sysdig

BUSINESS VALUE BRIEF

4 Critical Business Values Delivered by Sysdig Cloud Detection and Response

Modern threat actors are escalating their tactics, making attacks faster, more aggressive, and increasingly difficult to stop. Security leaders are faced with a rapidly changing and expanding cloud attack surface that substantially increases the risk of breaches. Legacy endpoint detection and response (EDR) tooling creates noise and visibility gaps.

Meanwhile, threats can exploit weaknesses in minutes of exposure and quickly progress attacks to access sensitive data. 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 **555 Benchmark**. Effective cloud detection and response (CDR) solutions must provide situational clarity, detect threats in real time, and take definitive action to help security teams stop attacks and prevent breaches at cloud speed.

See how our customers achieve these goals with the business values delivered by Sysdig CDR:

- Reduce time to detect and respond.
- Reduce the risk of breaches and minimize incident costs.
- Meet compliance requirements in the cloud.
- Reduce cost and increase productivity.

01 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.

With out-of-the-box detection rules and advanced cloud behavioral analytics, Sysdig detects threats and early signs of compromise, like reconnaissance and privilege escalation, in real time. Our platform streamlines investigations, automating correlation across resources, events, identities, and vulnerability data. These advanced capabilities counter advanced evasion techniques and reduce the time needed to investigate and eradicate threats.

Business values delivered:

- Rapid time to value from out-of-the-box managed policies and behavioral, threat intelligence created, and ML-based detections.
- Reduced mean-time-to-respond (MTTR) with context-rich and MITRE-mapped events.
- Enable digital forensic and incident response (DFIR) in ephemeral computing with real-time detection and by capturing evidence for analysis.

> "I do not want to know when someone's in my environment 15 minutes or several hours later. With Sysdig, we can identify and address potential threats in real time.

BIGCOMMERCE **Senior Infrastructure Security Engineer**

02 Reduce the risk of breaches and minimize incident costs

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, decrease in market value, and loss of trust. If security teams can detect and respond to threats early, they can prevent incidents from becoming breaches, minimizing or eliminating the associated cost.

Real-time detection and response reduces breach risk by lowering the likelihood of breaches and limiting the severity of escalated threats. Sysdig integrates advanced detection with real-time correlation and context, identifying threats and compromised identities at the first sign of compromise, across the cloud fabric.

Business values delivered:

- Meeting the 555 benchmark with an effective CDR solution can reduce breach risk by 41%, potentially saving $1.8 million[1] by reducing the likelihood and severity of breaches.
- Limit downtime costs with rich real-time context to make informed decisions. An hour of downtime typically costs between $145,000 and $450,000.
- Reduce risk by expanding beyond periodic checks to real-time detection across servers, containers and Kubernetes, cloud logs, and serverless environments in a single platform.

> “In the cloud, everything happens fast. Time is of the essence when stopping attacks. Breaches can be very costly. Sysdig enables us to quickly detect and respond to cloud attacks at cloud speed by knowing what is happening, the exact container or location in the cloud, and what is causing it, versus the hours it used to take to detect and understand what needs to be done.
>
> **Platform Tech Team Lead**

1 *Based on average data breach cost of $4.45 million from IBM Cost of a Data Breach Report 2023*

03 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. Detection and response is a key part of most compliance frameworks, and insights from Sysdig CDR are used to improve compliance. Sysdig is designed for the cloud, helping customers confidently pass audits and answer violation questions in case of incidents, but also fundamentally improve their risk exposure.

Business values delivered:

- Meet 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.

> We rely on Sysdig for threat detection in our production environment. The main benefits include a much stronger security position, greater ease in meeting compliance requirements, and simplified evidence collection for audits.
>
> onna **Director of Security**

04 Reduce cost and increase productivity

Security teams continue to struggle with 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, enabling security teams to spend their times responding to real risks rather than noise. Sysdig's deep runtime visibility prevents response from becoming an "all hands on deck" situation that requires increasingly senior level employees, potentially saving hundreds of thousands of dollars per year. Our platform scales governance, risk, and compliance, so cloud speed can be unleashed.

Business values delivered:

- Reduce time and cost of FTEs on investigation and response. One company spent 99 hours on just two security incidents, incurring 20% of the cost of Sysdig in a week.
- Consolidate multiple security tools into one, realizing significant cost savings.
- Save time through automation, gaining staffing efficiencies at scale (over 100,000 nodes).

> "Sysdig has helped automate what would otherwise be a mountain of manual work. We can now not only see our entire Kubernetes environment, but also take more immediate action to address problems or threats."
>
> apree health — **Senior Manager of Information Security**

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**.

PB-021 REV. D 3/25