sysdig

BUSINESS VALUE GUIDE

The Business Impact of Time in Cloud Security

3 Pillars to Secure Innovation in Seconds

Organizations are migrating to the cloud to accelerate innovation. Inherently, with the acquisition of cloud speed comes the risk of faster attacks. Sophisticated attackers are using automation to deliver attacks at warp speed and maximize their blast radius. To combat these attacks, technology leaders must stop attacks and mitigate risk, in real time, across their cloud environments.

Technology leaders are measured on increasing organizational agility, shortening time to market, and accelerating innovation. To do so, they need to enhance developer workflows by removing friction and offloading time-intensive tasks such as vulnerability management. Ultimately, technology leaders need the ability to unlock time so that they can prioritize what matters.

01 Time to Detect and Respond

Accelerating Incident Response

Sysdig's 2023 Global Cloud Threat Report shows that attackers need less than 5 minutes after credential discovery to initiate a targeted attack. Within an additional 5 minutes they can accomplish their goals, whether they be financial, espionage, or ideological. Security teams need to detect in seconds, not hours, to limit the impact of an attack. They also need capabilities that enable them to respond in 10 minutes or less across a diverse set of threats, including malware, anomalous behavior, and malicious misconfiguration, to protect organizational interests.

Business values delivered:

- → Time to detect: < 2 seconds.
- → 5x faster forensic cloud investigations vs. legacy approaches, which saves approximately $1.2 million per organization.*

> 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

> In the past, an investigation could take up to a week. With Sysdig, it's a 5-10-minute job.
>
> Information Security Leader, Security Operations Provider

02 Time to Market

Advance Secure Cloud Innovation

Time can be a critical barrier to continuous integration/continuous deployment (CI/CD), as developers walk the line between secure and continuous cloud innovation. Managing and prioritizing vulnerabilities can dominate DevOps workflows, especially without the appropriate triage and context capabilities. Further, without **runtime insights**, DevOps teams might miss an additional 10% of hidden malicious images that the combination of static analysis and vulnerability scanning can miss, as shown in **Sysdig's 2023 Global Cloud Threat Report**. Security leaders need to enhance DevOps security efficiencies to save time and further drive innovation.

Business values delivered:

- → 95% reduction in vulnerability noise.
- → 10% improvement in time to market.

> We have been able to cut vulnerabilities down by 95%, creating vast time savings with Sysdig runtime insights.
>
> Information Security Leader, Security Operations Provider

> Sysdig saves us 4 hours per week while increasing our releases by 10% per week, without increasing our team size.
>
> ICG CONSULTING BUSINESS PROCESS SOLUTIONS Technical Consultant

Ponemon Institute and IBM Security, Cost of a Data Breach Report, 2023.

03 Unlock Time

Progress Through Consolidation

Technology leaders often struggle to unlock time for key initiatives. Productivity is hamstrung by a never-ending torrent of alerts and complex workflows. Fragmented and incomplete approaches such as stand-alone cloud security posture management (CSPM) and retrofitted endpoint detection and response (EDR) tooling crush efficiency. Technology leaders need a robust and unified cloud-native application protection platform (CNAPP) to consolidate tools and reclaim time.

Business values delivered:

- → 20% time savings by consolidating into an integrated CNAPP, which translates to $800,000 in cost savings for an average enterprise.
- → Consolidate from 6 tools to 1 – 20% cost savings.

> “ With Sysdig, we consolidated 6 tools to 1, saving time and money.
>
> Arkose Labs IT Security Manager

> “ It’s 1 tool for everything. Compared to alternatives, Sysdig improves operations efficiency by 25% and developer efficiency by 20%.
>
> gini Head of Technical Operations

Conclusion

When every second counts, leaders can depend on Sysdig with runtime insights to deliver highly performant protection. Analysts can accelerate incident response and forensic investigations, rapidly mitigate cloud risks, and keep critical cloud and host assets secure. Reductions in noise and friction improve secure cloud innovation and developer time to market. Sysdig’s integrated CNAPP enhances the developer and security analyst experience so that they can save time and focus on priority initiatives.

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.

COPYRIGHT © 2023 SYSDIG,INC.
ALL RIGHTS RESERVED