KAIA-OR · DATASHEET · ENTERPRISE

Only the events that touch your sites, each showing how well it's corroborated.

Hazards, security incidents, disruptions and cyber events matched to your sites, software and suppliers in one shared picture, each with severity, confidence, source and why it matched.

DOCUMENT ID	DS-ENTERPRISE
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Chief security officers and their security operations, travel risk, executive protection and cyber teams

Who it's for

Security leaders who run a security operations centre, travel risk, executive protection or cyber function, and who need one picture they can act on and brief from. KAIA-OR Enterprise gives the organization a shared picture of its sites, software and suppliers, while each person keeps their own KAIA-OR.

The challenge

- **Too much noise.** Generic alerts wear teams down, and the event that actually touches a site is easy to miss.
- **No one can act on an unconfirmed report.** Without a clear view of severity, confidence and corroboration, teams cannot brief leadership or decide.
- **Teams in silos.** Physical, travel, executive protection and cyber teams work from separate tools, so the relationships between events are lost.

> In a 2026 survey of risk experts, cyber incidents were the top global risk for the fifth year in a row, at 42% of responses; business interruption ranked third, and natural catastrophes fifth, at 21%.[1]

What you get

Physical, cyber and supply chain in one picture

Hazards, incidents and disruptions on your sites; major breaches and newly exploited vulnerabilities that touch the software you use; and the suppliers exposed to them.

Confidence you can brief leadership on

Each event carries its severity, confidence, source and corroboration status, and unconfirmed reports are labelled.

Staff abroad: what changed, and a second look

Each traveller sees which events touch their trip and what changed in the official travel advisory, and gets a second look at suspicious messages and links. The organization sees its sites, not its people's whereabouts.

Your events in your own tools

Send events and their evidence into your own tools through a documented API and webhooks.

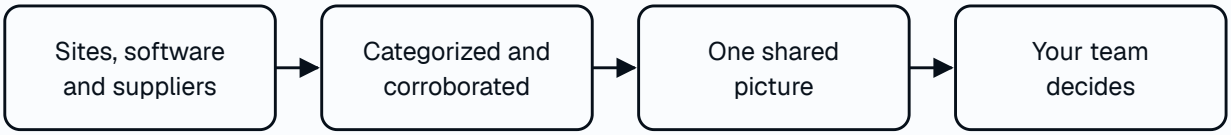
© Kaia Technologies, Inc.

AI under evidence

Answers are checked against the evidence and cite it. Model output grants no authority, and scanning agents act only within the limits you set and with your authorization.

© Kaia Technologies, Inc.

A day with KAIA-OR



One shared picture for the organization; each person keeps their own KAIA-OR.

1. The security team adds offices, data centres and key suppliers, and the software the organization depends on.
2. When a newly exploited vulnerability touches software the organization uses, it appears in the same picture as the sites, with the suppliers exposed to it.
3. When a hazard or incident report concerns a site, the team sees its severity, confidence, source and corroboration status. Unconfirmed reports are labelled.
4. The team briefs leadership from that picture and sends the event into its own tools through the documented API.
5. A traveller abroad sees what changed in the official travel advisory for their destination and gets a second look at a suspicious message.

Privacy and control

- The organization sees its sites, not its people's whereabouts. Each traveller's exact location stays on their own device.
- Roles manage membership, not people. Membership never grants access to another member's messages, devices, location or saved places. These membership boundaries, and the isolation between organizations, are enforced at the application layer.
- Nothing goes to cloud AI unless you agree first.
- Members sign in through the organization's own identity provider. Owners and Administrators download dated access reviews and see who changed what, and when.

Enterprise and government readiness

KAIA-OR fits the identity, security and governance tools an organization already runs.

© Kaia Technologies, Inc.

Capability	What it means for you
Single sign-on and provisioning	Members sign in through your identity provider, and SCIM 2.0 creates and removes their accounts as your directory changes.
Passkeys and authenticator sign-in	Sign in with a passkey, or with your password and an authenticator app as a second step. Sign-in codes are never sent by text message.
Least-privilege roles	Define your own roles beside Owner, Administrator and Member, each with only the permissions it needs.
Audit log export	Export the organization audit log to your own security tools, beside the dated access reviews you already keep.
Data residency choice	Choose the region where your organization's data is held.
Cloud AI under your control	Turn cloud AI features off for your workspace. The control only restricts: it never turns cloud AI on for a member and never overrides a member's own choice.
Your tools, through the API	Send events and evidence to your own systems through the API and webhooks.

Platforms and languages

Platforms	iOS, iPadOS, macOS, Android phones, Android TV, Windows and the web.
Languages	English, French (Canada), Turkish and Hebrew, with full right-to-left layout.

One account works on every platform, with the same features and the same privacy rules.

Package

KAIA-OR Enterprise. See Packages on the KAIA-OR website.

Request early access

> Membership is by invitation. Request early access on the KAIA-OR website and choose Enterprise, or choose Contact us on the KAIA-OR website.

© Kaia Technologies, Inc.

Sources

1. Allianz Commercial, Allianz Risk Barometer 2026, January 2026. Market context only.

© Kaia Technologies, Inc.

DS-ENTERPRISE · Version 1.0 · 3 November 2026

Capability availability depends on the edition and deployment. Capabilities are described as the committed KAIA-OR product scope.