Exaforce

aws

EXAFORCE AND AWS GUARDDUTY

Autonomous cloud detection, investigation, and response on AWS

SOLUTION BRIEF

The Challenge

GuardDuty gives security teams a strong detection signal, but a finding rarely tells the full story. Analysts still pivot through CloudTrail, AWS Config, VPC Flow Logs, identity data, and other tools to determine who acted, what changed, which resources were affected, and whether the activity represents real risk.

That manual work slows decisions and leaves teams evaluating isolated alerts instead of complete attack paths. As AWS environments expand, the challenge is turning each finding into a defensible verdict and the right response, around the clock.

The Solution

GuardDuty remains the detection anchor. Exaforce brings its findings together with CloudTrail, AWS Config, VPC Flow Logs, identity data, business context, and telemetry from the security tools already in place. Its unified security data platform ingests, normalizes, and correlates that telemetry, creating a common foundation for Exaforce to reason across identities, sessions, resources, and behaviors. This reveals what happened, why it matters, and what should happen next.

That shared context powers continuous triage and investigation, evidence-linked verdicts, natural-language exploration and visualization, and automated or human-approved response through existing controls. Exaforce can also create detections from the broader data it analyzes, extending coverage beyond GuardDuty findings. GuardDuty surfaces the threat; Exaforce turns it into a complete, actionable outcome.

KEY HIGHLIGHTS

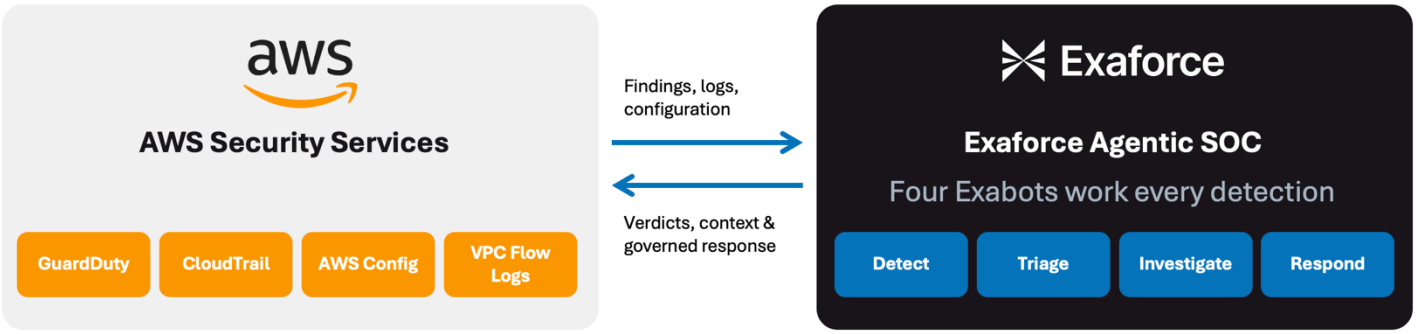
- **24/7 triage and investigation for GuardDuty findings**
- **Identity, session, resource, and business-context correlation**
- **Broader AWS detection coverage beyond GuardDuty findings**
- **Natural-language exploration and visual investigation**
- **Automated or human-approved response through existing controls**

Key Use Cases

USE CASE	SOLUTION	BENEFITS
Context-aware triage & response	Exaforce evaluates each GuardDuty finding against the identity, session, resource, behavioral, and business context surrounding it. Benign activity is closed with a clear rationale; confirmed threats move forward with evidence, root cause, and automated or human-approved response through existing controls.	Faster, more consistent decisions with less manual triage and continuous coverage after hours.
Identity, session & attack-path reconstruction	Exaforce maps roles and access keys to the human or workload behind them, reconstructs every action within the session, and correlates CloudTrail, AWS Config, VPC Flow Logs, and other telemetry into a visual, evidence-linked attack path.	See who acted, what they touched, and why it matters without assembling the story by hand.
Natural-language investigation & detection	Security and DevOps teams can ask questions and visually explore AWS data in plain language, with no SIEM query language. Investigations can be saved as standing detections, extending coverage across the broader AWS environment.	Deep investigation and new detection logic become accessible beyond specialized Tier-3 analysts.

How it Works

The Integration At-a-glance



Operational Outcomes

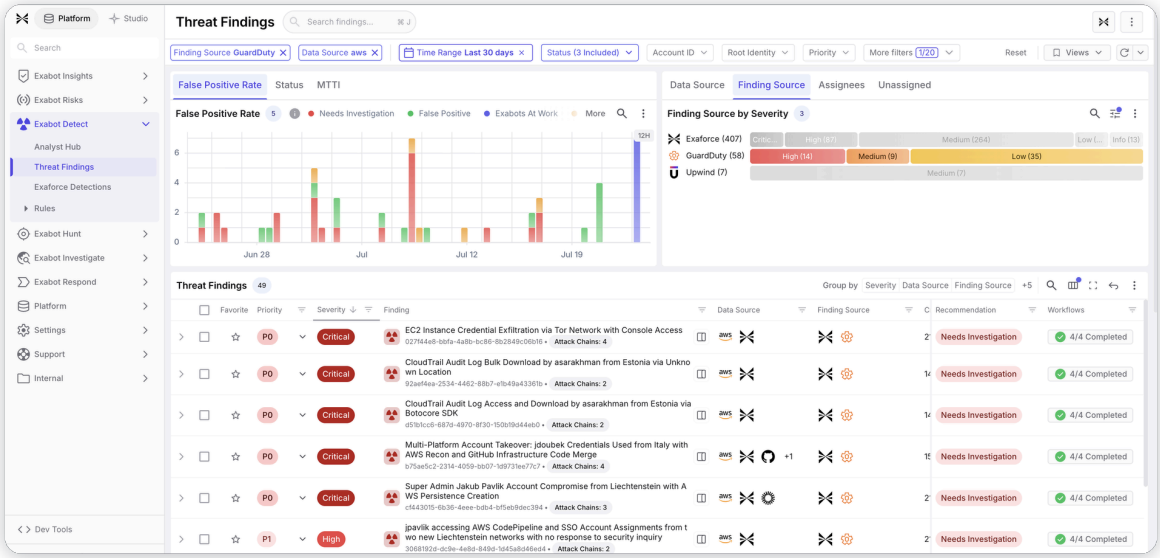
24/7 COVERAGE
autonomous triage and response for every GuardDuty finding

NATURAL LANGUAGE
ask and visually explore your AWS data, no query language

SESSION-BASED
triage on whole AWS sessions, not isolated events

AUTO-RESPONSE
contain incidents with automation in your own controls

Exaforce connects to your AWS accounts in minutes through least-privilege, read-only cross-account roles, ingesting GuardDuty findings, CloudTrail, Config, and VPC Flow Logs alongside the other security tools you already operate. Every finding is enriched with the context analysts normally assemble by hand and correlated into attack chains across those sources. Analysts then see true risk rather than an isolated alert: who acted, what they touched, from where, and why it matters.



GuardDuty findings triaged and investigated in Exaforce, correlated into attack chains with the other security tools you already run.

Exaforce then investigates every finding against a real-time knowledge map of your environment. Benign activity is closed with a clear verdict and rationale. Real threats are investigated end-to-end with evidence, timelines, and root cause. A response is then carried out through the controls you already operate. The net effect: your SOC queue stops growing, and what reaches analysts is confirmed and ready to act on.

The Integration in Action

When GuardDuty raises a high-severity finding after hours, Exaforce immediately begins triage, correlation, investigation, and governed response, while analysts stay in control, asking follow-up questions in natural language at any point.

2:47:00	**Detect.** GuardDuty raises a HIGH-severity finding: API calls from an unfamiliar location using a long-lived IAM access key.
	Triage. Exaforce stitches the key to its identity and the full session: GetCallerIdentity, then bucket enumeration and object reads on a sensitive S3 bucket, judged against how that identity normally behaves.
	Correlate. Exaforce connects CloudTrail, Config, and VPC Flow Logs: the key is a CI-role credential, exposed in a public repository hours earlier.
	Verdict. TRUE POSITIVE, high confidence: credential compromise with S3 reconnaissance, with a full timeline and root cause.
	Respond. Under policy, Exaforce revokes the session, blocks the destination through your existing controls, and surfaces evidence.
	Ask. Looped in on their phone, the analyst asks in natural language, “what else did this key access?”, and gets an evidence-linked answer in seconds, with no query language required.
2:5[illegible]:00	**Escalate.** With data-exfiltration risk, Exaforce escalates key deactivation and bucket lockdown to the on-call analyst, who approves with one click from their phone.

Attackers don’t wait for business hours. Now your cloud defense doesn’t either.

About Exaforce

Exaforce delivers an agentic SOC platform that helps security teams detect, triage, investigate, hunt, and respond to threats with greater speed and consistency. Its task-specific Exabots operate on a shared reasoning foundation and a unified, real-time view of the environment, enabling transparent, evidence-linked decisions across the full SOC lifecycle. Exaforce is available as a SaaS platform or as a fully managed 24/7 MDR service supported by experienced analysts, detection engineers, and incident response experts. The platform is designed for strong tenant isolation and enterprise security requirements, with support for SOC 2, HITRUST, HIPAA, ISO 27001, PCI DSS, and GDPR compliance. Read our customer case studies, explore the platform, or learn more at exaforce.com.

About AWS

Amazon Web Services (AWS) is the world’s most comprehensive and broadly adopted cloud, offering over 200 fully featured services from data centers globally. AWS security services, including Amazon GuardDuty, AWS CloudTrail, AWS Config, and Amazon VPC Flow Logs, give customers the visibility, threat detection, and coverage they need to run their most sensitive workloads with confidence. Learn more at aws.amazon.com.

Request an Exaforce + AWS demo today

See how Exaforce and Amazon GuardDuty close the loop on your own AWS accounts. Visit **exaforce.com** or scan the code to book a demo.

exaforce.com