sysdig

BUSINESS VALUE BRIEF

The Business Value of GenAI for Cloud Security

Accelerate human response with Sysdig Sage™

Cloud attacks are constantly evolving, becoming faster and more sophisticated. At a time when threat actors are weaponizing AI and automation to accelerate attacks, security teams must augment defense to stay ahead of threats. Legacy security tools and processes are increasingly insufficient — and inefficient — for teams dealing with the time pressures of modern cloud environments.

In cybersecurity, generative AI has emerged as a powerful tool to help organizations increase the effectiveness of security operations. To date, AI security assistants have provided basic queries and summarization, but more is required to investigate and understand the full picture of cloud threats in real time.

Sysdig Sage, Sysdig's generative AI security analyst, goes beyond simple summarization to thoroughly analyze incidents and accelerate human response. In this brief, you'll discover the impact that a well-designed, autonomous, and comprehensive AI security analyst can make in creating business value through increased productivity, reduction in breach impact, and lower costs of security operations.

Increase productivity, reduce escalations, and lower costs with AI

Organizations investing in the cloud are challenged by the complexity of securing cloud-native applications. The velocity and volume of releases, coupled with the speed of cloud attacks put strain on already taxed security teams. To make matters worse, organizations also report being challenged by a lack of cloud security knowledge and expertise.

According to ESG, in addition to a skills gap, factors like change, complexity, alert volume, and visibility gaps are reported as major challenges for security operations teams.

Biggest SecOps challenges for organizations' cloud applications.

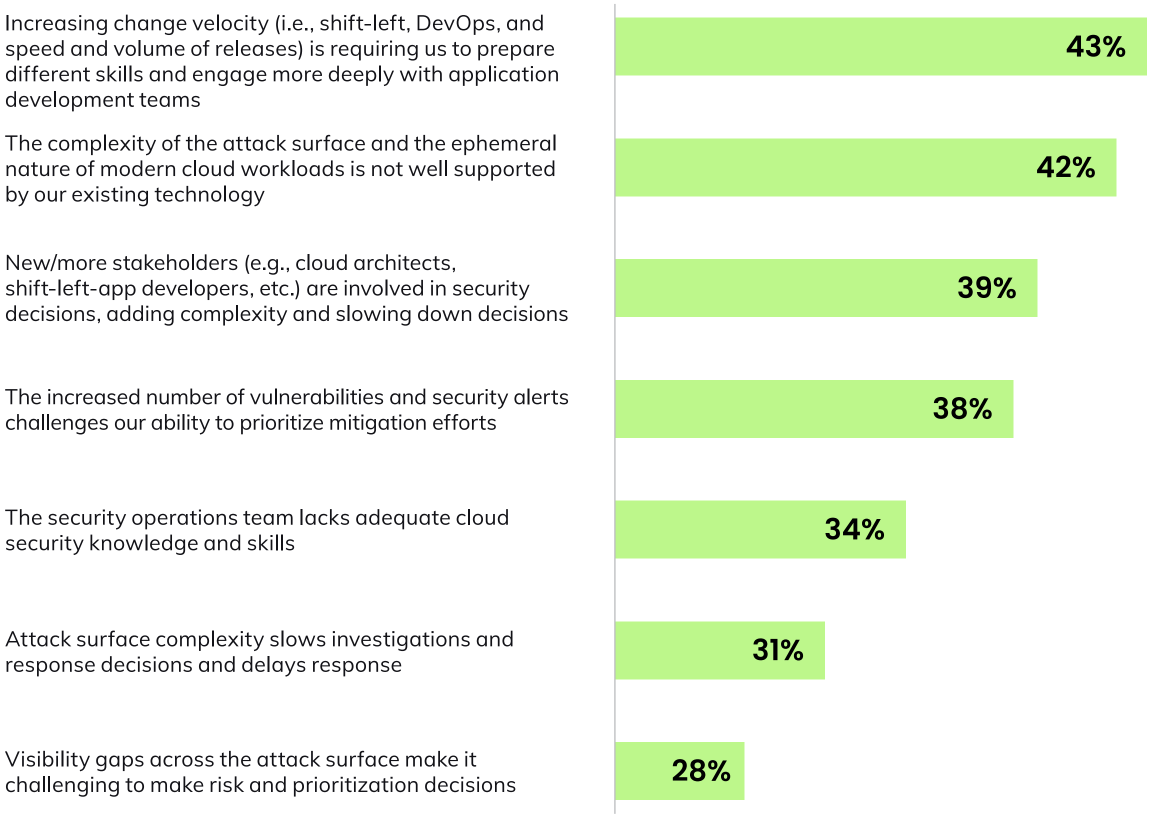


Figure 1: Biggest SecOps challenges for organizations' cloud applications.

ESG Cloud Detection and Response: Market Growth as an Enterprise Requirement Melinda Marks, Senior Analyst Jon Oltsik, Distinguished Analyst and ESG Fellow July 2023.

In 2024, the average total cost of a data breach increased to $4.88 million from $4.45 million in 2023. Unchecked security incidents produce a slew of costly impacts beyond just operational downtime. Serious breaches can result in lost business, lost customers, fines, and the significant cost expended for cleanup and damage control.

Given the potentially debilitating effects a cloud breach can have on a business, taking steps to harden defenses and equip staff with the tools they need as defenders is critical.

Traditional approaches to incident response incur delays as analysts search for details or escalate issues up the chain for deeper investigation. Generative AI (GenAI) has emerged as a top priority for organizations seeking to increase productivity and solve business problems. It holds great potential for aiding cloud security teams in understanding and responding to cloud security issues.

The 555 Benchmark for Cloud Detection and Response — five seconds to detect, five minutes to correlate, five minutes to respond — challenges organizations to acknowledge the realities of modern attacks. Sysdig has calculated that meeting the 555 Benchmark can reduce breach risk by 41% by reducing the likelihood of breaches and limiting the severity of escalated threats.

An AI security assistant trained as a specialist in the domain of cloud security holds the potential to help staff of all skill levels understand threats, and respond quickly and efficiently, to help meet the 555 benchmark — all through a simple conversation.

41%

Reduction in breach risk by meeting the 555 Benchmark.

Measuring the impact of AI on security

Security leaders are looking toward AI and automation solutions to close the skills gap, accelerate incident investigations, and reduce costs. In its most recent annual Cost of a Data Breach Report, IBM found that organizations that applied AI to the security domain saved an average of $2.2 million in breach costs compared to those with no AI use.

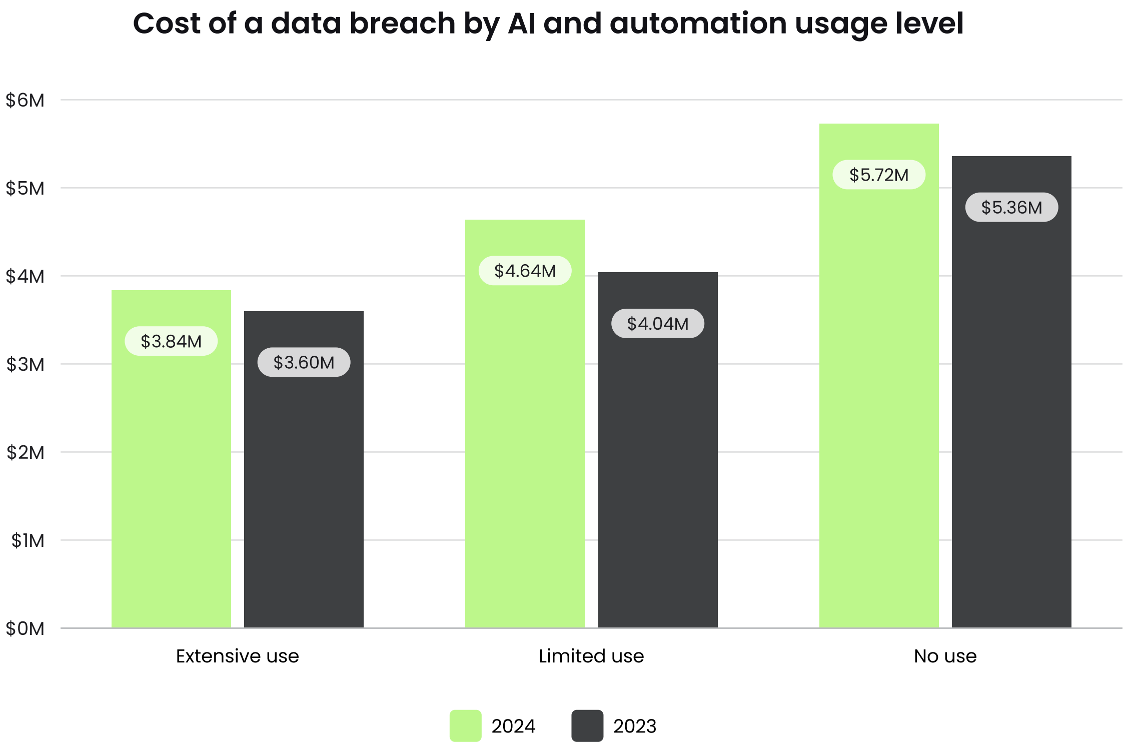


Figure 2: Cost of a data breach by AI and automation usage level

IBM Cost of a Data Breach Report 2024

IBM also reports that the use of AI and automation reduced the average mean time to identify (MTTI) and mean time to contain (MTTC) for investigation and response by 30%.

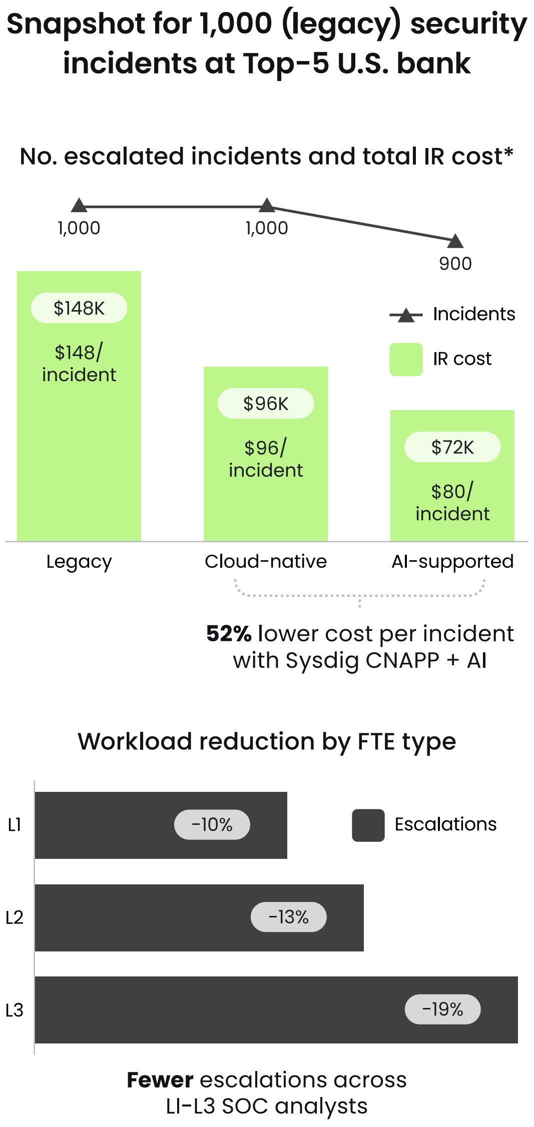
The business value of the Sysdig Sage AI cloud security analyst

Sysdig Sage, Sysdig's AI cloud security analyst, goes beyond simple AI summarization to assist security teams in analyzing cloud security incidents. As an integrated component of the Sysdig cloud security platform, Sysdig Sage turns lengthy investigations into fast, meaningful conversations that focus security teams on the cause of events and solutions to stop detected threats.

Using multi-step reasoning and contextual awareness, Sysdig Sage supports interaction with users through a conversation. Diverse staff of all skill levels benefit from collective industry knowledge and the expertise of the Sysdig Threat Research team. Sysdig Sage enables users to peel back the layers of sophisticated cloud threats and provides instant, in-context recommendations for the next steps to contain a security incident.

Sysdig collaborated with a leading U.S.-based bank to quantify the impact of the Sysdig platform together with Sysdig Sage on its incident response costs.

- The firm estimated a reduction in the cost of incident response by 52% relative to legacy processes.
- 16% of the cost reduction was attributed to the productivity impact of AI assistance.
- The estimated operational cost per 1,000 incidents dropped from $148k before Sysdig, to $72k with Sysdig Sage.
- Total incident escalations reduced up to 19%, saving 388 total working hours for security operations center (SOC) staff.



*Reduce legacy IR duration of 0.5-4 hrs per FTE (L1-L3, $125-$175k annual salary)

Figure 3: Snapshot for 1,000 security incidents at Top-5 U.S. bank

Bank,
Sysdig analysis.

As shown in the above example, rapid investigations powered by Sysdig Sage save security analysts valuable time, empower lower-level analysts to do more, and yield significantly reduced incident management costs.

With the global average cost of a data breach now at $4.88 million, attacks can cost victims tens of thousands of dollars each day they go unresolved. By aiding security teams in the work of investigation and response, Sysdig Sage helps prevent incidents from escalating into breaches, thereby minimizing or even eliminating the associated financial impact.

Empower security professionals with generative AI for cloud security

Cloud ecosystems and technology stacks have become incredibly complex and cloud security teams are under tremendous pressure to respond quickly to threats. Navigating the intricacies of public and private clouds, containers, and Kubernetes is costly and challenging for even seasoned professionals. Utilizing an AI analyst that can instantly deliver the collective wisdom of human experts and the continuous learnings of AI models provides tangible cost and risk reduction benefit.

Sysdig Sage accelerates human response with a purpose-built AI cloud security analyst. When you have only minutes to respond, the ability to have a conversation that helps understand and respond to a cybersecurity event is extremely powerful. Sysdig Sage delivers significant business value by making cybersecurity easier for everyone. It empowers you to take full advantage of the real-time nature of the Sysdig platform to:

- Streamline investigations
- Reduce incident escalations
- Enable employees of all levels to do more

> “Sysdig Sage dramatically reduces the potential for human error and will save us hundreds of hours. It’s amazing how fast we can drill into runtime security issues and explore prevention strategies.”
>
> Vice President, Engineering at a major U.S. bank

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Learn more at sysdig.com.

sysdig

BUSINESS VALUE BRIEF