sysdig

BUSINESS VALUE BRIEF

Unlocking Business Value with Enhanced Investigations

Modern cloud attacks are faster and more sophisticated than ever. Threat actors have weaponized automation to accelerate their attacks, swiftly moving between cloud accounts and workloads. When it comes to stopping these attacks, time is the most important factor. The longer a breach lasts, the more data an attacker can exfiltrate and the greater the cost to the organization. With attackers needing less than 10 minutes to execute an attack after identifying an exploit, the ability to conduct investigations with speed is critical.

Unfortunately, most cloud investigations take far too long to enable an effective response. Traditional endpoint detection and response (EDR) tools create visibility gaps and lack the necessary context to quickly understand what occurred in a cloud environment. Without full visibility, security teams are left with incomplete investigations where they can only see a portion of an attacker's actions. Siloed data forces analysts to manually collect and correlate evidence across multiple tools and domains, greatly slowing down remediation actions. Security teams need a tool designed for cloud-native environments that can correlate findings across multiple cloud domains.

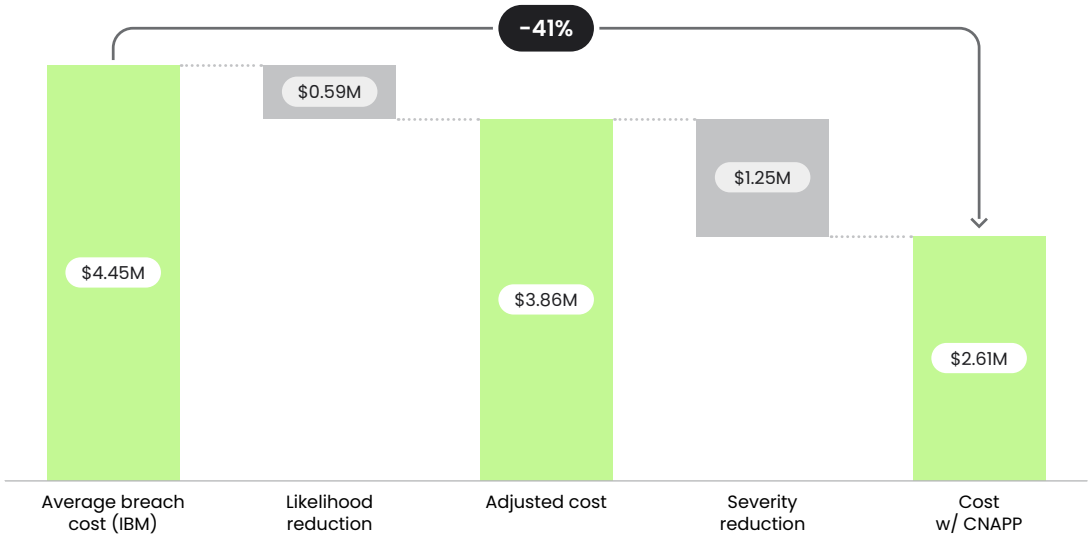
Discover in this brief how Sysdig creates business value and reduces breach costs through our enhanced cloud investigation, rapidly correlating insights and unearthing critical context to help security teams make better-informed, faster decisions.

Minimize incident costs with cloud detection and response

Rapid investigations enabled by real-time detection and cloud-native context not only save security analysts time, but also reduce incident costs. If security teams can investigate and respond before an attack can be executed fully, they can prevent the incident from becoming a breach, minimizing or even eliminating the associated cost. Efficient investigation is also key to containing incidents and reducing breach risk. Time is of the essence when it comes to preventing an incident from becoming a threat to the organization's sensitive data, as the duration of a breach is directly linked to its severity and cost. The global average cost of a data breach is **$4.45 million**,[1] and Sysdig's Threat Research Team has discovered attacks that can cost victims tens of thousands of dollars every day they remain unaddressed.

Incident response can also become an "all hands on deck" situation, requiring not just security practitioners, but developers, network engineers, architects, and leadership. These "war room" situations can cost tens or even hundreds of thousands of dollars annually, depending on the roles involved and frequency. Traditional solutions like EDR lack the ability to correlate across multiple domains and tools, requiring more and more people to fill the gap.

The 555 Benchmark for Cloud Detection and Respose - 5 seconds to detect, 5 minutes to correlate, 5 minutes to respond - challenges organizations to acknowledge the realities of modern attacks. Sysdig has calculated that meeting the 555 Benchmark with an effective cloud detection and response (CDR) solution can reduce breach risk by **41%, potentially saving $1.8 million**[2] by reducing the likelihood of breaches and limiting the severity of escalated threats (see figure below).



Sysdig reduces breach risk by 41%, potentially saving $1.8M given an average breach cost of $4.45M

1 IBM Cost of a Data Breach Report 2023

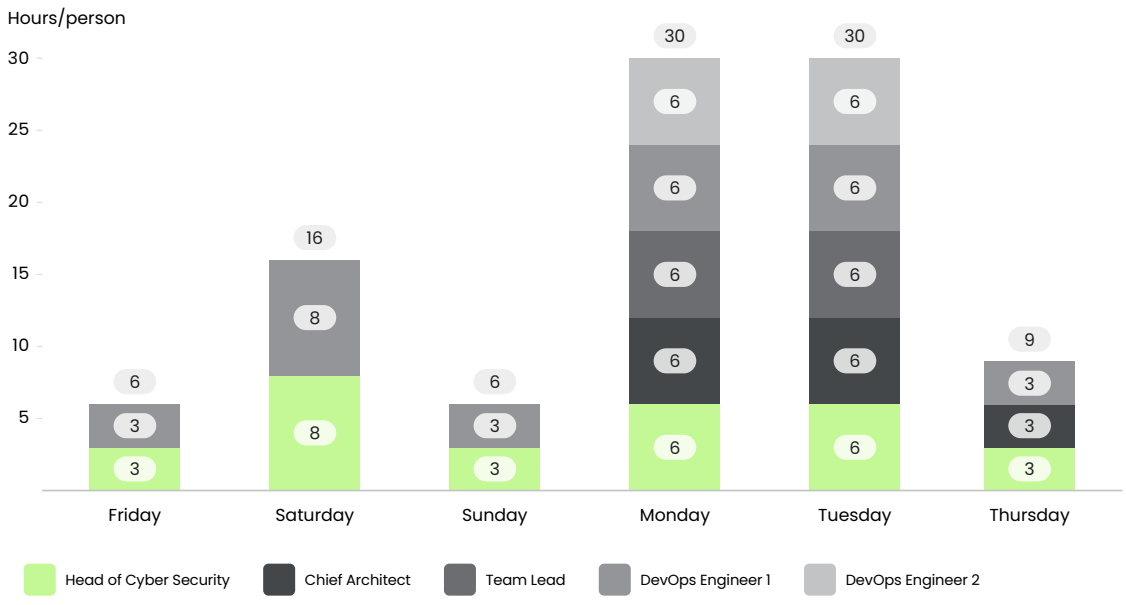
2 Based on average data breach cost of $4.45 million from IBM Cost of a Data Breach Report 2023

Sysdig achieves this by integrating advanced detection capabilities with comprehensive cloud-native context. Our platform streamlines investigations, automating correlation across environments between resources, events, identities, posture, and vulnerability data. This eliminates the manual work of collecting and correlating findings, saving security teams precious time, improving the efficacy of investigations, and ultimately reducing incident costs.

> An effective CDR solution can reduce breach risk by 41%, potentially saving $1.8 million."

Lost productivity from traditional investigations

Using traditional investigation tools, one financial services company expended 97 hours in a single week on just two security incidents. This included time investigating an actual incident, but also a significant amount of time confirming that another did not represent a risk. The incidents required time from five different people, including the Head of Cyber Security and Chief Architect. Based on market rates, **the company incurred 20% of the cost of Sysdig in hours spent for just these two incidents.**



This financial services company spent 97 hours in a single week on just two incidents

Eliminate downtime costs with context-driven decisions

When security teams lack the data to make effective decisions, they face a difficult choice when confronted with an indicator of compromise. They can take immediate mitigation steps, such as taking critical production systems offline, to protect valuable assets and data. However, this can lead to significant downtime and costs, with an hour of downtime **typically costing organizations between $145,000 and $450,000**. This massive potential financial hit makes it crucial to weigh this decision carefully.

On the other hand, with breaches costing companies millions of dollars, delays in taking systems offline can be exponentially more expensive. Adversaries often use simpler attacks, such as deploying a cryptominer, to distract from more complex and damaging activities. This was a key tactic in the SCARLETEEL operation, where the attackers used cryptomining as a distraction to find credentials and steal proprietary software.

The lack of relevant data can result in overreactions and unnecessary downtime, **easily escalating costs to $1 million or more**. This scenario highlights the need for accurate, real-time context to inform decision-making. Legacy tools like EDR lack meaningful multi-cloud insights and context, telling an incomplete story when it comes to cloud attacks. Security teams need the ability to investigate the full attack chain and understand the incident's complete scope.

Sysdig couples real-time insights with automatic cross-cloud context and correlation, helping security and development teams understand the "Five Ws" of a cloud investigation. Our rapid investigation flow enables teams to construct a rich context-driven attack narrative, revealing exactly what actions threat actors took, how they moved through the environment, and correlations between events and identities. Armed with this narrative, customers can make informed decisions about how to mitigate threats effectively without causing harm to the organization's operations and finances.

An hour of downtime can cost organizations between **$145,000 and $450,000**, easily escalating the cost of an incident to **$1 million or more**.

Prevent future incidents by optimizing investigation workflows

Security teams often attempt to stretch their EDR tooling for CDR use cases, but find they do not integrate with other preventative controls. Security and development teams essentially speak different languages when trying to connect the dots. EDR tools lack meaningful context around cloud incidents, compounding these challenges. This perpetuates a lack of collaboration between security teams, developers, and platform teams, weakening organizational posture and making it difficult to prevent future incidents. As an attack unfolds, these teams must work together to mitigate its scope by changing permissions or remediating exploited vulnerabilities.

Post-incident analysis is also essential for mitigating future incidents, as it helps teams understand the initial attack vector and subsequent activities. According to Mandiant, 68% of attacks begin with a vulnerability, phishing attack, or stolen credentials.[3] These entry points can be effectively secured against in the future, but only if an organization thoroughly understands the events leading to the incident. Comprehensive post-incident analysis allows security teams to identify the weaknesses exploited by attackers and strengthen defenses accordingly. This helps mitigate the immediate threat but also provides valuable insights to prevent similar incidents, ultimately reducing repeat incident costs.

Sysdig's enhanced investigation flow combines insights across multiple domains to help analysts collaborate and understand the trajectory of an attack instantly. By centralizing, enriching, and correlating identities with events, security and platform teams can break silos and readily share findings to expedite investigations. Sysdig fosters close cooperation between these teams, enhancing customers' ability to respond to threats in real-time and prevent future breaches. With this rapid understanding of how an incident occurred, organizations can not only limit immediate breach costs but also reduce future expenses by ensuring the same weaknesses are not exploited again.

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

3 Mandiant M-Trends 2023 Report

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-036 REV. A 6/24