BRIEF

4 Critical Business Values Delivered by Sysdig Cloud Detection and Response

Security leaders are challenged by the cloud's constantly changing and expanding attack surface that substantially increases the risk of breaches. Detection and response have been disrupted by noise and visibility gaps. Cloud services, containers, and identities sprawl creates a complex environment that is hard to protect and meet compliance on. Meanwhile, threats evolved to exploit any weakness in minutes of exposure and quickly progress attacks to maximum gain. Security teams are looking for solutions that can provide situational clarity, detect threats in real time, and take action so they can better manage risk, stop attacks, and prevent breaches.

See how our customers achieved these goals with the business values delivered by Sysdig Cloud Detection and Response:

- Reduce the risk of breaches.
- Meet compliance requirements in the cloud.
- Reduce time to detect and respond.
- Reduce cost, increase productivity, and securely accelerate innovation.

1 Reduce the Risk of Breaches

Risk is never eliminated but it must be managed, often attempted with a security team that is stretched thin. Breaches are a top business risk leading to costly fines, lawsuits, a decrease in market value, and particularly damaging, loss of trust and confidence. With Sysdig, our customers can better manage risk with a holistic security strategy to detect, in real time, misconfigurations, suspicious behavior, and threat activity in the cloud fabric — users, cloud services, and workloads.

Business values delivered:

- Reduced risk by expanding beyond periodic checks and delayed SIEM threat hunts to real-time intrusion detection across users, cloud services, and containers.
- Scaled security to thousands of cloud accounts, hosts, containers, and serverless without adding overhead.
- Flexibility to scope and tailor security to meet security needs without friction.

> "With the audit log inside our S3 buckets, we gain full visibility of activity, enhancing our monitoring and investigative capabilities. Having this information saves so much time, because without the audit trails, how do you know what happened? Other solutions do not offer this."
>
> *- Natnael Teferi, Lead DevSecOps Cloud Security Architect*
>
> worldpay from FIS

2 Meet Compliance in the Cloud

Cybersecurity laws, regulations, and standards are expanding and becoming increasingly complex, severe, and rigid. For organizations in regulated markets, the existing tools in place were not suited to meet compliance in dynamic and ephemeral environments. Even in less-regulated markets, ensuring security baselines are enforced can be a complex, time-consuming task. With Sysdig, our customers have security designed for the cloud. They not only increase their confidence to pass audits and answer violation questions in case of incidents, but also fundamentally improve their risk exposure.

Business values delivered:

- Met compliance needs (ISO 27001, PCI, GDPR, SOC2) in their cloud environments, including short-lived containers and serverless.
- Up to 50% reduction in operational overhead with streamlined compliance and simplified reporting.
- Expedited clearance of violation investigations with granular forensic data.

> "With Sysdig, it's simply night and day as to how quickly and accurately we can manage compliance. Even more importantly, we can save time and money, as well as avoid costs for being out of compliance."
>
> *- Michal Pazucha, Security Architect*
>
> BEEKEEPER

> "In the PoC, we tested every kind of Kubernetes attack known to us. For example, we created containers that were deliberately vulnerable. We also enacted scenarios where credentials for operations on Kubernetes clusters are stolen. The result was that Sysdig scored highest in 'unauthorized access detection.'"
>
> *- Hiroki Suezawa, Security Engineering Team*
>
> MERCARI

3 Reduce Time to Detect and Respond

Security teams are overmatched by the growing volume, types, and sophistication of attacks. Stolen credentials' availability in the dark web is a breach sentence with every second counting in the aftermath. Sysdig's end-to-end detection with multiple defense layers protects the cloud's attack surfaces and counters evasion techniques, reducing time to identify and stop threats. For our customers, Sysdig not only provides the underpinnings of a cloud-native system, but also serves as the point where all cloud detection and response is done.

Business values delivered:

- Immediate coverage with managed out-of-the-box, multi-cloud detections that combine behavioral, threat intelligence, and ML-based intrusion detections.
- Reduced mean-time-to-respond (MTTR) within SOC with context-rich and MITRE-mapped events.
- Enabled digital forensic and incident response (DFIR) in ephemeral computing with real-time detection and by capturing evidence for forensics.

4 Reduce Cost, Increase Productivity, and Securely Accelerate Innovation

The perennial and increasingly riskier nature of cyber threats is a call for organizations to think strategically. But security teams still struggle with old issues of alert overload, non-actionable events, and inefficient, siloed workflows, leading to wasted time and burnout. Sysdig reduces cost and increases productivity by consolidating tools and automatically prioritizing risk with Runtime Insights — no more wasting time of developers and security teams. For our customers, Sysdig provides a foundational platform where security governance, risk, and compliance scale, and speed can be unleashed.

Business values delivered:

- Consolidate six or more tools into one, realizing significant cost savings.
- Saved time through automation, gaining staffing efficiencies at scale (100k nodes).
- Freed at least one FTE to work on higher-value tasks.

> "At our scale, it is important to have a complete record, even if the containers last only a few seconds. We need to be able to capture this data at scale to conduct not only forensics investigations, but also security audits."
>
> *- Wes Williams, Global Head, Security Incident Response*
>
> Goldman Sachs