sysdig | aws

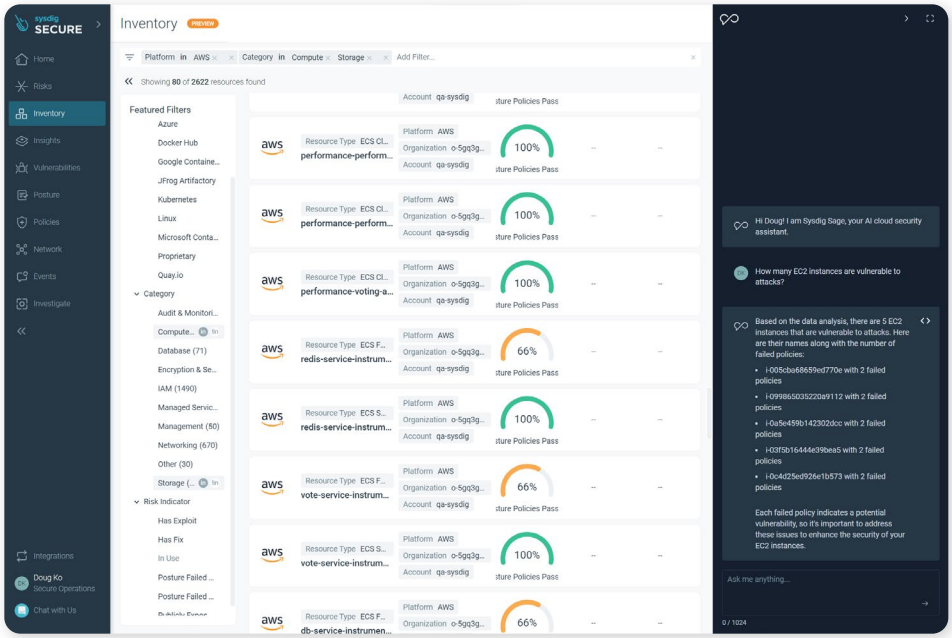
SOLUTION BRIEF

Sysdig Sage and Amazon Web Services (AWS)

Uncover Hidden Risks and Respond at Cloud Speed with the Power of Generative AI

In the cloud, every second counts. Sysdig Sage extends the power of the Sysdig cloud security platform, enabling AWS users to use natural language to identify cloud threats and respond faster. It leverages the power of Sysdig runtime insights to reveal hidden connections between risks and security events that would otherwise go undetected. To achieve this, Sysdig's AI architecture is built on the following foundational capabilities:

- **Multistep Reasoning:** Uses an iterative process to explore multiple investigative steps before providing the most plausible answer.
- **Multidomain Correlation:** Correlates data from vulnerabilities, compliance, permissions, runtime, and CI/CD to get a complete picture of risks.
- **Action Execution:** Makes suggestions on further queries, actions, and next steps, and is able to execute these actions directly from chat.



KEY BENEFITS

- Uncover Hidden Risks and Attack Paths
- Investigate and Remediate at Cloud Speed
- Supercharge Skills with Collective Intuition

> "Having an assistant that provides relevant context during an attack or for day-to-day tasks is extremely valuable. The architectural approach Sysdig has taken with Sysdig Sage is revolutionary and unlike anything we are seeing from other cloud security vendors"

onna
Principal Architect

Beyond a Chatbot - Speed Investigations and Remediations

Organizations have adopted cloud for speed and agility. Security and compliance are the primary considerations for customers adopting the cloud; they would like better visibility to manage their cloud workflows. Generative AI enhances decision-making, helping to prioritize risks, speed response, and simplify cloud security.

Sysdig Sage generative AI security assistant goes beyond typical AI chatbots by providing relevant context to aid your investigation, prioritize risks, and uncover hidden connections. Sorting through security alerts to identify and prioritize risks is time-consuming. To help AWS users protect their businesses, Sysdig Sage is designed to analyze thousands of runtime events, misconfigurations, vulnerabilities, and other anomalies to prioritize critical risks, provide relevant context, and suggest remediations - FAST.

aws PARTNER

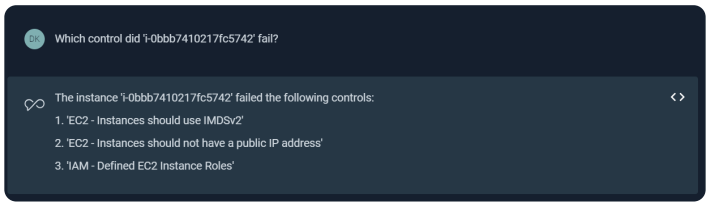
- DevOps Software Competency
- Security Software Competency
- Containers Software Competency
- Cloud Operations Software Competency

KEY USE CASES

- Cloud Asset Inventory Search
- Runtime Event Analysis (coming soon)
- Falco Detection Rule Creation and Tuning (coming soon)
- Attack Path Analysis (coming soon)

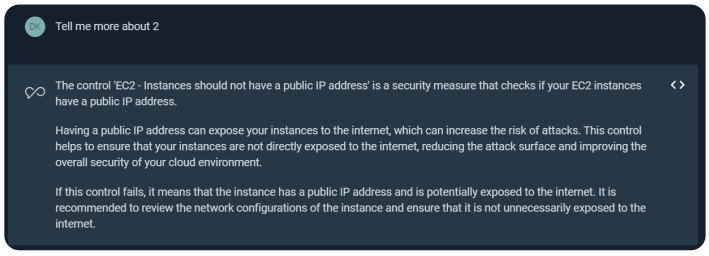
Sysdig Sage - Cloud Speed in Action

Investigate



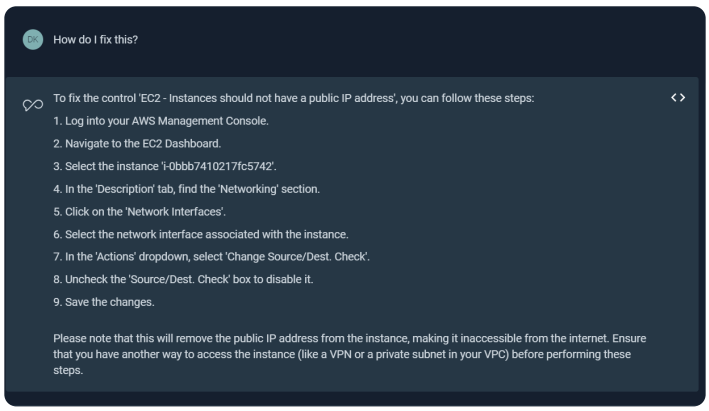
Investigate security risks of your AWS services such as Amazon EC2 instances, Amazon S3 buckets, Amazon ECS containers, and other resources.

Get Context



Get context to help you understand the issue and why it may be posing a security risk.

Remediate



Remediate and fix issues fast with suggested remediation steps.

Secure Every Second

To learn more about Sysdig, visit **sysdig.com.**

LEARN MORE →

sysdig

SOLUTION BRIEF

PB-031 REV. A 11/23