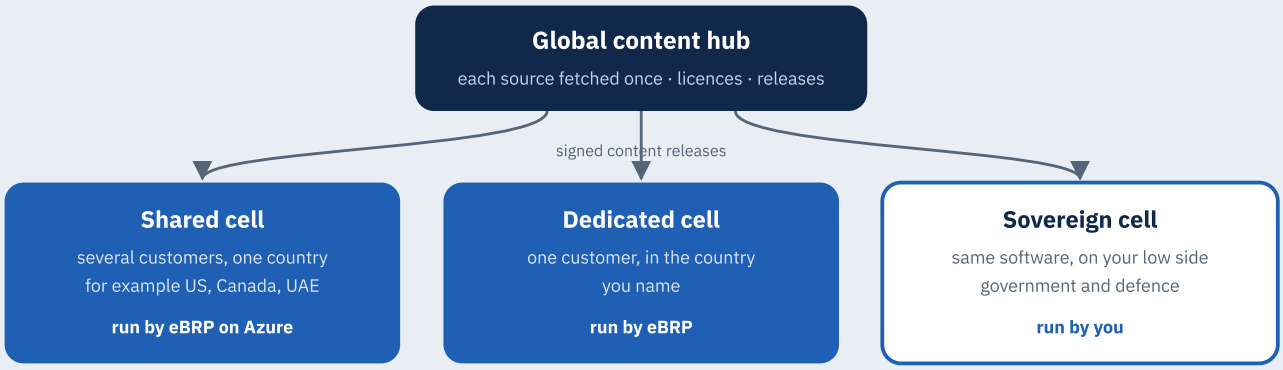
Run separate eRMA installs for the Americas, Europe or a country whose data law asks for it. Each takes a subset of your countries and receives only what is in its scope.

→ **One contract, many installs**

© 2026 eBRP Solutions. All rights reserved.

3 Hosted where you need it

Built for multinationals: your home is where you buy and where your Portal data lives; the content you need follows your footprint and is global. One content hub serves every customer; your data sits in a cell you choose.



Customer data never leaves its cell. The hub keeps only a register of customer codes, names and cells.

A database of your own

Each customer has its own tenant and archive databases. No query joins two customers, and the build for one customer runs with a credential that can open only that customer's data.

→ **Isolation you can show an auditor**

Roles held by groups

People sign in through your own directory. Administrator, subscription manager, content publisher and auditor roles go to directory groups, never to named people. Machines use certificates over mutual TLS.

→ **Access follows your directory**

No eBRP access by default

eBRP operators run the service without seeing your content. Support access needs a grant of at most eight hours, approved by your administrator and shown to your auditors.

→ **You hold the key to your data**

Two-person rule for keys

Signing keys sit in a hardware security module, are rotated yearly and can be revoked inside a bundle. Key and certificate actions need two security officers.

→ **No single person can sign alone**

Your time, your country

Each deployment records the country and time zone it runs in. Build windows follow local time, and delivery rules for that country are checked; a refusal names the rule.

→ **Global service, local rules**

Simple commercial model

One base fee per customer covering production, test and DR deployments, with channel tiers on top. Source licences are included: eBRP holds and pays them.

→ **No feed contracts to manage**

© 2026 eBRP Solutions. All rights reserved.

4 Evidence and assurance

Outside data you rely on in a crisis has to stand up to an auditor afterwards. The Portal records where every item came from and who did what, and keeps it as evidence.

Provenance for every item

For each document fetched: source, time, SHA-256 of the raw file, licence and parser version. In eRMA an item reads *Source NWS, fetched 14:02 UTC, Portal bundle 41*.

→ From alert back to source in one step

Tamper-evident audit

Sign-ins, administrative changes, keys, support grants and every bundle built are written to an append-only ledger, each entry chained to the one before, so editing or deleting one is detectable.

→ An audit trail that proves itself

Signed audit export

Your auditors export your audit records for a period as a signed file and check it offline with a small published tool. The export can be carried to the high side and attached to the intake log.

→ Evidence your auditor can verify alone

Retention and legal hold

Evidence is kept by class: raw source documents 13 months, bundles 90 days, audit and releases seven years. A legal hold on your tenant stops every purge.

→ Kept as long as you must keep it

Usage and delivery reporting

Dashboards for your administrators and auditors: data received per channel, bundles built, applied or missing, freshness against target and API usage, with signed scheduled reports.

→ Delivery you can measure

Source health

The Portal watches every source: last success, success rate and licence state. When a source fails, the next bundle tells eRMA, so your team knows why a channel is stale.

→ No silent gaps

SECURITY AND ASSURANCE PROGRAMME

Area	Approach
Transport and APIs	TLS 1.2 or later (1.3 preferred); mutual TLS for deployments; versioned REST API with a published OpenAPI 3.1 description, rate limits and idempotent writes.
Cryptography	FIPS 140-3 validated modules (Windows CNG in FIPS mode, cloud HSM); offline root key; yearly key rotation with revocation lists carried in bundles.
Certification	SOC 2 and ISO/IEC 27001 control frameworks, with controls mapped to NIST SP 800-53; FedRAMP Moderate for US federal customers of the hosted service.
Customer evidence	Evidence packs aligned to Canada ITSG-33 and Protected B, KSA NCA ECC and CCC, and the UAE Information Assurance Standard.
Service levels	Hosted availability of 99.9 % per cell, recovery point 15 minutes, recovery time 4 hours. A Portal outage delays data; it never stops eRMA.

© 2026 eBRP Solutions. All rights reserved.

eRMA Portal Services

Give your resilience programme eyes and ears on the world.

Ask for a walk-through built around your own footprint. We follow one alert from a national warning service, through a signed bundle and a two-person approval, to the map and the sites it affects in eRMA.

Eyes and ears | Emerging threats | Regulatory change | Honest and reliable | Air-gapped by design

THE WALK-THROUGH



eBRP Solutions
Mississauga, Ontario

web: www.ebrp.net
contact: info@eBRP.net

© 2026 eBRP Solutions. All rights reserved. eRMA and eRMA Portal Services are products of eBRP Solutions. Brochure edition PS-01, October 2026.