

See the Full Story Behind AI on AWS

Connect agents, identities, and AWS activity to secure AI with confidence

SOLUTION BRIEF

The Challenge

AI on AWS can invoke models, call tools, and reach sensitive data in a single workflow. Teams building with Amazon Bedrock and Amazon Bedrock AgentCore need to know which agent acted, whose permissions it used, what it accessed, and whether that behavior was expected.

Those answers span AI services, cloud logs, identities, and the systems agents touch. An allowed API call can still be risky. Without a connected view, security reviews slow production adoption, and teams struggle to distinguish normal automation from credential misuse or unintended agent behavior.

The Solution

Exaforce connects available Bedrock and AgentCore signals with CloudTrail, IAM context, and connected identity and security tools. Session stitching links agents and workloads to role sessions and observed actions, creating an evidence-linked timeline with the identity, resource, and behavioral context to assess risk.

Teams investigate that timeline in natural language and review the evidence behind each assessment. AWS controls enforce access boundaries; Exaforce adds context to understand activity and guide action. The same platform connects AI activity with broader cloud, endpoint, and SaaS evidence, helping teams move AI workloads into production with confidence.

KEY HIGHLIGHTS

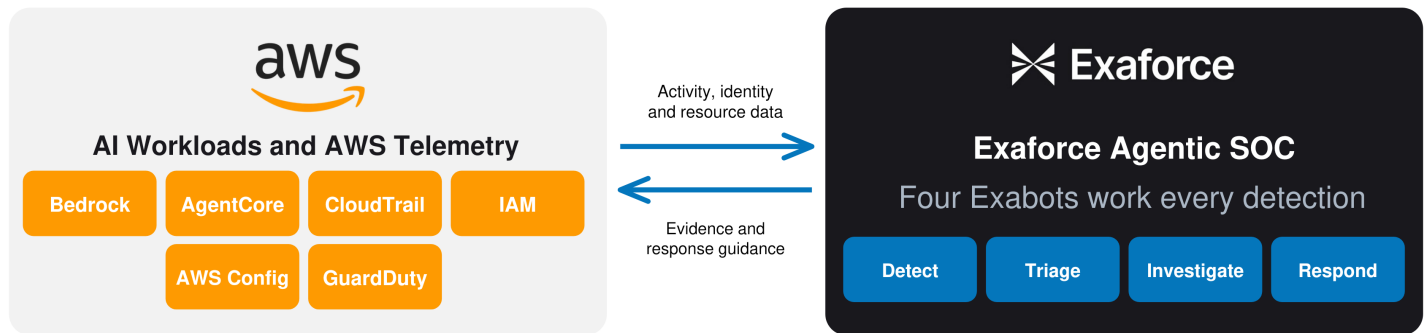
- ✓ **Visibility into AI activity on AWS and the resources it touches**
- ✓ **Agent identity, permissions, and ownership context**
- ✓ **Session stitching across agents, roles, tools, and accounts**
- ✓ **Natural-language investigation with linked evidence**
- ✓ **Behavioral risk assessment and guided response**

Key Use Cases

USE CASE	SOLUTION	BENEFITS
Overprivileged agent identities	A Bedrock-powered support agent reads a finance S3 bucket. Exaforce connects the role, owner, permissions, and observed access to reveal unexpected reach beyond its normal workload.	Identify risky access and give owners evidence to refine least privilege.
Risky tools and skills	An AI coding assistant uses AWS credentials from a developer's device. Exaforce assesses connected skill and MCP data, then correlates credential-access risk with endpoint and AWS activity.	Expose tool risks that can put AWS credentials and data within reach.
Auditable AI activity	A Bedrock agent accesses customer records through a tool. Session stitching connects available agent, role, tool, and data-access events so reviewers can reconstruct the session and identify affected resources.	Answer who acted and what was accessed with a traceable activity history.
Off-pattern agent behavior	An AgentCore workflow starts making repeated writes to a new S3 prefix. Exaforce assesses the activity against the agent's and owner's history, prioritizing unexpected bursts for review.	Bring context to human oversight and help owners address unintended behavior.

How it Works

The Integration at a Glance



Operational Outcomes

AI VISIBILITY

connect AI activity to owners, permissions, and affected resources

NATURAL LANGUAGE

ask questions of the evidence without writing a query

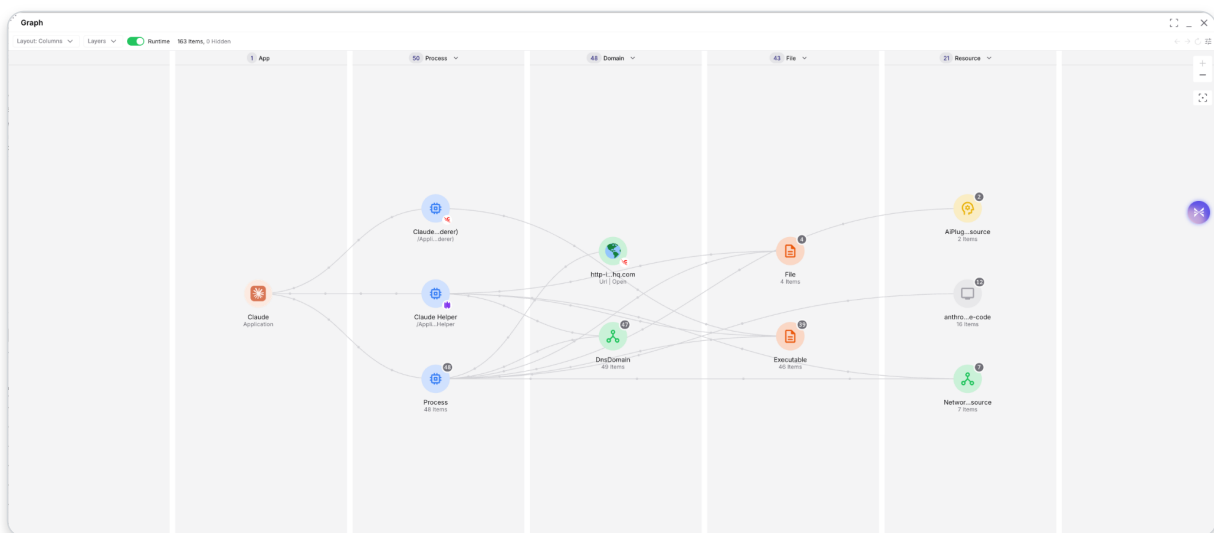
SESSION CONTEXT

follow agent and AWS actions as one connected timeline

INFORMED OVERSIGHT

give teams the evidence to approve, investigate, or restrict activity

Exaforce collects AWS telemetry through least-privilege, read-only cross-account roles. CloudTrail supplies API audit records for Bedrock and AgentCore; S3 data events record object reads and writes. Relevant AgentCore and S3 data events must be explicitly enabled. IAM supplies permission context, while AWS Config, VPC Flow Logs, and GuardDuty findings enrich investigations where connected. Detailed agent/tool traces require enabled application or AgentCore observability logs; model inputs and outputs require separate Bedrock invocation logging for supported APIs. Identity, endpoint, and repository data add ownership and tool context. Coverage follows enabled logging and connected sources.



Exaforce's runtime graph connects an AI application to its processes, domains, files, and resources.

Session stitching connects AWS audit events with agent/tool evidence using role sessions and available correlation identifiers. Exaforce evaluates unusual role use, new resource access, and unexpected activity bursts against behavioral context, then presents findings with supporting evidence and unresolved questions. Teams can ask, "Which resources did this agent session access?" and explore the answer in natural language. These insights help owners refine IAM permissions and tool access in AWS, while approved workflows can use existing identity and endpoint controls where supported.

The Integration in Action

A Bedrock-powered support agent on AgentCore begins reading finance records outside its usual scope. This illustrative workflow assumes CloudTrail management and relevant AgentCore/S3 data events, plus connected ownership data and application/tool logs with correlation identifiers.

2:47:00

Detect. Exaforce flags successful S3 GetObject calls by the agent role against a finance bucket, a departure from its usual support-data access.

Stitch. Exaforce uses role-session evidence and correlation identifiers in connected application/tool logs to associate the reads with the agent workflow and its owning team.

Correlate. IAM and resource context show that the role can reach both support and finance data. A recently added tool expands how the agent can use that access.

Investigate. S3 data events identify the objects requested and API outcomes. Connected tool logs help reconstruct the activity and assess whether the new tool explains the unexpected access.

Assess. Exaforce presents evidence of abnormal data access and the permissions involved. The assessment separates confirmed reads from unanswered questions about intent or onward disclosure.

Ask. The reviewer asks, “Did this session access any other sensitive resources?” Exaforce returns an evidence-linked answer across the connected AWS activity.

2:52:00

Act. With approval, the owner pauses the affected workflow and narrows its IAM permissions and tool access in AWS. Exaforce retains the investigation evidence and observes subsequent activity as telemetry arrives.

Give AI room to work, with the context to know when to step in.

About Exaforce

Exaforce helps organizations understand and secure activity across AI, cloud, identity, endpoints, and SaaS. Its platform combines semantic understanding, behavioral baselines, and relationship context to connect fragmented telemetry into evidence-linked investigations. Session stitching follows identities, credentials, and actions across systems, while natural-language exploration helps teams answer questions without building complex queries. AI security benefits from that broader view: an unusual agent action can be assessed alongside the owner’s sign-ins, device activity, and resource access. Teams gain a shared foundation for visibility, risk assessment, investigation, and approved response through existing integrations. Read our [customer case studies](#), explore the [platform](#), or learn more at [exaforce.com](#).

About AWS

Amazon Web Services (AWS) provides cloud services for building, running, and securing applications at scale. Amazon Bedrock supports generative AI applications, and Amazon Bedrock AgentCore provides services for deploying and operating AI agents. Together with AWS identity, logging, and security services, they give customers a foundation for bringing AI into production with access controls and operational visibility. Learn more at [aws.amazon.com](#).

See your AI on AWS in context

Request an Exaforce + AWS demo to connect agent activity, identity, and resource access into one story. Visit [exaforce.com](#) or scan the code to book a demo.

© 2026 Exaforce, Inc. Amazon Web Services, AWS, and related marks are trademarks of Amazon.com, Inc. or its affiliates. Use cases and investigation timings are illustrative. AI Security Solution Brief v1.3.



[exaforce.com](#)