sysdig

BUSINESS VALUE CHECKLIST

5 Critical Business Values Delivered by Sysdig Posture and Permission Management

In today's rapidly evolving business landscape, ensuring the security, compliance, and efficiency of your organization's digital assets is paramount. The deployment and maintenance of a robust security posture has led to a significant increase in the identification of issues and risk findings. Security, operations, and IT teams find themselves grappling with cloud misconfigurations and security weaknesses, which, in turn, expose organizations to potential threats for extended periods. As a response, security leaders are continuously exploring ways to prioritize these risks, reduce friction, and actively contribute to business growth. See how a handful of customers met their goals with the business values delivered by Sysdig:

- → Identify and Prioritize Real Risk
- → Accelerate Cloud Maturity Based on In-Use Permissions
- → Mitigate Compliance Risk with Runtime Insights
- → Save Time with In-Use Risk Prioritization
- → Reduce Cost by Consolidating Security Tools

01 Identify and Prioritize Real Risk In Real Time

In the Cloud, every second counts. Cloud attackers are quick and opportunistic, spending only 10 minutes staging the attack, while the median dwell time on-premises is 16 days. This shifting threat landscape has prompted organizations to reconsider their approach to Cloud Security Posture Management (CSPM). Our customer, BigCommerce, emphasizes the critical importance of real-time awareness in this context. With Sysdig's innovative approach leveraging runtime insights, BigCommerce is hardened with an intuitive platform for visualizing and analyzing threat data, empowering both security and engineering teams to swiftly identify and prioritize real risk in real time, detecting vulnerabilities, threats, and misconfigurations at runtime. This not only allows BigCommerce for comprehensive security posture tracking, but also ensures compliance with every regulatory requirement they need to meet.

> We like that Sysdig uses knowledge of what is in use during production to help us make better informed posture decisions. The bottom line is that CSPM is Sysdig's bread and butter, and that inspires confidence.

BIGCOMMERCE Senior Infrastructure Security Engineer

02 Accelerate Cloud Maturity Based on In-Use Permissions

90% of granted cloud permissions are not used. Weak or improperly applied identity policies and their particular permissions pose a serious vulnerability in cloud environments. Compromised credentials from identities with privileged access or excessive permissions are a significant security risk. They can lead to unauthorized access, data breaches, and potentially catastrophic consequences for an organization's data integrity, reputation, and overall security posture. Insights derived from IAM data and in-use permissions activity empower organizations to bolster their security, maintain compliance, and streamline operations. This ultimately contributes to improved business performance and risk management. Through continuous monitoring for permission changes, template misconfigurations, and adherence to IAM-related compliance controls, our customer was able to eliminate excessive entitlements. They did this by implementing recommended access policies based on in-use permissions. This allowed them to gain visibility into cloud identities and enforce least privilege in minutes. As a result, they successfully accelerated their journey towards becoming a mature, secure, and efficient cloud enterprise.

> It's critical for us to understand where we have overly permissive identities and due to the scale, we need an automated way to manage them. Trying to abide by the principle of least privilege, eliminating excessive permissions is a top security priority.

Booking.com Senior Product Manager

03 Mitigate Compliance Risk with Runtime Insights

Cloud compliance consists of the procedures and practices that ensure that a cloud environment complies with governance rules. These standards and compliance frameworks often include robust security requirements, ensuring that sensitive data is adequately protected. Meeting compliance standards in the cloud helps safeguard data from breaches and unauthorized access. By using Sysdig, our customer was able to automate the validation of compliance requirements like encrypting sensitive data, ensuring data recovery, and ultimately demonstrating that the organization identifies and addresses potential security issues.

> 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

04 Save Time with In-Use Risk Prioritization

Striking the optimal resource allocation balance within a security program remains a persistent challenge for organizations. At Sysdig, we harness the power of runtime insights to effectively prioritize risks, blending real-time contextual data, including in-use vulnerabilities and permissions, with static assessments, encompassing misconfigurations and known vulnerabilities. Our approach to in-use prioritization has empowered our customers to significantly enhance their risk management efficiency. They have streamlined their efforts by avoiding unnecessary time spent on inconsequential issues, accelerating the resolution of critical misconfigurations, and freeing up resources to be redirected towards more high-impact tasks.

> With previous solutions, we had a lot of alerts that forced us to spend more time triaging what was important and what wasn't. Sysdig enabled us to autotune the solution to focus on the most pressing issues, filter our rules, and reduce the burden of alert fatigue. Within the first few weeks, we achieved a 30% reduction in alerts without sacrificing security.
>
> ICG CONSULTING BUSINESS PROCESS SOLUTIONS Technical Consultant

05 Improve efficiency with Security Tools Consolidation

Managing a diverse set of security tools efficiently while ensuring operational continuity and developer productivity can be a daunting task within cloud environments. As the complexity and scale of cloud-native systems grow, the fragmentation of security tools not only leads to increased costs, but also introduces operational inefficiencies. By adopting a unified CSPM solution that centralizes the oversight of permissions, security postures, and compliance across all cloud environments, the organization has fortified its digital ecosystem with a more robust and effective security strategy. This consolidation has not only streamlined security operations but also optimized cost-effectiveness.

> "Being able to move between our environments allows us to run faster. It's one tool for everything, and not different tools optimized for specific environments. Having this single pane of glass, it doesn't matter where it runs or how it runs. Compared to alternatives, Sysdig improves operations efficiency by 25% and developer efficiency by 20%.
>
> gini Head of Technical Operations