

BUSINESS VALUE BRIEF

# 4 Critical Business Values Delivered by Sysdig Cloud Detection and Response (CDR)

Security leaders are challenged by the cloud's rapidly changing and expanding attack surface that substantially increases the risk of breaches. Detection and response have been disrupted by noise and visibility gaps, often due to legacy EDR tooling. Cloud services, ephemeral containers, and identity sprawl create a dynamic and complex environment that can prove difficult to protect and meet compliance on. Meanwhile, threats can exploit weaknesses in minutes of exposure and quickly progress attacks for maximum gain. In fact, the Sysdig Threat Research Team identified that cloud attacks, on average, only need 10 minutes to inflict damage. Because of this, organizations should look to mature their cloud security towards the **5/5/5 Benchmark**. These solutions should provide situational clarity, detect threats in real time, and take a definitive action so they can better manage risk, stop attacks, and ultimately prevent breaches at cloud speed.

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.

# 01 Reduce the Risk of Breaches

Risk is never eliminated but it must be managed to minimize the probability of a major security incident. Breaches are a top business risk that can lead to costly fines, lawsuits, a decrease in market value, and a loss of trust. With Sysdig, customers can better manage risk with a holistic security strategy to detect threats, in real time, across the cloud fabric.

## Business values delivered:

- Reduced risk by expanding beyond periodic checks and delayed SIEM threat hunts to real-time detection across servers, containers and Kubernetes, cloud logs and trails, and serverless environments.
- Enterprise scalability of security to cloud accounts, servers, containers, and serverless without adding overhead.
- Flexibility to scope and tailor security to meet security needs without creating 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.

**worldpay**  
from FIS

Lead DevSecOps  
Cloud Security  
Architect, FIS

# 02 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. 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 (SOC2, HIPAA, PCI, GDPR, ISO/IEC27001, HITRUST) in their cloud environments, including ephemeral 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.

 BEEKEEPER

Security Architect,  
Beekeeper

## 03 Reduce Time to Detect and Respond

Security teams are often overwhelmed by the growing volume, variety, and sophistication of cloud attacks. Sysdig's end-to-end detection and response capabilities enable rapid and scalable protection of today's multidimensional cloud attack surfaces. These advanced capabilities counter advanced evasion techniques and reduce the time needed to investigate and eradicate threats. 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:

Sysdig's end-to-end detection and response capabilities enable rapid and scalable protection of today's multidimensional cloud attack surfaces. These advanced capabilities counter advanced evasion techniques and reduce the time needed to investigate and eradicate threats.

### Business values delivered:

- Immediate and managed out-of-the-box coverage provides multi-cloud detections combining behavioral, threat intelligence created, and ML-based detections.
- Reduced mean-time-to-respond (MTTR) 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 analysis.



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.

**MERCARI** Mercari, Inc.'s  
Security  
Engineering Team

# 04 Reduce Cost, Increase Productivity, and Securely Accelerate Innovation

The perennial and increasingly risky nature of cyber threats is a call for organizations to think strategically. But security teams still struggle with issues of alert overload, non-actionable events, and siloed workflows, leading to lost time and burnout. Sysdig reduces cost and increases productivity by consolidating tools and automating risk prioritization with runtime Insights — no more wasting developer and security team time. For our customers, Sysdig provides a foundational platform where security governance, risk, and compliance scale, so cloud 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 other priority initiatives.



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.

**Goldman Sachs**

**Global Head,  
Security Incident  
Response,  
Goldman Sachs**

## 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](https://sysdig.com).

**sysdig**

BUSINESS VALUE BRIEF

COPYRIGHT © 2023-2024

SYSDIG, INC.

ALL RIGHTS RESERVED.

PB-021 REV. B 3/24